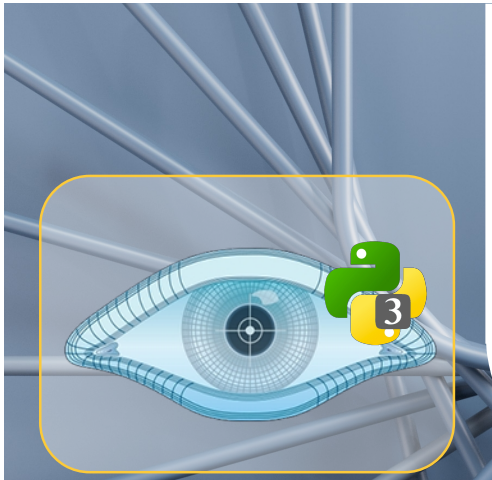


Penetration Testing (Reconnaissance)

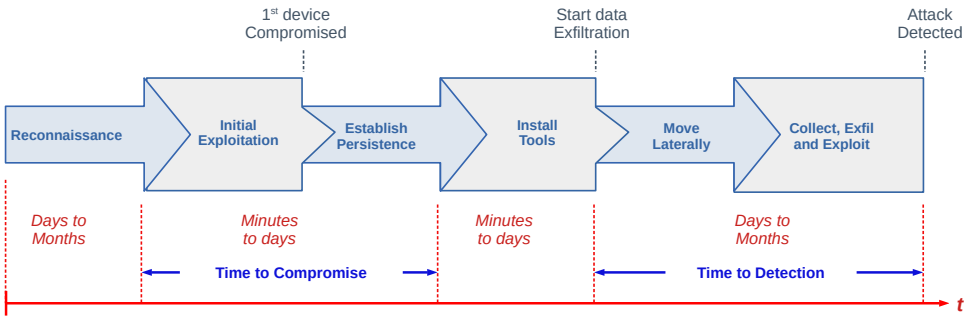
Dr Diarmuid Ó Briain

30 Oct 2023

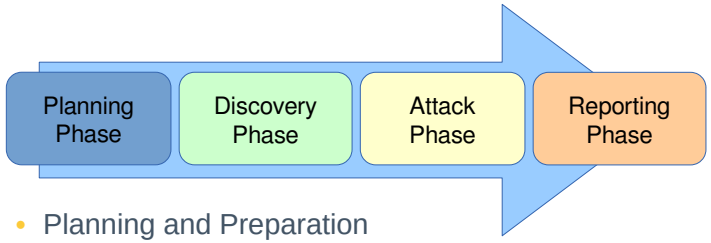
Learning objectives

- The Anatomy of a Cyber attack
- Introduction to Penetration testing
- Kali Linux
- Using `nmap` for reconnaissance

Anatomy of a Cyber attack



What steps are used to carry out pen test



- Planning and Preparation
- Information Gathering and Analysis
- Vulnerability Detection
- Penetration attempt
- Analysis and Reporting
- Cleaning up

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.

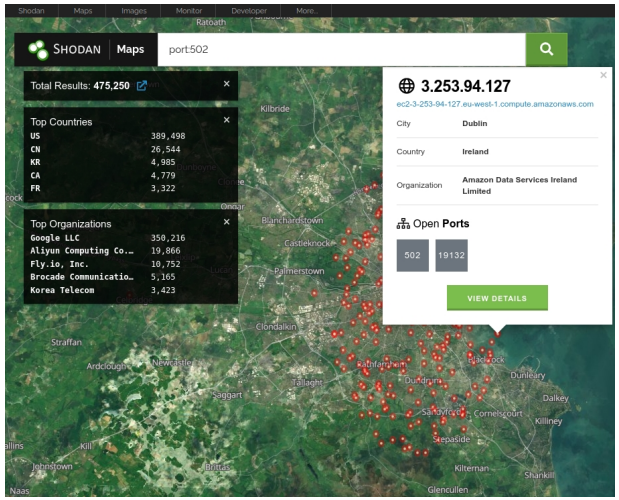
Tidy up

- 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



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
  - IACS
  - 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

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

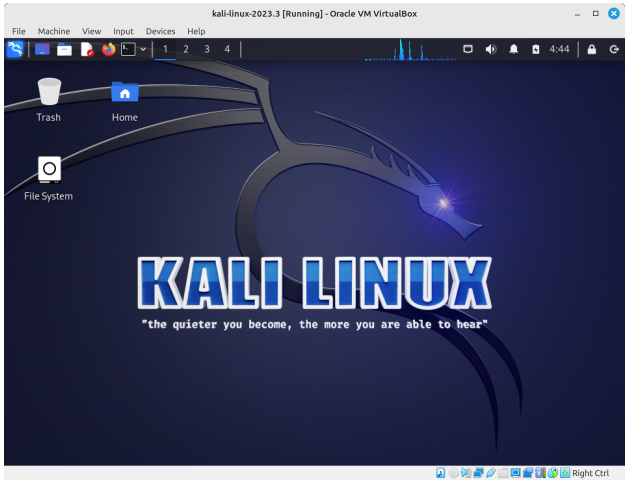
Exercise #9.1

Exercise #9.1

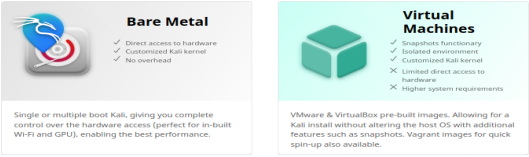
- Create a personal Shodan account.
- Login to Shodan.
- Discover the TCP port number for the DNP3 protocol.
- Search for DNP3 in the Ireland and copy down the information relating to the nearest one to your current location.
  - Who owns it?
  - What is the device?
  - What is the device Internet Protocol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

KALI

Kali Linux Desktop



Kali Linux Install



- Plus:
  - ARM: Raspberry Pi
  - Mobile: Android
  - Cloud: AWS
  - Containers: Docker and LXC/LXD
  - Live boot: USB
- Default user (**`kali`**) and pass (**`kali`**).

```
https://www.kali.org
https://www.kali.org/get-kali
```

Upgrading Kali Linux

- System update and upgrade

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


Kali Linux keyboard

- System upgrade

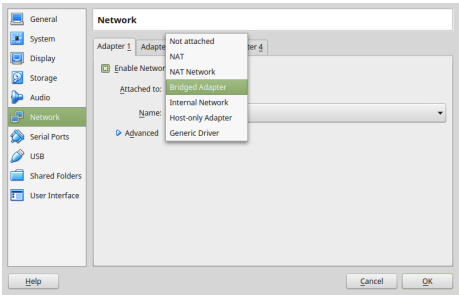
```
┌──(kali㉿kali)-[~]
└─$ setxkbmap -layout gb

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


Kali Linux network

- Network Address

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

- NAT or Bridged Adaptor



VirtualBox guest additions

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

Clean and reboot

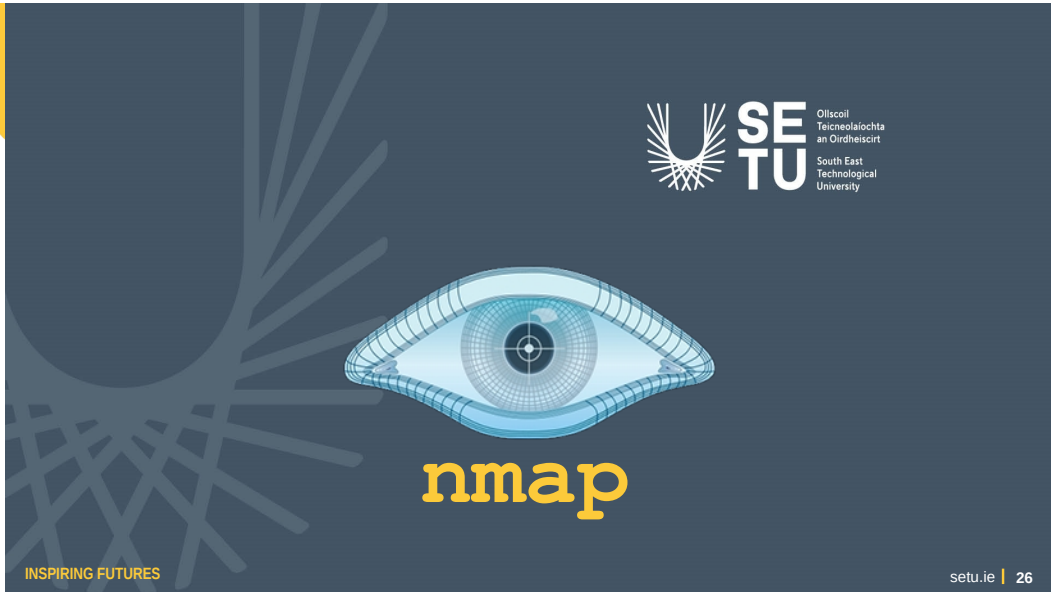
- Clean packages no longer required

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

- Reboot

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

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

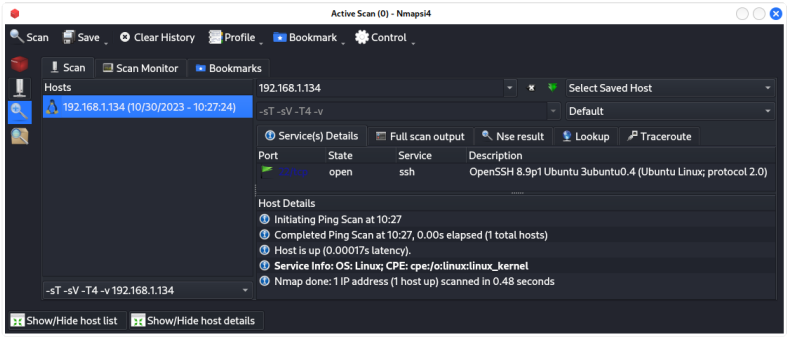
Network Mapper (`nmap`)

- 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.

`nmapsi4`

- `nmapsi4` graphical utility

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



Installing nmap

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

```
┌──(kali㉿kali)-[~]
└─$ python3 -m pip install
```

```
┌──(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
```


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.

Testing with nmap

```
┌──(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
```


Testing with nmap

```
┌──(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
```

Testing and Scan techniques with `nmap`

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

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

Scan techniques – TCP SYN 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
```


Host discovery

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

Port specification

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

Service and Version Detection

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

Operating System Detection

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

Timing

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

Performance

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<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

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

Useful NSE Scripts

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

Firewall / IDS Evasion and Spoofing

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

Output

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

Output

- Scan for web servers and grep to show which IPs are running web servers

```
┌──(kali㉿kali)-[~]
└─$ nmap -p80 -sV -oG - --open 192.168.1.1/24 | grep open
```

- Generate a list of the IPs of live hosts

```
┌──(kali㉿kali)-[~]
└─$ nmap -iR 10 -n -oX out.xml | grep "Nmap" | cut -d " " -f5 >
  live-hosts.txt
```

- Append IP to the list of live hosts

```
┌──(kali㉿kali)-[~]
└─$ nmap -iR 10 -n -oX out2.xml | grep "Nmap" | cut -d " "
  -f5 >> live-hosts.txt
```


Output

- Compare output from **nmap** using the **ndiff**

```
┌──(kali㉿kali)-[~]
└─$ ndiff scanl.xml scan2.xml
```

- Convert **nmap xml** files to **html** files

```
┌──(kali㉿kali)-[~]
└─$ xsltproc nmap.xml -o nmap.html
```

- Reverse sorted list of how often ports turn up

```
┌──(kali㉿kali)-[~]
└─$ grep " open " results.nmap | sed -r 's/ +/ /g' |
  sort | uniq -c | sort -rn | less
```


Miscellaneous and other useful commands

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

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

Debugging, Verbosity and Reason

```
┌──(kali㉿kali)-[~]
└─$  nmap 192.168.0.1 --reason -vv -d
Starting Nmap 7.80 ( https://nmap.org ) at 2021-07-06 09:14 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 09:14
Scanning 192.168.0.1 [2 ports]
Completed Ping Scan at 09:14, 0.00s elapsed (1 total hosts)
Overall sending rates: 1096.49 packets / s.
mass_rdns: Using DNS server 127.0.0.53
Initiating Parallel DNS resolution of 1 host. at 09:14
mass_rdns: 0.02s 0/1 [#: 1, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 09:14, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 1, OK: 1, NX: 0, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 09:14
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 09:14, 1.20s elapsed (1000 total ports)
Overall sending rates: 834.29 packets / s.
Nmap scan report for _gateway (192.168.0.1)
Host is up, received syn-ack (0.0088s latency).
Scanned at 2021-07-06 09:14:58 IST for 1s
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: srtt: 8831 rttvar: 411  to: 100000

Read from /usr/bin/../share/nmap: nmap-payloads nmap-services.
Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
```

-d: Increase debugging level
-v: Increase verbosity level
--reason: Reason a port is in a particular state

Try **-dd**, **-ddd** and **-vv**, **-vvv**

XML Output

```
┌──(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 srtt="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>
```

-oX <file>: Output scan in format
-[dash] in lieu of **<file>** redirects to **stdout**.
-p 22-1024: The well-known port range.
-sV: Enables version detection.

Anonymous use of nmap

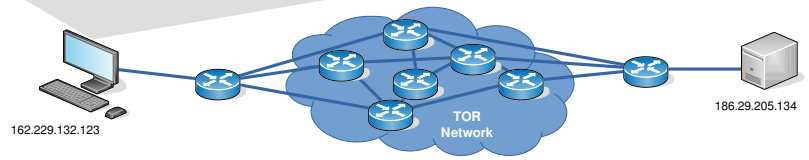
- For anonymous use of nmap it is possible to do so using “The Onion Router” (TOR) and ProxyChains.
- ProxyChains redirects TCP connections through proxy servers.

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


Anonymous use of nmap

```
┌──(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-<><>-186.29.205.134:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK
Nmap scan report for li489-237.members.linode.com (186.29.205.134)
Host is up (0.61s latency).
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

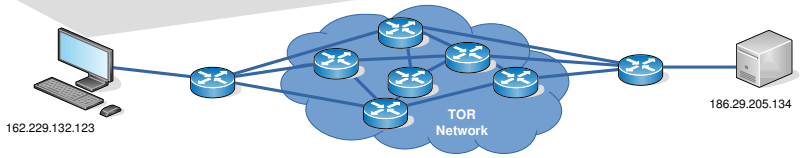
-sT:
TCP connect scan via the OS own Berkeley Socket API.



Anonymous use of nmap

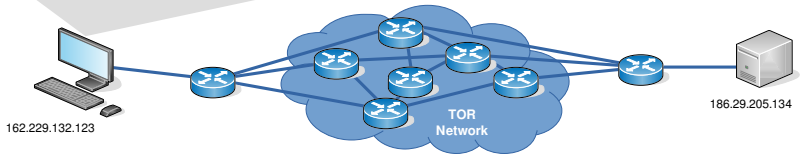
```
┌──(kali㉿kali)-[~]
└─$ proxychains nmap -Pn -sV -sT -p 22,80 186.29.205.134
ProxyChains-3.1 (http://proxychains.sf.net)

Starting Nmap 6.40 ( http://nmap.org ) at 2015-11-04 22:07 EAT
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:80-<><>-OK
|S-chain|-<>-127.0.0.1:9050-<><>-186.29.205.134:22-<><>-OK
Nmap scan report for li489-237.members.linode.com (186.29.205.134)
Host is up (0.61s latency).
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

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



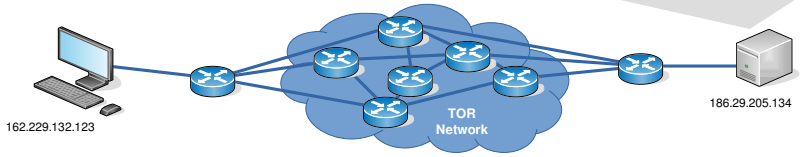
Anonymous use of nmap

```
┌──(kali㉿kali)-[~]
└─$ 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).
```



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
```

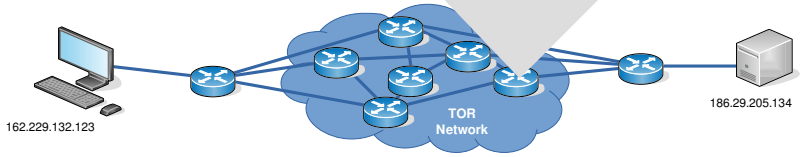


Anonymous use of nmap

- whois: 207.244.70.35
- Edge of the TOR network

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)



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)-[~]
└─$  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
```


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 and OT

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 IACS are primarily engineered for real-time functionality, lacking inherent security features.
- Even as minimal as an NMAP scan, carries potentially severe consequences

Scanning IACS 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**

IACS 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
```


IACS 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
```

Learning objectives

- The Anatomy of a Cyber attack ✓
- Introduction to Penetration testing ✓
- Kali Linux ✓
- Using nmap for reconnaissance ✓

Exercise #9.2

Answer the following questions

- 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.

Answer the following questions

- 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.

Answer the following questions

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

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

EUR ING Dr Diarmuid Ó Briain
Innealtóir Cairte agus Léachtóir

D +353 59 917 5426 | E diarmuid.obriain@setu.ie | **setu.ie**
Campas Bhóthar Chill Chainnigh, Ceatharlach, R93 V960, Éire

Ollscoil Teicneolaíochta an Oirdheiscirt
South East Technological University

engcore
advancing technology