312-50v10.exam.55q

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

312-50v10

Certified Ethical Hacker v10 Exam

Exam A

QUESTION 1
PGP, SSL, and IKE are all examples of which type of cryptography?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of the following is considered as one of the most reliable forms of TCP scanning?

A. TCP Connect/Full Open Scan
B. Half-open Scan
C. NULL ScanD. Xmas Scan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 3

Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

A. ICMP Echo scanning
B. SYN/FIN scanning using IP fragments
C. ACK flag probe scanning
D. IPID scanning

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Which of the following is the BEST way to defend against network sniffing?

A. Restrict Physical Access to Server Rooms hosting Critical Servers
B. Use Static IP Address
C. Using encryption protocols to secure network communications
D. Register all machines MAC Address in a Centralized Database

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
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 6
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 7
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 8

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 9
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 10
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 11
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 12
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 13
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 14

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 15
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 16
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 17
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 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

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 20
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 21
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 22
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 23
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 24
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 25
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 26
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 27
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 28
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 29
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 30
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 31
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 32
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 33
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 34
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 35
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best nmap command you will use?

A. nmap -T4 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -O 10.10.0.0/24

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

QUESTION 36
.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 38
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 39

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 40
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 41
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 42
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 43
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 44
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 45
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 46
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 47
If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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 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
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Privilege Escalation
B. Shoulder-Surfing
C. Hacking Active Directory
D. Port Scanning

Correct Answer: A
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?

A. Double quotation
B. Backslash
C. Semicolon
D. Single quotation
Correct Answer: D
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: