Vendor: GIAC

Exam Code: GSEC

Exam Name: GIAC Security Essentials

Version: DEMO

QUESTION 1
Your organization has broken its network into several sections/segments, which are separated by firewalls, ACLs and VLANs. The purpose is to defend segments of the network from potential attacks that originate in a different segment or that attempt to spread across segments. This style of defense-in-depth protection is best described as which of the following?

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

Answer: B

QUESTION 2
Which of the following systems acts as a NAT device when utilizing VMware in NAT mode?

A. Guest system
B. Local gateway
C. Host system
D. Virtual system

Answer: D

QUESTION 3
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 4
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 5

Which of the following elements is the most important requirement to ensuring the success of a business continuity plan?

A. Disaster Recover Plans
B. Anticipating all relevant threats
C. Executive buy-in
D. Clearly defining roles and responsibilities
E. Training

Answer: C

QUESTION 6
Which of the following TCP dump output lines indicates the first step in the TCP 3-way handshake?

A. 07:09:43.368615 download.net 39904 > ftp.com.21: S 733381829:733381829(0) win 8760 <mss 1460> (DF)
B. 07:09:43.370302 ftp.com.21 > download.net.39904: S 1192930639:1192930639(0} ack 733381830 win 1024 <mss 1460> (DF)
C. 09:09:22.346383 ftp.com.21 > download.net.39904: , rst 1 win 2440(DF)
D. 07:09:43.370355 download.net.39904 > ftp.com.21: , ack 1 win 8760 (DF)

Answer: A

QUESTION 7
Users at the Marketing department are receiving their new Windows XP Professional workstations. They will need to maintain local work files in the first logical volume, and will use a second volume for the information shared between the area group. Which is the best file system design for these workstations?

A. Both volumes should be converted to NTFS at install time.
B. First volume should be FAT32 and second volume should be NTFS.
C. First volume should be EFS and second volume should be FAT32.
D. Both volumes should be converted to FAT32 with NTFS DACLs.

Answer: A

QUESTION 8
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 9

What is TRUE about Workgroups and Domain Controllers?

A. By default all computers running Windows 2008 can only form Domain Controllers not Workgroups
B. Workgroups are characterized by higher costs while Domain Controllers by lower costs
C. You cannot have stand-alone computers in the midst of other machines that are members of a domain
D. Workgroup computers cannot share resources, only computers running on the same domain can
E. You can have stand-alone computers in the midst of other machines that are members of a domain.

Answer: E

QUESTION 10
What file instructs programs like Web spiders NOT to search certain areas of a site?

A. Robots.txt
B. Restricted.txt
C. Spider.txt
D. Search.txt

Answer: A

QUESTION 11
Which of the following is a benefit of using John the Ripper for auditing passwords?

A. John's Blowfish cracking routine uses a complex central computing loop that increases the cost of each hash computation.
B. John the Ripper is much slower for auditing passwords encrypted with MD5 and Blowfish.
C. John's MD5 cracking routine uses a simplified central computing loop that decreases the cost of each hash computation.
D. John cannot use the DES bit-slicing technique, so it is much slower than other tools, especially when used against DES-encrypted passwords.

Answer: C

QUESTION 12
Which of the following is an advantage of a Host Intrusion Detection System (HIDS) versus a Network Intrusion Detection System (NIDS)?

A. Ability to detect malicious traffic after it has been decrypted by the host
B. Ability to decrypt network traffic
C. Ability to listen to network traffic at the perimeter
D. Ability to detect malicious traffic before it has been decrypted

Answer: A

QUESTION 13
Which of the following is more commonly used for establishing high-speed backbones that interconnect smaller networks and can carry signals over significant distances?

A. Bluetooth
B. Ethernet
C. Token ring
D. Asynchronous Transfer Mode (ATM)

Answer: D

QUESTION 14
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 15
What is the main reason that DES is faster than RSA?

A. DES is less secure.
B. DES is implemented in hardware and RSA is implemented in software.
C. Asymmetric cryptography is generally much faster than symmetric.
D. Symmetric cryptography is generally much faster than asymmetric.

Answer: D

QUESTION 16
Which of the following statements would be seen in a Disaster Recovery Plan?

A. "Instructions for notification of the media can be found in Appendix A"
B. "The Emergency Response Plan should be executed in the case of any physical disaster listed on page 3."
C. "The target for restoration of business operations is 72 hours from the declaration of disaster."
D. "After arriving at the alternate site, utilize the server build checklist to rebuild all servers on the server rebuild list."

Answer: D

QUESTION 17
Your software developer comes to you with an application that controls a user device. The application monitors its own behavior and that of the device and creates log files. The log files are expected to grow steadily and rapidly. Your developer currently has the log files stored in the /bin folder with the application binary. Where would you suggest that the developer store the log files?

A. /var/log
B. /etc/log

C. /usr/log
D. /tmp/log
E. /dev/log

Answer: A

QUESTION 18
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 19
What would the following IP tables command do?

```
IP tables -I INPUT -s 99.23.45.1/32 -j DROP
```

A. Drop all packets from the source address
B. Input all packers to the source address
C. Log all packets to or from the specified address
D. Drop all packets to the specified address

Answer: A

QUESTION 20
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 21
Which of the following Unix syslog message priorities is the MOST severe?

A. err
B. emerg
C. crit
D. alert

Answer: B

QUESTION 22
During a scheduled evacuation training session the following events took place in this order:

1. Evacuation process began by triggering the building fire alarm.
2a. The meeting point leader arrived first at the designated meeting point and immediately began making note of who was and was not accounted for.
2b. Stairwell and door monitors made it to their designated position to leave behind a box of flashlights and prop the stairway doors open with a garbage can so employees can find exits and dispose of food and beverages.
2c. Special needs assistants performed their assigned responsibility to help employees out that require special assistance.
3. The safety warden communicated with the meeting point leader via walkie talkie to collect a list of missing personnel and communicated this information back to the searchers.
4. Searchers began checking each room and placing stick-it notes on the bottom of searched doors to designate which areas were cleared.
5. All special need assistants and their designated wards exited the building.
6. Searchers complete their assigned search pattern and exit with the Stairwell/door monitors.

Given this sequence of events, which role is in violation of its expected evacuation tasks?

A. Safety warden
B. Stairwell and door monitors
C. Meeting point leader
D. Searchers
E. Special needs assistants

Answer: B

QUESTION 23
What type of malware is a self-contained program that has the ability to copy itself without parasitically infecting other host code?

A. Trojans
B. Boot infectors
C. Viruses
D. Worms

Answer: D

QUESTION 24
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