312-50v10.160q

Number: 312-50v10
Passing Score: 800
Time Limit: 120 min

312-50v10

Certified Ethical Hacker v10 Exam

Exam A

QUESTION 1
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. Web site defacement vulnerability
C. SQL injection vulnerability
D. Cross-site Request Forgery vulnerability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.
Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. "GET/restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"
B. "GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"
C. "GET/restricted/bank.getaccount('Ned') HTTP/1.1 Host: westbank.com"
D. "GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of these is capable of searching for and locating rogue access points?

A. HIDS
B. NIDS
C. WISS
D. WIPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5

A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

A. White Hat
B. Suicide Hacker
C. Gray Hat
D. Black Hat

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
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 of the protocol?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
You have 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 toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

A. John the Ripper

B. SET
C. CHNTPW
D. Cain & Abel
Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

A. Cross-site request forgery
B. Cross-site scripting
C. Session hijacking
D. Server side request forgery

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
From the following table, identify the wrong answer in terms of Range (ft).

Standard	Range (ft)
802.11a	150-150
802.11b	150-150
802.11g	150-150
802.16(WiMax)	30 miles

A. 802.11b
B. 802.11g

C. 802.16(WiMax)
D. 802.11a
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
What would you enter, if you wanted to perform a stealth scan using Nmap?

A. nmap -sU
B. nmap -sS
C. nmap -sM
D. nmap -sT

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
You are doing an internal security audit and intend 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. Scan servers with MBSA
C. Telnet to every port on each server
D. Physically go to each server

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door.
In this case, we can say:

A. Although the approach has two phases, it actually implements just one authentication factor
B. The solution implements the two authentication factors: physical object and physical characteristic
C. The solution will have a high level of false positives
D. Biological motion cannot be used to identify people

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
What is not a PCI compliance recommendation?

A. Use a firewall between the public network and the payment card data.
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. Limit access to card holder data to as few individuals as possible.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
The "white box testing" methodology enforces what kind of restriction?

A. Only the internal operation of a system is known to the tester.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

A. SQL injection attack
B. Cross-Site Scripting (XSS)
C. LDAP Injection attack
D. Cross-Site Request Forgery (CSRF)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
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. wificracker
B. Airguard
C. WLAN-crack
D. Aircrack-ng

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
The following is part of a log file taken from the machine on the network with the IP address of 192.168.0.110:

Time:June 16 17:30:15 Port:20 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:17 Port:21 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:19 Port:22 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:21 Port:23 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:22 Port:25 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:23 Port:80 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:30 Port:443 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP

What type of activity has been logged?

A. Teardrop attack targeting 192.168.0.110
B. Denial of service attack targeting 192.168.0.105
C. Port scan targeting 192.168.0.110
D. Port scan targeting 192.168.0.105

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

A. nmap -A - Pn
B. nmap -sP -p-65535 -T5
C. nmap -sT -O -T0
D. nmap -A --host-timeout 99 -T1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Bob, your senior colleague, has sent you a mail regarding aa deal with one of the clients. You are requested to accept the offer and you oblige.
After 2 days, Bob denies that he had ever sent a mail.
What do you want to “know” to prove yourself that it was Bob who had send a mail?

A. Confidentiality
B. Integrity
C. Non-Repudiation

D. Authentication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
What is attempting an injection attack on a web server based on responses to True/False questions called?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?

A. Snort
B. Nmap
C. Cain & Abel
D. Nessus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 23
Which of the following will perform an Xmas scan using NMAP?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
Code injection is a form of attack in which a malicious user:

A. Inserts text into a data field that gets interpreted as code
B. Gets the server to execute arbitrary code using a buffer overflow
C. Inserts additional code into the JavaScript running in the browser
D. Gains access to the codebase on the server and inserts new code

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
The collection of potentially actionable, overt, and publicly available information is known as

A. Open-source intelligence
B. Human intelligence
C. Social intelligence
D. Real intelligence

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?

A. [cache:]
B. [site:]
C. [inurl:]
D. [link:]

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
This asymmetry cipher is based on factoring the product of two large prime numbers.

What cipher is described above?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 28
Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.
Which of the following types of firewalls can protect against SQL injection attacks?

A. Data-driven firewall
B. Stateful firewall
C. Packet firewall
D. Web application firewall

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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. DynDNS
B. DNS Scheme

C. DNSSEC
D. Split DNS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

A. Chosen-plaintext attack
B. Ciphertext-only attack
C. Adaptive chosen-plaintext attack
D. Known-plaintext attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend?

A. Command Injection Attacks
B. File Injection Attack
C. Cross-Site Request Forgery (CSRF)
D. Hidden Field Manipulation Attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which is the first step followed by Vulnerability Scanners for scanning a network?

A. TCP/UDP Port scanning
B. Firewall detection
C. OS Detection
D. Checking if the remote host is alive

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed. What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com
B. dnsnooping –rt update.antivirus.com
C. nslookup -norecursive update.antivirus.com
D. dns --snoop update.antivirus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 35
You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.

What kind of attack does the above scenario depict?

A. Botnet Attack
B. Spear Phishing Attack
C. Advanced Persistent Threats
D. Rootkit Attack

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36

Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?

A. Function Testing
B. Dynamic Testing
C. Static Testing
D. Fuzzing Testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 37
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?

A. The use of security agents in clients' computers
B. The use of DNSSEC
C. The use of double-factor authentication
D. Client awareness

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

A. Keyed Hashing
B. Key Stretching
C. Salting
D. Double Hashing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. -T0
B. -T5
C. -O
D. -A

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
Which of the following provides a security professional with most information about the system's security posture?

A. Wardriving, warchalking, social engineering
B. Social engineering, company site browsing, tailgating
C. Phishing, spamming, sending trojans
D. Port scanning, banner grabbing, service identification

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

A. The file reveals the passwords to the root user only.
B. The password file does not contain the passwords themselves.
C. He cannot read it because it is encrypted.
D. He can open it and read the user ids and corresponding passwords.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
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 computer is not using a private IP address.
B. The gateway is not routing to a public IP address.
C. The gateway and the computer are not on the same network.
D. The computer is using an invalid IP address.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?

A. Heuristic Analysis

B. Code Emulation
C. Integrity checking
D. Scanning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
An attacker scans a host with the below command. Which three flags are set? (Choose three.)

#nmap –sX host.domain.com

A. This is ACK scan. ACK flag is set
B. This is Xmas scan. SYN and ACK flags are set
C. This is Xmas scan. URG, PUSH and FIN are set
D. This is SYN scan. SYN flag is set

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal standpoint, 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: (none)
Explanation

Explanation/Reference:

QUESTION 48
Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

A. Internet Key Exchange (IKE)
B. Oakley
C. IPsec Policy Agent
D. IPsec driver

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 49
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines.
Which one of the following tools the hacker probably used to inject HTML code?

A. Wireshark
B. Ettercap
C. Aircrack-ng
D. Tcpdump

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
You are monitoring the network of your organizations. You notice that:

1. There are huge outbound connections from your Internal Network to External IPs
2. On further investigation, you see that the external IPs are blacklisted
3. Some connections are accepted, and some are dropped
4. You find that it is a CnC communication

Which of the following solution will you suggest?

A. Block the Blacklist IP's @ Firewall
B. Update the Latest Signatures on your IDS/IPS
C. Clean the Malware which are trying to Communicate with the External Blacklist IP's
D. Both B and C

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 51
Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy.

What is the main theme of the sub-policies for Information Technologies?

A. Availability, Non-repudiation, Confidentiality
B. Authenticity, Integrity, Non-repudiation
C. Confidentiality, Integrity, Availability
D. Authenticity, Confidentiality, Integrity

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

A. Omnidirectional antenna
B. Dipole antenna
C. Yagi antenna
D. Parabolic grid antenna

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
Why should the security analyst disable/remove unnecessary ISAPI filters?

A. To defend against social engineering attacks
B. To defend against webserver attacks
C. To defend against jailbreaking
D. To defend against wireless attacks

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
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. Randomizing
B. Bounding
C. Mutating
D. Fuzzing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?

A. -sP
B. -P
C. -r
D. -F

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by a coercion or torture?

A. Chosen-Cipher text Attack
B. Ciphertext-only Attack
C. Timing Attack
D. Rubber Hose Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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 whose credentials are known. It was written by sysinternals and has been integrated within the framework. The 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 used in the psexec module's 'smbpass' option?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?

A. Double quotation
B. Backslash C. Semicolon
D. Single quotation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
A virus that attempts to install itself inside the file it is infecting is called?

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?

A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
B. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
C. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
Sam is working as a pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?

A. Denial-of-Service
B. False Positive Generation
C. Insertion Attack
D. Obfuscating

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Cross-site request forgery involves:

A. A request sent by a malicious user from a browser to a server
B. Modification of a request by a proxy between client and server
C. A browser making a request to a server without the user's knowledge
D. A server making a request to another server without the user's knowledge

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65

```
ping -* 6 192.168.0.101
output
Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.101:
Packets: Sent=6, Received=6, Lost=0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
```

What does the option * indicate?

A. s
B. t
C. n
D. a

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
An Internet Service Provider (ISP) has a need to authenticate users connecting via analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is the most likely able to handle this requirement?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67
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?

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

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

D. Network-Based Intrusion Detection System

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
During the process of encryption and decryption, what keys are shared?

A. Private keys
B. User passwords
C. Public keys
D. Public and private keys

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
How does the Address Resolution Protocol (ARP) work?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

A. Black-box
B. Announced
C. White-box
D. Grey-box

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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 anti-virus program with a new one
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: (none)
Explanation

Explanation/Reference:

QUESTION 73
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 74
If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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: (none)
Explanation

Explanation/Reference:

QUESTION 76
Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentially, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Basic example to understand how cryptography works is given below:

SECURE (plain text)
+1 (+1 next letter.for example , the letter""T"" is used for "S" to encrypt.)
TFDVSF (encrypted text)
+=logic=>Algorithm
1=Factor=>Key

Which of the following choices true about cryptography?

A. Algorithm is not the secret; key is the secret.
B. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.
C. Secure Sockets Layer (SSL) use the asymmetric encryption both (public/private key pair) to deliver the shared session key and to achieve a communication way.
D. Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both encryption of plaintext and decryption of ciphertext.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
What is the difference between the AES and RSA algorithms?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
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: (none)
Explanation

Explanation/Reference:

QUESTION 79
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: (none)
Explanation

Explanation/Reference:

QUESTION 80
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: (none)
Explanation

Explanation/Reference:

QUESTION 81
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: (none)
Explanation

Explanation/Reference:

QUESTION 82
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.d
omain.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 INSOA srv1.domain.com. hostsrv1.do
main.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 who is 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 transferred the zone and enumerated the hosts.

Correct Answer: D

Section: (none)
Explanation
Explanation/Reference:

QUESTION 83
Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Application Layer
B. Data tier
C. Presentation tier
D. Logic tier

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system. B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.
D. Allocate funds for staffing of audit log review.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following Nmap commands will produce the following output?

Output:

```
Staring 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 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 –sT –sX –Pn –p 1-65535 192.168.1.1 B.
nmap –sN –Ps –T4 192.168.1.1

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus
B. Multipart virus
C. Macro virus
D. Stealth virus

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
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: (none)
Explanation

Explanation/Reference:

QUESTION 91
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: (none)
Explanation

Explanation/Reference:

QUESTION 92
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: (none)
Explanation

Explanation/Reference:

QUESTION 93
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,
“”11111111111111111111111111111111””);
}
Output:
Segmentation fault

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
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 attempts 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 UPL 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. Session Fixation
B. HTML Injection
C. HTTP Parameter Pollution
D. Clickjacking Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
John the Ripper is a technical assessment tool used to test the weakness of which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
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: (none)
Explanation
Explanation/Reference:

QUESTION 97
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: (none)
Explanation

Explanation/Reference:

QUESTION 98
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
Which service in a PKI will vouch for the identity of an individual or company?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
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: (none)
Explanation
Explanation/Reference:

QUESTION 102
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

A. Internal, Blackbox
B. External, Blackbox
C. External, Whitebox
D. Internal, Whitebox

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103

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


What is the code written for?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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. Make sure that legitimate network routers are configured to run routing protocols with authentication.
B. Disable all routing protocols and only use static routes
C. Only using OSPFv3 will mitigate this risk.
D. Redirection of the traffic cannot happen unless the admin allows it explicitly.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. IANA
B. CAPTCHA
C. IETF

D. WHOIS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
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. A stateful firewall can be used between intranet (LAN) and DMZ.
B. There is access control policy between VLANs.
C. MAC Spoof attacks cannot be performed.
D. Possibility of SQL Injection attack is eliminated.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 109
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. FISMA
B. ISO/IEC 27002
C. HIPAA
D. COBIT

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
Jesse receives an email with an attachment labeled “Court_Notice_21206.zip”. Inside the zip 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. Worm
B. Macro Virus
C. Key-Logger
D. Trojan

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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. Session management vulnerability
C. SQL injection vulnerability
D. Cross-site Request Forgery vulnerability

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 112
An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gain access to the DNS server and redirect the direction *www.google.com* to his own IP address. Now when the employees of the office wants to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 113
Which results will be returned with the following Google search query? site:target.com site:Marketing.target.com accounting

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 114
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. Malicious code is attempting to execute instruction a non-executable memory region.
B. A page fault is occuring, which forces the operating system to write data from the hard drive.
C. A race condition is being exploited, and the operating system is containing the malicious process.
D. Malware is executing in either ROM or a cache memory area.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 115
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization’s interest and your liabilities as a tester?

A. Service Level Agreement

B. Project Scope
C. Rules of Engagement
D. Non-Disclosure Agreement

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 117
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. Escalation
C. Scanning
D. Enumeration

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 118
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. Accept
B. Delegate
C. Mitigate
D. Avoid

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 119
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

A. openssl s_client –site www.website.com:443
B. openssl_client –site www.website.com:443
C. openssl_client –connect www.website.com:443
D. openssl s_client –connect www.website.com:443

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 120
Which of the following describes the characteristics of a Boot Sector Virus?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 121
John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

A. Increase his technical skills
B. Read the incident manual every time it occurs
C. Select someone else to check the procedures
D. Create an incident checklist

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 122
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
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 reflects the changes.
Which type of vulnerability is present on this site?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data. Which of the following terms best matches the definition?

A. Attack
B. Vulnerability
C. Threat
D. Risk

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

A. Armitage
B. Nikto
C. Metasploit
D. Nmap

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-211223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

A. He needs to gain physical access.
B. He must perform privilege escalation.

C. He already has admin privileges, as shown by the “501” at the end of the SID.
D. He needs to disable antivirus protection.

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 128
Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He is determined that the application is vulnerable to SQL injection and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

A. NoSQL injection
B. Blind SQL injection
C. Union-based SQL injection
D. Error-based SQL injection

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 129
You have successfully logged on a Linux system. You want to now cover your track. Your login attempt may be logged on several files located in /var/log. Which file does NOT belong to the list:

A. wtmp
B. user.log
C. btmp
D. auth.log

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
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: (none)
Explanation

Explanation/Reference:

QUESTION 131
The "Gray-box testing" methodology enforces what kind of restriction?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132

You have just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk. What is one of the first things you should do when given the job?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 133
The purpose of a _____is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Analyzer
B. Wireless Jammer
C. Wireless Access Point
D. Wireless Access Control List

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
What does the –oX flag do in an Nmap scan?

A. Perform an Xmas scan
B. Perform an eXpress scan
C. Output the results in truncated format to the screen D. Output the results in XML format to a file

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 135
During an Xmas scan, what indicates a port is closed?

A. RST
B. SYN
C. ACK
D. No return response

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 136
Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: -Verifies success or failure of an attack – Monitors system activities – Detects attacks that a network-based IDS fails to detect. – Near real-time detection and response – Does not require additional hardware – Lower entry cost. Which type of IDS is best suited for Tremp's requirements?

A. Network-based IDS
B. Open source-based IDS
C. Host-based IDS
D. Gateway-based IDS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 137
Which of the following parameters describe LM Hash:

I – The maximum password length is 14 characters
II – There are no distinctions between uppercase and lowercase
III – The password is split into two 7-byte halves

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 138
Which of the following is not a Bluetooth attack?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 139
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
A pen-tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Winprom
B. Libpcap
C. Winpsw
D. Winpcap

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Analyst is investigating proxy logs and found out that one of the internal user visited website storing suspicious java scripts. After opening one of them, he noticed that it is very hard to understand the code and that all codes differ from the typical java script. What is the name of this technique to hide the code and extend analysis time?

A. Steganography
B. Code encoding
C. Obfuscation
D. Encryption

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 142
During the security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 143
While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap –Pn –p –sl kiosk.adobe.com www.riaa.com kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using “-sl” with Nmap?

A. Conduct stealth scan
B. Conduct ICMP scan

C. Conduct IDLE scan
D. Conduct silent scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 144
What is the process of logging, recording, and resolving events that take place in an organization?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
During a black-box 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. Circuit
B. Stateful
C. Application
D. Packet Filtering

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
You are analyzing a traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs. – 192.168.8.0/24. What command you would use?

A. tshark –net 192.255.255.255 mask 192.168.8.0
B. wireshark –capture –local –masked 192.168.8.0 –range 24
C. sudo tshark –f “net 192.168.8.0/24”
D. wireshark –fetch “192.168.8/*”

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
Initiating an attack against targeted business and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits. What type of attack is outlined in the scenario?

A. Heartbeat Attack
B. Spear Phishing Attack
C. Shellshock Attack
D. Watering Hole Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148

What kind of detection techniques is being used in antivirus software that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment?

A. Behavioral based
B. Heuristics based
C. Honypot based
D. Cloud based

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149
Which security strategy requires using several, varying methods to protect IT systems against attacks?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150
Which utility will tell you in real time which ports are listening or in another state?

A. Netsat
B. Loki
C. Nmap
D. TCPView

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
Which of the following statements regarding ethical hacking is incorrect?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 152
Why containers are less secure than virtual machines?

A. Host OS on containers has a larger surface attack.
B. Containers are attached to the same virtual network.
C. Containers may fulfill disk space of the host.
D. A compromise container may cause a CPU starvation of the host.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
Which of the following is a component of a risk assessment?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 154
Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers. The time a hacker spends performing research to locate this information about a company is known as?

A. Exploration
B. Investigation
C. Reconnaissance
D. Enumeration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 155
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, DELETE, PUT, TRACE) using NMAP script engine. What Nmap script will help you with this task?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 156
Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

A. Accept the risk
B. Introduce more controls to bring risk to 0%
C. Mitigate the risk
D. Avoid the risk

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 157
Which of the following Linux commands will resolve a domain name into IP address?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 158
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. Nessus
B. Jack the ripper
C. Tcpdump
D. Ethereal

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
Which of the following steps for risk assessment methodology refers to vulnerability identification?

A. Assigns values to risk probabilities; Impact values
B. Determines risk probability that vulnerability will be exploited (High, Medium, Low)
C. Identifies sources of harm to an IT system (Natural, Human, Environmental)
D. Determines if any flaws exist in systems, policies, or procedures

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 160
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. Network sniffer
C. Intrusion Prevention System (IPS)

D. Vulnerability scanner

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: