

Advanced Cybersecurity (ACCB6000 | Level 6)

Lecture 3: Network Scanning & Enumeration

Lecturer: Assoc. Professor Carlene Campbell

Email: carlene.campbell@uwtsd.ac.uk

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

Learning outcomes

By the end of this combined session, students should be able to:

- Distinguish reconnaissance, scanning and enumeration in a penetration-testing workflow.
- Interpret host-discovery, port-state and service/version evidence without overclaiming.
- Explain common TCP/UDP scanning approaches and the role of TCP flags.
- Use enumeration findings to build a defensible picture of exposed network resources.
- Recommend defensive controls and identify evidence that may reveal scanning activity.

Where are we in the testing workflow?

1. Recon

What exists?

2. Scan

What responds?

3. Enumerate

What is exposed?

4. Assess

What is weak?

5. Validate

Can risk be proven?

Build evidence progressively. A scanner result is a lead, not automatically proof of a vulnerability.

Retrieval check: what can you conclude?

No hands up initially, think for 30 seconds, then discuss with a partner.

A host does not respond to ICMP Echo. Which conclusion is justified?

A

The host is definitely offline

B

ICMP Echo did not produce a reply

C

All TCP ports are closed

D

The firewall is definitely misconfigured

Network scanning: what are we trying to discover?

Hosts

Which systems appear reachable?

Ports

Which TCP/UDP endpoints respond?

Services

What appears to be listening?

Platform clues

OS / device characteristics

Exposure

What deserves deeper assessment?

Scanning progresses from “What is there?” → “What is accessible?” → “What is running?” → “What might it be?” → “What deserves further investigation?”

TCP flags: the language behind many scans

SYN

Start/synchronise

ACK

Acknowledge

RST

Reset

FIN

Finish

PSH

Push buffered data

URG

Urgent pointer valid

Why this matters: scan behaviour is inferred from how targets respond to deliberately crafted TCP packets.

TCP Connect scan: complete the handshake

Scanner → SYN → Target
Scanner ← SYN/ACK ←
Target
Scanner → ACK → Target

Open port

Handshake can complete

Closed port

Typically responds with RST

Professional interpretation: a successful connection shows reachability to a listening TCP service — not that the service is secure.

SYN scan: stop before a full connection

Scanner → SYN → Target
Scanner ← SYN/ACK ←
Target
Scanner → RST → Target

Open

SYN/ACK observed

Closed

RST observed

“Stealth” is contextual. Modern controls can still detect SYN-scan patterns.

FIN / NULL / Xmas scans: response-based inference

FIN

FIN set

NULL

No TCP flags set

Xmas

FIN + PSH + URG

For RFC 793-style behaviour, no response may indicate open|filtered; RST commonly indicates closed. Results vary by operating system and filtering.

Key question: what can you NOT conclude from “no response”?

UDP scanning: silence is ambiguous

UDP has no TCP-style handshake.

ICMP Port Unreachable

Strong evidence that the UDP port is closed

No response

May be open, filtered, or simply silent

UDP assessment often needs protocol-specific probes, retries and careful interpretation.

Tool focus: Nmap as an evidence gathering platform

- Host discovery and network inventory
- TCP/UDP port-state assessment
- Service/version detection
- OS/device fingerprinting clues
- Nmap Scripting Engine (NSE) for authorised service interrogation and assessment

Professional rule

Record target, scope, time, command/options, output and interpretation.

Wireshark: see what the scanner actually generated

**A command tells you what you asked the tool to do.
A packet capture helps you verify what happened on the wire.**

Observe

Flags, ports, timing

Correlate

Request ↔ response

Explain

What evidence supports your conclusion?

Interpret the evidence

Work in pairs for 2 minutes.

You send a TCP SYN to port 443 and receive SYN/ACK. What is the strongest justified conclusion?

A

HTTPS is securely configured

B

A TCP service is accepting connections on 443

C

The host is vulnerable

D

TLS 1.3 is enabled

Defender view: what might scanning look like?

- One source contacting many ports on one host
- One source contacting the same port across many hosts
- Repeated SYNs with limited completed sessions
- Unusual ICMP patterns or protocol probes
- Service/version requests across multiple exposed services
- Bursts that correlate across firewall, IDS/IPS, EDR and server logs

Countermeasures: reduce exposure, improve visibility

Reduce attack surface

Disable unused services;
close unnecessary ports

Control access

Firewalls, ACLs,
segmentation, least
privilege

Maintain systems

Patch, update firmware
and securely configure

Monitor

IDS/IPS, logs, EDR/SIEM
correlation

Self-assess

Authorised scanning and
retesting

Lecture continue next class

Scanning — checkpoint

You should now be able to explain how scan results are produced and why interpretation matters.

5–10 minutes break, then Lab session

Next class

Enumeration

From “a service exists” to “what information does that service expose?”

Scanning vs enumeration

Scanning

Identify reachable hosts, ports and service clues.

Question: “What appears to be there?”

Enumeration

Interact with exposed services to obtain more specific information.

Question: “What can the service tell us?”

Enumeration is typically more deliberate and service-specific, and therefore more likely to create observable evidence.

What might enumeration reveal?

Identity

Users, groups, host/domain names

Resources

Shares, printers, network services

Configuration

Policies, versions, service settings

Infrastructure

Routes, devices, DNS information

Applications

Service/application details

Relationships

Directory and trust clues

SMB / NetBIOS enumeration

- SMB may expose host/domain information, shares and service details.
- Legacy NetBIOS name services can reveal naming information in some environments.
- Modern Windows environments increasingly rely on DNS/SMB rather than NetBIOS, but legacy exposure still matters.
- Anonymous or overly permissive access can turn basic discovery into significant information disclosure.

Professional question: Which finding is merely informative, and which one materially increases attack opportunity?

SNMP enumeration

SNMP manager ↔ agent communication commonly uses UDP 161 for queries.

Potential data

Interfaces, routes, device details, counters

Risk factor

Weak/default community strings in older SNMP deployments

Defence

Prefer SNMPv3, restrict management access, monitor queries

Community strings are not equivalent to modern cryptographic credentials; treat legacy SNMP carefully.

LDAP / Active Directory enumeration

- LDAP provides structured access to directory information.
- Depending on permissions and configuration, queries may reveal users, groups, organisational units and directory attributes.
- In Active Directory environments, directory information can help map identity and privilege relationships.
- Defensive priorities: least privilege, secure LDAP where appropriate, strong authentication, auditing and exposure reduction.

DNS enumeration

Records

A/AAAA, MX, NS, TXT and others

Names

Hosts and service naming patterns

Zone transfer

Misconfiguration may expose a much larger record set

A successful zone transfer is a configuration finding — not something to assume every DNS server permits.

Other services: NTP, SMTP, RPC and VPN clues

NTP

Time service and implementation clues

SMTP

Mail-service behaviour; user validation often restricted

RPC

Service endpoint information

VPN/IPsec

Gateway and negotiation clues

Do not assume a protocol automatically leaks useful information. Modern configurations frequently restrict legacy enumeration behaviour.

Professional judgement: prioritise the findings

Small-group discussion — 3 minutes.

You discover the following during an authorised internal assessment:

- TCP/445 open on a file server
- An SMB share readable by all authenticated users
- SNMPv2c enabled on a network device
- DNS server refuses zone transfer

Which deserves deeper investigation first — and what evidence would you gather before assigning risk?

Enumeration countermeasures

- Remove or disable services that are not required.
- Restrict management protocols to trusted administration networks.
- Use strong authentication and least-privilege access.
- Prefer secure protocol versions and encrypted management channels.
- Harden directory, SMB, DNS and SNMP configuration.
- Monitor unusual queries, repeated service discovery and authentication failures.
- Retest after remediation to verify that exposure has actually changed.

Activity 3: what you will do in the lab

Discover

Identify hosts and network reachability

Scan

Assess TCP/UDP ports and service clues

Observe

Inspect selected traffic in Wireshark

Enumerate

Investigate authorised services such as SMB/SNMP

Evidence

Record output, interpretation and limitations



LAB ENVIRONMENT ONLY — use only the designated ACCB6000 targets.

Evidence record: think like a consultant

Finding	Evidence	What it means	What it does NOT prove	Next step
Example: TCP/22 open	SYN/ACK + service probe	A TCP service is reachable	That SSH is vulnerable	Validate service/version/configuration

**Use this mindset throughout the module: evidence → interpretation
→ limitation → next action.**

Knowledge check

Which statement best distinguishes enumeration from scanning?

A

Enumeration is always passive

B

Enumeration deliberately queries exposed services for more detail

C

Scanning only applies to wireless networks

D

Enumeration proves a vulnerability exists

Lecture 3 summary

- Scanning identifies reachable systems, ports and service clues.
- TCP/UDP behaviour must be interpreted carefully; “no response” is not the same as “open”.
- Enumeration goes deeper by querying exposed services for specific information.
- Tools generate evidence; professional judgement turns evidence into defensible findings.
- Defenders reduce exposure, monitor discovery behaviour and verify remediation through retesting.

References & resources

Core / authoritative resources

- Nmap Project — Nmap Reference Guide and Network Scanning documentation
<https://nmap.org/book/man.html>
- Wireshark Foundation — User's Guide
https://www.wireshark.org/docs/wsug_html_chunked/
- IETF RFC 9293 — Transmission Control Protocol (TCP)
<https://www.rfc-editor.org/rfc/rfc9293>
- IETF RFC 768 — User Datagram Protocol (UDP)
<https://www.rfc-editor.org/rfc/rfc768>
- MITRE ATT&CK — Network Service Scanning (T1046)
<https://attack.mitre.org/techniques/T1046/>
- Microsoft Learn — Windows/Active Directory and SMB documentation
<https://learn.microsoft.com/>

Questions?

Next practical: Activity 3 — Scanning & Enumerating Your Network