CertiProf

CEHPC

Ethical Hacking Professional Certification Exam

Questions & Answers (Demo)

Version: 4.0

Question: 1

What is Nmap?

A. It is an open-source command-line tool used to scan IP addresses and ports on a network and to detect services, operating systems, and running applications.

B. It is a Linux-based tool that works specifically to exploit computer vulnerabilities.

C. It is a program used only for pinging computers within a network or work environment.

Answer: A

Explanation:

Nmap, also known as Network Mapper, is a widely used open-source tool in ethical hacking and penetration testing. It plays a critical role during the reconnaissance and scanning phases of ethical hacking, where the primary goal is to collect information about target systems in a legal and authorized manner. Ethical hackers rely on Nmap to understand the structure and exposure of a network before moving forward with deeper security testing.

The tool works by sending various types of packets to target hosts and analyzing the responses.

Based on these responses, Nmap can identify active hosts, open and closed ports, running services, service versions, operating systems, and even certain firewall and intrusion detection configurations. This information is essential for identifying potential weaknesses such as unnecessary open ports, misconfigured services, or outdated software.

Option A correctly defines Nmap because it accurately reflects its purpose as a scanning and discovery tool rather than an exploitation utility. Option B is incorrect because Nmap does not exploit vulnerabilities; exploitation is typically performed using specialized frameworks such as vulnerability scanners or exploitation platforms. Option C is also incorrect because although Nmap can perform host discovery similar to ping, it offers far more advanced capabilities than simple network reachability checks.

From an ethical hacking perspective, Nmap supports preventive and defensive security objectives. By revealing network visibility issues and configuration flaws, it enables organizations to harden systems, reduce attack surfaces, and comply with security best practices. When used ethically and with proper authorization, Nmap is a foundational tool for strengthening information security.

Question: 2

Who uses Metasploit?

A. Agricultural engineers.

B. Food engineers.

C. Cybersecurity experts.

Answer: C

Explanation:

Metasploit is a widely used penetration testing framework designed to develop, test, and execute exploit code against target systems. It is primarily used by cybersecurity experts, including ethical hackers, penetration testers, red team members, and security researchers. Therefore, option C is the correct answer.

In the context of ethical hacking, Metasploit is most commonly used during the exploitation and post-exploitation phases of penetration testing. After reconnaissance and vulnerability scanning identify potential weaknesses, Metasploit allows security professionals to safely verify whether those vulnerabilities can be exploited in real-world scenarios. This helps organizations understand the actual risk level of discovered flaws rather than relying solely on theoretical vulnerability reports.

Metasploit provides a vast library of exploits, payloads, auxiliary modules, and post-exploitation tools. Ethical hackers use these modules in controlled environments and with proper authorization to test system defenses, validate security controls, and demonstrate attack paths to stakeholders. It is not designed for non-technical professions such as agriculture or food engineering, making options A and B incorrect.

From an ethical standpoint, Metasploit supports defensive security objectives by enabling organizations to identify weaknesses before malicious attackers do. It is frequently used in security assessments, red team exercises, and cybersecurity training programs. When used legally and responsibly, Metasploit helps improve system hardening, incident response readiness, and overall organizational security posture.

Question: 3

Which of the following was a famous hacktivist group?

A. Anonymous

B. Fan7a5ma

C. Hackers

Answer: A

Explanation:

Anonymous is one of the most well-known and influential hacktivist groups in the history of cybersecurity, making option A the correct answer. Hacktivism refers to the use of hacking techniques to promote political, social, or ideological causes. Understanding hacktivist movements is important when studying current security trends, as these groups have significantly influenced cyber threat landscapes.

Anonymous is characterized as a decentralized collective, meaning it has no formal leadership or membership structure. Its activities have included distributed denial-of-service (DDoS) attacks, website defacements, data leaks, and online campaigns targeting governments, corporations, and organizations perceived to be unethical or oppressive. These actions have brought global attention to issues such as censorship, privacy, corruption, and human rights.

Option B, “Fan7a5ma,” is not a widely recognized or historically significant hacktivist group, and option C, “Hackers,” is a generic term that describes individuals with technical skills rather than an organized hacktivist collective. Therefore, both are incorrect.

From an ethical hacking and defensive security perspective, studying groups like Anonymous helps organizations understand non-financially motivated threats. Hacktivist attacks often aim for public exposure, reputational damage, or service disruption rather than direct monetary gain. This requires different defensive strategies, including improved incident response, public communication planning, and monitoring of geopolitical and social developments that may trigger cyber campaigns.

Understanding hacktivist behavior is essential for modern cybersecurity professionals to anticipate emerging threats and strengthen organizational resilience.

Question: 4

What tool would you use to search for hidden directories or files?

A. Dirb

B. Shodan

C. Ping

Answer: A

Explanation:

DIRB is a specialized web content scanning tool used in ethical hacking and penetration testing to discover hidden directories and files on web servers. It operates by performing a dictionary-based brute-force attack against a target website, attempting to access directories and files that are not publicly linked but may still be accessible. This makes option A the correct answer.

DIRB is typically used during the web application reconnaissance and enumeration phases of penetration testing. Ethical hackers rely on it to uncover misconfigurations such as exposed admin panels, backup files, configuration files, or outdated directories that could lead to further compromise. These hidden resources often exist due to poor security practices or improper cleanup during development.

Option B, Shodan, is incorrect because Shodan is a search engine used to discover internet-connected devices and services, not hidden directories within a specific website. Option C, Ping, is also incorrect because it is a network utility used only to test host reachability and does not interact with web servers at the application layer.

From a defensive security perspective, DIRB helps organizations identify unnecessary exposure in web environments. Discovering hidden directories allows administrators to remove, restrict, or secure them before attackers exploit them. When used ethically and with authorization, DIRB is a powerful tool for improving web application security and reducing attack surfaces.

Question: 5

Is pinging considered a crime if it is done without authorization?

A. No, it is only used to validate if a service or host is active.

B. No, ping does not work at all.

C. Yes, privacy is being violated.

Answer: A

Explanation:

Pinging is a basic network diagnostic technique used to determine whether a host is reachable over a network. In most jurisdictions, pinging alone is not considered a crime, as it simply sends an Internet Control Message Protocol (ICMP) request and waits for a response. Therefore, option A is the correct answer.

In ethical hacking and cybersecurity operations, pinging is commonly used during the initial reconnaissance phase to identify live hosts within a network range. It does not access data, exploit vulnerabilities, or modify systems. Instead, it only confirms whether a system is online and responding to network traffic.

Option B is incorrect because ping is a fully functional and widely used networking utility. Option C is also incorrect because pinging does not violate privacy in itself; it does not retrieve personal data or system contents. However, it is important to note that while pinging is generally legal, organizational policies and laws vary, and repeated or aggressive scanning activity may still be considered suspicious.

From an ethical hacking standpoint, authorization is always required before performing any form of reconnaissance during a professional security assessment. Ethical hackers operate under strict legal agreements, even when using low-impact tools such as ping. Understanding the legal and ethical boundaries of reconnaissance techniques helps cybersecurity professionals avoid unintentional policy violations while conducting legitimate security testing.