Smartbridge Externship

AI for Cyber Security

Name: Raunak Jain

# Definition and Scope of Ethical Hacking:

Ethical hacking, also known as penetration testing or white-hat hacking, is a practice of intentionally probing computer systems, networks, applications, and other digital assets with the permission and for the benefit of the owner or organization. The primary purpose of ethical hacking is to identify vulnerabilities, weaknesses, and security flaws in these systems before malicious hackers can exploit them. Ethical hackers, often referred to as "white-hat hackers," use their skills and knowledge to help organizations enhance their cybersecurity posture and protect sensitive information.

Ethical hacking, also known as penetration testing or white-hat hacking, is a practice of intentionally probing computer systems, networks, applications, and other digital assets with the permission and for the benefit of the owner or organization. The primary purpose of ethical hacking is to identify vulnerabilities, weaknesses, and security flaws in these systems before malicious hackers can exploit them. Ethical hackers, often referred to as "white-hat hackers," use their skills and knowledge to help organizations enhance their cybersecurity posture and protect sensitive information.

The scope of ethical hacking encompasses several key aspects:

1. **Vulnerability Assessment**: Ethical hackers assess the security of a system or network by actively seeking vulnerabilities. This involves analyzing code, configurations, and system architecture to identify weaknesses that could be exploited by unauthorized individuals.
2. **Penetration Testing**: Ethical hackers perform controlled, authorized attacks on systems to simulate real-world cyberattacks. This helps organizations understand how well their defenses can withstand various threats.
3. **Web Application Testing**: This involves examining web applications, such as websites and web-based services, to uncover security vulnerabilities like SQL injection, cross-site scripting (XSS), and cross-site request forgery (CSRF).

4. **Network Testing**: Ethical hackers evaluate network security to identify misconfigurations, open ports, weak authentication mechanisms, and potential entry points for attackers.
5. **Wireless Network Assessment**: Assessing the security of wireless networks, including Wi-Fi networks, to detect vulnerabilities that could lead to unauthorized access.
6. **Social Engineering Testing**: Ethical hackers may employ social engineering techniques to test an organization's susceptibility to manipulation or deception by malicious actors. This includes phishing attacks and impersonation to gauge employee awareness and adherence to security policies.
7. **Physical Security Testing**: Evaluating the physical security of an organization's premises, including access controls, surveillance systems, and the protection of sensitive equipment.
8. **Security Policy and Procedure Review**: Reviewing an organization's security policies, procedures, and practices to ensure they are comprehensive, up-to-date, and effective.