ETHICAL HACKING- ESSENTIALS

PRESENTATION BY ASHISH CHAUHAN

Introduction

- "Ethical hacking describes the process of attacking and penetrating computer systems and networks to discover and point out potential security weaknesses for a client which is responsible for the attacked information technology environment."

A Brief History of Hacking

- • 2001 – In one of the biggest denial-of service attack, hackers launched attacks against eBay, Yahoo!, CNN.com, Amazon and others.

- • 2007 - Bank hit by "biggest ever" hack. Swedish Bank, Nordea recorded nearly $1 Million has been stolen in three months from 250 customer account.

Ethical Hacking Fundamentals

- Ethical hacking involves authorized testing of computer systems, networks, or applications to discover vulnerabilities. Key fundamentals include understanding programming languages, networking, and security protocols. It's crucial to stay updated on cybersecurity trends and tools. Ethical hackers should have strong problem-solving skills, attention to detail, and adhere to a strict code of ethics while ensuring the security and privacy of the systems they test. Continuous learning is essential in this dynamic field. Ethical hacking involves authorized testing of computer systems, networks, or applications to discover vulnerabilities. Key fundamentals include understanding programming languages, networking, and security protocols. It's crucial to stay updated on cybersecurity trends and tools. Ethical hackers should have strong problem-solving skills, attention to detail, and adhere to a strict code of ethics while ensuring the security and privacy of the systems they test. Continuous learning is essential in this dynamic field.

Importance of Ethical Hacking

- Protecting Sensitive Information

- Identifying and Fixing Vulnerabilities

- Prev enting Cyber Attacks

Scanning and Enumeration

- The process of scanning and identifying vulnerabilities in a target system. Utilizing enumeration techniques to gather specific information about the target. Emphasizing the importance of thorough analysis

Vulnerability Analysis

▪ Identifying and assessing security weaknesses in a target system. Utilizing automated tools to discover potential vulnerabilities. Emphasizing the need for responsible disclosure of identified vulnerabilities.
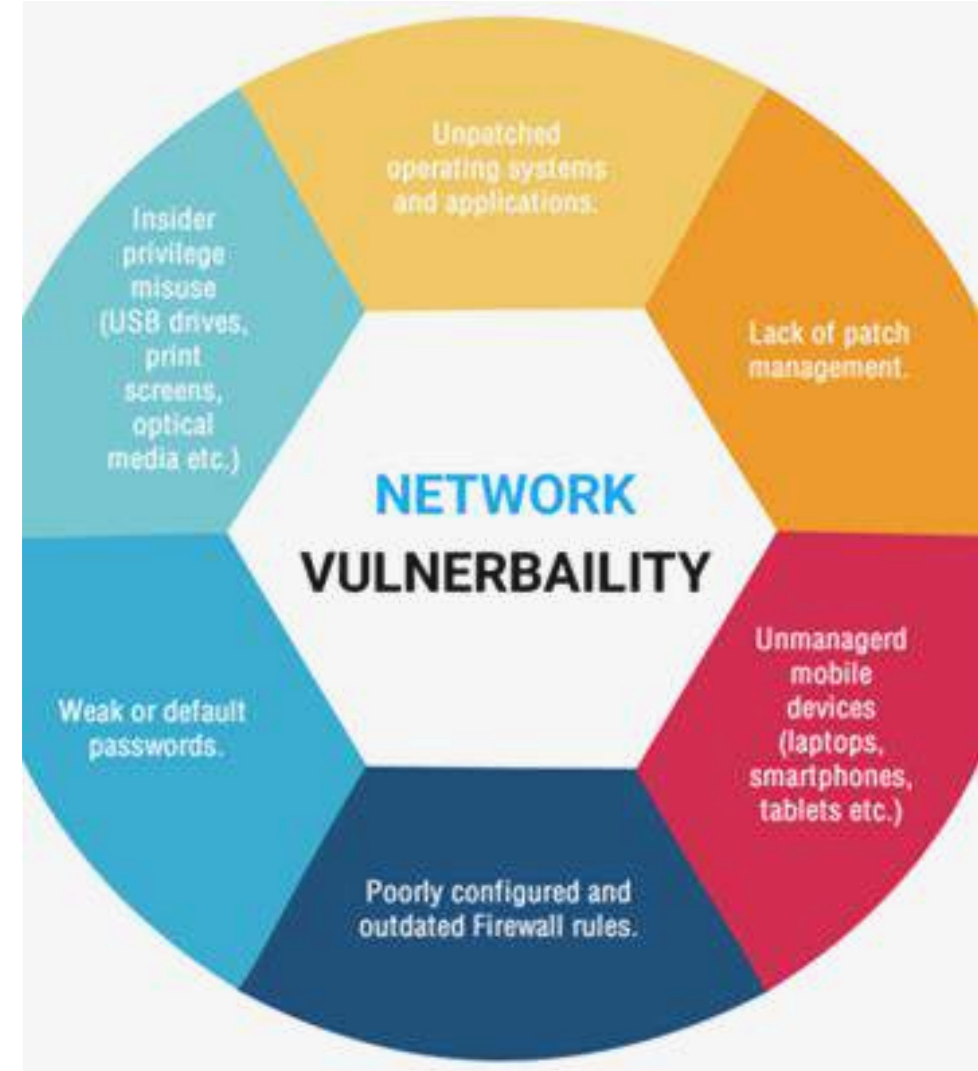
Exploitation and Post Exploitation

▪ Understanding the exploitation of identified vulnerabilities to gain access to a system. Exploring the ethical considerations of post-exploitation activities. Emphasizing the importance of ethical boundaries in exploitation.
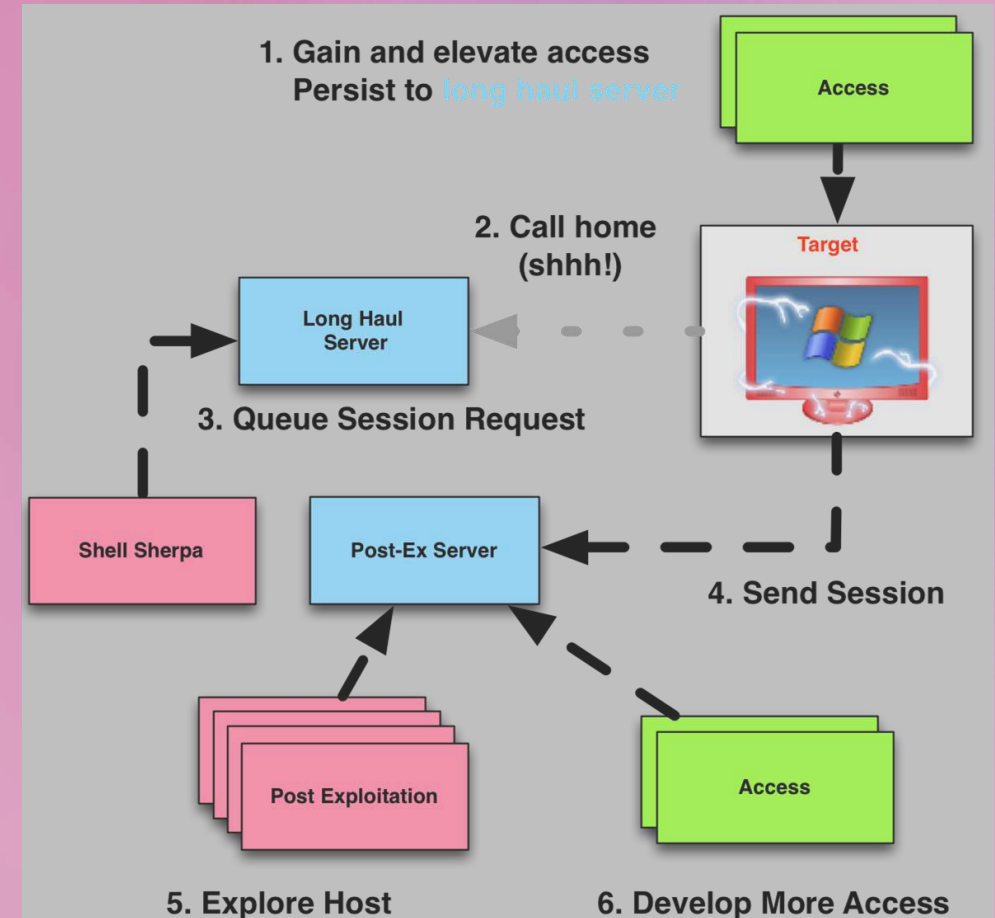
Social Engineering and Phishing

▪ Exploring the psychological tactics used in social engineering attacks. Understanding the ethical implications of phishing and its impact on cybersecurity. Emphasizing the need for awareness and education.
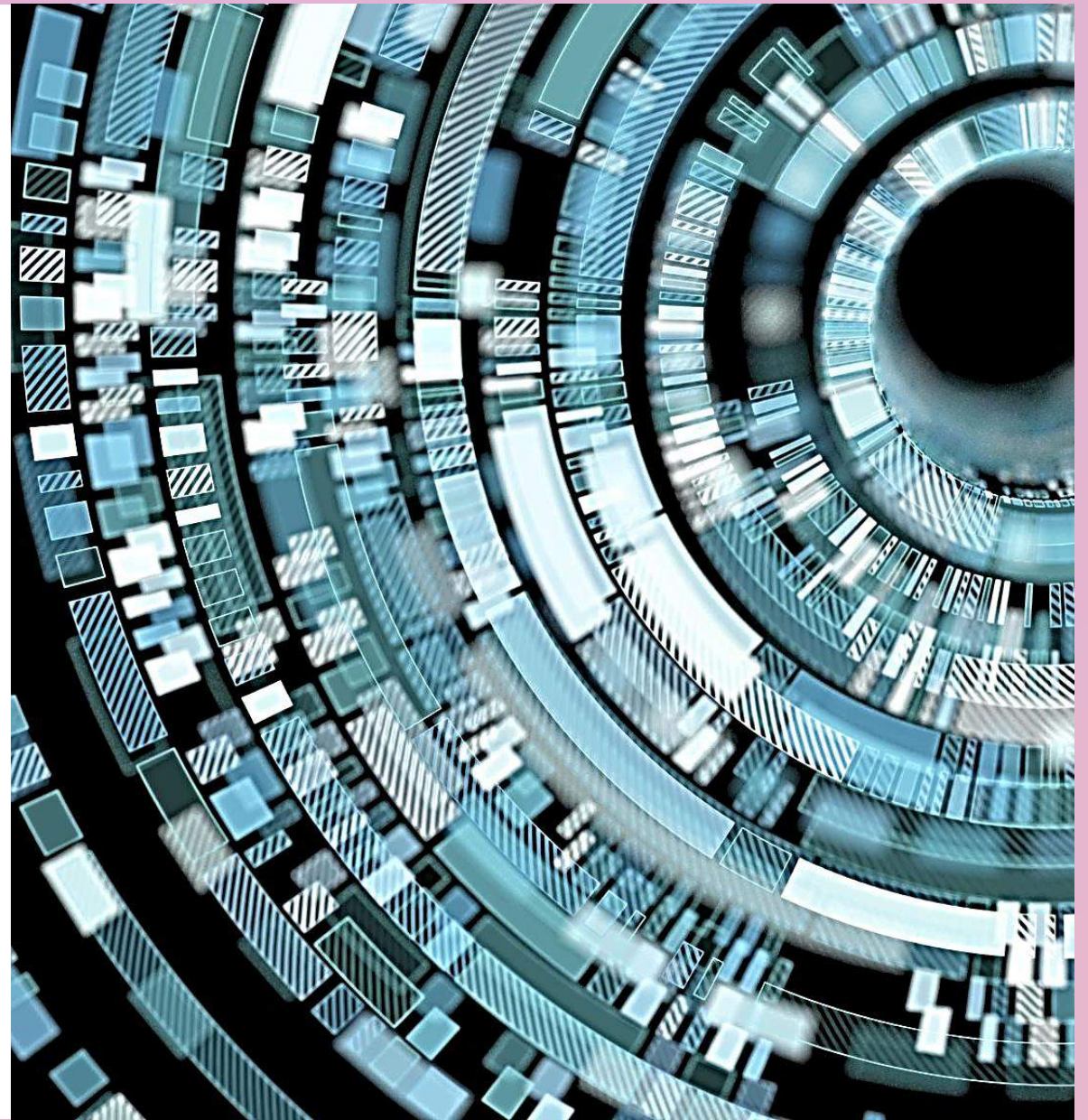
Web Application Security

- Identifying common web application vulnerabilities and their impact. Utilizing ethical hacking techniques to assess and improve web application security. Emphasizing the need for secure coding practices.
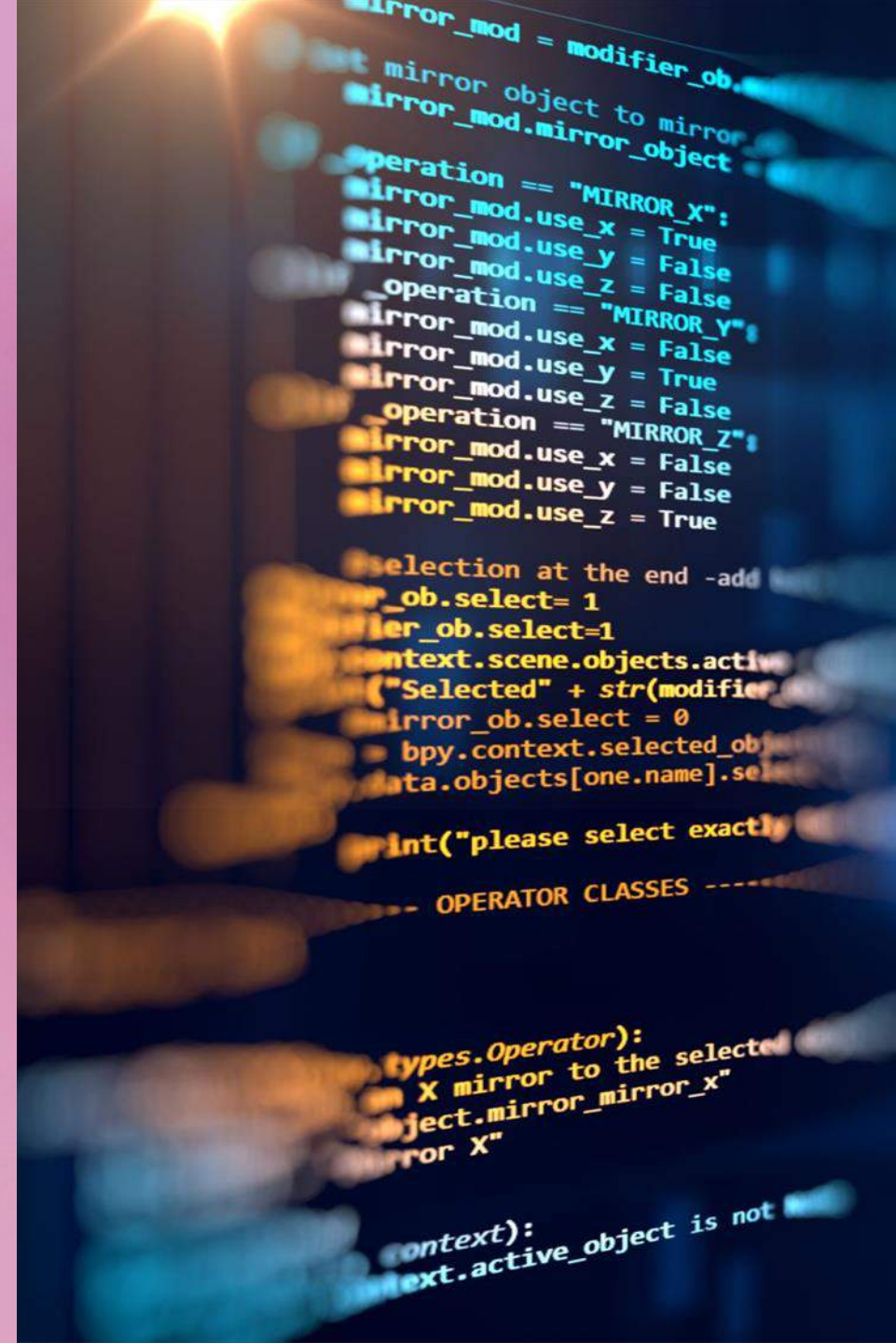
Trojan Attacks: Detection and Countermeasures

- Detection & Countermeasures ~Port Scan your own system regularly. ~If you find a irregular port open, on which you usually do not have a service running, then your system might have a Trojan installed. ~One can remove a Trojan using any normal Anti-Virus Software.
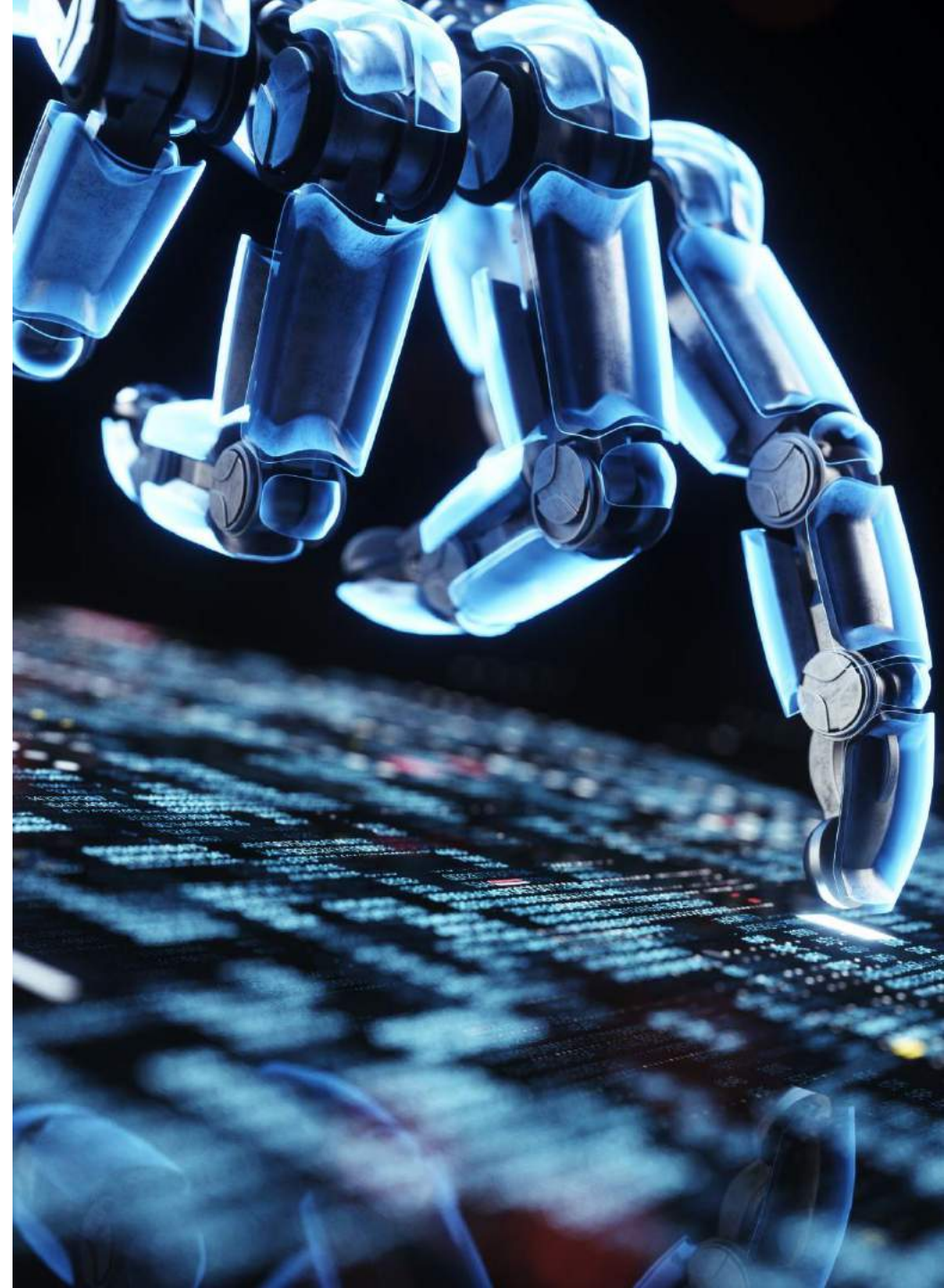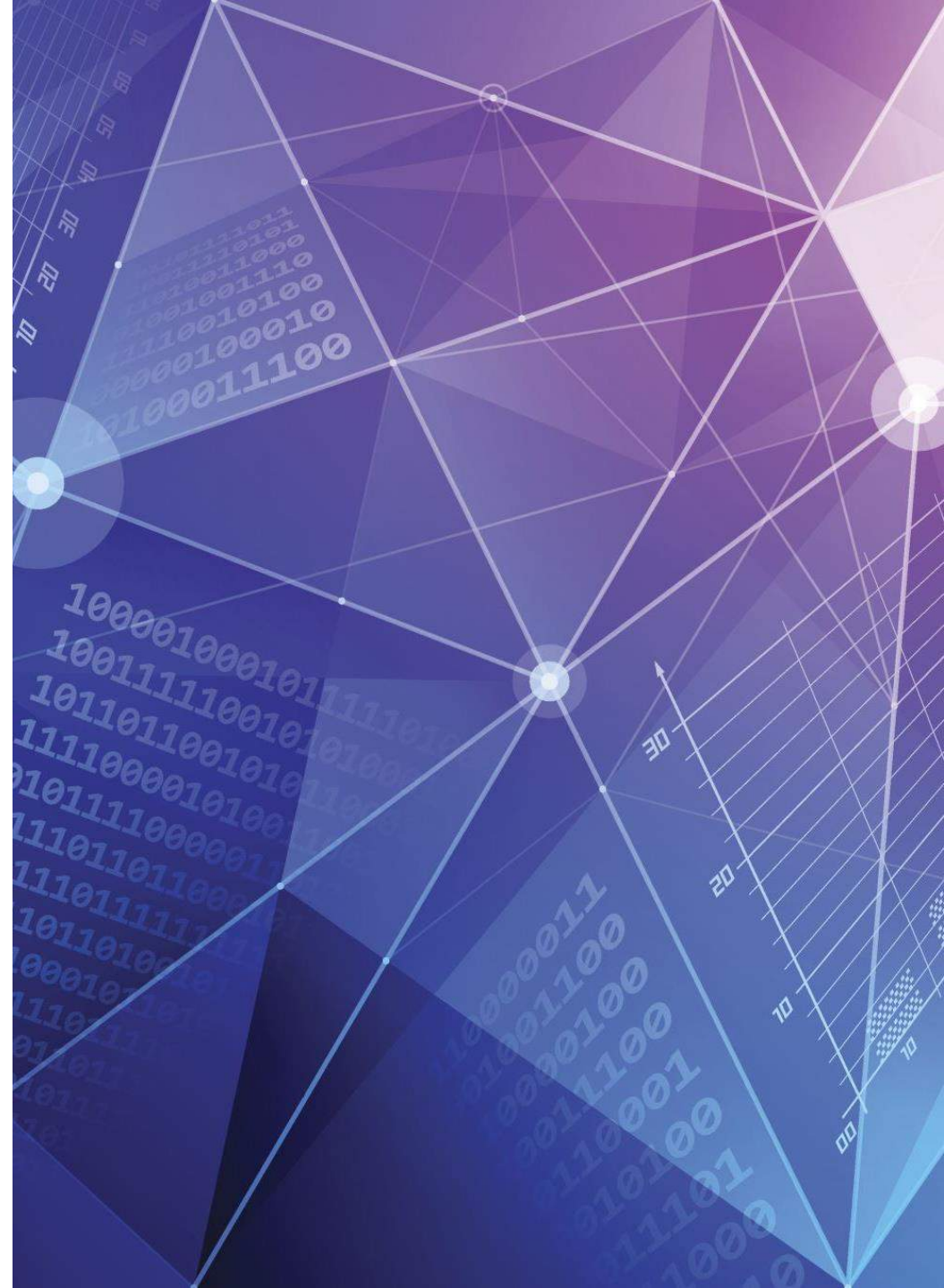
Legal and Ethical Considerations

- Navigating the legal landscape of ethical hacking and cybersecurity. Understanding the ethical responsibilities of ethical hackers. Emphasizing the significance of compliance with laws and regulations.

Conclusion

- In conclusion, ethical hacking is indispensable in today's cybersecurity landscape. By simulating cyber attacks, ethical hackers help organizations identify and patch vulnerabilities, ultimately fortifying systems against malicious threats. Emphasizing the importance of ethical hacking in your presentation highlights its role in proactively securing digital assets and maintaining a robust defense against cyber threats.

Thank You