312-50v10.142q

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

312-50v10

Certified Ethical Hacker v10 Exam

Exam A

QUESTION 1
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 2
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 3

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 4

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 5

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 6
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 7
Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library? This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 9
Which protocol is used for setting up secure channels between two devices, typically in VPNs?

A. PPP

B. IPSEC
C. PEM
D. SET
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

A. SHA-2
B. SHA-3
C. SHA-1
D. SHA-0

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Traceroute
B. Hping
C. TCP ping
D. Broadcast ping

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13

Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

A. Bootrom Exploit
B. iBoot Exploit
C. Sandbox Exploit
D. Userland Exploit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

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 15
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 16
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 17
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 18
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 19
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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
Shellshock allowed an unauthorized user to gain access to a server. It affected many Internet-facing services, which OS did it not directly affect?

A. Linux
B. Unix
C. OS X
D. Windows

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 29
Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

A. None of these scenarios compromise the privacy of Alice's data
B. Agent Andrew subpoenas Alice, forcing her to reveal her private key. However, the cloud server successfully resists Andrew's attempt to access the stored data
C. Hacker Harry breaks into the cloud server and steals the encrypted data
D. Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating system of that computer to launch further attacks. What process would help him?

A. Banner Grabbing
B. IDLE/IPID Scanning
C. SSDP ScanningD. UDP Scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
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 41
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 42
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 43
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?

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 44
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 45
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 46

A.

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 47
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 48
If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?
-sP
B. -P
C. -r

D. -F

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 49
In Risk Management, how is the term "likelihood" related to the concept of "threat?"

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

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 50
Which of the following statements is TRUE?

A. Sniffers operate on Layer 2 of the OSI model
B. Sniffers operate on Layer 3 of the OSI modelC. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
D. Sniffers operate on the Layer 1 of the OSI model.

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

QUESTION 51
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

A.

B. Recovery
C. Containment
D. Eradication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
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 53
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?
Double quotation
B. Backslash
C. Semicolon
D. Single quotation

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
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 55
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 56

A.

Sam is working as s 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 57
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 58

```
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 59
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 60
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 61
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 62
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 63
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 64
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 65
Which regulation defines security and privacy controls for Federal information systems and organizations?

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

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 66
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 67
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 68
The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What is the following options can be useful to ensure the integrity of the data?

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

Correct Answer: A **Section:**
(none) Explanation

Explanation/Reference:

QUESTION 69
What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

A. Passive
B. Active
C. Reflective
D. Distributive

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drown based on these scan results?

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
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 and resources that are necessary to maintain a biometric system
B. How long it takes to setup individual user accounts
C. The amount of time it takes to be either accepted or rejected from when an individual provides identification and authentication information
D. The amount of time it takes to convert biometric data into a template on a smart card

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
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. SQL Injection
C. Browser Hacking
D. Cross-Site Scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
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 this action so that is escalates to a DoS attack.
D. He will repeat the same attack against all L2 switches of the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78

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 79
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 80
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 81

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 82
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 83
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 84
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 85
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 86
A new wireless client is configured to join an 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 87
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 88
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: (none)
Explanation

Explanation/Reference:

QUESTION 89
A large mobile telephony and data network operator has a data center 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: (none)
Explanation

Explanation/Reference:

QUESTION 90
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: (none)
Explanation
Explanation/Reference:

QUESTION 91
The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

A. Port scan targeting 192.168.1.103
B. Teardrop attack targeting 192.168.1.106
C. Denial of service attack targeting 192.168.1.103
D. Port scan targeting 192.168.1.106

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
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: (none)
Explanation

Explanation/Reference:

QUESTION 93
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: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which type of security feature stops vehicles from crashing through the doors of a building?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
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: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications an unpatched security flaws in a computer system?

A. Nessus
B. Metasploit
C. Maltego
D. Wireshark

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
You want to analyze packets on your wireless network. Which program would you use?

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

Correct Answer: A
Section: (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
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. Public
B. Private
C. Shared
D. Root
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 111
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 112
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 113
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 114
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 115
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 116
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 117
It is an entity or event with the potential to adversely impact a system through unauthorized acces, 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 118
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 acces right before allowing access to protected information and UI controls.

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 119
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 120
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 121
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 122
An LDAP directory can be used to store information similar to a SQL database. LDAP uses a ____ database structure instead of SQL's _____ structure. Because of this, LDAP has difficulty representing many-to-one relationships.

A. Strict, Abstract
B. Simple, Complex

C. Relational, Hierarchical
D. Hierarchical, Relational

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
What is the purpose of DNS AAAA record?

A. Address prefix record
B. Address database record
C. Authorization, Authentication and Auditing record
D. IPv6 address resolution record

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 124
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 125

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
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 127
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 128
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 129
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 130
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 promiscous mode?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
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 132
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 133
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. A firewall IPTable
B. FTP Server rule
C. A Router IPTable
D. An Intrusion Detection System

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 134
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 organization is being described?

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

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 135
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 136
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 137
A common cryptographical tool is the use of XOR. XOR the following binary values: 10110001 00111010

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

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 138
Why containers are less secure that virtual machine?

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 139
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 140
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. Block the Blacklist IP's @ Firewall as well as Clean the Malware which are trying to Communicate with the External Blacklist IP's.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 141
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized 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. tcpsplice
B. Burp
C. Hydra
D. Whisker

Correct Answer: D

Section: (none)
Explanation
Explanation/Reference:

QUESTION 142
DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?

A. Spanning tree
B. Dynamic ARP Inspection (DAI)
C. Port security
D. Layer 2 Attack Prevention Protocol (LAPP)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference: