

Introduction to Ethical Hacking

Your journey to becoming a trusted cyber defender starts here. Welcome to the course.

COURSE INTRODUCTION



DEFINITION



What Is Ethical Hacking?

Ethical hacking means **legally probing systems** to find vulnerabilities before malicious hackers do – with permission, responsibility, and a mission to protect.

- ❑ Think of ethical hackers as **digital security detectives and guardians** – they think like attackers to defend like experts.

Why Ethical Hacking Matters Today

\$10.5T

39s

\$100M+

Annual Cybercrime Cost

Projected global damage by 2025
(Cybersecurity Ventures)

Every 39 Seconds
A cyberattack strikes a business somewhere in the world

Bug Bounty Payouts
Paid globally to ethical hackers for finding critical flaws



Meet the Hacker Types

Not all hackers are the same. Understanding the spectrum is the first step to knowing where ethical hackers stand.



Black Hat
Malicious hackers who exploit systems **illegally** for personal gain, espionage, or destruction.



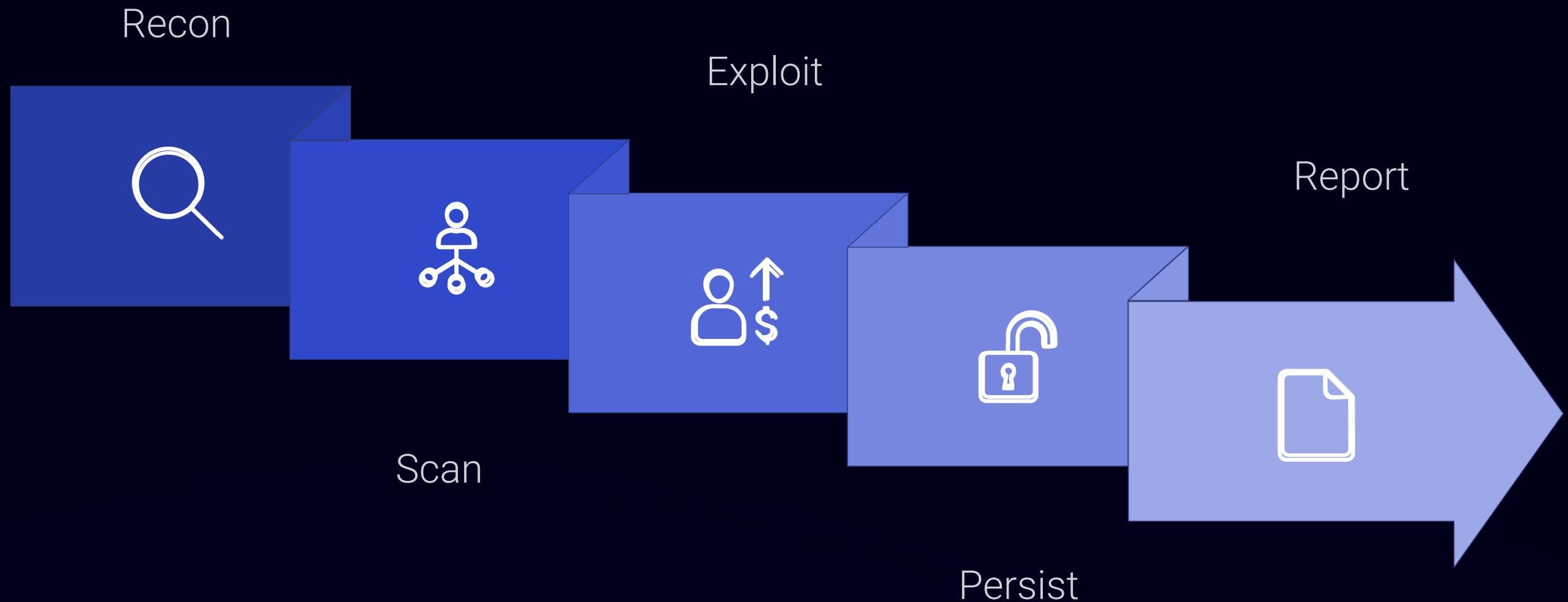
White Hat
Ethical hackers who **defend and secure** systems with authorization and professional integrity.



Grey Hat
Operate **between legal and illegal**, often exposing vulnerabilities publicly without prior permission.

The Ethical Hacking Process

Every professional penetration test follows a structured five-stage methodology.



Essential Tools You'll Learn

Industry-standard tools used by professional penetration testers worldwide.



Nmap

Network scanning and host discovery – map any network in minutes.



Metasploit

Powerful exploitation framework for penetration testing and vulnerability validation.



Wireshark

Deep packet inspection and real-time network traffic analysis.



Burp Suite

The go-to tool for web application security testing and intercepting requests.

Real-World Impact: Ethical Hackers in Action

Lives Saved

In 2023, ethical hackers helped prevent a ransomware attack on a major hospital network, protecting patient care systems.

\$100M+ in Bounties

Bug bounty programs paid over \$100 million globally in 2025 to researchers who uncovered critical security flaws.

National Security

Governments and Fortune 500 companies rely on ethical hackers to safeguard infrastructure and sensitive business assets.



Your Ethical Responsibilities

With great power comes great responsibility. Ethical hacking is built on a foundation of trust, legality, and professionalism.

- Always Get Permission
Never probe a system without **explicit written authorization** from the owner.
- Respect Privacy
Handle all data discovered during testing with strict **confidentiality**.
- Disclose Responsibly
Report all vulnerabilities to the appropriate parties – never exploit or withhold findings.
- Uphold the Law
Operate within **legal and professional standards** at all times, every engagement.

Career Paths & Opportunities

Ethical hacking opens doors to some of the most exciting and rewarding roles in tech.



Penetration Tester

Simulate attacks on systems to uncover vulnerabilities before adversaries do.



Security Analyst

Monitor, analyze, and respond to threats across enterprise environments.



Threat Hunter

Proactively search for hidden threats lurking inside networks and systems.



Certifications

CEH and **OSCP** are globally recognized – average US salary \$100,000+/year.



Ready to Become a Cyber Defender?

This course will equip you with **hands-on skills**, real industry tools, and the ethical mindset that sets true professionals apart.



Hands-On Skills

Practice with real tools in simulated environments.



Ethical Mindset

Hack to protect, never to harm.



Your Journey Starts Now

Let's build the next generation of trusted ethical hackers.