

Advanced Cybersecurity (ACCB6000 | Level 6)

Lectures 1–2: Foundations, Cyber Risk & Penetration Testing

Lecturer: Assoc. Prof. Carlene Campbell

Email: carlene.campbell@uwtsd.ac.uk

Website: <https://www.knowledgewithprofit.com/>

Today's Learning Journey



Start with Security: What Are We Protecting?

Asset

Something of value

Control

Reduces likelihood or
impact

Test

Checks whether the
control works

Information Security: Core Security Properties

Confidentiality

Only authorised access

Integrity

Accurate and unaltered

Availability

Accessible when needed

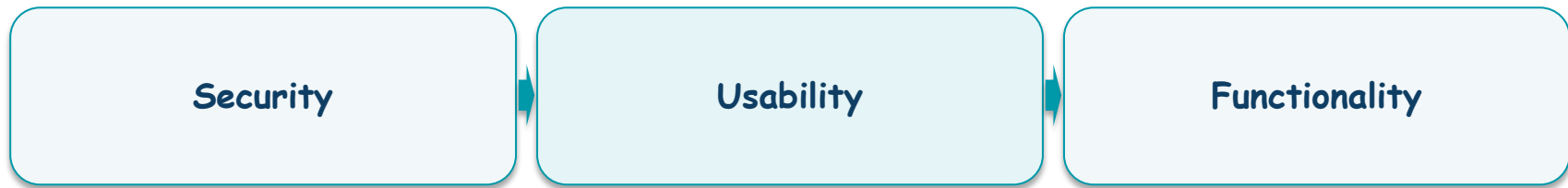
Authenticity

Genuine identity/source

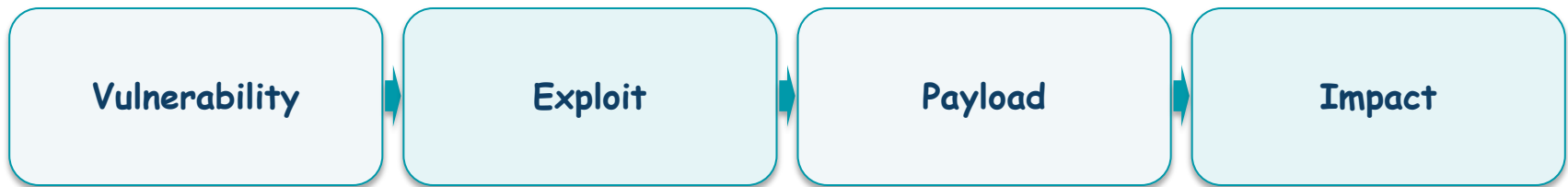
Non-repudiation

Actions cannot credibly be denied

Security Is a Trade-off



Terminology: Vulnerability → Exploit → Payload → Impact



Key distinction: an open port is evidence of exposure not automatically a vulnerability.

Quick Check: What Can You Conclude?

Nmap reports TCP/22 open on a server. Which conclusion is defensible?

- A. The server has been compromised.
- B. SSH is definitely vulnerable.
- C. SSH is exposed and requires further investigation.
- D. The firewall is misconfigured.

From Threat Actor to Business Impact



Common Attack Surfaces

Endpoint

OS, software, local
privilege

Identity

Credentials, MFA, privilege

Application

Code, APIs, configuration

Network

Services, protocols,
segmentation

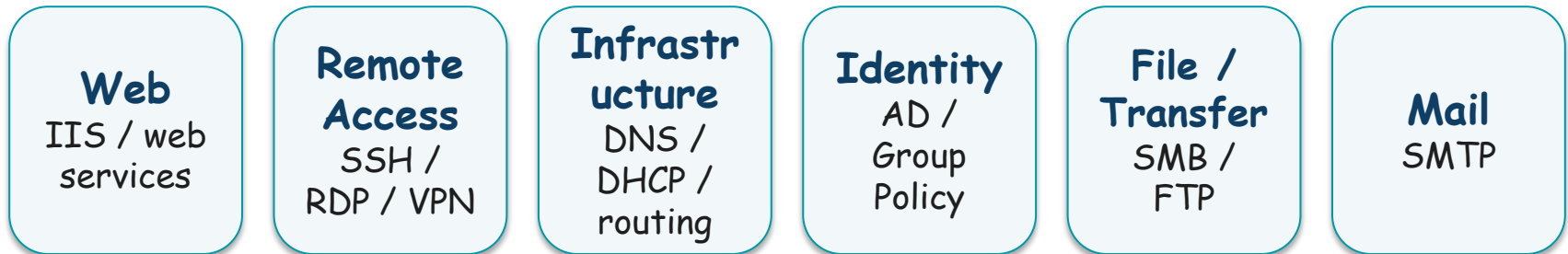
Cloud / Third Party

Configuration and trust

People

Social engineering and
error

Our Lab as an Attack Surface



LAB MINDSET: Discover → interpret → assess → validate → secure → retest

Ethical Hacking: Same Techniques, Different Authority

Authorisation

Written
permission

Scope

Defined systems
and boundaries

Rules of Engagement

Permitted
methods/times

Evidence

Secure handling
and reporting

Authorised testing is controlled professional work not “hacking anything that is reachable”.

Professional Testing Lifecycle



Scenario: Are You Authorised?

During an authorised test you discover a public-facing host owned by the client, but it is not listed in the agreed scope. What do you do?

- A. Scan it because the client owns it.
- B. Exploit only low-risk vulnerabilities.
- C. Pause and obtain scope clarification/authorisation.
- D. Ignore it and omit it from the report.

Lecture 1: What Should You Now Be Able to Explain?

Why security requires more than installing controls

The difference between vulnerability, exploit, payload and impact

Why exposed services require investigation rather than assumption

Why authorisation, scope and rules of engagement matter

How the module lab follows a discover → assess → validate → secure cycle

END OF TODAY'S LECTURE —5-10 minutes then lab session.

Lecture 2 Begins: Cyber Risk & Penetration Testing

RECAP: Threat $\neq$ vulnerability $\neq$ risk. How are they related?



Cyber Risk: Turning Technical Findings into Decisions

Likelihood

How plausible is the event?

Impact

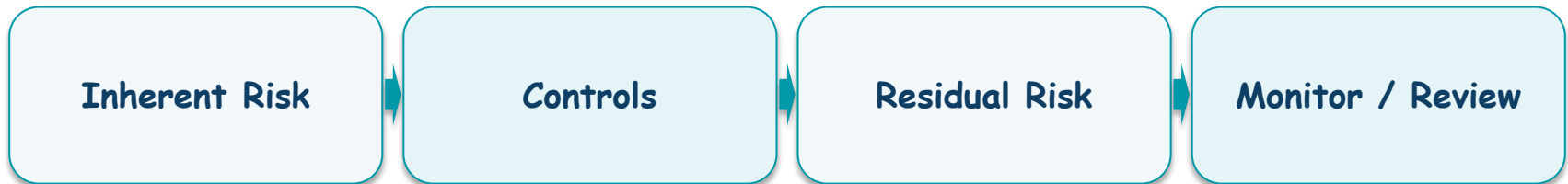
What happens if it occurs?

Context

Asset, exposure, business value

Risk prioritisation requires technical evidence + organisational context.

Inherent and Residual Risk



Risk Management Is Continuous



Communication and consultation run across the entire process.

NIST CSF 2.0: Six Functions

GOVERN

Strategy, policy, roles,
oversight

IDENTIFY

Assets, risks,
improvements

PROTECT

Safeguards and resilience

DETECT

Find/analyse events

RESPOND

Contain and manage
incidents

RECOVER

Restore and improve

Short video: NIST CSF 2.0 overview
<https://www.youtube.com/watch?v=pPPiaGU12Og>

Risk Scenario: Same Vulnerability, Different Risk?

A critical software vulnerability exists on two servers:

System A: internet-facing customer portal; processes sensitive data.

System B: isolated training VM; no production data; restricted network.

Question: Should the remediation priority automatically be identical? Why / why not?

Level 6 expectation: justify the decision using evidence and context.

What Penetration Testing Is and Is Not

Vulnerability Assessment

Find and characterise weaknesses

Penetration Test

Validate exploitability and impact

Security Audit

Assess against requirements/controls

Testing Knowledge Models

Unknown Environment

Little/no internal
information

Partially Known

Limited
information/credentials

Known Environment

Detailed
information/credentials

Older terms you will still encounter: black-box, grey-box, white-box.

Penetration Testing: Before, During, After

PRE-TEST

Authorise • scope • plan •
rules

TEST

Discover • assess •
validate • evidence

POST-TEST

Report • remediate •
retest • close

Methodologies and Knowledge Bases

NIST SP 800-115

Technical security testing
& assessment

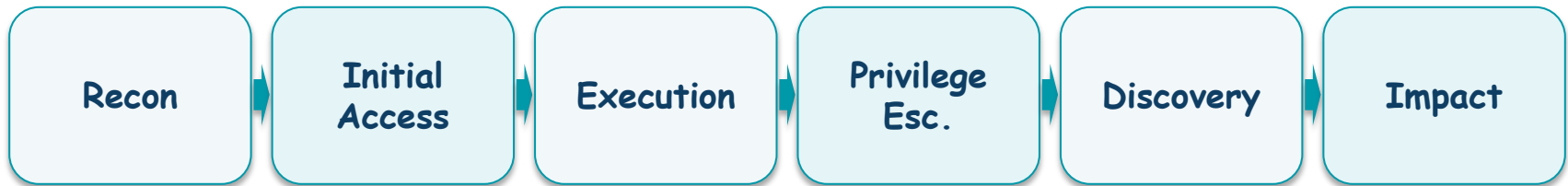
OWASP WSTG

Web application security
testing

MITRE ATT&CK

Adversary tactics &
techniques

MITRE ATT&CK: Why Did the Adversary Act?



ATT&CK helps describe behaviour; it is not a penetration-test “recipe”.

True or False — Justify Your Answer

1. A vulnerability scanner result is sufficient proof that exploitation will succeed.
2. Passive reconnaissance never requires consideration of authorisation or scope.
3. A known-environment test can sometimes provide deeper assurance than an unknown-environment test.
4. A successful penetration test proves the organisation is secure.

From Lecture to Lab: Your First Practical Steps



LAB ENVIRONMENT: intentionally insecure settings may be used for learning.

Assessment Connection

Build evidence progressively each week.

Record what you did, why you did it, what the evidence shows and what it does NOT prove.

Link technical findings to risk and mitigation.

Keep assessment evidence separate from the assessed CTF resources and do not expose CTF flags/solutions.

Evidence + interpretation + professional judgement > screenshots alone.

Lecture 2: Exit Check

What makes security testing ethical and professional?

Why can identical technical vulnerabilities have different organisational risk?

How does vulnerability assessment differ from penetration testing?

Why is retesting necessary after remediation?

Questions?

Questions?

References & Resources (1/2)

NIST (2024), Cybersecurity Framework (CSF) 2.0 — <https://www.nist.gov/cyberframework>

NIST SP 800-115, Technical Guide to Information Security Testing and Assessment — <https://csrc.nist.gov/pubs/sp/800/115/final>

OWASP, Web Security Testing Guide (WSTG) — <https://owasp.org/projects/web-security-testing-guide>

MITRE ATT&CK, Enterprise Tactics — <https://attack.mitre.org/tactics/>

References & Resources (2/2)

NIST (2024), “The NIST Cybersecurity Framework (CSF) 2.0” [video] — <https://www.youtube.com/watch?v=pPPiaGU12Og>

Existing ACCB6000 Lecture 1–2 material (2025), UWTSD internal teaching resource.

ACCB6000 approved assessment specification, UWTSD.

Activity 1 – Getting Ready and associated ACCB6000 lab resources, UWTSD.