312-50.exam.325q

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

312-50

Certified Ethical Hacker Exam

Sections
1. Security

2. Tools /Systems /Programs
3. Procedures/ Methodology
4. Regulations / Policy
5. MIX QUESTIONS

Exam A

QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
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 14
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 15
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 16
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

A. The tester must capture the WPA2 authentication handshake and then crack it.

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

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 17
Which type of antenna is used in wireless communication?

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

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 18
What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

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

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 19
One way to defeat a multi-level security solution is to leak data via

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

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 20
Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

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

Correct Answer: D

Section: Security
Explanation

Explanation/Reference:

QUESTION 21
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

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

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 22
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?
A. Using the Metasploit psexec module setting the SA / Admin credential
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Correct Answer: D
Section: Security
Explanation

Explanation/Reference:

QUESTION 23
The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

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

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 24
A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

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

Correct Answer: A
Section: Security
Explanation

Explanation/Reference:

QUESTION 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
A security policy will be more accepted by employees if it is consistent and has the support of

A. coworkers.
B. executive management..

https://www.vceplus.com/

C. the security officer.
D. a supervisor.

Correct Answer: B
Section: Security
Explanation

Explanation/Reference:

QUESTION 35
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 36
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 37
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

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

Correct Answer: C
Section: Security
Explanation

Explanation/Reference:

QUESTION 38
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 39

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 40
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 41
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 42
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

Explanation/Reference:

QUESTION 43
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 44
From the two screenshots below, which of the following is occurring?

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 45
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 46
Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.
B. They send alerts to security monitors.
C. They use the same packet analysis engine.
D. They use the same packet capture utility.

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

Explanation/Reference:

QUESTION 47

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

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

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

Explanation/Reference:

QUESTION 48
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

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

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

Explanation/Reference:

QUESTION 49
A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

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

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

Explanation/Reference:

QUESTION 50
To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

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

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

Explanation/Reference:

QUESTION 51
An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe B.
g++ hackersExploit.py -o calc.exe

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

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

QUESTION 52
A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

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

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

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

Explanation/Reference:

QUESTION 53
ICMP ping and ping sweeps are used to check for active systems and to check

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

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

Explanation/Reference:

QUESTION 54
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 55
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 56
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 57
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 58
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 59
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 60
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 61
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 62
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 63
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 64
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 65
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 66
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 67
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 68
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 69
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 70
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 71
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 72
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 73
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 74
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 75
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 76
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 77
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 keyC. 1536 bit key
D. 2048 bit key

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

Explanation/Reference:

QUESTION 78
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 79
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 80
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 81
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 82
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 83
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 84
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 85

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 86
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 87
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 88
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 89
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 90
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 91
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 92
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

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

Correct Answer: D
Section: Tools /Systems /Programs

Explanation

Explanation/Reference:

QUESTION 93
An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

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

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

Explanation/Reference:

QUESTION 94
Which tool can be used to silently copy files from USB devices?

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

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

Explanation/Reference:
QUESTION 95
Which of the following is used to indicate a single-line comment in structured query language (SQL)?

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

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

Explanation/Reference:

QUESTION 96
A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:

NMAP –n –sS –P0 –p 80 ***.***.**.**

What type of scan is this?

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

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

Explanation/Reference:

QUESTION 97
What is the broadcast address for the subnet 190.86.168.0/22?
A. 190.86.168.255
B. 190.86.255.255
C. 190.86.171.255
D. 190.86.169.255

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

Explanation/Reference:

QUESTION 98
A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

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

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

Explanation/Reference:

QUESTION 99
Which of the following does proper basic configuration of snort as a network intrusion detection system require?

A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to a single segment.
D. Limit the packets captured to the /var/log/snort directory.

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

QUESTION 100
How is sniffing broadly categorized?

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

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

Explanation/Reference:

QUESTION 101
What are the three types of authentication?

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

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

Explanation/Reference:
QUESTION 102
The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

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

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

Explanation/Reference:

QUESTION 103
What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

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

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

Explanation/Reference:

QUESTION 104
A botnet can be managed through which of the following?

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

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

Explanation/Reference:

QUESTION 105
Fingerprinting VPN firewalls is possible with which of the following tools?

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

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

Explanation/Reference:

QUESTION 106
What is a successful method for protecting a router from potential smurf attacks?

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

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

Explanation/Reference:

QUESTION 107
Which of the following is optimized for confidential communications, such as bidirectional voice and video?
A. RC4
B. RC5
C. MD4

D. MD5

Correct Answer: A
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 108
Advanced encryption standard is an algorithm used for which of the following?

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

Correct Answer: C
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 109
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

A. Multiple keys for non-repudiation of bulk data
B. Different keys on both ends of the transport medium
C. Bulk encryption for data transmission over fiber
D. The same key on each end of the transmission medium

Correct Answer: D
Section: Procedures/ Methodology
Explanation

Explanation/Reference:

QUESTION 110
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 111
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 112
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 113
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 114
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 115
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 116
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 117
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 118
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 119

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 120
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 121
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 122
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 123
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 124
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 125
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 126
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 127
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 128
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 129

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 130
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 131
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 132
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 133
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 134

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 135
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 136
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 137
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 138
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 139
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 140
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 141
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 142
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 143
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 144
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 145
You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?

alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!";)

A. An Intrusion Detection System
B. A firewall IPTable
C. A Router IPTable
D. FTP Server rule

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Snort is an open source network intrusion detection system (NIDS) for networks .
Snort rule example:

This example is a rule with a generator id of 1000001. alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

References: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

QUESTION 146
What is the benefit of performing an unannounced Penetration Testing?

A. The tester will have an actual security posture visibility of the target network.
B. Network security would be in a "best state" posture.
C. It is best to catch critical infrastructure unpatched.
D. The tester could not provide an honest analysis.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry.
A possible solution to this danger is to conduct intermittent “unannounced” penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with “announced” penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.

References: http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

QUESTION 147
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.

What is happening?

A. ICMP could be disabled on the target server.
B. The ARP is disabled on the target server.
C. TCP/IP doesn't support ICMP.
D. You need to run the ping command with root privileges.

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

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

QUESTION 148
Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test

state. Which of the following activities should not be included in this phase? (see exhibit) Exhibit:

I. Removing all files uploaded on the system

II. Cleaning all registry entries

III. Mapping of network state

IV. Removing all tools and maintaining backdoor for reporting

A. III
B. IV
C. III and IV
D. All should be included.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The post-attack phase revolves around returning any modified system(s) to the pretest state. Examples of such activities:

▪ Removal of any files, tools, exploits, or other test-created objects uploaded to the system during testing ▪
Removal or reversal of any changes to the registry made during system testing

References: Computer and Information Security Handbook, John R. Vacca (2012), page 531

QUESTION 149
It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

Which of the following regulations best matches the description?

A. HIPAA
B. ISO/IEC 27002
C. COBITD. FISMA

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)[15] By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".

References: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

QUESTION 150
Which of the following is a component of a risk assessment?

A. Administrative safeguards
B. Physical security
C. DMZ
D. Logical interface

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

Risk assessment include:

- The total process of identifying, measuring, and minimizing uncertain events affecting AIS resources. It includes risk analysis, cost benefit analysis, safeguard selection, security test and evaluation, safeguard implementation, and systems review.
- The total process of identifying, controlling, and eliminating or minimizing uncertain events that may affect system resources. It includes risk analysis, cost benefit analysis, selection, implementation and test, security evaluation of safeguards, and overall security review. References:

https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

QUESTION 151
A medium-sized healthcare IT business decides to implement a risk management strategy.
Which of the following is NOT one of the five basic responses to risk?

A. Delegate
B. Avoid
C. Mitigate
D. Accept

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.

References: http://www.dbpmanagement.com/15/5-ways-to-manage-risk

QUESTION 152
Your company was hired by a small healthcare provider to perform a technical assessment on the network.

What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use a scan tool like Nessus
B. Use the built-in Windows Update tool
C. Check MITRE.org for the latest list of CVE findings
D. Create a disk image of a clean Windows installation

Correct Answer: A

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.
The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based operating systems.
Note: Significant capabilities of Nessus include:
- Compatibility with computers and servers of all sizes.
- Detection of security holes in local or remote hosts.
- Detection of missing security updates and patches.
- Simulated attacks to pinpoint vulnerabilities.
- Execution of security tests in a contained environment.
- Scheduled security audits.

References: http://searchnetworking.techtarget.com/definition/Nessus

QUESTION 153
Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability.

What is this style of attack called?

A. zero-day
B. zero-hour
C. zero-sum
D. no-day

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software. References: https://en.wikipedia.org/wiki/Stuxnet

QUESTION 154

An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

<iframe src="http://www.vulnweb.com/updateif.php" style="display:none"></iframe>

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. SQL Injection
D. Browser Hacking

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 (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.
Different HTTP request methods, such as GET and POST, have different level of susceptibility to CSRF attacks and require different levels of protection due to their different handling by web browsers.

References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

QUESTION 155
It is a vulnerability in GNU's bash shell, discovered in September of 2014, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).

Which of the following vulnerabilities is being described?

A. Shellshock
B. Rootshock
C. Rootshell
D. Shellbash

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014.

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

QUESTION 156
When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.

What should you do?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.

References: https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_ConfigureScanEmailInboundAction.html

QUESTION 157

The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.

What tool can you use to view the network traffic being sent and received by the wireless router?

A. Wireshark
B. Nessus
C. Netcat
D. Netstat

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

Incorrect Answers:
B: Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.
C: Netcat (often abbreviated to nc) is a computer networking utility for reading from and writing to network connections using TCP or UDP.
D: Netstat provides network statistics.

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

QUESTION 158
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.

Based on this information, what should be one of your key recommendations to the bank?

A. Place a front-end web server in a demilitarized zone that only handles external web traffic
B. Require all employees to change their passwords immediately
C. Move the financial data to another server on the same IP subnet
D. Issue new certificates to the web servers from the root certificate authority

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.
References: https://en.wikipedia.org/wiki/DMZ_(computing)

QUESTION 159
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.

If a scanned port is open, what happens?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-ofstate Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.

References: https://capec.mitre.org/data/definitions/303.html

QUESTION 160
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

A. Split DNS
B. DNSSEC
C. DynDNS
D. DNS Scheme

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution. References: http://www.webopedia.com/TERM/S/split_DNS.html

QUESTION 161
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.

Which of the following tools is being described?
A. Aircrack-ng
B. Airguard
C. WLAN-crack
D. wificracker

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
Aircrack-ng is a complete suite of tools to assess WiFi network security.
The default cracking method of Aircrack-ng is PTW, but Aircrack-ng can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.

References: http://www.aircrack-ng.org/doku.php?id=aircrack-ng

QUESTION 162

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.

What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Private
B. Public
C. Shared
D. Root

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.
An attack may also reveal private keys of compromised parties.

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

QUESTION 163
In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.

Which Algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)
B. Wi-Fi Protected Access (WPA)
C. Wi-Fi Protected Access 2 (WPA2)
D. Temporal Key Integrity Protocol (TKIP)

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.

Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

References: https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html

QUESTION 164
This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.

Which of the following organizations is being described?

A. Payment Card Industry (PCI)
B. Center for Disease Control (CDC)
C. Institute of Electrical and Electronics Engineers (IEEE)
D. International Security Industry Organization (ISIO)

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information).

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

QUESTION 165
Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

A. Immediately stop work and contact the proper legal authorities.
B. Copy the data to removable media and keep it in case you need it.
C. Confront the client in a respectful manner and ask her about the data.

D. Ignore the data and continue the assessment until completed as agreed.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 166
Jesse receives an email with an attachment labeled “Court_Notice_21206.zip”. Inside the zip file is a file named “Court_Notice_21206.docx.exe” disguised as a word document. Upon execution, a window appears stating, “This word document is corrupt.” In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.

What type of malware has Jesse encountered?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
In computing, Trojan horse, or Trojan, is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.
References: https://en.wikipedia.org/wiki/Trojan_horse_(computing)

QUESTION 167
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 168
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 169
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 170
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 171
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 172
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 173
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 174
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 175
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 176
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 177
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 178
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 179
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 180
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 181
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 182
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 183
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 184
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

C.

A. ESP transport mode

B. AH permiscuous
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 185
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

C.

QUESTION 186

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.
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 187

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.

C.
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 188
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.
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 189
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

C.

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 190

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 191
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 192
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 193
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 194
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 195
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 196
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 197
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 198
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 199

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 200
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 201

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 202
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 203
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 204
The "gray box testing" methodology enforces what kind of restriction?

A. The internal operation of a system is only partly accessible to the tester.
B. 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 205
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 206
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
B. 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 207
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 208
Which of these options is the most secure procedure for storing backup tapes?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 209
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 210
Risks = Threats x Vulnerabilities is referred to as the:

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 211
Which of the following is designed to identify malicious attempts to penetrate systems?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 212
Which of the following is a low-tech way of gaining unauthorized access to systems?

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

Correct Answer: A

Section: MIX QUESTIONS
Explanation

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

QUESTION 213
PGP, SSL, and IKE are all examples of which type of cryptography?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

QUESTION 214
Which method of password cracking takes the most time and effort?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 215
What is the most common method to exploit the “Bash Bug” or “ShellShock" vulnerability?

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

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

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

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

QUESTION 216
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

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

Correct Answer: A

Section: MIX QUESTIONS
Explanation

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

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

QUESTION 217
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 218
Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

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

Correct Answer: A

Section: MIX QUESTIONS
Explanation

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

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

QUESTION 219
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Which tool can be used to perform session splicing attacks?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 220
Which of the following tools can be used for passive OS fingerprinting?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 221
You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 222
What does a firewall check to prevent particular ports and applications from getting packets into an organization?

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

Correct Answer: A

Section: MIX QUESTIONS
Explanation

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

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

QUESTION 223
You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

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

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

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

QUESTION 224
Which of the following types of firewalls ensures that the packets are part of the established session?

A. Stateful inspection firewall
B. Circuit-level firewall
C. Application-level firewall
D. Switch-level firewall

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 225
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:

- Policy – a policy provides a written set of principles, rules, or practices within an Organization.
- Response Plan/Strategy – after establishing organizational policies, now it is time to create a plan/strategy to handle incidents. This would include the creation of a backup plan.
- Communication – having a communication plan is necessary, due to the fact that it may be necessary to contact specific individuals during an incident.
- Documentation – it is extremely beneficial to stress that this element is particularly necessary and can be a substantial life saver when it comes to incident response.

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

QUESTION 226
Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'.

What technique is Ricardo using?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 227
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

QUESTION 228
Which of the following statements regarding ethical hacking is incorrect?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

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

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

QUESTION 229
Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 230
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

A. Password protected files
B. Hidden folders
C. BIOS password
D. Full disk encryption.

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 231
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.

An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is:
nmap 192.168.1.64/28.

Why he cannot see the servers?

A. The network must be down and the nmap command and IP address are ok.
B. He needs to add the command ""ip address"" just before the IP address.
C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.
D. He needs to change the address to 192.168.1.0 with the same mask.

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

QUESTION 232

Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

A. A new username and password
B. A fingerprint scanner and his username and password.
C. Disable his username and use just a fingerprint scanner.
D. His username and a stronger password.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 233
Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

A. A race condition is being exploited, and the operating system is containing the malicious process.
B. A page fault is occurring, which forces the operating system to write data from the hard drive.
C. Malware is executing in either ROM or a cache memory area.
D. Malicious code is attempting to execute instruction in a non-executable memory region.

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 234
Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

A. Blind SQLi
B. DMS-specific SQLi
C. Classic SQLi
D. Compound SQLi

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 235
In order to have an anonymous Internet surf, which of the following is best choice?

A. Use SSL sites when entering personal information
B. Use Tor network with multi-node
C. Use shared WiFi
D. Use public VPN

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 236
A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:

- Access List should be written between VLANs.
- Port security should be enabled for the intranet.
- A security solution which filters data packets should be set between intranet (LAN) and DMZ. -

A WAF should be used in front of the web applications.

According to the section from the report, which of the following choice is true?

A. MAC Spoof attacks cannot be performed.
B. Possibility of SQL Injection attack is eliminated.
C. A stateful firewall can be used between intranet (LAN) and DMZ.
D. There is access control policy between VLANs.

Correct Answer: C

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 237
Websites and web portals that provide web services commonly use the Simple Object Access Protocol SOAP. Which of the following is an incorrect definition or characteristics in the protocol?

A. Based on XML
B. Provides a structured model for messaging
C. Exchanges data between web services
D. Only compatible with the application protocol HTTP

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 238
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
B. He will activate OSPF on the spoofed root bridge.
C. He will repeat the same attack against all L2 switches of the network.
D. He will repeat this action so that it escalates to a DoS attack.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 239
A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.
B. As long as the physical access to the network elements is restricted, there is no need for additional measures.
C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
D. The operator knows that attacks and down time are inevitable and should have a backup site.

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 240
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A. The amount of time it takes to convert biometric data into a template on a smart card.
B. The amount of time and resources that are necessary to maintain a biometric system.
C. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.
D. How long it takes to setup individual user accounts.

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 241
Due to a slow down of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities
B. IT department would be telling employees who the boss is
C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
D. The network could still experience traffic slow down.

Correct Answer: C

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 242
In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 243
You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.

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

What is the main purpose of those static routes?

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

Correct Answer: D

Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 244
What is the correct process for the TCP three-way handshake connection establishment and connection termination?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 245
Emil uses nmap to scan two hosts using this command.

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

He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

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


What is his conclusion?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 246

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

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 247
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 248
Which protocol is used for setting up secured channels between two devices, typically in VPNs?

A. IPSEC
B. PEM
C. SET

D. PPP

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 249
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.

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

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 250
Which of the following Nmap commands will produce the following output?

Output:

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


A. nmap -sN -Ps -T4 192.168.1.1
B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1
C. nmap -sS -Pn 192.168.1.1
D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 251
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 252
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

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

Correct Answer: D

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 253
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 254
The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 255
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 256
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 257
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

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

Correct Answer: B

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
QUESTION 258
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 259
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 260
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 261
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 262
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 263

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 264

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 265

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 266
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 267
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 268

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 269

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 270

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 271
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 272
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 273
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 274
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 275
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 276
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 277
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 278
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 279

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 280
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 281
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 282
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 283
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 284
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 285
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 286
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 287
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 288
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

QUESTION 289
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 290
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 291
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

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
D. You need to run the ping command with root privileges

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 292
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 293
Which of the following is NOT an ideal choice for biometric controls?

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

Correct Answer: C
QUESTION 294

While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

A. Immediately stop work and contact the proper legal authorities
B. Ignore the data and continue the assessment until completed as agreed
C. Confront the client in a respectful manner and ask her about the data
D. Copy the data to removable media and keep it in case you need it

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 295
In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 296
Suppose you've gained access to your client's hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations has its file sharing enabled?

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

Section: MIX QUESTIONS
Explanation

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

Explanation/Reference:

QUESTION 297
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 298
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
QUESTION 299
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 300
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 301
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 302
LM hash is a compromised password hashing function. Which of the following parameters describe LM Hash:?

Section: MIX QUESTIONS
Explanation

Explanation/Reference:
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 303
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 304
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 305
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 306

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

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 307
What type of malware is it that restricts access to a computer system that it infects and demands that the user pay a certain amount of money, cryptocurrency, etc. to the operators of the malware to remove the restriction?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 308
The following are types of Bluetooth attack EXCEPT_____?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 309
A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 310
Which of the following is the BEST way to protect Personally Identifiable Information (PII) from being exploited due to vulnerabilities of varying web applications?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 311
A new wireless client that is 802.11 compliant cannot connect to a wireless network given that the client can see the network and it has compatible hardware and software installed. Upon further tests and investigation it was found out that the Wireless Access Point (WAP) was not responding to the association requests being sent by the wireless client. What MOST likely is the issue on this scenario?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 312
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

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

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 313
A software tester is randomly generating invalid inputs in an attempt to crash the program. Which of the following is a software testing technique used to determine if a software program properly handles a wide range of invalid input?

A. Mutating
B. Randomizing

C. Fuzzing
D. Bounding

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 314
What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

A. c:\compmgmt.msc
B. c:\gpedit
C. c:\ncpa.cpl
D. c:\services.msc

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 315
Which of the following is a wireless network detector that is commonly found on Linux?

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

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 316
Which specific element of security testing is being assured by using hash?
A. Authentication
B. Integrity
C. Confidentiality
D. Availability

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 317
Which of the following is a vulnerability in GNU's bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system?

A. Shellshock
B. Rootshell
C. Rootshock
D. Shellbash

Correct Answer: A
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 318
When security and confidentiality of data within the same LAN is of utmost priority, which IPSec mode should you implement?

A. AH Tunnel mode
B. AH promiscuous
C. ESP transport mode
D. ESP confidential

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 319
While performing online banking using a Web browser, Kyle receives an email that contains an image of a well-crafted art. Upon clicking the image, a new tab on the web browser opens and shows an animated GIF of bills and coins being swallowed by a crocodile. After several days, Kyle noticed that all his funds on the bank was gone. What Web browser-based security vulnerability got exploited by the hacker?

A. Clickjacking
B. Web Form Input Validation
C. Cross-Site Request Forgery
D. Cross-Site Scripting

Correct Answer: C
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 320
A hacker was able to easily gain access to a website. He was able to log in via the frontend user login form of the website using default or commonly used credentials. This exploitation is an example of what Software design flaw?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 321
Which type of cryptography does SSL, IKE and PGP belongs to?

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

Correct Answer: D
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 322
A recent security audit revealed that there were indeed several occasions that the company's network was breached. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

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

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 323
What are two things that are possible when scanning UDP ports? (Choose two.)

A. A reset will be returned
B. An ICMP message will be returned
C. The four-way handshake will not be completed
D. An RFC 1294 message will be returned

E. Nothing

Correct Answer: BE
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 324
(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.). Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?
What is odd about this attack? Choose the best answer.

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: OXA1D95 Ack: 0x53 Win: 0x400
...
05/20-17:06:58.685879 192.160.13.4:31337 ->
172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: 0XA1D95 Ack: 0x53 Win: 0x400
```


A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
B. This is back orifice activity as the scan comes from port 31337.
C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
D. These packets were crafted by a tool, they were not created by a standard IP stack.

Correct Answer: B
Section: MIX QUESTIONS
Explanation

Explanation/Reference:

QUESTION 325
Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by and IDS?

A. SYN scan
B. ACK scan
C. RST scan
D. Connect scan
E. FIN scan

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