312-50.exam.320q

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. MIX QUESTIONS

Exam A

QUESTION 1

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80. The engineer receives this output:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369
```


Which of the following is an example of what the engineer performed?

A. Cross-site scripting
B. Banner grabbing
C. SQL injection
D. Whois database query

Correct Answer: B

Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 2
An NMAP scan of a server shows port 69 is open. What risk could this pose?

A. Unauthenticated access
B. Weak SSL version
C. Cleartext login
D. Web portal data leak

Correct Answer: A
Section: Analysis/Assessment
Explanation

Explanation/Reference:

QUESTION 3
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 4
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 5
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 6
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 7
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 8
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 9

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 10
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 11
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 12
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 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 property ensures that a hash function will not produce the same hashed value for two different messages?

A. Collision resistance
B. Bit length
C. Key strength
D. Entropy

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 22
How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80HEAD / HTTP/1.0
B. telnet webserverAddress 80PUT / HTTP/1.0
C. telnet webserverAddress 80HEAD / HTTP/2.0
D. telnet webserverAddress 80PUT / HTTP/2.0

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 23
Low humidity in a data center can cause which of the following problems?

A. Heat
B. Corrosion
C. Static electricity
D. Airborne contamination

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 24
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

A. Man trap
B. Tailgating
C. Shoulder surfing
D. Social engineering

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 25
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

A. False positive
B. False negative
C. True positve

D. True negative

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:
QUESTION 26
While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

A. Validate web content input for query strings.
B. Validate web content input with scanning tools.
C. Validate web content input for type, length, and range.
D. Validate web content input for extraneous queries.

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 27
A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack

B. ARP spoofing attack
C. Social engineering attack
D. Scanning attack

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:
QUESTION 28
Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine
B. Nessus scripting engine
C. NMAP scripting engine
D. SAINT scripting engine

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 29
Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

A. Microsoft Security Baseline Analyzer
B. Retina
C. Core Impact
D. Microsoft Baseline Security Analyzer

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 30
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Firewall-management policy
B. Acceptable-use policy
C. Remote-access policy
D. Permissive policy

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 31
When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A. A bottom-up approach
B. A top-down approach
C. A senior creation approach
D. An IT assurance approach

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 32
Which of the following processes evaluates the adherence of an organization to its stated security policy?

A. Vulnerability assessment
B. Penetration testing
C. Risk assessment
D. Security auditing

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 33
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47

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 48
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 49
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/Reference:

QUESTION 50
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 51
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 52

Explanation

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 53
During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

A. The web application does not have the secure flag set. B.
The session cookies do not have the HttpOnly flag set.
C. The victim user should not have an endpoint security solution.
D. The victim's browser must have ActiveX technology enabled.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 54
The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

A. An attacker, working slowly enough, can evade detection by the IDS.
B. Network packets are dropped if the volume exceeds the threshold.
C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.
D. The IDS will not distinguish among packets originating from different sources.

Correct Answer: A
Section: Security
Explanation/Reference:

QUESTION 55
What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

A. They do not use host system resources.
B. They are placed at the boundary, allowing them to inspect all traffic.
C. They are easier to install and configure.
D. They will not interfere with user interfaces.

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 56
The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

A. Asymmetric
B. Confidential
C. Symmetric
D. Non-confidential

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

Explanation

QUESTION 57
When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

A. Drops the packet and moves on to the next one
B. Continues to evaluate the packet until all rules are checked
C. Stops checking rules, sends an alert, and lets the packet continue
D. Blocks the connection with the source IP address in the packet

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

Explanation/Reference:

QUESTION 58
Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

A. Detective
B. Passive
C. Intuitive
D. Reactive

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

Explanation/Reference:

QUESTION 59
An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

A. The wireless card was not turned on.
B. The wrong network card drivers were in use by Wireshark.
C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.

D. Certain operating systems and adapters do not collect the management or control packets.

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

QUESTION 60
From the two screenshots below, which of the following is occurring?

Explanation

First one:

```
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
3 Starting Nmap
5 Host 10.0.0.1 appears to be up.
6 MAC Address: 00:09:5B:29:FD:96 (Netgear)
7 Host 10.0.0.2 appears to be up.
8 MAC Address: 00:0F:B5:96:38:5D (Netgear)
9 Host 10.0.0.4 appears to be up.
10 Host 10.0.0.5 appears to be up.
11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)
12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399
seconds
```

Second one:

```
1 [10.0.0.252]# nmap -sO 10.0.0.2
3 Starting Nmap 4.01 at 2006-07-14 12:56 BST
4 Interesting protocols on 10.0.0.2:
5 (The 251 protocols scanned but not shown below are
6 in state: closed)
7 PROTOCOL STATE SERVICE
8 1 open icmp
9 2 open|filtered igmp
10 6 open tcp
11 17 open udp
12 255 open|filtered unknown
14 Nmap finished: 1 IP address (1 host up) scanned in
15 1.259 seconds
1 [10.0.0.253]# nmap -sP
1 [10.0.0.253]# nmap -sP
```

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.
C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

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

Explanation/Reference:

QUESTION 61
Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

A. Cain
B. John the Ripper
C. Nikto
D. Hping

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

Explanation/Reference:

QUESTION 62
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 63
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 64
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 65
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 66
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 67
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 68
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 69
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 70
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 71
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 72
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 73
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 74
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 75
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 76
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 77
When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

A. Network tap

B. Layer 3 switch
C. Network bridge
D. Application firewall

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

Explanation/Reference:

QUESTION 78
Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl
B. C++
C. Python
D. Java

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

Explanation/Reference:

QUESTION 79
Smart cards use which protocol to transfer the certificate in a secure manner?

A. Extensible Authentication Protocol (EAP) B.
Point to Point Protocol (PPP)
C. Point to Point Tunneling Protocol (PPTP)
D. Layer 2 Tunneling Protocol (L2TP)

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

Explanation/Reference:

QUESTION 80
Which of the following is a hashing algorithm?

A. MD5
B. PGP
C. DES
D. ROT13

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

Explanation/Reference:

QUESTION 81
Which of the following problems can be solved by using Wireshark?

A. Tracking version changes of source code
B. Checking creation dates on all webpages on a server
C. Resetting the administrator password on multiple systems
D. Troubleshooting communication resets between two systems

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

Explanation/Reference:

QUESTION 82
What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

A. tcp.src == 25 and ip.host == 192.168.0.125
B. host 192.168.0.125:25
C. port 25 and host 192.168.0.125

D. tcp.port == 25 and ip.host == 192.168.0.125

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

QUESTION 83
Which tool would be used to collect wireless packet data?

A. NetStumbler
B. John the Ripper
C. Nessus
D. Netcat

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

Explanation/Reference:

QUESTION 84
Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID

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

Explanation/Reference:

QUESTION 85
Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key
B. 1025 bit key C. 1536 bit key
D. 2048 bit key

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

Explanation/Reference:

QUESTION 86
After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

A. SHA1
B. Diffie-Helman
C. RSA
D. AES

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

Explanation/Reference:

QUESTION 87
What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.
B. LM hashes are based on AES128 cryptographic standard.
C. Uppercase characters in the password are converted to lowercase.
D. LM hashes are not generated when the password length exceeds 15 characters.

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

Explanation/Reference:

QUESTION 88
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

A. if (billingAddress = 50) {update field} else exit
B. if (billingAddress != 50) {update field} else exit
C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress <= 50) {update field} else exit

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

Explanation/Reference:

QUESTION 89
A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input field:

```
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC"
originalPath="vbscript:msgbox ("Vulnerable");>"
```

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".
Which web applications vulnerability did the analyst discover?

A. Cross-site request forgery
B. Command injection
C. Cross-site scripting
D. SQL injection

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

Explanation/Reference:

QUESTION 90
A security administrator notices that the log file of the company's webserver contains suspicious entries:

```
\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978
```

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. command injection.
B. SQL injection.
C. directory traversal.
D. LDAP injection.

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

Explanation/Reference:

QUESTION 91
Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

A. Firewall
B. Honeypot
C. Core server

D. Layer 4 switch

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

Explanation/Reference:

QUESTION 92
Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

A. ping 192.168.2.
B. ping 192.168.2.255
C. for %V in (1 1 255) do PING 192.168.2.%V
D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"

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

Explanation/Reference:

QUESTION 93
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 94

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 95
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 96
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 97
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 98
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 99

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 100
Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 101
Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop
B. SYN flood
C. Smurf attack
D. Ping of death

Correct Answer: A

Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 102
Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
C. Configure the firewall to allow traffic on TCP port 53.
D. Configure the firewall to allow traffic on TCP port 8080.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 103
While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:

<script>alert(" Testing Testing Testing ")</script>

Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

Correct Answer: D
Section: Procedures/ Methodology

Explanation
Explanation/Reference:

QUESTION 104
Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

A. They provide a repeatable framework.
B. Anyone can run the command line scripts.
C. They are available at low cost.
D. They are subject to government regulation.

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 105
The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

A. An extensible security framework named COBIT
B. A list of flaws and how to fix them
C. Web application patches
D. A security certification for hardened web applications

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 106
In the OSI model, where does PPTP encryption take place?

A. Transport layer
B. Application layer
C. Data link layer
D. Network layer

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 107
Which of the following is an example of IP spoofing?

A. SQL injections
B. Man-in-the-middle
C. Cross-site scripting
D. ARP poisoning

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 108
For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 109
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 110
Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?

A. Poly key exchange

B. Cross certification
C. Poly key reference
D. Cross-site exchange

Correct Answer: B
Section: Procedures/ Methodology
Explanation

Explanation/Reference:
QUESTION 111
Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
B. The root CA stores the user's hash value for safekeeping.
C. The CA is the trusted root that issues certificates.
D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 112
A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections
B. Mandating only client-side PKI certificates for all connections
C. Requiring client and server PKI certificates for all connections
D. Requiring strong authentication for all DNS queries

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 113
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 114
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 115
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 116
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 117
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 118

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 119
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 120
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 121
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 122
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 123
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 124
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 125
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 126
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 127
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 128
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 129
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 130
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 131
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 132
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 133
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 134
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 135
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 136
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 137
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 138
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 139
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 140
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

A. Maltego
B. Cain & Abel
C. MetasploitD. Wireshark

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining. References: https://en.wikipedia.org/wiki/Maltego

QUESTION 141

While using your bank's online servicing you notice the following string in the URL bar: "http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21"

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

Which type of vulnerability is present on this site?

A. Web Parameter Tampering
B. Cookie Tampering
C. XSS Reflection
D. SQL injection

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

References: https://www.owasp.org/index.php/Web_Parameter_Tampering

QUESTION 142
Perspective clients want to see sample reports from previous penetration tests.

What should you do next?

A. Decline but, provide references.
B. Share full reports, not redacted.
C. Share full reports with redactions.
D. Share reports, after NDA is signed.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Penetration tests data should not be disclosed to third parties.

QUESTION 143
During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.

What type of firewall is inspecting outbound traffic?

A. Application
B. Circuit
C. Stateful
D. Packet Filtering

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.

References: http://searchsoftwarequality.techtarget.com/definition/application-firewall

QUESTION 144
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. Piggybacking
B. Masqurading
C. Phishing
D. Whaling

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain

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

QUESTION 145
You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

A. CHNTPW
B. Cain & Abel
C. SET
D. John the Ripper

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference: chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.

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

QUESTION 146
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 147
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 148
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 149
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 150
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 151
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 152
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 153
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 154
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 155
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 156
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 157
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 158
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 159
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 160
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 161

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 162
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 163
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 164
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 165
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 166
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 167
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 168
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 169
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 170
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 171
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 172
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 173
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 174
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 175
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 176
> 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 177
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 178
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 179
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 180
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 181
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 182
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 183
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 184
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 185
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 186
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 187
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 188
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 189
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions
B. Privilege escalation
C. Directory traversal
D. Brute force login

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
To upload files the user must have proper write file permissions.

References: http://codex.wordpress.org/Hardening_WordPress

QUESTION 190
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.

What Web browser-based security vulnerability was exploited to compromise the user?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. Clickjacking
D. Web form input validation

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Example and characteristics

If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

Incorrect Answers:
C: Clickjacking (User Interface redress attack, UI redress attack, UI redressing) is a malicious technique of tricking a Web user into clicking on something different from what the user perceives they are clicking on, thus potentially revealing confidential information or taking control of their computer while clicking on seemingly innocuous web pages. It is a browser security issue that is a vulnerability across a variety of browsers and platforms. A clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function.
References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

QUESTION 191
A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
B. Attempts by attackers to access the user and password information stored in the company's SQL database.
C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.
Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.

References: https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

QUESTION 192
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

A. Cross-site scripting vulnerability
B. Cross-site Request Forgery vulnerability

C. SQL injection vulnerability
D. Web site defacement vulnerability

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

QUESTION 193
Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
As a matter of good practice any PII should be protected with strong encryption.

References: https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information

QUESTION 194
Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input

QUESTION 195
An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is most likely able to handle this requirement?

A. RADIUS
B. DIAMETER
C. Kerberos
D. TACACS+

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.

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

QUESTION 196
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

A. The WAP does not recognize the client's MAC address
B. The client cannot see the SSID of the wireless network

C. Client is configured for the wrong channel
D. The wireless client is not configured to use DHCP

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC Filtering is often used on wireless networks.

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

QUESTION 197
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.

What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer—or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.

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

QUESTION 198
An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

A. Insufficient input validation
B. Insufficient exception handling
C. Insufficient database hardening
D. Insufficient security management

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The most common web application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

References: https://www.owasp.org/index.php/Testing_for_Input_Validation

QUESTION 199
Which of the following is a protocol specifically designed for transporting event messages?

A. SYSLOG
B. SMS
C. SNMP
D. ICMP

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

References: https://en.wikipedia.org/wiki/Syslog#Network_protocol

QUESTION 200
Which of the following security operations is used for determining the attack surface of an organization?

A. Running a network scan to detect network services in the corporate DMZ

B. Training employees on the security policy regarding social engineering
C. Reviewing the need for a security clearance for each employee
D. Using configuration management to determine when and where to apply security patches

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.

References: http://meisecurity.com/home/consulting/consulting-network-scanning/

QUESTION 201

The security concept of "separation of duties" is most similar to the operation of which type of security device?

A. Firewall
B. Bastion host
C. Intrusion Detection System
D. Honeypot

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In most enterprises the engineer making a firewall change is also the one reviewing the firewall metrics for unauthorized changes. What if the firewall administrator wanted to hide something? How would anyone ever find out? This is where the separation of duties comes in to focus on the responsibilities of tasks within security.

References: http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requires-security-separation-of-duties

QUESTION 202
The "black box testing" methodology enforces which kind of restriction?

A. Only the external operation of a system is accessible to the tester.
B. Only the internal operation of a system is known to the tester.
C. The internal operation of a system is only partly accessible to the tester.
D. The internal operation of a system is completely known to the tester.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.

References: https://en.wikipedia.org/wiki/Black-box_testing

QUESTION 203

A.

B.

The "gray box testing" methodology enforces what kind of restriction?

The internal operation of a system is only partly accessible to the tester.
The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. Only the internal operation of a system is known to the tester.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application.

A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.

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

QUESTION 204
The "white box testing" methodology enforces what kind of restriction?

A. The internal operation of a system is completely known to the tester.
B. Only the external operation of a system is accessible to the tester.
C. Only the internal operation of a system is known to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

References: https://en.wikipedia.org/wiki/White-box_testing

QUESTION 205

B.

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

A. Fuzzing
Randomizing
C. Mutating
D. Bounding

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

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

QUESTION 206
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.

B.

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 207
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

hping2 host.domain.com
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 208
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 209
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?

B.

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 210
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 211
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 212

A.

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?

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 213
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 214
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 215
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 216
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 217
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 218
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 219
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 220
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 221
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 222
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 223
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 224
What is the difference between the AES and RSA algorithms?

A. Both are asymmetric algorithms, but RSA uses 1024-bit keys.
B. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.
C. Both are symmetric algorithms, but AES uses 256-bit keys.
D. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 225

Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?

```
Code:
#include <string.h>
int main(){
char buffer[8];
strcpy(buffer, ""1111111111111111111111111111"");
}
```

Output:
Segmentation fault

A. C#
B. Python
C. Java
D. C++

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 226
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. Also he needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router nobody can access to the ftp and the permitted hosts cannot access to the Internet. According to the next configuration what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

A. The ACL 110 needs to be changed to port 80
B. The ACL for FTP must be before the ACL 110
C. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
D. The ACL 104 needs to be first because is UDP

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 227
Bob received this text message on his mobile phone: ""Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com"". Which statement below is true?

A. This is probably a legitimate message as it comes from a respectable organization.
B. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.
C. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
D. This is a scam because Bob does not know Scott.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 228
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Port Scanning
B. Hacking Active Directory
C. Privilege Escalation
D. Shoulder-Surfing

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 229
Which of the following will perform an Xmas scan using NMAP?

A. nmap -sA 192.168.1.254
B. nmap -sP 192.168.1.254
C. nmap -sX 192.168.1.254D. nmap -sV 192.168.1.254

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 230
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

A. request smtp 25
B. tcp.port eq 25
C. smtp port
D. tcp.contains port 25

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 231
Which service in a PKI will vouch for the identity of an individual or company?

A. KDC
B. CA
C. CR
D. CBC

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 232
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

A. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.
B. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
C. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.
D. Vulnerabilities in the application layer are greatly different from IPv4.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 233
In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.

Example:
allintitle: root passwd

A. Maintaining Access
B. Gaining Access
C. Reconnaissance
D. Scanning and Enumeration

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 234

Which type of security feature stops vehicles from crashing through the doors of a building?

A. Turnstile
B. Bollards
C. Mantrap
D. Receptionist

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 235

.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

A. Collision Attack
B. Evil Twin Attack
C. Sinkhole Attack
D. Signal Jamming Attack

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 236

Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

A. Role Based Access Control (RBAC)
B. Discretionary Access Control (DAC)
C. Windows authentication
D. Single sign-on

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 237
What attack is used to crack passwords by using a precomputed table of hashed passwords?

A. Brute Force Attack
B. Hybrid Attack
C. Rainbow Table Attack
D. Dictionary Attack

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 238
Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?

A. Nothing, but suggest to him to change the network's SSID and password.
B. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.
C. Log onto to his network, after all it's his fault that you can get in.
D. Only use his network when you have large downloads so you don't tax your own network.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 239
Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?

A. Windows
B. Unix
C. LinuxD. OS X

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 240
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 241
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. RecoveryD. Discovery

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 242

```
#!/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 243
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 244
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 245
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 246
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 247
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 248
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 249
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 250
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 251
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 252
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 253
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 254
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 255
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 256
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 257
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 258
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 259
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 260
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 261
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 262
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 263
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 264
What kind of risk will remain even if all theoretically possible safety measures would be applied?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 265
While doing a Black box pen test via the TCP port (80), you noticed that the traffic gets blocked when you tried to pass IRC traffic from a web enabled host. However, you also noticed that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?

A. Stateful
B. Application
C. Circuit
D. Packet Filtering

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 266
It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages. Which of the following is being described?

A. SNMP

B. ICMP
C. SYSLOG
D. SMS

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 267
While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

A. The port will send an ACK
B. The port will send a SYN
C. The port will ignore the packets
D. The port will send an RST

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Reference: https://nmap.org/book/man-port-scanning-techniques.html

QUESTION 268
Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

A. Metasploit
B. Wireshark
C. Maltego
D. Cain & Abel

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 269
If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

A. Running a network scan to detect network services in the corporate DMZ
B. Reviewing the need for a security clearance for each employee
C. Using configuration management to determine when and where to apply security patches
D. Training employees on the security policy regarding social engineering

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 270
What is the best Nmap command to use when you want to list all devices in the same network quickly after you successfully identified a server whose IP address is 10.10.0.5?

A. nmap -T4 -F 10.10.0.0/24
B. nmap -T4 -q 10.10.0.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -r 10.10.1.0/24

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 271
You've just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?

A. TCP/IP doesn't support ICMP

B. ARP is disabled on the target server
C. ICMP could be disabled on the target server
D. You need to run the ping command with root privileges

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 272
What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)?

A. Armitage
B. Dimitry
C. Metagoofil
D. cdpsnarf

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 273
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 274
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 275
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 276
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 277
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 278
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 279
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

Explanation/Reference:

QUESTION 280
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 281
You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

A. The zombie you are using is not truly idle.
B. A stateful inspection firewall is resetting your queries.

C. Hping2 cannot be used for idle scanning.
D. These ports are actually open on the target system.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 282
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.
C. Spoof the source IP address.
D. Only scan the Windows systems.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 283
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 284
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 285
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 286
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 287
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 288

You have initiated an active operating system fingerprinting attempt with nmap against a target system:

```
[root@ceh NG]# /usr/local/bin/nmap -sT -O 10.0.0.1

Starting nmap 3.28 ( www.insecure.org/nmap/) at 2003-06-18 19:14 IDT
Interesting ports on 10.0.0.1:
(The 1628 ports scanned but not shown below are in state: closed)

Port State Service
21/tcp filtered ftp
22/tcp filtered ssh
25/tcp open smtp
80/tcp open http
135/tcp open loc-srv
139/tcp open netbios-ssn
389/tcp open LDAP
443/tcp open https
465/tcp open smtps
1029/tcp open ms-lsa
1433/tcp open ms-sql-s
2301/tcp open compaqdiag
5555/tcp open freeciv
5800/tcp open vnc-http
5900/tcp open vnc
6000/tcp filtered X11

Remote operating system guess: Windows XP, Windows 2000, NT4 or 95/98/98SE Nmap
run completed -- 1 IP address (1 host up) scanned in 3.334 seconds

Using its fingerprinting tests nmap is unable to distinguish between different groups of
Microsoft based operating systems - Windows XP, Windows 2000, NT4 or 95/98/98SE.
```


What operating system is the target host running based on the open ports shown above?

A. Windows XP
B. Windows 98 SE
C. Windows NT4 Server
D. Windows 2000 Server

Correct Answer: D

Section: MIX QUESTIONS
Explanation
Explanation/Reference:

QUESTION 289
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 290
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 291
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 292
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 293
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 294
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 295
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 296
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 297
Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?

A. Overloading Port Address Translation
B. Dynamic Port Address Translation
C. Dynamic Network Address Translation
D. Static Network Address Translation

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 298
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 299

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 300

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 301

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 302
MX record priority increases as the number increases. (True/False.)

A. True
B. False

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 303
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 304
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 305
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 306
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 307
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 308
Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS

B. A zone transfer is accomplished with the nslookup service
C. A zone transfer passes all zone information that a DNS server maintains
D. A zone transfer passes all zone information that a nslookup server maintains
E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
F. Zone transfers cannot occur on the Internet

Correct Answer: ACE
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 309
You have the SOA presented below in your Zone.
Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries? collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

A. One day
B. One hour
C. One week
D. One month

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 310
Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.

What do you think Tess King is trying to accomplish? Select the best answer.

A. A zone harvesting

B. A zone transfer
C. A zone update D. A zone estimate

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 311
A zone file consists of which of the following Resource Records (RRs)?

A. DNS, NS, AXFR, and MX records B.
DNS, NS, PTR, and MX records
C. SOA, NS, AXFR, and MX records
D. SOA, NS, A, and MX records

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 312
Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?

A. Install DNS logger and track vulnerable packets
B. Disable DNS timeouts
C. Install DNS Anti-spoofing
D. Disable DNS Zone Transfer

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 313
Which DNS resource record can indicate how long any "DNS poisoning" could last?

A. MX
B. SOA
C. NS
D. TIMEOUT

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 314
Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.
No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
Y0u @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

A. ARP spoofing
B. SQL injection

C. DNS poisoning
D. Routing table injection

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

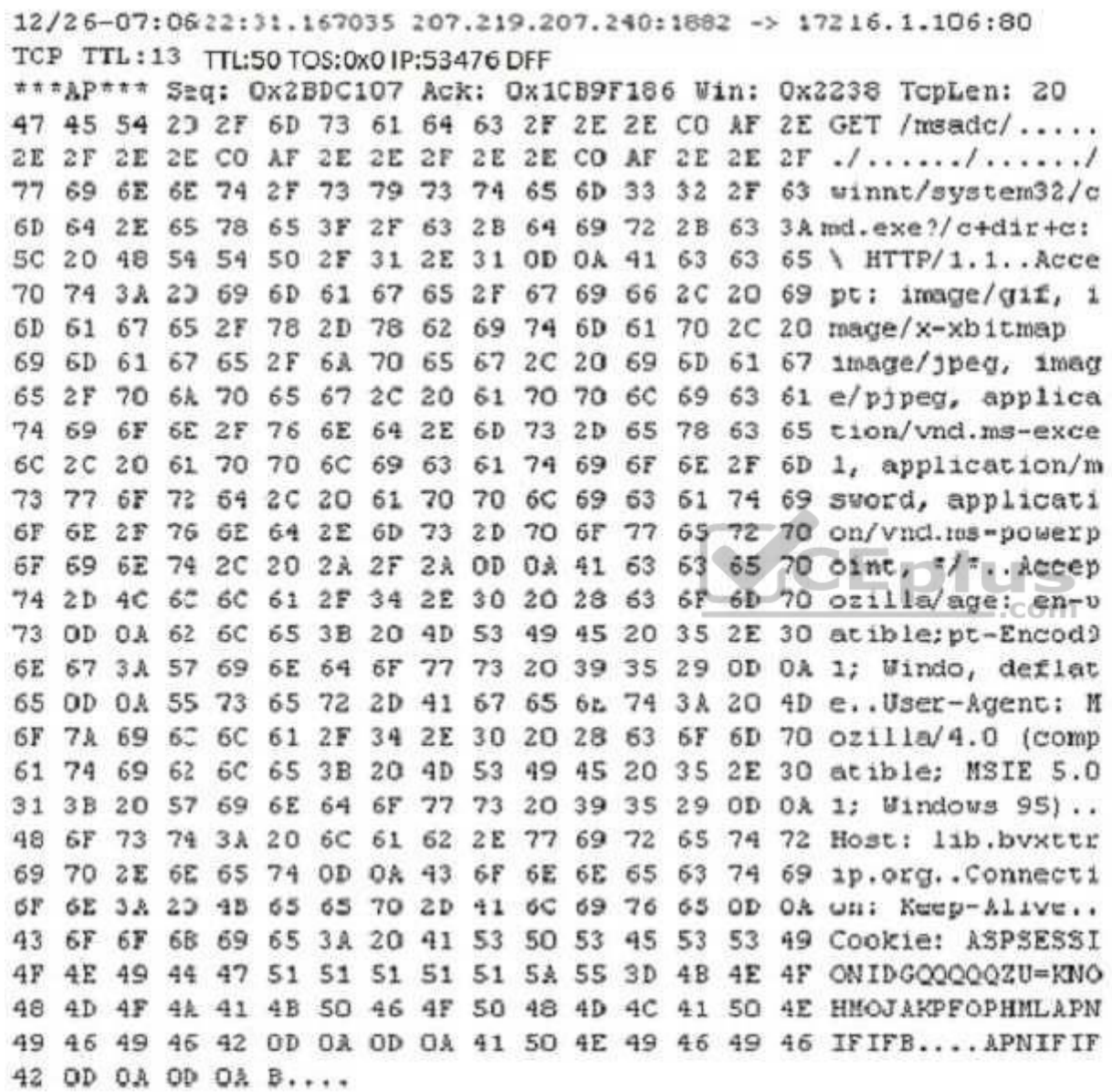
QUESTION 315
Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds
B. USER2SIDC. Cheops
D. SID2USER
E. DumpSec

Correct Answer: BDE
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 316
Study the following log extract and identify the attack.



```
12/26-07:06:22:31.167035 207.219.207.240:1682 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./....../....../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/pjpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, */*..Accep
74 2D 4C 61 6E 67 75 61 67 65 3A 20 65 6E 2D 75 t-Language: en-u
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-Encod3
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A 1; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 6B 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```

A. Hexcode Attack

B. Cross Site Scripting
C. Multiple Domain Traversal Attack
D. Unicode Directory Traversal Attack

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 317
Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

A. 137 and 139 B.
137 and 443 C.
139 and 443
D. 139 and 445

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 318
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack. You also notice "/bin/sh" in the ASCII part of the output.
As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:......
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.\)
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ....................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

A. The buffer overflow attack has been neutralized by the IDS
B. The attacker is creating a directory on the compromised machine
C. The attacker is attempting a buffer overflow attack and has succeeded
D. The attacker is attempting an exploit that launches a command-line shell

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 319

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt
B. SAM file
C. wwwroot
D. Repair file

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 320
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: