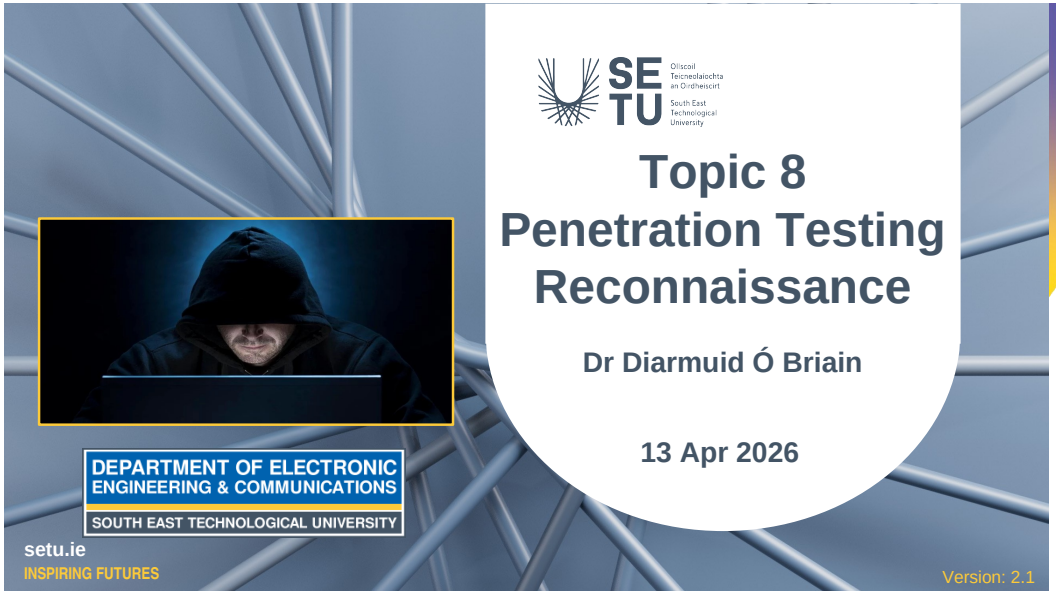


Topic 8
Penetration Testing Reconnaissance

Dr Diarmuid Ó Briain

13 Apr 2026

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

setu.ie
INSPIRING FUTURES

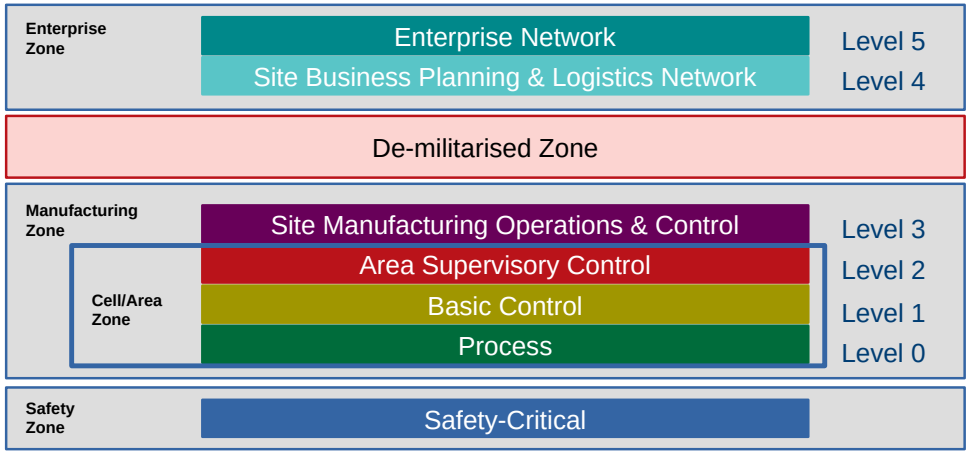
Version: 2.1

Learning objectives

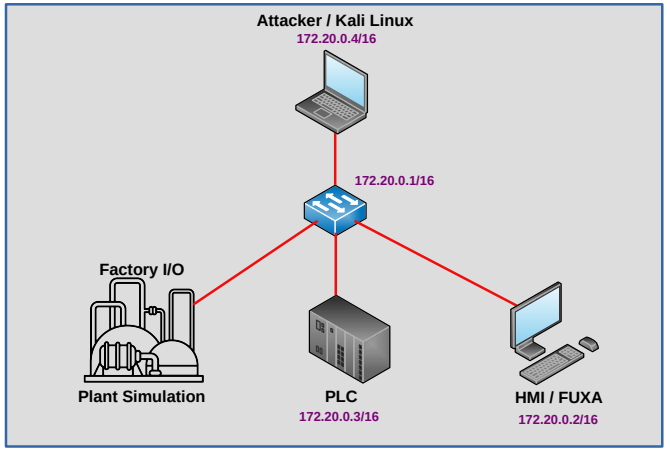
By the end of this topic, you will be able to:

- Carry out a reconnaissance on the VICSORT2 Operational Technology Simulation.

Purdue Model



VICSORT2 Testbed

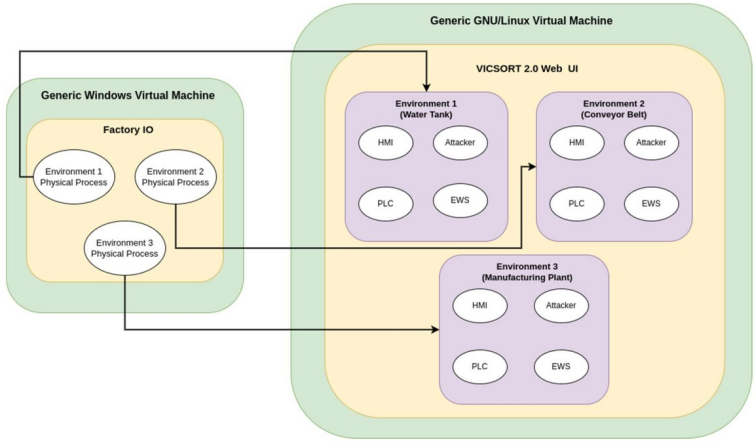


VICSORT2 Testbed

Node	IP Address Mapping
Bridge	172.20.0.1 /16
HMI / FUXA	172.20.0.2 /16
PLC	172.20.0.3 /16
Kali Linux	172.20.0.4 /16

PLC Username: openplc	Password: openplc
Kali Username: kasm_user	Password: password

Architecture Overview



Installing VICSORT2 Platform

Prerequisites

- You have downloaded the Ubuntu 22.04 LTS or 24.04 LTS Desktop version VM and set it up within VirtualBox.
- Assumes a clean VM.
- Google Chrome downloaded onto the VM.

Clone the repository

```
~$ sudo apt update && sudo apt install git -y
~$ git clone https://gitlab.com/ekisac10/vicsort2.0.git
~$ cd vicsort2.0
```

Run Initial Setup

```
~$ sudo bash scripts/setup.sh
```


Gunicorn Manager

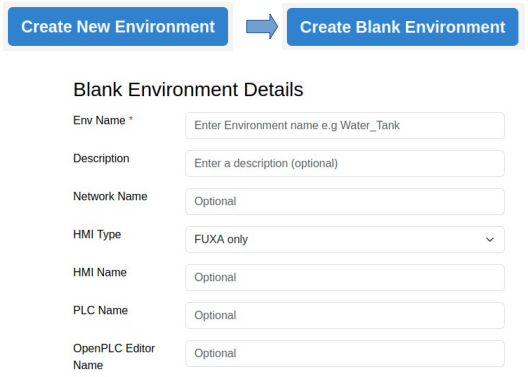
- Start in background
  ```
  ~$ ./scripts/gunicorn_manager.sh start
  ```
- Status / PID
  ```
  ~$ ./scripts/gunicorn_manager.sh status
  ```
- Error log. Also great for monitoring Docker install progress
  ```
  ~$ ./scripts/gunicorn_manager.sh logs
  ```
- Access log
  ```
  ~$ ./scripts/gunicorn_manager.sh logs access
  ```
- Foreground (for live debugging)
  ```
  ~$ ./scripts/gunicorn_manager.sh foreground
  ```
- Stop / Restart
  ```
  ~$ ./scripts/gunicorn_manager.sh stop
  ~$ ./scripts/gunicorn_manager.sh restart
  ~$ sudo bash scripts/setup.sh
  ```

Factory I/O

- Separate Microsoft Windows based VM
- Ensure Factory I/O is running and configured for Modbus TCP Server mode.
- Note its IP address and Modbus TCP port.
- In VICSORT 2.0, configure OpenPLC to connect to the Factory I/O instance.

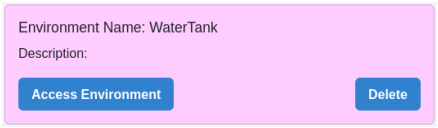
Running the VICSORT testbed

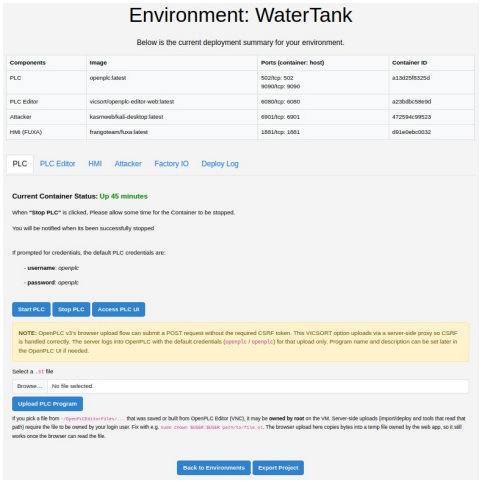
Create First Environment



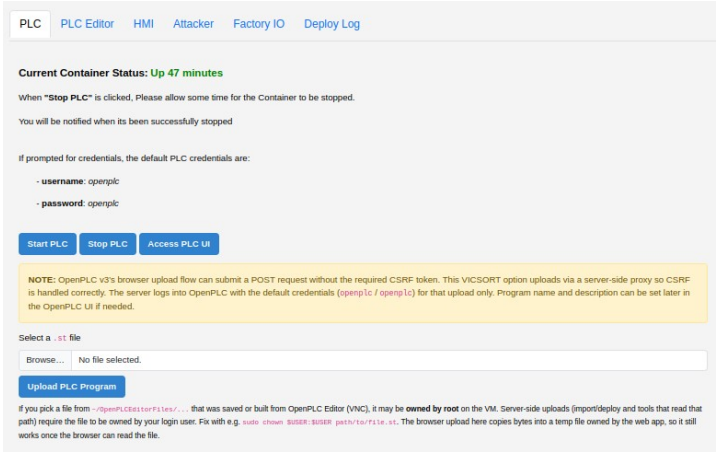

```
~$ bash ./scripts/gunicorn_manager.sh logs
```


Access First Environment

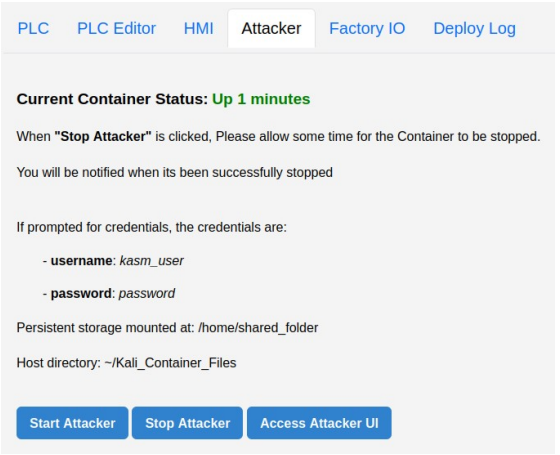




PLC



Kali Linux



Reconnaissance

Kali Linux

Wireshark

Wireshark

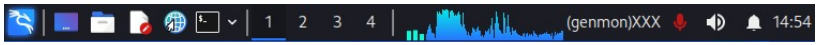
tshark

tshark


```
default:~$ tshark -D
1. eth0
2. any
3. lo (Loopback)
4. bluetooth-monitor
5. nflog
6. nfqueue
7. dbus-system
8. dbus-session
9. ciscodump (Cisco remote capture)
10. dpauxmon (DisplayPort AUX channel monitor capture)
11. randpkt (Random packet generator)
12. sdjournal (systemd Journal Export)
13. sshdig (SSH remote syscall capture)
14. sshdump (SSH remote capture)
15. udpdump (UDP Listener remote capture)
16. wifidump (Wi-Fi remote capture)
```

```
default:~$  tshark -F pcap -V > ~/tshark_out.pcap
Capturing on 'eth0'
903 ^C                                  [Control+C]
default:~$
```

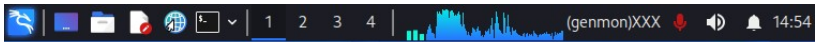
tshark




```
default:~$ head -20 ~/tshark_out.pcap
Frame 1: Packet, 110 bytes on wire (880 bits), 110 bytes captured (880 bits)
on interface eth0, id 0
Section number: 1
Interface id: 0 (eth0)
Interface name: eth0
Encapsulation type: Ethernet (1)
Arrival Time: Apr 3, 2026 15:10:34.161889543 UTC
UTC Arrival Time: Apr 3, 2026 15:10:34.161889543 UTC
Epoch Arrival Time: 1775229034.161889543
[Time shift for this packet: 0.000000000 seconds]
[Time since reference or first frame: 0.000000000 seconds]
Frame Number: 1
Frame Length: 110 bytes (880 bits)
Capture Length: 110 bytes (880 bits)
[Frame is marked: False]
[Frame is ignored: False]
[Protocols in frame: eth: ethertype:ip:tcp:tls]
Character encoding: ASCII (0)
Ethernet II, Src: b6:67:07:fb:5d:d8 (b6:67:07:fb:5d:d8), Dst: 7e:e3:58:83:5b:
1e (7e:e3:58:83:5b:1e)
Destination: 7e:e3:58:83:5b:1e (7e:e3:58:83:5b:1e)
.... LG bit: Locally administered address
( this is NOT the factory default)
```


Netdiscover

netdiscover

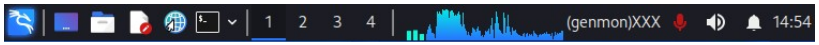



```
default:~$ sudo netdiscover -i eth0 -r 172.20.0.0/16

 Currently scanning: Finished!   |   Screen View: Unique Hosts

 2 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 84

 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------

 172.20.0.2      16:ee:df:9d:2f:7d      1      42  Unknown vendor
 172.20.0.3      72:23:f9:f6:77:80      1      42  Unknown vendor
```


p0f

p0f

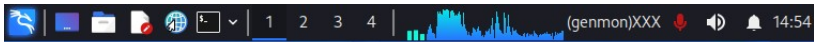
- Fingerprinting technique




```
default:~$ p0f -i eth0 -d -o /root/p0f-output.txt
--- p0f 3.09b by Michal Zalewski <lcamtuf@coredump.cx> ---

[!] Consider specifying -u in daemon mode (see README).
[+] Closed 1 file descriptor.
[+] Loaded 322 signatures from '/etc/p0f/p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file '/home/kasm-user/p0f-output.txt' opened for writing.
[+] Daemon process created, PID 24646 (stderr not kept).

Good luck, you're on your own now!

default:~$ ps -ef | grep p0f

root        24646       1  0 16:35 ?        00:00:00 p0f -i eth0 -d -o /home/kasm-
user/p0f-output.txt
kasm-us+        24769    24032  0 16:38 pts/3    00:00:00 grep p0f
```


p0f

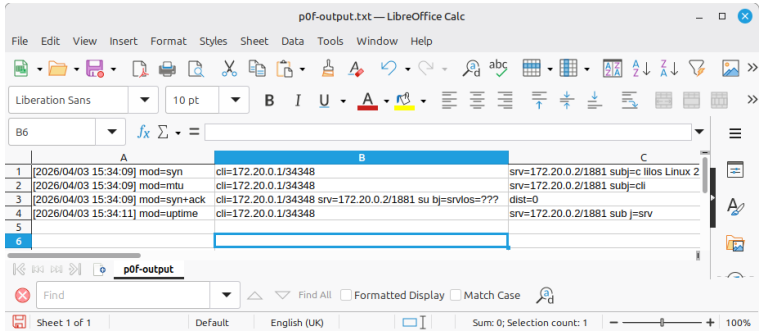
- Fingerprinting technique

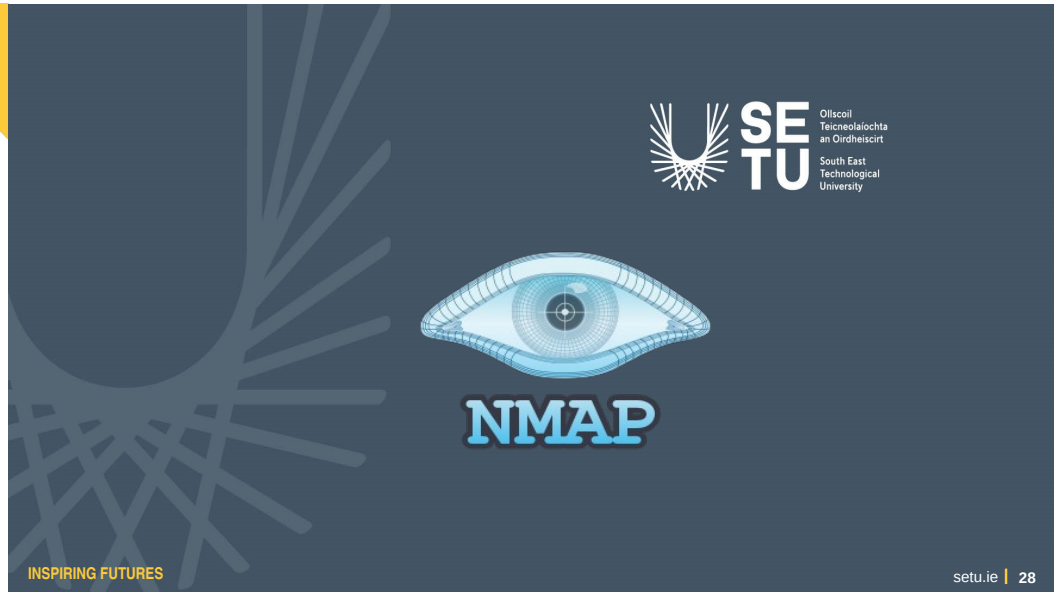



```
default:~$ sudo tail -f ~/p0f-output.txt
2026/04/03 15:34:09] mod=syn|cli=172.20.0.1/34348|srv=172.20.0
.2/1881 subj=c lilos Linux 2.2.x-3.x dist=0|params=generic|raw
_sig=4:64+0:0:1460:mss*44,10:m ss,sok,ts,nop,ws:df,id+:0
[2026/04/03 15:34:09] mod=mtu|cli=172.20.0.1/34348|srv=172.20.0
.2/1881 subj=cli|link=Ethernet or modem|raw_mtu=1500
[2026/04/03 15:34:09] mod=syn+ack|cli=172.20.0.1/34348 srv=172
.20.0.2/1881 su bj=srvlos=???|dist=0|params=none|raw_sig=4:64
+0:0:1460:mss*45,10:mss,sok,ts,n op,ws:df:0
[2026/04/03 15:34:09] mod=mtu|cli=172.20.0.1/34348 srv=172.20
.0.2/1881 subj=srv|link=Ethernet or modem|raw_mtu=1500
[2026/04/03 15:34:11] mod=uptime|cli=172.20.0.1/34348|srv=172
.20.0.2/1881 sub j=srv|uptime=43 days 6 hrs 46 min (modulo 49 days)|raw_freq=1000.00 Hz

default:~$ sudo kill -SIGKILL 24646

default:~$ ps -ef | grep p0f

default:~$  ps -ef | grep p0f
kasm-us+        25922    24032  0 16:38 pts/3    00:00:00 grep p0f
```


p0f

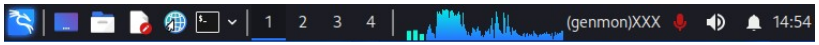
- Fingerprinting technique





NMAP

- Network Mapper




```
default:~$  nmap -sn 172.20.0.0/16 --exclude 172.20.0.4

Starting Nmap 7.98 (https://nmap.org) at 2026-04-03 16:01 +0000
Nmap scan report for vicsort2-VirtualBox.local (172.20.0.1)
Host is up (0.000056s latency).
MAC Address: 7E:E3:58:83:5B:1E (Unknown)
Nmap scan report for Water_Tank_fuxa. Water_Tank_network (172.20.0.2)
Host is up (0.000024s latency).
MAC Address: 16:EE:DF:9D:2F:7D (Unknown)
Nmap scan report for Water_Tank_plc.Water_Tank_network (172.20.0.3)
Host is up (0.00012s latency).
MAC Address: 72:23:F9:F6:77:80 (Unknown)
```


NMAP Options

-sn: Ping Scan - disable port scan.

-A: Enable OS detection, version detection, script scanning, and traceroute.

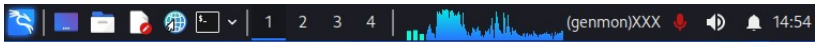
-T<0-5>: Set timing template (higher is faster).

-p: Only scan specified ports.

-p-: Scan for all 65,535 open ports on a target.

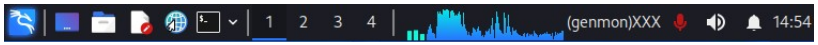
-v: Increase verbosity level (use -vv or more for greater effect)

NMAP




```
default:~$ nmap -v -sn 172.20.0.2

Starting Nmap 7.98 (https://nmap.org) at 2026-04-03 16:04 +0000
Initiating ARP Ping Scan at 16:04
Scanning 172.20.0.2 [1 port]
Completed ARP Ping Scan at 16:04, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:04
Completed Parallel DNS resolution of 1 host. at 16:04, 0.00s elapsed
Nmap scan report for Water_Tank_fuxa.Water_Tank_network (172.20.0.2)
Host is up (0.000050s latency).
MAC Address: 16:EE:DF:9D:2F:7D (Unknown)
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds Raw packets sent: 1 (28B) |
Rcvd: 1 (288)
```


NMAP




```
default:~$ nmap -v -sn 172.20.0.3

Starting Nmap 7.98 (https://nmap.org) at 2026-04-03 16:05 +0000
Initiating ARP Ping Scan at 16:05
Scanning 172.20.0.3 [1 port]
Completed ARP Ping Scan at 16:05, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:05
Completed Parallel DNS resolution of 1 host. at 16:05, 0.00s elapsed
Nmap scan report for Water_Tank_plc.Water_Tank_network (172.20.0.3)
Host is up (0.000061s latency).
MAC Address: 72:23:F9:F6:77:80 (Unknown)
Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds Raw packets sent: 1 (288) |
Rcvd: 1 (288)
```

NMAP

```
default:~$ nmap -A -T4 -p- 172.20.0.2
Starting Nmap 7.98 (https://nmap.org) at 2026-04-03 16:07 +0000
Nmap scan report for Water_Tank_fuxa.Water_Tank_network (172.20.0.2)
Host is up (0.00014s latency).
Not shown: 65534 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
1881/tcp open  http    Node.js Express framework
|_http-title: FUXA
MAC Address: 16:EE:DF:9D:2F:7D (Unknown)
Device type: general purpose
Running: Linux 4.X15.X
OS CPE: cpe:/o:linux:linux_kernel: 4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.155.19
Network Distance: 1 hop

TRACEROUTE
HOP      RTT       ADDRESS
1        0.14 ms Water_Tank_fuxa.Water_Tank_network (172.20.0.2)

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 15.50 seconds
```

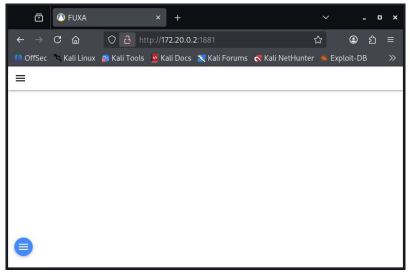

NMAP

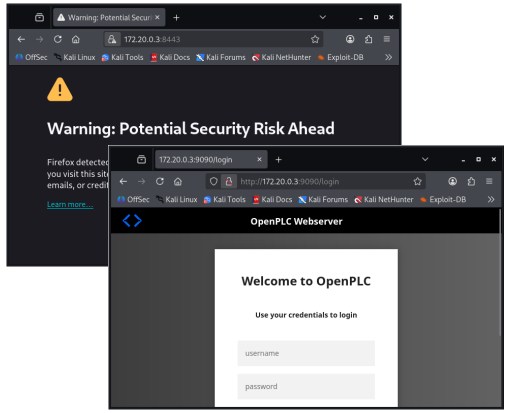
```
default:~$ nmap -A -T4 -p- 172.20.0.3
Starting Nmap 7.98 (https://nmap.org) at 2026-04-03 16:08 +0000
Nmap scan report for Water_Tank_plc.Water_Tank_network (172.20.0.3)
Host is up (0.00011s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8443/tcp open  ssl/http Werkzeug httpd 2.3.7 (Python 3.10.12)
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost
| Subject Alternative Name: DNS:localhost, IP Address: 127.0.0.1
| Not valid before: 2026-04-02T19:52:12
|-Not valid after: 2126-03-09T19:52:12
9090/tcp open http Werkzeug httpd 2.3.7 (Python 3.10.12)
|_http-server-header: Werkzeug/2.3.7 Python/3.10.12
| http-title: Site doesn't have a title (text/html; charset=utf-8).
|_Requested resource was /login
MAC Address: 72:23:F9:F6:77:80 (Unknown)
Device type: general purpose
Running: Linux 4.X15.X
OS CPE: cpe:/o:linux:linux_kernel: 4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 5.19
Network Distance: 1 hop
TRACEROUTE
HOP RTT      ADDRESS
1   0.11 ms Water_Tank_plc.Water_Tank_network (172.20.0.3)
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 47.17 seconds
```


NMAP

IP Address	Port	Service	Software/Platform	Role
172.20.0.2	1881	HTTP	FUXA (Node.js)	Visualisation / Dashboard
172.20.0.3	8443	HTTPS	Werkzeug (Python)	Secure Admin/API
172.20.0.3	9090	HTTP	Werkzeug (Python)	Web Login / Management

Browse to the ports indicated from NMAP scans

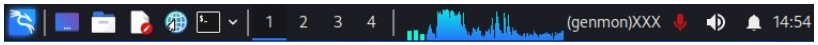




Nikto

Nikto

- Scan webservers for known vulnerabilities




```
default:~$ sudo apt purge nikto

default:~$ sudo apt install nikto

default:~$  nikto -host 172.20.0.3 -port 9090
+ Target IP:        172.20.0.3
+ Target Hostname:   172.20.0.3
+ Target Port:      9090
+ Platform:         Unknown
+ Start Time:       2026-04-03 23:04:31 (GMT0)
---------------------------------------------------------------------------
+ Server: Werkzeug/2.3.7 Python/3.10.12
+ No CGI Directories found (use -C all' to force check all possible dirs). C GI tests
skipped.
+ [013587]/: Suggested security header missing: referrer-policy. See: https:
//developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

.....
```


metasploit

Metasploit Framework

- Metasploit Framework is a penetration testing framework from Rapid7 and has the following key characteristics:
  - **Comprehensive Testing**: provides extensive options for penetration testing, helping identify vulnerabilities in systems and networks.
  - **Exploit Development**: aids in developing and testing exploits for identified vulnerabilities, enhancing system security.
  - **Payload Crafting**: users can create payloads to gain control over compromised systems, providing a deeper understanding of potential threats.
  - **Post-Exploitation Tools**: includes tools for extracting valuable data and maintaining access after a successful breach.
  - **Network Analysis**: offers capabilities to analyse network structures and identify potential entry points for securing the network.

Metasploit Framework

- To get started with metasploit install the **metasploit-framework**.

```
default:~$ sudo apt update
```

- Start the Postgresql Database.

```
default:~$ service postgresql status
18/main (port 5432): down
default:~$ sudo service postgresql start
Starting PostgreSQL 18 database server: main.
```


Metasploit Framework

- Reinitialise the database.

```
default:~$ sudo msfdb reinit
[+] Starting database
[+] Deleting configuration file
[i] Database already stopped
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file
'/usr/share/metasploit-framework/config/datab ase.yml'
[+] Creating initial database schema
```


Metasploit Framework

- Start the database.

```
default:~$ sudo msfdb reinit
[+] Starting database
[i] The database appears to be already configured, skipping
initialization
```

- Check the postgresql database.

```
default:~$ sudo msfdb status
[i] No network service running
[+] Detected configuration file
(/usr/share/metasploit-framework/config/database.yml)
```


Metasploit Console

```
default:~$ msfconsole
Metasploit tip: When in a module, use back to go back to the top level prompt

       =[ metasploit v6.4.124-dev                               ]
+ -- --=[ 2,632 exploits - 1,328 auxiliary - 1,707 payloads     ]
+ -- --=[ 431 post - 49 encoders - 14 nops - 12 evasion         ]


Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework os a Rapid7 Open Source Project

msf >
```

Keep Metasploit Updated

```
default:~$ sudo apt update; sudo apt install metasploit-framework
```


Metasploit using nmap

- **nmap** exists as a module within **metasploit**, use it to get a list of IP addresses on the network. Note that this command will take some time, go for a tea break perhaps?

-Pn: Treat all hosts as online -- skip host discovery.

-sS: Use the TCP SYN scan technique.

-A: Enable OS detection, version detection, script scanning, and traceroute.

-oX netscan: Output as eXtensible Markup Language (XML) to the file **netscan**.

Metasploit using nmap

```
msf > nmap -Pn -sS -A -OX netscan.xml 172.20.0.0/29 -exclude 172.20.0.4
[*] exec: nmap -Pn -sS -A -OX netscan.xml 172.20.0.0/29 -exclude 172.20.0.4

Starting Nmap 7.98 (https://nmap.org) at 2026-04-11 06:43 +0000
Nmap scan report for vicsort2-VirtualBox.local (172.20.0.1)
Host is up (0.000099s latency).
Not shown: 996 closed tcp ports (reset)
PORT       STATE   SERVICE            VERSION
6901/tcp   open    ssl/jetstream?
| ssl-cert: Subject:
commonName=kasm/organizationName=None/stateOrProvinceName=VA/countryName=US
| Not valid before: 2026-04-11T05:48:11
|_Not valid after: 2036-04-08T05:48:11
|_ssl-date: TLS randomness does not represent time
. . . . .
```


Metasploit using nmap

- Import the retrieved data, in the XML file, into Metasploit

```
msf > db_import netscan.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.14.5'
[*] Importing host 172.20.0.1
[*] Importing host 172.20.0.2
[*] Importing host 172.20.0.3
[*] Successfully imported /root/netscan.xml
```

Metasploit using nmap

```
msf > hosts

Hosts
=====

address     mac                name          os_name       os_flavor  os_sp  purpose
-------     ---                ----          -------       ---------  -----  -------
172.20.0.1  52:7f:8a:cd:e1:63  vicsort2-VirtualBox.local   Linux      4.X    server
172.20.0.2  42:5c:72:48:cd:80  Water_Tank_fuxa.Water_Tan   Unknown           device
                               k__network
172.20.0.3  ba:d0:f6:20:21:2d  Water_Tank_plc.Water_Tank   Linux      4.X    server
                               __network

msf > hosts -o /home/kasm-user/scanned_hosts.csv
[*] Wrote hosts to /home/kasm-user/scanned_hosts.csv
```


Metasploit using nmap

```
default:~$ cat /home/kasm-user/scanned_hosts.csv

address,mac, name, os_name,os_flavor, os_sp, purpose, info,comments
"172.20.0.1", "52:7f:8a:cd:e1:63", "vicsort2-VirtualBox.local",
"Linux","", "4.X", "server"
"172.20.0.2","42:5c:72:48:cd:80", "Water_Tank_fuxa.
Water_Tank_network", "Unknown","","", "device"
" 172.20.0.3", "ba:d0:f6:a0:21:2d",
"Water_Tank_plc.Water_Tank_network", "Linux","", "4.X", "server"
default:~$
```


Metasploit using nmap

```
msf > services

Services
========

host            port  proto  name           state  info
----            ----  -----  ----           -----  ----
172.20.0.1      6901  tcp    ssl/jetstream  open
172.20.0.1      8000  tcp    tcpwrapped     open
172.20.0.1      8080  tcp    http           open   Apache Tomcat language: en
172.20.0.1      9090  tcp    http           open   Werkzeug httpd 2.3.7 Python 3.10.12
172.20.0.3      8443  tcp    ssl/http       open   Werkzeug httpd 2.3.7 Python 3.10.12
172.20.0.3      9090  tcp    http           open   Werkzeug httpd 2.3.7 Python 3.10.12

msf > services -o /home/kasm-user/scanned_services.csv
[*] Wrote hosts to /home/kasm-user/scanned_services.csv
```


Metasploit using nmap

```
default:~$ cat /home/kasm-user/scanned_hosts.csv

host, port, proto, name, state, info, resource, parents
"172.20.0.1", "6901", "tcp", "ssl/jetstream", "open",
"172.20.0.1", "8000", "tcp", "tcpwrapped", "open","","{}"
" 172.20.0.1", "8080' "tcp", "http", "open", "Apache Tomcat language:
en", "{}","" "172.20.0.1", "9090' tcp "http", "open", "Werkzeug httpd
2.3.7 Python 3.10.12","{}",""
"172.20.0.3", "8443", "tcp", "ssl/http", "open", "Werkzeug httpd
2.3.7 Python 3.10.12""""" "172.20.0.3", "9090", "tcp", "http",
"open", "Werkzeug httpd 2.3.7 Python 3.10.12","{}",
```

Searching for Modules

- A core functionality of the Metasploit Framework is its extension via modules.
- To hunt for specific modules use the command format:

```
msf > search <search-term>
```

- Replace **<search-term>** with relevant keywords or terms.

Searching for Modules

- For example, to find exploits associated with port scanning:

```
msf > search portscan

Matching Modules
================

#  Name                                              Disclosure Date  Rank    Check Description
-  ----                                              ---------------  ----    ----- -----------
0  auxiliary/scanner/portscan/ftpbounce                               normal  No    FTP Bounce Port Scanner
1  auxiliary/scanner/natpmp/natpmp_portscan                           normal  No    NAT-PMP External Port
Scanner
2  auxiliary/scanner/sap/sap_router_portscanner                       normal  No    SAPRouter Port Scanner
3  auxiliary/scanner/portscan/xmas                                    normal  No    TCP "XMas" Port Scanner
4  auxiliary/scanner/portscan/ack                                     normal  No    TCP ACK Firewall Scanner
5  auxiliary/scanner/portscan/tcp                                     normal  No    TCP Port Scanner
6  auxiliary/scanner/portscan/syn                                     normal  No    TCP SYN Port Scanner
7  auxiliary/scanner/http/wordpress_pingback_access                   normal  No    Wordpress Pingback Locator

Interact with a module by name or index. For example info 7, use 7 or use
auxiliary/scanner/http/wordpress_pingback_access
```


Searching for Modules

- After identifying a desired module, activate it with the following command: `use <number | exploit-name>`

```
msf > use 6
msf auxiliary(scanner/portscan/tcp) >
```


Configuring Module Parameters

- Before deploying a module, adjusting specific parameters, such as target IP, port, or chosen payload, is often necessary.
- List a module's configurable options:

```
msf auxiliary(scanner/portscan/tcp) > show options

Module options (auxiliary/scanner/portscan/tcp):

Name         Current Setting  Required  Description
----         ---------------  --------  -----------
CONCURRENCY  10               yes       The number of concurrent ports to check per host
DELAY        0                yes       The delay between connections, per thread, in ms
JITTER       0                yes       The delay jitter factor (maximum value by which to +/-
PORTS        8443,9090        yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS       172.20.0.3       yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/usi
                                        ng-metasploit.html
THREADS      50               yes       The number of concurrent threads (max one per host)
TIMEOUT      1000             yes       The socket connect timeout in ms


View the full module info with the info, or info -d command.
```

Execute the Module

```
msf auxiliary(scanner/portscan/tcp) > run
[+] 172.20.0.3:         - 172.20.0.3:9090 - TCP OPEN
[+] 172.20.0.3:         - 172.20.0.3:8443 - TCP OPEN
[*] 172.20.0.3:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


Learning objectives

- Carry out a reconnaissance on the VICSORT2 Operational Technology Simulation. ✓

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

D +353 59 917 5000 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

Thank you

engcore
advancing technology