

# Proactive Defence & Offensive Reconnaissance

Dr Diarmuid Ó Briain

8 Nov 2026

DEPARTMENT OF ELECTRONIC ENGINEERING & COMMUNICATIONS
SOUTH EAST TECHNOLOGICAL UNIVERSITY

setu.ie
INSPIRING FUTURES

Version: 1.0

## Licence

This work is licenced under a Creative Commons Attribution-ShareAlike 4.0 International Licence.
Full Licence: http://creativecommons.org/licenses/by-sa/4.0



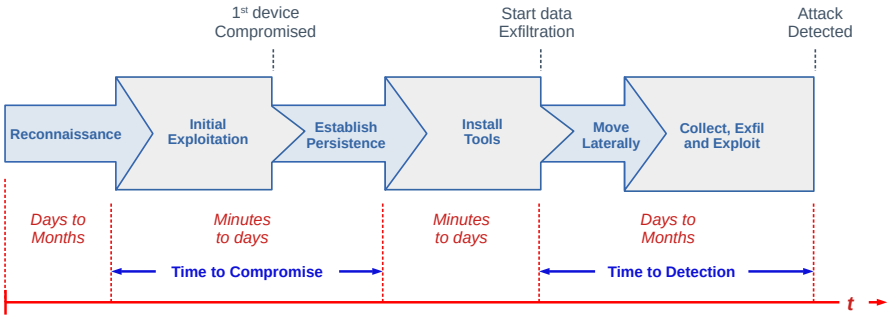
## Learning objectives

- At the end of this topic you will be able to:
  - Map an organisation's attack surface by leveraging Shodan for passive asset discovery and configuring Nmap for precise target specification and host discovery.
  - Formulate advanced Nmap scanning strategies that optimise performance, utilise XML output, and implement Firewall/IDS evasion techniques while diagnosing issues via NSE debugging.
  - Evaluate the risks of scanning IACS and safely execute non-disruptive, IACS-specific NSE scripts to prevent industrial downtime.
  - Design and deploy honeypots and network canaries within an architecture to detect early-stage reconnaissance and alert security operations before a breach escalates.



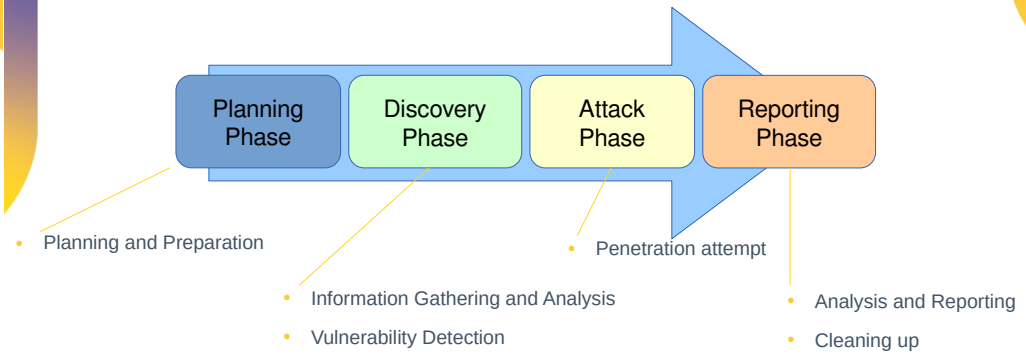
# Open-Source Intelligence & Passive Reconnaissance

## Anatomy of a Cyber attack






## What steps are used to carry out pen test






## Planning and Preparation

- **Kick-off meeting**
  - Clear objective for pen-test
  - Timing and duration allowed for the pen-tests
  - Personnel involved
  - Are staff being informed of the tests?
  - Network and Computers involved
  - Operational requirements during the pen-test
  - How the results are to be presented at the conclusion of the test.



## Planning and Preparation

- **Penetration Test Plan**
  - Detailed plan
  - Confidentiality Statement
  - Acceptance Sign-off Sheet

## Information gathering and analysis

- Gathering of as much information as possible as a reconnaissance is essential.
  - What does the network look like?
  - What devices are on the network?
  - Who works at the company?
  - What does the organogram of the company look like?



## Vulnerability detection

- Once a picture of the target organisation has been compiled a scan of vulnerabilities is the next step.



## Penetration attempt

- Identifying the best targets from the machines showing vulnerability is important particularly if the time given is short.
- IT personnel nomenclature to use functional names like MAILSVR or FTPSERVER etc…
- Define the list of machines that are to be given special additional treatment.
- Try password cracking tools, dictionary, brute force and hybrid attacks.



## Analysis and Reporting

- A detailed report must be furnished to the client at the conclusion of the tests. It should include:
  - A summary of successful penetration tests.
  - A list of all information gathered during the pen-test.
  - A complete list and description of vulnerabilities found.
  - A suggested list of next steps to close the vulnerabilities and increase security at the client company.

## Tidy up

- During the pen-testing a detailed list of steps taken should be maintained.
- Pen-testers work with the client staff ensure that the steps have not left any residual issues
  - entries in configuration files
  - new users
  - groups
  - etc...



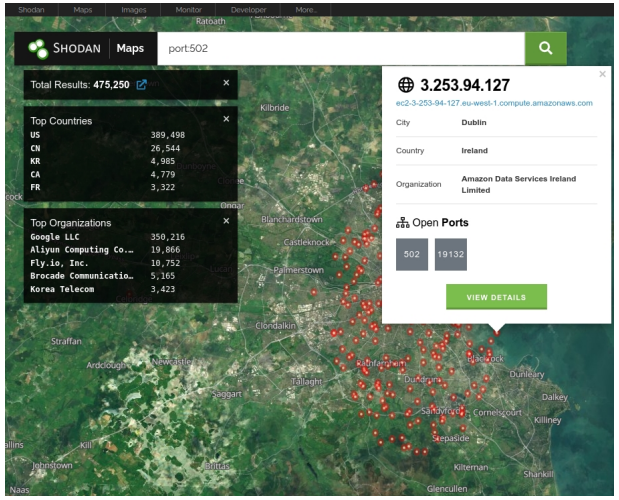
SETU Ollscoil Teicneolaíochta an Oirdheiscirt South East Technological University

# SHODAN



## Shodan

https://www.shodan.io






## Shodan

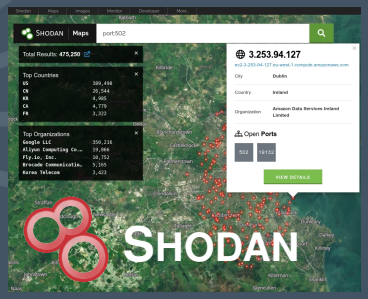
- Search engine that finds devices connected to the Internet
- Scans the Internet for devices that respond to ICMP ping requests
- Collects information, and indexes the banners that devices send out
- Used to find a wide variety of devices, including:
  - Switches
  - Routers
  - Webcams
  - Security cameras
  - ACS
  - HVAC
  - Smart TVs
  - Refrigerators

## Shodan

- Valuable tool for security researchers, as it can help them to discover new vulnerabilities and to track the deployment of malware
- It is not a hacking tool, it is a search engine that helps people to find devices connected to the Internet
- Here are some examples of how Shodan can be used:
  - Find all of the Modbus devices that are publicly accessible on the Internet
  - Find all of the routers that are using a specific firmware with a known vulnerability
  - Identify all of the devices on a network that are exposed to the Internet to mitigate security risks



# Exercise






## Exercise

- Create a personal Shodan account.
- Login to Shodan.
- Discover the TCP port number for the DNP3 protocol.
- Search for DNP3 in Ireland and copy down the information relating to the nearest one to your current location.
  - Who owns it?
  - What is the device?
  - What is the device Internet Protocol (IP) Address?






# Network Mapper Deep Dive

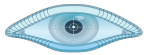


## Network Mapper (nmap)

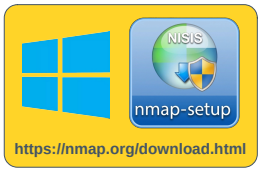
- Open source network exploration and security auditing tool
- Designed to rapidly scan large networks
- Uses raw IP packets in novel ways to determine:
  - What hosts are available on the network
  - What services (application name and version) those hosts are offering
  - What operating systems (and OS versions) they are running
  - What type of packet filters/firewalls are in use
  - … and many more functions
- **nmap** is commonly used for security audits as well as routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.



## Installing nmap



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install nmap nmapsi4
```



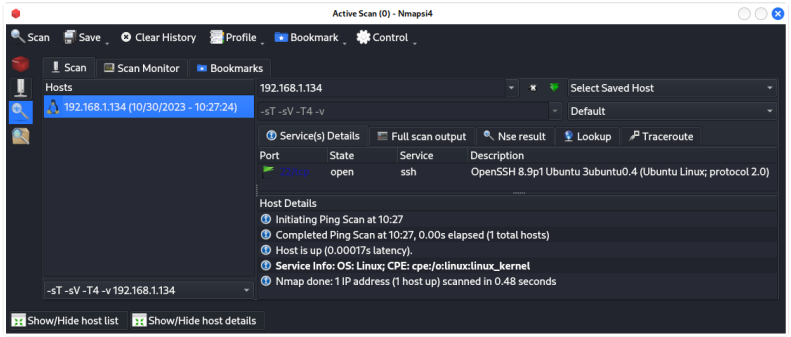

```
┌──(kali㉿kali)-[~]
└─$ nmap --version
Nmap version 7.80 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.3 openssl-1.1.1d nmap-libssh2-1.8.2
libz-1.2.11 libpcre-8.39 libpcap-1.9.1 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
```



## nmapsi4

- **nmapsi4** graphical utility

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install -y nmapsi4
```






## nmap states

- **Open**
  - Application is actively accepting TCP connections, UDP datagrams or SCTP associations on this port
- **Closed**
  - Port is accessible, but there is no application listening on it.
- **Filtered**
  - Cannot determine whether the port is open because packet filtering prevents its probes from reaching the port.
- **Unfiltered**
  - Port is accessible, but unable to determine whether it is open or closed.
- **Open | filtered**
  - Unable to determine whether a port is open or filtered.
- **Closed | filtered**
  - Unable to determine whether a port is closed or filtered.

# Exercise






## Basic scan

```
┌──(kali㉿kali)-[~]
└─$ nmap scanme.nmap.org
```

- **Response:**

- **Why that response?**



## Basic scan

```
┌──(kali㉿kali)-[~]
└─$ nmap scanme.nmap.org
```

- Without **sudo**
  - TCP Connect scan (-sT option)
  - Leverage the operating system's standard Berkeley Sockets API.
  - OS handles the connection states
  - Forces computer to complete the full standard three-way handshake every single time.
- With **sudo**
  - Nmap defaults to a TCP SYN scan. (-sS option)
  - Nmap creates custom, half-open packets and inject them directly onto the network card.
  - Creating these raw network packets requires direct hardware access, which operating systems strictly limit to administrative accounts to prevent security abuse.
  - Possible to tear a connection down before the three-way handshake completes.



## Silent Probes (TCP SYN Scan)

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS -p 22,80,9929 scanme.nmap.org
```

- **Response:**

- **Why that response?**

## Silent Probes (TCP SYN Scan)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 22,80,9929 scanme.nmap.org
```

- Response:

- Why that response?



## Silent Probes (TCP SYN Scan)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -p 22,80,9929 scanme.nmap.org
```

- What are the -sS and -p flags? How do they impact?

```
┌──(kali㉿kali)-[~]
└─$ nmap --help | grep -e 'sS'
```

```
┌──(kali㉿kali)-[~]
└─$ nmap --help | grep -e '-p '
```



## Aggressive Service Fingerprinting

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV --version-intensity 5 -p 80 scanme.nmap.org
```

- Response:

- Why is no sudo required?
- Why that response?



## OS Guessing and Timing Control

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -T4 scanme.nmap.org
```

- Response:

- Determine what the flags -O and -T4 are for?

## Generating the XML Evidence Dump

```
┌──(kali㉿kali)-[~]
└─$ nmap -sT -F -oX live_audit_report.xml scanme.nmap.org
```

- **Response:**

- **Determine what the flags -F and -oX are for?**



## Generating the XML Evidence Dump

```
┌──(kali㉿kali)-[~]
└─$ more live_audit_report.xml
```

- **Response:**

- **Can you find the exact lines that reflect the `open` or `filtered` port states?**



## Extract Questions

- What happens if you run an aggressive version scan (-sV) with a slow timing profile (-T1 or -T2)?

- Why did the TCP Connect scan (-sT) not require sudo privileges?



# Anonymous use of



nmap

## Anonymous use of nmap

- For anonymous use of nmap it is possible to do so using “The Onion Router” (TOR) and ProxyChains.
- ProxyChains redirects TCP connections through proxy servers.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install tor proxychains4
```

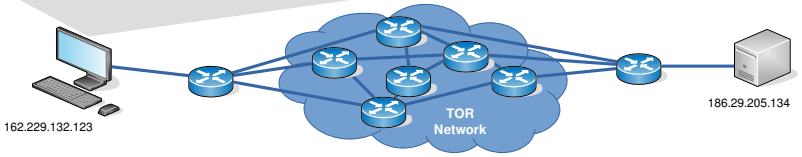


## Anonymous use of nmap

```
┌──(kali㉿kali)-[~]
└─$ proxychains4 nmap -Pn -sT -p 22,80 186.29.205.134
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-11-08 11:00 GMT
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  186.29.205.134:80-<><>-OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  186.29.205.134:80-<><>-OK
Nmap scan report for dynamic-186-29-205-134.dynamic.etb.net.co (186.29.205.134)
Host is up (15s latency).

PORT   STATE  SERVICE
22/tcp closed ssh
80/tcp closed http
```

**-sT**:
TCP connect scan via the OS own Berkeley Socket API.

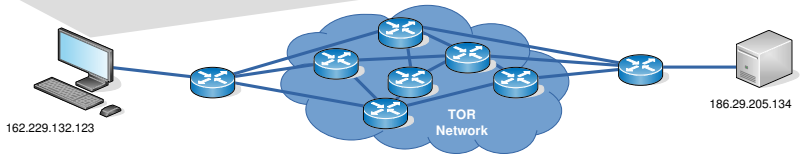





## Anonymous use of nmap

```
┌──(kali㉿kali)-[~]
└─$ proxychains4 nmap -Pn -sV -sT -p 22,80 186.29.205.134
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
Starting Nmap 7.94SVN ( https://nmap.org ) at 2026-11-08 11:00 GMT
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  186.29.205.134:80-<><>-OK
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  186.29.205.134:80-<><>-OK
Nmap scan report for li489-237.members.linode.com (186.29.205.134)
Host is up (0.71s latency).
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.22 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

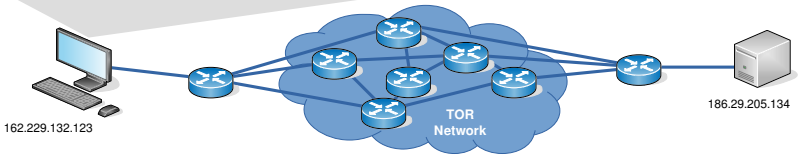
**-sV**:
Enable version detection.
It can be used to help differentiate the truly open ports from the filtered ones.





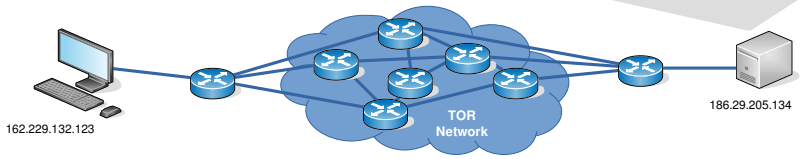

## Anonymous use of nmap

```
┌──(kali㉿kali)-[~]
└─$ proxychains4 ssh root@186.29.205.134
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  186.29.205.134:22
root@186.29.205.134's password:
Permission denied, please try again.
root@186.29.205.134's password:
Permission denied, please try again.
root@186.29.205.134's password:
Permission denied (publickey,password).
```



## Anonymous use of nmap

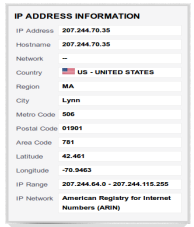
```
root@server:~# tail /var/log/auth.log
Nov  4 19:09:26 www sshd[1146]: Failed password for root from 207.244.70.35 port
45909 ssh2
Nov  4 19:09:33 www sshd[1146]: Failed password for root from 207.244.70.35 port
45909 ssh2
Nov  4 19:09:40 www sshd[1146]: Failed password for root from 207.244.70.35 port
45909 ssh2
Nov  4 19:09:40 www sshd[1146]: Connection closed by 207.244.70.35 [preauth]
Nov  4 19:09:40 www sshd[1146]: PAM 2 more authentication failures; logname= uid=0
euid=0 tty=ssh ruser= rhost=207.244.70.35  user=root
```

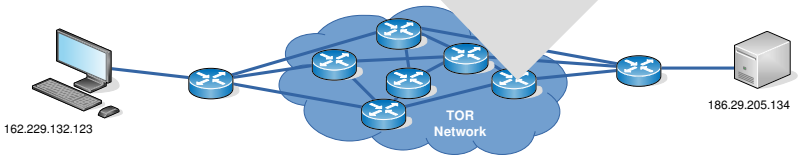





## Anonymous use of nmap

- whois: 207.244.70.35
- Edge of the TOR network






## Public key, possible IDentifier

- Public key possible Identifier if traffic is being monitored in TOR.
- Generate new key for use over TOR.

```
┌──(kali㉿kali)-[~]
└─$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/ada/.ssh/id_rsa): id_rsa_ANONY
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_rsa_ANONY.
Your public key has been saved in id_rsa_ANONY.pub.
The key fingerprint is:
bc:34:b1:23:fd:5a:f2:4b:d9:88:af:70:f7:d6:39:a2
The key's randomart image is:
+--[ RSA 2048]----+
|         .       |
|        o o      |
|       . S       |
|        o * +    |
|       . = B .. . |
|        o O .o +  |
|         o.E+.. . |
+-----------------+
```



## Anonymous use of nmap

```
┌──(kali㉿kali)-[~]
└─$  proxychains4 ssh -i /home/ada/.ssh/id_rsa_ANONY root@186.29.205.134

[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] Strict chain  ...  127.0.0.1:9050  ...  186.29.205.134:22
root@176.58.111.237's password: BADPASS
Permission denied, please try again.
root@176.58.111.237's password: GOODPASS
Linux www 4.1.5-x86_64-linode61 #7 SMP Mon Aug 24 13:46:31 EDT 2015 x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Mon Nov  9 03:20:34 2015 from 160.242.131.178
```

## Anonymous use of nmap

```
root@ece:~# tail /var/log/auth.log
Nov 10 09:46:10 ece sshd[21706]: Failed password for root from 43.229.53.25 port 11978 ssh2
Nov 10 09:46:12 ece sshd[21706]: Failed password for root from 43.229.53.25 port 11978 ssh2
Nov 10 09:46:12 ece sshd[21706]: Received disconnect from 43.229.53.25: 11:  [preauth]
Nov 10 09:46:12 ece sshd[21706]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh
ruser= rhost=43.229.53.25  user=root
```

**IP ADDRESS INFORMATION**

| | |
|---|---|
| IP Address | 43.229.53.25 |
| Hostname | 43.229.53.25 |
| Network | Asia Pacific Network Information Centre |
| Country | JP - JAPAN |
| Latitude | 36 |
| Longitude | 138 |
| IP Range | 43.0.0.0 - 43.233.35.255 |
| IP Network | American Registry for Internet Numbers (ARIN) |

**IP ADDRESS INFORMATION**

| | |
|---|---|
| IP Address | 81.7.15.115 |
| Hostname | 81-7-15-115.blue.kundencontroller.de |
| Network | RIPE Network Coordination Centre |
| Country | DE - GERMANY |
| Latitude | 51 |
| Longitude | 9 |
| IP Range | 81.7.0.0 - 81.7.63.255 |
| IP Network | American Registry for Internet Numbers (ARIN) |





# Nmap Scripting Engine (NSE)



## Nmap Scripting Engine (NSE)

- Powerful and flexible feature of **nmap**.
- Users can write simple scripts, using the Lua programming language, to automate a wide variety of networking tasks.
- Efficiency and speed are gained as these scripts are executed in parallel.

```
┌──(kali㉿kali)-[~]
└─$ ls /usr/share/nmap/scripts | grep .nse | wc -l
598
```



## NSE Scripts

| Switch | Example | Description |
|---|---|---|
| -sC | nmap 192.168.1.1 -sC | Scan with default NSE scripts. Considered useful for discovery and safe |
| --script default | nmap 192.168.1.1 --script default | Scan with default NSE scripts. Considered useful for discovery and safe |
| --script | nmap 192.168.1.1 --script=banner | Scan with a single script. Example banner |
| --script | nmap 192.168.1.1 --script=http* | Scan with a wildcard. Example http |
| --script | nmap 192.168.1.1 --script=http,banner | Scan with two scripts. Example http and banner |
| --script | nmap 192.168.1.1 --script "not intrusive" | Scan default, but remove intrusive scripts |
| --script-args | nmap --script snmp-sysdescr --script-args snmpcommunity=admin 192.168.1.1 | NSE script with arguments |

# Operational Technology & Legacy Scanning



## Legacy Systems

- The Problem with Scanning Legacy Devices
  - Device freezing
  - Permanent malfunction (bricking)
- The absence of sufficient security mechanisms and the utilisation of outdated software significantly contribute to these issues, especially when the system receives an NMAP-TCP packet
- Legacy ACS are primarily engineered for real-time functionality, lacking inherent security features.
- Even as minimal as an NMAP scan, carries potentially severe consequences



## Scanning ACS in a Penetration Test

- Never scan a live system
- Tailor the scans aggressiveness and mitigate risks
  - Scan Option: Timing **`-Tx`**
- Specify a TCP connect scan, which is generally safer than other scan types
  - Scan Option: Full TCP handshake **`-sT`**
- Limit parallel operations to one at a time
  - Scan Option: **`--max-parallelism 1`**



## ACS Specific scripts for NSE

- NSE Redpoint repository

```
┌──(kali㉿kali)-[~]
└─$ cd /usr/share/nmap/scripts

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo git clone https://github.com/digitalbond/Redpoint.git
Cloning into 'Redpoint'...
remote: Enumerating objects: 343, done.
remote: Total 343 (delta 0), reused 0 (delta 0), pack-reused 343
Receiving objects: 100% (343/343), 191.10 KiB | 1.59 MiB/s, done.
Resolving deltas: 100% (194/194), done.

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls Redpoint/
atg-info.nse   dnp3-info.nse   modicon-info.nse    proconos-info.nse
BACnet-discover-enumerate.nse  enip-enumerate.nse  omrontcp-info.nse  README.md  codesys-
v2-discover.nse   fox-info.nse  omronudp-info.nse  s7-enumerate.nse  cspv4-info.nse
LICENSE       pcworx-info.nse
```

## ACS Specific scripts for NSE

- NSE Redpoint repository

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ sudo nmap -p 502 --script Redpoint/modicon-info.nse -sV 192.168.1.134
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-30 11:21 EDT
NSE: DEPRECATION WARNING: bin.lua is deprecated. Please use Lua 5.3 string.pack
Nmap scan report for riomhaire-OB (192.168.1.134)
Host is up (0.00050s latency).

PORT    STATE SERVICE VERSION
502/tcp open  mbap?

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 135.69 seconds
```



# Active Defence & Deception



## Monitoring – IDS tools

- **Honey Pot**
  - A trap set to detect, deflect, or in some manner counteract attempts at unauthorised use of information systems
  - **Enticement**
    - A Honey Pot placed with open security vulnerabilities and services with known exploits is enticement
    - Perpetrator makes their own decision to perform the exploit.
  - **Entrapment**
    - If the honey pot actively solicits subjects to access it and then the owner charges them with unauthorised intrusion
    - Typically llegal.



## Vulnerability scanner

- Search for and map systems for weaknesses
  1) Look for active IP addresses, open ports, OS's and any applications running
  2) Create a report or move to the next step
  3) Attempt to determine the patch level of the OS or applications.
     - Can cause an exploit such as crash the OS or application
  4) Attempt to exploit the vulnerability.
- Scanners may either be malicious or friendly. Friendly scanners usually stop at step 2 and occasionally step 3 but never go to step 4.

## Vulnerability scanner types

- **Port Scanner**
  - NMAP.
- **Network Scanner**
  - OpenVAS, Metasploit.
- **Web Application Security Scanner**
  - OWASP Zed Attack Proxy (ZAP).
- **Computer worm**
  - Self-replicating computer program that replicates itself to other nodes
  - Unlike a virus, it does not need to attach itself to an existing program
  - Worms almost always cause at least some harm to the network, if only by consuming bandwidth, whereas viruses almost always corrupt or devour files on a targeted computer.



## Penetration testing

- Penetration testing is a method of evaluating security by simulating an attack, (Black Hat Hacker, or Cracker)
  - Active analysis of the system
  - Analysis from the position of a potential attacker
  - Active exploitation of security vulnerabilities.
- Security issues found are presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution
- Penetration testing determines the feasibility of an attack and the business impact of a successful exploit
- It is a component of a full security audit.



## Padded cell

- A padded cell is like a honey pot but is used for intruder isolation.
- When the IDS detects an intruder he/she is transferred to the padded cell.
- The padded cell has the look of an actual system but with fake programs and data, a simulated environment of sorts.



# Exercise



## Evasion Techniques and Intrusion Detection Systems

**A penetration tester is tasked with mapping an external attack surface without alerting the client's automated IDS. Which option outlines a legitimate evasion strategy supported by Nmap?**

A) Sending tiny fragmented IP packets (-f) paired with polite timing templates to slow down probe delivery.

B) Programmatically altering the Nmap source code to force a mandatory step 4 vulnerability exploit.

C) Wrapping the payload within a self-replicating computer worm to bypass packet filtering rules entirely.

D) Forcing all outbound scan packets to utilise an unallocated, non-RFC-compliant IPv6 destination block.



## Evasion Techniques and Intrusion Detection Systems

**A penetration tester is tasked with mapping an external attack surface without alerting the client's automated IDS. Which option outlines a legitimate evasion strategy supported by Nmap?**

A) **Sending tiny fragmented IP packets (-f) paired with polite timing templates to slow down probe delivery.** ✓

B) Programmatically altering the Nmap source code to force a mandatory step 4 vulnerability exploit.

C) Wrapping the payload within a self-replicating computer worm to bypass packet filtering rules entirely.

D) Forcing all outbound scan packets to utilise an unallocated, non-RFC-compliant IPv6 destination block.

INSPIRING FUTURES


## Friendly Vulnerability Scanners

**During a security audit, an administrator deploys a friendly vulnerability scanner to map network weaknesses. According to standard assessment methodologies, at which phase must a friendly scanner stop to prevent accidental system downtime?**

A) It must immediately log an exception at step 1 before scanning open ports or identifying active IP addresses.

B) It must terminate or restrict its actions by step 2 or 3, never proceeding to execute a step 4 vulnerability exploit.

C) It must transition directly into a padded cell environment to isolate production system data.

D) It must continuously cycle through self-replicating discovery loops without human intervention..



## Friendly Vulnerability Scanners

**During a security audit, an administrator deploys a friendly vulnerability scanner to map network weaknesses. According to standard assessment methodologies, at which phase must a friendly scanner stop to prevent accidental system downtime?**

A) It must immediately log an exception at step 1 before scanning open ports or identifying active IP addresses.

B) **It must terminate or restrict its actions by step 2 or 3, never proceeding to execute a step 4 vulnerability exploit.** ✓

C) It must transition directly into a padded cell environment to isolate production system data.

D) It must continuously cycle through self-replicating discovery loops without human intervention..

INSPIRING FUTURES

## Nmap in OT

- Which scan timing options are recommended for OT environments to balance thoroughness and caution?

☐ `-T1` ☐ `-T2` ☐ `-T3` ☐ `-T4` ☐ `-T5`

- What does the `-sT` option in NMAP signify for enhancing scanning safety in OT networks?

○ UDP Connect Scan ○ TCP Connect Scan ○ SYN Stealth Scan

- How does the `--max-parallelism 1` option in a scan configuration contribute to safe scanning in OT environments?

○ It increases the number of parallel operations, enhancing scan speed.
○ It limits parallel probing to one at a time, reducing the risk of disruptions
○ It scans multiple hosts simultaneously to save time.



## Nmap in OT

- Which scan timing options are recommended for OT environments to balance thoroughness and caution?

☐ `-T1` ☑ `-T2` ☐ `-T3` ☐ `-T4` ☐ `-T5`

- What does the `-sT` option in NMAP signify for enhancing scanning safety in OT networks?

○ UDP Connect Scan ● TCP Connect Scan ○ SYN Stealth Scan

- How does the `--max-parallelism 1` option in a scan configuration contribute to safe scanning in OT environments?

○ It increases the number of parallel operations, enhancing scan speed.
● It limits parallel probing to one at a time, reducing the risk of disruptions
○ It scans multiple hosts simultaneously to save time.



## Maintaining Anonymity in External Reconnaissance

**A security professional wants to execute an anonymous network scan through a proxy chain via the TOR network. Which technical configuration is required to accurately simulate application-layer behaviour while preventing public identity leaks?**

A) Relying exclusively on raw packet injection tools that completely bypass the local host's Berkeley Socket API.

B) Routing scanning traffic through an open production proxy that dynamically drops ICMP echo requests.

C) Forcing the scanner to guess operating system fingerprints aggressively using the intense timing template (-T5).

D) Utilising a TCP connect scan (-sT) while ensuring any existing personal SSH public key is not exposed.



## Maintaining Anonymity in External Reconnaissance

**A security professional wants to execute an anonymous network scan through a proxy chain via the TOR network. Which technical configuration is required to accurately simulate application-layer behaviour while preventing public identity leaks?**

A) Relying exclusively on raw packet injection tools that completely bypass the local host's Berkeley Socket API.

B) Routing scanning traffic through an open production proxy that dynamically drops ICMP echo requests.

C) Forcing the scanner to guess operating system fingerprints aggressively using the intense timing template (-T5).

D) **Utilising a TCP connect scan (-sT) while ensuring any existing personal SSH public key is not exposed.** ✓

## Distinguishing Enticement from Entrapment

**A security officer is setting up a honey pot to detect unauthorised activity. To ensure the deployment is legal, which configuration strategy must they follow?**

A) The honey pot actively solicits subjects to access it and the owner charges them with intrusion.

B) The honey pot presents open security vulnerabilities, leaving the decision to exploit up to the perpetrator.

C) The honey pot acts as a friendly vulnerability scanner that executes step 4 exploits on network nodes.

D) The honey pot captures legitimate production traffic to filter out internet worm signatures.That the system completely matches external data privacy obligations and minimises operational budget requirements.



## Distinguishing Enticement from Entrapment

**A security officer is setting up a honey pot to detect unauthorised activity. To ensure the deployment is legal, which configuration strategy must they follow?**

A) The honey pot actively solicits subjects to access it and the owner charges them with intrusion.

B) **The honey pot presents open security vulnerabilities, leaving the decision to exploit up to the perpetrator.** ✓

C) The honey pot acts as a friendly vulnerability scanner that executes step 4 exploits on network nodes.

D) The honey pot captures legitimate production traffic to filter out internet worm signatures.That the system completely matches external data privacy obligations and minimises operational budget requirements.






## Learning outcomes

You should now be able to:

- Map an organisation's attack surface by leveraging Shodan for passive asset discovery and configuring Nmap for precise target specification and host discovery. ✓
- Formulate advanced Nmap scanning strategies that optimise performance, utilise XML output, and implement Firewall/IDS evasion techniques while diagnosing issues via NSE debugging. ✓
- Evaluate the risks of scanning IACS and safely execute non-disruptive, IACS-specific NSE scripts to prevent industrial downtime. ✓
- Design and deploy honeypots and network canaries within an architecture to detect early-stage reconnaissance and alert security operations before a breach escalates. ✓

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

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

# Thank you

EOLAS-I Research Centre