Introduction to Ethical Hacking

Mr. Vaishnav Shegale
Assistant Professor
Department of Computer Studies (MCA)
Vivekanand College, Kolhapur (An Empowered Autonomous Institute)

What is Hacking?

- **Definition**: Hacking is the act of gaining unauthorized access to data in a system or computer.
- Hackers use technical knowledge to exploit vulnerabilities in software, networks, or systems.
- Goals vary: personal gain, damage, or ethical reasons.

To Understand Hacking, What Do You Need to Know?

1. **Networking Concepts**
   - IP addresses, ports, protocols (TCP/IP, UDP, etc.).
   - Data flow in networks.
   - Tools: Wireshark, Nmap.
2. **Operating Systems**
   - Mainly Linux and Windows.
   - File structures, commands, system configuration.
3. **Programming/Scripting Languages**
   - Basic: HTML, JavaScript.
   - Advanced: Python, Bash, PowerShell.
4. **Databases and Web Applications**
   - SQL, NoSQL databases.
   - Web tech (HTTP, cookies, sessions).
5. **Security Tools & Concepts**
   - Firewalls, VPNs, encryption.
   - Tools: Metasploit, Burp Suite, John the Ripper.

What is Ethical Hacking?

- **Definition**: Legally breaking into computers and devices to test an organization’s defenses (also called penetration testing or white-hat hacking).
- Ethical hackers are hired to find and fix security flaws before malicious hackers exploit them.
- **Example**: A security expert legally tests a company’s system to identify and fix weak spots.

Key Points of Ethical Hacking

- **Legal & Authorized**: Done with permission from the system owner.
- **Goal-Oriented**: Find vulnerabilities to improve security.
- **Protective Role**: Prevents cyberattacks, data breaches, and financial losses.

Who Performs Ethical Hacking?

- Security Researchers
- Penetration Testers
- Information Security Analysts
- Certified Ethical Hackers (CEH)

Types of Ethical Hacking

Type	Description
Network Hacking	Finding weaknesses in networks (routers, firewalls). Tools: Nmap, Wireshark.
Web Application Hacking	Testing websites for bugs like SQL injection, XSS. Tools: Burp Suite, OWASP ZAP.
Wireless Network Hacking	Checking Wi-Fi networks for weak passwords. Tools: Aircrack-ng.
System Hacking	Targeting OS or devices for unauthorized access.
Social Engineering	Tricking people into revealing sensitive information.
Mobile Hacking	Testing Android/iOS apps or devices for security flaws.

Purpose of Hacking

Purpose	**Ethical (White Hat)**	**Malicious (Black Hat)**
Security Testing	Yes ✓	No 55
Stealing Data	No 55	Yes ✓
Improving Systems	Yes ✓	No 55
Causing Damage	No 55	Yes ✓
Finding Vulnerabilities	Yes ✓	Sometimes 55

Advantages of Ethical Hacking

- Identifies weak points to fix security holes.
- Improves security awareness.
- Prevents financial losses from data breaches.
- Protects user and business data.
- Fulfills compliance requirements (e.g., banking, healthcare).

Disadvantages of Ethical Hacking

- **Misuse of Knowledge**: Ethical hackers could turn malicious.
- **Privacy Issues**: Testing may expose confidential data.
- **System Damage**: Aggressive testing may crash systems.
- **Legal Issues**: Hacking without permission is illegal.
- **Expensive**: Hiring skilled ethical hackers can be costly.

Types of Hackers

Type	**Description**
White Hat	Ethical hackers improving security with permission.
Black Hat	Malicious hackers breaking in illegally.
Grey Hat	Mix of both; may act without permission but no harm.
Script Kiddie	Inexperienced hackers using pre-made tools.
Hacktivist	Hacks for political or social causes.
State-sponsored	Government-backed hackers for intelligence.
Red Hat	Vigilante hackers fighting black hats aggressively.
Blue Hat	External testers finding bugs before software release.

Code of Ethics for Ethical Hackers

- **Permission First**: Always get written approval.
- **Stay Within Scope**: Test only allowed areas.
- **Report All Findings**: Share all vulnerabilities with the client.
- **No Data Misuse**: Never leak confidential information.
- **Minimal Damage**: Avoid harming systems during testing.
- **Confidentiality**: Keep client data secure.
- **Follow the Law**: Obey all cyber laws.

Types of Attacks

Attack Type	Description
Phishing	Fake emails/messages tricking users for credentials.
DoS/DDoS	Flooding servers with traffic to cause crashes.
SQL Injection	Injecting SQL code to access databases.
Man-in-the-Middle	Intercepting data between two parties.
Malware Attack	Using viruses, worms, ransomware to harm/steal data.
Brute Force	Trying many password combinations to break in.
Zero-Day Attack	Exploiting unknown vulnerabilities before patching.
XSS	Injecting malicious scripts into websites.

Attack Vectors

Attack Vector	**Description**
Email Attachments	Malware sent via fake email files.
Malicious Links	Fake websites or phishing links.
USB Devices	Infected pen drives plugged into systems.
Web Applications	Exploiting bugs in websites (SQLi, XSS).
Social Engineering	Tricking users into revealing passwords.
Weak Passwords	Cracking easy-to-guess credentials.
RDP	Gaining access via exposed remote desktops.
Mobile Apps	Using unsafe apps with hidden malware.

Prevention from Hackers

- **Strong Passwords**: Use complex passwords with mixed characters.
- **Two-Factor Authentication (2FA)**: Add OTP or authenticator apps.
- **Firewalls**: Block unauthorized access.
- **Antivirus/Anti-Malware**: Detect and remove malicious software.
- **Regular Updates**: Patch OS and software to prevent exploits.
- **Avoid Suspicious Links/Emails**: Don’t click unknown URLs.
- **Secure Wi-Fi**: Use WPA3 encryption and strong passwords.
- **Backup Data**: Keep offline/online backups to prevent ransomware loss.

The Indian IT Act 2000 and Its 2008 Amendments

- **Key Objectives**:
  - Legal recognition of electronic documents and digital signatures.
  - Prevent and punish cybercrimes.
  - Legal framework for secure e-commerce and digital communication.
- **Important Sections**:
  - Sec 43: Penalty for unauthorized access, data theft, viruses.
  - Sec 66: Hacking punishment (3 years jail + ₹5 lakh fine).
  - Sec 66C: Identity theft using digital signatures/passwords.
  - Sec 66D: Cheating by impersonation (email frauds, OTP scams).
  - Sec 67: Publishing obscene material online.
  - Sec 69: Government interception of digital communication.

Phases of Hacking (Cyber Kill Chain)

Phase	Description	Tools/Example
Reconnaissance	Information gathering about the target.	Nmap, Maltego
Scanning	Probing for open ports and services.	Nmap, Nessus
Gaining Access	Exploiting vulnerabilities to enter.	Metasploit, SQLmap
Maintaining Access	Creating backdoors for future entry.	Netcat, Reverse shells
Clearing Tracks	Deleting logs to avoid detection.	Rootkits, log editing
Reporting	Documenting findings (ethical hackers).	Vulnerability reports