GIAC.Premium.GPEN.79q - DEMO

Number: GPEN
Passing Score: 800
Time Limit: 120 min
File Version:

Exam Code: GPEN

Exam Name: GIAC Certified Penetration Tester

Website: www.VCEplus.io
Twitter: www.twitter.com/VCE_Plus

Exam A

QUESTION 1
Which of the following can be used to mitigate the evil twin phishing attack?
A. SARA
B. Obiwan
C. Magic Lantern
D. IPSec VPN

Correct Answer: D
Section:
Explanation:

QUESTION 2
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. The combination of parameters may then be used to infer the remote operating system (OS fingerprinting), or incorporated into a device fingerprint. Which of the following Nmap switches can be used to perform TCP/IP stack fingerprinting?
A. nmap -sS
B. nmap -sT
C. nmap -sU -p
D. nmap -O -p

Correct Answer: D
Section:
Explanation:

QUESTION 3
Which of the following protocols is the mandatory part of the WPA2 standard in the wireless networking?
A. TKIP
B. ARP
C. CCMP
D. WEP

Correct Answer: C
Section:
Explanation:

QUESTION 4
You want to get the Windows administrator account even when it is renamed. Which of the following tools will you use?
A. Ntop
B. Brutus
C. Sniffer
D. Sid2user

Correct Answer: D
Section:
Explanation:

QUESTION 5
Which of the following can be used to perform session hijacking?
Each correct answer represents a complete solution. Choose all that apply.
A. Cross-site scripting

B. ARP spoofing
C. Session sidejacking
D. Session fixation

Correct Answer: A, C, D
Section:
Explanation:

QUESTION 6

You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company has recently provided fifty laptops to its sales team members. You are required to configure an 802.11 wireless network for the laptops. The sales team members must be able to use their data placed at a server in a cabled network. The planned network should be able to handle the threat of unauthorized access and data interception by an unauthorized user.

You are also required to prevent the sales team members from communicating directly to one another. Which of the following actions will you take to accomplish the task?

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

A. Implement the open system authentication for the wireless network.
B. Configure the wireless network to use WEP encryption for the data transmitted over a wireless network.
C. Using group policies, configure the network to allow the wireless computers to connect to the ad hoc networks only.
D. Using group policies, configure the network to allow the wireless computers to connect to the infrastructure networks only.
E. Implement the IEEE 802.1X authentication for the wireless network.

Correct Answer: B, D, E
Section:
Explanation:

QUESTION 7

Which of the following can be used as a countermeasure to the rainbow password attack?

A. Using salt in the password.
B. Using alphanumeric characters.
C. Using hashed password.
D. Using 8 character password.

Correct Answer: A
Section:
Explanation:

QUESTION 8

Which of the following encryption encoding techniques is used in the basic authentication method?

A. Base64
B. DES (ECB mode)
C. HMAC_MD5
D. Md5

Correct Answer: A
Section:
Explanation:

QUESTION 9

Which of the following password cracking attacks is based on a pre-calculated hash table to retrieve plain text passwords?

A. Rainbow attack
B. Brute Force attack
C. Hybrid attack

D. Dictionary attack

Correct Answer: A
Section:
Explanation:

QUESTION 10
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He finds that the We-are-secure server is vulnerable to attacks. As a countermeasure, he suggests that the Network Administrator should remove the IPP printing capability from the server. He is suggesting this as a countermeasure against __________.

A. SNMP enumeration
B. NetBIOS NULL session
C. DNS zone transfer
D. IIS buffer overflow

Correct Answer: D
Section:
Explanation:

QUESTION 11
Which of the following tools is used for the 802.11 HTTP, HTTPS based MITM attacks?

A. Ettercap
B. dsniff
C. AirJack
D. wsniff

Correct Answer: D
Section:
Explanation:

QUESTION 12
You have just installed a Windows 2003 server. What action should you take regarding the default administrator and guest accounts for securing a computer?

A. Disable both and create new accounts with different names for those functions.
B. Disable the administrator account but keep the guest account.
C. Leave them as they are, since they are needed for Windows Server Operation.
D. Disable the guest account but keep the administrator account.

Correct Answer: A
Section:
Explanation:

QUESTION 13
Which of the following are the two different file formats in which Microsoft Outlook saves e-mail messages based on system configuration?
Each correct answer represents a complete solution. Choose two.

A. .xst
B. .ost
C. .pst
D. .txt

Correct Answer: B, C
Section:
Explanation:

QUESTION 14

Which of the following statutes is enacted in the U.S., which prohibits creditors from collecting data from applicants, such as national origin, caste, religion etc?

A. The Electronic Communications Privacy Act
B. The Equal Credit Opportunity Act (ECOA)
C. The Fair Credit Reporting Act (FCRA)
D. The Privacy Act

Correct Answer: B
Section:
Explanation:

QUESTION 15

John works as a professional Ethical Hacker. He is assigned a project to test the security of www.we-are-secure.com. John has gained the access to the network of the organization and placed a backdoor in the network. Now, he wants to clear all event logs related to previous hacking attempts. Which of the following tools can John use if we-are-secure.com is using the Windows 2000 server?
Each correct answer represents a complete solution. Choose two.

A. AuditPol
B. Blindside
C. elsave.exe
D. WinZapper

Correct Answer: C, D
Section:
Explanation:

QUESTION 16

Alice wants to prove her identity to Bob. Bob requests her password as proof of identity, which Alice dutifully provides (possibly after some transformation like a hash function); meanwhile, Eve is eavesdropping the conversation and keeps the password. After the interchange is over, Eve connects to Bob posing as Alice; when asked for a proof of identity, Eve sends Alice's password read from the last session, which Bob accepts.
Which of the following attacks is being used by Eve?

A. Session fixation
B. Cross site scripting
C. Firewalking
D. Replay

Correct Answer: D
Section:
Explanation:

QUESTION 17

A war dialer is a tool that is used to scan thousands of telephone numbers to detect vulnerable modems. It provides an attacker unauthorized access to a computer. Which of the following tools can an attacker use to perform war dialing?
Each correct answer represents a complete solution. Choose all that apply.

A. THC-Scan
B. NetStumbler
C. ToneLoc
D. Wingate

Correct Answer: A, C
Section:
Explanation:

QUESTION 18

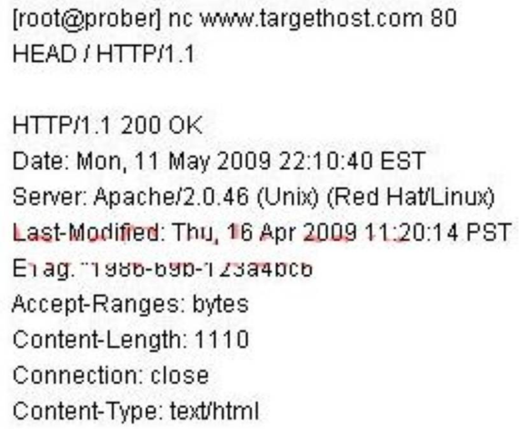
Mark works as a Network Administrator for Infonet Inc. The company has a Windows 2000 Active Directory domain-based network. The domain contains one hundred Windows XP Professional client computers. Mark is deploying an 802.11 wireless LAN on the network. The wireless LAN will use Wired Equivalent Privacy (WEP) for all the connections. According to the company's security policy, the client computers must be able to automatically connect to the wireless LAN. However, the unauthorized computers must not be allowed to connect to the wireless LAN and view the wireless network. Mark wants to configure all the wireless access points and client computers to act in accordance with the company's security policy. What will he do to accomplish this? Each correct answer represents a part of the solution. Choose three.

A. Configure the authentication type for the wireless LAN to Open system.
B. Broadcast SSID to connect to the access point (AP).
C. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.
D. Install a firewall software on each wireless access point.
E. Configure the authentication type for the wireless LAN to Shared Key.
F. On each client computer, add the SSID for the wireless LAN as the preferred network.

Correct Answer: C, E, F
Section:
Explanation:

QUESTION 19

John works as a Network Security Professional. He is assigned a project to test the security of www.we-are-secure.com. He establishes a connection to a target host running a Web service with netcat and sends a bad html request in order to retrieve information about the service on the host.



```
[root@prober] nc www.targethost.com 80
HEAD / HTTP/1.1

HTTP/1.1 200 OK
Date: Mon, 11 May 2009 22:10:40 EST
Server: Apache/2.0.46 (Unix) (Red Hat/Linux)
Last-Modified: Thu, 16 Apr 2009 11:20:14 PST
ETag: "1986-69b-123a4bc6
Accept-Ranges: bytes
Content-Length: 1110
Connection: close
Content-Type: text/html
```

Which of the following attacks is John using?

A. Banner grabbing
B. War driving
C. Eavesdropping
D. Sniffing

Correct Answer: A
Section:
Explanation:

QUESTION 20

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 successfully completed the following steps of the preattack phase:
* Information gathering
* Determining network range
* Identifying active machines
* Finding open ports and applications
* I OS fingerprinting
* Fingerprinting services
Now John wants to perform network mapping of the We-are-secure network. Which of the following tools can he use to accomplish his task?
Each correct answer represents a complete solution. Choose all that apply.

A. Traceroute

B. NeoTrace
C. Cheops
D. Ettercap

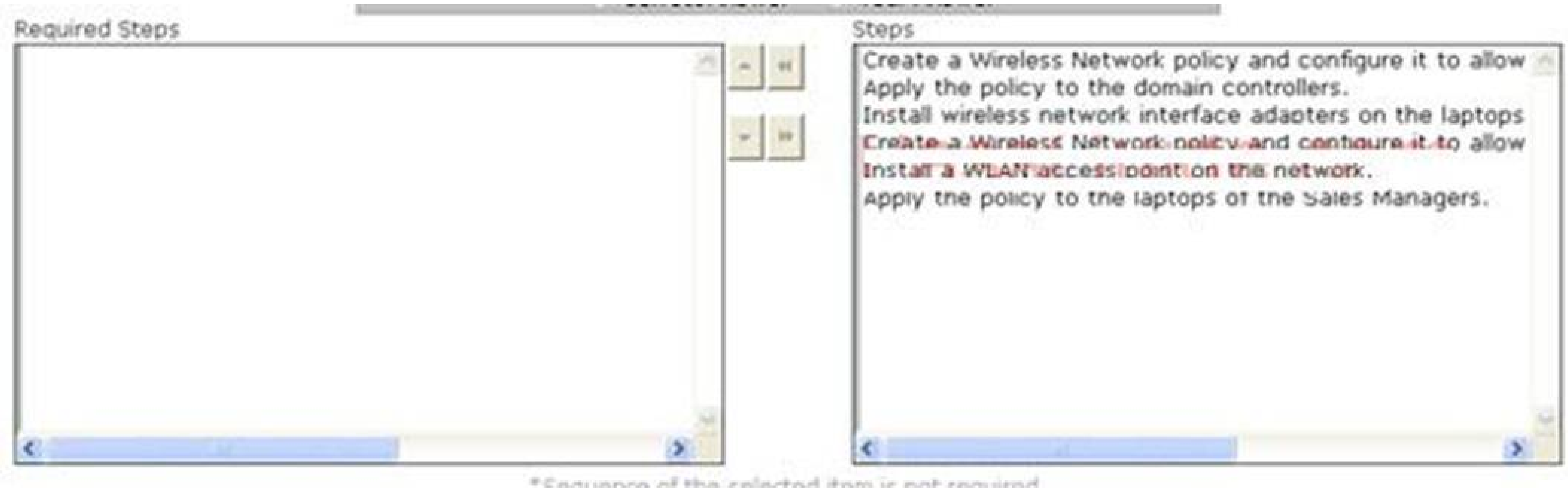
Correct Answer: A, B, C
Section:
Explanation:

QUESTION 21
You work as a Network Administrator for McNeil Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The company's management has decided to provide laptops to its sales team members. These laptops are equipped with smart card readers. The laptops will be configured as wireless network clients. You are required to accomplish the following tasks:
* The wireless network communication should be secured.
* The laptop users should be able to use smart cards for getting authenticated.
* n order to accomplish the tasks, you take the following steps:
* Configure 802.1x and WEP for the wireless connections.
* Configure the PEAP-MS-CHAP v2 protocol for authentication.
What will happen after you have taken these steps?
A. The wireless network communication will be secured.
B. The laptop users will be able to use smart cards for getting authenticated.
C. Both tasks will be accomplished.
D. None of the tasks will be accomplished

Correct Answer: A
Section:
Explanation:

QUESTION 22
DRAG DROP
You work as a Network Administrator for Tech Perfect Inc. The company has a Windows Active Directory-based single domain single forest network. The functional level of the forest is Windows Server 2003. The Sales Managers in the company use laptops for connecting to the network. You are required to provide wireless connectivity on the network to all the Sales Managers. The security policy of the company dictates that the laptops should connect only to the access points on the network. The laptops should not be able to directly communicate with each other. You are required to implement the security policy of the company.
Choose the steps that you will take to accomplish the task.

Select and Place:



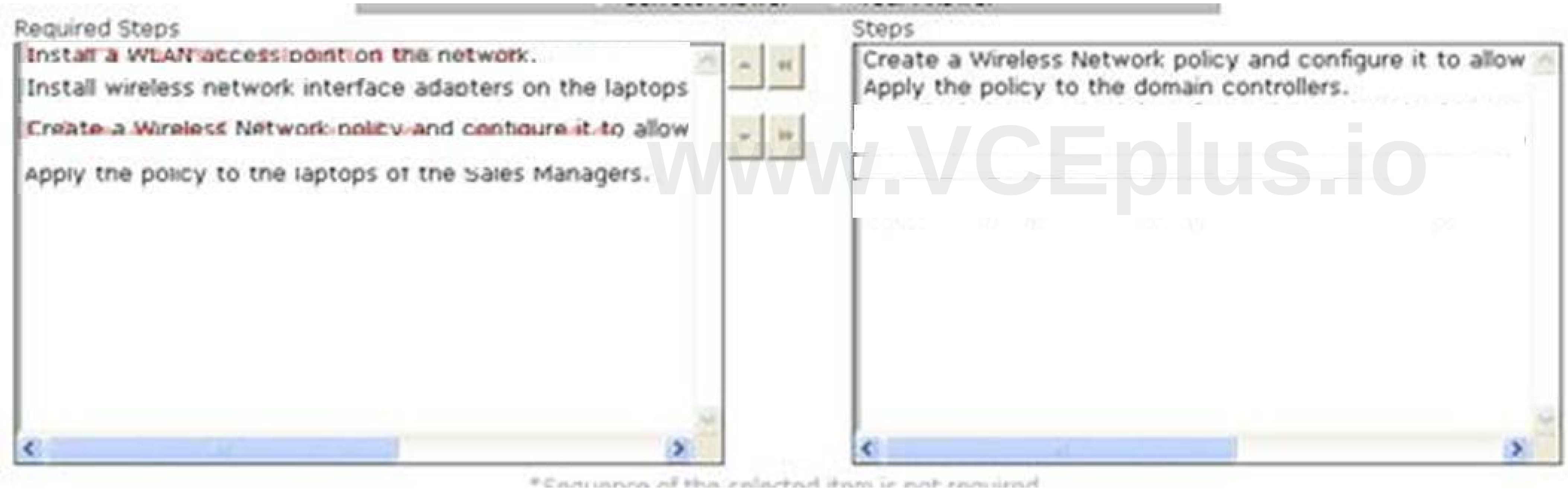
Required Steps

Steps

Create a Wireless Network policy and configure it to allow
Apply the policy to the domain controllers.
Install wireless network interface adapters on the laptops
Create a Wireless Network policy and configure it to allow
Install a WLAN access point on the network.
Apply the policy to the laptops of the Sales Managers.

*Sequence of the selected item is not required

Correct Answer:



Required Steps

Install a WLAN access point on the network.
Install wireless network interface adapters on the laptops
Create a Wireless Network policy and configure it to allow
Apply the policy to the laptops of the Sales Managers.

Steps

Create a Wireless Network policy and configure it to allow
Apply the policy to the domain controllers.

*Sequence of the selected item is not required

Section:
Explanation:
Install a WLAN access poin on the network
Install wireless network interface adapters on the laptops
Create a Wireless Network policy and configure it to allow
Apply the policy to the laptomps of the Sales Managers.

QUESTION 23
You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

A. Ettercap
B. Nmap

C. Netcraft
D. Ethereal

Correct Answer: C
Section:
Explanation:

QUESTION 24
You see the career section of a company's Web site and analyze the job profile requirements. You conclude that the company wants professionals who have a sharp knowledge of Windows server2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?

A. Scanning
B. Gaining access
C. Reconnaissance
D. Covering tracks

Correct Answer: C
Section:
Explanation:

QUESTION 25
John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. He performs a Teardrop attack on the we-are-secure server and observes that the server crashes. Which of the following is the most likely cause of the server crash?

A. The ICMP packet is larger than 65,536 bytes.
B. Ping requests at the server are too high.
C. The spoofed TCP SYN packet containing the IP address of the target is filled in both the source and destination fields.
D. The we-are-secure server cannot handle the overlapping data fragments.

Correct Answer: D
Section:
Explanation:

QUESTION 26
The 3-way handshake method is used by the TCP protocol to establish a connection between a client and the server. It involves three steps:
1- In the first step, a SYN message is sent from a client to the server.
2- In the second step, a SYN/ACK message is sent from the server to the client.
3- In the third step, an ACK (usually called SYN-ACK-ACK) message is sent from the client to the server. At this point, both the client and the server have received acknowledgements of the TCP connection.
If the Initial Sequence Numbers of the client and server were 241713111 and 241824111 respectively at the time when the client was sending the SYN message in the first step of the TCP 3-way handshake method, what will be the value of the acknowledgement number field of the server's packet when the server was sending the SYN/ACK message to the client in the second step of the TCP 3-way handshake method?

A. 241824112
B. 241713111
C. 241824111
D. 241713112

Correct Answer: D
Section:
Explanation:

QUESTION 27
Which of the following tools crashes computers running Windows 2000/XP/NT by sending crafted SMB requests?

A. NBTdeputy
B. SMBGrind

C. SMBDie
D. Samdump

Correct Answer: C
Section:
Explanation:

QUESTION 28
Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?
A. Post-attack phase
B. On-attack phase
C. Attack phase
D. Pre-attack phase

Correct Answer: D
Section:
Explanation:

QUESTION 29
You work as a Network Administrator in the SecureTech Inc. The SecureTech Inc. is using Linuxbased server. Recently, you have updated the password policy of the company in which the server will disable passwords after four trials. What type of attack do you want to stop by enabling this policy?
A. Cookie poisoning
B. XSS
C. Brute force
D. Replay

Correct Answer: C
Section:
Explanation:

QUESTION 30
Which of the following is the correct sequence of packets to perform the 3-way handshake method?
A. SYN, ACK, SYN/ACK
B. SYN, SYN/ACK, ACK
C. SYN, SYN, ACK
D. SYN, ACK, ACK

Correct Answer: B
Section:
Explanation:

QUESTION 31
John is a black hat hacker. FBI arrested him while performing some email scams. Under which of the following US laws will john be charged?
A. 18 U.S.C. 2510
B. 18 U.S.C. 2701
C. 18 U.S.C. 1362
D. 18 U.S.C. 1030

Correct Answer: D
Section:
Explanation:

QUESTION 32
Which of the following is a person-to-person attack in which an attacker convinces the target that he or she has a problem or might have a certain problem in the future and that he, the attacker, is ready to help solve the problem?

A. Dumpster diving
B. Social engineering
C. Vulnerability scanning
D. Reverse social engineering

Correct Answer: D
Section:
Explanation:

QUESTION 33
You work as a professional Ethical Hacker. You are assigned a project to perform blackhat testing on www.we-are-secure.com. You visit the office of we-are-secure.com as an air-condition mechanic. You claim that someone from the office called you saying that there is some fault in the air-conditioner of the server room. After some inquiries/arguments, the Security Administrator allows you to repair the air-conditioner of the server room.
When you get into the room, you found the server is Linux-based. You press the reboot button of the server after inserting knoppix Live CD in the CD drive of the server. Now, the server promptly boots backup into Knoppix. You mount the root partition of the server after replacing the root password in the /etc/shadow file with a known password hash and salt. Further, you copy the netcat tool on the server and install its startup files to create a reverse tunnel and move a shell to a remote server whenever the server is restarted. You simply restart the server, pull out the Knoppix Live CD from the server, and inform that the air-conditioner is working properly.
After completing this attack process, you create a security auditing report in which you mention various threats such as social engineering threat, boot from Live CD, etc. and suggest the countermeasures to stop booting from the external media and retrieving sensitive data. Which of the following steps have you suggested to stop booting from the external media and retrieving sensitive data with regard to the above scenario?
Each correct answer represents a complete solution. Choose two.

A. Setting only the root level access for sensitive data.
B. Encrypting disk partitions.
C. Placing BIOS password.
D. Using password protected hard drives.

Correct Answer: B, D
Section:
Explanation:

QUESTION 34
What
happens when you scan a broadcast IP address of a network?
Each correct answer represents a complete solution. Choose all that apply.

A. It may show smurf DoS attack in the network IDS of the victim.
B. It leads to scanning of all the IP addresses on that subnet at the same time.
C. It will show an error in the scanning process.
D. Scanning of the broadcast IP address cannot be performed.

Correct Answer: A, B
Section:
Explanation:

QUESTION 35
Which of the following tools can be used to perform Windows password cracking, Windows enumeration, and VoIP session sniffing?

A. Cain
B. L0phtcrack
C. Pass-the-hash toolkit
D. John the Ripper

Correct Answer: A
Section:
Explanation:

QUESTION 36

John works as a Professional Penetration Tester. He has been assigned a project to test the Website security of www.we-are-secure Inc. On the We-are-secure Website login page, he enters='or''=' as a username and successfully logs on to the user page of the Web site. Now, John asks the we-are-secure Inc. to improve the login page PHP script. Which of the following suggestions can John give to improve the security of the we-are-secure Website login page from the SQL injection attack?

A. Use the session_regenerate_id() function
B. Use the escapeshellcmd() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellarg() function

Correct Answer: C
Section:
Explanation:

QUESTION 37

Which of the following attacks can be overcome by applying cryptography?

A. Buffer overflow
B. Web ripping
C. DoS
D. Sniffing

Correct Answer: D
Section:
Explanation:

QUESTION 38

Which of the following tools uses exploits to break into remote operating systems?

A. Nessus
B. Metasploit framework
C. Nmap
D. John the Ripper

Correct Answer: B
Section:
Explanation:

QUESTION 39

Which of the following penetration testing phases involves gathering data from whois, DNS, and network scanning, which helps in mapping a target network and provides valuable information regarding the operating system and applications running on the systems?

A. Post-attack phase
B. Attack phase
C. Pre-attack phase
D. On-attack phase

Correct Answer: C
Section:
Explanation:

QUESTION 40

John works as a Penetration Tester in a security service providing firm named you-are-secure Inc.
Recently, John's company has got a project to test the security of a promotional Website www.missatlanta.com and assigned the pen-testing work to John. When John is performing penetration testing, he inserts the following script in the search box at the company home page:
<script>alert('Hi, John')</script>
After pressing the search button, a pop-up box appears on his screen with the text - 'Hi, John.'
Which of the following attacks can be performed on the Web site tested by john while considering the above scenario?

A. Replay attack
B. Buffer overflow attack
C. CSRF attack
D. XSS attack

Correct Answer: D
Section:
Explanation:

QUESTION 41
Which of the following 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 and also detects wireless networks marking their relative position with a GPS?

A. NetStumbler
B. Tcpdump
C. Kismet
D. Ettercap

Correct Answer: A
Section:
Explanation:

QUESTION 42
Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?

A. Whishker
B. Nmap
C. Nessus
D. SARA

Correct Answer: C
Section:
Explanation:

QUESTION 43
Which of the following attacks allows an attacker to sniff data frames on a local area network (LAN) or stop the traffic altogether?

A. Man-in-the-middle
B. ARP spoofing
C. Port scanning
D. Session hijacking

Correct Answer: B
Section:
Explanation:

QUESTION 44
You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com Web site.

For this, you want to perform the idle scan so that you can get the ports open in the we-are-secure.com server. You are using Hping tool to perform the idle scan by using a zombie computer. While scanning, you notice that every IPID is being incremented on every query, regardless whether the ports are open or close. Sometimes, IPID is being incremented by more than one value. What may be the reason?

A. The zombie computer is the system interacting with some other system besides your comp uter.
B. The firewall is blocking the scanning process.
C. The zombie computer is not connected to the we-are-secure.com Web server.
D. Hping does not perform idle scanning.

Correct Answer: A
Section:
Explanation:

QUESTION 45

You execute the following netcat command:

c:\target\nc -1 -p 53 -d -e cmd.exe

What action do you want to perform by issuing the above command?

A. Capture data on port 53 and performing banner grabbing.
B. Capture data on port 53 and delete the remote shell.
C. Listen the incoming traffic on port 53 and execute the remote shell.
D. Listen the incoming data and performing port scanning.

Correct Answer: C
Section:
Explanation:

QUESTION 46

You work as a Penetration Tester for the Infosec Inc. Your company takes the projects of security auditing. Recently, your company has assigned you a project to test the security of the we-aresecure. com Website. The we-are-secure.com Web server is using Linux operating system. When you port scanned the we-are-secure.com Web server, you got that TCP port 23, 25, and 53 are open. When you tried to telnet to port 23, you got a blank screen in response. When you tried to type the dir, copy, date, del, etc. commands you got only blank spaces or underscores symbols on the screen. What may be the reason of such unwanted situation?

A. The we-are-secure.com server is using honeypot.
B. The we-are-secure.com server is using a TCP wrapper.
C. The telnet service of we-are-secure.com has corrupted.
D. The telnet session is being affected by the stateful inspection firewall.

Correct Answer: B
Section:
Explanation:

QUESTION 47

Which of the following tools is used to verify the network structure packets and confirm that the packets are constructed according to specification?

A. snort_inline
B. EtherApe
C. Snort decoder
D. AirSnort

Correct Answer: C
Section:
Explanation:

QUESTION 48

You have just set up a wireless network for customers at a coffee shop. Which of the following are good security measures to implement?

Each correct answer represents a complete solution. Choose two.

A. MAC filtering the router
B. Using WPA encryption
C. Using WEP encryption
D. Not broadcasting SSID

Correct Answer: B, C
Section:
Explanation:

QUESTION 49

You work as an Administrator for Bluesky Inc. The company has 145 Windows XP Professional client computers and eighty Windows 2003 Server computers. You want to install a security layer of WAP specifically designed for a wireless environment. You also want to ensure that the security layer provides privacy, data integrity, and authentication for client-server communications over a wireless network. Moreover, you want a client and server to be authenticated so that wireless transactions remain secure and the connection is encrypted. Which of the following options will you use to accomplish the task?

A. Wired Equivalent Privacy (WEP)
B. Virtual Private Network (VPN)
C. Wireless Transport Layer Security (WTLS)
D. Recovery Console

Correct Answer: C
Section:
Explanation:

QUESTION 50

You run the following PHP script:

```
<?php
$name = mysql_real_escape_string($_POST['name']);
$password = mysql_real_escape_string($_POST['password']);
?>
```

What is the use of the mysql_real_escape_string() function in the above script.
Each correct answer represents a complete solution. Choose all that apply

A. It escapes all special characters from strings $_POST['name'] and $_POST['password'].
B. It escapes all special characters from strings $_POST['name'] and $_POST['password'] except ' and '.
C. It can be used to mitigate a cross site scripting attack.
D. It can be used as a countermeasure against a SQL injection attack.

Correct Answer: A, D
Section:
Explanation:

QUESTION 51

You run the following bash script in Linux:

```
for i in 'cat hostlist.txt' ;do
nc -q 2 -v $i 80 < request.txt
done
```

where, hostlist.txt file contains the list of IP addresses and request.txt is the output file. Which of the following tasks do you want to perform by running this script?

A. You want to perform port scanning to the hosts given in the IP address list.
B. You want to transfer file hostlist.txt to the hosts given in the IP address list.
C. You want to perform banner grabbing to the hosts given in the IP address list.
D. You want to put nmap in the listen mode to the hosts given in the IP address list.

Correct Answer: C
Section:
Explanation:

QUESTION 52

You want to perform an active session hijack against Secure Inc. You have found a target that allows Telnet session. You have also searched an active session due to the high level of traffic on the network. What should you do next?

A. Use a sniffer to listen network traffic.
B. Use macoff to change MAC address.
C. Guess the sequence numbers.
D. Use brutus to crack telnet password.

Correct Answer: C
Section:
Explanation:

QUESTION 53

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

A. To use firewalking, the attacker needs the IP address of the last known gateway before the firewall and the IP address of a host located behind the firewall.
B. Firewalking works on the UDP packets.
C. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
D. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.

Correct Answer: A, C, D
Section:
Explanation:

QUESTION 54

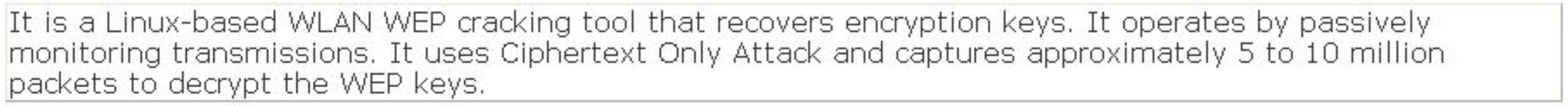
Which of the following Web attacks is performed by manipulating codes of programming languages such as SQL, Perl, Java present in the Web pages?

A. Command injection attack
B. Cross-Site Scripting attack
C. Cross-Site Request Forgery
D. Code injection attack

Correct Answer: D
Section:
Explanation:

QUESTION 55

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. AirSnort
B. PsPasswd
C. Cain
D. Kismet

Correct Answer: A
Section:
Explanation:

QUESTION 56
What happens when you scan a broadcast IP address of a network?
Each correct answer represents a complete solution. Choose all that apply.
A. It will show an error in the scanning process.
B. Scanning of the broadcast IP address cannot be performed.
C. It may show smurf DoS attack in the network IDS of the victim.
D. It leads to scanning of all the IP addresses on that subnet at the same time.

Correct Answer: C, D
Section:
Explanation:

QUESTION 57
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 successfully completed the following pre-attack phases while testing the security of the server:
Footprinting Scanning Now he wants to conduct the enumeration phase. Which of the following tools can John use to conduct it?
Each correct answer represents a complete solution. Choose all that apply.
A. PsFile
B. PsPasswd
C. UserInfo
D. WinSSLMiM

Correct Answer: A, B, C
Section:
Explanation:

QUESTION 58
You want to search the Apache Web server having version 2.0 using google hacking. Which of the following search queries will you use?
A. intitle:'Test Page for Apache Installation' 'You are free'
B. intitle:'Test Page for Apache Installation' 'It worked!'
C. intitle:test.page 'Hey, it worked !' 'SSl/TLS aware'
D. intitle:Sample.page.for.Apache Apache.Hook.Function

Correct Answer: D
Section:
Explanation:

QUESTION 59
The employees of EWS Inc. require remote access to the company's Web servers. In order to provide solid wireless security, the company uses EAP-TLS as the authentication protocol. Which of the following statements are true about EAP-TLS?
Each correct answer represents a complete solution. Choose all that apply.
A. It provides a moderate level of security.
B. It uses password hash for client authentication.
C. It uses a public key certificate for server authentication.
D. It is supported by all manufacturers of wireless LAN hardware and software.

Correct Answer: C, D

Section:
Explanation:

QUESTION 60
Fill in the blank with the appropriate tool.
____scans IP networks for NetBIOS name information and works in the same manner as nbtstat, but it operates on a range of addresses instead of just one.
A. NBTscan

Correct Answer: A
Section:
Explanation:

QUESTION 61
Which of the following tools can be used as a Linux vulnerability scanner that is capable of identifying operating systems and network services?
Each correct answer represents a complete solution. Choose all that apply.
A. Cheops
B. Fport
C. Elsave
D. Cheops-ng

Correct Answer: A, D
Section:
Explanation:

QUESTION 62
In which of the following attacks does an attacker use packet sniffing to read network traffic between two parties to steal the session cookie?
A. Cross-site scripting
B. Session fixation
C. Session sidejacking
D. ARP spoofing

Correct Answer: C
Section:
Explanation:

QUESTION 63
Which of the following Nmap commands is used to perform a UDP port scan?
A. nmap -sS
B. nmap -sY
C. nmap -sN
D. nmap --sU

Correct Answer: D
Section:
Explanation:

QUESTION 64
Fill in the blank with the appropriate act name.
The___ act gives consumers the right to ask emailers to stop spamming them.
A. CAN-SPAM

Correct Answer: A

Section:
Explanation:

QUESTION 65

John works as an Ethical Hacker for uCertify Inc. He wants to find out the ports that are open in uCertify's server using a port scanner. However, he does not want to establish a full TCP connection. Which of the following scanning techniques will he use to accomplish this task?

A. TCP FIN
B. Xmas tree
C. TCP SYN/ACK
D. TCP SYN

Correct Answer: D
Section:
Explanation:

QUESTION 66

Which of following tasks can be performed when Nikto Web scanner is using a mutation technique?
Each correct answer represents a complete solution. Choose all that apply.

A. Guessing for password file names.
B. Sending mutation payload for Trojan attack.
C. Testing all files with all root directories.
D. Enumerating user names via Apache.

Correct Answer: A, C, D
Section:
Explanation:

QUESTION 67

You are sending a file to an FTP server. The file will be broken into several pieces of information packets (segments) and will be sent to the server. The file will again be reassembled and reconstructed once the packets reach the FTP server. Which of the following information should be used to maintain the correct order of information packets during the reconstruction of the file?

A. Acknowledge number
B. TTL
C. Checksum
D. Sequence number

Correct Answer: D
Section:
Explanation:

QUESTION 68

Which of the following is the frequency range to tune IEEE 802.11a network?

A. 1.15-3.825 GHz
B. 5.15-5.825 GHz
C. 5.25-9.825 GHz
D. 6.25-9.825 GHz

Correct Answer: B
Section:
Explanation:

QUESTION 69

Which of the following tools monitors the radio spectrum for the presence of unauthorized, rogue access points and the use of wireless attack tools?

A. IDS
B. Firewall
C. Snort
D. WIPS

Correct Answer: D
Section:
Explanation:

QUESTION 70
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. cookie files
C. Temporary files
D. EDB and STM database files

Correct Answer: A, C, D
Section:
Explanation:

QUESTION 71
You work as a Web developer in the IBM Inc. Your area of proficiency is PHP. Since you have proper knowledge of security, you have bewared from rainbow attack. For mitigating this attack, you design the PHP code based on the following algorithm:

key = hash(password + salt)
for 1 to 65000 do
key = hash(key + salt)
Which of the following techniques are you implementing in the above algorithm?
A. Key strengthening
B. Hashing
C. Sniffing
D. Salting

Correct Answer: A
Section:
Explanation:

QUESTION 72
You are concerned about war driving bringing hackers attention to your wireless network. What is the most basic step you can take to mitigate this risk?
A. Implement WEP
B. Implement MAC filtering
C. Don't broadcast SSID
D. Implement WPA

Correct Answer: C
Section:
Explanation:

QUESTION 73
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 the Linux operating system. He wants to use a wireless sniffer to sniff the We-are-

secure network. Which of the following tools will he use to accomplish his task?

A. NetStumbler
B. Snadboy's Revelation
C. WEPCrack
D. Kismet

Correct Answer: D
Section:
Explanation:

QUESTION 74

You work as a Network Penetration tester in the Secure Inc. Your company takes the projects to test the security of various companies. Recently, Secure Inc. has assigned you a project to test the security of a Web site. You go to the Web site login page and you run the following SQL query:

```
SELECT email, passwd, login_id, full_name
FROM members
WHERE email = 'attacker@somehwere.com'; DROP TABLE members; --'
```

What task will the above SQL query perform?

A. Performs the XSS attacks.
B. Deletes the entire members table.
C. Deletes the rows of members table where email id is 'attacker@somehwere.com' given.
D. Deletes the database in which members table resides.

Correct Answer: B
Section:
Explanation:

QUESTION 75

John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. He performs Web vulnerability scanning on the We-are-secure server.

The output of the scanning test is as follows:

```
C:\whisker.pl -h target_IP_address
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net -- = - = - = - = - =
= Host: target_IP_address
= Server: Apache/1.3.12 (Win32) ApacheJServ/1.1
mod_ssl/2.6.4 OpenSSL/0.9.5a mod_perl/1.22
+ 200 OK: HEAD /cgi-bin/printenv
```

John recognizes /cgi-bin/printenv vulnerability ('Printenv' vulnerability) in the We_are_secure server. Which of the following statements about 'Printenv' vulnerability are true?

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

A. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.
B. The countermeasure to 'printenv' vulnerability is to remove the CGI script.
C. This vulnerability helps in a cross site scripting attack.
D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

Correct Answer: B, C, D
Section:
Explanation:

QUESTION 76

Ryan wants to create an ad hoc wireless network so that he can share some important files with another employee of his company. Which of the following wireless security protocols should he choose for setting up an ad hoc wireless network?

Each correct answer represents a part of the solution. Choose two.

A. WPA2 -EAP

B. WPA-PSK
C. WPA-EAP
D. WEP

Correct Answer: B, D
Section:
Explanation:

QUESTION 77
Which of the following statements are true about NTLMv1?
Each correct answer represents a complete solution. Choose all that apply.
A. It uses the LANMAN hash of the user's password.
B. It is mostly used when no Active Directory domain exists.
C. It is a challenge-response authentication protocol.
D. It uses the MD5 hash of the user's password.

Correct Answer: A, B, C
Section:
Explanation:

QUESTION 78
Which of the following can be used as a countermeasure against the SQL injection attack?
Each correct answer represents a complete solution. Choose two.
A. mysql_real_escape_string()
B. Prepared statement
C. mysql_escape_string()
D. session_regenerate_id()

Correct Answer: A, B
Section:
Explanation:

QUESTION 79
You send SYN packets with the exact TTL of the target system starting at port 1 and going up to port 1024 using hping2 utility. This attack is known as __________.
A. Port scanning
B. Spoofing
C. Cloaking
D. Firewalking

Correct Answer: D
Section:
Explanation: