Warm up Lab review

- Internet connections determined by the gateway
- Typical Gateway:
  - 192 is ISP ethernet or VM
  - 172 is ISP Wireless or sometimes ethernet router.
  - 10 is NBN home router
  - 132 is UTS router
- DNS server:
  - 10 is NBN home router
  - 132 is UTS router
  - UTS web server on 54 is **not** at UTS. It is in the cloud (AWS)

Digital Forensics

Introduction to Forensics

Week 1

Nelson Text - Ch 1

Readings – Week 1

Useful Skills you will learn

- Developed from Network Security
  - apply what you know from Network Security to Forensics
- Develop skills in Digital Analysis
  - combine knowledge of Hardware, Software and Networking
- Useful start for employment in Forensics
  - sideline is Incident Response
  - banking, government, police, lawyers
  - a related field is Cyber Security
- Introduction to Pen Testing
- Knowledge is appropriate for an Industry Exam - CISSP
  - http://en.wikipedia.org/wiki/Certified_Information_Systems_Security_Professional

Related Activities

- Cyber Security
  - Available in TAFE NSW (SIT)
- Web Application cracking
  - Using interactive proxies – see OWASP
- Penetration Testing of a Network
  - Look for misconfigurations
- Scripted automatic attacks
  - Can be simulated in python
- Packet crafting to bypass firewalls
  - Typically using Python/Scapy

Caveat

- Some material and instructions in the lectures or labs can be used for illegal or commercial gain purposes
- The student must not use any technique described against any entity without the written permission of that entity

32309 Subject Objectives

- Demonstrate an in-depth, theoretical understanding of digital forensics.
- Design and support the collecting, preserving, storing and analysing of digital forensic evidence.
- Distinguish how to implement forensically sound digital security practices in industry.
- Apply experience with IT equipment to certification exams and career opportunities.

48436 Subject Objectives

- Elaborate on, compare and evaluate theories of digital forensics
- Support digital forensics specialists by collecting, preserving, storing and analysing digital forensic evidence
- Use their experience and newly acquired skills working in teams to implement forensically sound digital security practices in industry.
- Be aware of Industry recognised Digital Forensic Courses, such as CISSP, CHFI and SANS

A forensic example

- A person contacted police in Kansas in 2005 saying he had information about the killing of a young mother.
- He mailed a disk in an envelope expecting to remain anonymous.
- Extracting the metadata from the rtf file on the disk revealed Title=Christ Lutheran Church and Last Saved by=Dennis.
- Dennis Radar a Lutheran Church Elder is now in jail serving ten consecutive life sentences for 10 murders he committed.

Digital Forensics

- Digital forensics is a branch of forensic science encompassing the recovery and investigation of material found in digital devices, often in relation to computer crime.
- There are three forms of digital forensics
  - forensic analysis where evidence is recovered to support or oppose a hypothesis before a criminal court
  - eDiscovery, a form of discovery related to civil litigation
  - Intrusion detection which is a specialist investigation into the nature and extent of an unauthorised network intrusion
- http://en.wikipedia.org/wiki/Digital_forensics

ISO 27037

- The International Digital Forensics Standard.
- Ratified October 2012
- Guidelines for the Identification, collection, acquisition and preservation of digital evidence.
- Agencies should develop their policies and procedures in accord with this standard so multinational cases can proceed unhindered.

Training required by ISO 27037

- Digital Evidence First Responder (DEFR)
  - Has the skill and training to arrive on an incident scene, assess the situation and take precautions to acquire and preserve evidence.
- When necessary call for specialised equipment or a specialist

- Digital Evidence Specialist (DES)
  - has the skill to analyse the data and determine when another specialist should be called in to assist with the analysis

Types of Forensics

- Industrial Actions
  - failure to comply with employment guidelines
- Civil Actions
  - clandestine business operations
  - operating a company while at work
  - divorce proceedings
- Criminal Actions
  - using a device to commit a crime
  - stealing the device
- Intrusion by Malware

Intrusions on digital devices

- Script Kiddies trying out their new found apps
  - Typically deface the site
- Black Hat hackers
  - Getting high on testing their skills
- Criminals
  - Stealing credit card and banking details
  - Using you to purchase goods on their behalf
- The Big Boys
  - Monitoring the data and actions of employees
  - Manufacturing, Infrastructure and Defence

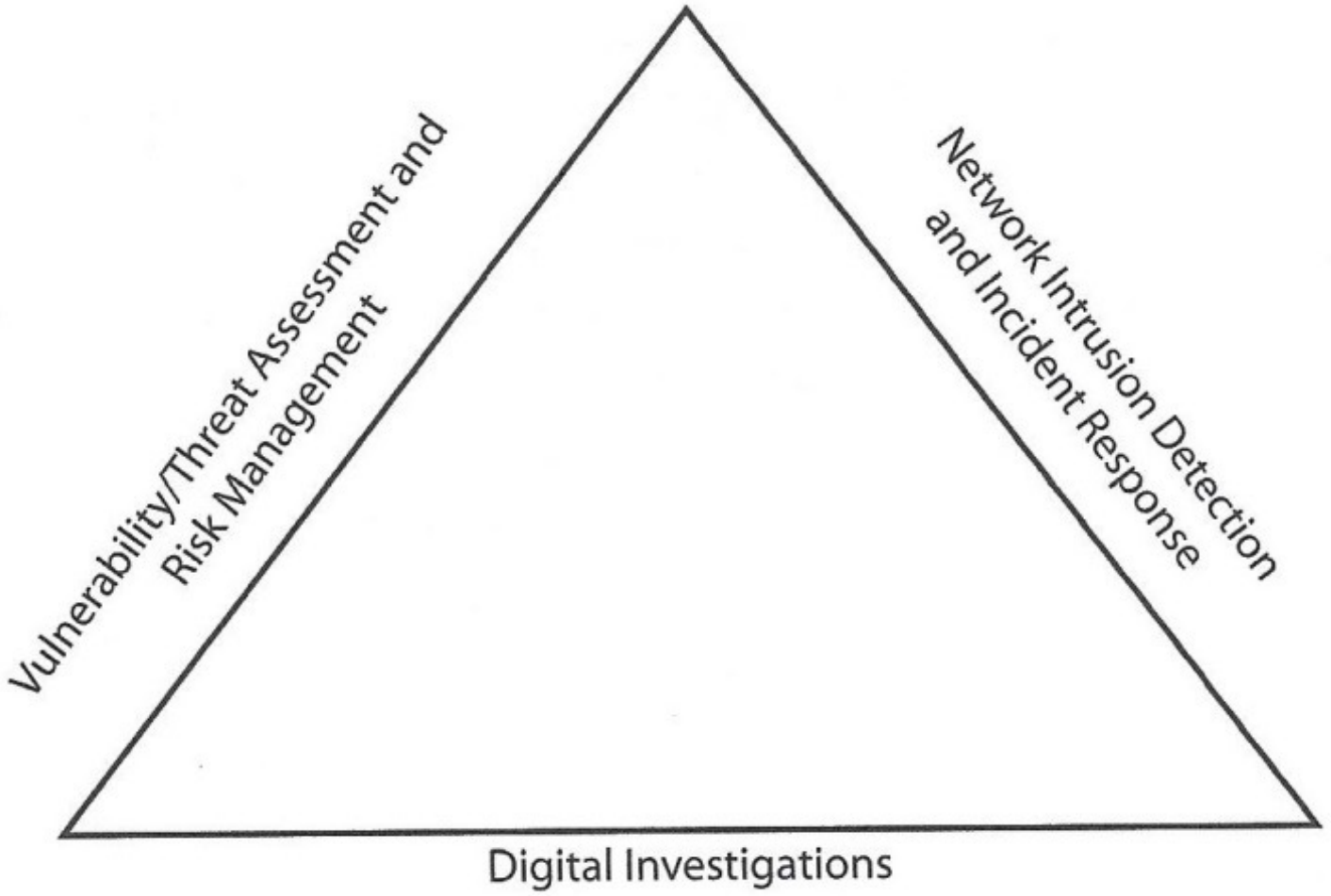
Malware

- Attacks on digital security are growing
  - In speed
  - In intensity
  - in sophistication
  - In lost value to the client
- In spite of the best efforts, attacks will succeed in penetrating the defenses
- The client wants to prevent a repeat attack succeeding
- The client may want to take action against the attacker

We've been hacked!

- When an enterprise discovers an incident
- The Investigation team springs into action
- Their aim is to provide Computing Security
- They test and verify the integrity of Workstations and Servers
- They look for Vulnerabilities using Penetration Testing
- They identify attacks using Firewall logs
- They collect Evidence for Civil or Criminal litigation

The Investigations Triad



The Digital Investigations group

- This group manage the investigation
- They decide if litigation is possible
- They conduct Forensic Analysis
- They present evidence in a Court of Law

Definitions

- Digital
  - A device using software to process digital communications
  - Computer, Laptop, Ipad, mobile phone, Router, Cloud and IOT
- Forensics
  - scientific tests or techniques used in the investigation of a crime
- Digital Evidence
  - Data stored or transmitted that supports or refutes a theory that an offence has occurred

Digital Forensics Investigators

- There are commercial firms that investigate forensic civil and criminal cases
  - Deloittes, EY, PWC
- There are Law Enforcement bodies
  - State Police (NSW Pol), Federal Police (AFP) , Crime Commission,
- There are government departments that investigate cyber crime at the national level
  - ASIO, DSD, Australian Criminal Intelligence Commission (ACIC)


AUSTRALIAN CRIMINAL INTELLIGENCE COMMISSION
AUSTRALIAN
CRIMINAL
INTELLIGENCE
COMMISSION
Crime types
Cybercrime
Fraud
Exploitation of business structures
Financial crimes
Identity crime
Illicit drugs
Illicit firearms
Money laundering
Public sector corruption
Violence

Evidence Collection – rfc3227

- A security incident is a security-relevant system event in which the system's security policy is breached.
- rfc3227 provides guidelines on the collection and archiving of evidence relevant to such a security incident.
- Evidence collection can quickly become a major task
- Unless the evidence collection is done correctly the evidence can be thrown out in court.

Identifying evidence example

- Prosecutors upgraded the charges against a suspect to murder on the basis of evidence of premeditation found on his office computer.
- Tech Support had done a routine investigation during an upgrade and checked the suspect's cookies
- They found websites with cookies that were refered from Google.
- The search terms included kill+spouse, accidental+death, smother, poison, homicides and murder

Devices to expect

- Suspects will use commonly available devices as well as devices suitable for performing hidden tasks.
- A list of common platforms can be found at w3counter.com/globalstats.php

Top 10 Web Browsers		
1	Chrome 83	40.15%
2	Safari 13	11.80%
3	Chrome 81	5.64%
4	Chrome 80	3.02%
5	Samsung 11	2.47%
6	Edge 18	2.44%
7	Firefox 77	2.41%

Top 10 Platforms		
1	Windows 10	23.51%
2	Android 9	13.16%
3	iOS 13	11.57%
4	Windows 7	8.67%
5	Android 10	8.21%
6	Android 8	8.12%
7	Mac OS X	4.78%

Lab security requirements

- Setup the Forensics lab in an enclosed room.
- Floor, ceiling and walls must be fixed in place with no removable panels.
- The door must have a secure lock limited to authorised users
- The lab must use a media safe for evidence containers.
- A visitor's log must record access times for every person.

Selecting a workstation

- For productivity, you need the best performance device you can afford.
- You can use VMs to get support for multiple Operating systems on the one device
- Many suspect devices are Windows based so your team needs extensive Windows experience
- Many forensics tools are Linux based

Selecting forensic software

- Some Linux platforms are designed for forensics, such as Kali Linux.
- The Police use commercial software such as Encase
- There is commercial software for breaking into phones such as Cellebrite

Forensic Tools #1

- There are many tools developed for forensic analysis
- We will use many in this subject
- Here is an overview of the available tools

Forensic Tools #2

- A digital device contains complex hardware and software
- The device actively uses Gigabytes of storage and process millions of instructions each second
- Forensic methods involve locating and piecing together many small pieces evidence hidden in all that data
- Many forensic software tools have been developed to ease this process

Tool Philosophy

- We need to look at evidence on a device
- We need to get past the user displays to see the raw data
- We need to use tools with a small footprint to minimise evidence disruption
- We like tools that provide a txt output for later analysis and reporting
- For all these reason we prefer command line tools

Forensic Tools #3

- There are many Open Source tools developed by enthusiastic individuals
  - usually written for the Linux platform
- A forensic investigation may involve the use of many of these tools
- There are some commercial products that combine these tools into a tool kit
- Some tool kits allow the collection of evidence by an unskilled person for later evaluation by a remote forensic expert

Forensic Tools #4

- We use a variety of forensic tools in this subject
- Most are free
- We focus on Windows tools, but the best tools are Linux based
- Here are some tool websites worth visiting
  - This is where the tools we use in the Labs come from
  - This is the right place to start when you want a new tool for your case study (or assignment)
  - When you work in forensics you will need more tools
- We will mention more sites later

Forensics Tools Warning

- Guiding Principle:
  - Nothing is ever free - **You** are the product

- Rule1) Be prepared for Trojans in the software!
  - Use a VM to Sandbox the software. Run a fully patched VM with Antivirus.

- Rule2) Never give true profile information.
  - Use a throwaway email address with fake details

Forensic Tool Kits

- We will use several toolkits in the Labs
  - OSForensics
  - ProDiscover
  - Autopsy
- A good free toolkit is SIFT
  - The Sans Investigative Forensic Toolkit
  - https://www.sans.org/tools/sift-workstation/

Forensic Tool Websites

- SysInternals
  - www.sysinternals.com
  - developed by Mark Russinovich in 1996
  - now part of the Windows support website technet.microsoft.com
  - good utilities, popular, well supported web site
- Windows
  - quite a few useful tools come with Windows
  - more are available as Windows Resource Kits
  - available from www.microsoft.com/download

Forensic Tool Websites #2

- Kali Linux
  - This a collection of Linux tools supplied as a Linux Distro
  - Kali.org/
- The Sleuth Kit (TSK)
  - A collection of disk analysis tools
  - Available on Windows and Linux
  - sleuthkit.org

Forensic Tool Websites #3

- Commercial tools
- The best known is Encase
- Used by professional investigators

https://security.opentext.com/encase-forensic

- Another popular tool collection is FTK Imager

https://www.exterro.com/ftk-imager

- COFEE

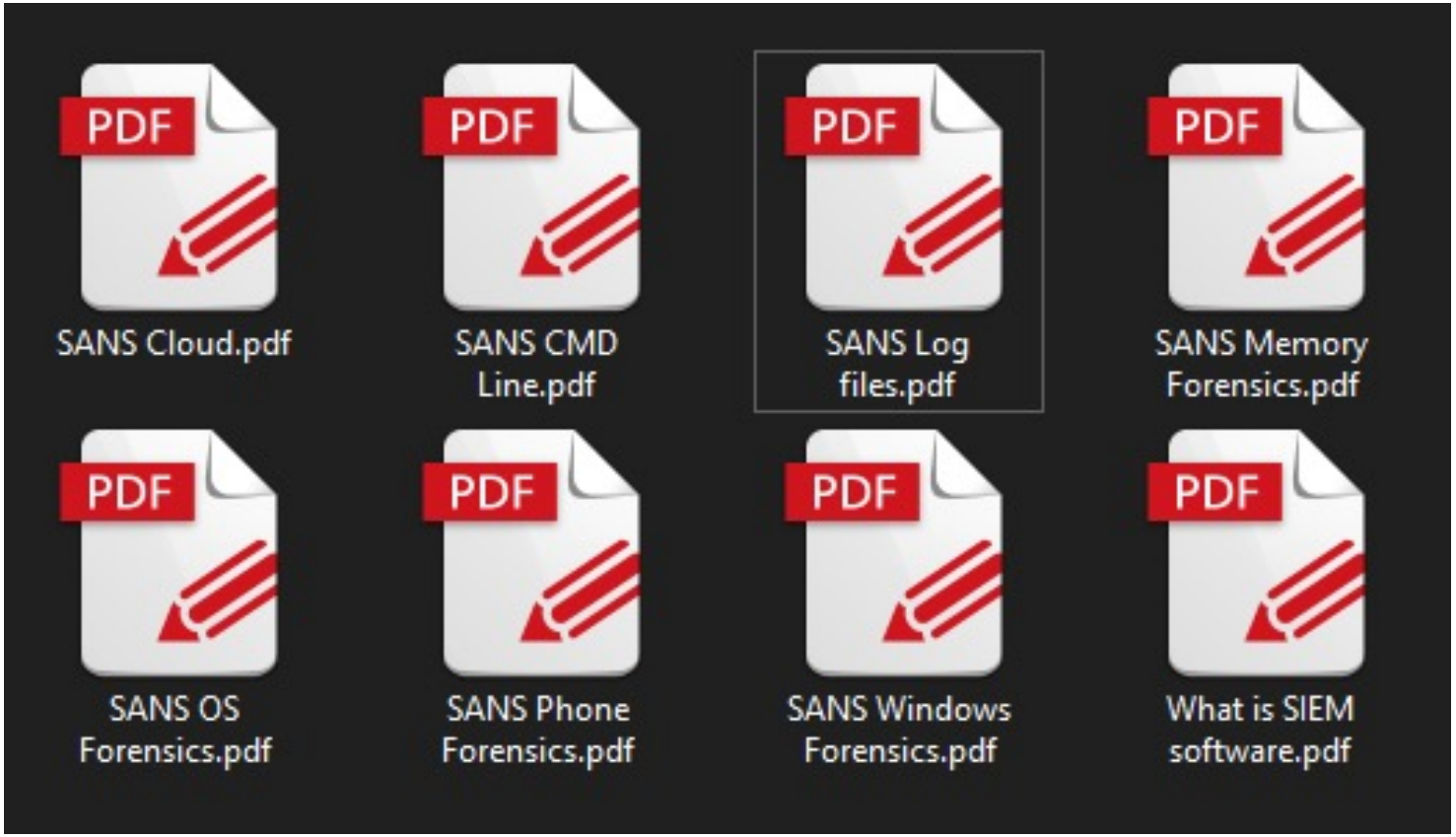
http://en.wikipedia.org/wiki/Computer_Online_Forensic_Evidence_Extractor

Forensic Tool Websites #4

- Magnet Forensics
  - Used in Business
  - https://www.magnetforensics.com/
- A list of common tools
  - https://en.wikipedia.org/wiki/List_of_digital_forensics_tools

SANS – how to Posters

- https://www.sans.org/security-resources/posters/dfir



Anti Forensics

- How do you hide from forensics?
- Try to be anonymous
- Leave a small footprint
- Quite a thriving area of activity
- Some Tools:
- The TOR proxy/VPN network
- Anonymous browsers (Ice Weasel)
- Disposable email addresses
- Disk/USB/email encryption

FIN