Vendor:EC-COUNCIL

Exam Code:312-50V9

Exam Name: Certified Ethical Hacker Exam V9

Version: Demo

QUESTION 1

Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

A. Sarbanes-Oxley Act (SOX)

B. Gramm-Leach-Bliley Act (GLBA)

C. Fair and Accurate Credit Transactions Act (FACTA)

D. Federal Information Security Management Act (FISMA)

Correct Answer: A Section: (none)

QUESTION 2

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 new username and password

B. A fingerprint scanner and his username and password.

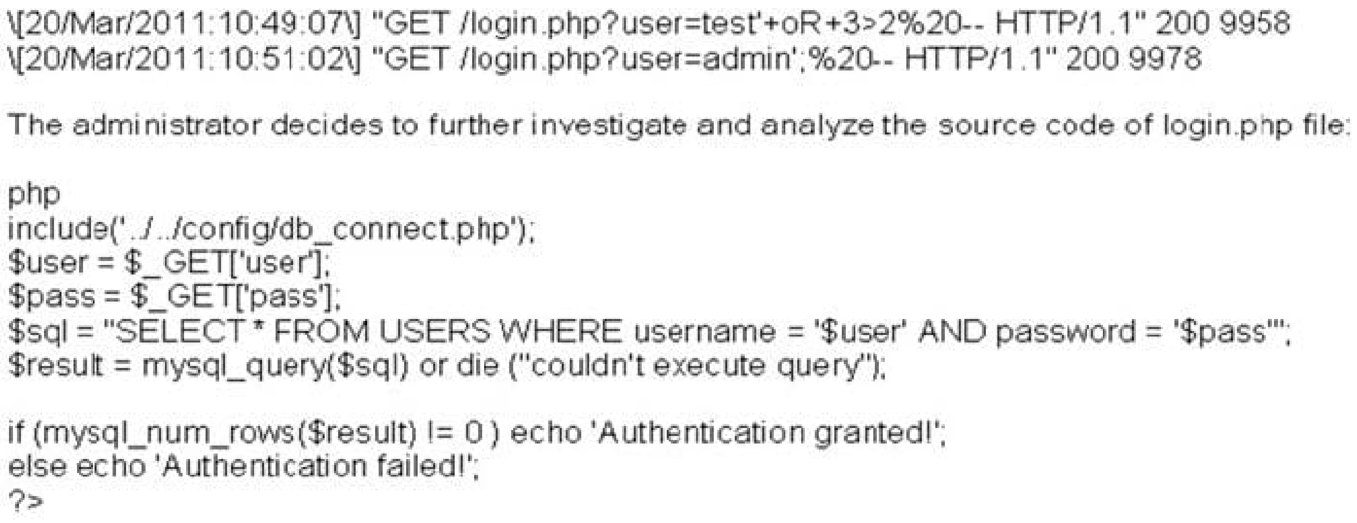
C. Disable his username and use just a fingerprint scanner.

D. His username and a stronger password.

Correct Answer: B Section: (none)

QUESTION 3

A security administrator notices that the log file of the company\\'s webserver contains suspicious entries:



```
\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978
```

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. command injection.

B. SQL injection.

C. directory traversal.

D. LDAP injection.

Correct Answer: B Section: (none)

QUESTION 4

A consultant has been hired by the V.P. of a large financial organization to assess the company\\'s security posture. During the security testing, the consultant comes across child pornography on the V.P.\\'s computer. What is the consultant\\'s obligation to the financial organization?

A. Say nothing and continue with the security testing.

B. Stop work immediately and contact the authorities.

C. Delete the pornography, say nothing, and continue security testing.

D. Bring the discovery to the financial organization\\'s human resource department.

Correct Answer: B Section: (none)

QUESTION 5

Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log

B. ./snort -dev -l ./log

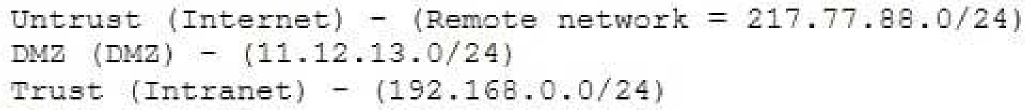
C. ./snort -dev -o ./log

D. ./snort -dev -p ./log

Correct Answer: B Section: (none)

QUESTION 6

A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:



```
Untrust (Internet) - (Remote network = 217.77.88.0/24)
DMZ (DMZ) - (11.12.13.0/24)
Trust (Intranet) - (192.168.0.0/24)
```

The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?

A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389

B. Permit 217.77.88.12 11.12.13.50 RDP 3389

C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389

D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

Correct Answer: B Section: (none)

QUESTION 7

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

A. Firewall-management policy

B. Acceptable-use policy

C. Remote-access policy

D. Permissive policy

Correct Answer: C Section: (none)

QUESTION 8

A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.

Which sort of trojan infects this server?

A. Botnet Trojan

B. Turtle Trojans

C. Banking Trojans

D. Ransomware Trojans

Correct Answer: A Section: (none)

In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. A coordinated DDoS attack by multiple botnet machines also resembles a zombie horde attack.

Incorrect Answers:

B: Turtle Trojans are about getting backdoor access to an intruder.

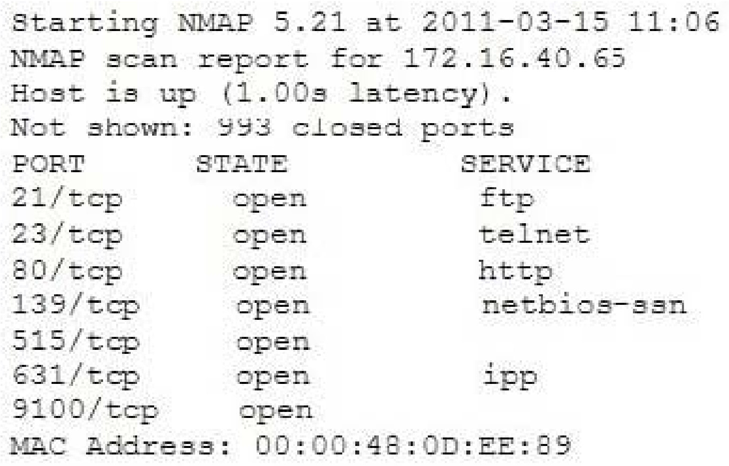
C: A Banker Trojan-horse (commonly called Banker Trojan) is a malicious program used in an attempt to obtain confidential information about customers and clients using online banking and payment systems.

D: Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system\\'s hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan.

References: https://en.wikipedia.org/wiki/Botnet

QUESTION 9

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.

Correct Answer: A Section: (none)

The Internet Printing Protocol (IPP) uses port 631.

References: https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

---

QUESTION 10

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 in the protocol?

A. Based on XML

B. Provides a structured model for messaging

C. Exchanges data between web services

D. Only compatible with the application protocol HTTP

Correct Answer: D Section: (none)

QUESTION 11

What information should an IT system analysis provide to the risk assessor?

A. Management buy-in

B. Threat statement

C. Security architecture

D. Impact analysis

Correct Answer: C Section: (none)

QUESTION 12

What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

A. Legal, performance, audit

B. Audit, standards based, regulatory

C. Contractual, regulatory, industry

D. Legislative, contractual, standards based

Correct Answer: D Section: (none)