ECCouncil

Exam 312-50v9

Certified Ethical Hacker Exam V9

Version: 7.0

[Total Questions: 125]

Question No : 1

An Intrusion Detection System(IDS) has alerted the network administrator to a possibly malicious sequence of packets went to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.

What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer
B. Intrusion Prevention System (IPS)
C. Vulnerability scanner
D. Network sniffer

Answer: B

Question No : 2

PGP, SSL, and IKE are all examples of which type of cryptography?

A. Hash Algorithm
B. Secret Key
C. Public Key
D. Digest

Answer: C

Question No : 3

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

Question No : 4

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

Question No : 5

Which of the following is not a Bluetooth attack?

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

Answer: B

Question No : 6

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

Answer: A

Question No : 7

A company's Web development team has become aware ofa certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of web application vulnerability likely exists in their software?

A. Web site defacement vulnerability
B. SQL injection vulnerability
C. Cross-site Scripting vulnerability
D. Cross-site Request Forgery vulnerability

Answer: C

Question No : 8

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

Answer: D

Question No : 9

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

Question No : 10

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

Question No : 11

Under the “Post-attach Phase and Activities,” it is the responsibility of the tester to restore the system to a pre-test state.

Which of the following activities should not be included in this phase?

I.Removing all files uploaded on the system

II.Cleaning all registry entries

III.Mapping of network state

IV.Removing all tools and maintaining backdoor for reporting

A. III
B. IV
C. III and IV
D. All should be included.

Answer: A

Question No : 12

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

Question No : 13

Which of the following statements regarding ethical hacking is incorrect?

A. Testing should be remotely performed offsite.
B. Ethical hackers should never use tools that have potential of exploiting vulnerabilities in the
organizations IT system.
C. Ethical hacking should not involve writing to or modifying the target systems.
D. An organization should use ethical hackers who do not sell hardware/software or other consulting services.

Answer: B

Question No : 14

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

Question No : 15

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

Question No : 16

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

Question No : 17

Which of the following is an extremelycommon IDS evasion technique in the web world?

A. post knocking
B. subnetting
C. unicode characters
D. spyware

Answer: C

Question No : 18

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

Question No : 19

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

Answer: C

Question No : 20

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

Question No : 21

Which of the following is a design pattern based on distinct pieces ofsoftware providing application functionality as services to other applications?

A. Lean Coding
B. Service Oriented Architecture
C. Object Oriented Architecture
D. Agile Process

Answer: B

Question No : 22

Which of the following statements is TRUE?

A. Sniffers operation on Layer 3 of the OSI model
B. Sniffers operation on Layer 2 of the OSI model
C. Sniffers operation on the Layer 1 of the OSI model
D. Sniffers operation on both Layer 2 & Layer 3 of the OSImodel

Answer: D

Question No : 23

Which of the following is a command line packet analyzer similar to GUI-based Wireshark?