

COS30015 – Lab 6

nmap

Presented by Jamie Ooi

jooi@swin.edu.au

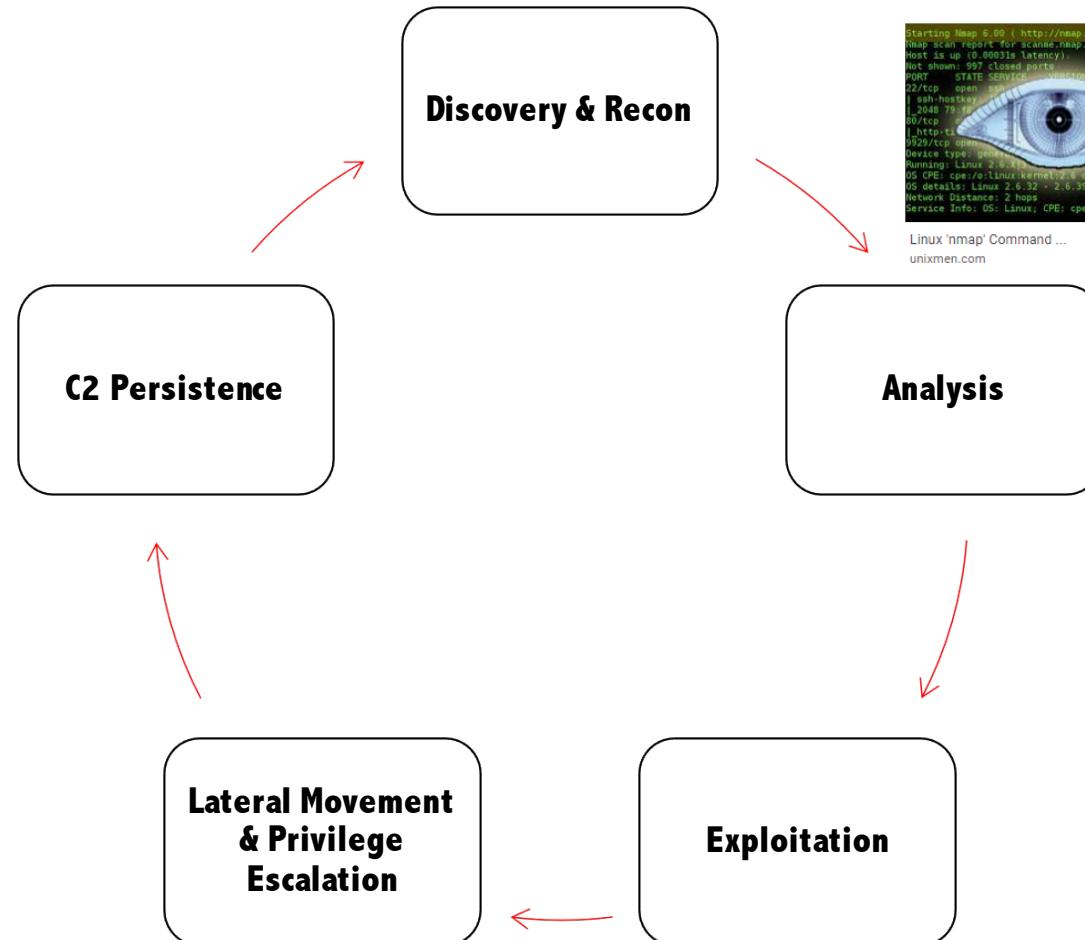
Thursday 8 September, 2022



developers to connect over code ...
devrant.com

COS30015 IT Security – Lab 6 Background

Red Team Methodology



Lab 6 – Network Mapping

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-05-17 12:54+00  
Nmap scan report for scanme.nmap.org (74.207.244.221)  
Host is up (0.0003s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
22/tcp    open  ssh  
|_ssh-hostkey: 1024 bits, SHA-1 digest: 67:54:96  
| 2048 79:fa:4d:1c:4e:3f:00:00:00:00:00:00:00:00:00:00  
| 443/tcp  open  https  
|_http-title: Linux  
| 8029/tcp open  http  
Device type: general purpose  
Running: Linux 2.6.32  
OS CPE: cpe:/o:linux:kernel:2.6  
OS details: Linux 2.6.32 - 2.6.39, Linux 2.6.38 - 3.6  
Network Distance: 2 hops  
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel  
  
Linux 'nmap' Command ...  
unixmen.com
```

COS30015 IT Security – Lab 6 Background

Nmap “Network Mapper”

Penetration Tester SWISS Army Knife



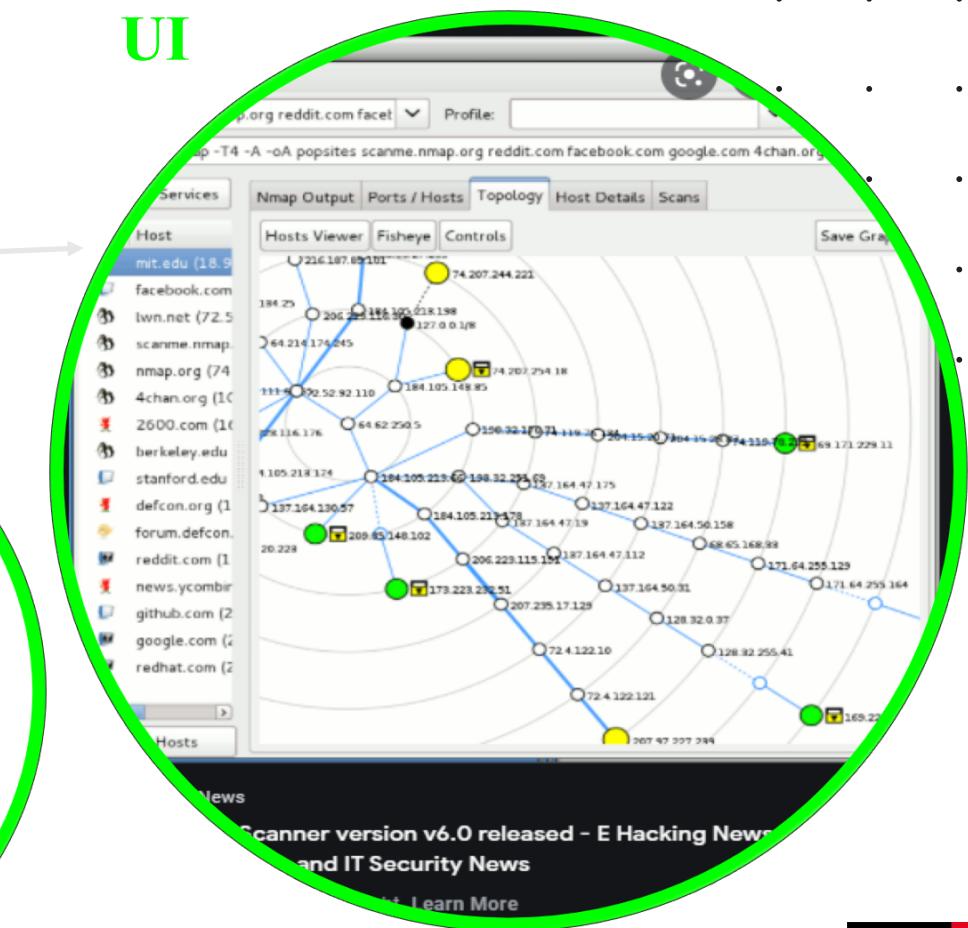
CLI

```
bratch * nmap -T5 -sV -O localhost
Nmap 4.53 ( http://insecure.org ) at 2008-03-12 19:07
Scanning ports on localhost (127.0.0.1);
Host count: 1709 closed ports
      STATE SERVICE VERSION
      open  ftp    vsftpd 2.0.5
  2/tcp  open  ssh    OpenSSH 4.7 (protocol 2.0)
  0/tcp  open  http   Apache httpd
  443/tcp open  ssl/http Apache httpd
  10000/tcp open  http   Webmin httpd
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.17 - 2.6.21
Uptime: 0.136 days (since Wed Mar 12 15:52:05 2008)
Network Distance: 0 hops
Service Info: OS: Unix

done; 1 IP address (1 host up) scanned in 13,241 seconds
-2ddektop bratch *
```

Mikidata

UI



COS30015 IT Security – Lab 6 Background



knock knock, "who's there?" N...
memegenerator.net

Nmap “Network Mapper”

- Free security scanner
- Scans and *fingerprints* specified IP address(es) and ports
- TCP and UDP scans using, Ping, SYN, ARP, FIN
- Returns the available ports, services, software packages, Operating Systems
- Ability to write and run scripts including providing arguments
- Interacts with available services
- Ability to configure scans including speed, stealth
- Outputs in .nmap, .xml, or greppable .txt

COS30015 IT Security – Lab 6 Background



COS30015 IT Security – Lab 6 Background

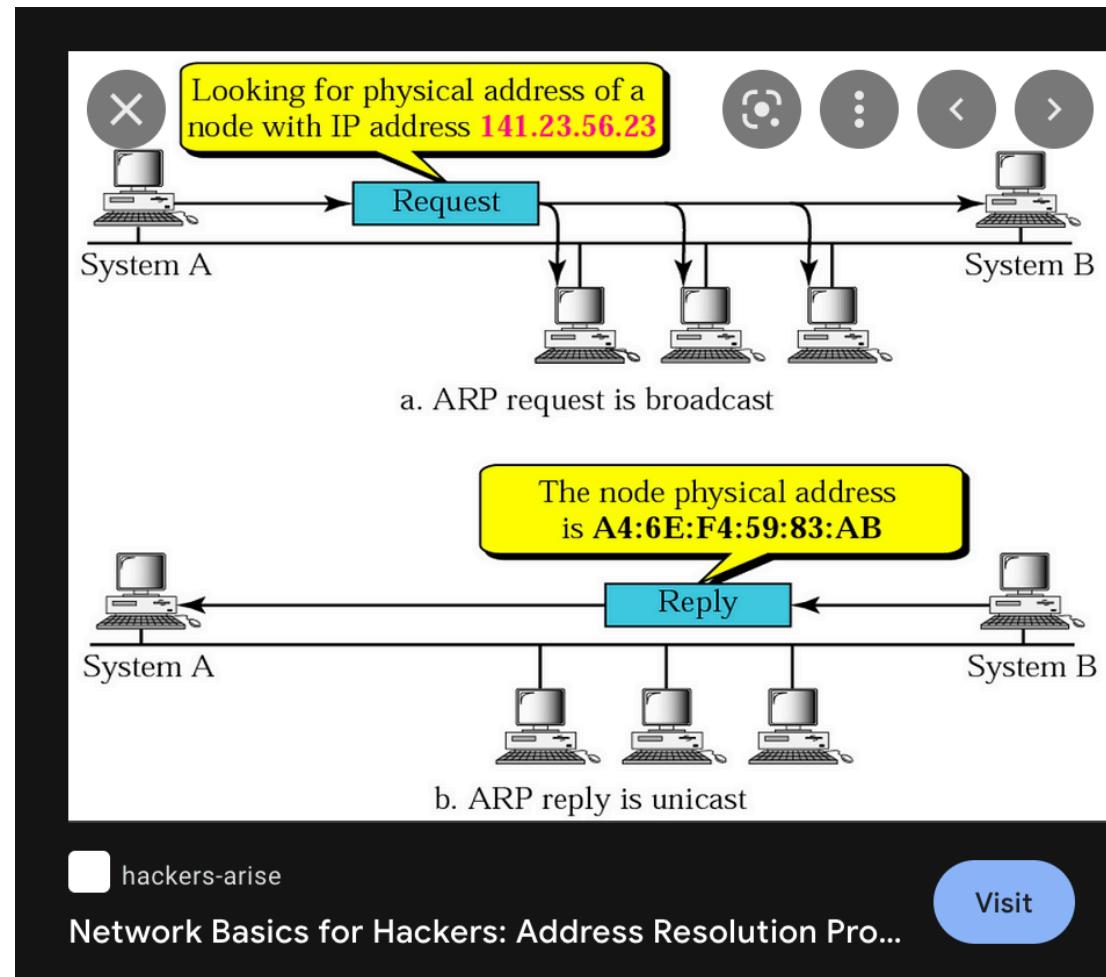
Where are you authorised to use penetration testing tools:

- Pentesterlab: <https://pentesterlab.com/>
- Hackthebox: <https://www.hackthebox.eu/>
- Overthewire: <https://overthewire.org/wargames/>
- DownUnderCTF: <https://downunderctf.com/>
- BugCrowd: <https://www.bugcrowd.com/>
- HackerOne: <https://www.hackerone.com/>
- Many others

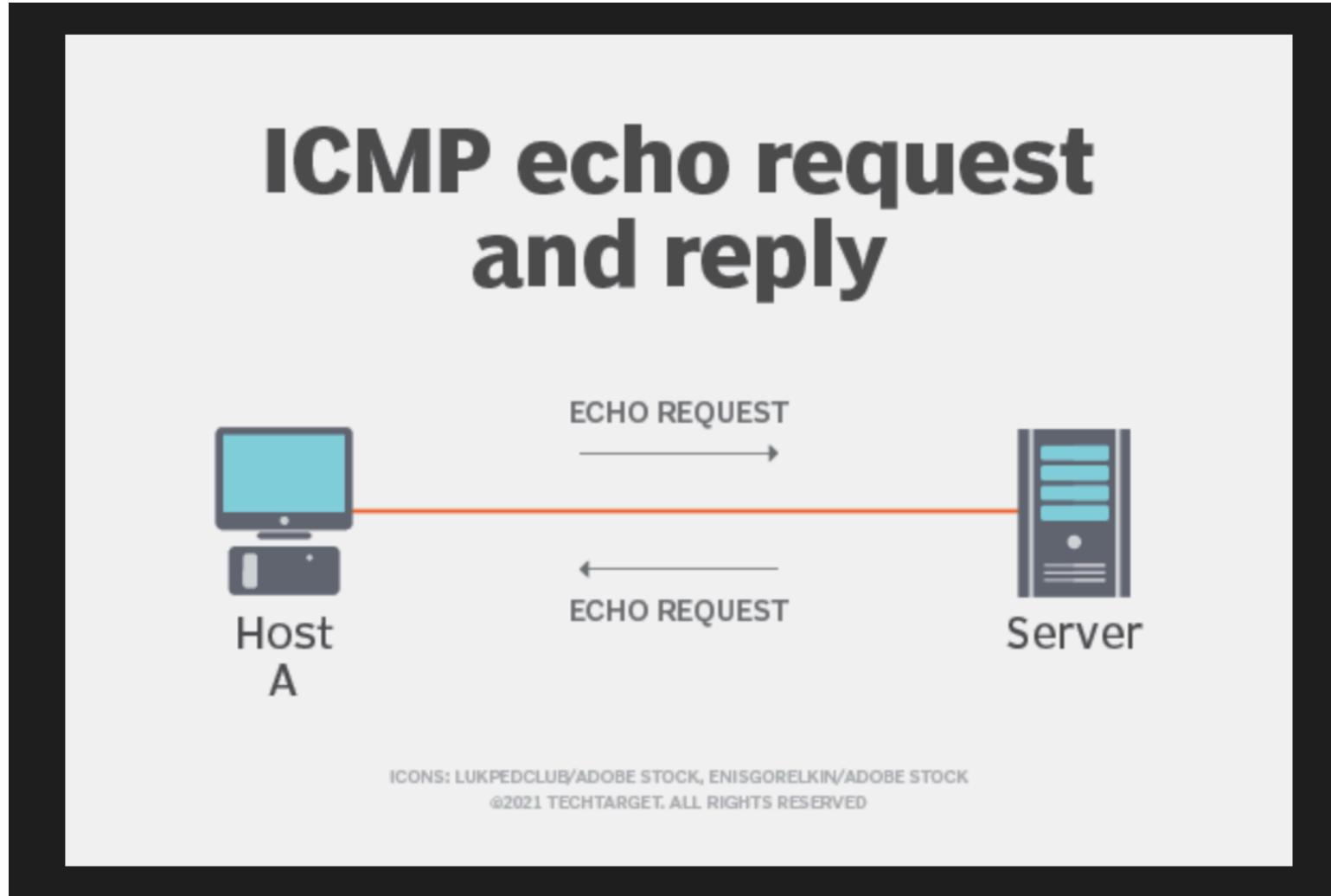


COVID Victoria: Children and parents ...
theage.com.au

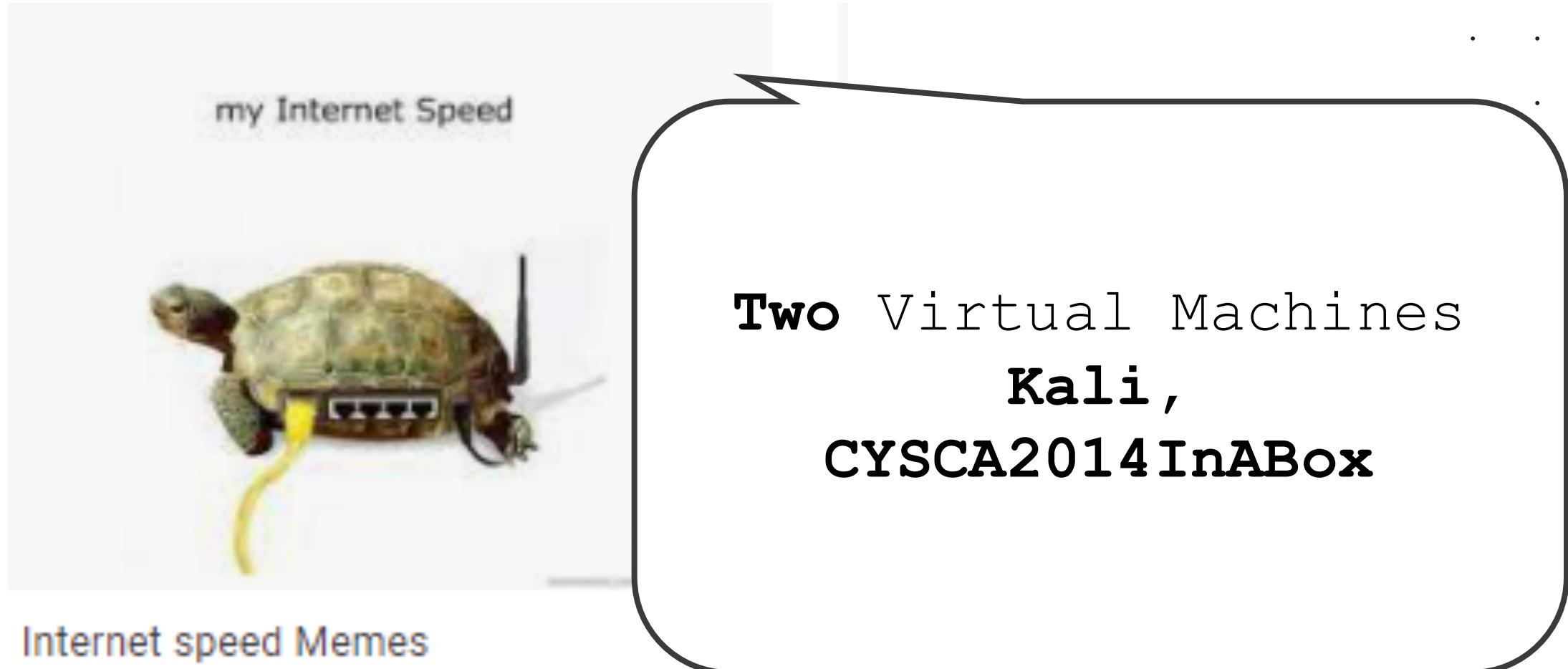
COS30015 IT Security – Lab 6 Background



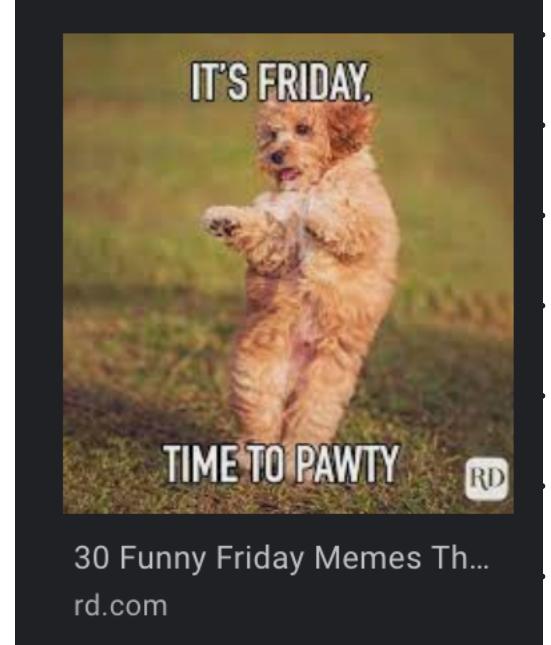
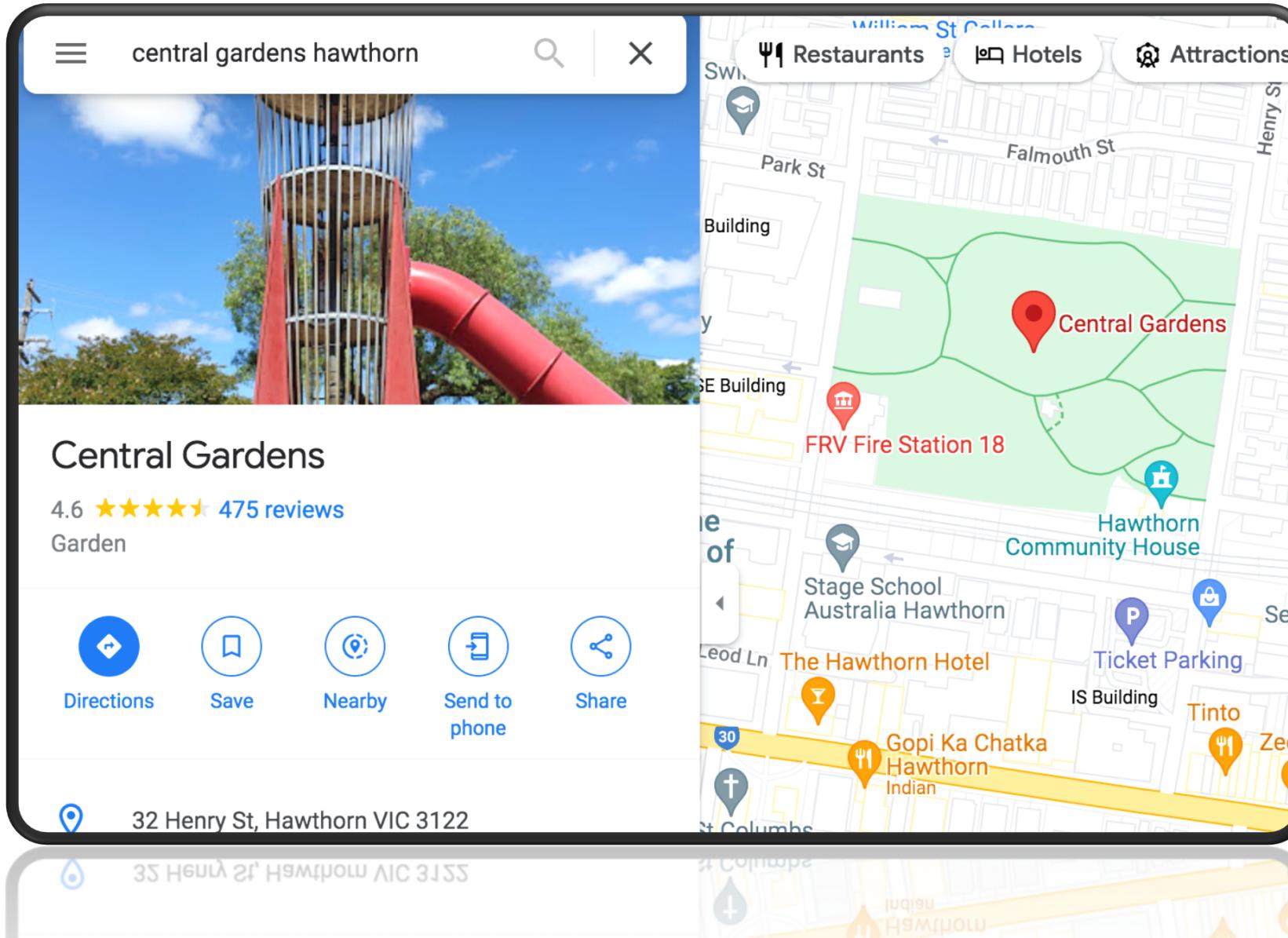
COS30015 IT Security – Lab 6 Background



COS30015 IT Security – Lab 6 Background



COS30015 IT Security – Mid Term Party



IT Security Mid Term Party

Friday the 30th September
From 4:30pm onwards
Sausage sizzle, drinks and war stories

Invite your other infosec friends ☺

Questions ?

Email: jooi@swin.edu.au

Linkedin: <https://www.linkedin.com/in/jamie-ooi-15297b98/>

Thursday 8 September, 2022

Most used nmap commands

Nmap cheatsheet

nmap <timing> <scan type> <target> <port> <script> <output type>	Most used nmap arguments Timing: T0 Paranoid, T1 Sneaky, T2 Polite, T3 Standard (Default), T4 Aggressive, T5 Insane
nmap -T4 -A -iL <targets-filename> -p- -oA <output-filename>	Run ALL tests on ALL TCP ports for specified targets in provided file and generate output in all formats in specified output filename
nmap -sn <target-subnet>	Ping scan of specific target subnet This is used for identify live hosts on that subnet
nmap -sV -O <target>	Service detection and Operating System detection for specified target on top 100 most common ports
nmap -T4 -sV -O -iL <targets-filename> -p 80,443,139,445 -oA <output-filename>	When ICMP ping is disabled, you can specify commonly available ports on your target servers to identify live hosts E.g. Windows servers usually have ports 139 (netbios) and 445 (smb) available Cisco switches usually have port 22 (ssh) and 161 (snmp) available
nmap -sU <targets>	Scan most common UDP ports available on specific targets
nmap --script-help	Provided information for the specific script
nmap -T4 -sV -O <target> -p 80,443 --script=http*	Run all http scripts on specified target