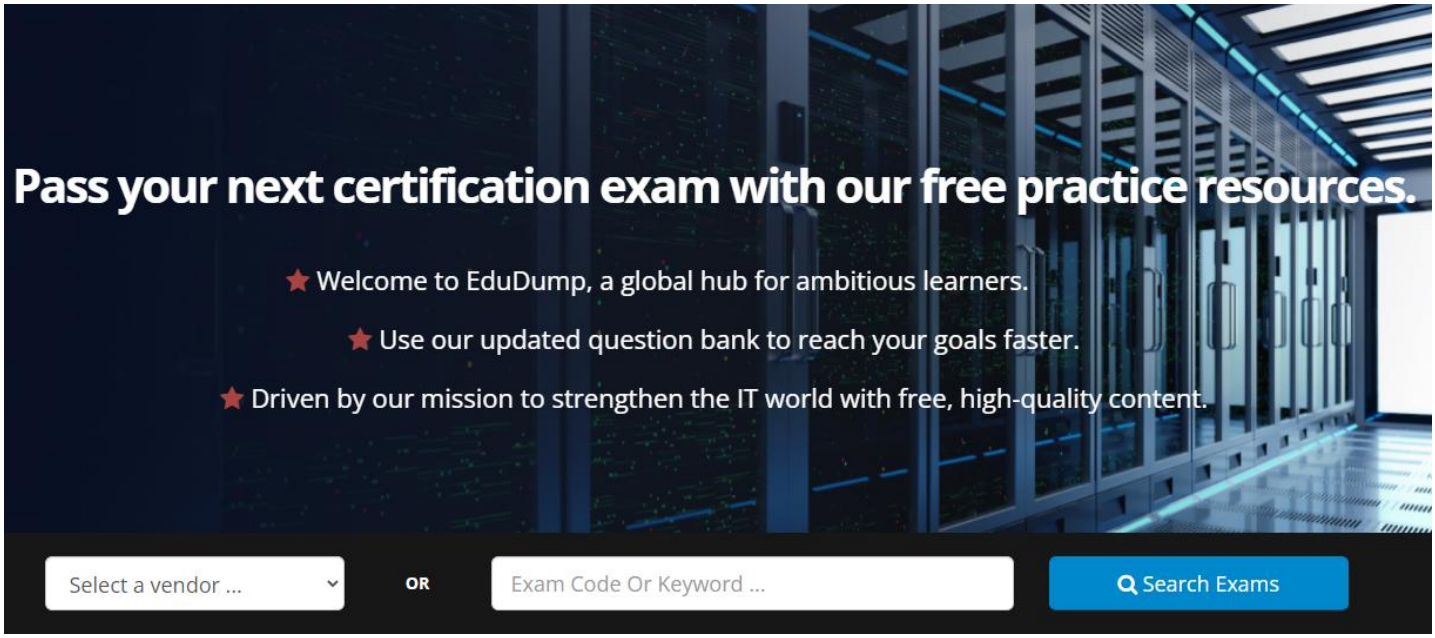

Security & Privacy
ActualVCE respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.

Instant Download
After Payment, our system will send you the products you purchase in mailbox in a minute after payment. If not received within 2 hours, please contact ActualVCE.

365 Days Free Updates
Free update is available within 365 days after your purchase. After 365 days, you will get 50% discounts for updating.

Try Before Buy
ActualVCE offers free demo of each product. You can check out the interface, question quality and usability of our practice exams before you decide to buy.

95%	97%	98%
Said the test questions were almost same	Passed the exams with the material	Found the study quides effective and helpful

https://www.edudump.com/

Leading Professional Certification Hub & Verified Exam Community Prep

Exam : **312-50v10**

Title : Certified Ethical Hacker Exam (CEH v10)

Vendor : EC-COUNCIL

Version : DEMO

NO.1 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. Delegate

B. Avoid

C. Mitigate

D. Accept

Answer: A

Explanation

There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.

References:

http://www.dbpmanagement.com/15/5-ways-to-manage-risk

NO.2 Matthew received an email with an attachment named "YouWon$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file.

Without his knowledge, the file copies itself to Matthew's APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

A. Key-logger

B. Trojan

C. Worm

D. Macro Virus

Answer: B

NO.3 Due to a slowdown of normal network operations, 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.

Answer: C

NO.4 Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength

B. AES 1024 bit strength

C. RSA 512 bit strength

D. AES 512 bit strength

Answer: A

NO.5 The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

A. Multiple keys for non-repudiation of bulk data

B. Different keys on both ends of the transport medium
C. Bulk encryption for data transmission over fiber
D. The same key on each end of the transmission medium
Answer: D

NO.6 A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following 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/tcp     open          ipp
9100/tcp    open
MAC Address: 00:00:48:0D:EE:89
```

A. The host is likely a printer.
B. The host is likely a Windows machine.
C. The host is likely a Linux machine.
D. The host is likely a router.
Answer: A
Explanation
The Internet Printing Protocol (IPP) uses port 631.
References: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

NO.7 A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites. 77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?
A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0
Answer: B

NO.8 TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote

device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?

A. nmap
B. ping
C. tracert
D. tcpdump
Answer: D

NO.9 What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response
Answer: F

NO.10 A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:
NMAP -n -sS -P0 -p 80 ***.***.**.**
What type of scan is this?

A. Quick scan
B. Intense scan
C. Stealth scan
D. Comprehensive scan
Answer: C

NO.11 Which of the following Nmap commands would be used to perform a stack fingerprinting?

A. Nmap -O -p80 <host(s.>
B. Nmap -hU -Q<host(s.>
C. Nmap -sT -p <host(s.>
D. Nmap -u -o -w2 <host>
E. Nmap -sS -0p targe
Answer: B

NO.12 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 password file does not contain the passwords themselves.
B. He can open it and read the user ids and corresponding passwords.
C. The file reveals the passwords to the root user only.
D. He cannot read it because it is encrypted.
Answer: A

NO.13 John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

A. Create an incident checklist.

B. Select someone else to check the procedures.

C. Increase his technical skills.

D. Read the incident manual every time it occurs.

Answer: C

NO.14 What are two things that are possible when scanning UDP ports? (Choose two.)

A. A reset will be returned

B. An ICMP message will be returned

C. The four-way handshake will not be completed

D. An RFC 1294 message will be returned

E. Nothing

Answer: B E

NO.15 You are performing a penetration test. You achieved access via a buffer overflow 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. Report immediately to the administrator

B. Do not report it and continue the penetration test.

C. Transfer money from the administrator's account to another account.

D. Do not transfer the money but steal the bitcoins.

Answer: A

NO.16 The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

A. Have the network team document the reason why the rule was implemented without prior manager approval.

B. Monitor all traffic using the firewall rule until a manager can approve it.

C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.

D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

NO.17 A covert channel is a channel that

A. transfers information over, within a computer system, or network that is outside of the security policy.
B. transfers information over, within a computer system, or network that is within the security policy .
C. transfers information via a communication path within a computer system, or network for transfer of data.
D. transfers information over, within a computer system, or network that is encrypted.
Answer: A

NO.18 Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?
A. Maltego
B. Cain & Abel
C. Metasploit
D. Wireshark
Answer: A
Explanation
Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva.
Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.
References: https://en.wikipedia.org/wiki/Maltego

NO.19 The "gray box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is only partly accessible to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. Only the internal operation of a system is known to the tester.
Answer: A
Explanation
A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.
References: https://en.wikipedia.org/wiki/Gray_box_testing

NO.20 In order to have an anonymous Internet surf, which of the following is best choice?
A. Use SSL sites when entering personal information
B. Use Tor network with multi-node
C. Use shared WiFi
D. Use public VPN
Answer: B

NO.21 Which type of antenna is used in wireless communication?

A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional
Answer: A

NO.22 When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender 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. Reply to the sender and ask them for more information about the message contents.
C. Delete the email and pretend nothing happened
D. Forward the message to your supervisor and ask for her opinion on how to handle the situation
Answer: A
Explanation
By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.
References:
https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_Confi

NO.23 What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you've compromised and gained root access to?
A. Install Cryptcat and encrypt outgoing packets from this server.
B. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.
C. Use Alternate Data Streams to hide the outgoing packets from this server.
Answer: B

NO.24 Which of the following is an example of two factor authentication?
A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID
Answer: D

NO.25 The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?
A. Investigate based on the maintenance schedule of the affected systems.
B. Investigate based on the service level agreements of the systems.

C. Investigate based on the potential effect of the incident.
D. Investigate based on the order that the alerts arrived in.
Answer: C

NO.26 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 same value is?
A. Collision
B. Collusion
C. Polymorphism
D. Escrow
Answer: A

NO.27 Which method of password cracking takes the most time and effort?
A. Brute force
B. Rainbow tables
C. Dictionary attack
D. Shoulder surfing
Answer: A
Explanation
Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.
References: https://en.wikipedia.org/wiki/Password_cracking

NO.28 Which of the following steps for risk assessment methodology refers to vulnerability identification?
A. Determines if any flaws exist in systems, policies, or procedures
B. Assigns values to risk probabilities; Impact values.
C. Determines risk probability that vulnerability will be exploited (High. Medium, Low)
D. Identifies sources of harm to an IT system. (Natural, Human. Environmental)
Answer: C

NO.29 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. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
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. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account
Answer: C

NO.30 Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet

B. Nessus

C. Netstumbler

D. Abel

Answer: A

Explanation

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b,

802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

References: https://en.wikipedia.org/wiki/Kismet_(software)

NO.31 While performing online banking using a Web browser, Kyle receives an email that contains an image of a well-crafted art. Upon clicking the image, a new tab on the web browser opens and shows an animated GIF of bills and coins being swallowed by a crocodile. After several days, Kyle noticed that all his funds on the bank was gone. What Web browser-based security vulnerability got exploited by the hacker?

A. Clickjacking

B. Web Form Input Validation

C. Cross-Site Request Forgery

D. Cross-Site Scripting

Answer: C

NO.32 A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.

B. Create a document that will crash the computer when opened and send it to friends.

C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.

D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

Answer: D

NO.33 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

Answer: C

NO.34 What port number is used by LDAP protocol?
A. 110
B. 389
C. 464
D. 445
Answer: B

NO.35 In Risk Management, how is the term "likelihood" related to the concept of "threat?"
A. Likelihood is the probability that a threat-source will exploit a vulnerability.
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 vulnerability is a threat-source.
Answer: A
Explanation
The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.
References:
http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attac