1. How can ethical hacking help cybersecurity?

Ethical Hacking steps are crucial for software development, operations, and cybersecurity professionals as it helps them improve the organization's security posture. Ethical hackers undertake several phases of hacking by identifying and fixing attack vectors to help software teams evade the impacts of a successful black hat hacking attack. Some benefits of implementing an ethical hacking process include:

Ethical Hacking helps in Vulnerability Detection

Ethical hacks pinpoint system weaknesses and threat vectors that malicious actors may exploit in production. White hat attacks include hacking tools such as fuzzing to destabilize and crash applications, helping them gain deeper insights into security vulnerabilities.

Helps teams to implement secure networks

Ethical hacks involve probing the network infrastructure and access policies to detect security gaps. Reports documenting the findings of ethical hacks help organizations protect network ports, implement effective policies, and configure secure firewalls, thereby helping to enforce a robust security posture.

Helps teams keep data secure

By mimicking attackers' techniques to access system and user data, ethical hacks help teams assess the effectiveness of their data security policies. This allows security professionals to change their security constructs to address data security threats from within and outside the network.

Prevention of Cyber Attacks

Ethical hackers inform organizations of looming threat vectors and evolving attack techniques, enabling cyber security teams to configure safer infrastructure. With this approach, organizations can avoid the consequences of successful attacks such as loss of reputation, reduced customer trust, and hefty fines due to lack of compliance.

2. What are the most common types of ethical hacking?

Different types of systems are exposed to threat vectors, and each requires its own ethical hacking practices. The most common types of ethical hacking techniques include:

Social engineering

With social engineering, ethical hackers exploit human psychology rather than technical security gaps to access data and applications. They trick legitimate users into submitting their passwords or installing malicious software that grants them access to network machines and services. It is common knowledge that human users are the weakest link for cyber security, so ethical hackers conduct social engineering simulations to assess an organization-wide understanding of security controls.

Web application hacking

Web application attacks are commonly exploited because the web app acts as the interface between the clients and the webserver. The attackers intercept data transmitted in HTML pages over the HTTP protocol to perform injection and parameter tampering attacks. Ethical hackers test web applications for vulnerabilities that enable attackers to manipulate the application, such as:

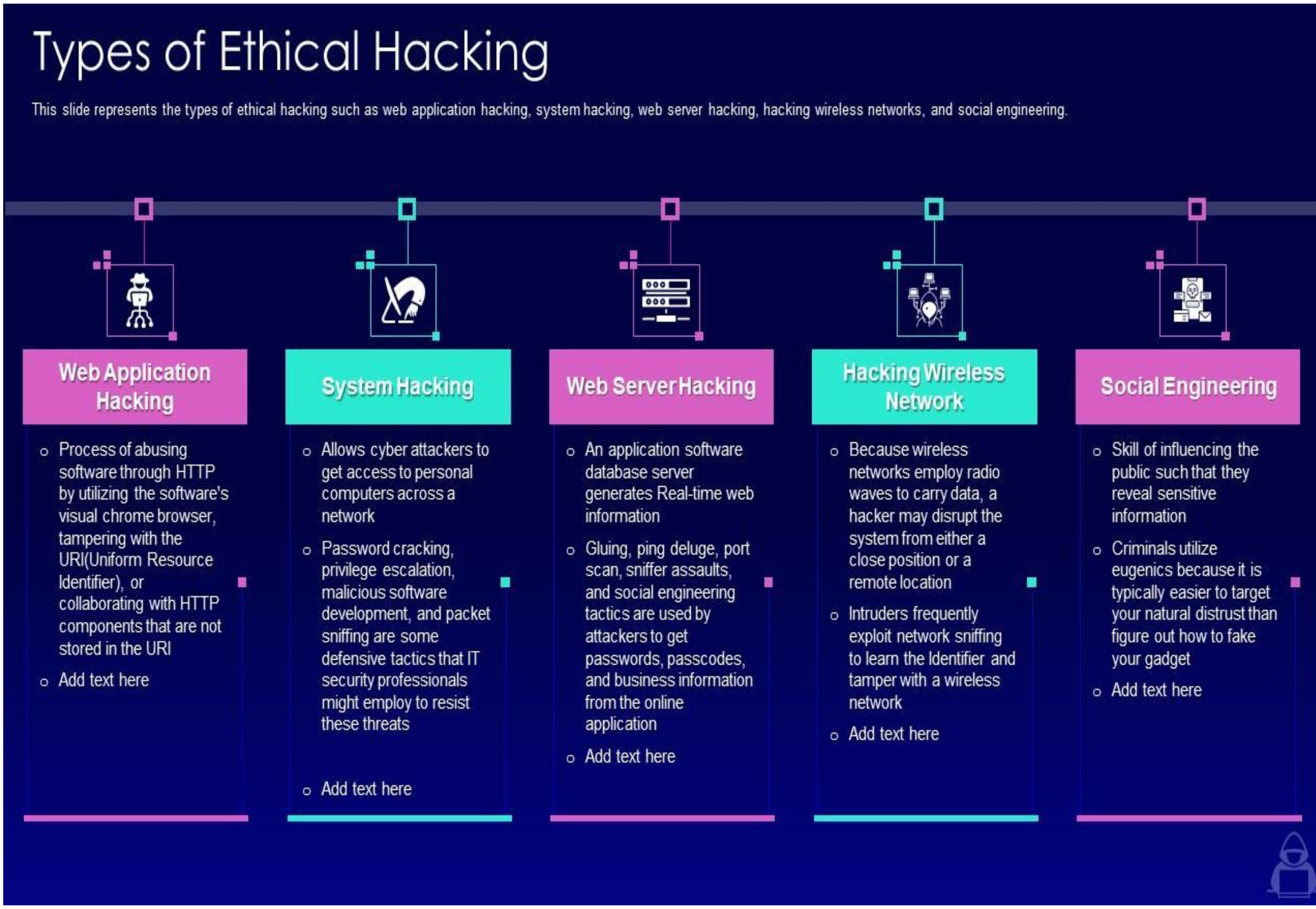
- Cross-Site Scripting
- Cross-Site Request Forgery
- Insecure configuration
- Injection attacks

Hacking wireless networks

Wireless networks have been adopted favorably since they offer quick access speeds, require little space, and enable boundless connectivity. Attackers leverage many tools and techniques to exploit these networks' vulnerabilities and gain unauthorized access. Ethical hackers, on the other hand, utilize such tools to find and patch any vulnerabilities present in the networks.

System hacking

In system hacking, attackers target servers, personal computers, and other hosts connected to the network. They exploit weaknesses in the machines' operating systems to obtain sensitive information or gain unauthorized access to abuse privileges. Ethical hackers simulate system hacks to identify weaknesses in the operating systems and software installed on these machines.



Types of Ethical Hacking

This slide represents the types of ethical hacking such as web application hacking, system hacking, web server hacking, hacking wireless networks, and social engineering.

Web Application Hacking

- Process of abusing software through HTTP by utilizing the software's visual chrome browser, tampering with the URI(Uniform Resource Identifier), or collaborating with HTTP components that are not stored in the URI
- Add text here

System Hacking

- Allows cyber attackers to get access to personal computers across a network
- Password cracking, privilege escalation, malicious software development, and packet sniffing are some defensive tactics that IT security professionals might employ to resist these threats
- Add text here

Web Server Hacking

- An application software database server generates Real-time web information
- Gluing, ping deluge, port scan, sniffer assaults, and social engineering tactics are used by attackers to get passwords, passcodes, and business information from the online application
- Add text here

Hacking Wireless Network

- Because wireless networks employ radio waves to carry data, a hacker may disrupt the system from either a close position or a remote location
- Intruders frequently exploit network sniffing to learn the Identifier and tamper with a wireless network
- Add text here

Social Engineering

- Skill of influencing the public such that they reveal sensitive information
- Criminals utilize eugenics because it is typically easier to target your natural distrust than figure out how to fake your gadget
- Add text here

3. How Can I Prevent Hacking attacks?

The following best practices can be used to help safeguard applications from hacking attacks:

1. Use a strong firewall to secure networks and host machines
2. Constantly update the OS for the latest security patches and fixes
3. Use **HTTPS** for secure client-server communication
4. Implement organization-wide training on security posture and controls
5. Use genuine software that receives constant security updates
6. Use automated scanning tools to detect and fix security gaps
7. Implement Effective Intrusion Detection Systems