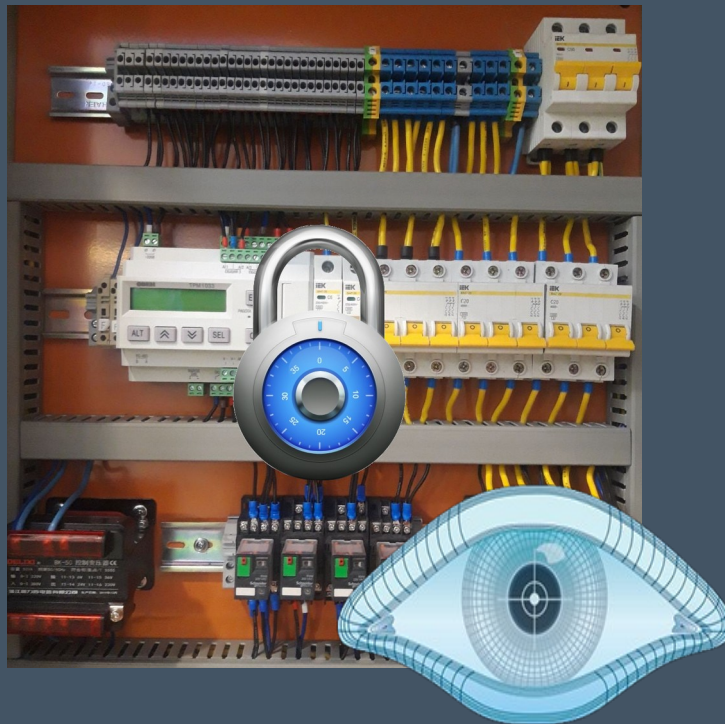


Topic 10

Penetration Testing Reconnaissance



Dr Diarmuid Ó Briain
Version: 3.0

Copyright © 2025 C²S Consulting

Licensed under the EUPL, Version 1.2 or – as soon they will be approved by the European Commission - subsequent versions of the EUPL (the "Licence");

You may not use this work except in compliance with the Licence.

You may obtain a copy of the Licence at:

https://joinup.ec.europa.eu/sites/default/files/custom-page/attachment/eupl_v1.2_en.pdf

Unless required by applicable law or agreed to in writing, software distributed under the Licence is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

See the Licence for the specific language governing permissions and limitations under the Licence.

Dr Diarmuid Ó Briain



Table of Contents

1 Objectives.....	5
2 Introduction.....	5
3 The Anatomy of a Cyber attack.....	6
3.1 Reconnaissance.....	6
3.2 Initial Exploitation and Establishment Persistence.....	6
3.3 Install tools.....	7
3.4 Move Laterally.....	7
3.5 Collect, Exfiltrate and Exploit.....	7
4 Introduction to Penetration testing.....	8
4.1 Penetration testing steps.....	8
5 Shodan.....	11
5.1 Exercise #10.1.....	12
6 The Kali Linux Virtual Machine.....	13
6.1 Update and Upgrade.....	14
6.2 Keyboard.....	14
6.3 Network.....	14
6.4 Change theme.....	16
6.5 Install Oracle Guest Additions.....	16
6.6 Clean the install packages and reboot.....	16
7 Network Mapper (NMAP).....	17
7.1 Network Mapper.....	17
7.2 nmapsi4.....	17
8 Install NMAP.....	18
9 Operating NMAP.....	19
9.1 Target Specification.....	19
9.2 Scan Techniques.....	21
9.3 Host Discovery.....	22
9.4 Port Specification.....	24
9.5 Service and Version detection.....	24
9.6 Operating System Detection.....	25
9.7 Timing.....	25
9.8 Performance.....	26
9.9 NMAP Scripting Engine (NSE).....	27
9.10 Firewall / IDS Evasion and Spoofing.....	28
9.11 Output.....	29
9.12 Miscellaneous Options.....	30
9.13 Other useful nmap Commands.....	30
9.14 Debugging, Verbosity and Reason.....	31
9.15 XML output.....	32

9.16 Use NMAP anonymously.....	33
10 OT Network Security, Scanning and Enumeration with NMAP.....	37
10.1 The Problem with Scanning Legacy Devices.....	37
10.2 Scanning ACS in a Penetration Test.....	37
10.3 Quiz.....	38
10.4 ACS Specific scripts for NSE.....	39
10.5 Exercise #10.2.....	39

Table of Figures

Figure 1: Anatomy of a Cyber attack.....	6
Figure 2: Penetration test steps.....	8
Figure 3: Shodan scan of Dublin City for Modbus devices.....	11
Figure 4: Kali Linux Desktop.....	13
Figure 5: VirtualBox Network Configuration.....	15
Figure 6: Kali Linux Network test.....	15
Figure 7: nmapsi4 graphical nmap front-end.....	17
Figure 8: Using the TOP network.....	33
Figure 9: IP addressing info.....	35
Figure 10: Source for connections through TOR.....	36

Index of Tables

Table 1: Nmap port scan techniques.....	21
Table 2: Nmap host discovery control options.....	23
Table 3: Nmap port specification.....	24
Table 4: Nmap Service and Version detection.....	24
Table 5: Nmap OS detection.....	25
Table 6: Nmap timing options.....	25
Table 7: Nmap fine-tuning scan performance options.....	26
Table 8: Nmap NSE Scripts.....	27
Table 9: Nmap NSE script examples.....	28
Table 10: Nmap commands and techniques for evasion and spoofing.....	28
Table 11: Nmap output options.....	29
Table 12: Nmap output examples.....	30
Table 13: Namp miscellaneous options.....	30
Table 14: Other useful Nmap commands.....	30

1 Objectives

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

- Design a penetration testing reconnaissance plan for an OT network.
- Assess the security posture of an OT network based on a penetration test reconnaissance.
- Develop a Python script to automate the scanning and enumeration of an OT network.
- Evaluate the effectiveness of different penetration testing reconnaissance tools and techniques.

2 Introduction

Penetration testing, also known as pen testing, is the practice of simulating cyberattacks on a computer system or network to identify security vulnerabilities that could be exploited by malicious actors. Penetration testers use a variety of tools and techniques to mimic the real-world tactics of cybercriminals, and their findings can help organisations to improve their security posture and reduce their risk of being breached. Penetration testing is an important part of any comprehensive cybersecurity programme. It can help organisations to:

- Identify and fix security vulnerabilities before they can be exploited by attackers
- Improve their security posture by implementing the recommendations of the pen test report
- Comply with industry regulations and standards
- Demonstrate their commitment to security to customers and stakeholders.

Pen testing is typically conducted in four phases:

- **Planning:** The pen tester works with the organisation to understand their scope and goals, and to develop a plan for the test.
- **Information gathering:** The pen tester gathers information about the organisation's systems and networks, such as Internet Protocol (IP) addresses, operating systems, and applications.
- **Vulnerability assessment:** The pen tester uses a variety of tools and techniques to identify security vulnerabilities in the organisation's systems and networks.
- **Exploitation:** The penetration tester attempts to exploit the identified vulnerabilities to gain access to the organisation's systems and data.

Once the pen test is complete, the penetration tester will generate a report that documents the findings and recommendations. The report should include a detailed description of the vulnerabilities that were found, as well as steps that the organisation can take to mitigate the risk.

3 The Anatomy of a Cyber attack

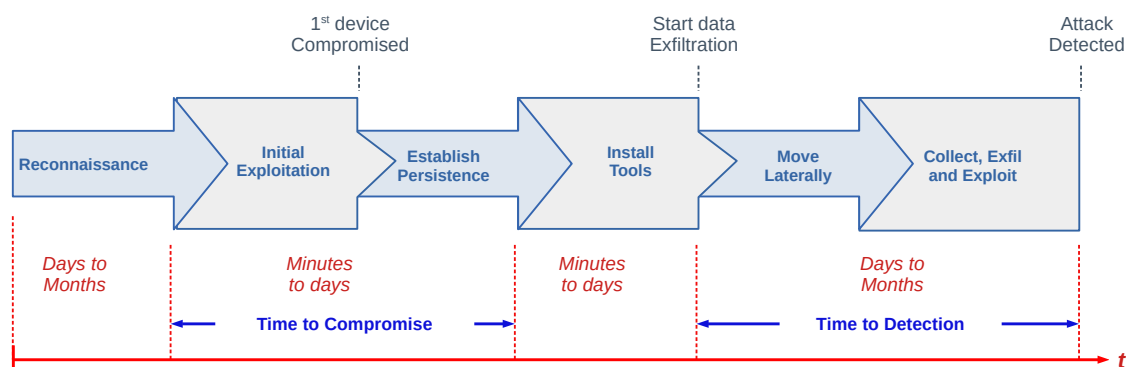


Figure 1: Anatomy of a Cyber attack

3.1 Reconnaissance

The first element of the anatomy of a cyber attack is reconnaissance. The attacker, often termed hackers, usually start by researching and gathering information about the target organisation. This phase is a search for useful vectors of attacks, network ranges, IP addresses, port numbers and domain names. Another avenue of research in the reconnaissance is a search for email addresses of key individuals throughout the organisation such as C-suite officers, managers and even employees. Vulnerable employees can be identified via phishing emails who may initially have been identified via corporate websites or personal contacts at trade shows or conferences.

The next reconnaissance step is a scan for vulnerabilities in the network, which is a process that can take some time. Once a viable attack vector has been identified via network vulnerabilities or employee email address, attackers proceed to an initial exploitation attack.

3.2 Initial Exploitation and Establishment Persistence

Once a foothold has been established via the network for example, the attack uses this to further infiltrate the organisation's network. To gain further access the attacking hacker requires access privileges. By using tools such as precomputed tables for caching the output of cryptographic hash functions, called rainbow tables, the hacker attempts to crack password hashes in an attempt to identify usable credentials to upgrade access to administrator privileges on either the foothold system or another nearby system.

3.3 Install tools

With this the hacker has wider access to the network of systems and can traverse systems installing tools that leverage further access.

3.4 Move Laterally

The next phase of the anatomy of a cyber attack the move laterally or sometimes termed the expansion and obfuscation. Hackers intrude further on systems that may not be related to the initial foothold. For example the foothold might be through WiFi on a printer and access is gained from it to a compromised computer that permits access to the control levels of the manufacturing operation. Installing malicious programs that enable the attackers to hide in multiple systems and regain access to the network even after one or more access vectors have been detected. This move laterally gives the hacker the space to obfuscate, or hide, the origins of the attack and establish exploit processes that avoid getting detected. The main purpose of obfuscation is confusing and disorienting the forensic experts and various tools and techniques such as spoofing, log cleaning, zombied accounts, and Trojan commands are used for this purpose.

3.5 Collect, Exfiltrate and Exploit

With access achieved the final step is the collect and exfiltrate as much data as possible and exploit both the data and the access before detection and moved by cybersecurity experts to mitigate, remediate and block the attack.

4 Introduction to Penetration testing

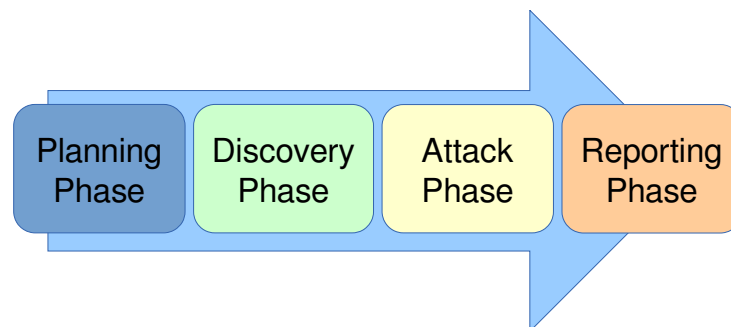


Figure 2: Penetration test steps

Penetration testing (pen-testing) is the practice of testing a computer system, network or web application to find vulnerabilities that an attacker can exploit. It is a proactive and authorised attempt to evaluate the security of an Information Technology (IT) or Operations Technology (OT) infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behaviour.

4.1 Penetration testing steps

In many ways the pen-test mimics the anatomy of a cyber attack but with different objectives. The pen-test is an attempt to identify existing vulnerabilities that could present an attack vector to a hacker. Once these vulnerabilities are identified the organisation needs to establish and implement a plan to remove or mitigate these.

4.1.1 Planning and Preparation

A kick-off meeting with the management to discuss in detail the scope and the overall objective of the pen-test. A clear objective is essential for the pen-test such as to demonstrate that exploitable vulnerabilities do in fact exist within the business infrastructure, whether that be IT or OT. As part of the scoping identify:

- Timing and duration allowed for the pen-tests
- Personnel involved
- Are staff being informed of the tests?
- Network, Computers, Devices and processes involved
- Operational requirements during the pen-test
- How the results are to be presented at the conclusion of the test.

After this scoping meeting the pen-testers need to develop a **Penetration Test Plan** which should be shared with the client company. It must include:

- The detailed test plan itself. What tests are to be performed and on what.
- A **Confidentiality statement** that is signed by both the pen-testers and the client.
- A clear **Acceptance sign-off sheet** that the **Penetration Test Plan** is acceptable to the client and affords legal protection to the pen-testers.

Remember the pen-testers are actually conducting tests that are deemed illegal and therefore require the indemnity of the Acceptance sign-off from the client company.

4.1.2 Reconnaissance, 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?

4.1.3 Vulnerability detection

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

4.1.4 Penetration attempt

Once a list of vulnerabilities have been identified and logged it is time to attempt a penetration. Identifying the best targets from the machines showing vulnerability is important particularly if the time given is short. Identifying the juicy targets may be as simply as looking at the machine names as it is a habit of IT personnel 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.

4.1.5 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 (including on machines not singled out for a penetration attempt).
- A suggested list of next steps to close the vulnerabilities and increase security at the client company.

4.1.6 Tidy up

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

The remainder of this topic will focus on the initial step of penetration testing, the reconnaissance.

5 Shodan

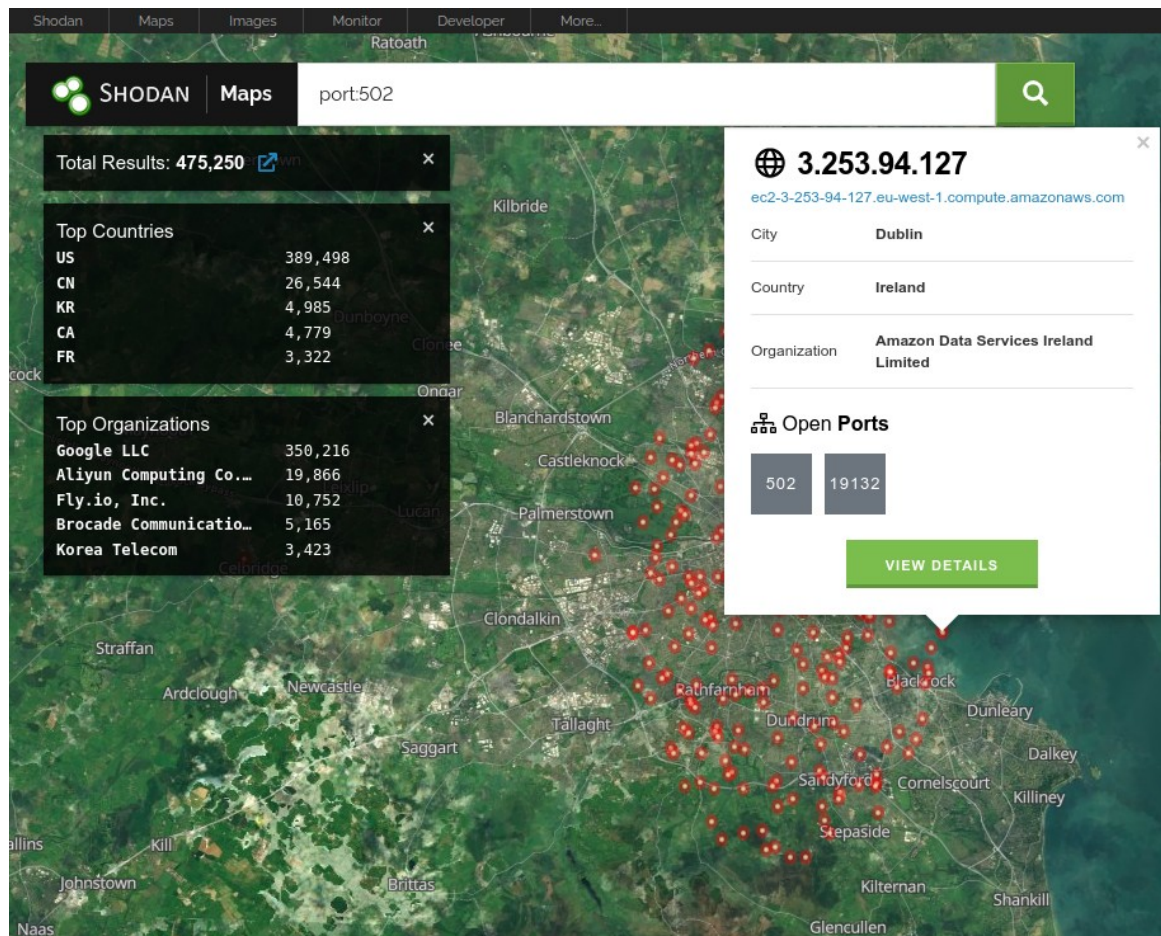


Figure 3: Shodan scan of Dublin City for Modbus devices

Shodan (<https://www.shodan.io>) is a search engine that finds devices connected to the Internet. It is a powerful tool for security researchers, hackers, and anyone who wants to learn more about the Internet of Things (IoT).

Shodan works by scanning the Internet for devices that respond to Internet Control Message Protocol (ICMP) ping requests. It then collects information about the devices, such as their IP addresses, operating systems, and open ports. Shodan also indexes the banners that devices send out, which can reveal additional information about the devices.

Shodan can be used to find a wide variety of devices, including:

- Switches
- Routers
- Webcams
- Security cameras
- Automation and Control Systems (ACS)
- Heating, Ventilation, and Air Conditioning (HVAC) systems
- Smart TVs
- Refrigerators

Shodan can be a valuable tool for security researchers, as it can help them to discover new vulnerabilities and to track the deployment of malware. Shodan can also be used by hackers to find targets for attacks. However, it's important to note that Shodan is not a hacking tool. It's simply a search engine that helps people to find devices connected to the Internet. It's up to the user to decide how to use the information that Shodan provides.

Here are some examples of how Shodan can be used:

- A security researcher can use Shodan to find all of the Modbus devices that are publicly accessible on the Internet. This could help discover new vulnerabilities in Programmable Logic Controllers (PLC) or to track the deployment of malware that targets PLCs.
- A hacker could use Shodan to find all of the routers that are using a specific firmware with a known vulnerability. This could allow them to exploit the vulnerability and gain access to the routers.
- A business could use Shodan to find all of the devices on their network that are exposed to the Internet. This could help identify and mitigate security risks.

Shodan is a powerful tool that can be used for a variety of purposes. It's important to be aware of the potential risks of using Shodan, but it can also be a valuable tool for learning more about the internet and for improving security.

5.1 Exercise #10.1

- Create a personal Shodan account.
- Login to Shodan.
- Discover the Transmission Control Protocol (TCP) port number for the Distributed Network Protocol version 3 (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 IP Address?

6 The Kali Linux Virtual Machine

Using the Kali Linux image provided on the website below, install **VirtualBox**, build the **.ova** image, install and run.

<https://www.kali.org/get-kali/#kali-virtual-machines>

Login to the image with the default root username (**kali**) and password (**kali**).

There can be problems associated with the USB2.0 ports until the Oracle VirtualBox Guest Additions have been installed.

Adjust the Virtual screen to your preferred comfort level. In my case I adjust to:

View >> Virtual Screen 1 >> Scale to 200% (autoscaled output)

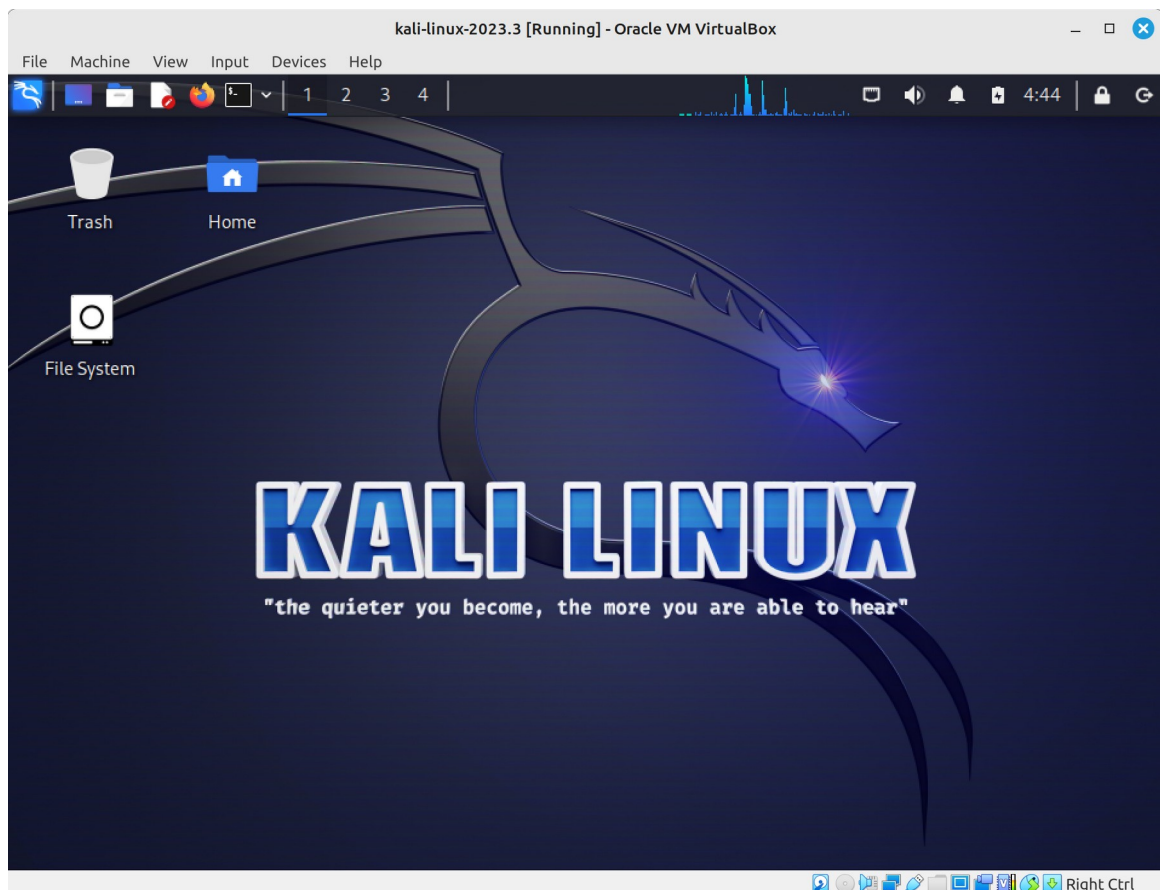


Figure 4: Kali Linux Desktop

6.1 Update and Upgrade

Run up a shell, use upgrade to download package information from the Kali Linux repository sources and then install available upgrades of all packages currently installed on the system. This can take some time.

```
(kali㉿kali)-[~]  
└─$ sudo apt update && sudo apt -y upgrade  
[sudo] password for kali: kali
```

6.2 Keyboard

Run up a shell and establish the keyboard layout. For example British English.

```
(kali㉿kali)-[~]  
└─$ setxkbmap -layout gb
```

```
(kali㉿kali)-[~]  
└─$ setxkbmap -query  
rules:          evdev  
model:          pc105  
layout:         gb
```

6.3 Network

Confirm connectivity with the Internet.

```
(kali㉿kali)-[~]  
└─$ ip addr list dev eth0 | grep 'inet ' | awk '{print $2}'  
10.0.2.15/24
```

The IP Address is assigned by Network Address Translation (NAT) to the Virtual Machine (VM). It is possible to bridge the VM Ethernet interface (eth0) with the active interface on the host to get an IP address from the real world Dynamic Host Configuration Protocol (DHCP) Server.

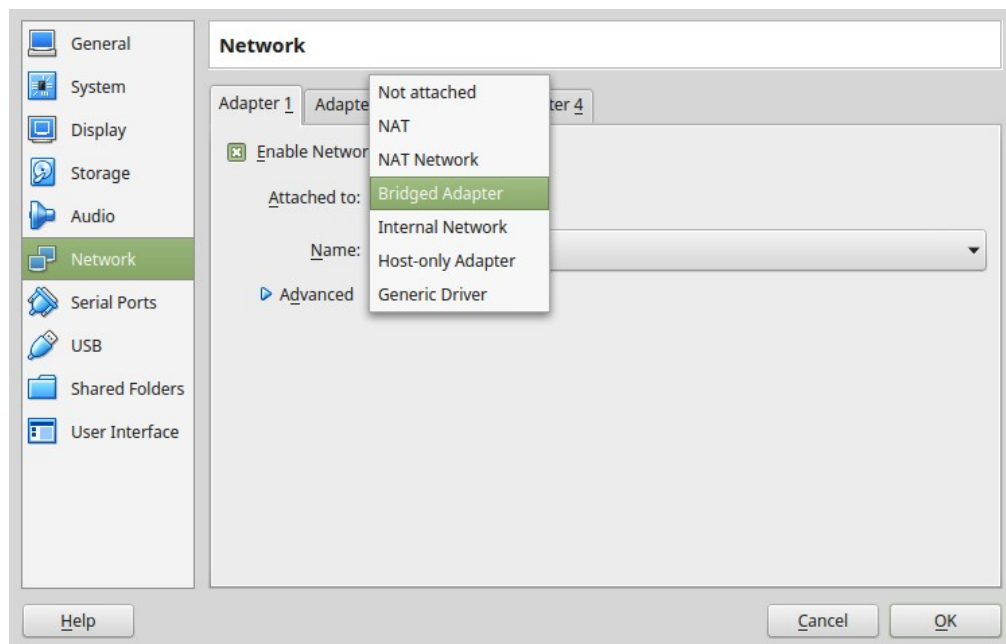


Figure 5: VirtualBox Network Configuration

Whichever system is used the IP Packet InterNet Groper (PING) test to the main google nameserver at 8.8.8.8 should elicit a response.

```
(kali㉿kali)-[~]  
$ ping -c3 8.8.8.8  
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=18.7 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=16.2 ms  
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=16.4 ms  
  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 16.193/17.113/18.729/1.146 ms
```

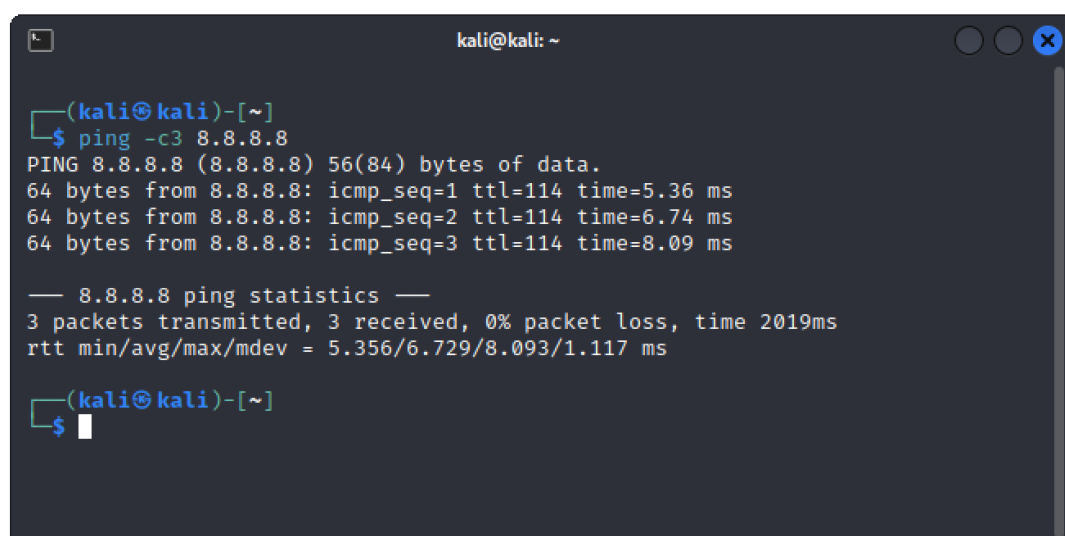


Figure 6: Kali Linux Network test

6.4 Change theme

Some prefer the light theme to the default dark theme. To change if required:

Settings >> Appearance >>

Style: Kali-Light

Icons: Flat-Remix-Blue-Light

6.5 Install Oracle Guest Additions

Oracle VirtualBox Guest Additions provides the VM device drivers and system applications to optimise the Kali Linux operating system for better performance and usability.

```
(kali㉿kali)-[~]  
└─$ sudo apt install -y virtualbox-guest-x11
```

6.6 Clean the install packages and reboot

Remove any packages that were automatically installed and are no longer required, then reboot the VM.

```
(kali㉿kali)-[~]  
└─$ sudo apt autoremove
```

```
(kali㉿kali)-[~]  
└─$ sudo reboot now
```


7 Network Mapper (NMAP)

The remainder of this module will focus on one aspect of the pen-test, reconnaissance, and in particular using Network Mapper (**nmap**) and the Python programming language to perform reconnaissance.

7.1 Network Mapper

nmap is an open source network exploration and security auditing tool. It was designed to rapidly scan large networks, although it works fine against single hosts too. **nmap** 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 dozens of other characteristics. While **nmap** is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

7.2 nmapsi4

A Qt4 front-end interface for **nmap** exists as illustrated in Figure 7.

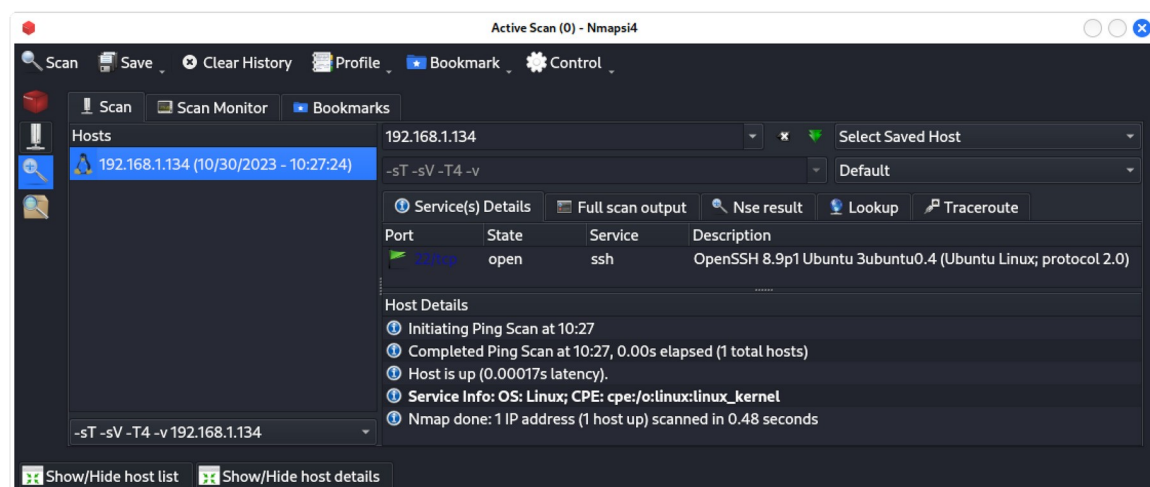


Figure 7: nmapsi4 graphical nmap front-end

8 Install NMAP

Install **nmap** and **nmapsi4** packages on the operating system.

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

Test **nmap** version.

```
(kali㉿kali)-[~]  
└─$ nmap --version  
nmap --version  
Nmap version 7.94 ( https://nmap.org )  
Platform: x86_64-pc-linux-gnu  
Compiled with: liblua-5.4.4 openssl-3.0.11 libssh2-1.11.0 libz-1.2.13  
libpcre-8.39 libpcap-1.10.4 nmap-libdnet-1.12 ipv6  
Compiled without:  
Available nsock engines: epoll poll select
```

9 Operating NMAP

9.1 Target Specification

At its simplest **nmap** checks the target for open ports. In the example below the Secure Shell (SSH) and Hyper Text Transfer Protocol (HTTP) daemons are active as TCP ports 22 and 80 are open. This scan of 1,000 TCP ports returns a granular list of states:

9.1.1 open

An application is actively accepting TCP connections, User Datagram Protocol (UDP) datagrams or Stream Control Transmission Protocol (SCTP) associations on this port. Finding these is often the primary goal of port scanning. Security-minded people know that each open port is an avenue for attack. Attackers and pen-testers want to exploit the open ports, while administrators try to close or protect them with firewalls without thwarting legitimate users. Open ports are also interesting for non-security scans because they show services available for use on the network.

9.1.2 closed

A closed port is accessible (it receives and responds to **nmap** probe packets), but there is no application listening on it. They can be helpful in showing that a host is up on an IP address (host discovery, or ping scanning), and as part of OS detection. Because closed ports are reachable, it may be worth scanning later in case some open up. Administrators may want to consider blocking such ports with a firewall. Then they would appear in the filtered state, discussed next.

9.1.3 filtered

nmap cannot determine whether the port is open because packet filtering prevents its probes from reaching the port. The filtering could be from a dedicated firewall device, router rules, or host-based firewall software. These ports frustrate attackers because they provide so little information. Sometimes they respond with ICMP error messages such as type 3 code 13 (destination unreachable: communication administratively prohibited), but filters that simply drop probes without responding are far more common. This forces **nmap** to retry several times just in case the probe was dropped due to network congestion rather than filtering. This slows down the scan dramatically.

9.1.4 unfiltered

The unfiltered state means that a port is accessible, but **nmap** is unable to determine whether it is open or closed. Only the ACK scan, which is used to map firewall rulesets, classifies ports into this state. Scanning unfiltered ports with other scan types such as Window scan, SYN scan, or FIN scan, may help resolve whether the port is open.

9.1.5 open|filtered

nmap places ports in this state when it is unable to determine whether a port is open or filtered. This occurs for scan types in which open ports give no response. The lack of response could also mean that a packet filter dropped the probe or any response it elicited. So **nmap** does not know for sure whether the port is open or being filtered. The UDP, IP protocol, FIN, NULL, and Xmas scans classify ports this way.

9.1.6 closed|filtered

This state is used when **nmap** is unable to determine whether a port is closed or filtered. It is only used for the IP ID idle scan.

```
(kali㉿kali)-[~]  
$ nmap 10.0.2.7  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 14:42 GMT  
Nmap scan report for 10.0.2.7  
Host is up (0.00087s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http
```

A scan can also be carried out on a range of addresses.

```
(kali㉿kali)-[~]  
$ nmap 10.0.2.0/24  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 14:46 GMT  
Nmap scan report for _gateway (10.0.2.1)  
Host is up (0.00058s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
53/tcp    open  domain  
  
Nmap scan report for 10.0.2.2  
Host is up (0.00061s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
631/tcp   open  ipp  
  
Nmap scan report for scapy (10.0.2.6)  
Host is up (0.00025s latency).  
Not shown: 999 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
  
Nmap scan report for 10.0.2.7  
Host is up (0.00020s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
  
Nmap done: 256 IP addresses (4 hosts up) scanned in 3.15 seconds
```

Other options are included in the following table.

Switch	Example	Description
	<code>nmap 192.168.1.1</code>	Scan a single IP
	<code>nmap 192.168.1.1 192.168.2.1</code>	Scan specific IPs
	<code>nmap 192.168.1.1-254</code>	Scan a range
	<code>nmap scanme.nmap.org</code>	Scan a domain
	<code>nmap 192.168.1.0/24</code>	Scan using CIDR notation
<code>-iL</code>	<code>nmap -iL targets.txt</code>	Scan targets from a file
<code>-iR</code>	<code>nmap -iR 100</code>	Scan 100 random hosts
<code>--exclude</code>	<code>nmap --exclude 192.168.1.1</code>	Exclude listed hosts

9.2 Scan Techniques

Most of the scan types are only available to privileged users. This is because they send and receive raw packets, which requires **root** access.

While **nmap** attempts to produce accurate results, bear in mind that all of its insights are based on packets returned by the target machines (or firewalls in front of them). Such hosts may be untrustworthy and send responses intended to confuse or mislead **nmap**. Much more common are non-RFC-compliant hosts that do not respond as they should to **nmap** probes. FIN, NULL, and Xmas scans are particularly susceptible to this problem. Such issues are specific to certain scan types and so are discussed in the individual scan type entries.

Table 1 lists the port scan techniques supported by **nmap**. Only one method may be used at a time, except that UDP scan (`-sU`) and any one of the SCTP scan types (`-sY`, `-sZ`) may be combined with any one of the TCP scan types. Port scan type options are of the form `-s<C>`, where `<C>` is a prominent character in the scan name, usually the first. The one exception to this is the deprecated FTP bounce scan (`-b`). By default, **nmap** performs a SYN Scan, though it substitutes a connect scan if the user does not have proper privileges to send raw packets. Of the scans listed in this section, unprivileged users can only execute connect and FTP bounce scans.

Table 1: Nmap port scan techniques

Switch	Example	Description
<code>-sS</code>	<code>nmap 192.168.1.1 -sS</code>	TCP SYN port scan (Default)
<code>-sT</code>	<code>nmap 192.168.1.1 -sT</code>	TCP connect port scan (Default without root privilege)
<code>-sU</code>	<code>nmap 192.168.1.1 -sU</code>	UDP port scan
<code>-sA</code>	<code>nmap 192.168.1.1 -sA</code>	TCP ACK port scan
<code>-sW</code>	<code>nmap 192.168.1.1 -sW</code>	TCP Window port scan
<code>-sM</code>	<code>nmap 192.168.1.1 -sM</code>	TCP Maimon port scan

```
(kali㉿kali)-[~]  
$ sudo nmap 10.0.2.7 -sS  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 17:23 GMT  
Nmap scan report for 10.0.2.7  
Host is up (0.00016s latency).  
Not shown: 998 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 08:00:27:A3:92:BA (Oracle VirtualBox virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

```
(kali㉿kali)-[~]  
$ sudo nmap 10.0.2.7 -sU  
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-11 17:24 GMT
```

9.3 Host Discovery

One of the very first steps in any network reconnaissance is to reduce a set of IP ranges into a list of active or interesting hosts. Scanning every port of every single IP address is slow and usually unnecessary. Of course what makes a host interesting depends greatly on the scan purposes. Network administrators may only be interested in hosts running a certain service, while security auditors may care about every single device with an IP address. An administrator may be comfortable using just an ICMP ping to locate hosts on his internal network, while an external penetration tester may use a diverse set of dozens of probes in an attempt to evade firewall restrictions.

Because host discovery needs are so diverse, **nmap** offers a wide variety of options for customising the techniques used. Host discovery is sometimes called ping scan, but it goes well beyond the simple ICMP echo request packets associated with the standard ping tool. Users can skip the discovery step entirely with a list scan (**-sL**) or by disabling host discovery (**-Pn**), or engage the network with arbitrary combinations of multi-port TCP SYN/ACK, UDP, SCTP INIT and ICMP probes. The goal of these probes is to solicit responses which demonstrate that an IP address is actually active (is being used by a host or network device). On many networks, only a small percentage of IP addresses are active at any given time. This is particularly common with RFC1918 private address blocks such as 10.0.0.0/8. That network has 16 million IPs but a company may only use a small fraction of them. Host discovery can find those machines in a sparsely allocated sea of IP addresses.

If no host discovery options are given, **nmap** sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request. (For IPv6, the ICMP timestamp request is omitted because it is not part of ICMPv6.) The exceptions to this are the Address Resolution Protocol (ARP) (for IPv4) and Neighbour Discovery (for IPv6) scans which are used for any targets on a local Ethernet network. For unprivileged users, the default probes are a SYN packet to ports 80 and 443 using the connect system call. This host discovery is often sufficient when scanning local networks, but a more comprehensive set of discovery probes is recommended for security auditing.

The **-P*** options (which select ping types) can be combined. The odds of penetrating strict firewalls can be increased by sending many probe types using different TCP

ports/flags and ICMP codes. Also note that ARP/Neighbour Discovery is carried out by default against targets on a local Ethernet network even if other **-P*** options are specified, because it is almost always faster and more effective.

By default, **nmap** performs host discovery and then performs a port scan against each host it determines is online. This is true even if non-default host discovery types are specified such as UDP probes (**-PU**). Table 2 lists the host discovery control options:

Table 2: Nmap host discovery control options

Switch	Example	Description
-sL	<code>nmap 192.168.1.1-3 -sL</code>	No Scan. List targets only
-sn	<code>nmap 192.168.1.1/24 -sn</code>	Disable port scanning. Host discovery only.
-Pn	<code>nmap 192.168.1.1-5 -Pn</code>	Disable host discovery. Port scan only.
-PS	<code>nmap 192.168.1.1-5 -PS22-25,80</code>	TCP SYN discovery on port x. Port 80 by default
-PA	<code>nmap 192.168.1.1-5 -PA22-25,80</code>	TCP ACK discovery on port x. Port 80 by default
-PU	<code>nmap 192.168.1.1-5 -PU53</code>	UDP discovery on port x. Port 40125 by default
-PR	<code>nmap 192.168.1.1-1/24 -PR</code>	ARP discovery on local network
-n	<code>nmap 192.168.1.1 -n</code>	Never do DNS resolution

9.4 Port Specification

Table 3 outlines various Nmap commands and their uses for port scanning.

Table 3: Nmap port specification

Switch	Example	Description
-p	<code>nmap 192.168.1.1 -p 21</code>	Port scan for port x
-p	<code>nmap 192.168.1.1 -p 21-100</code>	Port range
-p	<code>nmap 192.168.1.1 -p U:53,T:21-25,80</code>	Port scan multiple TCP and UDP ports
-p-	<code>nmap 192.168.1.1 -p-</code>	Port scan all ports
-p	<code>nmap 192.168.1.1 -p http,https</code>	Port scan from service name
-F	<code>nmap 192.168.1.1 -F</code>	Fast port scan (100 ports)
--top-ports	<code>nmap 192.168.1.1 --top-ports 2000</code>	Port scan the top x ports
-p-65535	<code>nmap 192.168.1.1 -p-65535</code>	Leaving off initial port in range makes the scan start at port 1
-p0-	<code>nmap 192.168.1.1 -p0-</code>	Leaving off end port in range makes the scan go through to port 65535

9.5 Service and Version detection

Table 4 provides an overview of Nmap commands used for service and version detection.

Table 4: Nmap Service and Version detection

Switch	Example	Description
-sV	<code>nmap 192.168.1.1 -sV</code>	Attempts to determine the version of the service running on port
-sV --version-intensity	<code>nmap 192.168.1.1 -sV --version-intensity 8</code>	Intensity level 0 to 9. Higher number increases possibility of correctness
-sV --version-light	<code>nmap 192.168.1.1 -sV --version-light</code>	Enable light mode. Lower possibility of correctness. Faster
-sV --version-all	<code>nmap 192.168.1.1 -sV --version-all</code>	Enable intensity level 9. Higher possibility of correctness. Slower
-A	<code>nmap 192.168.1.1 -A</code>	Enables OS detection, version detection, script scanning, and traceroute

9.6 Operating System Detection

Table 5 details Nmap commands used for operating system (OS) detection.

Table 5: Nmap OS detection

Switch	Example	Description
-O	<code>nmap 192.168.1.1 -O</code>	Remote OS detection using TCP/IP stack fingerprinting
-O --osscan-limit	<code>nmap 192.168.1.1 -O --osscan-limit</code>	If at least one open and one closed TCP port are not found it will not try OS detection against host
-O --osscan-guess	<code>nmap 192.168.1.1 -O --osscan-guess</code>	Makes nmap guess more aggressively
-O --max-os-tries	<code>nmap 192.168.1.1 -O --max-os-tries 1</code>	Set the maximum number x of OS detection tries against a target
-A	<code>nmap 192.168.1.1 -A</code>	Enables OS detection, version detection, script scanning, and traceroute

9.7 Timing

Table 6 lists the different Nmap timing templates and their descriptions.

Table 6: Nmap timing options

Switch	Example	Description
-T0	<code>nmap 192.168.1.1 -T0</code>	Paranoid (0) Intrusion Detection System evasion
-T1	<code>nmap 192.168.1.1 -T1</code>	Sneaky (1) Intrusion Detection System evasion
-T2	<code>nmap 192.168.1.1 -T2</code>	Polite (2) slows down the scan to use less bandwidth and use less target machine resources
-T3	<code>nmap 192.168.1.1 -T3</code>	Normal (3) which is default speed
-T4	<code>nmap 192.168.1.1 -T4</code>	Aggressive (4) speeds scans; assumes you are on a reasonably fast and reliable network
-T5	<code>nmap 192.168.1.1 -T5</code>	Insane (5) speeds scan; assumes you are on an extraordinarily fast network

9.8 Performance

Table 7 outlines various Nmap commands for fine-tuning scan performance.

Table 7: Nmap fine-tuning scan performance options

Switch	Example input	Description
--host-timeout <time>	1s; 4m; 2h	Give up on target after this long
--min-rtt-timeout/ max-rtt-timeout/ initial-rtt-timeout <time>	1s; 4m; 2h	Specifies probe round trip time
--min-hostgroup/ max-hostgroup <size>	50; 1024	Parallel host scan group sizes
--min-parallelism/max-parallelism <numprobes>	10; 1	Probe parallelisation
--scan-delay/ --max-scan-delay <time>	20ms; 2s; 4m; 5h	Adjust delay between probes
--max-retries <tries>	3	Specify the maximum number of port scan probe retransmissions
--min-rate <number>	100	Send packets no slower than <number> per second
--max-rate <number>	100	Send packets no faster than <number> per second

9.9 NMAP Scripting Engine (NSE)

The NMAP Scripting Engine (NSE) is a powerful and advanced functionality within **nmap**, enabling users to develop custom scripts for automated scanning and extending the capabilities of **nmap**. These scripts are written in Lua, a fast and potent programming language, allowing for tasks like host discovery, service scanning, and version detection. NSE aids in the identification of running services, detecting vulnerabilities, and gathering additional target information. Security professionals can leverage NSE to automate diverse scanning tasks, such as identifying specific services on devices or detecting vulnerabilities across IP address ranges. NSE proves to be an indispensable tool for efficiently scanning networks and pinpointing potential vulnerabilities.

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

Table 8 details Nmap commands used for running NSE scripts and Table 9 provides examples of Nmap commands for various scanning tasks, including web server analysis, DNS enumeration, and vulnerability detection.

Table 8: Nmap 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

9.9.1 Useful NSE Scripts

Table 9: Nmap NSE script examples

Command	Description
<code>nmap -Pn --script=http-sitemap-generator scanme.nmap.org</code>	http site map generator
<code>nmap -n -Pn -p 80 --open -sV -vvv --script banner,http-title -iR 1000</code>	Fast search for random web servers
<code>nmap -Pn --script=dns-brute domain.com</code>	Brute forces DNS hostnames guessing subdomains
<code>nmap -n -Pn -vv -O -sV --script smb-enum*,smb-ls,smb-mbenum,smb-os-discovery,smb-s*,smb-vuln*,smbv2* -vv 192.168.1.1</code>	Safe SMB scripts to run
<code>nmap --script whois* domain.com</code>	Whois query
<code>nmap -p80 --script http-unsafe-output-escaping scanme.nmap.org</code>	Detect cross site scripting vulnerabilities
<code>nmap -p80 --script http-sql-injection scanme.nmap.org</code>	Check for SQL injections

9.10 Firewall / IDS Evasion and Spoofing

Table 10 details various Nmap commands and techniques for evasion and spoofing.

Table 10: Nmap commands and techniques for evasion and spoofing

Switch	Example	Description
<code>-f</code>	<code>nmap 192.168.1.1 -f</code>	Requested scan (including ping scans) use tiny fragmented IP packets. Harder for packet filters
<code>--mtu</code>	<code>nmap 192.168.1.1 --mtu 32</code>	Set your own offset size
<code>-D</code>	<code>nmap -D 192.168.1.101,192.168.1.102,192.168.1.103,192.168.1.23 192.168.1.1</code>	Send scans from spoofed IPs
<code>-D</code>	<code>nmap -D decoy-ip1,decoy-ip2,your-own-ip,decoy-ip3,decoy-ip4 remote-host-ip</code>	Above example explained
<code>-S</code>	<code>nmap -S www.microsoft.com www.facebook.com</code>	Scan Facebook from Microsoft (-e eth0 -Pn may be required)
<code>-g</code>	<code>nmap -g 53 192.168.1.1</code>	Use given source port number
<code>--proxies</code>	<code>nmap --proxies http://192.168.1.1:8080, http://192.168.1.2:8080 192.168.1.1</code>	Relay connections through HTTP/SOCKS4 proxies
<code>--data-length</code>	<code>nmap --data-length 200 192.168.1.1</code>	Appends random data to sent packets

9.10.1 Example IDS Evasion command

```
(kali㉿kali)-[~]
$ nmap -f -t 0 -n -Pn --data-length 200 -D
192.168.1.101,192.168.1.102, 192.168.1.103,192.168.1.23 192.168.1.1
```

9.11 Output

Table 11 provides an overview of Nmap commands for controlling output and debugging and Table 12 presents a collection of Nmap command-line examples and their descriptions, demonstrating various uses of the tool.

Table 11: Nmap output options

Switch	Example	Description
-oN	nmap 192.168.1.1 -oN normal.file	Normal output to the file normal.file
-oX	nmap 192.168.1.1 -oX xml.file	XML output to the file xml.file
-oG	nmap 192.168.1.1 -oG grep.file	Grepable output to the file grep.file
-oA	nmap 192.168.1.1 -oA results	Output in the three major formats at once
-oG -	nmap 192.168.1.1 -oG -	Grepable output to screen. -oN -, -oX - also usable
--append-output	nmap 192.168.1.1 -oN file.file --append-output	Append a scan to a previous scan file
-v	nmap 192.168.1.1 -v	Increase the verbosity level (use -vv or more for greater effect)
-d	nmap 192.168.1.1 -d	Increase debugging level (use -dd or more for greater effect)
--reason	nmap 192.168.1.1 --reason	Display the reason a port is in a particular state, same output as -vv
--open	nmap 192.168.1.1 --open	Only show open (or possibly open) ports
--packet-trace	nmap 192.168.1.1 -T4 --packet-trace	Show all packets sent and received
--iflist	nmap --iflist	Shows the host interfaces and routes
--resume	nmap --resume results.file	Resume a scan

9.11.1 NMAP Output examples

Table 12: Nmap output examples

Command	Description
<code>nmap -p80 -sV -oG - --open 192.168.1.1/24 grep open</code>	Scan for web servers and grep to show which IPs are running web servers
<code>nmap -iR 10 -n -oX out.xml grep "Nmap" cut -d " " -f5 > live-hosts.txt</code>	Generate a list of the IPs of live hosts
<code>nmap -iR 10 -n -oX out2.xml grep "Nmap" cut -d " " -f5 >> live-hosts.txt</code>	Append IP to the list of live hosts
<code>ndiff scan1.xml scan2.xml</code>	Compare output from nmap using the ndif
<code>xsltproc nmap.xml -o nmap.html</code>	Convert nmap xml files to html files
<code>grep " open " results.nmap sed -r 's/ +/ /g' sort uniq -c sort -rn less</code>	Reverse sorted list of how often ports turn up

9.12 Miscellaneous Options

Table 13 shows some common Nmap switches, including a brief description and an example of how to use them.

Table 13: Namp miscellaneous options

Switch	Example	Description
-6	<code>nmap -6 2607:f0d0:1002:51::4</code>	Enable IPv6 scanning
-h	<code>nmap -h</code>	nmap help screen

9.13 Other useful nmap Commands

Table 14 shows some other useful Nmap commands that are useful for network discovery and host enumeration without performing a full port scan.

Table 14: Other useful Nmap commands

Command	Description
<code>nmap -iR 10 -PS22-25,80,113,1050,35000 -v -sn</code>	Discovery only on ports x, no port scan
<code>nmap 192.168.1.1-1/24 -PR -sn -vv</code>	ARP discovery only on local network, no port scan
<code>nmap -iR 10 -sn -traceroute</code>	Traceroute to random targets, no port scan
<code>nmap 192.168.1.1-50 -sL --dns-server 192.168.1.1</code>	Query the Internal DNS for hosts, list targets only

9.14 Debugging, Verbosity and Reason

- v**: Increase verbosity level, use **-vv** or more for greater effect.
- d**: Increase debugging level, use **-dd** or more for greater effect.
- reason**: Display the reason a port is in a particular state.

```
(kali㉿kali)-[~]
$ nmap 192.168.0.1 --reason -vv -d
Starting Nmap 7.80 ( https://nmap.org ) at 2021-05-26 14:11 IST
PORTS: Using top 1000 ports found open (TCP:1000, UDP:0, SCTP:0)
----- Timing report -----
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
-----
Initiating Ping Scan at 14:11
Scanning 192.168.0.1 [2 ports]
Completed Ping Scan at 14:11, 0.00s elapsed (1 total hosts)
Overall sending rates: 962.93 packets / s.
mass_rdns: Using DNS server 127.0.0.53
Initiating Parallel DNS resolution of 1 host. at 14:11
mass_rdns: 0.04s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 14:11, 0.04s elapsed
DNS resolution of 1 IPs took 0.04s. Mode: Async [#: 1, OK: 1, NX: 0,
DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 14:11
Scanning _gateway (192.168.0.1) [1000 ports]
Discovered open port 53/tcp on 192.168.0.1
Discovered open port 80/tcp on 192.168.0.1
Discovered open port 49152/tcp on 192.168.0.1
Completed Connect Scan at 14:11, 1.20s elapsed (1000 total ports)
Overall sending rates: 834.20 packets / s.
Nmap scan report for _gateway (192.168.0.1)
Host is up, received syn-ack (0.0057s latency).
Scanned at 2021-05-26 14:11:42 IST for 2s
Not shown: 994 closed ports
Reason: 994 conn-refused
PORT      STATE      SERVICE REASON
22/tcp    filtered  ssh      no-response
23/tcp    filtered  telnet   no-response
53/tcp    open       domain   syn-ack
80/tcp    open       http     syn-ack
111/tcp   filtered  rpcbind  no-response
49152/tcp open       unknown  syn-ack
Final times for host: srth: 5686 rttvar: 131  to: 100000

Read from /usr/bin/./share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 1.27 seconds
```

9.15 XML output

- **-oX <file>**: Output scan in format, using [dash] i.e. '-' in lieu of <file> redirects to standard out (**stdout**).
- **-p 22-1024**: The well-known port range.
- **-sV**: Enables version detection.

```
(kali㉿kali)-[~]
$ nmap -oX - -p 22-1024 -sV 192.168.0.1
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE nmaprun>
<?xml-stylesheet href="file:///usr/bin/../share/nmap/nmap.xsl"
type="text/xsl"?>
<!-- Nmap 7.80 scan initiated Tue Jul  6 09:52:09 2021 as: nmap -oX - -p 22-
1024 -sV 192.168.0.1 -->
<nmaprun scanner="nmap" args="nmap -oX - -p 22-1024 -sV 192.168.0.1"
start="1625561529" startstr="Tue Jul  6 09:52:09 2021" version="7.80"
xmloutputversion="1.04">
<scaninfo type="connect" protocol="tcp" numservices="1003" services="22-
1024"/>
<verbose level="0"/>
<debugging level="0"/>
<host starttime="1625561529" endtime="1625561536"><status state="up"
reason="syn-ack" reason_ttl="0"/>
<address addr="192.168.0.1" addrtype="ipv4"/>
<hostnames>
<hostname name="_gateway" type="PTR"/>
</hostnames>
<ports><extraports state="closed" count="998">
<extrareasons reason="conn-refused" count="998"/>
</extraports>
<port protocol="tcp" portid="22"><state state="filtered" reason="no-response"
reason_ttl="0"/><service name="ssh" method="table" conf="3"/></port>
<port protocol="tcp" portid="23"><state state="filtered" reason="no-response"
reason_ttl="0"/><service name="telnet" method="table" conf="3"/></port>
<port protocol="tcp" portid="53"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="domain" product="dnsmasq" version="2.78"
method="probed"
conf="10"><cpe>cpe:/a:thekelleys:dnsmasq:2.78</cpe></service></port>
<port protocol="tcp" portid="80"><state state="open" reason="syn-ack"
reason_ttl="0"/><service name="http" product="lighttpd" method="probed"
conf="10"><cpe>cpe:/a:lighttpd:lighttpd</cpe></service></port>
<port protocol="tcp" portid="111"><state state="filtered" reason="no-
response" reason_ttl="0"/><service name="rpcbind" method="table"
conf="3"/></port>
</ports>
<times srtd="5523" rttvar="178" to="100000"/>
</host>
<runstats><finished time="1625561536" timestr="Tue Jul  6 09:52:16 2021"
elapsed="7.53" summary="Nmap done at Tue Jul  6 09:52:16 2021; 1 IP address
(1 host up) scanned in 7.53 seconds" exit="success"/><hosts up="1" down="0"
total="1"/>
</runstats>
</nmaprun>
```


9.16 Use NMAP anonymously

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 proxychains
```

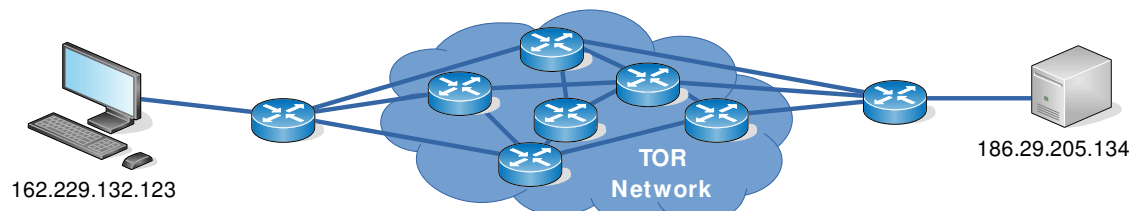


Figure 8: Using the TOR network

Consider the following **nmap** scan through a proxy chain via the TOR network. Some additional options here:

- **-sT**: TCP connect scan, instead of writing raw packets as most other scan types do, **nmap** asks the underlying OS to establish a connection with the target machine and port by issuing the connect system call. This more exactly simulates what network enabled applications would do. Basically, **nmap** is making use of the OS own Berkeley Socket API.

```
(kali@kali)-[~]
$ proxychains nmap -Pn -sT -p 22,80 186.29.205.134
```

```
ProxyChains-3.1 (http://proxychains.sf.net)
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-04 22:07 EAT
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK
Nmap scan report for 186.29.205.13
Host is up (0.61s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
```

Adding an additional option to detect the OS.:

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

```
(kali㉿kali)-[~]
$ proxychains nmap -Pn -sV -sT -p 22,80 186.29.205.134

ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-10 12:13 EAT
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK
|S-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
```

Attempt at SSH connection using user root failed but as it passed through the TOR network the attempt was anonymous.

```
(kali㉿kali)-[~]
$ proxychains ssh root@186.29.205.134

ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK
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).
```

On the server that the compromise attempt occurred check the authentication logs.

```
root@ece:~# tail /var/log/auth.log

Nov  4 19:09:26 ece sshd[1146]: Failed password for root from
207.244.70.35 port 45909 ssh2
Nov  4 19:09:33 ece sshd[1146]: Failed password for root from
207.244.70.35 port 45909 ssh2
Nov  4 19:09:40 ece sshd[1146]: Failed password for root from
207.244.70.35 port 45909 ssh2
Nov  4 19:09:40 ece sshd[1146]: Connection closed by 207.244.70.35
[preauth]
Nov  4 19:09:40 ece sshd[1146]: PAM 2 more authentication failures;
logname= uid=0 euid=0 tty=ssh ruser= rhost=207.244.70.35 user=root
```

Note the IP address from where the attempt connection originated, it is not from the source 62.229.132.123 but from 207.244.70.35 which is the edge of the TOR at that time for that connection.

9.16.1 SSH Public Key as possible Identifier in TOR

One thing to consider about making SSH connections through the TOR network is that by default the connection will attempt to authenticate using your public key first. If you have one and this has been made public then it could be an identifier if in the unlikely but possible even that someone is capturing the connection. To remove this possibility create a new public key first specify it in the SSH connection:

IP ADDRESS INFORMATION	
IP Address	207.244.70.35
Hostname	207.244.70.35
Network	--
Country	US - UNITED STATES
Region	MA
City	Lynn
Metro Code	506
Postal Code	01901
Area Code	781
Latitude	42.461
Longitude	-70.9463
IP Range	207.244.64.0 - 207.244.115.255
IP Network	American Registry for Internet Numbers (ARIN)

Figure 9: IP addressing info

```
(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+.. .         |
+-----+

```

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

ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-127.0.0.1:9050-<>-186.29.205.134:22-<>-OK
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

```

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
Nov 10 09:46:13 ece sshd[21708]: pam_unix(sshd:auth): authentication failure;
logname= uid=0 euid=0 tty=ssh ruser= rhost=43.229.53.25 user=root
Nov 10 09:46:15 ece sshd[21708]: Failed password for root from 43.229.53.25
port 28216 ssh2
Nov 10 09:46:17 ece sshd[21708]: Failed password for root from 43.229.53.25
port 28216 ssh2
Nov 10 09:46:19 ece sshd[21708]: Failed password for root from 43.229.53.25
port 28216 ssh2
Nov 10 09:46:19 ece sshd[21708]: Received disconnect from 43.229.53.25: 11:
[preauth]
Nov 10 09:46:19 ece sshd[21708]: PAM 2 more authentication failures; logname=
uid=0 euid=0 tty=ssh ruser= rhost=43.229.53.25 user=root

```

Each time the source is a different address as the exit point from TOR changes.

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)

Figure 10: Source for connections through TOR

10 OT Network Security, Scanning and Enumeration with NMAP

10.1 The Problem with Scanning Legacy Devices

Scanning legacy ACS can result in device freezing or even permanent malfunction (commonly referred to as "*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. This design approach renders them more susceptible to cyber threats. Given their integration into Critical National Infrastructure (CNI), any compromise, even as minimal as an NMAP scan, carries potentially severe consequences. Safeguarding these systems against such risks is paramount.

Adversaries are indifferent to a device's resistance to scanning; their objective is to infiltrate the network and enumerate connected devices. Regardless of a device's robustness to scanning, determined adversaries seek unauthorised access to the network, emphasising the critical importance of comprehensive security measures to thwart potential breaches.

10.2 Scanning ACS in a Penetration Test

To conduct or abstain from scanning poses a critical decision. An NMAP scan functions as a practical stress test for your OT, revealing its response to such probing. It serves as a way to gauge the system's resilience under simulated scanning conditions. However, caution must be exercised due to potential negative impacts on system stability and functionality during the scanning process. A thorough evaluation of the benefits and risks of scanning is vital before proceeding, ensuring that the benefits outweigh the potential disruptions or damage that may occur. Ultimately, informed judgment and readiness are essential in making an appropriate decision regarding scanning.

10.2.1 Never scan a live system

Prioritise obtaining appropriate permissions before initiating any network scan. It is crucial to restrict scanning activities to instances when the target is in a maintenance or downtime phase. This precaution ensures that the scanning process doesn't interfere with active operations or disrupt critical services. Timing the scan with precision is essential to minimise any potential impact on the target system's performance. Adhering to this practice safeguards against unintended consequences and aligns with responsible scanning procedures. Always exercise caution and the target system before proceeding with a network scan.

10.2.2 Scan Option: Timing -Tx

Enhancing the scan's safety involves leveraging the timing options provided by NMAP. Utilise the **-T** option followed by a number ranging from 0 to 5 to tailor the scan's aggressiveness and mitigate risks. For OT environments, a recommended approach is to opt for either **-T1** or **-T2** to strike a balance between thoroughness and caution. However, if the intent is to stress-test the system, consider the more aggressive option, **-T5**, for a rigorous and exhaustive assessment. Choose the appropriate timing option in line with the specific security and operational requirements of the OT network.

10.2.3 Scan Option: Full TCP handshake -sT

Another measure to enhance scanning safety involves utilising the **-sT** option in NMAP. This option specifies a TCP connect scan, which is generally safer than other scan types. **-sT** establishes a full TCP connection with the target, minimising the chance of disrupting services or causing system damage during the scan. When conducting scans in sensitive OT environments, prioritising safety through a TCP connect scan is recommended to reduce potential negative impacts while still gaining valuable insights into the target network.

10.2.4 Scan Option: Limit parallel probing

Utilising the **--max-parallelism 1** option in the scan configuration limits the parallel operations to one at a time. This setting minimises the load on the target system, significantly reducing the risk of disruptions or potential damage during the scan. In OT environments, where cautious scanning is vital, employing this option ensures a meticulous and safe scanning process, aligning with the imperative to prioritise system stability and security.

10.3 Quiz

1. Which scan timing options are recommended for OT environments to balance thoroughness and caution?
☐ **-T1** ☐ **-T2** ☐ **-T3** ☐ **-T4** ☐ **-T5**
2. What does the **-sT** option in NMAP signify for enhancing scanning safety in OT networks?
☐ UDP Connect Scan ☐ TCP Connect Scan ☐ SYN Stealth Scan
3. 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.

10.4 ACS Specific scripts for NSE

The NSE is a powerful and advanced functionality within NMAP, and it can be enhanced by adding more OT specific scripts to the NMAP Scripting Engine from github. To integrate a collection of ICS enumeration tools from the Redpoint repository, clone this repository into the NMAP script folder:

```
(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

(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
```

10.5 Exercise #10.2

Carry out a pen-test reconnaissance on the IP address given to you by the lecturer.

This page is intentionally blank