DUMPSBOSS.

Ethical Hacking Professional Certification Exam

CertiProf CEHPC

Version Demo

Total Demo Questions: 8

Total Premium Questions: 81

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Introduction to Ethical Hacking	22
Topic 2, Footprinting and Reconnaissance	9
Topic 3, Scanning Networks	5
Topic 4, Vulnerability Analysis	8
Topic 5, System Hacking	7
Topic 6, Malware Threats	7
Topic 7, Social Engineering	7
Topic 8, Evading IDS, Firewalls, and Honeypots	1
Topic 9, Hacking Web Servers	1
Topic 10, Hacking Web Applications	7
Topic 11, SQL Injection	3
Topic 12, Cryptography	4
Total	81

QUESTION NO: 1

Which command is used to update Kali Linux from the console?

A. sudo update upgrade

B. sudo apt-get update••

C. sudo apt-get update

ANSWER: C

Explanation:

`sudo apt-get update` is the correct command because it refreshes Kali Linux's local package-index cache using the software repositories configured in `/etc/apt/sources.list` and related source files. Running it with `sudo` grants the administrative privileges needed to write the updated repository metadata to the system's APT cache. This lets the system discover current versions of packages, including security fixes and updated Kali tools, before an upgrade operation is performed.

In normal maintenance workflows, refreshing package information is the first essential step. Afterward, an administrator can use an upgrade command, such as `sudo apt full-upgrade`, to actually install the available package changes. Kali's documentation specifically recommends updating the package lists before performing a full distribution upgrade, helping ensure that package-resolution decisions are based on current repository information. Therefore, when the question asks for the console command used to update package information on Kali Linux, `sudo apt-get update` is the appropriate answer. See the Kali Linux documentation on updating Kali and the Debian apt-get manual page.

QUESTION NO: 2

Which of the following is a network security protocol designed to authenticate and authorize remote users to securely access network resources?

A. SSL (Secure Sockets Layer).

B. FTP (File Transfer Protocol).

C. SSH (Secure Shell).

ANSWER: C

Explanation:

SSH (Secure Shell) is the correct answer because it is a cryptographic client-server protocol built to provide secure remote access to systems and network resources across untrusted networks. An SSH server verifies a connecting user's identity through methods such as passwords, public-key authentication, certificates, or multifactor authentication integrations. Following successful authentication, the server applies its configured access controls to determine what the user is permitted to do, such as opening a remote command session, running permitted commands, forwarding ports, or accessing files through SSH-based transfer services.

SSH protects the remote-access session with encryption, preventing credentials and session content from being exposed in transit. It also provides integrity protection, helping detect modification of transmitted data, and server authentication, which helps the client verify that it is connecting to the intended host. These capabilities make SSH a foundational protocol for securely administering servers, network devices, and cloud workloads. The Internet Engineering Task Force specifies the SSH transport architecture and its security properties in RFC 4253. For practical guidance on SSH authentication and server configuration, see the OpenSSH manual pages.

QUESTION NO: 3

What is an Acceptable Use Policy?

A. An acceptable use policy (AUP) is a type of security policy directed at all employees with access to one or more organizational assets.

B. A NON-Acceptable Use Policy (AUP) is a type of security policy directed at all employees with access to one or more organizational assets.

C. Are the terms and conditions in the software.

ANSWER: A

Explanation:

An acceptable use policy (AUP) is a security policy that establishes the permitted, required, and prohibited ways in which authorized users may use an organization's technology assets. Therefore, "An acceptable use policy (AUP) is a type of security policy directed at all employees with access to one or more organizational assets." correctly identifies both the nature and audience of an AUP. In practice, the policy commonly applies not only to employees but also to contractors, temporary workers, and other users who are granted access to systems, networks, devices, email, cloud services, or organizational data.

AUPs are administrative security controls: they communicate behavioral expectations and make users accountable for using assets responsibly. Typical policy content addresses appropriate internet and email use, protection of credentials and sensitive information, restrictions on unauthorized software or unsafe activity, reporting of security incidents, and the organization's authority to monitor systems. Clear acknowledgment of these requirements supports security awareness, consistent enforcement, incident response, and organizational governance. The U.S. National Institute of Standards and Technology includes acceptable-use policies among the security-policy concepts used to define and manage appropriate system use. See the NIST definition of an acceptable use policy and NIST's Introduction to Information Security for policy and security-program context.

QUESTION NO: 4

A Shodan result shows an organization's public IP address with an exposed service banner. What is the most appropriate conclusion for an authorized ethical hacker?

A. The exposed service has already been compromised.

B. The service is guaranteed to be vulnerable because it appears in Shodan.

C. The service may be internet-facing and should be validated within the approved scope.

D. The organization's internal network is directly accessible without controls.

ANSWER: C

Explanation:

The result indicates that the service appears to be exposed to the internet and should be validated within the approved scope. Shodan data is useful for reconnaissance and external asset discovery, but it can be incomplete, outdated, or associated with infrastructure that is no longer owned by the organization.

A banner alone does not prove a vulnerability or a compromise. The tester should correlate the result with the engagement scope and perform only authorized validation before reporting the exposure or assessing its security impact.

QUESTION NO: 5

What is SQL Injection?

A. The manipulation of SQL queries to access, modify, or delete data within a database without authorization.

B. A database system used by hackers.

C. SQL code execution that only administrators can perform.

ANSWER: A

Explanation:

The manipulation of SQL queries to access, modify, or delete data within a database without authorization is the correct definition of SQL injection. This web-application vulnerability occurs when an application builds a database query using untrusted input in an unsafe way. An attacker may provide specially crafted input that changes the intended meaning or logic of the SQL statement sent to the database. The resulting query can act outside the application's intended authorization controls, potentially exposing confidential records or changing data.

SQL injection is important in ethical hacking because testing for it helps identify weaknesses at the boundary between an application and its data store. Demonstrating the issue in an authorized, controlled assessment can show the impact of insecure query construction and support remediation. Effective prevention centers on parameterized queries or prepared statements, which keep data separate from SQL commands, together with appropriate input handling and least-privilege database accounts. OWASP describes SQL injection as an attack in which malicious SQL statements control a database server, and its guidance emphasizes safe query parameterization. See the OWASP SQL Injection overview and the OWASP SQL Injection Prevention Cheat Sheet.

QUESTION NO: 6

What is a public IP address?

A. An IP address that everyone uses.

B. An IP address assigned by an Internet Service Provider (ISP) that is accessible over the internet.

C. An IP address assigned by a modem to devices within a local network.

ANSWER: B

Explanation:

An IP address assigned by an Internet Service Provider (ISP) that is accessible over the internet is a public IP address. Public addresses are globally routable: internet routers can use them to deliver traffic between a network and other systems on the public internet. An ISP commonly assigns a public address to a customer's router, firewall, or internet-facing service, either dynamically or statically. The organization can then use that address for externally reachable services, subject to its firewall, routing, and access-control configuration.

Public IP addressing is distinct from the private IPv4 address ranges reserved for internal networks. Devices using private addresses typically reach the internet through network address translation, where a router or firewall maps internal traffic to its assigned public address. For ethical-hacking and defensive assessments, identifying public IP addresses helps define the externally visible attack surface and determine which hosts and services may be reachable from outside the organization. Proper exposure management includes limiting unnecessary listening services and enforcing firewall rules. The Internet Assigned Numbers Authority describes special-purpose and private-use address spaces in its Private Address Space reference, while the underlying IPv4 addressing standard is defined in RFC 791.

QUESTION NO: 7

On which website can you check if your email account has been compromised?

A. https://facebook.com

B. https://haveibeenpwned.com

C. https://rincondelvago.com

ANSWER: B

Explanation:

https://haveibeenpwned.com is the appropriate service for checking whether an email address has appeared in publicly reported data breaches. The site, created by security researcher Troy Hunt, maintains a searchable database of breach records and lets users enter an email address to see whether it was included in known incidents. This supports a practical account-security workflow: if an address is found, the account owner should promptly change the affected password, ensure that the password is unique, enable multi-factor authentication where available, and review account activity or recovery settings for unexpected changes. The service can also notify subscribers when an email address appears in future breaches through its notification feature. A breach result indicates that data associated with the address was exposed in a reported incident; it is an important signal to take protective action, though it does not alone establish that a specific account has been accessed by an attacker. Have I Been Pwned explains its data sources and search function on its About page, and its searchable breach-check service is available at haveibeenpwned.com.

QUESTION NO: 8

What is a security breach?

A. A cybersecurity incident that results in unauthorized access to personal or corporate data.

B. The hacking of the entire internet.

C. An internet shutdown or breakup.

ANSWER: A

Explanation:

A cybersecurity incident that results in unauthorized access to personal or corporate data is a security breach. A breach occurs when an individual, application, or other entity accesses protected information or systems without authorization. The key feature is the loss of authorized control over confidential data or resources; this may include viewing, copying, disclosing, altering, or stealing information. In an organizational setting, affected data can include customer records, employee information, financial details, intellectual property, account credentials, or other sensitive business data.

Security breaches can result from technical vulnerabilities, misconfigurations, compromised credentials, social-engineering attacks, malicious software, or unauthorized activity by insiders. Their consequences may include privacy harm, operational disruption, financial loss, regulatory obligations, and reputational damage. For ethical hacking professionals, understanding this definition is important because assessments aim to identify the weaknesses that could enable unauthorized access before a real adversary exploits them. Effective security programs use preventive controls, monitoring, incident-response procedures, and remediation to reduce breach likelihood and impact. The Cybersecurity and Infrastructure Security Agency's data-breach guidance and the NIST Privacy Framework provide further authoritative context on protecting sensitive data and managing related risks.