312-50v10.exam.85q

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

312-50v10

Certified Ethical Hacker v10 Exam

Exam A

QUESTION 1
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 2
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 3
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 4
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 5
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 tool 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 6
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 7
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 8
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 9
Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

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

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
QUESTION 10
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 11
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 12
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 13
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 14
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 15
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 16
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 17
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 18
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 19
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 20
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 21
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 22
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

A. ACK flag scanning
B. TCP Scanning
C. IP Fragment Scanning
D. Inverse TCP flag scanning

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
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 24
You perform a scan of your company’s network and discover that TCP port 123 is open. What services by default run on TCP port 123?

A. Telnet
B. POP3
C. Network Time Protocol
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

A. SSH communications are encrypted it's impossible to know who is the client or the server
B. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
C. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server
D. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
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 27
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 28
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 29
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 30

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 31
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 32
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 33
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 34
You are monitoring the network of your organizations. You notice that:

- There are huge outbound connections from your Internal Network to External IPs
- On further investigation, you see that the external IPs are blacklisted
- Some connections are accepted, and some are dropped

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 35
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 36
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 37
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 38
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 39
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 40
What is the least important information when you analyze a public IP address in a security alert?

A. ARP
B. Whois
C. DNS
D. Geolocation

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41

You are the Network Admin, and you get a compliant that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

A. Traffic is Blocked on UDP Port 53 B.
Traffic is Blocked on UDP Port 80 C.
Traffic is Blocked on UDP Port 54
D. Traffic is Blocked on UDP Port 80

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
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 43
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 44
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 45
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 46
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 47
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system whose credentials are known. It was written by sysinternals and has been integrated within the framework. The penetration testers successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48

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

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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 50
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 51
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 52

```
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 53
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 54
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 55
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 56
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 57
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 58
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 59
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 60
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 61
If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

A. Spoof Scan
B. TCP SYN
C. TCP Connect scan
D. Idle scan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the value is?

A. Polymorphism
B. Escrow
C. Collusion
D. Collision

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
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 64
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 65
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 66
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 67
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 68
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses.
In which order should he perform these steps?

A. The sequence does not matter. Both steps have to be performed against all hosts.
B. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
C. First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.
D. The port scan alone is adequate. This way he saves time.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
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 70
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 71
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 72
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 73
What does a firewall check to prevent particular ports and applications from getting packets into an organization?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?

Code:
#include <string.h> int main(){ char buffer[8];
strcpy(buffer,
““11111111111111111111111111111””);
}

Output:
Segmentation fault

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Scenario:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
3. Victim clicks to the interesting and attractive content url.
4. Attacker creates a transparent 'iframe' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or url that exists in the transparent 'iframe' which is setup by the attacker.

What is the name of the attack which is mentioned in the scenario?

A. Session Fixation
B. HTML Injection
C. HTTP Parameter Pollution
D. Clickjacking Attack

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
John the Ripper is a technical assessment tool used to test the weakness of which of the following?

A. Usernames

B. File permissions
C. Firewall rulesets D. Passwords

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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 78
A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems.

What is the best security policy concerning this setup?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
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 80
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

A. Both pharming and phishing attacks are identical.
B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
C. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
D. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
What is the role of test automation in security testing?

A. It is an option but it tends to be very expensive.
B. It should be used exclusively. Manual testing is outdated because of low spend and possible test setup inconsistencies.
C. Test automation is not usable in security due to the complexity of the tests.
D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.
B. A biometric system that bases authentication decisions on physical attributes.

C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. An authentication system that uses passphrases that are converted into virtual passwords.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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 85
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:

https://vceplus.com/