



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Introduction To Ethical Hacking

Lecture 1

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Module Overview and Assessment

Overall Module Assessment: 100% (Portfolio-based)

In this module, students will:

- Research real-world cyber security attacks and penetration testing techniques
- Apply theory and tools to a **virtualized, simulated environment**
- Demonstrate understanding through structured analysis, screenshots, and written reporting
- Produce documentation similar to what a professional penetration tester would submit to a client

Learning Outcomes

- **Explain** ethical hacking and penetration testing concepts
- **Distinguish** between threats, vulnerabilities, and risk
- **Identify** common types of cyber attacks and tests
- **Describe** the purpose and benefits of penetration testing
- **Document** findings and recommend mitigation or risk acceptance

Caution

- The tools and techniques discussed and used in this course should only be used on systems you personally own, or have written permission to use.
- Some of the tools used have the potential to disrupt or break IT systems.

Legal and Ethical Warning

- Penetration testing tools can cause **service disruption, data loss, or system crashes**
- You must **only** test systems you personally own or have **explicit written permission** to test
- Unauthorized testing is **illegal** and may result in **criminal** charges
- Ethical behaviour is **mandatory** throughout this module

This course teaches **defensive security skills**, not criminal activity.

Ethical Hacking

Hacking is the act of exploring systems to understand how they work in practice.

Ethical hacking means:

- Testing systems with permission
- Operating within legal boundaries
- Documenting findings responsibly
- Reporting vulnerabilities so they can be fixed

Ethical hacking exists to **improve security**, not to cause harm.

Definition of a Hacker

A hacker examines how systems are designed to function and investigates how they actually behave in practice.

In a cyber security context, a hacker:

- **Identifies** weaknesses in systems, applications, or networks
- **Analyzes** and tests those weaknesses to understand potential impact
- **Uses** that knowledge either to exploit vulnerabilities

The difference between an ethical and a malicious attacker comes down to intent and permission. Ethical hackers work with authorization to improve security, while malicious actors act without consent for personal gain or harm.

Types of Hackers

White Hat Hackers

- Authorized security professionals working within legal boundaries
- Identify and report vulnerabilities responsibly
- **Example:** A penetration tester hired to assess a company's web application

Black Hat Hackers

- Act without permission
- Exploit vulnerabilities for personal gain, financial profit, or disruption
- **Example:** Deploying ransomware to demand payment

Types of Hackers

Grey Hat Hackers

- Operate without permission but typically without malicious intent
- May disclose vulnerabilities publicly instead of responsibly reporting them
- **Example:** Accessing a system to prove a weakness exists, then notifying the organization

Script Kiddies

- Limited technical knowledge
- Use pre built tools or exploit kits created by others
- **Example:** Downloading automated attack tools to target random websites

Types of Hackers

Hacktivists

- Motivated by political or social causes
- Target organizations to promote an agenda
- **Example:** Defacing a website to spread a political message

Insider Threat Actors

- Employees or contractors misusing legitimate access
- May act maliciously or negligently
- **Example:** Copying sensitive company data before leaving employment

Penetration Tester Mindset

Successful penetration testers:

- **Think** creatively and critically
- **Question** assumptions about security controls
- **View** systems from an attacker's perspective
- **Focus** on logic flaws as much as technical vulnerabilities

They do not simply follow checklists - they **think like adversaries**.



Professional Work Practice

A professional penetration tester must be:

- **Methodical**: follow a structured testing process
- **Thorough**: explore findings fully, not superficially
- **Careful**: avoid unnecessary system disruption
- **Ethical**: respect scope and authorization
- **Well-documented**: keep clear notes and evidence

A key rule: **If a finding cannot be reproduced, it is not a valid finding.**

Threat, Vulnerability, and Risk

- **Threat**: Any circumstance or event that could cause harm
- **Vulnerability**: A weakness that could be exploited
- **Risk**: The likelihood and impact of a threat exploiting a vulnerability

Risk only exists when **a threat targets a vulnerability**.

Understanding this relationship is critical for meaningful security testing.

Role of the Penetration Tester

A penetration tester's role is to:

- **Identify** vulnerabilities in systems or applications
- **Assess** how realistic the threat of exploitation is
- **Demonstrate** potential impact to the organization
- **Recommend** practical mitigation and corrective actions

You are not just finding problems - you are **helping fix them**.

Types of Attacks

Active Attacks

- Involve modification or disruption of systems or data
- Examples include malware, phishing, and man-in-the-middle attacks

Passive Attacks

- Involve monitoring without altering systems
- Example: network or wireless traffic sniffing

All attacks compromise **Confidentiality, Integrity, or Availability**.

Internal vs External Attacks

Internal Attacks

- Launched from within an organization
- Insider threats or compromised internal users



External Attacks

- Originating from the internet
- Partner or third-party connections
- Exposed wireless networks



Penetration Testing

Penetration testing:

- Focuses on identifying **exploitable vulnerabilities**
- **Uses** the same techniques attackers use
- Is a **subset** of ethical hacking
- Goes beyond identification to **prove compromise**

The goal is to show what an attacker could realistically achieve.

Security Assessments

Security assessments aim to identify weaknesses **without exploitation**, including:

- Vulnerability scanning
- Architecture reviews
- Configuration reviews
- Code reviews
- Compliance and security audits



They are often safer but may not show real-world impact.

Benefits of Security Assessments

Security assessments:

- Are less likely to **disrupt** systems
- Are safer for **production** environments
- **Provide** early insight into weaknesses
- **Offer** multiple perspectives from different specialists

They are often used as a first step before penetration testing.

Why Penetration Testing Matters

Penetration testing:

- **Finds** vulnerabilities before attackers do
- **Helps** management understand real business risk
- **Validates** security monitoring and detection
- **Improves** incident response readiness

Security teams are sometimes not informed of tests to assess detection effectiveness.

Handling Findings

From the system owner's perspective:

- **Findings** must be clearly documented
- **Risks** should be prioritized
- **Action** plans should be developed
- **Vulnerabilities** should be mitigated or formally accepted

Professional reporting is as important as technical skill.

Types of Penetration Tests

Common types include:

- Infrastructure and network testing
- Web application testing (front-end and back-end)
- Wireless testing
- Social engineering
- Physical security testing
- IoT and industrial systems testing

Each type requires different tools and techniques.

Next Week

- **Learn** the key phases of penetration testing, from reconnaissance to post exploitation
- **Compare** blind, double-blind, and targeted testing styles and when to use them
- **Understand** the real-world limits of penetration testing and what it can and cannot uncover
- **Get** introduced to essential tools, operating systems, and lab setups used by testers



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Any Questions?

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk