

➤ **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 832

in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?

- A. IDEA
- B. Triple Data Encryption standard
- C. MDS encryption algorithm
- D. AES

Answer: B

QUESTION 833

To create a botnet, the attacker can use several techniques to scan vulnerable machines. The attacker first collects Information about a large number of vulnerable machines to create a list. Subsequently, they infect the machines. The list is divided by assigning half of the list to the newly compromised machines. The scanning process runs simultaneously. This technique ensures the spreading and installation of malicious code in little time. Which technique is discussed here?

- A. Hit-list-scanning technique
- B. Topological scanning technique
- C. Subnet scanning technique
- D. Permutation scanning technique

Answer: A

QUESTION 834

Which file is a rich target to discover the structure of a website during web-server footprinting?

- A. Document root
- B. Robots.txt
- C. domain.oct
- D. index.html

Answer: A

Explanation:

The document root is a directory (a folder) that is stored on your host's servers and that is designated for holding web pages. When someone else looks at your web site, this is the location they will be accessing. In order for a website to be accessible to visitors, it must be published to the correct directory, the "document root."

You might think that there would only be one directory in your space on your host's servers, but often hosts provide services beyond just publishing a website. In this case, they are likely to set up every account with several directories, since each service would require its own.

QUESTION 835

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

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

John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?

- A. Advanced persistent
- B. threat Diversion theft
- C. Spear-phishing sites
- D. insider threat

Answer: A

QUESTION 836

Clark, a professional hacker, was hired by an organization to gather sensitive information about its competitors surreptitiously. Clark gathers the server IP address of the target organization using Whois footprinting. Further, he entered the server IP address as an input to an online tool to retrieve information such as the network range of the target organization and to identify the network topology and operating system used in the network. What is the online tool employed by Clark in the above scenario?

- A. AOL
- B. ARIN
- C. DuckDuckGo
- D. Baidu

Answer: C

QUESTION 837

Louis, a professional hacker, had used specialized tools or search engines to encrypt all his browsing activity and navigate anonymously to obtain sensitive/hidden information about official government or federal databases. After gathering the information, he successfully performed an attack on the target government organization without being traced. Which of the following techniques is described in the above scenario?

- A. Dark web footprinting
- B. VoIP footprinting
- C. VPN footprinting
- D. website footprinting

Answer: A

QUESTION 838

Daniel is a professional hacker who is attempting to perform an SQL injection attack on a target website. www.moviescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as ``or '1'='1" in any SQL injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.

- A. Null byte
- B. IP fragmentation
- C. Char encoding
- D. Variation

Answer: A

QUESTION 839

Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection. Identify the behavior of the adversary in the above scenario.

- A. use of command-line interface
- B. Data staging
- C. Unspecified proxy activities
- D. Use of DNS tunneling

Answer: A

QUESTION 840

To invisibly maintain access to a machine, an attacker utilizes a toolkit that sits undetected in the core components of the operating system. What is this type of rootkit an example of?

- A. Hypervisor rootkit
- B. Kernel toolkit
- C. Hardware rootkit
- D. Firmware rootkit

Answer: B

Explanation:

Kernel-mode rootkits run with the best operating system privileges (Ring 0) by adding code or replacement parts of the core operating system, as well as each the kernel and associated device drivers. Most operative systems support kernel-mode device drivers, that execute with a similar privileges because the software itself. As such, several kernel-mode rootkits square measure developed as device drivers or loadable modules, like loadable kernel modules in Linux or device drivers in Microsoft Windows. This category of rootkit has unrestricted security access, however is tougher to jot down. The quality makes bugs common, and any bugs in code operative at the kernel level could seriously impact system stability, resulting in discovery of the rootkit. one amongst the primary wide familiar kernel rootkits was developed for Windows NT four.0 and discharged in Phrack magazine in 1999 by Greg Hoglund. Kernel rootkits is particularly tough to observe and take away as a result of they operate at a similar security level because the software itself, and square measure therefore able to intercept or subvert the foremost sure software operations. Any package, like antivirus package, running on the compromised system is equally vulnerable. during this scenario, no a part of the system is sure.

QUESTION 841

which of the following information security controls creates an appealing isolated environment for hackers to prevent them from compromising critical targets while simultaneously gathering information about the hacker?

- A. intrusion detection system
- B. Honeypot
- C. Botnet
- D Firewall

Answer: B

QUESTION 842

Bob, an attacker, has managed to access a target IoT device. He employed an online tool to gather information related to the model of the IoT device and the certifications granted to it. Which of the following tools did Bob employ to gather the above Information?

- A. search.com
- B. EarthExplorer
- C. Google image search
- D. FCC ID search

Answer: D

QUESTION 843

Samuel, a professional hacker, monitored and Intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host

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

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

machine responded with <| packet having an Incremented ISN. Consequently, Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob. What is the type of attack performed by Samuel in the above scenario?

- A. UDP hijacking
- B. Blind hijacking
- C. TCP/IP hacking
- D. Forbidden attack

Answer: C

Explanation:

A TCP/IP hijack is an attack that spoofs a server into thinking it's talking with a sound client, once actually it's communication with an assaulter that has condemned (or hijacked) the tcp session. Assume that the client has administrator-level privileges, which the attacker needs to steal that authority so as to form a brand new account with root-level access of the server to be used afterward. A tcp Hijacking is sort of a two-phased man-in-the-middle attack. The man-in-the-middle assaulter lurks within the circuit between a shopper and a server so as to work out what port and sequence numbers are being employed for the conversation.

First, the attacker knocks out the client with an attack, like Ping of Death, or ties it up with some reasonably ICMP storm. This renders the client unable to transmit any packets to the server. Then, with the client crashed, the attacker assumes the client's identity so as to talk with the server. By this suggests, the attacker gains administrator-level access to the server.

One of the most effective means of preventing a hijack attack is to want a secret, that's a shared secret between the shopper and also the server. looking on the strength of security desired, the key may be used for random exchanges. this is often once a client and server periodically challenge each other, or it will occur with each exchange, like Kerberos.

QUESTION 844

Boney, a professional hacker, targets an organization for financial benefits. He performs an attack by sending his session ID using an MITM attack technique. Boney first obtains a valid session ID by logging into a service and later feeds the same session ID to the target employee. The session ID links the target employee to Boney's account page without disclosing any information to the victim. When the target employee clicks on the link, all the sensitive payment details entered in a form are linked to Boney's account. What is the attack performed by Boney in the above scenario?

- A. Session donation attack
- B. Session fixation attack
- C. Forbidden attack
- D. CRIME attack

Answer: A

QUESTION 845

During an Xmas scan what indicates a port is closed?

- A. No return response
- B. RST
- C. ACK
- D. SYN

Answer: B

QUESTION 846

Steve, an attacker, created a fake profile on a social media website and sent a request to Stella. Stella was enthralled by Steve's profile picture and the description given for his profile, and she initiated a conversation with him soon after accepting the request. After a few days, Steve started asking about her company details and eventually gathered all the essential information regarding her company. What is the social engineering technique Steve employed in the above scenario?

- A. Diversion theft
- B. Baiting
- C. Honey trap
- D. Piggybacking

Answer: D

QUESTION 847

The network users are complaining because their system are slowing down. Further, every time they attempt to go a website, they receive a series of pop-ups with advertisements. What types of malware have the system been infected with?

- A. Virus
- B. Spyware
- C. Trojan
- D. Adware

Answer: D

Explanation:

Adware, or advertising supported computer code, is computer code that displays unwanted advertisements on your pc. Adware programs can tend to serve you pop-up ads, will modification your browser's homepage, add spyware and simply bombard your device with advertisements. Adware may be a additional summary name for doubtless unwanted programs. It's roughly a virulent disease and it's going to not be as clearly malicious as a great deal of different problematic code floating around on the net. create no mistake concerning it, though, that adware has to return off of no matter machine it's on. Not solely will adware be extremely annoying whenever you utilize your machine, it might additionally cause semipermanent problems for your device.

Adware a network users the browser to gather your internet browsing history so as to 'target' advertisements that appear tailored to your interests. At their most innocuous, adware infections square measure simply annoying. as an example, adware barrages you with pop-up ads that may create your net expertise markedly slower and additional labor intensive.

QUESTION 848

Attacker Lauren has gained the credentials of an organization's internal server system, and she was often logging in during irregular times to monitor the network activities. The organization was skeptical about the login times and appointed security professional Robert to determine the issue. Robert analyzed the compromised device to find incident details such as the type of attack, its severity, target, impact, method of propagation, and vulnerabilities exploited. What is the incident handling and response (IH&R) phase, in which Robert has determined these issues?

- A. Preparation
- B. Eradication
- C. Incident recording and assignment
- D. Incident triage

Answer: C

QUESTION 849

Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information. Which of the following techniques is employed by Susan?

- A. web shells
- B. Webhoos
- C. REST API
- D. SOAP API

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 850

Sam, a professional hacker, targeted an organization with intention of compromising AWS IAM credentials. He attempted to lure one of the employees of the organization by initiating fake calls while posing as a legitimate employee. Moreover, he sent phishing emails to steal the AWS IAM credentials and further compromise the employee's account. What is the technique used by Sam to compromise the AWS IAM credentials?

- A. Social engineering
- B. insider threat
- C. Password reuse
- D. Reverse engineering

Answer: A

QUESTION 851

Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?

- A. Distributed assessment
- B. Wireless network assessment
- C. Most-based assessment
- D. Application assessment

Answer: B

Explanation:

Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system. Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner. This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment. It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses. Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

QUESTION 852

what is the port to block first in case you are suspicious that an IoT device has been compromised?

- A. 22
- B. 443
- C. 48101
- D. 80

Answer: B

Explanation:

You can perceive Port 443 as an online browsing port went to secure browser communication or HTTPS services. It will offer coding and transport over secure ports. Thus, the information you transfer across such connections are extremely proof against third-party eavesdropping and interruption.

Moreover, the identity of the server that you just connect remotely may be documented confidently.

Once the association is established, internet browsers can show signs sort of a padlock, Associate in Nursing unbroken key, etc. within the standing region of your window, informing you regarding the secured connections.

Though Port 443 is that the commonplace port for HTTPS traffic, HTTPS port 443 also can support HTTP sites. just in case the positioning uses HTTPS however is unable to load over port 443, port eighty that handles all unencrypted HTTP internet traffic can step in to load the HTTPS-enabled web site.