



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

Ethical Hacking Fundamentals

Lecture 2

Trawsnewid Addysg; Trawsnewid Bywydau
Transforming Education; Transforming Lives



www.uwtsd.ac.uk

Learning Outcomes

- **Explain** the purpose and value of penetration testing in improving security.
- **Describe** the key phases and testing approaches used in penetration testing.
- **Identify** common limitations and types of vulnerabilities addressed by penetration tests.
- **Select** appropriate tools, operating systems for basic penetration testing activities.
- **Apply** ethical and legal principles when conducting or evaluating penetration tests.

Ethical Hacking Fundamentals

Penetration testing helps organizations understand how attackers might break in.

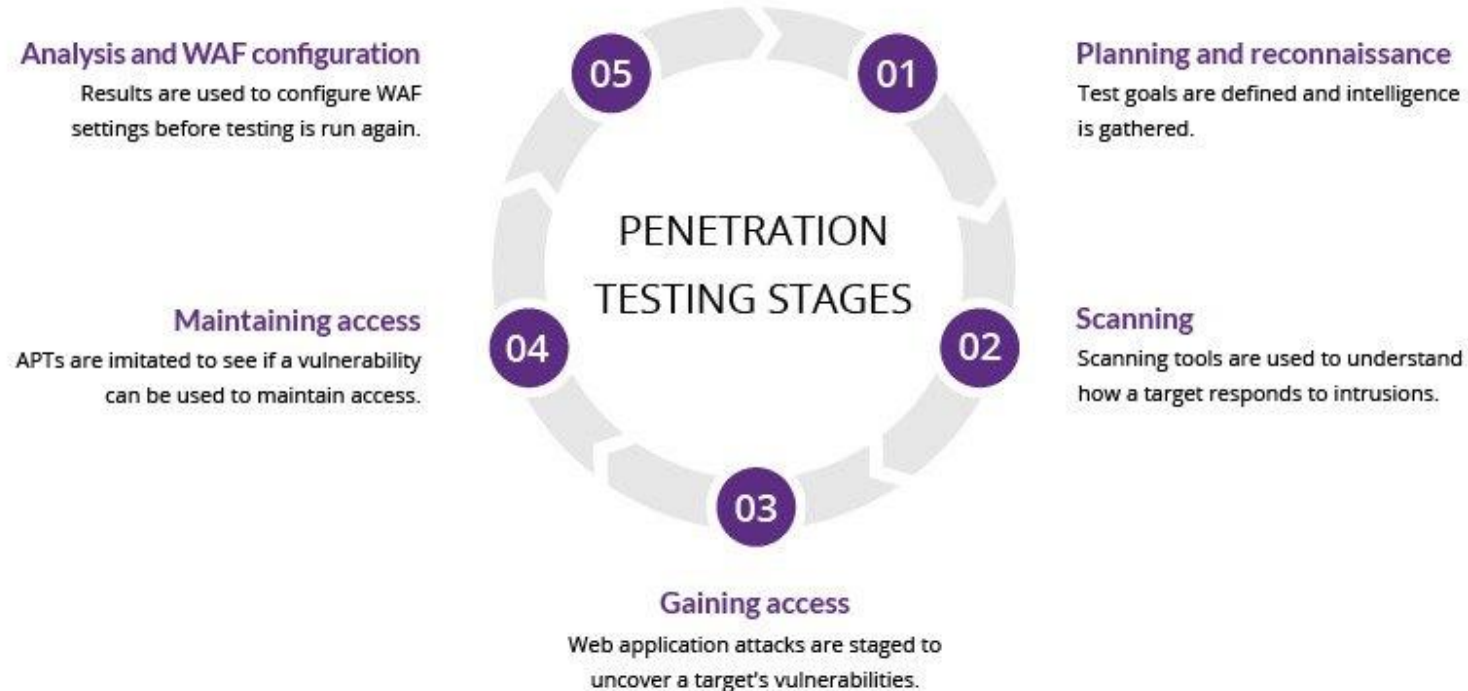
- The goal is not damage, but learning how to improve defenses.
- Think of it like hiring someone to test your locks before a real thief does.

Penetration Testing Phases

Penetration testing usually follows a series of phases.

- These phases help testers stay organized and focused.
- In practice, testers may move back and forth between phases.

Penetration Testing Phases



Phase 1: Reconnaissance

Reconnaissance is about gathering information.

- Testers look for technologies, systems, and entry points.
- Similar to scouting a building before trying to enter it.

Phase 2: Scanning

Scanning looks for weaknesses in the systems discovered earlier.

- Tools are used to find open ports and known vulnerabilities.
- This is like checking which doors or windows are unlocked.

Phase 3: Exploitation

Exploitation tests whether vulnerabilities can actually be used.

- This phase confirms risk instead of guessing.
- Access is gained carefully and in a controlled way.

Phase 4: Post-Exploitation

Post-exploitation shows what an attacker could do after getting access.

- Ethical testers stop short of causing harm.
- Real attackers may steal data, hide access, or erase evidence.

Types of Penetration Testing

- Blind testing simulates an attack with very little information given.
- Double-blind testing keeps defenders unaware of the test.
- Targeted testing involves cooperation and shared feedback.

Post exploitation and Malicious Behavior

Malicious attackers (hacker) go further

- Maintaining access
- Covert Channels
- Data Exfiltration
- Covering Tracks (anti-forensics)

Real-World Penetration Testing

Real tests are rarely neat or predictable.

- Experienced testers rely on intuition and past experience.
- Unexpected discoveries are common.

Limitations of Penetration Testing

Not every vulnerability can be found.

- Time and scope are always limited.
- Some issues only appear under specific conditions.

Known vs Unknown Vulnerabilities

Most tools find known vulnerabilities.

- Finding unknown vulnerabilities requires advanced skills.
- These deeper tests are costly and rarely approved.

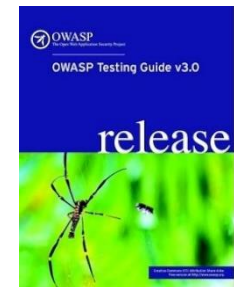
Public Testing Methodologies

Methodologies provide structure and best practices.

- Examples include OSSTMM, OWASP, and NIST guidelines.
- They act as roadmaps rather than strict rules.

OSSTMM 3.0.
The Open Source Security Testing Methodology Manual
Release Candidate 3.0 - Pending the inclusion of Comments, Peer
Review and Final Review
NOT FOR PUBLIC RELEASE
Created by Mike Hocking

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES



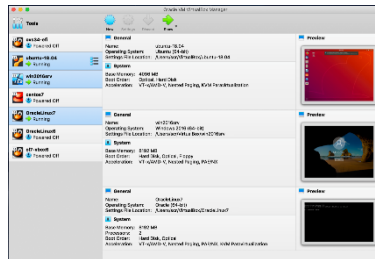
Public Methodologies URL's

- Open-Source Security Testing Methodology Manual (OSSTMM)
<http://www.isecom.org/research/osstmm.html>
- OWASP Testing Framework
https://www.owasp.org/index.php/The_OWASP_Testing_Framework
- NIST SP800-115
<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf>
<http://www.pen-tests.com/penetration-testing-framework.html>
- Penetration Testing Framework 0.59
<http://www.vulnerabilityassessment.co.uk/Penetration%20Test.html>

Tools and Operating Systems

Penetration testers often use multiple operating systems.

- Linux and Windows skills are essential.
- Some tools work better on specific platforms.



Tools Used in This Course

Kali Linux will be the primary testing platform.

- Virtual machines allow safe experimentation.
- Always test tools in controlled environments.

Some Sources of Tools and Exploits

- Exploit Database: <http://www.exploit-db.com/>
- Packet Storm: <http://packetstormsecurity.com/>
- Pentest-Tools: <https://pentest-tools.com/home>
- Audit: <http://www.security-audit.com/blog/penetration-testing-tools/>

I AM NOT ENDORSING THESE SITES, JUST MAKING YOU AWARE OF THEM.

Vulnerability Research

- US-CERT: <https://www.us-cert.gov/>
- National Vulnerability Database: <http://nvd.nist.gov/home.cfm>
- Mitre CVE: <http://cve.mitre.org/>
- Exploit Database: <http://www.exploit-db.com/>
- CVE Details: <http://www.cvedetails.com/>

Building a Testing Lab

Labs are safe places to learn and experiment.

- Virtual machines can be reset or deleted easily.
- Old hardware works just fine for practice.

Cloud and ISP Considerations

ISPs may flag penetration testing as malicious.

- Always get permission before starting Pen Testing.
- Cloud providers have strict rules around security testing.

Key Takeaways

Penetration testing improves security through controlled testing.

- Structure helps, but flexibility is required.
- Ethics and permission are critical.

Next Week

- Understand how port scanning reveals open services and potential vulnerabilities
- Get familiar with common scan types and tools like Nmap and ping sweeps
- Learn how basic scripting can automate and speed up security testing



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