

➤ **Vendor:** EC-Council

➤ **Exam Code:** 312-50v11

➤ **Exam Name:** Certified Ethical Hacker Exam (CEH v11)

➤ **New Updated Questions from [Braindump2go](#) (Updated in [March/2021](#))**

[Visit Braindump2go and Download Full Version 312-50v11 Exam Dumps](#)

QUESTION 874

You are a penetration tester working to test the user awareness of the employees of the client xyz. You harvested two employees' emails from some public sources and are creating a client-side backdoor to send it to the employees via email. Which stage of the cyber kill chain are you at?

- A. Reconnaissance
- B. Command and control
- C. Weaponization
- D. Exploitation

Answer: C

Explanation:

This stage coupling exploit with backdoor into deliverable payload Next, attackers can re-engineer some core malware to suit their functions victimization subtle techniques. counting on the requirements and talents of the assaulter, the malware might exploit antecedently unknown vulnerabilities, aka "zero-day" exploits, or some combination of vulnerabilities, to quietly defeat a network's defenses. By reengineering the malware, attackers scale back the probability of detection by ancient security solutions. This method typically involves embedding specially crafted malware into Associate in Nursing otherwise benign or legitimate document, like a press release or contract document, or hosting the malware on a compromised domain.

QUESTION 875

jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes. In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain valuable information. What is the attack technique employed by Jane in the above scenario?

- A. website mirroring
- B. Session hijacking
- C. Web cache poisoning
- D. Website defacement

Answer: C

QUESTION 876

You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions. What Google dork operator would you use?

- A. filetype
- B. ext
- C. inurl
- D. site

Answer: A

[312-50v11 Exam Dumps](#) [312-50v11 Exam Questions](#) [312-50v11 PDF Dumps](#) [312-50v11 VCE Dumps](#)

<https://www.braindump2go.com/312-50v11.html>

QUESTION 877

Which of the following commands checks for valid users on an SMTP server?

- A. RCPT
- B. CHK
- C. VRFY
- D. EXPN

Answer: C

Explanation:

The VRFY commands enables SMTP clients to send an invitation to an SMTP server to verify that mail for a selected user name resides on the server. The VRFY command is defined in RFC 821. The server sends a response indicating whether the user is local or not, whether mail are going to be forwarded, and so on. A response of 250 indicates that the user name is local; a response of 251 indicates that the user name isn't local, but the server can forward the message. The server response includes the mailbox name.

QUESTION 878

Jane invites her friends Alice and John over for a LAN party. Alice and John access Jane's wireless network without a password. However, Jane has a long, complex password on her router. What attack has likely occurred?

- A. Wireless sniffing
- B. Piggybacking
- C. Evil twin
- D. Wardriving

Answer: A

QUESTION 879

If you send a TCP ACK segment to a known closed port on a firewall but it does not respond with an RST, what do you know about the firewall you are scanning?

- A. There is no firewall in place.
- B. This event does not tell you anything about the firewall.
- C. It is a stateful firewall
- D. It is a non-stateful firewall.

Answer: C

QUESTION 880

Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mail servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API. Which of the following tools is used by Wilson in the above scenario?

- A. Factiva
- B. Netcraft
- C. infoga
- D. Zoominfo

Answer: A

QUESTION 881

During the enumeration phase, Lawrence performs banner grabbing to obtain information such as OS details and versions of services running. The service that he enumerated runs directly on TCP port 445.

Which of the following services is enumerated by Lawrence in this scenario?

[312-50v11 Exam Dumps](#) [312-50v11 Exam Questions](#) [312-50v11 PDF Dumps](#) [312-50v11 VCE Dumps](#)

<https://www.braindump2go.com/312-50v11.html>

- A. Server Message Block (SMB)
- B. Network File System (NFS)
- C. Remote procedure call (RPC)
- D. Telnet

Answer: A

QUESTION 882

Samuel a security administrator, is assessing the configuration of a web server. He noticed that the server permits SSLv2 connections, and the same private key certificate is used on a different server that allows SSLv2 connections. This vulnerability makes the web server vulnerable to attacks as the SSLv2 server can leak key information. Which of the following attacks can be performed by exploiting the above vulnerability?

- A. DROWN attack
- B. Padding oracle attack
- C. Side-channel attack
- D. DUHK attack

Answer: A

QUESTION 883

Robin, an attacker, is attempting to bypass the firewalls of an organization through the DNS tunneling method in order to exfiltrate data. He is using the NSTX tool for bypassing the firewalls. On which of the following ports should Robin run the NSTX tool?

- A. Port 53
- B. Port 23
- C. Port 50
- D. Port 80

Answer: A

QUESTION 884

In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

- A. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
- B. Extraction of cryptographic secrets through coercion or torture.
- C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
- D. A backdoor placed into a cryptographic algorithm by its creator.

Answer: B

QUESTION 885

in this attack, an adversary tricks a victim into reinstalling an already-in-use key. This is achieved by manipulating and replaying cryptographic handshake messages. When the victim reinstall the key, associated parameters such as the incremental transmit packet number and receive packet number are reset to their initial values. What is this attack called?

- A. Chop chop attack
- B. KRACK
- C. Evil twin
- D. Wardriving

Answer: B

QUESTION 886

Jim, a professional hacker, targeted an organization that is operating critical Industrial Infrastructure. Jim used Nmap to scan open ports and running services on systems connected to the organization's OT network. He used an Nmap command to identify Ethernet/IP devices connected to the Internet and further gathered information such as the vendor name, product code and name, device name, and IP address. Which of the following Nmap commands helped Jim retrieve the required information?

- A. `nmap -Pn -sU -p 44818 -script emp-info < Target IP >`
- B. `nmap -Pn -sT -p 46824A < Target ip >`
- C. `nmap -Pn -sT -scan-delay is -max-parallelism 1 -p < Port List >< Target IP >`
- D. `nmap -Pn -sT -p 102 -script s7-info < Target IP >`

Answer: D

QUESTION 887

Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

- A. Time Keeper
- B. NTP
- C. PPP
- D. OSPP

Answer: B

QUESTION 888

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bob denies that he had ever sent a mail. What do you want to "know" to prove yourself that it was Bob who had sent a mail?

- A. Authentication
- B. Confidentiality
- C. Integrity
- D. Non-Repudiation

Answer: D

QUESTION 889

John, a disgruntled ex-employee of an organization, contacted a professional hacker to exploit the organization. In the attack process, the professional hacker installed a scanner on a machine belonging to one of the victims and scanned several machines on the same network to identify vulnerabilities to perform further exploitation. What is the type of vulnerability assessment tool employed by John in the above scenario?

- A. Proxy scanner
- B. Agent-based scanner
- C. Network-based scanner
- D. Cluster scanner

Answer: B

QUESTION 890

You are a penetration tester and are about to perform a scan on a specific server. The agreement that you signed with the client contains the following specific condition for the scan: "The attacker must scan every port on the server several

[312-50v11 Exam Dumps](#) [312-50v11 Exam Questions](#) [312-50v11 PDF Dumps](#) [312-50v11 VCE Dumps](#)

<https://www.braindump2go.com/312-50v11.html>



- A. The -A flag
- B. The -g flag
- C. The -f flag
- D. The -D flag

flags `--source-port` and `-g` are equivalent and instruct `nmap` to send packets through a selected port. this option is used to try to cheat firewalls whitelisting traffic from specific ports. the following example can scan the target from the port twenty to ports eighty, 22, 21,23 and 25 sending fragmented packets to LinuxHint.

A. Hybrid
B. Community
C. Public
D. Private

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

A. Bluesmacking
B. Bluebugging
C. Bluejacking
D. Bluesnarfing

<https://www.braindump2go.com/312-50v11.html>

to "invisible" or "non-discoverable" you're not going to receive these messages. Also, keeping your smartphone or device set to "invisible" whereas you're in a very busy or open Wi-Fi space. this can forestall Bluejacking and also the next 2 well- liked styles of hacks.

QUESTION 894

After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 369. Which service Is this and how can you tackle the problem?

- A. The service is LDAP. and you must change it to 636. which is LDAPS.
- B. The service is NTP. and you have to change It from UDP to TCP in order to encrypt it
- C. The findings do not require immediate actions and are only suggestions.
- D. The service is SMTP, and you must change it to SMIME. which is an encrypted way to send emails.

Answer: A

QUESTION 895

What would be the fastest way to perform content enumeration on a given web server by using the Gobuster tool?

- A. Performing content enumeration using the bruteforce mode and 10 threads
- B. Shipping SSL certificate verification
- C. Performing content enumeration using a wordlist
- D. Performing content enumeration using the bruteforce mode and random file extensions

Answer: D

QUESTION 896

John, a professional hacker, targeted an organization that uses LDAP for accessing distributed directory services. He used an automated tool to anonymously query the IDAP service for sensitive information such as usernames. addresses, departmental details, and server names to launch further attacks on the target organization. What is the tool employed by John to gather information from the IDAP service?

- A. jxplorer
- B. Zabasearch
- C. EarthExplorer
- D. Ike-scan

Answer: A

Explanation:

JXplorer could be a cross platform LDAP browser and editor. it's a standards compliant general purpose LDAP client which will be used to search, scan and edit any commonplace LDAP directory, or any directory service with an LDAP or DSML interface. It is extremely flexible and can be extended and custom in a very number of the way. JXplorer is written in java, and also the source code and source code build system ar obtainable via svn or as a packaged build for users who wish to experiment or any develop the program.

JX is is available in 2 versions; the free open source version under an OSI Apache two style licence, or within the JXWorkBench Enterprise bundle with inbuilt reporting, administrative and security tools.

JX has been through a number of different versions since its creation in 1999; the foremost recent stable release is version 3.3.1, the August 2013 release. JXplorer could be a absolutely useful LDAP consumer with advanced security integration and support for the harder and obscure elements of the LDAP protocol. it's been tested on Windows, Solaris, linux and OSX, packages are obtainable for HPUX, AIX, BSD and it should run on any java supporting OS.

QUESTION 897

Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. which two SQL Injection types would give her the results she is looking for?

- A. Out of band and boolean-based
- B. Time-based and union-based
- C. union-based and error-based
- D. Time-based and boolean-based

Answer: A

QUESTION 898

what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?

- A. httpd.conf
- B. administration.config
- C. idq.dll
- D. php.ini

Answer: C

Explanation:

idq.dll may be a library employed by ISAPI for indexing.idq.dll may be a system process that's needed for your PC to figure properly. It shouldn't be removed.The idq.dll is an executable file on your computer's disk drive . This file contains machine language . If you begin the software Microsoft Windows on your PC, the commands contained in idq.dll are going to be executed on your PC. For this purpose, the file is loaded into the most memory (RAM) and runs there as a Microsoft Indexing Service ISAPI Extension process (also called a task).

Is idq.dll harmful?This process is taken into account safe. it's unlikely to pose any harm to your system.

Can I stop or remove idq.dll?Since idq.dll may be a system process it shouldn't be stopped. the method is required for your PC to figure properly. Also the corresponding software Microsoft Windows shouldn't be uninstalled.

Is idq.dll CPU intensive?This process is taken into account to be CPU intensive. Without proper management, CPU intensive processes can manipulate system resources causing speed loss. Check the Microsoft Windows settings to ascertain if you'll close up unneeded modules or services.

Why is idq.dll giving me errors?System process issues are mainly a results of conflicting applications running on your PC. Consider uninstalling any applications you're not using.

Then reboot your computer.

QUESTION 899

Richard, an attacker, aimed to hack IoT devices connected to a target network. In this process. Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence. Subsequently, he started injecting the segregated command sequence on the same frequency into the IoT network, which repeats the captured signals of the devices. What Is the type of attack performed by Richard In the above scenario?

- A. Side-channel attack
- B. Replay attack
- C. CrypTanalysis attack
- D. Reconnaissance attack

Answer: C

QUESTION 900

Sam is working as a system administrator In an organization. He captured the principal characteristics of a vulnerability and produced a numerical score to reflect Its severity using CVSS v3.0 to property assess and prioritize the organization's vulnerability management processes. The base score that Sam obtained after performing cvss rating was 4.0. What is the CVSS severity level of the vulnerability discovered by Sam in the above scenario?

- A. Medium
- B. Low
- C. Critical

[312-50v11 Exam Dumps](#) [312-50v11 Exam Questions](#) [312-50v11 PDF Dumps](#) [312-50v11 VCE Dumps](#)

<https://www.braindump2go.com/312-50v11.html>

D. High

Answer: B

QUESTION 901

A friend of yours tells you that he downloaded and executed a file that was sent to him by a coworker. Since the file did nothing when executed, he asks you for help because he suspects that he may have installed a trojan on his computer. what tests would you perform to determine whether his computer is infected?

- A. Use ExifTool and check for malicious content.
- B. You do not check; rather, you immediately restore a previous snapshot of the operating system.
- C. Upload the file to VirusTotal.
- D. Use netstat and check for outgoing connections to strange IP addresses or domains.

Answer: A

QUESTION 902

Gerard, a disgruntled ex-employee of Sunglass IT Solutions, targets this organization to perform sophisticated attacks and bring down its reputation in the market. To launch the attacks process, he performed DNS footprinting to gather information about DNS servers and to identify the hosts connected in the target network. He used an automated tool that can retrieve information about DNS zone data including DNS domain names, computer names, IP addresses, DNS records, and network Whois records. He further exploited this information to launch other sophisticated attacks. What is the tool employed by Gerard in the above scenario?

- A. Knative
- B. zANTI
- C. Towelroot
- D. Bluto

Answer: A

QUESTION 903

Garry is a network administrator in an organization. He uses SNMP to manage networked devices from a remote location. To manage nodes in the network, he uses MIB, which contains formal descriptions of all network objects managed by SNMP. He accesses the contents of MIB by using a web browser either by entering the IP address and Lseries.mib or by entering the DNS library name and Lseries.mib. He is currently retrieving information from an MIB that contains object types for workstations and server services. Which of the following types of MIB is accessed by Garry in the above scenario?

- A. LNMIB2.MIB
- B. WINS.MIB
- C. DHCP.MIB
- D. MIB_II.MIB

Answer: D

QUESTION 904

Nicolas just found a vulnerability on a public-facing system that is considered a zero-day vulnerability. He sent an email to the owner of the public system describing the problem and how the owner can protect themselves from that vulnerability. He also sent an email to Microsoft informing them of the problem that their systems are exposed to. What type of hacker is Nicolas?

- A. Red hat
- B. white hat
- C. Black hat
- D. Gray hat

Answer: B

QUESTION 905

Which of the following are well known password-cracking programs?

- A. L0phtcrack
- B. NetCat
- C. Jack the Ripper
- D. Netbus
- E. John the Ripper

Answer: AE