GIAC

Exam GSEC

GIAC Security Essentials

Version: 7.0

[Total Questions: 279]

Question No : 1

Which of the following ports is the default port for Layer 2 Tunneling Protocol (L2TP)?

A. TCP port 443
B. UDP port 161
C. TCP port 110
D. UDP port 1701

Answer: D

Question No : 2

What is the process of simultaneously installing an operating system and a Service Pack called?

A. Synchronous Update
B. Slipstreaming
C. Simultaneous Update
D. Synchronizing

Answer: B

Question No : 3

What is the name of the Windows XP/2003 tool that you can use to schedule commands to be executed on remote systems during off-peak hours?

A. SCHTASKS.EXE
B. SCHEDULETSKS.EXE
C. SCHEDULR.EXE
D. SCHRUN.EXE

Answer: A

Question No : 4

How are differences in configuration settings handled between Domain and Local Group Policy Objects (GPOs)?

A. Local and Domain GPOs control different configuration settings, so there will not be conflicts.
B. Settings in the domain-wide GPO override conflicting settings in the local GPO on each computer.
C. Settings in the local GPO override conflicting settings when the domain-wide GPO is applied.
D. Precedence depends on which GPO was updated first.

Answer: B

Question No : 5

When should you create the initial database for a Linux file integrity checker?

A. Before a system is patched
B. After a system has been compromised
C. Before a system has been compromised
D. During an attack

Answer: C

Question No : 6

An IT security manager is trying to quickly assess the risks associated with not implementing a corporate firewall system. What sort of risk assessment is most appropriate?

A. Annualized Risk Assessment
B. Qualitative risk assessment
C. Quantitative risk assessment
D. Technical Risk Assessment
E. Iterative Risk Assessment

Answer: B

Question No : 7

Which of the following protocols allows an e-mail client to access and manipulate a remote e-mail file without downloading it to the local computer?

A. IMAP
B. SNMP
C. POP3
D. SMTP

Answer: A

Question No : 8

John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. He is working as a root user on the Linux operating system. He wants to delete his private.txt file from his operating system. He knows that the deleted file can be recovered easily. Hence, he wants to delete the file securely. He wants to hide the shredding, and so he desires to add a final overwrite of the file private.txt with zero. Which of the following commands will John use to accomplish his task?

A. rmdir -v private.txt
B. shred -vfu private.txt
C. shred -vfuz private.txt
D. rm -vf private.txt

Answer: C

Question No : 9

Which of the following languages enable programmers to store cookies on client computers? Each correct answer represents a complete solution. Choose two.

A. DHTML
B. Perl
C. HTML
D. JavaScript

Answer: B,D

Question No : 10

You work as a Network Administrator for Net World Inc. The company has a Linux-based network. You are optimizing performance and security on your Web server. You want to know the ports that are listening to FTP. Which of the following commands will you use?

A. netstat -a | grep FTP
B. FTP netstat -r
C. FTP netstat -a
D. netstat -r | grep FTP

Answer: A

Question No : 11

Which of the following protocols provides maintenance and error reporting function?

A. UDP
B. ICMP
C. PPP
D. IGMP

Answer: B

Question No : 12

What technical control provides the most critical layer of defense if an intruder is able to bypass all physical security controls and obtain tapes containing critical data?

A. Camera Recordings
B. Security guards
C. Encryption
D. Shredding
E. Corrective Controls

Answer: C

Question No : 13

Which layer of the TCP/IP Protocol Stack Is responsible for port numbers?

A. Network
B. Transport
C. Internet
D. Application

Answer: B

Question No : 14

You work as a Network Administrator for McNeil Inc. You are installing an application. You want to view the log file whenever a new entry is added to the /var/log/messages log file. Which of the following commands will you use to accomplish this?

A. TAIL -show /var/log/messages
B. TAIL -f /var/log/messages
C. TAIL -50 /var/log/messages
D. TAIL -view /var/log/messages

Answer: B

Question No : 15

Which of the following protocols is used by a host that knows its own MAC (Media Access Control) address to query a server for its own IP address?

A. RARP
B. ARP
C. DNS
D. RDNS

Answer: A

Question No : 16

One of your Linux systems was compromised last night. According to change management

history and a recent vulnerability scan, the system's patches were up-to-date at the time of the attack. Which of the following statements is the Most Likely explanation?

A. It was a zero-day exploit.
B. It was a Trojan Horse exploit.
C. It was a worm exploit.
D. It was a man-in-middle exploit.

Answer: A

Question No : 17

What is the function of the TTL (Time to Live) field in IPv4 and the Hop Limit field in IPv6 In an IP Packet header?

A. These fields are decremented each time a packet is retransmitted to minimize the possibility of routing loops.
B. These fields are initialized to an initial value to prevent packet fragmentation and fragmentation attacks.
C. These fields are recalculated based on the required time for a packet to arrive at its destination.
D. These fields are incremented each time a packet is transmitted to indicate the number of routers that an IP packet has traversed.

Answer: A

Question No : 18

The Linux command to make the /etc/shadow file, already owned by root, readable only by root is which of the following?

A. chmod 444/etc/shadow
B. chown root: root/etc/shadow
C. chmod 400/etc/shadow
D. chown 400 /etc/shadow

Answer: C

Question No : 19

When a packet leaving the network undergoes Network Address Translation (NAT), which of the following is changed?

A. TCP Sequence Number
B. Source address
C. Destination port
D. Destination address

Answer: B

Question No : 20

On which of the following OSI model layers does IPSec operate?

A. Physical layer
B. Network layer
C. Data-link layer
D. Session layer

Answer: B

Question No : 21

Which of the following protocols work at the Session layer of the OSI model? Each correct answer represents a complete solution. Choose all that apply.

A. Border Gateway Multicast Protocol (BGMP)
B. Internet Security Association and Key Management Protocol (ISAKMP)
C. Trivial File Transfer Protocol (TFTP)
D. User Datagram Protocol (UDP)

Answer: A,B

Question No : 22

Which of the following is a new Windows Server 2008 feature for the Remote Desktop Protocol (RDP)?

A. The ability to allow the administrator to choose a port other than the default RDP port (TCP 3389)
B. The ability to support connections from mobile devices like smart phones
C. The ability to allow clients to authenticate over TLS
D. The ability to allow clients to execute individual applications rather than using a terminal desktop

Answer: D

Question No : 23

Which of the following is NOT typically used to mitigate the war dialing threat?

A. Setting up monitored modems on special phone numbers
B. Setting modems to auto-answer mode
C. Proactively scanning your own phone numbers
D. Monitoring call logs at the switch

Answer: B

Question No : 24

When an IIS filename extension is mapped, what does this mean?

A. Files with the mapped extensions cannot be interpreted by the web server.
B. The file and all the data from the browser's request are handed off to the mapped interpreter.
C. The files with the mapped extensions are interpreted by CMD.EXE.
D. The files with the mapped extensions are interpreted by the web browser.

Answer: B

Question No : 25

Which of the following is a characteristic of hash operations?

A. Asymmetric
B. Non-reversible
C. Symmetric
D. Variable length output

Answer: D

Question No : 26

You have implemented a firewall on the company's network for blocking unauthorized network connections. Which of the following types of security control is implemented in this case?

A. Detective
B. Preventive
C. Directive
D. Corrective

Answer: B

Question No : 27

Which of the following is an advantage of private circuits versus VPNs?

A. Flexibility
B. Performance guarantees
C. Cost
D. Time required to implement

Answer: B

Question No : 28

You work as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. You are required to search for the error messages in the /var/log/messages

log file. Which of the following commands will you use to accomplish this?

A. ps /var/log/messages
B. cat /var/log/messages | look error
C. cat /var/log/messages | grep error
D. cat /var/log/messages

Answer: C

Question No : 29

Which of the following attack vectors are addressed by Xinetd and TCP Wrappers?

A. Outsider attack from network
B. Outsider attack from a telephone
C. Insider attack from local network
D. Attack from previously installed malicious code
E. A and B
F. A and C
G. B and D
H. C and D

Answer: B

Question No : 30

What would the file permission example "rwsr-sr-x" translate to in absolute mode?

A. 1755
B. 6755
C. 6645
D. 1644

Answer: B

Question No : 31

You are going to upgrade your hard disk's file system from FAT to NTFS. What are the major advantages of the NTFS file system over FAT16 and FAT32 file systems?

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

A. NTFS gives better file security than FAT16 and FAT32.
B. Automatic backup.
C. NTFS file system supports for larger hard disks.
D. NTFS give improved disk compression than FAT16 and FAT32.

Answer: A,C,D

Question No : 32

Which aspect of UNIX systems was process accounting originally developed for?

A. Data warehouse
B. Time sharing
C. Process tracking
D. Real time

Answer: C

Question No : 33

The Return on Investment (ROI) measurement used in Information Technology and Information Security fields is typically calculated with which formula?

A. ROI = (gain - expenditure)/(expenditure) X 100%
B. ROI = (gain + expenditure)/(expenditure) X 100%
C. ROI = (loss + expenditure)/(expenditure) X 100%
D. ROI = (loss - expenditure)/(expenditure) X 100%

Answer: A

Question No : 34

Many IIS servers connect to Microsoft SQL databases. Which of the following statements about SQL server security is TRUE?

A. SQL Server patches are part of the operating system patches.
B. SQL Server should be installed on the same box as your IIS web server when they communicate as part of the web application.
C. It is good practice to never use integrated Windows authentication for SQL Server.
D. It is good practice to not allow users to send raw SQL commands to the SQL Server.

Answer: D

Question No : 35

Which of the following is an advantage of an Intrusion Detection System?

A. It is a mature technology.
B. It is the best network security.
C. It never needs patching.
D. It is a firewall replacement.

Answer: A

Question No : 36

In order to capture traffic for analysis, Network Intrusion Detection Systems (NIDS) operate with network cards in what mode?

A. Discrete
B. Reporting
C. Promiscuous
D. Alert

Answer: C

Question No : 37

The following three steps belong to the chain of custody for federal rules of evidence. What

additional step is recommended between steps 2 and 3?

STEP 1 - Take notes: who, what, where, when and record serial numbers of machine(s) in question.

STEP 2 - Do a binary backup if data is being collected.

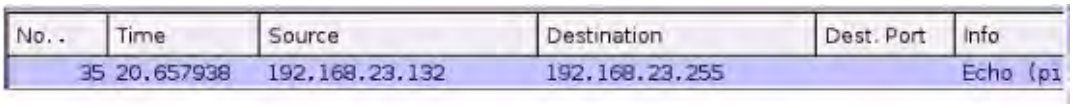
STEP 3 - Deliver collected evidence to law enforcement officials.

A. Rebuild the original hard drive from scratch, and sign and seal the good backup in a plastic bag.
B. Conduct a forensic analysis of all evidence collected BEFORE starting the chain of custody.
C. Take photographs of all persons who have had access to the computer.
D. Check the backup integrity using a checksum utility like MD5, and sign and seal each piece of collected evidence in a plastic bag.

Answer: D

Question No : 38

You are examining a packet capture session in Wire shark and see the packet shown in the accompanying image. Based on what you see, what is the appropriate protection against this type of attempted attack?



No. .	Time	Source	Destination	Dest. Port	Info
35	20.657938	192.168.23.132	192.168.23.255		Echo (pi

A. Block DNS traffic across the router
B. Disable forwarding of unsolicited TCP requests
C. Disable IP-directed broadcast requests
D. Block UDP packets at the firewall

Answer: C

Question No : 39

Which of the following is an UDP based protocol?

A. telnet
B. SNMP
C. IMAP
D. LDAP

Answer: B

Question No : 40

You are responsible for technical support at a company. One of the employees complains that his new laptop cannot connect to the company wireless network. You have verified that he is entering a valid password/passkey. What is the most likely problem?

A. A firewall is blocking him.
B. His laptop is incompatible.
C. MAC filtering is blocking him.
D. His operating system is incompatible.

Answer: C

Question No : 41

Your organization is developing a network protection plan. No single aspect of your network seems more important than any other. You decide to avoid separating your network into segments or categorizing the systems on the network. Each device on the network is essentially protected in the same manner as all other devices.

This style of defense-in-depth protection is best described as which of the following?

A. Uniform protection
B. Threat-oriented
C. Information-centric
D. Protected enclaves

Answer: A

Question No : 42