EC-Council

Exam Questions 312-50v9

Certified Ethical Hacker Exam

NEW QUESTION 1
An attacker gains access to a Web server's database and display the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

A. Insufficient security management
B. Insufficient database hardening
C. Insufficient exception handling
D. Insufficient input validation

Answer: D

NEW QUESTION 2
What does a firewall check to prevent particularports and applications from getting packets into an organizations?

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

Answer: A

NEW QUESTION 3
Which of the followingtypes of firewalls ensures that the packets are part of the established session?

A. Switch-level firewall
B. Stateful inspection firewall
C. Application-level firewall
D. Circuit-level firewall

Answer: B

NEW QUESTION 4
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?

A. Bounding
B. Mutating
C. Puzzing
D. Randomizing

Answer: C

NEW QUESTION 5
An attacker changes the profile information of a particular user on a target website (the victim). 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.
<frame src=http://www/vulnweb.com/updataif.php Style="display:none"></iframe> What is this type of attack (that can use either HTTP GET or HRRP POST) called?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. SQL Injection
D. Browser Hacking

Answer: A

NEW QUESTION 6
It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up windows, webpage,or email warning from what looks like an officialauthority. It explains your computer has been locked because of possible illegal activities and demands payment before you can access your files and programs again.
Which term best matches this definition?

A. Spyware
B. Adware
C. Ransomware
D. Riskware

Answer: C

NEW QUESTION 7
The configuration allows a wired or wireless network interface controller to pass all trafice it receives to thecentral processing unit (CPU), rather than passing only the frames that the controller is intended to receive.
Which of the following is being described?

A. WEM
B. Multi-cast mode
C. Promiscuous mode
D. Port forwarding

Answer: B

NEW QUESTION 8
Perspective clients wantto see sample reports from previous penetration tests. What should you do next?

A. Share full reports, not redacted.
B. Share full reports, with redacted.
C. Decline but, provide references.
D. Share reports, after NDA is signed.

Answer: B

NEW QUESTION 9
Risk = Threats x Vulnerabilities is referred to as the:

A. Threat assessment
B. Disaster recovery formula
C. BIA equation
D. Risk equation

Answer: D

NEW QUESTION 10
An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, digital Subscriber Line (DSL), wireless data services, and virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is most likely able to handle this requirement?

A. DIAMETER
B. Kerberos
C. RADIUS
D. TACACS+

Answer: D

NEW QUESTION 10
While performing online banking using a web browser, a user receives an email that contains alink 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. Cross-Site Request Forgery
B. Cross-Site Scripting
C. Web form input validation
D. Clickjacking

Answer: A

NEW QUESTION 11
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. Copy the data to removable media and keep it in case you need it.
B. Ignore the data and continue the assessment until completed as agreed.
C. Confront theclient on a respectful manner and ask her about the data.
D. Immediately stop work and contact the proper legal authorities.

Answer: D

NEW QUESTION 13
When you are testing a web application, it is very useful to employ a prosy tool to save every request and response.Nyou 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. Dimitry
C. Proxychains
D. Maskgen

Answer: A

NEW QUESTION 17
Which of the following is not a Bluetooth attack?

A. Bluejacking
B. Bluedriving
C. Bluesnarfing
D. Bluesmaking

Answer: B

NEW QUESTION 20
It is a short-range wireless communication technology intended to replace the cables connecting portables of fixed deviceswhile maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short- range wireless connection.
Which of the following terms best matches the definition?

A. Bluetooth
B. Radio-Frequency Identification
C. WLAN
D. InfraRed

Answer: A

NEW QUESTION 23
You have successfully gained access to your client's internal network and successfully comprised a linux server which is part of the internal IP network. You want to know which
Microsoft Windows workstation have the sharing enabled.
Which port would you see listeningon these Windows machines in the network?

A. 1443
B. 3389
C. 161
D. 445

Answer: D

NEW QUESTION 25
Which of the following is the BEST way to defend against network sniffing?

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

Answer: A

NEW QUESTION 26
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Inherent Risk
B. ResidualRisk
C. Deferred Risk
D. Impact Risk

Answer: B

NEW QUESTION 31
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing inconcluding the Operating System (OS) version installed. Considering the NMAP result below, which of the follow is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report
for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80 /tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tec open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

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

Answer: A

NEW QUESTION 32
You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?

A. c:\services.msc
B. c:\ncpa.cp
C. c:\compmgmt.msc
D. c:\gpedit

Answer: C

NEW QUESTION 34
The NMAP command above performs which of the following?

A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan

Answer: A

NEW QUESTION 39
Which of these options is the most secure procedure for strong backup tapes?

A. In a climate controlled facility offsite
B. Inside the data center for faster retrieval in afireproof safe
C. In a cool dry environment
D. On a different floor in the same building

Answer: A

NEW QUESTION 44
A company's security states that all web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.
B. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
C. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
D. Attempts by attacks to access the user and password information stores in the company's SQL database.

Answer: C

NEW QUESTION 46
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. Move the financial data to another server on the same IP subnet
B. Place a front-end web server in a demilitarized zone that only handles external web traffic
C. Issue new certificates to the web servers from the root certificate authority
D. Require all employees to change their passwords immediately

Answer: A

NEW QUESTION 49
During a blackbox pen test you attempt to pass IRC traffic over post 80/TCP from a compromised web enabled host. The traffic gets blocked; however outbound HTTP traffic is unimpeded.
What type of firewall is inspecting outbound traffic?

A. Circuit
B. Packet Filtering
C. Application
D. Stateful

Answer: C

NEW QUESTION 54
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping but you didn't get any response back.
What is happening?

A. TCP/IP doesn't support ICMP.
B. ICMP could be disabled on the target server.
C. The ARP is disabled on the target server.
D. You need to run the ping command with root privileges.

Answer: A

NEW QUESTION 57
You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.
What tool will help you with the task?

A. Armitage

B. Dimitry
C. cdpsnarf
D. Metagoofil

Answer: D

NEW QUESTION 58
It isan entity or event with the potential to adversely impact a system through unauthorized access destruction disclosures denial of service or modification of data.
Which of the following terms best matches this definition?

A. Threat
B. Attack
C. Risk
D. Vulnerability

Answer: A

NEW QUESTION 59
When you return to your desk after a lunch break, you notice a strange email in your inbox. The senders is someone you did business with recently but the subject line has strange characters in it.
What should you do?

A. Forward the message to your company’s security response team and permanently delete the message from your computer.
B. Delete the email and pretend nothing happened.
C. Forward the message to your supervisor andask for her opinion on how to handle the situation.
D. Reply to the sender and ask them for more information about the message contents.

Answer: A

NEW QUESTION 64
You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from the server will not be caught by a Network Based Intrusion Detection System (NIDS).
Which is the best way to evade the NIDS?

A. Out of band signaling
B. Encryption
C. Alternate Data Streams
D. Protocol Isolation

Answer: B

NEW QUESTION 65
You are performing a penetration test. You achieved access via a bufferoverflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator’s bank account password and login information for the administrator’s bitcoin account.
What should you do?

A. Do not transfer the money but steal the bitcoins.
B. Report immediately to the administrator.
C. Transfer money from the administrator’s account to another account.
D. Do not report it and continue the penetration test.

Answer: B

NEW QUESTION 66
You have compromised a server on a network and successfully open a shell. You aimed to identify all operating systems running on the network. However, as you attemptto fingerprint all machines in the machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server:~$nmap –T4 –O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxxx. QUITTING!
```

What seems to be wrong?

A. The outgoing TCP/IP fingerprinting is blocked by the host firewall.
B. This is a common behavior for a corrupted nmap application.
C. OS Scan requires root privileged.
D. The nmap syntax is wrong.

Answer: D

NEW QUESTION 71
The “Gray box testing” methodology enforces what kind of restriction?

A. Only the external operation of a system is accessible to the tester.
B. Only the internal operation of a system is known to the tester.
C. The internal operation of a system is completely known to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Answer: D

NEW QUESTION 72
You are usingNMAP to resolve domain names into IP addresses for a ping sweep later. Which of the following commands looks for IP addresses?

A. >host –t ns hackeddomain.com
B. >host –t AXFR hackeddomain.com
C. >host –t soa hackeddomain.com
D. >host –t a hackeddomain.com

Answer: D

NEW QUESTION 75
What is the most common method to exploit the “Bash Bug” or ShellShock” vulnerability?

A. SSH
B. SYN Flood
C. Manipulate format strings in text fields
D. Through Web servers utilizing CGI (CommonGateway Interface) to send a malformed environment variable to a vulnerable Web server

Answer: D

NEW QUESTION 80
Your company was hired by a small healthcare provider to perform a technical assessment on the network.
What is the best approach for discovering vulnerabilities on a Windows-based computer?

A. Use the built-in Windows Update tool
B. Create a disk imageof a clean Windows installation
C. Check MITRE.org for the latest list of CVE findings
D. Used a scan tool like Nessus

Answer: D

NEW QUESTION 82
You’ve just been hired to perform a pentest on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.
What is one of the first thing you should to when the job?

A. Start the wireshark application to start sniffing network traffic.
B. Establish attribution to suspected attackers.
C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
D. Interview all employees in the company to rule out possible insider threats.

Answer: C

NEW QUESTION 85
The security concept of “separation of duties” is most similar to the operation ofwhich type of security device?

A. Bastion host
B. Honeypot
C. Firewall
D. Intrusion Detection System

Answer: C

NEW QUESTION 90
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

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

Answer: C

NEW QUESTION 92
The “Black box testing” methodology enforces which kind of restriction?

A. Only the external operation of a systemis accessible to the tester
B. The internal operation of a system is completely known to the tester.
C. Only the internal operation of a system is known to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Answer: A

NEW QUESTION 97
Using Windows CMD, how would an attacker list all the shares to which the current user context hasaccess?

A. NET CONFIG
B. NET USE
C. NET FILE
D. NET VIEW

Answer: D

NEW QUESTION 101
Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

A. Verity access right before allowing access to protected information and UI controls
B. Use security policies and procedures to define and implement proper security settings
C. Validate and escape all information sent over to a server
D. Use digital certificates to authenticate a server prior to sending data

Answer: A

NEW QUESTION 102
The “white box testing” methodology enforces what kind of restriction?

A. The internal operation of a system is completely known to the tester.
B. Only the internal operation of a system is known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. The internal operation of a system is only partly accessible to the tester.

Answer: A

NEW QUESTION 105
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do this fast and efficiently you must user regular expressions.
Which command-line utility are you most likely to use?

A. Notepad
B. MS Excel
C. Grep
D. Relational Database

Answer: C

NEW QUESTION 106
Ricardo wants to send secret messages to acompetitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message, the technique provides 'security through obscurity'. What technique is Ricardo using?

A. RSA algorithm
B. Steganography
C. Encryption
D. Public-key cryptography

Answer: B

NEW QUESTION 111
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark,and EtherPeek?

A. Nessus
B. Tcptraceroute
C. Tcptrace
D. OpenVAS

Answer: C

NEW QUESTION 115
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 shallscript 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 the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function providedby 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.
Which kind of vulnerability must be present to make this remote attack possible?

A. Filesystem permissions
B. Brute Force Login
C. Privilege Escalation
D. Directory Traversal

Answer: D

NEW QUESTION 120

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

A. Sniffing
B. Social engineering
C. Scanning
D. Eavesdropping

Answer: B

NEW QUESTION 122
Your team has won a contract to infiltrate an organization. The company wants to have the attack be a realistic as possible; therefore, they did not provide any information besides the company name.
What should be thefirst step in security testing the client?

A. Scanning
B. Escalation
C. Enumeration
D. Reconnaissance

Answer: D

NEW QUESTION 123
Which of the following is considered the best way to prevent Personally Identifiable Information (PII) from web application vulnerabilities?

A. Use encrypted communications protocols to transmit PII
B. Use full disk encryption on all hard drives to protect PII
C. Use cryptographic storage to store all PII
D. Use a security token to log onto into all Web application that use PII

Answer: A

NEW QUESTION 126
Session splicing is an IDS evasiontechnique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.
Which tool can used to perform session splicing attacks?

A. Hydra
B. Burp
C. Whisker
D. Tcpsplice

Answer: C

NEW QUESTION 127
The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate theSLE, ARO, and ALE. Assume the EF = 1 (100%).
What is the closest approximate cost of this replacement and recovery operation per year?

A. $100
B. $146
C. 440
D. 1320

Answer: B

NEW QUESTION 128
This asymmetry cipther is based on factoring the product of two large prime numbers. What cipher is described above?

A. SHA
B. RC5
C. RSA
D. MD5

Answer: C

NEW QUESTION 132
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website byinserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known toincorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.
What type of attack is outlined in the scenario?

A. Watering Hole Attack
B. Spear Phising Attack
C. Heartbleed Attack
D. Shellshock Attack

Answer: A

NEW QUESTION 135
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGI's?

A. Snort
B. Dsniff
C. Nikto
D. John the Ripper

Answer: C

NEW QUESTION 139
What isa “Collision attach” in cryptography?

A. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
B. Collision attacks try to break the hash into three parts to get the plaintext value.
C. Collision attacks try to find two inputs producing the same hash.
D. Collision attacks try to get the public key

Answer: C

NEW QUESTION 141
A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?

A. Mitigate
B. Avoid
C. Accept
D. Delegate

Answer: D

NEW QUESTION 146
The Open Web Application Security Project (OWASP) isthe worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP’s Top Ten Project most Critical Web application Security Rules?

A. Injection
B. Cross site Scripting
C. Cross site Request Forgery
D. Path Disclosure

Answer: A

NEW QUESTION 149
After trying multiple exploits, you’ve gained root access to a Centos 6 answer. To ensure you maintain access. What would you do first?

A. Disable IPTables
B. Create User Account
C. Downloadand Install Netcat
D. Disable Key Services

Answer: C

NEW QUESTION 150
In Risk Management, how is the term “likelihood” related to the concept of “threat?”

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

Answer: D

NEW QUESTION 154
When you are collecting information to perform a dataanalysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.
What command will help you to search files using Google as a search engine?

A. site:target.com file:xls username password email
B. domain: target.com archive:xls username password email
C. site: target.com filetype:xls username password email
D. inurl: target.com filename:xls username password email

Answer: C

NEW QUESTION 156
You just set up a security system in your network. In what kind of system would you find thefollowing string of characters used as a rule within its configuration?
alert tcp any any ->192.168.100.0/24 21 (msg: "FTP on the network!";)

A. A firewall IPTable
B. A Router IPTable
C. An Intrusion Detection System
D. FTP Server rule

Answer: C

NEW QUESTION 161
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such as audit?

A. Port scanner
B. Protocol analyzer
C. Vulnerability scanner
D. Intrusion Detection System

Answer: C

NEW QUESTION 164
Which of the following is designed to indentify malicious attempts to penetrate systems?

A. Proxy
B. Router
C. Firewall
D. Intrusion Detection System

Answer: D

NEW QUESTION 166
......