Tell us what you think

Practical Cybersecurity
Week 4

Instructor – Aman Bhalla

LEARNING OBJECTIVES

By the end of this session, you will:

- Understand the **principles and practices of ethical hacking.**
- Explore **real-world hacking methods and tools.**
- Analyze breach case studies to understand how they occurred.
- Participate in a **hands-on hacking simulation (no install/sign-up)**
- Be fully prepared for the **final assessment.**


WHAT IS ETHICAL
HACKING?

WHAT IS ETHICAL HACKING?

Definition: Ethical hacking refers to the authorized, legal testing of systems to identify vulnerabilities.

Purpose: It is conducted to identify weak points and help organizations strengthen system security.

Example: Ethical hackers simulate phishing to identify weak user behavior.

WHAT IS ETHICAL HACKING?

Aspect	Ethical Hacker	Unethical Hacker
Intent	Protect systems	Exploit systems
Legality	Fully authorized	Illegal
Outcome	Improves security	Causes harm

Ethical hackers must adhere to the scope, report responsibly, and obtain clear consent.

HACKING METHODOLOGIES – THE 5 PHASES

Common ethical hacking framework (mirrors attacker behavior):

1. Reconnaissance.
2. Scanning & Enumeration.
3. Gaining Access.
4. Maintaining Access.
5. Covering Tracks.

PHASE 1 – RECONNAISSANCE (FOOTPRINTING)

- Gathering public info: domains, IPs, job postings, LinkedIn
- Passive: Google Dorking, WHOIS, Shodan
- Active: Ping sweeps, DNS brute force

Example: Using Shodan, an attacker finds exposed security cameras online.

PHASE 2 – SCANNING & ENUMERATION

Identify live systems, open ports, services, and OS versions.

Tools: **Nmap**, Netcat, banner grabbing.

Example: An Nmap scan reveals an open FTP service on port 21 with anonymous access.

PHASE 3 – GAINING ACCESS

Exploiting weak authentication or misconfigured systems.

Exploit techniques:

- SQL Injection
- Command Injection
- Exploiting outdated CMS plugins

Example: In 2012, attackers exploited LinkedIn's weak SHA-1 password hashes and leaked 6.5M accounts.

PHASE 4 - MAINTAINING ACCESS & PRIVILEGE ESCALATION

- Installing backdoors (e.g., reverse shells).
- Adding new admin accounts.
- Exploiting misconfigurations (e.g., SUID binaries in Linux).

Example: In the **Target breach (2013)**, attackers installed malware on POS systems **after gaining access through a third-party HVAC vendor**.

PHASE 5 - COVERING TRACKS

- Log tampering (e.g., clearing syslogs, rotating files).
- Obfuscating malware to avoid detection.
- Disabling antivirus or altering timestamps.

Example: In the **Sony Pictures Hack (2014)**, attackers deleted critical backups and left a fake ransom note to mask real motives (espionage).

PENETRATION TESTING LIFECYCLE

- **Planning & Scoping**
- **Information Gathering**
- **Vulnerability Scanning**
- **Exploitation**
- **Post-Exploitation**
- **Reporting**

Example: Used during **pre-audit security reviews** or compliance testing.

BUG BOUNTY PROGRAMS

Platforms: **HackerOne**, **Bugcrowd**, **Open Bug Bounty**

Example: Teen hacker earned **$36,000** from Apple for iCloud vulnerability.

Benefits: Crowd-sourced vulnerability discovery and responsible reporting.

CAPITAL ONE BREACH (2019)

Exploit: Misconfigured AWS firewall

- Attacker accessed **100M+ customer records.**
- Hacker used **server-side request forgery (SSRF).**

Prevented by: Proper cloud configuration, WAF rules, and access control policies.

CASE STUDY – BRITISH AIRWAYS (2018)

Hackers used **Magecart** to inject JavaScript into the BA payment page.

- Collected **payment data in real time.**
- Entered via **compromised third-party scrip.**

Impact: 500K users; £20M GDPR fine.

Mitigation: Monitor third-party scripts and Content Security Policies (CSPs).

CYBERSECURITY ETHICS

Ethical hackers must:

- Have **documented permission.**
- Stay within the **authorized scope.**
- Report vulnerabilities **confidentially.**
- Breaking rules = legal consequences.

Example: Hacking without permission, even to report a bug, is still **illegal**.

CYBER LAWS & LEGAL BOUNDARIES

Canada: PIPEDA.

US: Computer Fraud and Abuse Act (CFAA).

Europe: GDPR.

They cover data privacy, breach notification, and accountability.

Example: Violations = fines, bans, or jail time.

REFLECTION & DISCUSSION

- What vulnerabilities do you find easiest to exploit?
- What protections could be enforced to stop these attacks?
- Should all companies offer bug bounties? Why/why not?

FINAL EXAM OVERVIEW

Date: March 27 – April 2

Closed-Book | 1.5 Hours.

Reporting Time 6pm, same room as lectures.

No electronics allowed.

Two Equal Parts (50% Each)

Part 1	Part 2
15 Multiple Choice Questions	1 Scenario-Based Question
5 Definition Questions	3 Short Answer + 2 Long Answer

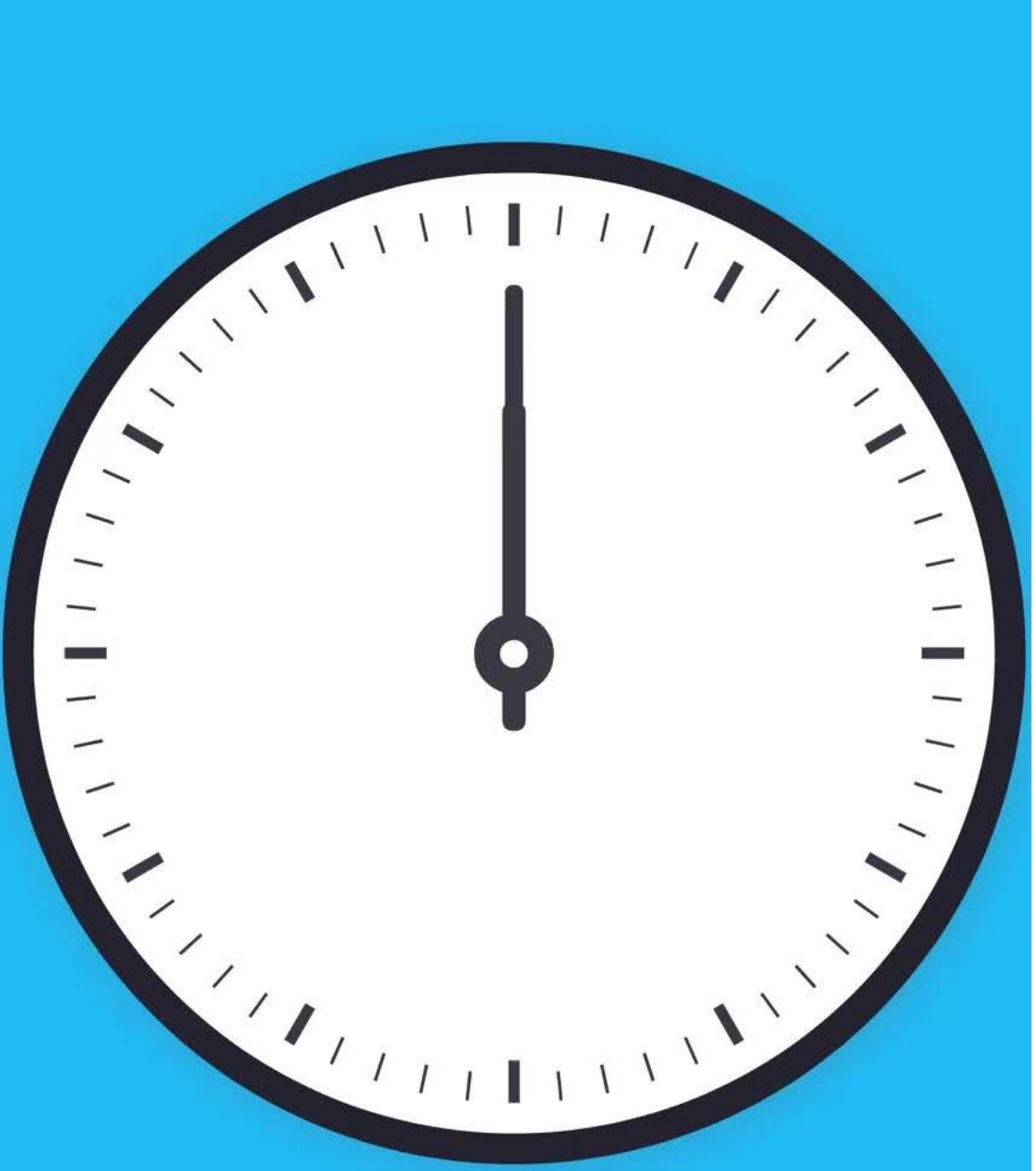
All course topics are covered:

- Cyber Threats.
- OWASP.
- Network & Data Security.
- Incident Response.
- Laws & Ethics.
- Malwares.

FINAL Q&A + WRAP-UP

Open floor for:

- Clarifying exam details.
- Revisiting challenging concepts.
- Sharing reflections on the course.
- Discussing career paths in cybersecurity.



Quiz Time!

- Time Limit – 15 Minutes. The quiz begins at 7:45 pm and will conclude at 8:00 pm.
- Questions: MCQs, True or False and Long Answer.

THANK YOU FOR JOINING!