Ethical Hacking

Short notes for beginners · CEH · cyber security students · bug bounty

Uncodemy Handwritten Notes · free for students

I. Ethical Hacking Basics

- **Ethical hacking** = testing a system for weaknesses with the owner's written permission, so they can be fixed before a real attacker finds them. Same skills as an attacker, but legal, scoped and reported.
- **CIA triad**: Confidentiality (only authorised people see data), Integrity (data is not changed wrongly), Availability (system works when needed). Other goals: authentication, non-repudiation.

➤ Types of hackers

Type	Meaning
White hat	Ethical, has permission, works to protect
Black hat	Criminal, breaks in for money, damage or data theft
Grey hat	No permission but no bad intent, still illegal
Script kiddie	Uses ready made tools without understanding them
Hacktivist	Hacks for a political or social cause

- Law in India: **IT Act 2000** (Sec 43 damage to computer systems, Sec 66 hacking offences, Sec 66C identity theft, Sec 66D cheating by impersonation). Always get a signed scope and **rules of engagement** first. Report incidents to CERT-In.

REMEMBER No written permission = no testing. Practise only on your own lab, intentionally vulnerable apps and legal platforms.

2. Five Phases of Hacking

Phase	Goal	Example activity
1. Reconnaissance	Collect information	WHOIS, OSINT, social media
2. Scanning	Find live hosts, ports, services	Nmap, vulnerability scan
3. Gaining access	Exploit a weakness	Weak password, unpatched service
4. Maintaining access	Stay inside the system	Backdoor, persistence (attacker)
5. Covering tracks	Hide evidence	Clearing logs (attacker)

- Ethical hackers follow phases 1 to 3, then **report** instead of hiding. Phases 4 and 5 are only simulated, with permission, to show the real risk.
- Common methodologies: PTES, OWASP Testing Guide, NIST SP 800-115, OSSTMM. The **Cyber Kill Chain** (Lockheed Martin) has 7 steps: recon, weaponisation, delivery, exploitation, installation, command and control, actions on objective.
- **MITRE ATT&CK** is a public knowledge base of attacker tactics and techniques. Defenders use it to plan detection.

3. Footprinting and Reconnaissance

- **Passive recon**: no direct contact with the target (search engines, WHOIS, public records, job posts, social media). Almost impossible to detect. **Active recon**: direct interaction (ping, port scan). It can be logged.
- **OSINT** (open source intelligence): domain details, email formats, employee names, technologies in use, leaked data on public sites.

Tool	Use
whois	Domain owner, registrar, name servers
nslookup / dig	DNS records (A, MX, NS, TXT)
theHarvester	Emails, subdomains from public sources
Shodan	Search engine of internet connected devices
Maltego	Link analysis, relation graphs

Tool	Use
Wayback Machine	Old versions of a website

- **Google dorking** uses search operators such as site: and filetype: to find exposed files. Defence: do not leave sensitive files public, review what the company shares online.

4. Scanning and Enumeration

- **Scanning** finds which hosts are alive, which ports are open and which services and versions run. **Enumeration** extracts more details (users, shares, banners) from those services.
- **TCP three way handshake**: client SYN → server SYN/ACK → client ACK. A SYN (half open) scan sends SYN and checks the reply without completing the connection.

Port	Service	Port	Service
21	FTP	110	POP3
22	SSH	139 / 445	SMB
23	Telnet	443	HTTPS
25	SMTP	3306	MySQL
53	DNS	3389	RDP
80	HTTP	8080	HTTP alternate

- **Nmap** options: -sS SYN scan, -sV service version, -O OS detection, -p ports, -Pn skip host discovery, -A aggressive (OS + version + scripts), -oN save output.

EXAMPLE On your own lab machine: nmap -sV -p 1-1000 192.168.1.10 lists open ports from 1 to 1000 with the service version. Never scan networks you do not own or have permission for.

- Vulnerability scanners: **Nessus**, **OpenVAS**, **Nikto** (web server checks). Results need manual checking because scanners give false positives.

5. Common Attacks and Their Defence

Attack	What it is	Defence
Phishing	Fake email or site to steal data	Training, MFA, mail filters
Brute force / dictionary	Trying many passwords	Long passwords, lockout, MFA
SQL injection	Bad input changes database query	Prepared statements, validation
XSS	Script injected into a web page	Output encoding, CSP
CSRF	Tricks logged in user into an action	Anti-CSRF tokens, SameSite cookies
MITM / sniffing	Attacker reads traffic in between	HTTPS/TLS, VPN, secure Wi-Fi
DoS / DDoS	Floods service to stop it	Rate limit, CDN, scrubbing
Ransomware	Encrypts files for payment	Backups, patching, least privilege

- **Social engineering** attacks people, not machines: phishing, vishing (voice), smishing (SMS), pretexting, tailgating. Humans are the weakest link, so awareness training is the best control.

EXAMPLE Password strength: 8 lowercase letters = 26^8 ≈ 2 x 10^11 combinations. 8 letters+digits (mixed case) = 62^8 ≈ 2 x 10^14. 12 such characters = 62^12 ≈ 3 x 10^21. Length wins.

- **Malware** types: virus (needs a host file), worm (spreads by itself), trojan (looks useful), ransomware, spyware, keylogger, rootkit, botnet.

6. OWASP Top 10 and Web Security

- **OWASP Top 10** lists the most critical web risks. The 2021 edition: A01 Broken Access Control, A02 Cryptographic Failures, A03 Injection, A04 Insecure Design, A05 Security Misconfiguration.
- A06 Vulnerable and Outdated Components, A07 Identification and Authentication Failures, A08 Software and Data Integrity Failures, A09 Security Logging and

Monitoring Failures, A10 Server-Side Request Forgery (SSRF).

- Secure coding: validate all input, use parameterised queries, hash passwords with salt (bcrypt, Argon2), set secure cookie flags, keep libraries updated, show generic error messages.
- Practise legally on **DVWA**, **OWASP Juice Shop**, **WebGoat**, **bWAPP**, **TryHackMe**, **Hack The Box**, **OverTheWire** and **VulnHub** machines.

7. Tools and Linux Basics

Tool	Purpose
Kali Linux	Linux distro with security tools pre-installed
Wireshark	Packet capture and protocol analysis
Burp Suite	Intercept and test web requests (proxy)
Metasploit	Framework for authorised exploit testing
John the Ripper / Hashcat	Password hash auditing
Aircrack-ng	Wi-Fi security auditing (own network only)
sqlmap / Gobuster	SQL injection testing / directory discovery
Snort / Suricata	IDS and IPS to detect attacks

- Linux commands: ip a (network), ping, traceroute, netstat or ss (connections), whoami, id, ls -l, cat, grep, find, chmod (permissions), sudo, ps, top.
- Permissions: rwx for owner, group, others. chmod 755 = owner rwx, others r-x. Virtual labs: VirtualBox or VMware with Kali + a vulnerable target on a host-only network.

8. Cryptography and Defence

- **Symmetric** encryption (AES) uses one shared key: fast. **Asymmetric** (RSA, ECC) uses public and private key pair: key exchange, signatures. **Hash** (SHA-256) is one-way and gives a fixed length digest. MD5 and SHA-1 are considered broken.
- **Digital signature** = hash signed with the private key, proves sender and integrity. **SSL/TLS** secures web traffic (HTTPS). **Salt** = random data added to a password

before hashing.

- Defence in depth: firewall, IDS/IPS, WAF, patch management, least privilege, strong authentication (MFA), encryption, logging with SIEM, backups, incident response plan, user awareness.
- **Pentest types**: black box (no information), grey box (some information), white box (full information, source code). Security teams: red team attacks, blue team defends, purple team combines.

9. Reporting, Careers and Practice

- A good report has: executive summary, scope, method, findings with proof, risk rating, impact and clear fix steps. Ratings use **CVSS** scores: 0.1 to 3.9 Low, 4.0 to 6.9 Medium, 7.0 to 8.9 High, 9.0 to 10 Critical.
- Bug bounty: platforms like HackerOne and Bugcrowd. Read the program scope, never test out of scope, report privately, and give clear steps to reproduce.
- Certifications: CEH, CompTIA Security+, eJPT, OSCP, GPEN. Roles: penetration tester, SOC analyst, security consultant, red team member, bug bounty hunter.
- Study plan: networking → Linux → one language (Python or Bash) → web basics → labs on TryHackMe / Hack The Box → write-ups → certification.

10. Most Asked Questions (practice)

1. Define ethical hacking. Differentiate white, black and grey hat hackers.
2. Explain the five phases of hacking with an example each.
3. Passive vs active reconnaissance. Name 5 recon tools.
4. What is the TCP three way handshake? List common ports.
5. Explain SQL injection, XSS and CSRF with defences.
6. What is the CIA triad? Explain with an example.
7. Difference between symmetric and asymmetric encryption.
8. What is the OWASP Top 10? Name any five items.

9. What is social engineering? How can it be prevented?

10. Write the structure of a penetration testing report.

TIP Interviews: explain a vulnerability, how to find it ethically and how to fix it. Build a home lab and keep write-ups of your practice labs on GitHub or a blog.