Penetration Testing Reconnaissance

Dr Diarmuid Ó Briain

22 Apr 2024

setu.ie
INSPIRING FUTURES

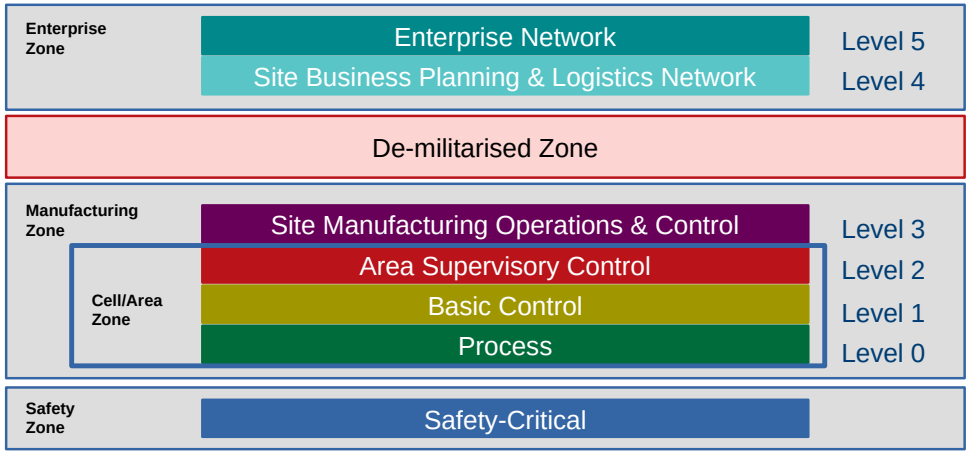
Version: 1.1

Learning objectives

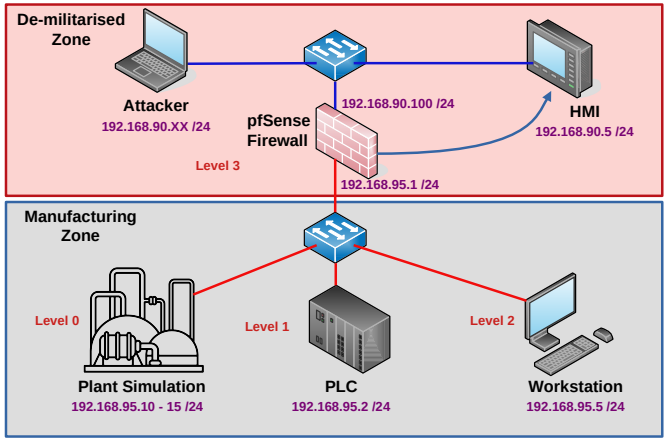
By the end of this topic, you will be able to:

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

Purdue Model



ICS Testbed

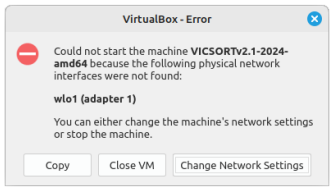


ICS Testbed

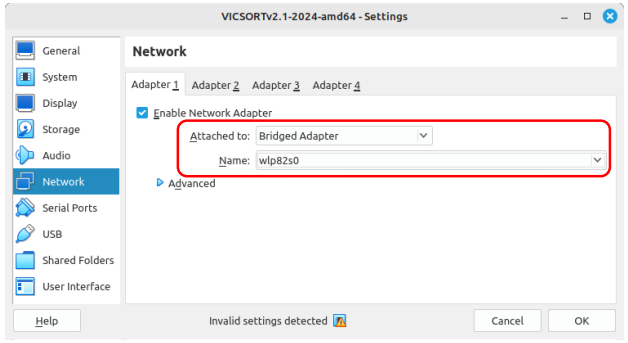
Node	IP Address Mapping
HMI	192.168.90.5 /24
Firewall	- WAN: 192.168.90.100 /24 - LAN: 192.168.95.100 /24
PLC	192.168.95.2 /24
Engineering Workstation	192.168.95.5 /24
Plant Simulation	192.168.95.10 - 15 /24
Attacker	192.168.90.XX /24

Firewall Username: admin	Password: pfsense
HMI Username: admin	Password: admin
Kali Username: kali	Password: kali

Network settings

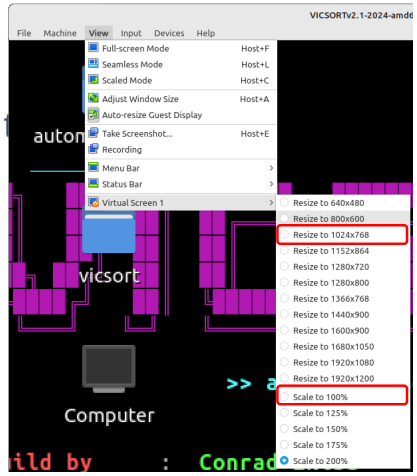


Show



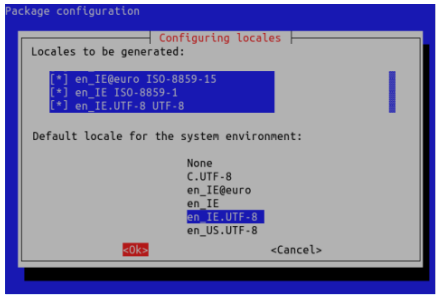
Pin QTerminal to the toolbar

- Open a terminal, LXQt icon >> QTerminal.
- Using the left mouse key, drag t



Generate preferred the locale

```
vicsort@vicsort:~$ sudo dpkg-reconfigure locales
```

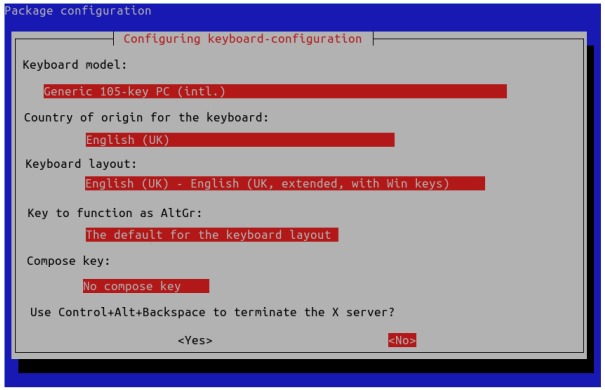



```
Generating locales (this might take a while)...
  en_IE.ISO-8859-1... done
  en_IE.UTF-8... done
  en_IE.ISO-8859-15@euro... done
  en_US.UTF-8... done
  en_US.UTF-8... done
Generation complete.
```

```
vicsort@vicsort:~$ sudo apt update && sudo apt upgrade
```

Configure keyboard layout

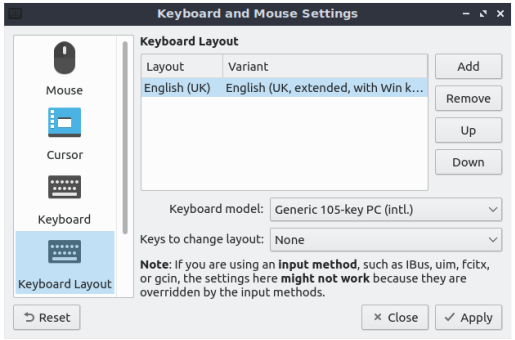
```
vicsort@vicsort:~$ sudo dpkg-reconfigure keyboard-configuration
```




```
vicsort@vicsort:~$ sudo apt reboot now
```


Configure keyboard layout for LXQt Desktop

Preferences >> LXQt Settings >> Keyboard and Mouse



The Domain Name System

Domain Name Service on the VM

```
vicsort@vicsort:~$ systemd-resolve --status |grep
"Current DNS Server"
  Current DNS Server: 89.34.154.5

vicsort@vicsort:~$ dig +short -x 89.34.154.5
limk1-dns02.ripple.net.

vicsort@vicsort:~$ sudo apt install fping

vicsort@vicsort:~$ fping www.google.com
www.google.com is alive
```

Running the VICSORT testbed

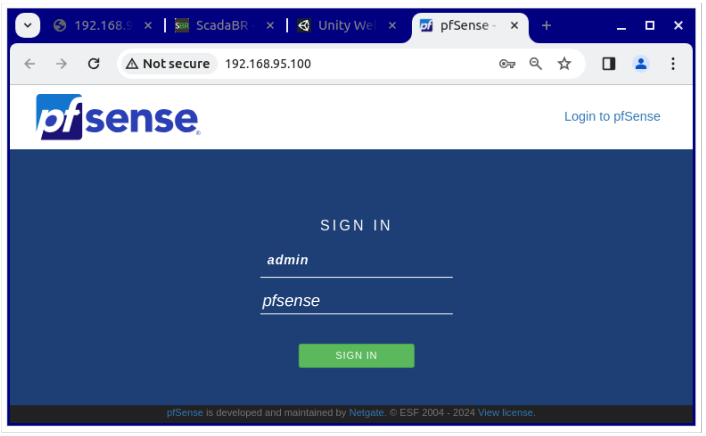
Start the VICSORT testbed

```
vicsort@vicsort:~$ testbed_startup

**** Testbed Ready to go ****

vicsort@vicsort:~$ lxc list
+----------------------+---------+----------------------+-----------+-----------+
|         NAME         |  STATE  |         IPV4         |   TYPE    | SNAPSHOTS |
+----------------------+---------+----------------------+-----------+-----------+
| attacker-container   | RUNNING | 192.168.90.197 (eth1) | CONTAINER | 0         |
+----------------------+---------+----------------------+-----------+-----------+
| hmi-container        | RUNNING | 192.168.90.5 (eth1)   | CONTAINER | 0         |
+----------------------+---------+----------------------+-----------+-----------+
| plc-container        | RUNNING | 192.168.95.2 (eth1)   | CONTAINER | 0         |
+----------------------+---------+----------------------+-----------+-----------+
| simulation-container | RUNNING | 192.168.95.15 (eth7)  | CONTAINER | 0         |
|                      |         | 192.168.95.14 (eth6)  |           |           |
|                      |         | 192.168.95.13 (eth5)  |           |           |
|                      |         | 192.168.95.12 (eth4)  |           |           |
|                      |         | 192.168.95.11 (eth3)  |           |           |
|                      |         | 192.168.95.10 (eth2)  |           |           |
+----------------------+---------+----------------------+-----------+-----------+
| workstation-container | RUNNING | 192.168.95.5 (eth1)  | CONTAINER | 0         |
+----------------------+---------+----------------------+-----------+-----------+
```

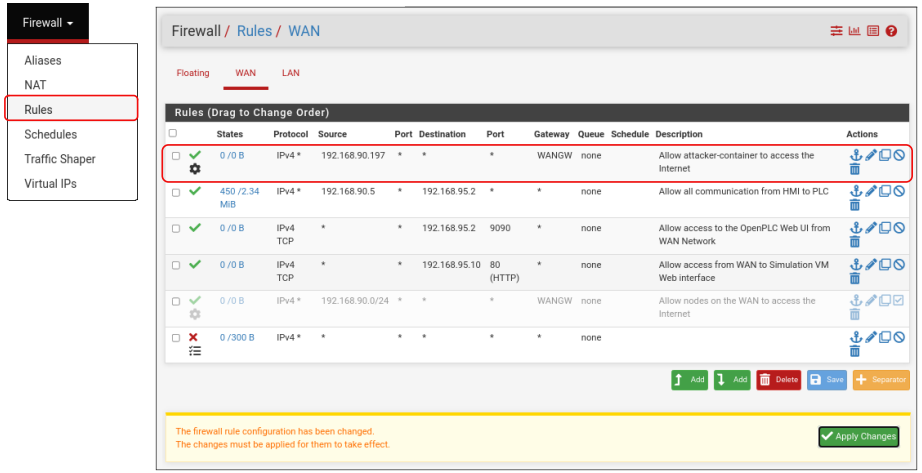

PfSense Firewall



Internet Access Rule

- **Action**: Pass
- **Interface**: WAN
- **Protocol**: Any
- **Source**: single host or alias: 192.168.90.197
- **Description**: Allow attacker-container to access the Internet
- **Advanced Options**:
  - **Gateway**: WANGW - 192.168.90.1 - WAN Gateway

PfSense Firewall Rule



DNS on the Attacker Container

```
vicsort@vicsort:~$ lxc exec attacker-container bash
┌──(root  attacker-container)-[~]
└─# cat /etc/resolv.conf | grep nameserver
nameserver 192.168.90.1

┌──(root  attacker-container)-[~]
└─# dig +short -x 192.168.90.1
_gateway.lxd.

┌──(root  attacker-container)-[~]
└─# fping www.google.com
www.google.com is alive
```


Kali Linux Archive GPG Key

```
┌──(root  attacker-container)-[~]
└─# cd /usr/share/keyrings


┌──(root  attacker-container)-[/usr/share/keyrings]
└─# curl https://archive.kali.org/archive-key.asc | gpg --dearmor >
archive-key.gpg
  % Total    % Received % Xferd  Average Speed   Time    Time
Time  Current
                                 Dload  Upload   Total   Spent
Left  Speed
100  3155  100  3155    0     0   7346      0 --:--:-- --:--:--
--:--:--  7354

┌──(root  attacker-container)-[/usr/share/keyrings]
└─# cp archive-key.gpg /etc/apt/trusted.gpg.d
```


Kali Linux Archive GPG Key

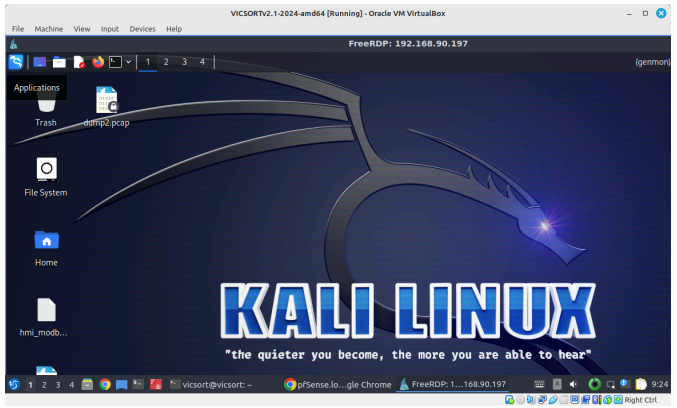
```
┌──(root  attacker-container)-[/usr/share/keyrings]
└─# file /etc/apt/trusted.gpg.d/archive-key.gpg
/etc/apt/trusted.gpg.d/archive-key.gpg: OpenPGP Public Key Version 4,
Created Mon Mar  5 14:56:40 2012, RSA (Encrypt or Sign, 4096 bits);
User ID; Signature; OpenPGP Certificate


┌──(root  attacker-container)-[~]
└─# apt update && apt upgrade -y
```

Reconnaissance

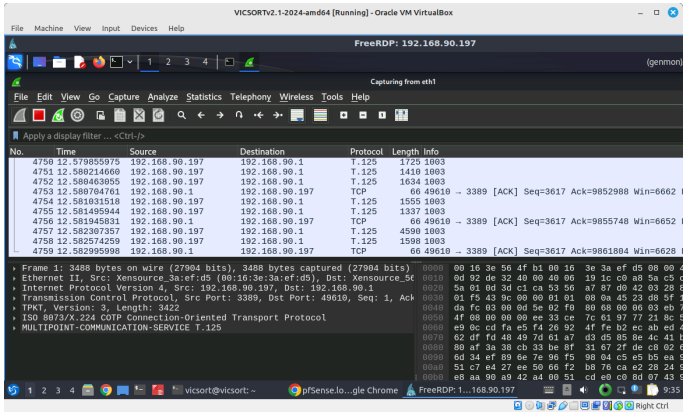
XRDP server on the attacher-container

```
vicsort@vicsort:~$ rdp_attacker
```



Wireshark

```
kali@attacker-container:~$ sudo wireshark
```



Tshark Network Protocol Analyser

```
┌──(root  attacker-container)-[~]
└─# tshark -D
Running as user "root" and group "root". This could be dangerous.
1. eth1
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. sshdump (SSH remote capture)
14. udpdump (UDP Listener remote capture)
```

Tshark Network Protocol Analyser

```
┌──(root  attacker-container)-[~]
└─# tshark -F pcap -V > /root/tshark_out.pcap
Running as user "root" and group "root". This could be
dangerous.
Capturing on 'eth1'
 ** (tshark:2274) 12:56:46.982335 [Main MESSAGE] -- Capture
started.
 ** (tshark:2274) 12:56:46.982394 [Main MESSAGE] -- File:
"/tmp/wireshark_eth1H1V7G2.pcapng"
```


Tshark Network Protocol Analyser

```
┌──(root  attacker-container)-[~]
└─# head -94 /root/tshark_out.pcap
Frame 1: 4875 bytes on wire (39000 bits), 4875 bytes captured (39000
bits) on interface eth1, id 0
    Interface id: 0 (eth1)
        Interface name: eth1
    Encapsulation type: Ethernet (1)
    Arrival Time: Jan  3, 2024 12:56:46.986995902 GMT
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1704286606.986995902 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 4875 bytes (39000 bits)
    Capture Length: 4875 bytes (39000 bits)
```


Netdiscover

```
┌──(root  attacker-container)-[~]
└─# netdiscover -i eth1 -r 192.168.90.0/24
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 126

 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.90.1    00:16:3e:56:4f:b1      1      42  Xensource, Inc.

 192.168.90.5    00:16:3e:63:0d:8b      1      42  Xensource, Inc.

 192.168.90.100  52:54:00:d7:8f:bd      1      42  Unknown vendor
```


P0f passive fingerprinting

- Run **p0f** as a daemon

```
┌──(root  attacker-container)-[~]
└─# apt install p0f

┌──(root  attacker-container)-[~]
└─# p0f -i eth1 -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 'eth1'.
[+] Default packet filtering configured [+VLAN].
[+] Log file '/root/p0f-output.txt' opened for writing.
[+] Daemon process created, PID 2882 (stderr not kept).

Good luck, you're on your own now!
```

P0f passive fingerprinting

```
┌──(root  attacker-container)-[~]
└─# ps -ef | grep p0f


root    2882     1  0 16:35 ?      00:00:00 p0f -i eth1 -d -o /root/p0f-output.txt
root    2891  1376  0 16:38 pts/1  00:00:00 grep --color=auto p0f

┌──(root  attacker-container)-[~]
└─# tail -f /root/p0f-output.txt
[2024/01/05 16:42:18] mod=syn|cli=192.168.90.197/52988|
srv=209.85.202.95/443|subj=cli|os=Linux 2.2.x-3.x|dist=0|
params=generic|
raw_sig=4:64+0:0:1460:mss*44,7:mss,sok,ts,nop,ws:df,id+:0
[2024/01/05 16:42:18] mod=mtu|cli=192.168.90.197/52988|
srv=209.85.202.95/443|subj=cli|link=Ethernet or modem|raw_mtu=1500
[2024/01/05 16:42:18] mod=syn+ack|cli=192.168.90.197/52988|
srv=209.85.202.95/443|subj=srv|os=???|dist=7|params=none|
```


P0f passive fingerprinting

- Terminate the **p0f** as a daemon

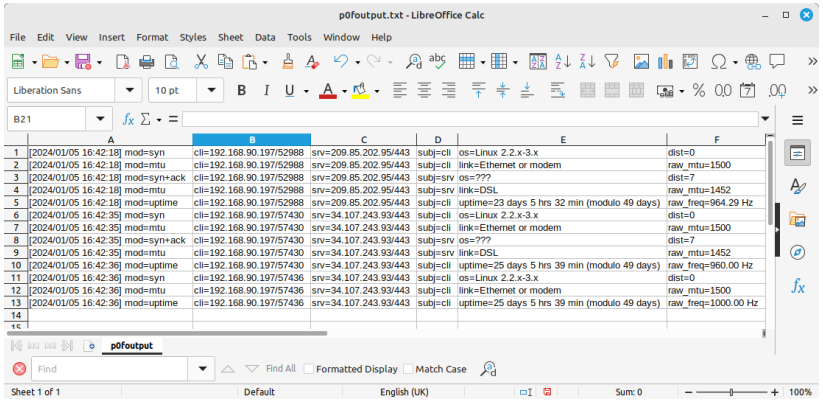
```
┌──(root  attacker-container)-[~]
└─# kill -SIGKILL 2882

┌──(root  attacker-container)-[~]
└─# ps -ef | grep p0f

┌──(root  attacker-container)-[~]
└─# ps -ef | grep p0f
root    3013  1376  0 16:50 pts/1  00:00:00 grep --color=auto p0f
```


P0f passive fingerprinting

- Output as a spreadsheet



	A	B	C	D	E	F
1	[2024/01/05 16:42:18] mod=syn	cli=192.168.90.197/52988	srv=209.85.202.95/443	subj=cli	os=Linux 2.2.x-3.x	dist=0
2	[2024/01/05 16:42:18] mod=mtu	cli=192.168.90.197/52988	srv=209.85.202.95/443	subj=cli	link=Ethernet or modem	raw_mtu=1500
3	[2024/01/05 16:42:18] mod=syn+ack	cli=192.168.90.197/52988	srv=209.85.202.95/443	subj=srv	os=???	dist=7
4	[2024/01/05 16:42:18] mod=mtu	cli=192.168.90.197/52988	srv=209.85.202.95/443	subj=srv	link=DSL	raw_mtu=1452
5	[2024/01/05 16:42:18] mod=uptime	cli=192.168.90.197/52988	srv=209.85.202.95/443	subj=cli	uptime=23 days 5 hrs 32 min (modulo 49 days)	raw_freq=964.29 Hz
6	[2024/01/05 16:42:35] mod=syn	cli=192.168.90.197/57430	srv=34.107.243.93/443	subj=cli	os=Linux 2.2.x-3.x	dist=0
7	[2024/01/05 16:42:35] mod=mtu	cli=192.168.90.197/57430	srv=34.107.243.93/443	subj=cli	link=Ethernet or modem	raw_mtu=1500
8	[2024/01/05 16:42:35] mod=syn+ack	cli=192.168.90.197/57430	srv=34.107.243.93/443	subj=srv	os=???	dist=7
9	[2024/01/05 16:42:35] mod=mtu	cli=192.168.90.197/57430	srv=34.107.243.93/443	subj=srv	link=DSL	raw_mtu=1452
10	[2024/01/05 16:42:36] mod=uptime	cli=192.168.90.197/57430	srv=34.107.243.93/443	subj=cli	uptime=25 days 5 hrs 39 min (modulo 49 days)	raw_freq=960.00 Hz
11	[2024/01/05 16:42:36] mod=syn	cli=192.168.90.197/57436	srv=34.107.243.93/443	subj=cli	os=Linux 2.2.x-3.x	dist=0
12	[2024/01/05 16:42:36] mod=mtu	cli=192.168.90.197/57436	srv=34.107.243.93/443	subj=cli	link=Ethernet or modem	raw_mtu=1500
13	[2024/01/05 16:42:36] mod=uptime	cli=192.168.90.197/57436	srv=34.107.243.93/443	subj=cli	uptime=25 days 5 hrs 39 min (modulo 49 days)	raw_freq=1000.00 Hz
14						
15						

Nmap for network exploration and security auditing

```
┌──(root  attacker-container)-[~]
└─# nmap -sn 192.168.90.0/24 --exclude 192.168.90.197
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-05 17:50 GMT
Nmap scan report for _gateway.lxd (192.168.90.1)
Host is up (0.000084s latency).
MAC Address: 00:16:3E:56:4F:B1 (Xensource)
Nmap scan report for hmi-container.lxd (192.168.90.5)
Host is up (0.000044s latency).
MAC Address: 00:16:3E:63:0D:8B (Xensource)
Nmap scan report for 192.168.90.100
Host is up (0.0017s latency).
MAC Address: 52:54:00:D7:8F:BD (QEMU virtual NIC)
Nmap done: 255 IP addresses (3 hosts up) scanned in 2.02 seconds
```

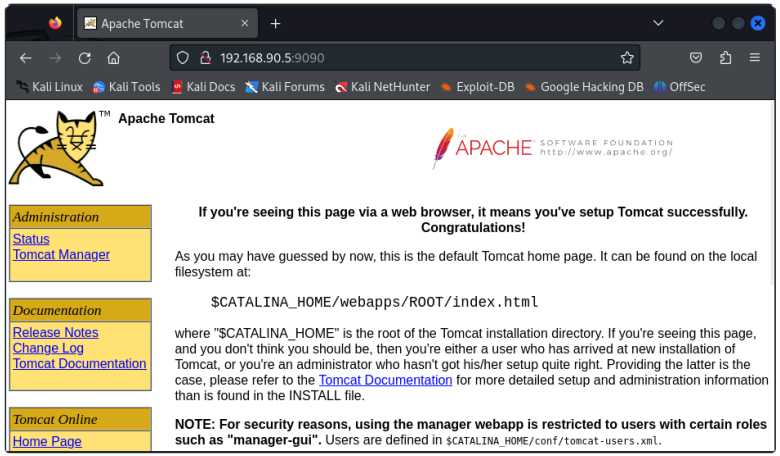
Nmap for network exploration and security auditing

```
┌──(root  attacker-container)-[~]
└─# nmap -v -sn 192.168.90.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-05 17:54 GMT
Initiating ARP Ping Scan at 17:54
Scanning 192.168.90.5 [1 port]
Completed ARP Ping Scan at 17:54, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:54
Completed Parallel DNS resolution of 1 host. at 17:54, 0.00s elapsed
Nmap scan report for hmi-container.lxd (192.168.90.5)
Host is up (0.000054s latency).
MAC Address: 00:16:3E:63:0D:8B (Xensource)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```


Nmap for network exploration and security auditing

```
┌──(root  attacker-container)-[~]
└─# nmap -A -T4 -p- 192.168.90.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-05 12:52 GMT
Nmap scan report for hmi-container.lxd (192.168.90.5)
Host is up (0.000093s latency).
Not shown: 65533 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
8009/tcp open  ajp13   Apache Jserv (Protocol v1.3)
| ajp-methods:
|   Supported methods: GET HEAD POST PUT DELETE OPTIONS
|   Potentially risky methods: PUT DELETE
|_  See https://nmap.org/nsedoc/scripts/ajp-methods.html
9090/tcp open  http    Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat
|_http-favicon: Apache Tomcat
```


Apache Tomcat



Nikto

- Shell utility to scan web servers for known vulnerabilities
- Update Nikto

```
┌──(root  attacker-container)-[~]
└─# apt purge nikto

┌──(root  attacker-container)-[~]
└─# apt install nikto
```

Running Nikto

```
┌──(root  attacker-container)-[~]
└─# nikto -host 192.168.90.5 -port 9090
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          192.168.90.5
+ Target Hostname:    192.168.90.5
+ Target Port:        9090
+ Start Time:         2024-03-19 19:06:46 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache-Coyote/1.1
+ /: The anti-clickjacking X-Frame-Options header is not present. See:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the
site in a different fashion to the MIME type. See:
https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /favicon.ico: identifies this app/server as: Apache Tomcat (possibly 5.5.26 through 8.0.15), Alfresco
Community. See: https://en.wikipedia.org/wiki/Favicon
+ Multiple index files found: /index.jsp, /index.html.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, PUT, DELETE, OPTIONS .
+ HTTP method ('Allow' Header): 'PUT' method could allow clients to save files on the web server.
+ HTTP method ('Allow' Header): 'DELETE' may allow clients to remove files on the web server.
+ /: Appears to be a default Apache Tomcat install.
+ /examples/servlets/index.html: Apache Tomcat default JSP pages present.
.....
```


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

- Install, initialise a postgresql DB and run the framework

```
┌──(root  attacker-container)-[~]
└─# apt update; apt install metasploit-framework

┌──(root  attacker-container)-[~]
└─# msfdb init

┌──(root  attacker-container)-[~]
└─# msfconsole

Would you like to use and setup a new database (recommended)? Yes

Would you like to init the webservice? (Not Required) [no]: no
```

Ensure the postgresql database is running

- Check the database is now running

```
┌──(root  attacker-container)-[~]
└─# msfdb status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/usr/lib/systemd/system/postgresql.service; enabled; preset: disabled)
    Drop-In: /run/systemd/system/service.d
             └─zzz-lxc-service.conf
     Active: active (exited) since Sun 2024-04-21 22:05:49 IST; 1min 3s ago
    Process: 2484 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 2484 (code=exited, status=0/SUCCESS)

Apr 21 22:05:49 attacker-container systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Apr 21 22:05:49 attacker-container systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

COMMAND   PID     USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
postgres 2447 postgres    5u  IPv6 121586      0t0  TCP localhost:5432 (LISTEN)
postgres 2447 postgres    6u  IPv4 121587      0t0  TCP localhost:5432 (LISTEN)

UID          PID    PPID  C STIME TTY      STAT   TIME CMD
postgres    2447       1  0 22:05 ?        Ss     0:00 /usr/lib/postgresql/14/bin/postgres -D /var/li

[+] Detected configuration file (/usr/share/metasploit-framework/config/database.yml)
```


Metasploit Console

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

       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

[*] Starting persistent handler(s)…

msf6 >
```


Metasploit Console

```
msf6 > nmap -Pn -sS -A -oX netscan 192.168.90.0/24 --exclude 192.168.90.197
[*] exec: nmap -Pn -sS -A -oX netscan 192.168.90.0/24 --exclude 192.168.90.197

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-28 11:01 GMT
Nmap scan report for 192.168.90.1
Host is up (0.00012s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
22/tcp   open  ssh           OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   3072 00:ea:24:9b:d9:e1:47:42:af:1b:60:2f:f2:26:f1:3e (RSA)
|   256 91:24:20:29:d9:04:0a:90:51:e2:fe:90:07:cb:e0:18 (ECDSA)
|_  256 63:6f:76:b5:66:3f:e3:b7:0d:15:87:ab:a8:03:a9:6f (ED25519)
53/tcp   open  domain        dnsmasq 2.80
| dns-nsid:
|_  bind.version: dnsmasq-2.80
3389/tcp open  ms-wbt-server xrdp
MAC Address: 00:16:3E:56:4F:B1 (Xensource)
```


Metasploit Console

```
msf6 > db_import netscan
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.10'
[*] Importing host 192.168.90.1
[*] Importing host 192.168.90.5
[*] Importing host 192.168.90.100
[*] Successfully imported /root/netscan

msf6 > hosts

Hosts
=====

address         mac                name          os_name  os_flavor  os_sp  purpose
-------         ---                ----          -------  ---------  -----  -------
66.96.161.141                                    Unknown                    device
192.168.90.1    00:16:3e:56:4f:b1                Linux               4.X    server
192.168.90.5    00:16:3e:63:0d:8b  192.168.90.5  Linux               4.X    server
192.168.90.100  52:54:00:d7:8f:bd                FreeBSD             11.X   device
192.168.95.2                                     Unknown                    device
```

Metasploit Console

```
msf6 > hosts -o /root/scanned_hosts.csv
[*] Wrote hosts to /root/scanned_hosts.csv

msf6 > exit

┌──(root  attacker-container)-[~]
└─# cat scanned_hosts.csv
address,mac,name,os_name,os_flavor,os_sp,purpose,info,comments
"66.96.161.141","","","Unknown","","","device","",""
"192.168.90.1","00:16:3e:56:4f:b1","","Linux","","4.X","server","",""
"192.168.90.5","00:16:3e:63:0d:8b","192.168.90.5","Linux","","4.X","server","",""
"192.168.90.100","52:54:00:d7:8f:bd","","FreeBSD","","11.X","device","",""
"192.168.95.2","","","Unknown","","","device","",""
```


Metasploit Console

```
msf6 > services
Services
========

host            port  proto  name           state  info
----            ----  -----  ----           -----  ----
66.96.161.141   80    tcp    http           open
192.168.90.1    22    tcp    ssh            open   OpenSSH 8.2p1 4ubuntu0.11 Linux; 2.0
192.168.90.1    53    tcp    domain         open   dnsmasq 2.80
192.168.90.1    3389  tcp    ms-wbt-server  open   xrdp
192.168.90.5    8009  tcp    ajp13          open   Apache Jserv Protocol v1.3
192.168.90.5    9090  tcp    http           open   Apache Tomcat/Coyote JSP engine 1.1
192.168.90.100  22    tcp    ssh            open   OpenSSH 7.9 protocol 2.0
192.168.90.100  53    tcp    domain         open   generic dns response: REFUSED
192.168.90.100  80    tcp    http           open   nginx
192.168.95.2    22    tcp                   open
192.168.95.2    502   tcp                   open
192.168.95.2    8080  tcp                   open
```


Metasploit Console

```
msf6 > hosts -o /root/scanned_services.csv
[*] Wrote hosts to /root/scanned_services.csv

msf6 > cat scanned_services.csv
host,port,proto,name,state,info
"66.96.161.141","80","tcp","http","open",""
"192.168.90.1","22","tcp","ssh","open","OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 Ubuntu
Linux; protocol 2.0"
"192.168.90.1","53","tcp","domain","open","dnsmasq 2.80"
"192.168.90.1","3389","tcp","ms-wbt-server","open","xrdp"
"192.168.90.5","80","tcp","http","open",""
"192.168.90.5","8009","tcp","ajp13","open","Apache Jserv Protocol v1.3"
"192.168.90.5","9090","tcp","http","open","Apache Tomcat/Coyote JSP engine 1.1"
"192.168.90.100","22","tcp","ssh","open","OpenSSH 7.9 protocol 2.0"
"192.168.90.100","53","tcp","domain","open","generic dns response: REFUSED"
"192.168.90.100","80","tcp","http","open","nginx"
"192.168.95.2","22","tcp","","open",""
"192.168.95.2","502","tcp","","open",""
"192.168.95.2","8080","tcp","","open",""
```


Metasploit Module

```
msf6 > 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
```

Metasploit Module

```
msf6 > use 6
msf6 auxiliary(scanner/portscan/syn) >

msf6 > show options

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

Name       Current Setting  Required  Description
----       ---------------  --------  -----------
BATCHSIZE  256              yes       The number of hosts to scan per set
DELAY      0                yes       The delay between connections, per thread, in ms
INTERFACE                   no        The name of the interface
JITTER     0                yes       The delay jitter factor (max value by which to +/- DELAY) in ms.
PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-
metasploit/basics/using-metasploit.html
SNAPLEN    65535            yes       The number of bytes to capture
THREADS    1                yes       The number of concurrent threads (max one per host)
TIMEOUT    500              yes       The reply read timeout in ms


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


Metasploit Module

```
msf6 auxiliary(scanner/portscan/syn) > set threads 50
threads => 50
msf6 auxiliary(scanner/portscan/syn) > set rhosts 192.168.90.5
rhosts => 192.168.90.5
msf6 auxiliary(scanner/portscan/syn) > set ports 80,9090
Ports => 80,9090


msf6 auxiliary(scanner/portscan/syn) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```


Metasploit Module TCP Scan

```
msf6 auxiliary(scanner/portscan/syn) > use 5
msf6 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 +/- DELAY)
in ms.
PORTS        1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
RHOSTS                        yes       The target host(s), see
https://docs.metasploit.com/docs/using-metasploit/basics/usi
                                           ng-metasploit.html
THREADS      1                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.
```


Metasploit Module TCP Scan

```
msf6 auxiliary(scanner/portscan/tcp) > set threads 10
threads => 10

msf6 auxiliary(scanner/portscan/tcp) > set rhosts 192.168.90.5
rhosts => 192.168.90.5

msf6 auxiliary(scanner/portscan/tcp) > set ports 9090
ports => 9090

msf6 auxiliary(scanner/portscan/tcp) > run
[+] 192.168.90.5:         - 192.168.90.5:9090 - TCP OPEN
[*] 192.168.90.5:         - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Learning objectives

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

TUS
Ollscoil Teicneolaíochta na Sionainne: Lár Tíre, An Iarthar Láir
Technological University of the Shannon: Midlands Midwest

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir Sinsearach

E diarmuid.obriain@tus.ie | W tus.ie
Campas Maoilis, Páirc Maoilis,
Luimneach, V94 EC5T, Éire

CISSP®

Thank you

TUS