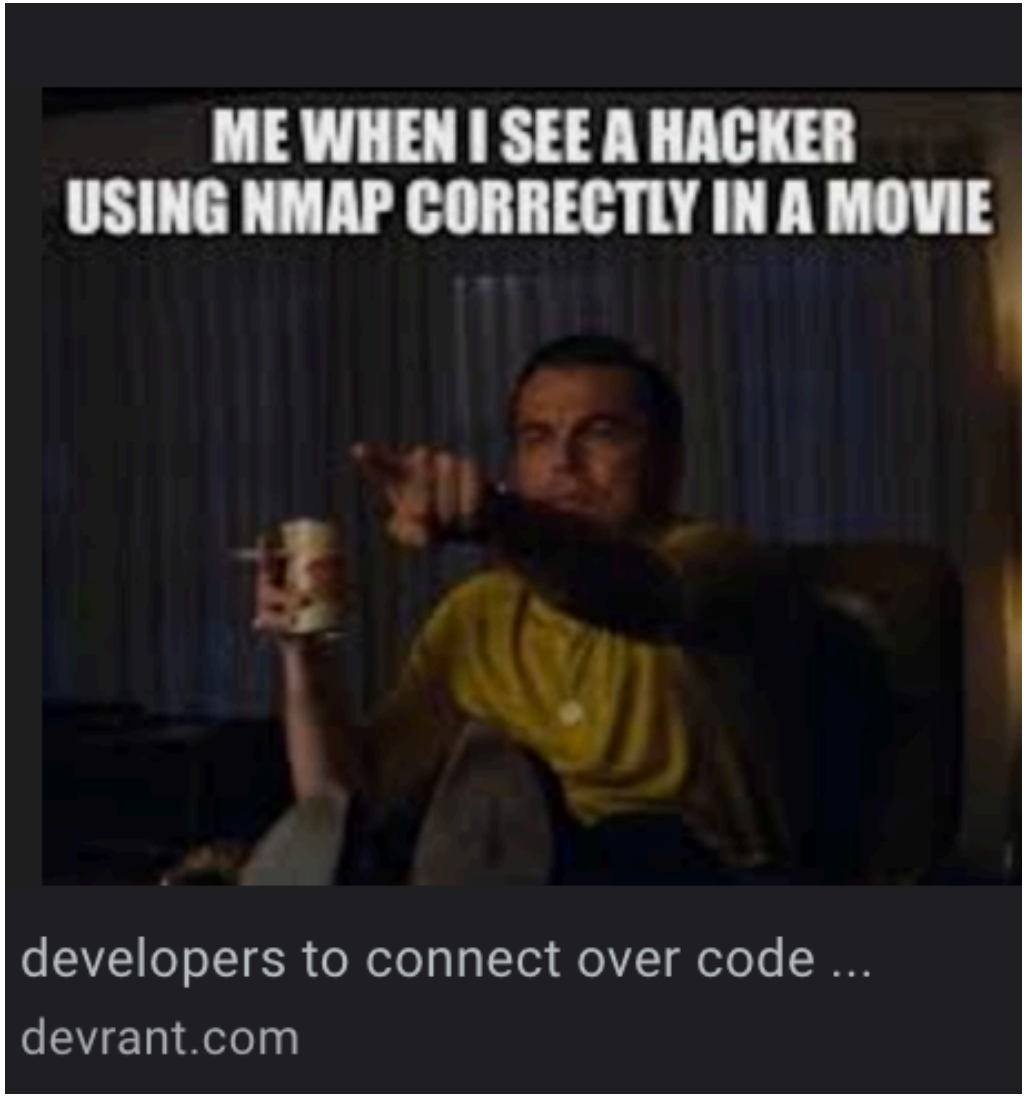
COS30015 – Lab 6

nmap

Presented by Jamie Ooi

jooi@swin.edu.au

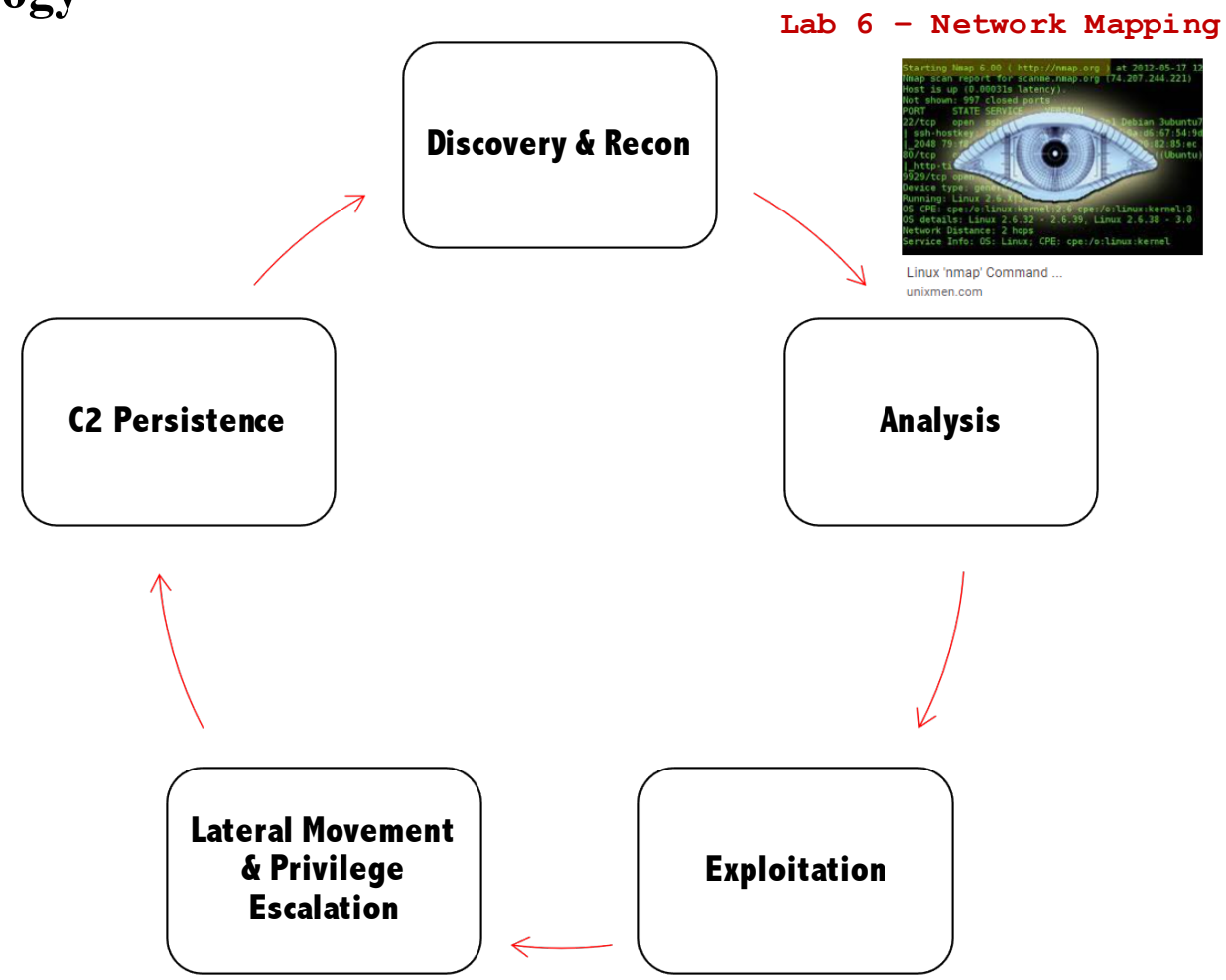
Thursday 8 September, 2022



SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 6 Background

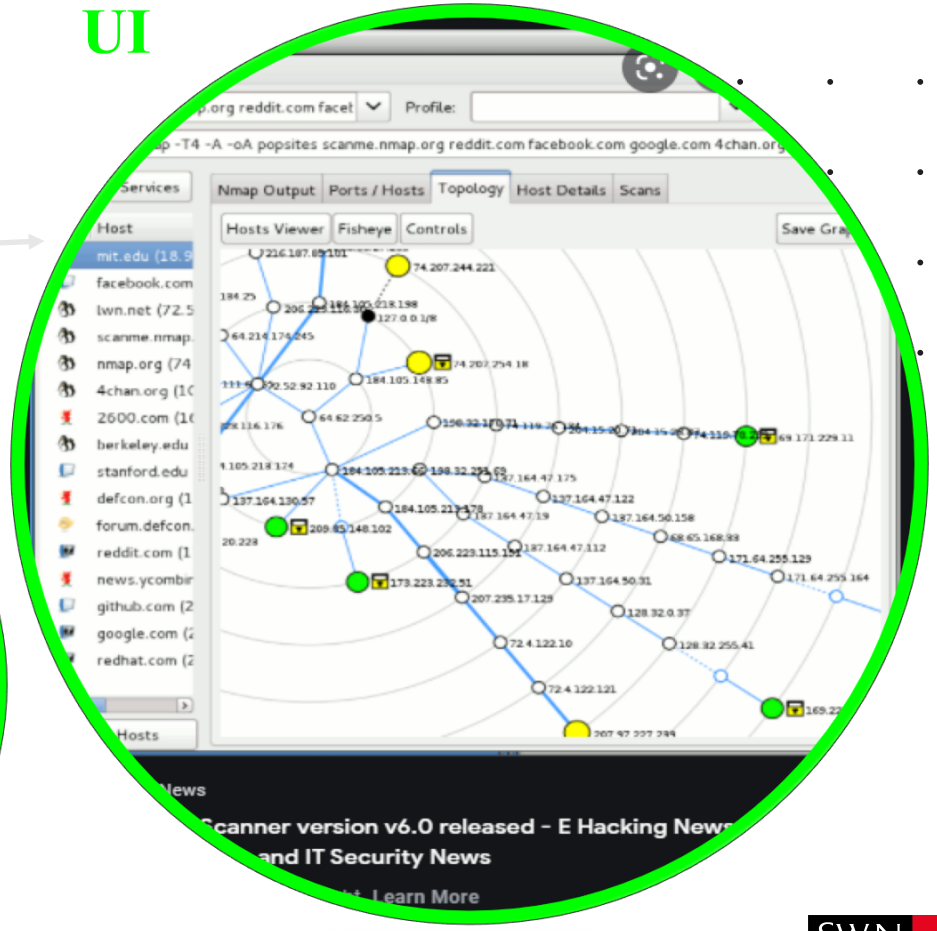
Red Team Methodology



COS30015 IT Security – Lab 6 Background

Nmap "Network Mapper"

Penetration Tester SWISS Army Knife



UI

CLI

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

COS30015 IT Security – Lab 6 Background

IT CAN BE CONSIDERED A CRIME

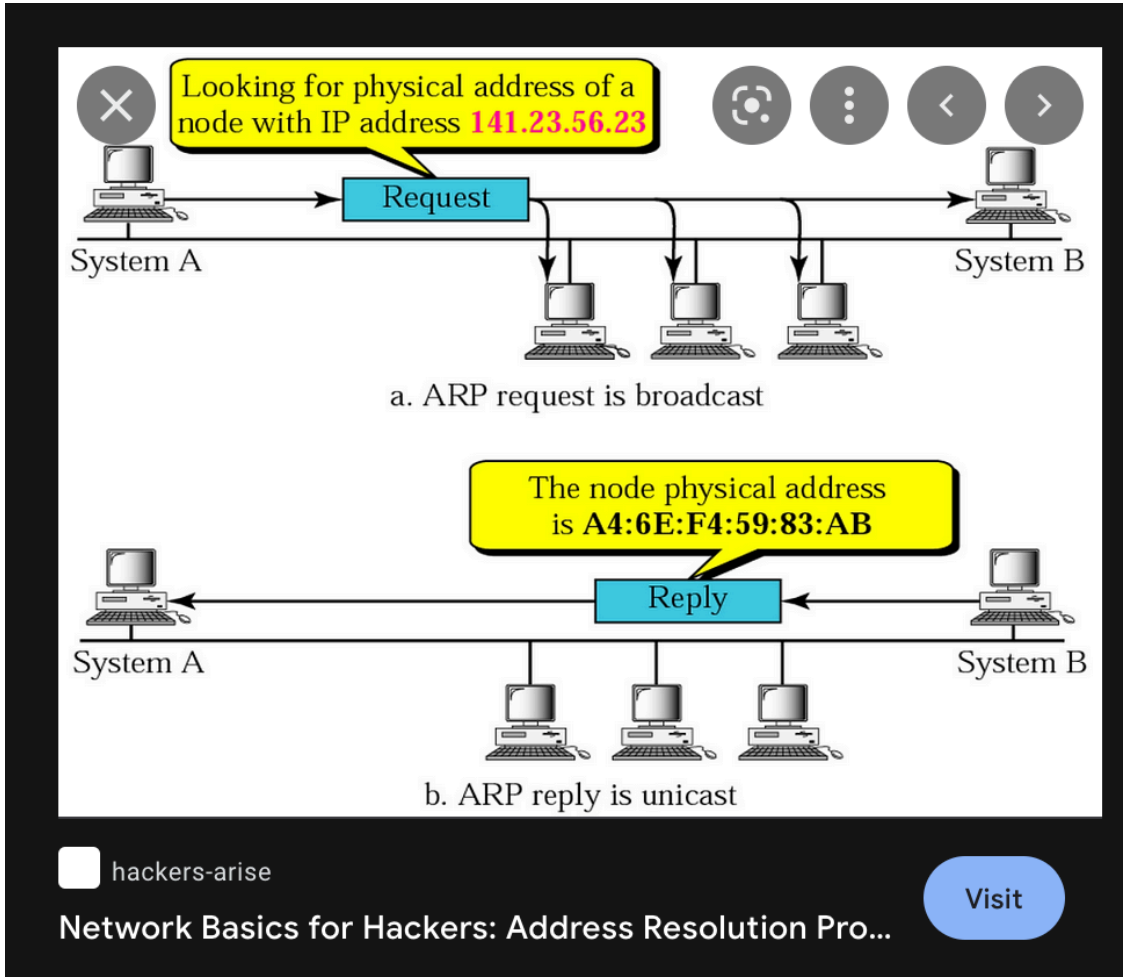
COS30015 IT Security – Lab 6 Background

Where are you authorised to use penetration testing tools:

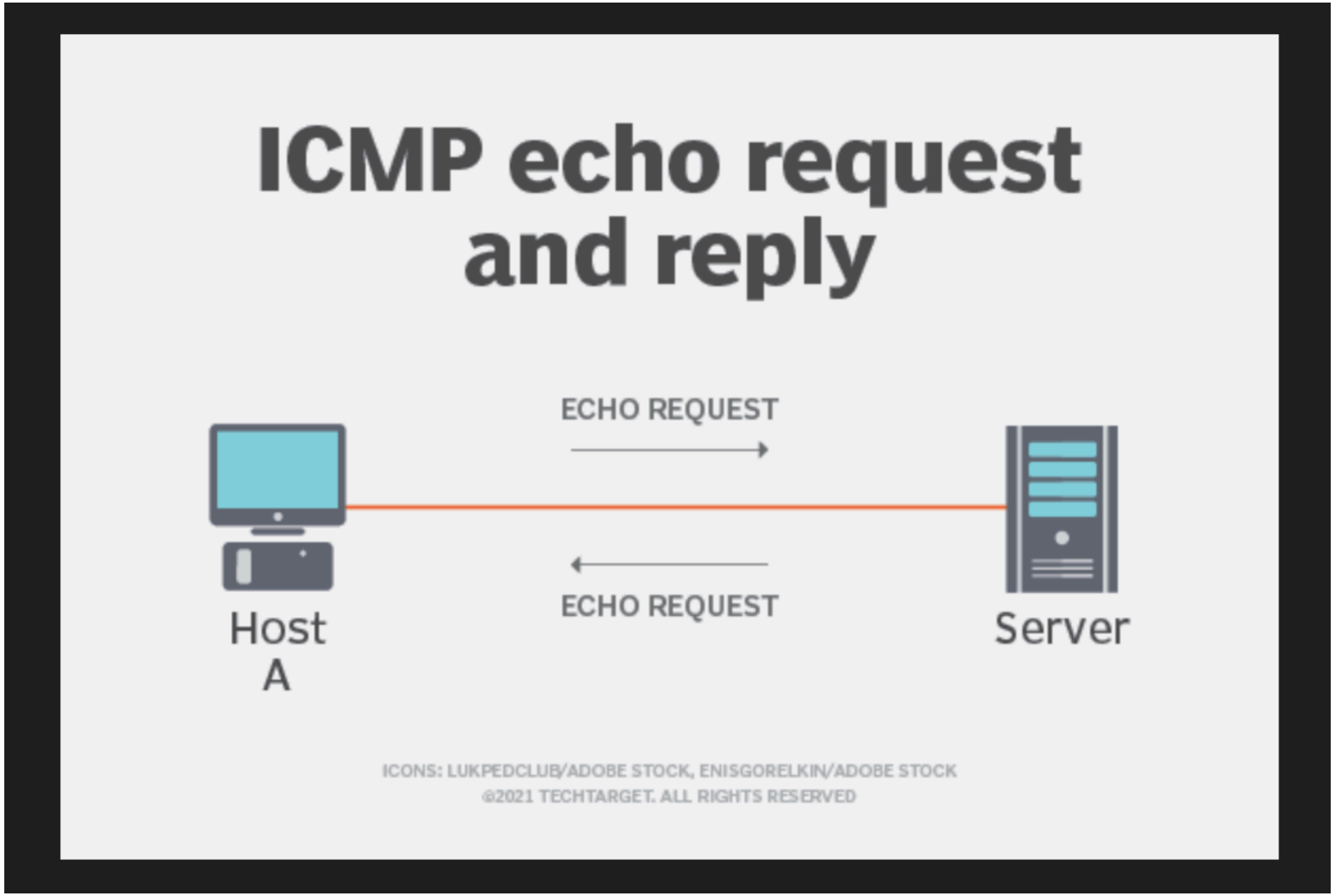
- Pentesterlab: https://pentesterlab.com/
- Hackthebox: https://www.hackthebox.eu/
- Overthewire: https://overthewire.org/wargames/
- DownUnderCTF: https://downunderctf.com/
- BugCrowd: https://www.bugcrowd.com/
- HackerOne: https://www.hackerone.com/
- Many others

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

COS30015 IT Security – Lab 6 Background

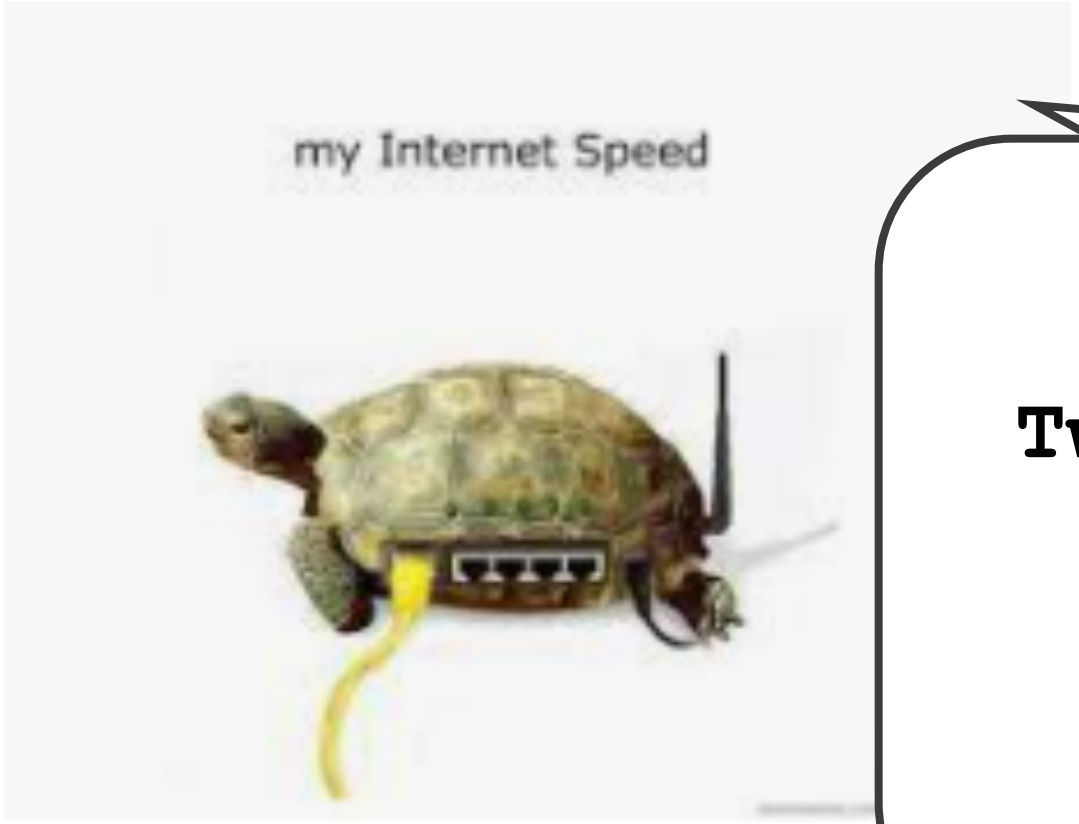


COS30015 IT Security – Lab 6 Background



https://www.techtarget.com/searchnetworking/definition/ping

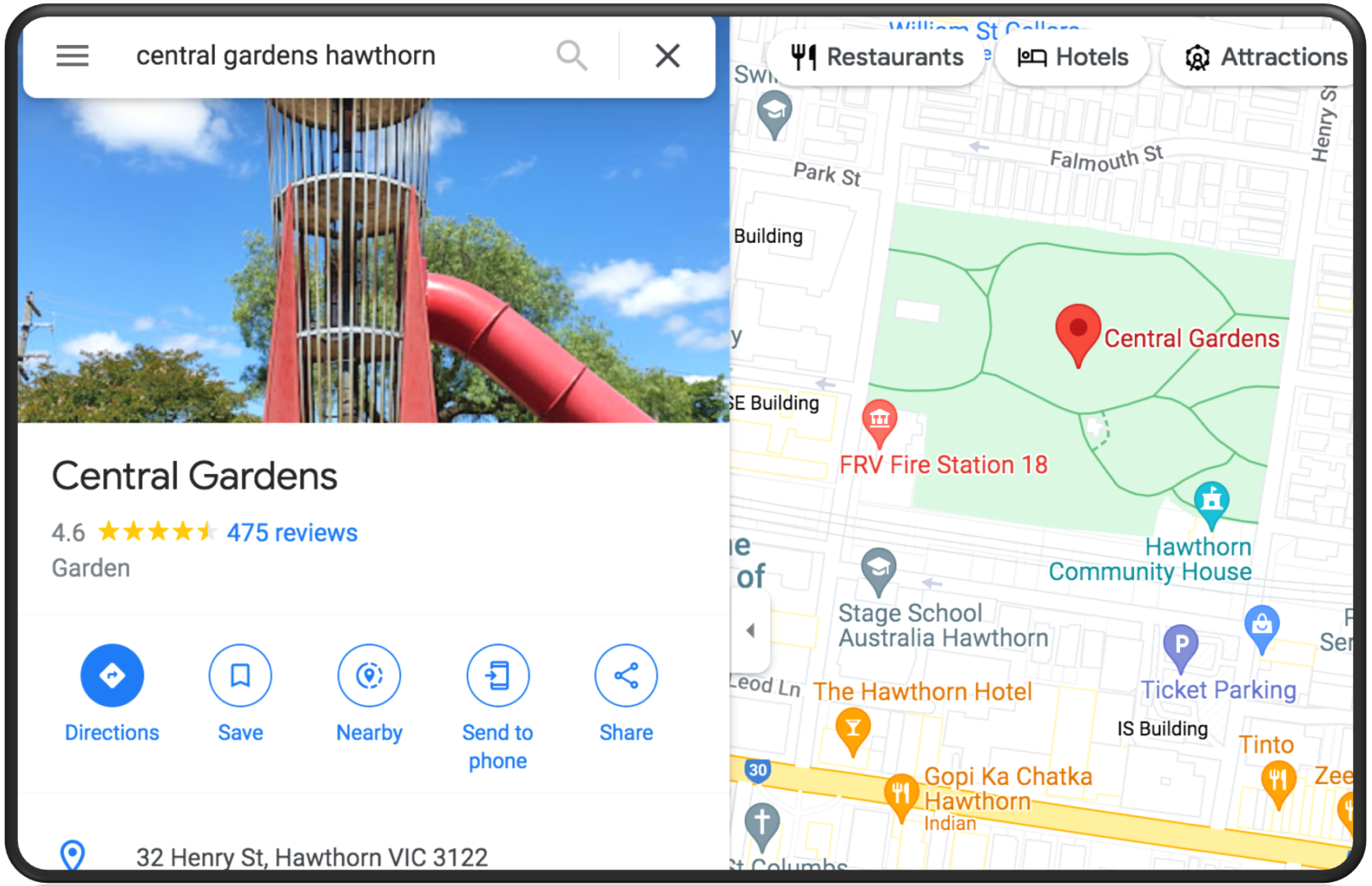
COS30015 IT Security – Lab 6 Background

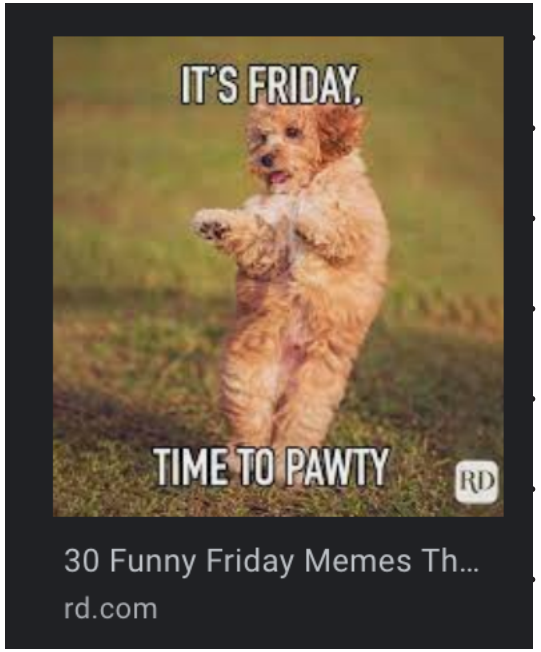


Internet speed Memes
memesmonkey.com

Two Virtual Machines
Kali,
CYSCA2014InABox

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 ☺

SWINBURNE UNIVERSITY OF TECHNOLOGY

Questions ?

Email: jooi@swin.edu.au
Linkedin: https://www.linkedin.com/in/jamie-ooi-15297b98/

Thursday 8 September, 2022

Most used nmap commands

SWINBURNE UNIVERSITY OF TECHNOLOGY

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