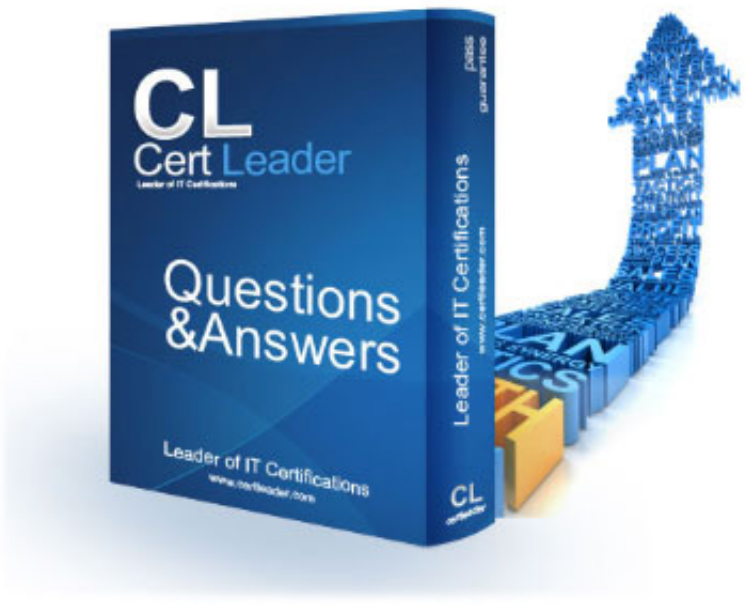
# 312-50v9 Dumps

# Certified Ethical Hacker Exam

**https://www.certleader.com/312-50v9-dumps.html**



**NEW QUESTION 1**
A common cryptographically tool is the use of XOR. XOR the following binary value: 10110001
00111010

A. 10001011
B. 10011101
C. 11011000
D. 10111100

**Answer:** A

**NEW QUESTION 2**
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 3**
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 4**
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 5**
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 6**
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.

**Answer:** B

**NEW QUESTION 7**
Which of the following describes the characteristics of a Boot Sector Virus?

A. Overwrites the original MBR and only executes the new virus code
B. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
C. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
D. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

**Answer:**

C

**NEW QUESTION 8**
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

**NEW QUESTION 9**
Jesse receives an email with an attachment labeled “Court_Notice_21206.zip”. Inside the zip file is a file named “Court_Notice_21206.docx.exe” disguised as a word document.Upon execution, a windows appears stating, “This word document is corrupt.” In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Jesse encountered?

A. Trojan
B. Worm
C. Key-Logger
D. Micro Virus

**Answer:** A

**NEW QUESTION 10**
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

**Answer:** C

**NEW QUESTION 10**
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 11**
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 14**
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 15**
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 19**
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 24**
Which of the following is component of a risk assessment?

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

**Answer:** C

**NEW QUESTION 27**
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

**Answer:** D

**NEW QUESTION 32**
Which of the following parameters describe LM Hash: I – The maximum password length is 14 characters.
II – There are no distinctions between uppercase and lowercase.
III – It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I
B. I and II
C. II
D. I, II and III

**Answer:** D

**NEW QUESTION 37**
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 38**
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attach along with some optimizations like Korek attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

A. Wificracker
B. WLAN-crack
C. Airguard
D. Aircrack-ng

**Answer:** D

**NEW QUESTION 39**
A hacker has successfully infected an internet-facing server, which he will then use to send junk mail, take part incoordinated attacks, or host junk email content.
Which sort of trojan infects this server?

A. Botnet Trojan
B. Banking Trojans
C. Ransomware Trojans
D. Turtle Trojans

**Answer:** A

**NEW QUESTION 44**
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 48**
Which of the following isthe greatest threat posed by backups?

A. An un-encrypted backup can be misplaced or stolen
B. A back is incomplete because no verification was performed.
C. A backup is the source of Malware or illicit information.
D. A backup is unavailable duringdisaster recovery.

**Answer:** A

**NEW QUESTION 50**
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

**NEW QUESTION 51**
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 54**
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 59**
During a security audit of IT processes, an IS auditor found that there was no documented security procedures. What should the IS auditor do?

A. Terminate the audit.
B. Identify and evaluate existing practices.
C. Create a procedures document
D. Conduct compliance testing

**Answer:**

B

**NEW QUESTION 60**
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 62**
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 63**
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

**Answer:** D

**NEW QUESTION 67**
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 68**
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 69**
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.
What wireshark filter will show the connections from the snort machineto kiwi syslog machine?

A. tcp.dstport==514 && ip.dst==192.168.0.150
B. tcp.dstport==514 &&ip.dst==192.168.0.99
C. tcp.srcport==514 && ip.src==192.168.0.99
D. tcp.srcport==514 && ip.src==192.168.150

**Answer:** A

**NEW QUESTION 72**
You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System.
What is the best approach?

A. Install and use Telnet to encrypt all outgoing traffic from this server.

B. Install Cryptcat and encrypt outgoing packets from this server
C. Use Alternate Data Streams to hide the outgoing packets from this server.
D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

**Answer:** A

**NEW QUESTION 73**
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 77**
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. Netstumbler
C. Abel
D. Nessus

**Answer:** A

**NEW QUESTION 80**
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 82**
As a Certified Ethical hacker, you were contracted by aprivate firm to conduct an external security assessment through penetration testing.
What document describes the specified of the testing, the associated violations, and essentially protects both the organization’s interest and your li abilities as a tester?

A. Term of Engagement
B. Non-Disclosure Agreement
C. Project Scope
D. Service Level Agreement

**Answer:** B

**NEW QUESTION 87**
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?

A. Nmap –T4 –F 10.10.0.0/24
B. Nmap –T4 –q 10.10.0.0/24
C. Nmap –T4 –O 10.10.0.0/24
D. Nmap –T4 –r 10.10.0.0/24

**Answer:** A

**NEW QUESTION 91**
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 94**

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 96**
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

A. ICMP
B. TCP
C. UDP
D. UPX

**Answer:** B

**NEW QUESTION 100**
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 105**
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. Jack the ripper
B. nessus
C. tcpdump
D. ethereal

**Answer:** C

**NEW QUESTION 107**
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

**NEW QUESTION 111**
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 115**
Which of the following is assured by the use of a hash?

A. Availability
B. Confidentiality
C. Authentication
D. Integrity

**Answer:** D

**NEW QUESTION 118**
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

**NEW QUESTION 123**
The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.
What tool can you use to view the network traffic being sent and received by the wireless router?

A. Netcat
B. Wireshark
C. Nessus
D. Netstat

**Answer:** B

**NEW QUESTION 127**
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 128**
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 133**
Which of the following is the successor of SSL?

A. RSA
B. GRE
C. TLS
D. IPSec

**Answer:** C

**NEW QUESTION 135**
You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

A. False Negative
B. True Negative
C. True Positive
D. False Positive

**Answer:** A

**NEW QUESTION 136**
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 137**
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

**NEW QUESTION 142**
A new wireless client is configured to join a 802.11 network. Thisclient uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.
What is a possible source of this problem?

A. The client cannot see the SSID of the wireless network
B. The wireless client is not configured to use DHCP
C. The WAP does not recognize the client's MAC address
D. Client isconfigured for the wrong channel

**Answer:** C

**NEW QUESTION 144**
Which of the following security operations is used for determining the attack surface of an organization?

A. Reviewing the need for a security clearance for each employee
B. Running a network scan to detect network services in the corporate DMZ
C. Training employees on the security policy regarding social engineering
D. Using configuration management to determine when and where to apply security patches

**Answer:** B

**NEW QUESTION 146**
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 147**
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 150**
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

**Answer:** A

**NEW QUESTION 155**
Which of the followingis the least-likely physical characteristic to be used in biometric control that supports a large company?

A. Iris patterns
B. Voice
C. Fingerprints
D. Height and Weight

**Answer:**

D

**NEW QUESTION 159**
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 163**
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 168**
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 173**
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to www.MyPersonalBank.com, that the user is directed to a phishing site.
Which file does the attacker needto modify?

A. Hosts
B. Networks
C. Boot.ini
D. Sudoers

**Answer:** A

**NEW QUESTION 177**
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 182**
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 184**
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 188**
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

**NEW QUESTION 193**
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 194**
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 195**
Which tool allows analysis and pen testers to examine links between data using graphs and link analysis?

A. Metasploit
B. Maltego
C. Wireshark
D. Cain &Abel

**Answer:** B

**NEW QUESTION 199**
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 204**
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 208**
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal Network.
What is this type of DNS configuration commonly called?

A. DNS Scheme
B. DynDNS
C. Split DNS
D. DNSSEC

**Answer:** C

**NEW QUESTION 209**
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

**NEW QUESTION 211**
When you are getting informationabout a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.
What nmap script will help you with this task?

A. http enum
B. http-git
C. http-headers
D. http-methods

**Answer:** B

**NEW QUESTION 212**
What is the best description of SQL Injection?

A. It is a Denial of Service Attack.
B. It is an attack used to modify code in an application.
C. It is and attack used to gain unauthorized access to a database.
D. It isa Man-in-the-Middle attack between your SQL Server and Web App Server.

**Answer:** D

**NEW QUESTION 215**
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 217**
Which method of password cracking takes the most time and effect?

A. Rainbow Tables
B. Shoulder surfing
C. Bruce force
D. Directory attack

**Answer:** C

**NEW QUESTION 222**
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 223**
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

**NEW QUESTION 228**
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 229**
.....

# Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

## 100% Pass Your 312-50v9 Exam with Our Prep Materials Via below:

https://www.certleader.com/312-50v9-dumps.html