Vendor: ECCouncil

Exam Code: 312-50v9

Exam Name: Certified Ethical Hacker Exam V9

Version: Demo

QUESTION 1
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

Correct Answer: B

QUESTION 2
Which of the following incident handling process phases is responsible for defining rules, creating a back-up plan, and testing the plans for an enterprise?

A. Preparation phase
B. Recovery phase
C. Identification phase
D. Containment phase

Correct Answer: A

QUESTION 3
The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Access Point
B. Wireless Analyzer
C. Wireless Access Control list
D. Wireless Intrusion Prevention System

Correct Answer: D

QUESTION 4
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

Correct Answer: D

QUESTION 5
Jimmy is standing outside a secure entrance to a facility. He is pretending to having a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it beginsto close. What just happened?

A. Masquading
B. Phishing
C. Whaling
D. Piggybacking

Correct Answer: D

QUESTION 6
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

Correct Answer: C

QUESTION 7
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

Correct Answer: C

QUESTION 8
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

Correct Answer: A

QUESTION 9
Nation-state threat actors often discover vulnerabilitiesand hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of this vulnerability. What is this style of attack called?

A. zero-hour
B. no-day
C. zero-day
D. zero-sum

Correct Answer: C

QUESTION 10
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.

Correct Answer: A

QUESTION 11
Which regulationdefines security and privacy controls for Federal information systems and organizations?

A. HIPAA
B. EU Safe Harbor
C. PCI-DSS
D. NIST-800-53

Correct Answer: D

QUESTION 12
Which of the following is component of a risk assessment?

A. Logical interface
B. DMZ
C. Administrative safeguards
D. Physical security

Correct Answer: C

QUESTION 13
You've gained physical access to a Windows 2008 R2 server which has as accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD.Which Linux tool has the ability to change any user's password or to activate disabled Windows Accounts?

A. John the Ripper
B. CHNTPW
C. Cain & Abel
D. SET

Correct Answer: A

QUESTION 14
You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Host-based IDS
B. Firewall
C. Network-Based IDS
D. Proxy

Correct Answer: C

QUESTION 15
> NMAP -sn 192.168.11.200-215

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

Correct Answer: A

QUESTION 16
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. PKI
B. biometrics
C. SOA
D. single sign on

Correct Answer: A

QUESTION 17
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.

Correct Answer: D

QUESTION 18
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

Correct Answer: A

QUESTION 19
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.

Correct Answer: C

QUESTION 20
env x= `(){ :;};echo exploit ` bash -c `cat/etc/passwd

What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host?

A. Add new user to the passwd file
B. Display passwd contents to prompt
C. Change all password in passwd
D. Remove the passwd file.

Correct Answer: B