COS80013 Internet Security

Week 6

Presented by Dr Rory Coulter

06 April 2025

SWINBURNE UNIVERSITY OF TECHNOLOGY

Week 6 Class

Weeks 1 – 6 Recap

Quiz

Week 8 in class quiz

Weeks 1 to 6 inclusive

- Weeks 1 to 6 lecture, class, supplementary and lab content
- 30 questions, concepts than specifics
  - E.g., know MITRE ATT&CK tactics rather than command line options
- 1 hour
- Turn up to your class, log in to Canvas, take quiz, lab machine only
- Closed book, MCQ
- A practice quiz will be made available
- Answers will be provided 2 weeks after
- Any funny questions, we will review, don't need to email us
- Medical certificate required if you can't attend
- Attendance will be taken, StudentID cards please
- Attend your assigned class
- We will audit when a quiz was completed and when your class is

SWINBURNE UNIVERSITY OF TECHNOLOGY

Week 1

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Confidentiality

- Only those entitled to access the information can see it
- Authorise, encrypt, access control, authenticate, restrict physical access

Integrity

- Information cannot be altered and changes are immediately detectable
- Backup, checksum, hash, correction code

Availability

- Information is available (to read, write) to those who need it without interruption or onerous access restrictions
- Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security

Confidentiality

- Only those entitled to access the information can see it
- Authorise, encrypt, access control, authenticate, restrict physical access

Integrity

- Information cannot be altered and changes are immediately detectable
- Backup, checksum, hash, correction code

Availability

- Information is available (to read, write) to those who need it without interruption or onerous access restrictions
- Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections

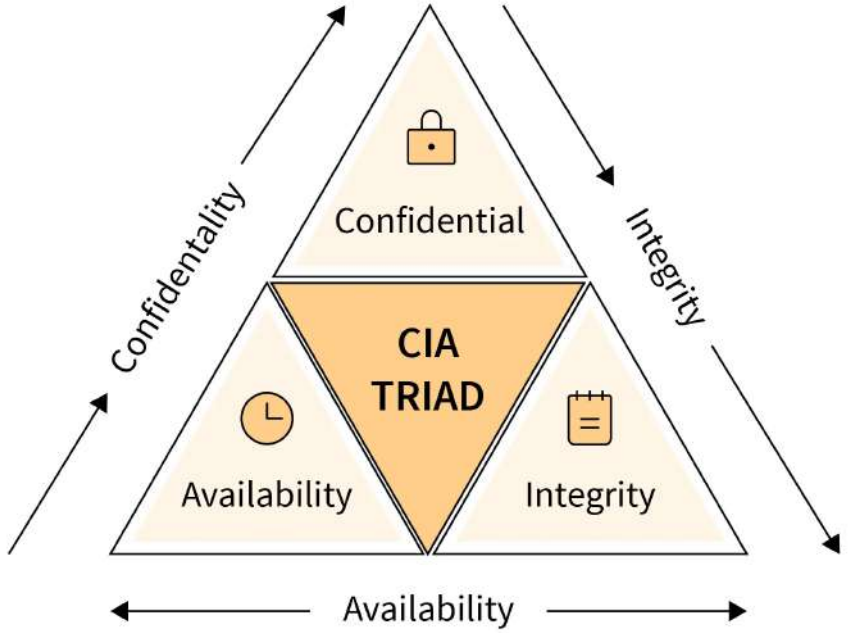
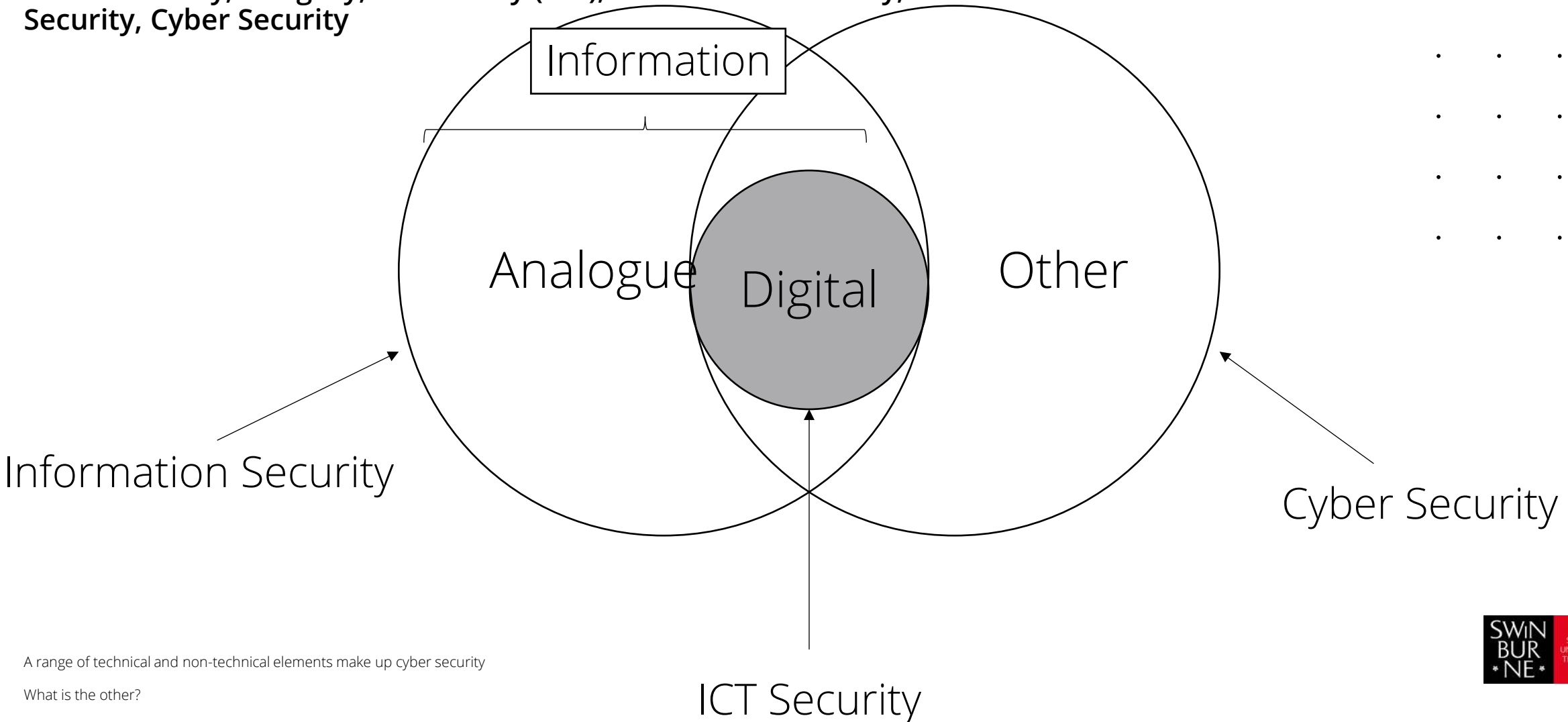


IMAGE SOURCE: https://www.scaler.com/topics/cyber-security/cia-triad/

Security Paradigms

Confidentiality, Integrity, Availability (CIA), Information Security, ICT Security, Cyber Security



A range of technical and non-technical elements make up cyber security

What is the other?

Threat Landscape

Common cyber threats

Not a complete list by any means

Threats	Objectives
Cryptomining	Often stealing processing power to mine crypto currency
Data Spill	Data leakage, exfiltration, breach
Denial of Service	Service or Resource is made unavailable (CIA?), Distributed DOS
Hacking	Unauthorised access to a computer system (CIA?)
Identity Theft	Stealing of personal information often for benefits
Malicious insiders	Employees, contractors for example with access, may steal, destroy and sabotage data, service or resources
Malware	Malicious software
Phishing	Steal confidential information
Ransomware	Type of malware which encrypts files for fee
Webshell Malware	Enable remote access to compromised device (think Trojan)

SWINBURNE UNIVERSITY OF TECHNOLOGY

Know your Extorsion

An example of how security is an ever changing game

We've heard of ransomware, lets understand the demands

Extorsion Type	Characteristic
Single	Encrypt, demand a ransom
Double	Threaten to release the data to encourage payment
Triple	Deny service to key systems (DoS)
Quadruple	Extort third parties and victims of incident to encourage payment

https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti

MITRE ATT&CK Tactics, Techniques and Procedures

Understanding attackers and attacks

"The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique"

- 14 Tactics
  - Consider as technical objective
- 240+ techniques and 370+ sub-techniques for enterprise
  - Way an adversary may achieve an objective
- Procedures as technique method and process

https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures

NIST SP 800-150 Tactics, Techniques, and Procedures (TTPs)

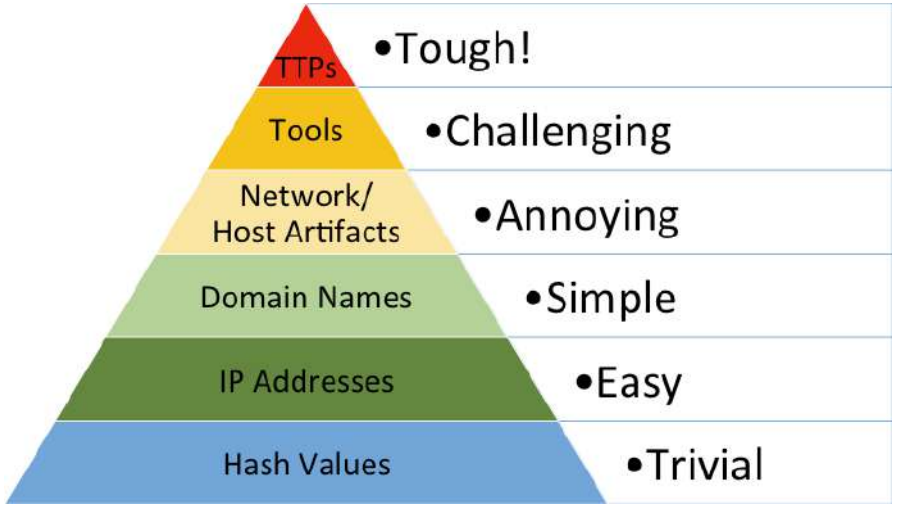
SWINBURNE UNIVERSITY OF TECHNOLOGY

Threat Detection or Incident Response

TTPs are the end game

Attacker artefacts which might contribute to TTPs

- Hash values: Signature of artefact, e.g., SHA-1 and MD5. Could be software or string
- IP addresses: Destination device
- Domain names: Attacker domain or compromised domain
- Network artifacts/host artifacts: Result of activity
- Tools: Attacker tools
- Tactics, techniques, and procedures (TTPs): Attacker behaviour or modus operandi which helps identify



Bianco, D. (2013). The pyramid of pain. Enterprise Detection & Response. https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

Cyber Risk

Risk is a driving factor across multiple cyber viewpoints

Let's consider two perspectives on risk

- Risk itself can be considered exposure to danger, harm, loss, negative impact
- Loss of confidentiality, integrity, or availability of information, data, or information (or control) systems
  - potential adverse impacts to organisational operations and assets, individuals, other organizations, and the Nation
- Potential Impact of Threat x Attack Likelihood = Cyber Risk
- The existence of risk requires it to be framed, assessed, respond and monitored
  - Components of Risk management
  - Multitiered Risk Management

https://csrc.nist.gov/glossary/term/cybersecurity_risk

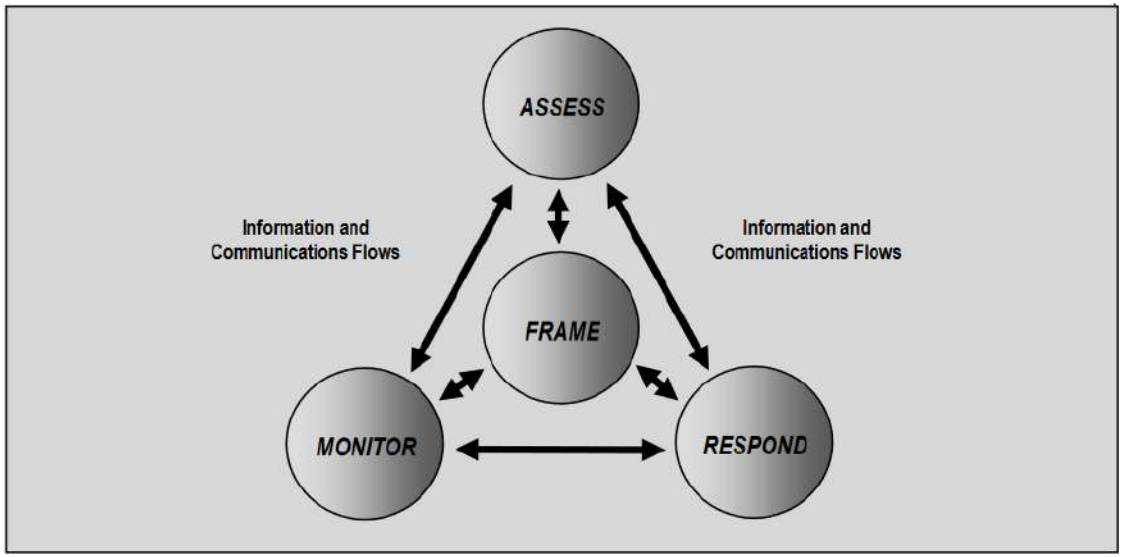
https://www.tenable.com/principles/cyber-risk-principles#chapter-2

Risk Management

Components

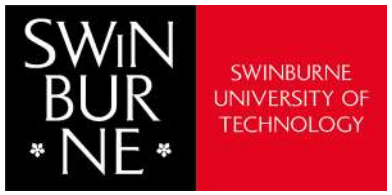
Let's consider two perspectives on risk

- Frame or "describing the environment in which risk-based decisions are made"
  - Assumptions, constraints, tolerance, priorities
- Assess
  - Assess given framing context
- Respond
  - Develop to implement risk response
- Monitor
  - Verify, ongoing effectiveness, changes



https://csrc.nist.gov/glossary/term/cybersecurity_risk

Week 2

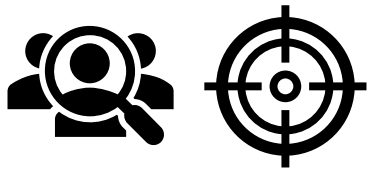


Offensive vs Defensive Security

Ultimately organisations favour defensive security over active probing production systems, but require a mixture

Understand the concepts

- Offensive
- Proactive approach to identify weakness, vulnerabilities
- Penetration tests***, mimic
- Active



- Defensive
- Preventative measures
- Detect incidents
- Passive

*** Very common for audit purposes

Physical Security

Physical security refers to the measures taken to protect physical assets, such as people, property, and resources, from unauthorised access, theft, damage, or harm

Physical security framework is made up of three main components:

- Access Control
- Surveillance
- Testing

Protection of people, space/dwelling, equipment, inventory, or information

The success of an organisation's physical security program can often be attributed to how well each of these components is implemented, improved, and maintained

Converged Security Overview (Continued)

Risks

Typically:

Physical world: Potentially to get caught and spotted

Digital World: Easy to blend in with noise

Biggest threat type: Insiders

Converged:

Physical + Digital: Better blend of controls

Biggest threat type: Insiders

Discretionary access control (DAC)

Allows the owner of a resource to control access to that resource and what level of access they are granted

- Access control list (ACL) is a
- List of users or groups who have been granted access to the resource and their corresponding level of access
- Examples ACLs in Windows, Linux: Assumes everyone who has permission exercises it responsibly
- Advantage :
  - simplicity , flexibility
- Limitations
  - not provide any protection against users who abuse their access privileges
  - difficult to manage ACL for large systems with many resources and users

Mandatory access control (MAC)

Access to resources is determined by a security policy that is enforced by the operating system or security software

Every resource (files, folders, and devices) is assigned a security label or classification that indicates the sensitivity or importance of the resource

- The security policy defines the rules for how access is granted based on the labels assigned to resources and users
- Example – SE Linux
  - Assumes no-one who has access can be trusted to exercise it responsibly
- Even root can have no authority
- Advantages:
  - provides a higher level of protection against unauthorised access
  - reduces the risk of accidental data leaks or breaches
- Limitations
  - more complex and difficult to manage than DAC
  - security policy must be carefully designed and maintained

Role-based access control (RBAC)

Provides access based on the roles and responsibilities of users within an organisation

Users can be assigned to multiple roles, each with a different set of permissions

- Users can be assigned to multiple roles, each with a different set of permissions
- These roles are based on the user's job function, responsibilities, and level of authority within the organisation
- Advantages:
  - simplifies the management of access control (central control)
  - more secure?

Attribute-based access control (ABAC)

Grants access to resources based on a set of attributes associated with users, resources, and the environment

Attributes associated with a user or resource can include a wide range of factors such as time of day, location, device type , sensitivity of the data

- Advantages:
  - flexible
  - granular
- Limitations
  - more complex to manage than other access control models
  - it requires a well-defined attribute-based policy and a system for collecting and managing the attributes associated with users and resources

Authentication

Verifying the identity of a user, process, or device, often as required to allow access to systems, resources in an information system

Maintain confidentiality

- Authentication is critical in preventing unauthorised access to:
  - Data
  - Systems
  - Resources
  - Applications
- Can lead to system impact, data breaches, financial loss, and reputational damage if breached
- Authentication requires
  - Identity
  - Secret

- User identity and secret is shared to system to authenticate to
  - Password-based authentication is the predominate method for authentication
- Identity and password are passed, password is looked up in table for authenticate*
- Users re-use passwords
- Obtain the password list, adversaries can look up or try to match the password hash

Assuming a hash-based scheme is employed

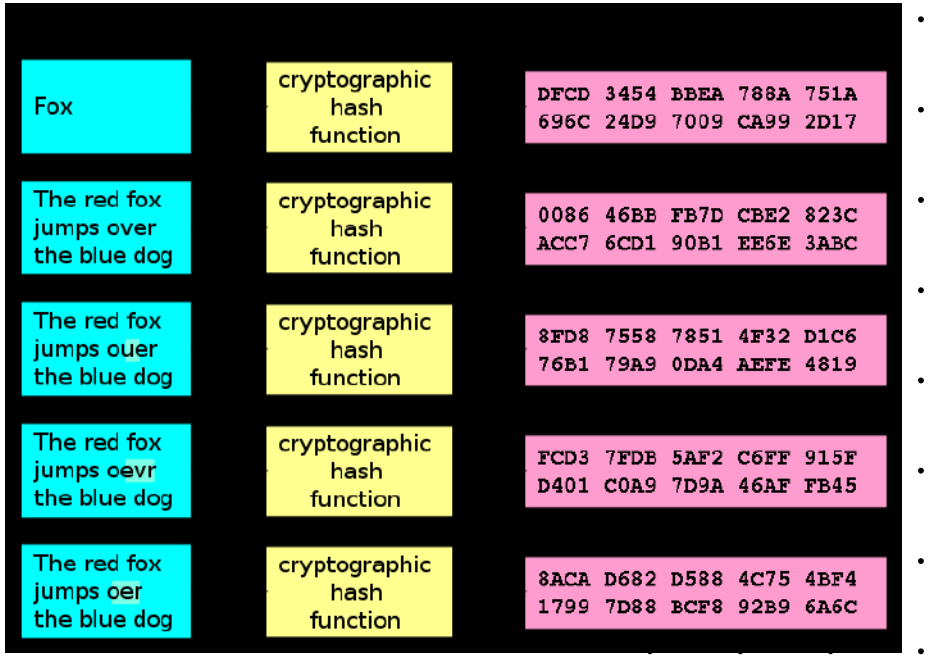
See top 10000 passwords: https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords

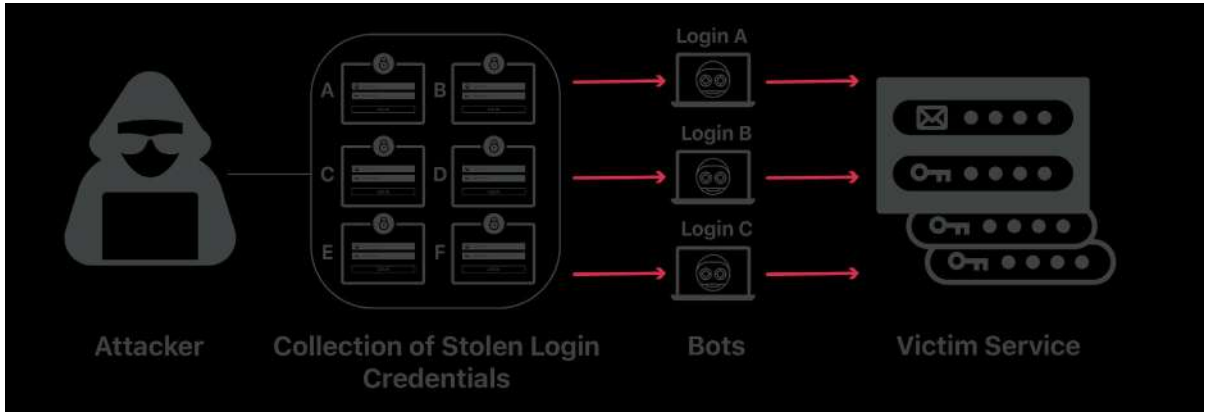
Password Attacks

Brute Force: T1110

Just a single technique and sub-techniques

Technique	Name	Details
T1110.001	Password Guessing	Guess password in attempt to login into account
T1110.002	Password Cracking	Try to crack or recover passwords, when pass the hash is not applicable*
T1110.003	Password Spraying	Single or small list of passwords across a range of accounts
T1110.003	Credential Stuffing	Using credentials obtained from data breach





Credential hashes are passed to authenticate

IMAGE SOURCE:

https://medium.com/@cmcorrales3/password-hashes-how-they-work-how-theyre-hacked-and-how-to-maximize-security-e04b15ed98d

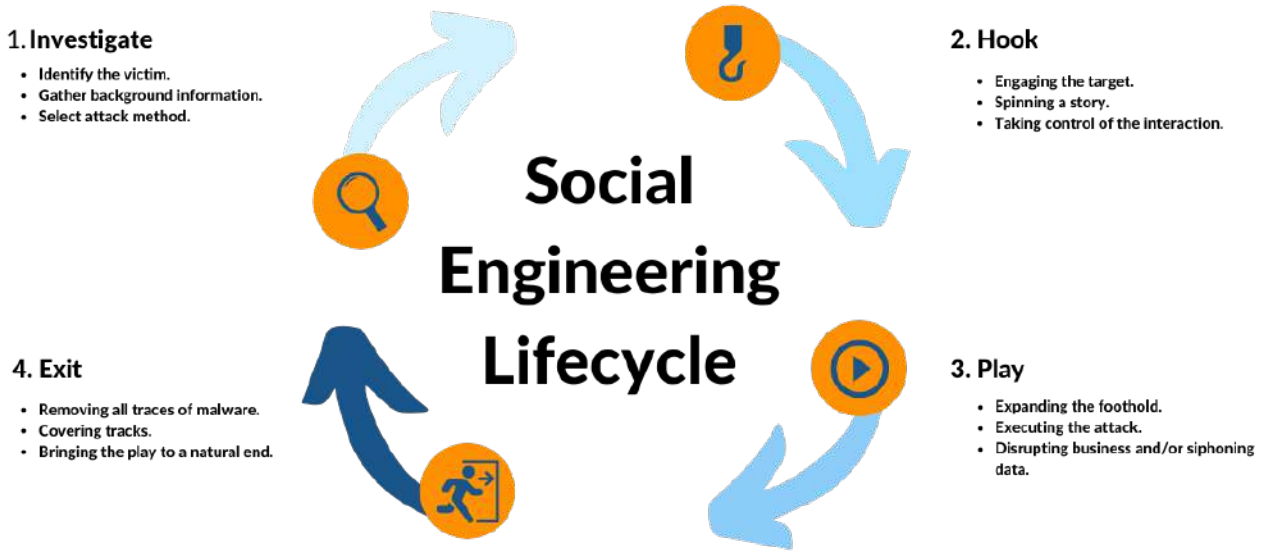
https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/

Social Engineering

Manipulation of individuals in seeking action or the release (divulging) of sensitive information

Influence over another which is not in their best interest

- Information gathering
- Engaging with victim
- Attacking
- Closing interaction



Social Engineering Forms

Some but not all

- Baiting: Like phishing, but using different items to lure victims (think free stuff for example)
- Dumpster diving: Physically sorting through rubbish
- Pretexting: Providing background or pretending to be another
- Phishing: Baiting with fake links to fake resources for
- Pharming: DNS level redirection to fake resources
- Reconnaissance: Information gathering
- Surveillance: Observing
- Shoulder surfing: Watching over someone's shoulder for information or passwords
- Tailgating: Trick employees to open doors for attackers

SET: Social Engineering Toolkit, open-source pen test framework geared for social engineering bundled within Kali Linux

Key Takeaways

Humans are the weak element

Technology will work as configured

- Many security system are rule or pattern based
  - These will operate as configured, or misconfigured

- Humans are susceptible to phishing and social engineering attacks
  - Scams are continuously successful

He could be getting scammed/phished right now

Phishing (cont.)

Common examples

- Phishing: General, bulk in nature
- Spearphishing: Limited receipting, targeted
- Whaling: High profile targets
- Vishing: Calls made over IP
- Smishing: Messages sent to recipients via phone
- Watering hole attack: Set a fake/malicious website or service

These examples see an adversary making use of their own infrastructure* or “cold calling”

*Loosely

Business Email Compromise (BEC)

Targeted phishing or spearphishing

Relationships are key in the success of phishing

- The relationship my introduce other characteristics:
- Pressure
- Time or financial sensitivities

Adversaries seek to leverage these with BEC

Emails are used to masquerade as business representatives

- Compromised accounts of employees
- Request payment through invoice
- Request change of details
- Request direct communication

External accounts can also be used, more time in preparing and grooming target

SWINBURNE UNIVERSITY OF TECHNOLOGY

Week 3

SWINBURNE UNIVERSITY OF TECHNOLOGY

Operating Systems

System software which manages hardware, software, provides and enables resources to services/programs

A collection of software that manages computer hardware resources and provides common services for computer programs

- Operating Systems provide some key functions to users, hardware, software
- An operating system manages the ways applications access the resources in a computer, including its disk drives, CPU, main memory, input devices, output devices, and network interfaces, user interface
- Kernel
  - Schedules time and resources to a process
- File system
  - Provides a framework to specify the handling of files and folders, permissions (RWX) for users and groups
- Memory management
  - Provide, manage and isolate memory required for software
- Processes
  - An instance of a program currently running
- Operating Systems are not secured by default typically
- Require additional configuration for security
- Where the computer exists plays an important role

https://csrc.nist.gohttps://csrc.nist.gov/glossary/term/operating_systemv/glossary/term/operating_system
NIST SP 800-152

SWINBURNE UNIVERSITY OF TECHNOLOGY

Security

Provide CIA to the computer system

Typical measures in which this can be achieved

- User or group permissions
  - Specifying who and a collection of users have access too
- Antivirus, Endpoint detection and response
  - Match known signatures, signatures, rules, behaviour, policy
- Policy
  - Specify setting which can be allowed or blocked
- Firewall
  - Block or allow connections incoming or outgoing connections
- Authentication
  - Method to whom can access system
- Access control
  - Fine grain settings
- Monitoring
  - Ability to log what is occurring
- Security software
  - Installation and running of additional programs to aid security (e.g., app locker)

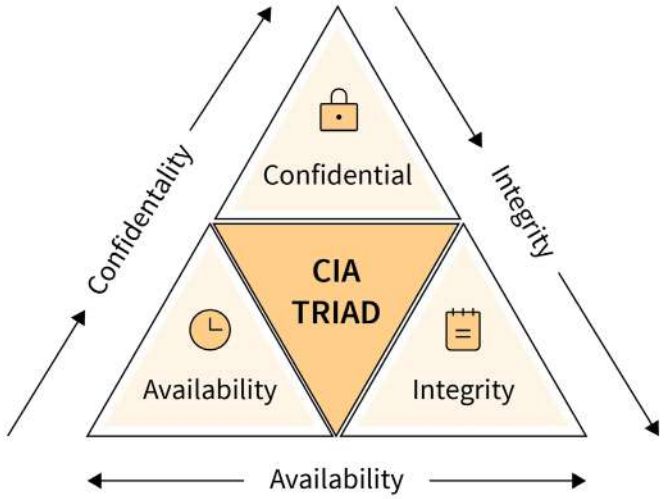


IMAGE SOURCE: https://www.scaler.com/topics/cyber-security/cia-triad/

Users and Passwords

Linux and Windows perspectives

Passwords are stored as hashes between operating systems

Each operating system employs different ways to manage passwords

Linux	Windows
Users stored in /etc/passwd and associated hashes /etc/shadow	Security Accounts Manager (SAM) file, C:\Windows\System32\config, hash via HKEY_LOCAL_MACHINE\SAM

The SAM file is restricted at runtime, the shadow file is not

Both these files can be copied and then studied offline to crack passwords

Range of tools for dumping passwords from SAM database

LASASS process in Windows very popular to dump hashes from (Local Security Authority Subsystem Service)

Salting: password + string ☞ hash, associated with the password

Peppering: password + secret ☞ hash, kept separate with the password

Authorisation

While you might be able to authentication, you might not have authorisation to the request

Compare the pair

- As discussed, authentication allows a user to confirm who they are
- When authenticating, they might not be authorised to access
- The user may or may not have the permission

System Monitoring

How are systems events handled

Broadly between Unix-based (let's just say Linux) and Windows

- Events occur within a system
- Event logs capture:
  - Date, time
  - Device
  - Description
  - Level
  - Associated application/process
  - Specific event type
  - Characteristic
  - Networking information in relevant
- Typically, Operating system event logs relate to
- System events from the operating system itself
- E.g., Syslog/Auth (Linux), Sysmon (Windows)
- Applications
  - Security events
  - Application logging may include
  - Request type
  - Status
  - Message
  - Networking
  - Event type
- Log structures are standardised, structured
- Logs should be centralised for monitoring
- Not everything is logged from install

Week 4

Terms

Let's set some common language

Across both topics today, and from a cyber security perspective

- Malware: Malicious Software
- Goodware, benign software: Safe, normal program
- Vulnerability: A flaw within an organisation per its controls or system procedures, implementation, software or hardware which could be exploited
- Exploit: Software or code (mostly) that takes advantage of a vulnerability to gain unauthorised access, disclosure, privilege or perform malicious actions on a system (see compromise)
- Implant: Code which is often injected or inserted into a system to maintain command and control (C2), or perform malicious actions after compromise
- Compromise: unauthorised disclosure, modification, substitution or use of sensitive data, unauthorised access or modification to systems, devices or processes
- Payload: Malicious action or function of malware
- Sandbox
  - Usually an application we can run malware in to analyse it

Malware (cont.)

Often developed and used by cyber actors*

Comparisons

- Viruses and Worms:
- Both self-replicate, viruses attach to files
- Worms spread across systems independently

- Trojans and Ransomware:
- Trojans pretend to be useful, give hacker access
- Ransomware locks files, demands payment

- Keyloggers and Spyware:
- Keyloggers record keystrokes, send to scammers
- Spyware covertly observes user actions

*what would we define good guys using malware, is it still malware?

Malware Delivery Vectors

How does malware even get onto our systems?

Not an exhaustive list:

- Phishing Emails
- Spear Phishing
- Malvertising
- Drive-By Downloads
- Watering Hole Attacks
- Infected USB Drives
- Social Engineering
- Ransomware Payloads
- Exploit Kits
- Remote Desktop Protocol (RDP) Attacks
- Brute Force Attacks
- Social Media Attacks
- Instant Messaging and Chat
- Fake Software Updates
- Trojanised Applications
- Drive-by App Downloads
- Email Attachments
- Peer-to-Peer Networks
- Physical Media
- Wi-Fi Networks

Preventative Measures

Being cyber safe

Some thoughts

- Preventive Measures:
  - Use antivirus software with daily updates
  - Keep all software updated
  - Employ strong passwords/passphrases
  - Backup files daily
  - Disable unused Microsoft Office macros
  - Regularly review and uninstall unused software

- Secure Application Installation:
  - Malware distributed via spam emails, malicious websites, and fake applications
  - Use reputable app stores for downloads
  - Avoid third-party download sites
  - Don't click on online ads for downloads, use ad-blockers
  - Avoid peer-to-peer network downloads
  - Be cautious with email/instant message links or attachments
  - Scan applications before installing, especially from email/USB

SWINBURNE UNIVERSITY OF TECHNOLOGY

Malware Analysis

Three main types

Automated, Static, Dynamic

- Automated
  - Use tools to analyse it
- Static
  - Dump the contents and investigate
- Dynamic
  - Run it, and investigate

*what would we define good guys using malware, is it still malware?

SWINBURNE UNIVERSITY OF TECHNOLOGY

Understanding Vulnerabilities

The good and the bad

Vulnerabilities

- Vulnerabilities are weaknesses in software or systems that can be exploited by attackers
- They can lead to unauthorised access, data breaches, or system crashes
- Vulnerabilities can be caused by coding errors, design flaws, or configuration issues
- CVEs (Common Vulnerabilities and Exposures) are standardised identifiers for known vulnerabilities
- Vulnerability databases like CVE Details and NVD list and provide information about CVEs
- Vulnerability scanning tools help identify weaknesses in systems and software
- Patches are updates released by software vendors to fix vulnerabilities
- Organisations should regularly update software and systems to protect against known vulnerabilities
- Zero-day vulnerabilities are exploited by attackers before vendors release patches
- Threat actors actively exploit unpatched vulnerabilities, making timely updates crucial

Vulnerability Types

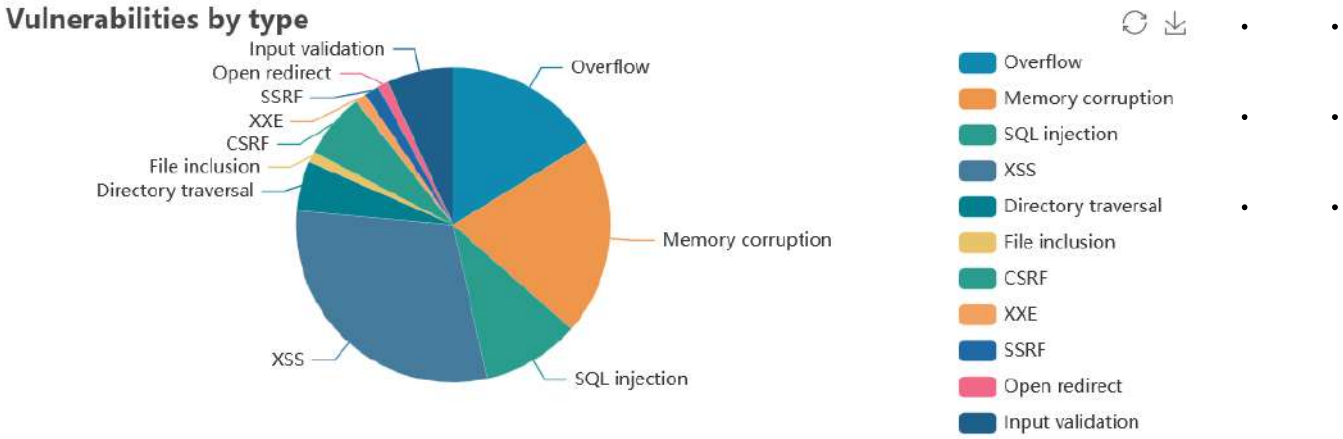
Vulnerabilities can exist in any type of software

Types

- Code Execution
- Bypass
- Privilege Escalation
- Denial of Service
- Information Leak

Categories

- Overflow
- Memory
- Corruption
- Sql Injection
- XSS
- Directory Traversal
- File Inclusion
- CSRF
- XXE
- SSRF
- Open Redirect
- Input Validation



SOURCE: https://www.cvedetails.com/browse-by-date.php

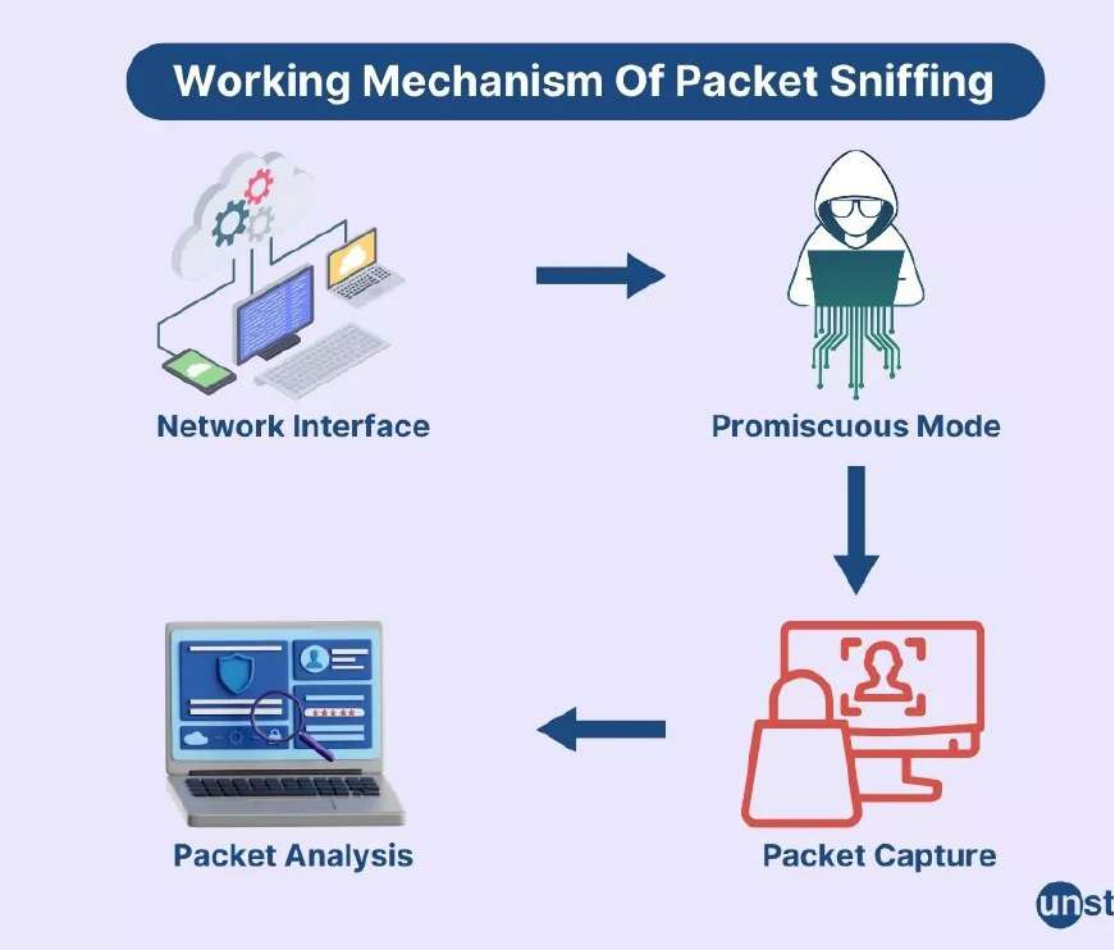
Week 5

SWINBURNE UNIVERSITY OF TECHNOLOGY

Common Attacks

Sniffing a NIC/hub/wifi broadcast.

- Sniffing means capturing IP packets and displaying/analysing them.
- Common sniffing programs include Snort and Wireshark.
- Local NIC is set to Promiscuous Mode.
- Sniffing program records packets presented to NIC, including all packets passing through the hub.
- Switches are also susceptible to ARP cache poisoning and MAC flooding. Switches act like hubs when overloaded.

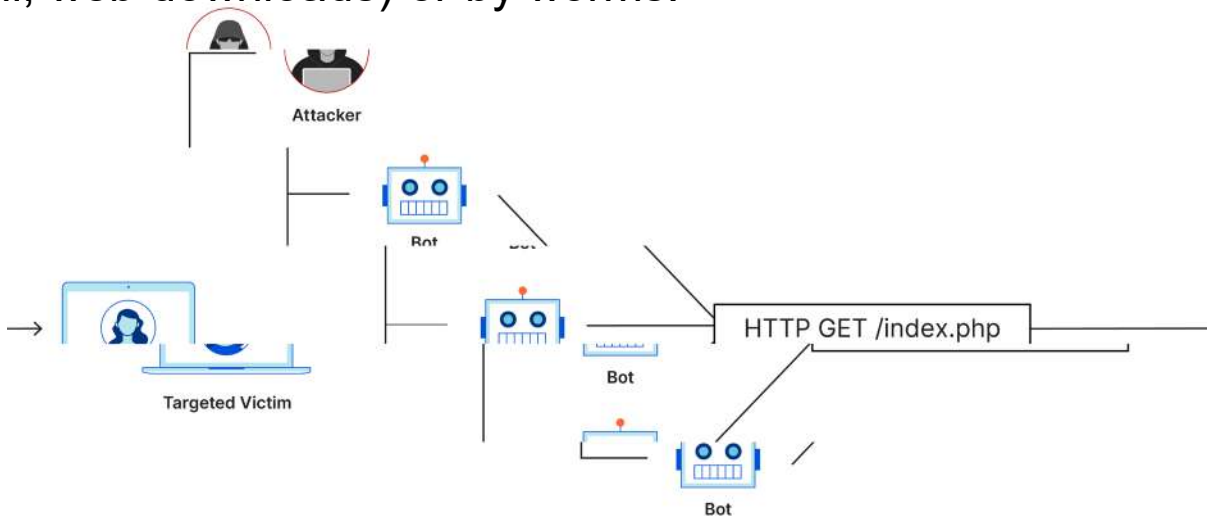


DDoS

- A Distributed DOS involves simultaneous attacks on a single site by 'zombie' machines infected with a 'bot'. Each bot is controlled by a 'bot-herder' originally through IRC channels and now through http. A bot-herder's 'bot-net' may range in size from a few hundred to millions of infected PCs.

- Each bot is actually a small server program which has installed itself and is capable of launching DOS attacks, sending spam, infecting other machines, or all of the above.

- Spread by trojans (e-mail, web downloads) or by worms.



https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/

Defence Strategies

Identify attack early

overprovision bandwidth

defend at the network perimeter

talk to your ISP

- filtering, rate-limiting
- port knocking

call a DDoS mitigation specialist

- some services do not need to be protected
- some services should not be on the Internet (use a private corporate network)

Week 6

SWINBURNE UNIVERSITY OF TECHNOLOGY

Introduction to CIS Controls

What Are CIS Controls?

•The **CIS Controls** (formerly known as the SANS Top 20) are a **prioritized set of best practices** developed by the Center for Internet Security (CIS).

•They help organizations **strengthen their cybersecurity posture** by focusing on **actionable defense mechanisms**.

Three Implementation Groups (IGs)

•**IG1 (Basic)**-Essential cyber hygiene for small organizations.

•**IG2 (Foundational)**- For organizations handling sensitive data.

•**IG3 (Advanced)**-For enterprises with critical assets and complex risks.

Top Examples of CIS Controls

Red Teams

The role of the Red Team is to identify the gaps in the organisation in an authorized manner

- Have to think like a hacker
- Test the effectiveness of the organisation's security program
- Emulate the tactics, techniques, and procedures used by likely adversaries
- Runs tests over a prolonged period to find vulnerabilities and weakness
- Provide a complete audit of testing results
- Perform Regular Penetration Testing to determine how secure the systems are and what are the vulnerabilities or misconfigurations
    - White-box
    - Black-box
    - Grey-box

Tools

- C2 Frameworks: Metasploit
- Social Engineering frameworks: Social Engineering Toolkit (SET)
- Asset Discovery tools: Amass, Shodan

SWINBURNE UNIVERSITY OF TECHNOLOGY

Blue Teams

The role of the Blue Team is to defend the organization against threats in the wild and improve the organisation's defences

- Defends against both real attackers and red teams
- Align security tooling and detection to TTPs, protect crown jewels
- Validate IRP and playbooks in case of an incident
- Adjust security posture based on insights from the red team and SOC
- Continuously improve detection and response
- Keep up with new threat intelligence
- Deploy and maintain security tooling
    - SOAR (Security Orchestration, Automation and Response)
    - SIEM (Security information and event management) tools

Purple Teaming

Red Team + Blue Team = Purple Teaming

- Members between the Red and Blue Teams
- To prepare red and blue teams and promote intel sharing
  - helps the Red Team understand the organisation's security policies and procedures
  - helps the Blue Team understand the vulnerabilities that the Red Team has identified
  - helps the Blue Team improve their incident response capabilities by providing feedback on their performance during simulated attacks
- Purple Teaming is a methodology and not a team inside the organisation

Thank you

COS80013
Internet Security

Week 6

Presented by Yasas

7 April 2025

SWINBURNE UNIVERSITY OF TECHNOLOGY

Acknowledgement of Country

We respectfully acknowledge the Wurundjeri People of the Kulin Nation, who are the Traditional Owners of the land on which Swinburne's Australian campuses are located in Melbourne's east and outer-east, and pay our respect to their Elders past, present and emerging.

We are honoured to recognise our connection to Wurundjeri Country, history, culture, and spirituality through these locations, and strive to ensure that we operate in a manner that respects and honours the Elders and Ancestors of these lands.

We also respectfully acknowledge Swinburne's Aboriginal and Torres Strait Islander staff, students, alumni, partners and visitors.

We also acknowledge and respect the Traditional Owners of lands across Australia, their Elders, Ancestors, cultures, and heritage, and recognise the continuing sovereignties of all Aboriginal and Torres Strait Islander Nations.

Agenda

- The fundamentals of ethical hacking
- Red, Purple & Blue Teams
- Purple Teaming
- Security Tools and Commands

The fundamentals of ethical hacking

What is Ethical Hacking?

Ethical Hacking (White Hat)

Legally simulates cyberattacks to test and strengthen system security.

Malicious Hacking (Black Hat)

Illegally infiltrates systems to steal, destroy, or ransom information.

Mixed-Intent Hacking (Grey Hat)

Accesses systems without permission, often out of curiosity — doesn't seek to harm or help.

Key Points

- Ethical hackers use the same tools as black hats — the difference lies in **intent and legality**.
- They help organizations **identify vulnerabilities** before real attackers do.

SWINBURNE UNIVERSITY OF TECHNOLOGY

A Brief History of Hacking

960s–1970s: The Prank Era

•Began in institutions like MIT — hacking was seen as a **challenge** or **tech puzzle**.

•Password cracking and system access were acts of **skill**, not malice.

2000s Onwards: The Profit Era

•Information became **monetized** — data used for marketing, manipulation, and profit.

•Hacking evolved into an **economic tool**, with cybercrime rings and ransomware groups.

Academic Milestones

•First IEEE articles on ethical hacking published: **2001–2002**.

•Oldest cited academic work on penetration testing dates -back to **1975**.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Understanding Systems & System Hacking

Computer System Components

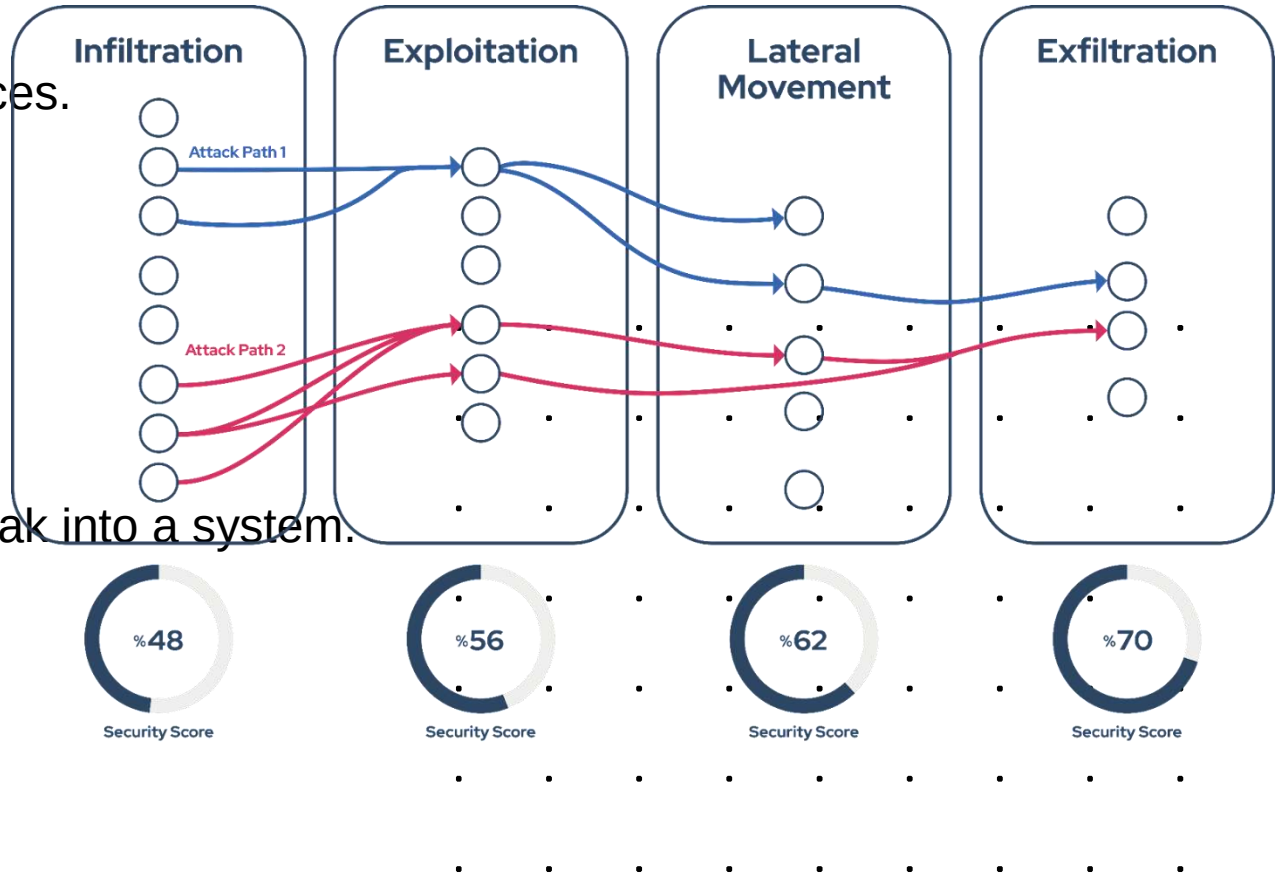
- **Hardware:** Physical parts (CPU, RAM, GPU, etc.)
- **Software:** Operating systems, applications, and services.

Role of the Operating System (OS)

- Manages hardware resources.
- Provides a platform for software to run.

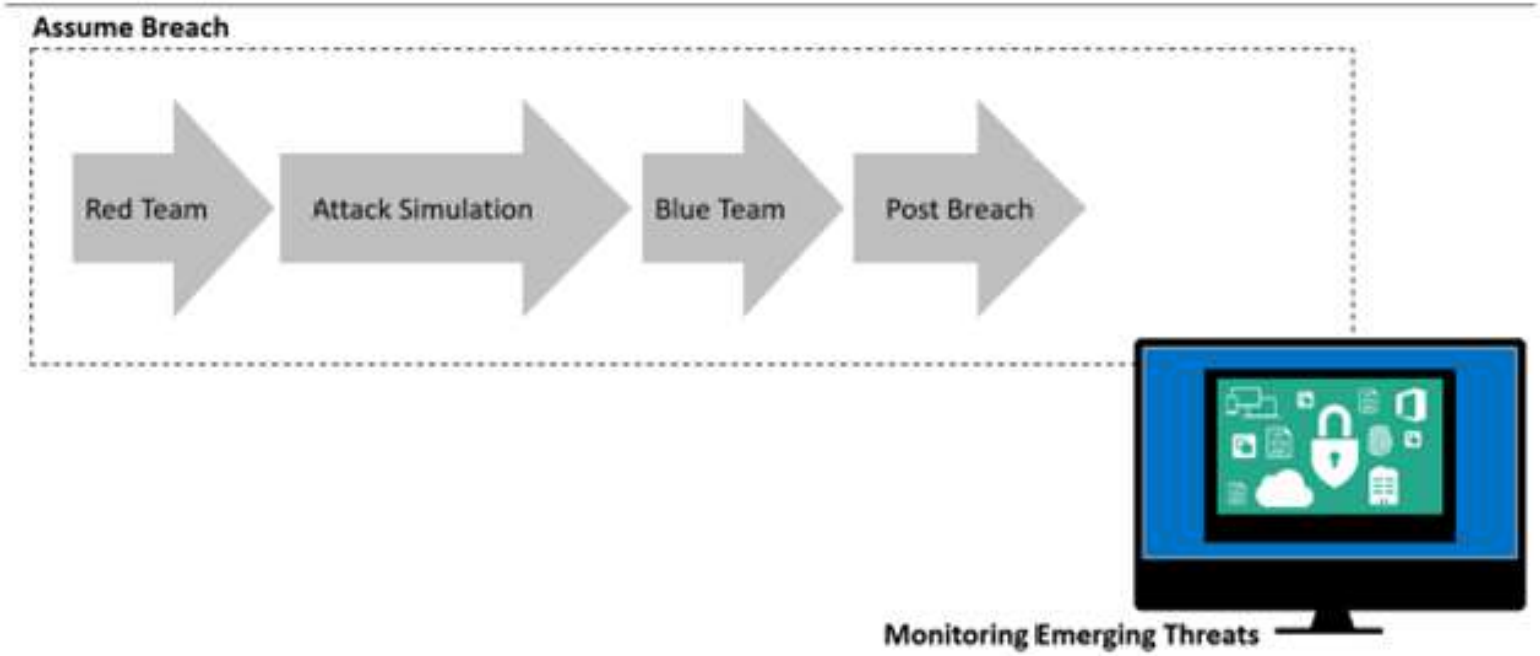
System Hacking Defined

- The **unauthorized** use of tools and frameworks to break into a system.
- Goal: **Steal, alter, or destroy** sensitive data.



https://www.picussecurity.com/resource/glossary/what-is-attack-path-visualization

An example of red and blue simulation



SWINBURNE UNIVERSITY OF TECHNOLOGY

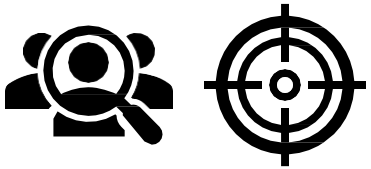
Red, Purple & Blue Teams, Security Tools and Commands

Offensive vs Defensive Security

Ultimately organisations favour defensive security over active probing production systems, but require a mixture

Understand the concepts

- Offensive
- Proactive approach to identify weakness, vulnerabilities
- Penetration tests***, mimic
- Active



- Defensive
- Preventative measures
- Detect incidents
- Passive

*** Very common for audit purposes

SWINBURNE UNIVERSITY OF TECHNOLOGY

Player Recap

Broad Perspective(s)

Apposing sides defined by legality

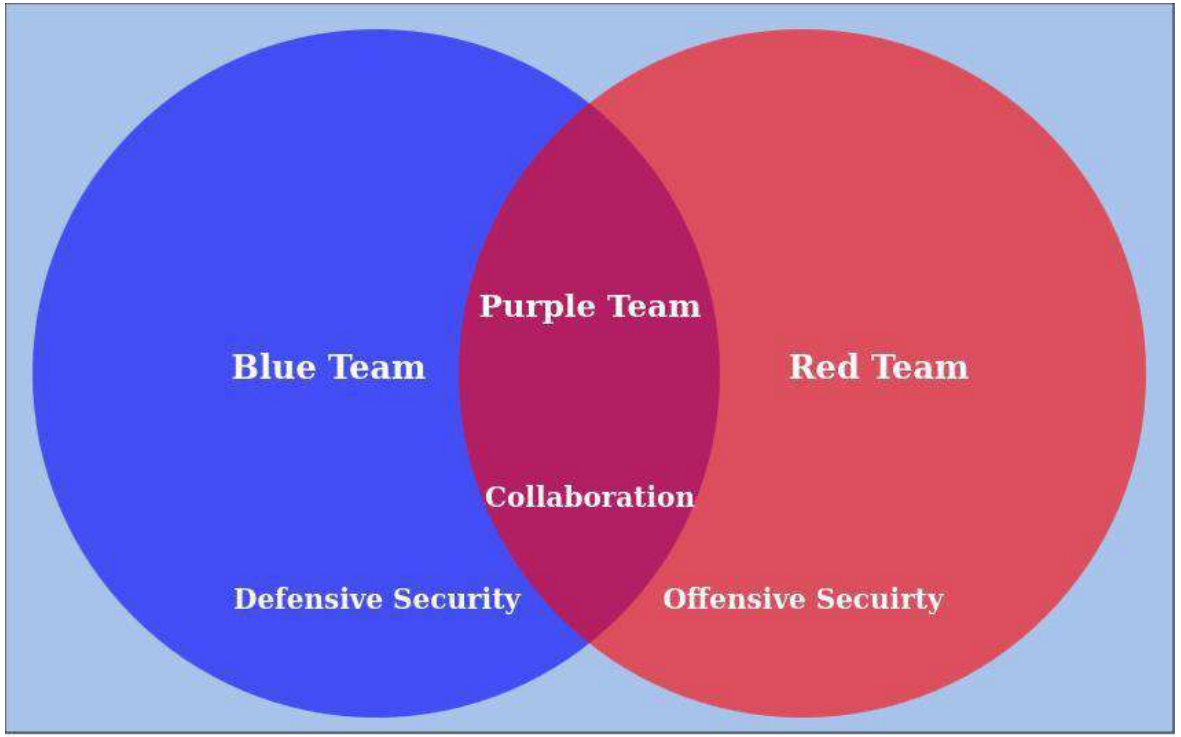
Good intentions don't justify the action

Perspective 1	Perspective 2	Action
Patch	Exploit	Scan vulnerability
Report	Catalogue	Scan vulnerability
Automation/ administration	Persistence	Schedule task
Expose	Ransom	Website defacement
Expose	Ransom	Data leak

SOURCE: https://www.geeksforgeeks.org/what-are-white-hat-gray-hat-and-black-hat-hackers/

Role Terms

Commonly used jargon to explain where your role aligns



Cyber Roles

Typical roles from graduate to principal

Mixture of offensive and defensive roles, and paper team

How to stand out? Blog or social posts investigating tools, use cases, pen test write ups, OSINT analysis, etc.

Role	Technical?
Incident Responder (forensic analysis)	Yes
Incident Handler	No
Threat Hunter	Yes
Malware Analyst	Yes
Governance, Risk & Compliance (GRC)	No
Vulnerability Management	Yes
Network***	Yes
Analyst (SOC, SIEM, Security Tool***)	Yes
Administrator	Yes
Penetration Tester	Yes
Consultant	Mixed
Technical Writer	Mixed
Infrastructure	Mixed
Intelligence	Mixed
Project manager, communications, legal	No

SWINBURNE UNIVERSITY OF TECHNOLOGY

Cyber Roles

Typical roles from graduate to principal

Potential designation

Role	Technical?
Incident Responder (forensic analysis)	Yes
Incident Handler	No
Threat Hunter	Yes
Malware Analyst	Yes
Governance, Risk & Compliance (GRC)	No
Vulnerability Management	Yes
Network***	Yes
Analyst (SOC, SIEM, Security Tool***)	Yes
Administrator	Yes
Penetration Tester	Yes
Consultant	Mixed
Technical Writer	Mixed
Infrastructure	Mixed
Intelligence	Mixed
Project manager, communications, legal	No

SWINBURNE UNIVERSITY OF TECHNOLOGY

Red, Purple & Blue Teams

Red Teams

The role of the Red Team is to identify the gaps in the organisation in an authorized manner

- Have to think like a hacker
- Test the effectiveness of the organisation's security program
- Emulate the tactics, techniques, and procedures used by likely adversaries
- Runs tests over a prolonged period to find vulnerabilities and weakness
- Provide a complete audit of testing results
- Perform Regular Penetration Testing to determine how secure the systems are and what are the vulnerabilities or misconfigurations
  - White-box
  - Black-box
  - Grey-box

Tools

- C2 Frameworks: Metasploit
- Social Engineering frameworks: Social Engineering Toolkit (SET)
- Asset Discovery tools: Amass, Shodan

SWINBURNE UNIVERSITY OF TECHNOLOGY

Red Teams - Penetration Testing

	Black-Box *aka close box penetration testing*	Grey-Box *combination of black box and white box testing*	White-Box *aka open box penetration testing*
Goal	Mimic a true cyber attack	Assess an organization's vulnerability to insider threats	Simulate an attack where an attacker gains access to a privileged account
Access Level	Zero access or internal information	Some internal access and internal information	Complete open access to applications and systems
Pros	Most realistic Testing is performed from point of view of attacker	More efficient than black-box andsaves on time and money Testing is performed from point of view of attacker	More comprehensive, less likely to miss a vulnerability and faster Testing is performed from point of view of attacker
Cons	Time consuming and more likely to miss a vulnerability	No real cons for this type of testing	More data (ex, source code) is required to be released to the tester and more expensive

SOURCE: https://www.packetlabs.net/posts/types-of-penetration-testing/

Red team methodologies

Phase	Purpose	Key Actions	Common Tools
Gathering Information	Collect publicly available data about the target system and network	- Research employees via social media - Use advanced Google searches - Map the network	- Social Engineering (Phishing, Direct contact) - Nmap (Network mapper) - Wireshark (Network packet analyzer)
Scanning	Probe the system for open ports, services, and vulnerabilities	- Identify OS and services - Detect open/closed ports - Determine firewall rules	- Nmap - Wireshark
Gaining Access	Exploit discovered vulnerabilities to break into the system	- Password cracking - Exploiting OS vulnerabilities - Uploading payloads	- Metasploit (Exploitation framework) - John the Ripper (Password cracker) - Hydra (Brute-force attack tool) - Cain & Abel
Maintaining Access	Stay connected to the compromised system without detection	- Create backdoors - Use privilege escalation (Vertical & Horizontal)	- Metasploit - Beast (Remote Access Trojan - RAT)
Covering Tracks	Erase digital footprints to avoid detection	- Delete log files - Modify registry entries - Clear command history	- Metasploit - OSForensics (For log and registry clearing)

Blue Teams

The role of the Blue Team is to defend the organization against threats in the wild and improve the organisation's defences

- Defends against both real attackers and red teams
- Align security tooling and detection to TTPs, protect crown jewels
- Validate IRP and playbooks in case of an incident
- Adjust security posture based on insights from the red team and SOC
- Continuously improve detection and response
- Keep up with new threat intelligence
- Deploy and maintain security tooling
    - SOAR (Security Orchestration, Automation and Response)
    - SIEM (Security information and event management) tools

Blue team methodologies

Aspect	Description	Common Tools/Technologies
Network Monitoring	Continuously observes network traffic for anomalies or unauthorized activity	- SIEM (e.g., Splunk, QRadar) - IDS (e.g., Snort) - IPS (e.g., Suricata)
Security Operations Center (SOC)	Central hub where security analysts monitor, detect, and respond to security incidents	- SOC Dashboards - Incident Response Platforms
Endpoint Detection & Response (EDR)	Provides real-time monitoring and data collection from endpoint devices	- CrowdStrike Falcon - Microsoft Defender for Endpoint - SentinelOne
Identity and Access Management (IAM)	Controls user privileges, roles, and authentication mechanisms	- Okta - Azure AD - LDAP - MFA Solutions
Behavioral Analysis & ML	Uses machine learning and behavioral analytics to detect anomalies and predict threats	- UEBA (User & Entity Behavior Analytics) - AI-integrated SIEM platforms
Privilege Management	Ensures employees have only necessary access, and removes access for ex-employees	- Role-Based Access Control (RBAC) - Privileged Access Management (PAM)
Alert Management	Responds to and prioritizes alerts generated from various tools and logs	- SIEM Alerting Rules - Automation Tools (e.g., SOAR platforms)

Blue Team Tools

A collection of useful tools

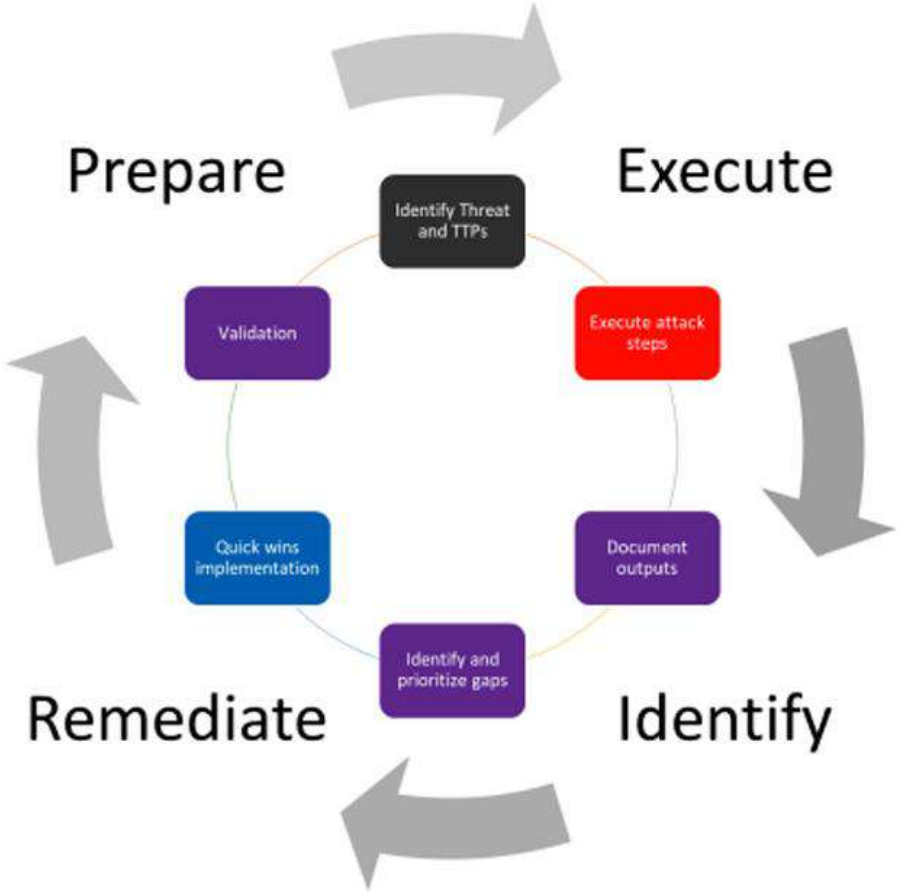
- Threat Intelligence
- MISP
- Malware Detection and Analysis
- VirusTotal
- IDA (disassembler and debugger)
- Ghidra (reverse engineering tool)
- Data Recovery
- Recuva
- TestDisk
- Digital Forensics
- SANS SIFT
- The Sleuth Kit (disk analysis)
- Autopsy (forensic platform)

Purple Teaming

Red Team + Blue Team = Purple Teaming

- Members between the Red and Blue Teams
- To prepare red and blue teams and promote intel sharing
  - helps the Red Team understand the organisation's security policies and procedures
  - helps the Blue Team understand the vulnerabilities that the Red Team has identified
  - helps the Blue Team improve their incident response capabilities by providing feedback on their performance during simulated attacks
- Purple Teaming is a methodology and not a team inside the organisation

Advanced purple teaming in action



PEIR model cycle

Introduction to CIS Controls

What Are CIS Controls?

•The **CIS Controls** (formerly known as the SANS Top 20) are a **prioritized set of best practices** developed by the Center for Internet Security (CIS).

•They help organizations **strengthen their cybersecurity posture** by focusing on **actionable defense mechanisms**.

Three Implementation Groups (IGs)

•**IG1 (Basic)-**Essential cyber hygiene for small organizations.

•**IG2 (Foundational)-** For organizations handling sensitive data.

•**IG3 (Advanced)-**For enterprises with critical assets and complex risks.

Top Examples of CIS Controls

SWINBURNE UNIVERSITY OF TECHNOLOGY

CIS Controls in Purple Teaming

CIS Control	Red Team Role	Blue Team Role
CIS Control 8: Audit Log Management	Attempts to bypass or delete logs	Detects anomalies, configures alerts
CIS Control 4: Secure Configuration	Exploits misconfigurations	Applies hardened system templates
CIS Control 5: Account Management	Tests for privilege escalation paths	Monitors and limits unnecessary access
CIS Control 18: Penetration Testing	Conducts red team activities	Uses findings to reinforce defense mechanisms

Red Team Tools

A small selection of notable tools across various MITRE ATT&CK Tactics

- Reconnaissance
- Showdan[.]io (search engine)
- Initial Access
- Hydra (brute force)
- King Phisher
- Execution
- Rubeus (Active directory hack tool)
- Credential Access
- Mimikatz (Windows credential extractor)
- hashcat Password hash cracking
- John the Ripper Password hash cracking
- Collection
- BloodHound (Active directory visualisation)
- Impact
- SlowLoris (Simple denial of service)

Red Team Commands

Educational Only – Do not perform

- Hiding the local admin account
- reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /t REG_DWORD /v hiddenaccountname /d 0 /f
- reg add: Adds or modifies registry keys and values
- "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList": Specifies the registry key path where the user account settings are stored
- /t REG_DWORD: Specifies the data type (DWORD) for the value
- /v hiddenaccountname : Sets the name of the value
- /d 0: Sets the value data to 0, which means the user account will be hidden
- /f: Forces the operation without prompting for confirmation

SWINBURNE UNIVERSITY OF TECHNOLOGY

Red Team Commands

Educational Only – Do not perform

- Drop Defender signatures
- %Program Files%\Windows Defender\MpCmdRun.exe" -RemoveDefinitions –All
- -RemoveDefinitions -All: These parameters instruct Windows Defender to remove all virus and spyware definitions
- Determine is host is within a VM
- reg query HKLM\SYSTEM /s | findstr /S "VirtualBox VBOX VMWare"
- eg query command to search the HKLM\SYSTEM registry hive
- The | findstr /S "VirtualBox VBOX VMWare" part filters the results to include only lines containing the specified keywords
- If any references to VirtualBox, VBOX, or VMWare are found, they will be displayed

SWINBURNE UNIVERSITY OF TECHNOLOGY

Purple Team Case Study

Design an Purple Team Activity

Plan an evaluation of security tooling using 1 offensive and 1 defensive tool – A significant hint for Assignment 2

Evaluate which position is successful

- Bring red and blue teams together to improve organisation posture and response
- Simulate adversary activity and get a snapshot , validate security tools, processes
- Document and select tools from each position
- Outline steps to be undertaken
- Map MITRE TTPs
- Provide metrics to evaluate which position is favourable

SWINBURNE UNIVERSITY OF TECHNOLOGY