312-50v10.exam.96q

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

312-50v10

Certified Ethical Hacker v10 Exam

Exam A

QUESTION 1

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 2

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 3

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 4

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 5
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 6
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 7
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 8

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 9

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 10
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 11
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 12
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 13
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 14

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.

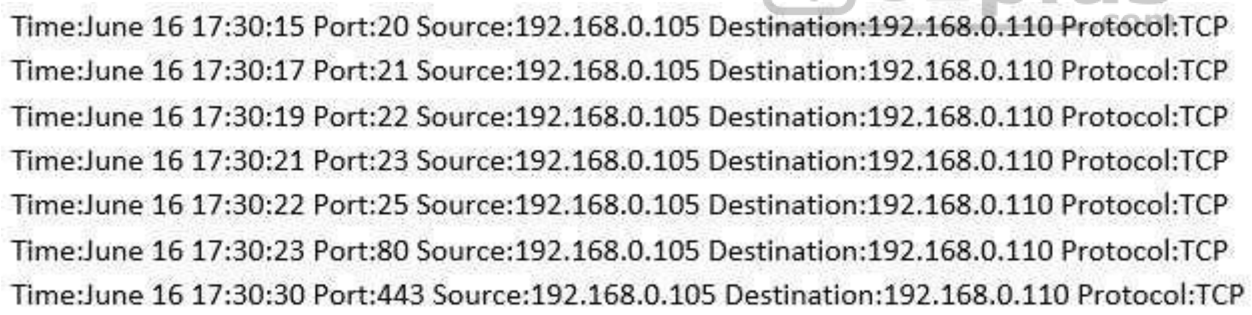
Which of the following tools is being described?

A. wificracker
B. Airguard
C. WLAN-crack
D. Aircrack-ng

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
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 16

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 17

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 18

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 19

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 20
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 21
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 22

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 23

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 24

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 25
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network.
What should Bob do to avoid this problem?

A. Disable unused ports in the switches
B. Separate students in a different VLAN
C. Use the 802.1x protocol
D. Ask students to use the wireless network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient’s consent, similar to email spamming?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28

Which of the following program infects the system boot sector and the executable files at the same time?
A. Stealth virus
B. Polymorphic virus
C. Macro virus
D. Multipartite Virus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29

An IT employee got a call from one of our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?

A. The employees cannot provide any information; but, anyway, he/she will provide the name of the person in charge.
B. Since the company's policy is all about Customer Service, he/she will provide information.

C. Disregarding the call, the employee should hang up.
D. The employee should not provide any information without previous management authorization.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
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 31
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 32
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 33
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 34
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 35
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 36
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 37
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 38
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 39
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 40
Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

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

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
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 42
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 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?

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 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

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47

Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company. What is the main security risk associated with this scenario?

A. External script contents could be maliciously modified without the security team knowledge
B. External scripts have direct access to the company servers and can steal the data from there
C. There is no risk at all as the marketing services are trustworthy
D. External scripts increase the outbound company data traffic which leads greater financial losses

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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 49
Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends “many” IP packets, based on the average number of packets sent by all origins and using some thresholds.
In concept, the solution developed by Bob is actually:

A. Just a network monitoring tool
B. A signature-based IDS
C. A hybrid IDS
D. A behavior-based IDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
When tuning security alerts, what is the best approach?

A. Tune to avoid False positives and False Negatives
B. Rise False positives Rise False Negatives
C. Decrease the false positives
D. Decrease False negatives

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52

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 53

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

What should you do?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54

You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are staring an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

A. Event logs on the PC
B. Internet Firewall/Proxy log
C. IDS log
D. Event logs on domain controller

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

A. 123
B. 161
C. 69
D. 113

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
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 57

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 58

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59

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 60
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 61
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 62
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 63
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 64

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 65

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

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

A. The 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 66

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 67

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 20011-03-15 11:06 NMAP scan report for 172.16.40.65 Host ip 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 68

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 69

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 70

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 71
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 72
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 73

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

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

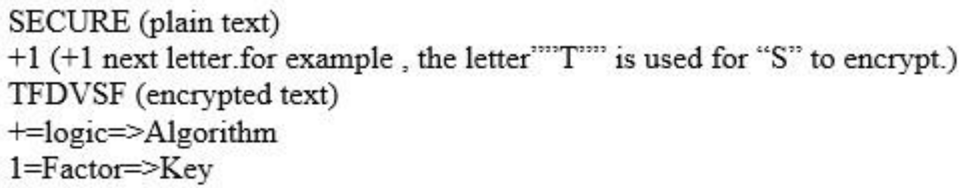
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74

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 75
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 76
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 77
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 78
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 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

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 84

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 85

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

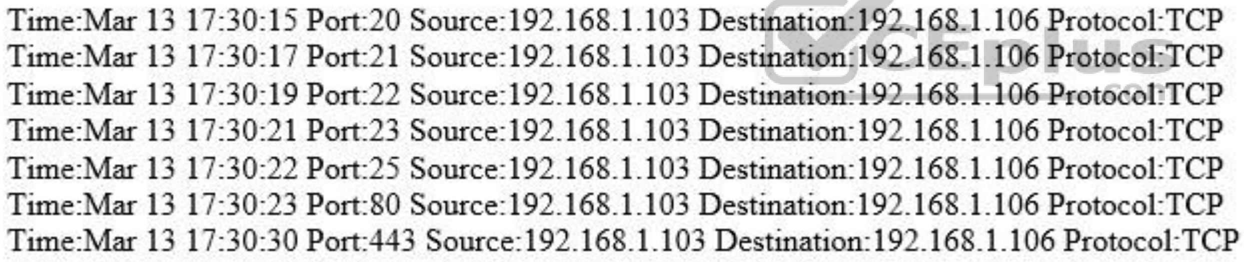
B. Containment phase
C. Identification phase
D. Recovery phase

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86

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 87

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 88

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 89

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 90
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 91
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 92
In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

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

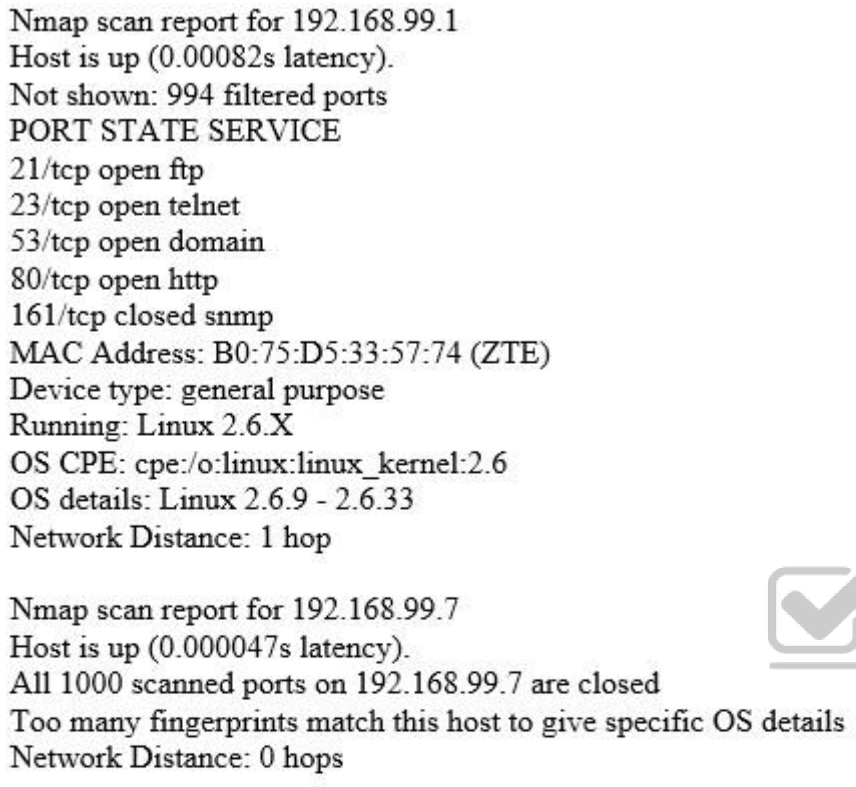
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Emil uses nmap to scan two hosts using this command:

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

He receives this output:



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

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

What is his conclusion?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
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 95
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 96
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: