

➤ **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 853**

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 -q 10.10.0.0/24
- B. nmap -T4 -F 10.10.0.0/24
- C. nmap -T4 -r 10.10.1.0/24
- D. nmap -T4 -O 10.10.0.0/24

**Answer:** B

**QUESTION 854**

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network to identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

- A. internal assessment
- B. Passive assessment
- C. External assessment
- D. Credentialed assessment

**Answer:** D

**QUESTION 855**

This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-256, MMAC-SHA384, and ECDSA using a 384-bit elliptic curve. Which is this wireless security protocol?

- A. WPA2 Personal
- B. WPA3-Personal
- C. WPA2-Enterprise
- D. WPA3-Enterprise

**Answer:** D

**Explanation:**

Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data: Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256) Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384) Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve

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

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

Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve? Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) The 192-bit security mode offered by WPA3- Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.

**QUESTION 856**

What firewall evasion scanning technique make use of a zombie system that has low network activity as well as its fragment identification numbers?

- A. Decoy scanning
- B. Packet fragmentation scanning
- C. Spoof source address scanning
- D. Idle scanning

**Answer:** D

**QUESTION 857**

SQL injection (SOU) attacks attempt to inject SQL syntax into web requests, which may Bypass authentication and allow attackers to access and/or modify data attached to a web application.

Which of the following SQLI types leverages a database server's ability to make DNS requests to pass data to an attacker?

- A. Union-based SQLI
- B. Out-of-band SQLI
- C. In-band SQLI
- D. Time-based blind SQLI

**Answer:** A

**QUESTION 858**

in the Common Vulnerability Scoring System (CVSS) v3.1 severity ratings, what range does medium vulnerability fall in?

- A. 3.0-6.9
- B. 4.0-6.0
- C. 4.0-6.9
- D. 3.9-6.9

**Answer:** C

**QUESTION 859**

You are a penetration tester tasked with testing the wireless network of your client Brakeme SA. You are attempting to break into the wireless network with the SSID "Brakeme-Internal." You realize that this network uses WPA3 encryption, which of the following vulnerabilities is the promising to exploit?

- A. Dragonblood
- B. Cross-site request forgery
- C. Key reinstallation attack
- D. AP Myconfiguration

**Answer:** A

**QUESTION 860**

Attacker Steve targeted an organization's network with the aim of redirecting the company's web traffic to another malicious website. To achieve this goal, Steve performed DNS cache poisoning by exploiting the vulnerabilities in the DNS server software and modified the original IP address of the target website to that of a fake website. What is the technique employed by Steve to gather information for identity theft?

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

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

- A. Pretexting
- B. Pharming
- C. Wardriving
- D. Skimming

**Answer: B**

**Explanation:**

A pharming attacker tries to send a web site's traffic to a faux website controlled by the offender, typically for the aim of collection sensitive data from victims or putting in malware on their machines. Attacker tend to specialize in making look-alike ecommerce and digital banking websites to reap credentials and payment card data. Though they share similar goals, pharming uses a special technique from phishing. "Pharming attacker are targeted on manipulating a system, instead of tricking people into reaching to a dangerous web site," explains David Emm, principal security man of science at Kaspersky. "When either a phishing or pharming attacker is completed by a criminal, they need a similar driving issue to induce victims onto a corrupt location, however the mechanisms during which this is often undertaken are completely different."

**QUESTION 861**

what is the correct way of using MSFvenom to generate a reverse TCP shellcode for windows?

- A. msfvenom -p windows/meterpreter/reverse\_tcp RHOST= 10.10.10.30 LPORT=4444 - f.exe > shell.exe
- B. msfvenom -p windows/meterpreter/feversetcp LHOST=10.10.10.30 LP0RT=4444-f c
- C. msfvenom -p windows/rmeterpreter/reverse\_tcpRMOST=i0.i 0.10.30 LPORT =4444-fc
- D. msfvenom -p windows/meterpreter/reverse.tcp lhost=io.i 0.1030 lport=4444 -f exe > shell.exe

**Answer: A**

**QUESTION 862**

Harry, a professional hacker, targets the IT infrastructure of an organization. After preparing for the attack, he attempts to enter the target network using techniques such as sending spear-phishing emails and exploiting vulnerabilities on publicly available servers. Using these techniques, he successfully deployed malware on the target system to establish an outbound connection. What is the APT lifecycle phase that Harry is currently executing?

- A. Preparation
- B. Cleanup
- C. Persistence
- D. initial intrusion

**Answer: D**

**QUESTION 863**

Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?

- A. Quid pro quo
- B. Diversion theft
- C. Elicitation
- D. Phishing

**Answer: B**

**QUESTION 864**

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

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

Ricardo has discovered the username for an application in his targets environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application, what type of attack is Ricardo performing?

- A. Known plaintext
- B. Password spraying
- C. Brute force
- D. Dictionary

**Answer: C**

#### **QUESTION 865**

Richard, an attacker, targets an MNC. in this process, he uses a footprinting technique to gather as much information as possible. Using this technique, he gathers domain information such as the target domain name, contact details of its owner, expiry date, and creation date. With this information, he creates a map of the organization's network and misleads domain owners with social engineering to obtain internal details of its network. What type of footprinting technique is employed by Richard?

- A. VoIP footprinting
- B. VPN footprinting
- C. Whois footprinting
- D. Email footprinting

**Answer: D**

#### **Explanation:**

Email header reveals information about the mail server, original sender's email id, internal IP addressing scheme, also because the possible architecture of the target network. Tracking Email Communications?Email tracking is employed to watch the delivery of emails to an intended recipient.?Attackers track emails to collect information a few target recipient so as to perform social engineering and other attacks.?Get recipient's system IP address?Geolocation of the recipient?When the e-mail was received and skim?Whether or not the recipient visited any links sent to them?Get recipient's browser and OS information?Time spent on reading the emails

#### **QUESTION 866**

Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?

- A. WebSite Watcher
- B. web-Stat
- C. Webroot
- D. WAFW00F

**Answer: B**

#### **Explanation:**

Increase your web site's performance and grow! Add Web-Stat to your site (it's free!) and watch individuals act together with your pages in real time. Learn how individuals realize your web site. Get details concerning every visitor's path through your web site and track pages that flip browsers into consumers. One-click install. observe locations, in operation systems, browsers and screen sizes and obtain alerts for new guests and conversions

#### **QUESTION 867**

Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.

What is the technique used by Kevin to evade the IDS system?

- A. Desynchronization
- B. Obfuscating

- C. Session splicing
- D. Urgency flag

**Answer: B**

**Explanation:**

Adversaries could decide to build an application or file difficult to find or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is often common behavior which will be used across totally different platforms and therefore the network to evade defenses.

Payloads may be compressed, archived, or encrypted so as to avoid detection. These payloads may be used throughout Initial Access or later to mitigate detection. Typically a user's action could also be needed to open and Deobfuscate/Decode Files or info for User Execution. The user can also be needed to input a parole to open a parole protected compressed/encrypted file that was provided by the malware. Adversaries can also use compressed or archived scripts, like JavaScript.

Portions of files can even be encoded to cover the plain-text strings that will otherwise facilitate defenders with discovery. Payloads can also be split into separate, ostensibly benign files that solely reveal malicious practicality once reassembled. Adversaries can also modify commands derived from payloads or directly via a Command and Scripting Interpreter. Surroundings variables, aliases, characters, and different platform/language specific linguistics may be used to evade signature based malware detections and application management mechanisms.

**QUESTION 868**

Henry is a cyber security specialist hired by BlackEye - Cyber security solutions. He was tasked with discovering the operating system (OS) of a host. He used the UnKornScan tool to discover the OS of the target system. As a result, he obtained a TTL value, which indicates that the target system is running a Windows OS. Identify the TTL value Henry obtained, which indicates that the target OS is Windows.

- A. 64
- B. 128
- C. 255
- D. 138

**Answer: B**

**QUESTION 869**

Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?

- A. HIPAA/PHI
- B. PII
- C. PCI DSS
- D. ISO 2002

**Answer: B**

**QUESTION 870**

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Traceroute
- B. Hping
- C. TCP ping
- D. Broadcast ping

**Answer: B**

**QUESTION 871**

Steven connected his iPhone to a public computer that had been infected by Clark, an attacker. After establishing the connection with the public computer, Steven enabled iTunes WI-FI sync on the computer so that the device could continue communication with that computer even after being physically disconnected. Now, Clark gains access to Steven's iPhone through the infected computer and is able to monitor and read all of Steven's activity on the iPhone, even after the device is out of the communication zone.

Which of the following attacks is performed by Clark in above scenario?

- A. IOS trustjacking
- B. IOS Jailbreaking
- C. Exploiting SS7 vulnerability
- D. Man-in-the-disk attack

**Answer: A**

**QUESTION 872**

Alice, a professional hacker, targeted an organization's cloud services. She infiltrated the targets MSP provider by sending spear-phishing emails and distributed custom-made malware to compromise user accounts and gain remote access to the cloud service. Further, she accessed the target customer profiles with her MSP account, compressed the customer data, and stored them in the MSP. Then, she used this information to launch further attacks on the target organization. Which of the following cloud attacks did Alice perform in the above scenario?

- A. Cloud hopper attack
- B. Cloud cryptojacking
- C. Cloudborne attack
- D. Man-in-the-cloud (MITC) attack

**Answer: A**

**Explanation:**

Operation Cloud Hopper was an in depth attack and theft of data in 2017 directed at MSP within the uk (U.K.), us (U.S.), Japan, Canada, Brazil, France, Switzerland, Norway, Finland, Sweden, South Africa , India, Thailand, South Korea and Australia. The group used MSP as intermediaries to accumulate assets and trade secrets from MSP client engineering, MSP industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies. Operation Cloud Hopper used over 70 variants of backdoors, malware and trojans. These were delivered through spear-phishing emails. The attacks scheduled tasks or leveraged services/utilities to continue Microsoft Windows systems albeit the pc system was rebooted. It installed malware and hacking tools to access systems and steal data.

**QUESTION 873**

While testing a web application in development, you notice that the web server does not properly ignore the "dot dot slash" (../) character string and instead returns the file listing of a folder structure of the server.

What kind of attack is possible in this scenario?

- A. Cross-site scripting
- B. Denial of service
- C. SQL injection
- D. Directory traversal

**Answer: D**