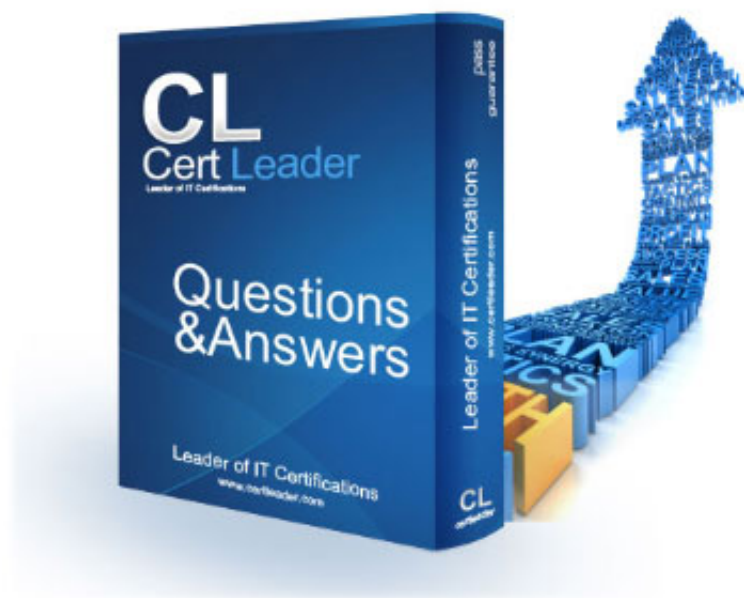


312-50v9 Dumps

Certified Ethical Hacker Exam

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



NEW QUESTION 1

What does a firewall check to prevent particular ports and applications from getting packets into an organization's?

- 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 2

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

What is the Shellshock bash vulnerability attempting to do on a 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 3

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 4

In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.

Which algorithm is this referring to?

- A. Wired Equivalent Privacy (WEP)
- B. Temporal Key Integrity Protocol (TKIP)
- C. Wi-Fi Protected Access (WPA)
- D. Wi-Fi Protected Access 2 (WPA2)

Answer: A

NEW QUESTION 5

An attacker changes the profile information of a particular user on a target website (the victim). The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

<frame src=http://www.vulnweb.com/updataif.php Style="display:none"></iframe> What is this type of attack (that can use either HTTP GET or HTTP POST) called?

- A. Cross-Site Request Forgery
- B. Cross-Site Scripting
- C. SQL Injection
- D. Browser Hacking

Answer: A

NEW QUESTION 6

Perspective clients want to 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 7

This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.

Which of the following organizations is being described?

- A. Payment Card Industry (PCI)
- B. International Security Industry Organization (ISIO)
- C. Institute of Electrical and Electronics Engineers (IEEE)

D. Center for Disease Control (CDC)

Answer: B

NEW QUESTION 8

What is the process of logging, recording, and resolving events that take place in an organization?

- A. Metrics
- B. Security Policy
- C. Internal Procedure
- D. Incident Management Process

Answer: D

NEW QUESTION 9

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 10

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 10

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 14

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 begins to close.

What just happened?

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

Answer: D

NEW QUESTION 15

You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected.

What testing method did you use?

- A. Piggybacking
- B. Tailgating
- C. Eavesdropping
- D. Social engineering

Answer: D

NEW QUESTION 19

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You 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 23

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 attack 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. Wifcracker
- B. WLAN-crack
- C. Airguard
- D. Aircrack-ng

Answer: D

NEW QUESTION 26

Which of the following is not a Bluetooth attack?

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

Answer: B

NEW QUESTION 28

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

Answer: A

NEW QUESTION 29

Which of the following is the BEST way to defend against network sniffing?

- A. Using encryption protocols to secure network communications
- B. Restrict Physical Access to Server Rooms hosting Critical Servers
- C. Use Static IP Address
- D. Register all machines MAC Address in a centralized Database

Answer: A

NEW QUESTION 30

Which of the following is the 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 during disaster recovery.

Answer: A

NEW QUESTION 35

Which of the following is a design pattern based on distinct pieces of software 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 36

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

Answer: A

NEW QUESTION 38

An incident investigator asks to receive a copy of the event from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The network devices are not all synchronized
- B. The security breach was a false positive.
- C. The attack altered or erased events from the logs.
- D. Proper chain of custody was not observed while collecting the logs.

Answer: C

NEW QUESTION 42

Which regulation defines 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 46

During a blackbox pen test you attempt to pass IRC traffic over port 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 48

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 53

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 machine to 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 56

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 57

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 59

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. Delete the email and pretend nothing happened.
- C. Forward the message to your supervisor and ask 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 64

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

NEW QUESTION 69

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 70

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 72

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 attempt to fingerprint all 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) xxxxxxxx xxxxxx xxxxxxxxxxxx. 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

NEW QUESTION 75

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.

Answer: D

NEW QUESTION 77

Which of the following is assured by the use of a hash?

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

Answer: D

NEW QUESTION 81

What is the most common method to exploit the “Bash Bug” or ShellShock” vulnerability?

- A. SSH
- B. SYN Flood
- C. Manipulate format strings in text fields
- D. Through Web servers utilizing CGI (CommonGateway Interface) to send a malformed environment variable to a vulnerable Web server

Answer: D

NEW QUESTION 83

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 image of a clean Windows installation
- C. Check MITRE.org for the latest list of CVE findings
- D. Used a scan tool like Nessus

Answer: D

NEW QUESTION 85

The security concept of “separation of duties” is most similar to the operation of which type of security device?

- A. Bastion host
- B. Honeypot
- C. Firewall
- D. Intrusion Detection System

Answer: C

NEW QUESTION 86

The “Black box testing” methodology enforces which kind of restriction?

- A. Only the external operation of a system is accessible to the tester
- B. The internal operation of a system is completely known to the tester.
- C. Only the internal operation of a system is known to the tester.
- D. The internal operation of a system is only partly accessible to the tester.

Answer: A

NEW QUESTION 90

Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

- A. Verify 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

Answer: A

NEW QUESTION 92

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 96

The “white box testing” methodology enforces what kind of restriction?

- A. The internal operation of a system is completely known to the tester.
- B. Only the internal operation of a system is known to the tester.
- C. Only the external operation of a system is accessible to the tester.
- D. The internal operation of a system is only partly accessible to the tester.

Answer: A

NEW QUESTION 98

A new wireless client is configured to join a 802.11 network. This client 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 is configured for the wrong channel

Answer: C

NEW QUESTION 99

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 use 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 101

Ricardo wants to send secret messages to a competitor 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 102

What is the benefit of performing an unannounced Penetration Testing?

- A. The tester will have an actual security posture visibility of the target network.
- B. The tester could not provide an honest analysis.
- C. Network security would be in a “best state” posture.
- D. It is best to catch critical infrastructure unpatched.

Answer: A

NEW QUESTION 103

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 104

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 105

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 106

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 need to modify?

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

Answer: A

NEW QUESTION 109

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 the SLE, 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 113

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 OSI model

Answer: D

NEW QUESTION 116

This asymmetry cipher 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 117

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

Answer: C

NEW QUESTION 121

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 126

The heartland bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2004-1060. This bug affects the OpenSSL implementation of the transport Layer security (TLS) protocols defined in RFC6520.

What types of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

- A. Root
- B. Private
- C. Shared
- D. Public

Answer: A

NEW QUESTION 129

What is a "Collision attack" in cryptography?

- A. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
- B. Collision attacks try to break the hash into three parts to get the plaintext value.
- C. Collision attacks try to find two inputs producing the same hash.
- D. Collision attacks try to get the public key

Answer: C

NEW QUESTION 131

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. Download and Install Netcat
- D. Disable Key Services

Answer: C

NEW QUESTION 134

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 137

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 138

When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.

What command will help you to search files using Google as a search engine?

- A. site:target.com file:xls username password email
- B. domain: target.com archive:xls username password email
- C. site: target.com filetype:xls username password email
- D. inurl: target.com filename:xls username password email

Answer: C

NEW QUESTION 139

Which method of password cracking takes the most time and effort?

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

Answer: C

NEW QUESTION 141

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 142

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 145

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 147

.....

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>