EC-Council

Hackers are here. Where are you?

About The Exam: CEH v11

Number of Questions: 125

Test Duration: 4 Hours

Test Format: Multiple Choice

Test Delivery: ECC EXAM, VUE

Exam Prefix: 312-50 (ECC EXAM), 312-50 (VUE)

Passing Score:

In order to maintain the high integrity of our certification exams, EC-Council Exams are provided in multiple forms (I.e. different question banks). Each form is carefully analyzed through beta testing with an appropriate sample group under the purview of a committee of subject matter experts that ensure that each of our exams not only has academic rigor but also has real world applicability. We also have a process to determine the difficulty rating of each question. The individual rating then contributes to an overall cut score for each exam form. To ensure each form has equal assessment standards, cut scores are set on a "per exam form" basis. Depending on which exam form is challenged, cut scores can range from 60% to 85%.

Question 1:

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

A. Hash value

B. Digital signature

C. Private key

D. Digital certificate

Answer: D

Question 2:

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

A. All are tools that can be used not only by hackers, but also security personnel

B. All are hacking tools developed by the legion of doom

C. All are tools that are only effective against Windows

D. All are tools that are only effective against Linux

E. All are DDOS tools

Answer: E

Question 3:

A zone file consists of which of the following Resource Records (RRs)?

A. DNS, NS, PTR, and MX records

B. SOA, NS, A, and MX records

C. DNS, NS, AXFR, and MX records

D. SOA, NS, AXFR, and MX records

Answer: B

Question 4:

Which of the following is the primary objective of a rootkit?

A. It creates a buffer overflow

B. It provides an undocumented opening in a program

C. It replaces legitimate programs

D. It opens a port to provide an unauthorized service

Answer: C

Question 5:

CompanyXYZ has asked you to assess the security of their perimeter email gateway. From your

office in New York, you craft a specially formatted email message and send it across the Internet to

an employee of CompanyXYZ. The employee of CompanyXYZ is aware of your test. Your email

message looks like this:

From: jim_miller@companyxyz.com

To: michelle_saunders@companyxyz.com Subject: Test message

Date: 4/3/2017 14:37

The employee of CompanyXYZ receives your email message.

This proves that CompanyXYZ's email gateway doesn't prevent what?

A. Email Harvesting

B. Email Masquerading

C. Email Phishing

D. Email Spoofing

Answer: D

Question 6:

When discussing passwords, what is considered a brute force attack?

A. You wait until the password expires

B. You create hashes of a large number of words and compare it with the encrypted passwords

C. You attempt every single possibility until you exhaust all possible combinations or discover the

password

D. You load a dictionary of words into your cracking program

E. You threaten to use the rubber hose on someone unless they reveal their password

Answer: C

Question 7:

You are trying to break into a highly classified top-secret mainframe computer with highest

security system in place at Merclyn Barley Bank located in Los Angeles.

You know that conventional hacking doesn't work in this case, because organizations such as banks

are generally tight and secure when it comes to protecting their systems.

In other words, you are trying to penetrate an otherwise impenetrable system.

How would you proceed?

A. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or

more "zombies" and "bots"

B. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy

the necessary exploits from these hackers and target the bank's network

C. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the

Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques

D. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or

disgruntled employee, and offer them money if they'll abuse their access privileges by providing you

with sensitive information

Answer: D

Question 8:

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

This is an attack that takes advantage of a web site vulnerability in which the site displays

content that includes un-sanitized user-provided data.

What is this attack?

A. URL Traversal attack

B. Buffer Overflow attack

C. Cross-site-scripting attack

D. SQL Injection

Answer: C

Question 9:

You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.

Your peer, Peter Smith who works at the same department disagrees with you.

He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.

What is Peter Smith talking about?

A. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to

detect these attacks

B. Continuous Spam e-mails cannot be blocked by your security system since spammers use different

techniques to bypass the filters in your gateway

C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will

not be able to detect these attacks

D. Untrained staff or ignorant computer users who inadvertently become the weakest link in your

security chain

Answer: D

Question 10:

Which of the following are well known password-cracking programs?

A. Jack the Ripper

B. L0phtcrack

C. John the Ripper

D. Netbus

E. NetCat

Answer: B,C

Question 11:

An LDAP directory can be used to store information similar to a SQL database. LDAP uses a

_____ database structure instead of SQL's _____ structure. Because of this, LDAP has difficulty

representing many-to-one relationships.

A. Strict, Abstract

B. Hierarchical, Relational

C. Simple, Complex

D. Relational, Hierarchical

Answer: B

Question 12:

To reach a bank web site, the traffic from workstations must pass through a firewall. You

have been asked to review the firewall configuration to ensure that workstations in network

10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following

firewall rules meets this requirement?

A. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then

permit

B. If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then

permit

C. If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then

permit

D. If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443)

then permit

Answer: A

Question 13:

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

A. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

B. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account

C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques

D. Package the Sales.xls using Trojan wrappers and telnet them back your home computer

Answer: C

Question 14:

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

A. tcp.port ==21 || tcp.port ==22

B. tcp.port ==21

C. tcp.port = 23

D. tcp.port != 21

Answer: A

Question 15:

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", the user is directed to a phishing site.

Which file does the attacker need to modify?

A. Sudoers

B. Hosts

C. Boot.ini

D. Networks

Answer: B

Question 16:

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 security breach was a false positive.

B. The network devices are not all synchronized.

C. Proper chain of custody was not observed while collecting the logs.

D. The attacker altered or erased events from the logs.

Answer: B

Question 17:

What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?

A. Replay attack

B. Traffic analysis attack

C. Meet-in-the-middle attack

D. Man-in-the-middle attack

Answer: C

Question 18:

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

A. Eavesdropping

B. Piggybacking

C. Social engineering

D. Tailgating

Answer: C

Question 19:

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

A. Clickjacking

B. Cross-Site Scripting

C. Cross-Site Request Forgery

D. Web form input validation

Answer: C

Question 20:

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

A. KDC

B. CR

C. CBC

D. CA

Answer: D

Question 21:

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. LDAP Injection attack

B. Cross-Site Scripting (XSS)

C. SQL injection attack

D. Cross-Site Request Forgery (CSRF)

Answer: B

Question 22:

User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?

A. Application

B. Transport

C. Session

D. Presentation

Answer: D

Question 23:

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client. What is a possible source of this problem?

A. The WAP does not recognize the client's MAC address

B. The client cannot see the SSID of the wireless network

C. Client is configured for the wrong channel

D. The wireless client is not configured to use DHCP

Answer: A

Question 24:

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

A. –r

B. –F

C. –P

D. –sP

Answer: B

Question 25:

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

A. SOA

B. biometrics

C. single sign on

D. PKI

Answer: D

Question 26:

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

A. Social engineering

B. Piggybacking

C. Tailgating

D. Eavesdropping

Answer: A

Question 27:

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

A. Traceroute

B. Hping

C. TCP ping

D. Broadcast ping

Answer: B

Question 28:

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

A. OS Detection

B. Firewall detection

C. TCP/UDP Port scanning

D. Checking if the remote host is alive

Answer: D

Question 29:

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

A. Using encryption protocols to secure network communications

B. Register all machines MAC Address in a Centralized Database

C. Use Static IP Address

D. Restrict Physical Access to Server Rooms hosting Critical Servers

Answer: A

Question 30:

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

A. Only the external operation of a system is accessible to the tester.

B. The internal operation of a system in only partly accessible to the tester.

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

D. The internal operation of a system is completely known to the tester.

Answer: B

Question 31:

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

A. Behavioral based

B. Heuristics based

C. Honeypot based

D. Cloud based

Answer: D

Question 32:

A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.

Based on this information, what should be one of your key recommendations to the bank?

A. Place a front-end web server in a demilitarized zone that only handles external web traffic

B. Require all employees to change their anti-virus program with a new one

C. Move the financial data to another server on the same IP subnet

D. Issue new certificates to the web servers from the root certificate authority

Answer: A

Question 33:

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the Transport Layer Security (TLS) protocols defined in RFC6520.What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A. Public

B. Private

C. Shared

D. Root

Answer: B

Question 34:

Which of the following is assured by the use of a hash?

A. Authentication

B. Confidentiality

C. Availability

D. Integrity

Answer: D

Question 35:

The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive. Which of the following is being described?

A. Multi-cast mode

B. Promiscuous mode

C. WEM

D. Port forwarding

Answer: B

Question 36:

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.

Answer: D

Question 37:

By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you are and something you remember

B. Something you have and something you know

C. Something you know and something you are

D. Something you have and something you are

Answer: B

Question 38:

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

Answer: C

Question 39:

Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal standpoint, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities

B. IT department would be telling employees who the boss is

C. Not informing the employees that they are going to be monitored could be an invasion of privacy.

D. The network could still experience traffic slow down.

Answer: C

Question 40:

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The “ps” command shows that the “nc” file is running as process, and the netstat command shows the “nc” process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

A. File system permissions

B. Privilege escalation

C. Directory traversal

D. Brute force login

Answer: A

Question 41:

When discussing passwords, what is considered a brute force attack?

A. You attempt every single possibility until you exhaust all possible combinations or discover the password

B. You threaten to use the rubber hose on someone unless they reveal their password

C. You load a dictionary of words into your cracking program

D. You create hashes of a large number of words and compare it with the encrypted passwords

E. You wait until the password expires

Answer: A

Question 42:

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures. Which tool can be used to perform session splicing attacks?

A. tcpsplice

B. Burp

C. Hydra

D. Whisker

Answer: D

Question 43:

An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

A. Make sure that legitimate network routers are configured to run routing protocols with authentication.

B. Disable all routing protocols and only use static routes

C. Only using OSPFv3 will mitigate this risk.

D. Redirection of the traffic cannot happen unless the admin allows it explicitly.

Answer: A

Question 44:

Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.

Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

A. Hardware, Software, and Sniffing.

B. Hardware and Software Keyloggers.

C. Passwords are always best obtained using Hardware key loggers.

D. Software only, they are the most effective.

Answer: A

Question 45:

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

Answer: D

----------END----------