Introduction to Ethical Hacking

1. What is Ethical Hacking?

Definition:

Ethical hacking is the authorized practice of bypassing system security to identify potential data breaches and threats in a network. Ethical hackers aim to improve security posture, not exploit it.

Also called: *White-hat hacking* or *penetration testing (pentesting)*

---

2. Types of Hackers

Hacker Type	Description
White Hat	Ethical hackers who test systems with permission
Black Hat	Malicious hackers who exploit systems illegally
Grey Hat	Hackers who find vulnerabilities without permission but don't exploit
Script Kiddies	Inexperienced users using existing tools without understanding

Hacktivists	Politically or socially motivated hackers
State-sponsored Hackers	Work for governments to infiltrate enemy systems

---

3. Objectives of Ethical Hacking

- **Identify vulnerabilities** in systems before malicious hackers do
- **Validate** security controls and implementations
- **Ensure compliance** with standards (e.g., ISO 27001, PCI-DSS)
- **Support development** of more secure applications
- **Simulate real-world attacks** to prepare for incident response

---

4. Phases of Ethical Hacking (Based on Penetration Testing Lifecycle)

Phase	Description
1. Reconnaissance	Collecting information about the target system/network
2. Scanning	Identifying open ports, services, and potential entry points (e.g., Nmap, Nessus)
3. Gaining Access	Exploiting vulnerabilities (e.g., SQL injection, buffer overflow)
4. Maintaining Access	Creating backdoors to access the system later
5. Covering Tracks	Deleting logs and hiding intrusion evidence

---

6. Reporting	Documenting vulnerabilities, risk assessment, and mitigation suggestions

---

5. Key Tools Used

Tool	Purpose
Nmap	Network scanning and port discovery
Nessus	Vulnerability assessment
Burp Suite	Web application testing, interception, and attack simulation
Metasploit	Exploitation framework for payload delivery
Wireshark	Network traffic analysis

---

6. Legal and Ethical Considerations

- **Always have written permission** before testing systems.
- **Follow laws** such as the IT Act (India), Computer Fraud and Abuse Act (USA), GDPR, etc.
- **Report findings responsibly**, without disclosing sensitive information to unauthorized parties.

---

7. Difference Between Ethical Hacking and Malicious Hacking

Feature	Ethical Hacking	Malicious Hacking
Authorization	Yes	No
Intent	Security improvement	Data theft/damage
Legal Status	Legal	Illegal
Outcome	Strengthened systems	Compromised systems

---

8. Industry Relevance

Industry	Use Case
Banking	Securing digital transactions, mobile apps
Healthcare	Protecting patient records (HIPAA compliance)
E-Commerce	Testing payment gateways and customer data leaks
Government	Securing national infrastructure and defense systems
IT Services	Regular client-requested pentests

---

9. Career Path in Ethical Hacking

Roles:

- Penetration Tester
- Security Analyst
- Red Team Engineer
- Cybersecurity Consultant
- Bug Bounty Hunter

Certifications:

- CEH (Certified Ethical Hacker)
- OSCP (Offensive Security Certified Professional)
- CompTIA Security+
- CISSP (Certified Information Systems Security Professional)

---

10. Summary

- Ethical hacking is a critical part of cybersecurity strategy.
- It helps organizations stay ahead of malicious attacks.
- Must be practiced responsibly and legally.
- Tools like Nmap, Nessus, and Burp Suite are essential in a hacker’s toolkit.