Confidentiality. Integrity. Availability. CIA.

Confidentiality, integrity, and availability are considered the three pillars of cyber security. Whenever a cyber security breach occurs, the violation will relate to, one of, if not, all of the three key pillars.

Confidentiality.

- Confidentiality is the protection of information, especially from unauthorised access.
- Confidentiality involves separating and organising data according to sensitivity and accessibility.
- Confidentiality is about defining and enforcing certain and specific access levels for information.
- Confidentiality is about how sensitive the data is and who is allowed to access it.
- Confidentiality is about managing the data using access control lists, volume and file encryption, and file permissions.

Integrity.

- Integrity relates to the integrity and reliability of the data.
- Integrity is about protecting the data from deletion or modification by unauthorised users.
- Integrity is about damage control when an authorised user makes incorrect changes. Can the data be recovered? Can the process be reversed?

Availability.

- Availability refers to the actual availability of the data.
- Availability refers to how authentication mechanisms, access channels and systems need to work properly to protect and ensure information is available when needed.

Hacking.

What are black hats and what is black hat hacking?

- Black hats, like all hackers, have extensive knowledge about breaking into computer systems and networks, and bypassing security protocols.
- Black hats design and use malware to gain access to systems.
- Black hats are motivated by personal and financial gain, cyber espionage, political protest, even entertainment.
- Black hats range from amateurs and beginners who spread malware, to experts who steal, modify, and destroy highly sensitive data such as personal and financial data, login credentials, and passwords.
- Black hats break the law and are considered cyber-criminals.

What are white hats and what is white hat hacking?

- White hats are also known as ethical hackers.
- White hats are typically employed as security specialists to find security vulnerabilities in systems owned by the companies who employ them.
- Ethical hacking is not considered illegal because white hats have permission of system owners.
- White hats perform penetration testing, test security systems and structures and perform vulnerability assessments for companies.
- There are white hat courses, training, conferences, and certifications available for those who would like a career in ethical hacking.

What are grey hats and what is grey hat hacking?

- Grey hats are a mixture of black and white hats.
- Grey hats will look for vulnerabilities in systems and disclose discoveries to system owners in exchange for some form of reward.
- Grey hats, whilst not typically malicious, have been known to post findings publicly because owners have been unwilling to provide rewards.
- Grey hats are unethical and are still considered cyber-criminals because no permission is sought from system owners prior to hacking or discovery attempts

What is hacktivism?

- Hacktivism is the act of misusing a computer system or network for a socially or politically motivated reason.
- Hacktivists draw the public's attention to the hacktivist's belief or cause, such as freedom of information, human rights, or religious views.

Code of Ethics.

Ethical codes are adopted by organizations to assist members in understanding the difference between right and wrong and in applying that understanding to their decisions.

International Information System Security Certification Consortium (I S C squared).

- ISC squared is a not-for-profit organisation that specialises in training and certification for cybersecurity professionals such as the Certified Information Systems Security Professionals or C I S S P.

ISC squared code of ethics states:

- Members of I S C squared must protect society, the commonwealth, and the infrastructure.
- Members of I S C squared must act honourably, honestly, justly, responsibly, and legally.
- Members of I S C squared provide diligent and competent service to principals.
- Members of I S C squared advance and protect the profession.

Institute of Electrical and Electronics Engineers (IEEE).

The IEEE is a professional association for electrical and electronic engineers that aims to uphold the highest standards of integrity, responsible behaviour, and ethical conduct in professional activities.

IEEE code of ethics states:

- IEEE members must ensure the safety, health, and welfare of the public.
- IEEE members must help the public understand the capabilities and societal implications of conventional and emerging tech, including intelligent systems.
- IEEE members must avoid conflicts of interests, whether real or perceived, and disclose them to stakeholders if conflicts of interests exist.
- IEEE members must avoid unlawful conduct in professional activities and reject bribery in all forms.
- IEEE members must seek, accept, and offer honest criticism of technical work and acknowledge and correct errors.
- IEEE members must undertake tasks, only if qualified.
- IEEE members must treat everyone fairly (indiscriminately) and with respect.
- IEEE members must not engage in harassment and bullying.
- IEEE members must avoid injury to people and property.
- IEEE members must provide support to colleagues to promote and uphold the code of ethics

Australian Computing Society (ACS).

The Australian Computer Society is an association for information and communications technology professionals with aims to uphold and advance the honour, dignity, and effectiveness of being an ACS member and computing professional.

ACS code of ethics states:

- ACS members must place the interests of the public above those of personal, business, or sectional interests.
- ACS members must strive to enhance the quality of life of those affected by the work being produced.
- ACS members must be honest in the representation of skills, knowledge, services, and products.
- ACS members must work competently and diligently for all stakeholders.
- ACS members must enhance one's own professional development, and that of one's staff.
- ACS members must enhance the integrity of the ACS and the respect of its members for each other.

Ports and port scanning.

What are ports and port numbers?

- Computer ports are the central docking point for the flow of information from a program or the internet, to a device or another computer in the network, and vice versa. Like a parking spot for data to be exchanged.
- Port numbers are used for consistency and programming.
- Port numbers combined with IP addresses form the vital information kept by ISPs to fulfill requests.
- Ports range from 0 to 65,536 and are basically ranked by popularity.
- Ports from 0 to 1023 are well known port numbers designed for internet use and have specialised purposes. They are administered by the Internet Assigned Numbers Authority (IANA) and are held by top-tier companies like Apple, SQL services, Google etcetera.
- Port 20 is a User Datagram Protocol or UDP that holds a File Transfer Protocol (FTP) used for data transfer.
- Port 22 is a Transmission Control Protocol or TCP that holds Secure Shell protocol or SSH for secure logins.
- Port 53 is a UDP for Domain Name System (DNS) which translates names to IP addresses.
- Ports 1024 to 49151 are considered registered ports meaning they are registered by software corporations.
- Ports 49151 to 65536 are dynamic and private ports and are accessible to nearly everyone.

Open ports.

- Open ports are computer ports that are actively listening and are essentially open for communication.
- Open ports indicate the target server or network is actively accepting connections or datagrams.
- Open port discovery is the ultimate goal of a cyber-criminal looking for a way in to a system.
- Open ports need protection with use of firewalls to limit unauthorised access without limiting access for legitimate users.

Closed ports.

- Closed ports are computer ports that are not actively listening and essentially closed for communication.
- Closed ports are still accessible, and they can be useful in showing that a host is on an IP address.
- Closed ports should still be monitored in the event they change to an open status and potentially create vulnerabilities.
- Closed ports should be firewalled to create filtered ports.

Filtered ports.

- Filtered ports are computer ports that are not actively listening and provide no response to packets received.
- Filtered ports are typically firewalled meaning, they block requests.
- Filtered ports respond with error messages such as destination unreachable and prevent hackers from obtaining further information.

What is port scanning?

- Port scanning is a method of determining which ports on a network are open and could be receiving or sending data.
- Port scanning is a process for sending packets to specific ports on a host and analysing responses to identify vulnerabilities.
- Port scanning cannot take place without first identifying a list of active hosts and mapping those hosts to their IP addresses.
- Port scanning aims to identify the organisation of IP addresses, hosts, and ports to properly determine open or vulnerable server locations and diagnose security levels.
- Port scanning can reveal the presence of security measures in place such as a firewall between the server and the user's device.
- Port scanning can identify open ports on a network that may enable unauthorized access, once a thorough network scan is completed, and a list of active hosts is compiled.

What is a network mapper or N-Map?

- N-map is a free, open-source tool for vulnerability scanning and network discovery.
- N-map is used to help network administrators identify devices running on their systems.
- N-map is used to discover hosts that are available, and the services being offered.
- N-map is used to find open ports and for detecting security risks.
- N-map is a port scanning, port discovery, and enumeration tool.

How do devices communicate and what is a 3-way handshake?

- A three-way handshake is a method used in a TCP IP network to create a connection between a local host or client and a server.
- It is a three-step method designed to allow both communication ends to initiate and negotiate the parameters of the connection.
- The three-way handshake also known as the SYN-SYN-ACK requires both the client and server to exchange synchronization (SYN) and acknowledgment (ACK) packets before actual data communication begins.
- The first step in handshake is a connection between the client and server that is established through the server's open ports. The client sends a SYN packet over IP network to the server to see whether the server is accepting new connections.
- The second step is the server responding with an ACK to the SYN packet it received or SYN-ACK. It then sends its own SYN packet back to the client for acknowledgement.
- The third step is the client receiving the SYN ACK packet that is sent by the server and responds with an ACK packet subsequently allowing the client and server to connect and communicate.

What is TCP SYN scan?

- TCP SYN scan is also known as SYN-scanning or half-open scanning
- TCP SYN scanning is where the full TCP connection is never made.
- TCP SYN scanning only sends the first packet, the SYN packet. It waits for the response from the server and replies with an TCP reset or RST packet.
- TCP SYN scanning is beneficial for hackers because most server logging applications only create log entries when an ACK is received from the client, and not when an RST received.
- TCP SYN scans can be thwarted by making sure ports are filtered, unused ports are closed, and periodical scans are completed at least bi-annually or when there is a major change to system infrastructure.

What is Metasploit?

- Metasploit is a penetration testing tool.
- Metasploit can be used to probe networks and applications for flaws and vulnerabilities at any point along the production and deployment process.
- Metasploit is ruby-based and open-sourced and allows for testing via command line or GUI.

Cryptography.

Symmetric encryption.

- Symmetric key encryption involves encrypting data using a single key to encrypt the data and using the same key to decipher or decrypt the coded data.
- Symmetric key algorithms use either stream or block ciphers to encrypt or decrypt data. A stream cipher converts plaintext into ciphertext one byte at a time, and a block cipher converts entire units, or blocks, of plaintext using a predetermined key length, such as 128, 192, or 256 bits.
- Symmetric encryption is secure, fast and is industry approved.

What are some examples of symmetric encryption?

- Data Encryption Standard or D E S is a 56-bit block cipher, but it is obsolete and considered a legacy algorithm due to its ineffectiveness to safeguard against brute-force attacks.
- Triple D E S or 3 D E S is a 64-bit block cipher and uses the D E S cipher 3 times to encrypt data, but it is also considered a legacy algorithm and will be decommissioned and disallowed in 2023 because of its security flaws.
- Advanced Encryption Standard or A E S is a 256-bit block cipher and is considered the global standard due to its use of a Substitution Permutation Network algorithm or SPN algorithm which applies multiple rounds of encryption. This standard is used by government agencies, healthcare, and banking, as well as by VPN providers, and communication apps like WhatsApp and Signal.

Asymmetric encryption.

- Asymmetric encryption uses two different but matching keys for encryption and decryption. The first key is a public key encryption and used to encrypt the data. The second key is the private key, used for deciphering the encrypted data.
- Asymmetric encryption means key distribution is not necessary which reduces the chance of keys falling into the wrong hands.

Hash algorithms.

- Hash algorithms is a function that converts a data string into a numeric string output of fixed length. The output string is generally much smaller than the original data.
- Hash algorithms are designed to be collision-resistant, meaning that there is a very low probability that the same string would be created for different data.
- Hash algorithms are used to protect the integrity of a transmission. Should any tampering occur the hash value will change. For example, if the hash of a plaintext changes, the plaintext itself changes.

Internet of things. IOT.

IOT.

- IOT is used to describe any device that uses the internet to transfer data to a separate device as part of a communication process.
- IOT applications include personal, public, and private infrastructure.
- IOT is essentially everywhere and connected to everything society does.
- IOT such as smart and connected devices and technology helps improve processes, productivity, user experience, and cost reduction.
- IOT can be observed in factories, hospitals, cities, homes and in vehicles.
- IOT devices are subject to vulnerabilities and security risks and challenges.
- IOT devices are predominantly low-powered devices with limited computational capacity which leaves them vulnerable because they lack the necessary built-in security controls to defend against threats.

IOT Vulnerabilities.

- IOT vulnerabilities include weak password protection.
- Lack of regular patches and updates and weak update mechanism.
- Insecure interfaces.
- IOT vulnerabilities include insecure network services.
- Insufficient privacy and data protection.
- Poor IoT device management.
- IOT vulnerabilities include insecure Data Transfer and Storage.
- The IoT skills gap.
- Outdated components.
- Lack of Physical Hardening.

The best algorithm for IOT encryption.

- A E S or Two-Fish are both symmetric block algorithms. However, Two-Fish works efficiently with lower capacity processors and IOT device smart cards which may suit a broader spectrum of IOT devices.

Web security.

In general, web security refers to the protective measures and protocols that organizations adopt to protect the organization from, cyber criminals and threats that use the web channel. Web security is critical to business continuity and to protecting data, users, and companies from risk.

What is Structured Query Language (SQL)?

- SQL is a data management language used to handle data in relational databases.
- SQL helps create and modify the structure of databases and tables.
- SQL can be used to store, manipulate, and retrieve data from databases and tables.
- SQL is a non-procedural or declarative query language, which means the user specifies which data is required without specifying how to retrieve it.

What is SQL injection?

- SQL injection is a web security vulnerability that allows an attacker to interfere with the queries that an application makes to its database.
- SQL injection generally allows an attacker to view data that they are not normally able to retrieve, including data belonging to other users or any other data that the application itself is able to access.
- SQL injections allow the hacker to modify or delete this data, causing persistent changes to the application's content or behaviour.
- SQL injection attacks can be escalated to compromise the underlying server, other back-end infrastructure or to perform a denial-of-service attack.
- SQL injection attacks can result in unauthorized access to sensitive data, such as passwords, credit card details, or personal user information.

What is O W A S P?

The Open Web Application Security Project is an online community that produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security. The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

O W A S P Top 10 vulnerabilities 2021.

- Number 1, Broken Access Control**.** Access controls enforce policies so that users cannot act outside of their intended permissions. Failures typically lead to unauthorized information disclosure or modification, destruction of data, or performing a business function outside the user's limits.
- Number 2, Cryptographic Failures. Previously known as Sensitive Data Exposure, Cryptographic Failures involve protecting data in transit and at rest. This includes passwords, credit card numbers, health records, personal information, and business secrets that require extra protection, especially if that data falls under privacy laws.
- Number 3, Injection. Injection, which now includes Cross-Site Scripting, occurs when untrusted data is sent to an interpreter as part of a command or query, tricking the interpreter into executing unintended commands or accessing data without proper authorization.
- Number 4, Insecure Design. Insecure Design focuses on risks related to design flaws. This means using more threat modelling, secure design patterns and principles, and reference architectures to address security concerns earlier in the development process.
- Number 5, Security Misconfiguration. This category includes such things as missing security hardening across any part of the application stack, improperly configured permissions on cloud services, any unnecessary features that are enabled or installed, and unchanged default accounts or passwords.
- Number 6, Vulnerable and Outdated Components. This category includes any software that is vulnerable, unsupported, or out of date. Meaning versions components are unknown (including all direct and indirect dependencies) or added risk because regular scans are not completed to test components. There are, however, effective automated Software Composition Analysis solutions available to help manage open source dependencies.
- Number 7, Identification and Authentication Failures. Security risk occurs when a user identity, authentication, or session management is not properly handled, allowing attackers to exploit passwords, keys, session tokens, or implementation flaws to assume user identities, temporarily or permanently.

- Number 8, Software and Data Integrity Failures. Software and data integrity failures refer to code and infrastructure that fails to protect against integrity violations. This includes software updates, critical data, and continuous integration and continuous delivery pipelines that are implemented without verification. Examples include objects or data encoded or serialized into a structure that an attacker can modify, or applications that rely upon plug-ins, libraries, or modules from untrusted sources, or apps with auto-update functionality, in which updates are downloaded without sufficient integrity verification and applied to a previously trusted application. In the last example, the integrity failure relates to potential infiltration of the supply chain by an attacker to distribute malicious updates.
- Number 9, Security Logging and Monitoring Failures. This category includes errors in detecting, escalating, and responding to active breaches. Without logging and monitoring, breaches cannot be detected. Examples of insufficient logging, detection, and monitoring include not logging auditable events like log-ins or failed log-ins, warnings and errors that generate inadequate or unclear log messages, or logs that are only stored locally. Failures in this category impact visibility, incident alerting, and forensics.
- Number 10, Server-Side Request Forgery or SSRF. Server-Side Request Forgery is an attack that allows attackers to send malicious requests to other systems via a vulnerable web server. Typical SSRF attacks include forcing the server to connect to internal-only services within the organization's infrastructure or forcing the server to connect to arbitrary external systems, potentially leaking sensitive data such as authorization credentials. SSRFs can be circumvented by using firewalls, by using black and whitelisting, by not sending raw responses, and by enforcing URL schemas, like not using ftp, file, or http. Sticking only to https.

Null sessions.

- Null sessions are anonymous connections to an inter-process communication network service on Windows-based computers.
- Null sessions are designed to allow named pipe connections but may be used by attackers to remotely gather information about the system.
- Null sessions occurs when a system log-in requires no username or password.
- Null sessions have multiple security issues that include allowing hackers read and write access on the computers on the network.
- Null sessions can be used to insert malicious code and other materials onto computers without passwords.

Countermeasures:

- Disable null sessions.
- Monitor incoming sessions with firewall.
- Educate administrators not to use null sessions.

Malware.

- Malware is short for and used as an umbrella term to describe all types of malicious software.
- Malware is a file or a code, designed to cause damage to a user's personal computer and network.
- Malware is designed to attack organizations, corporations, and individuals by destroying data and resources, causing errors, and reducing the performance of computer systems.
- Malware can be delivered to a networked system through emails, software installations or surfing the web.
- Malware which includes viruses such as trojan horses and worms, and spyware are considered the more harmful types of malicious software.
- Malware can be removed by anti-virus software.

Spyware.

- Spyware is a form of malware designed to track and collect user information.
- Spyware programs generally install themselves on a user's computer and provides profit to the third parties by collecting user data without the user's awareness.
- Spyware includes keyloggers that track and log keystrokes and screen shots which could contain personal and financial information, such as passwords, pin codes, credit card numbers for identity theft crimes.

Payload.

- Payload, in computer networking is the carrying capacity of a packet or other transmission data unit, the "actual data".
- Payload in cybersecurity refers to the component of a computer virus that executes a malicious activity. For example, payload of malicious programs includes damage to data, theft of confidential information and damage to computer-based systems or processes.

Root Access.

- Root access is the highest permission elevation on a computer system with authorization to execute any command and access any resource on a device.
- Root access permission is typically reserved for those who are authorized to make operating system level changes.
- Root access is essentially the name of the administrator account that gives the full access to system folders and files and enables their editing.

Wireless Security.

What is IEEE 802.11? and what does it mean?

- IEEE 802.11 refers to the set of standards that define communication for wireless local area networks or W-LAN.
- IEEE 802.11 is overseen by the IEEE LAN and MAN Standards Committee.
- IEEE 802.11 is the set of technical guidelines for implementing Wi-Fi. Selling products under this trademark is overseen by an industry trade association called Wi-Fi Alliance.
- IEEE 802.11 family of standards refers to one standard (IEEE 802.11-2007) but many amendments. Commonly known amendments include 802.11a, 802.11b, 802.11G, and 802.11n.

What is Wi-Fi Protected Setup? or WPS?.

- WPS is a wireless network security standard that tries to make connections between a router and wireless devices faster and easier.
- WPS typically involves a push button method to connect.
- WPS is not 100 per cent secure and is susceptible to brute-force attacks.
- WPS can be activated by anyone who has physical access to the router.

What is Wired Equivalent Privacy? Or WEP?

- WEP is a security protocol, specified in the IEEE Wireless Fidelity or Wi-Fi standard, 802.11b.
- WEP uses encryption algorithms applied to data streams, called stream ciphers, and can be vulnerable to attacks when a key is reused. The protocol's relatively small key space makes it impossible to avoid reusing keys.
- WEP uses an RC4 algorithm which has come under cryptographic scrutiny and is no longer considered safe.

What is Wi-Fi Protected Access? Or WPA and WPA2?

- WPA security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks.
- WPA was considered as an intermediate measure to take the place of WEP pending the availability of the full IEEE 802.11i standard.
- WPA2 replaced WPA in 2004 and supported A E S encryption modes providing more security than the WPA standard.
- WPA2 is to be used whenever possible.

What is a Media Access Control address? Or MAC address?

- A MAC address is a hexadecimal number that uniquely identifies each device on a network.
- MAC addresses are provided by the Network Interface Controller card and used to ensure the physical address of the device.
- MAC addresses are different from an IP addresses.
- MAC addresses defines the devices' identity, but IP address describes how the devices are connected to the network.
- MAC addresses can be used to allow or block devices from joining a network by using access controls.
- MAC addresses can be spoofed which is a technique used to mask or change a computer's identity.

What is the difference between static and dynamic IP addresses?

- Static IP addresses are simply IP addresses that do not change.
- Static IP addresses are typically assigned to a device until it's decommissioned or there are major network changes.
- Static IP addresses are generally used by servers and assigned by Internet Service Providers.
- Static IP addresses may be IPv4 or IPv6.
- Static IP addresses makes it easier for hackers due to the static nature.
- Dynamic IP addresses are non-static and subject to change.
- Dynamic addresses are assigned, as needed, by Dynamic Host Configuration Protocol servers otherwise known as DHCP servers.
- Dynamic addresses are used in situations where IPv4 doesn't provide enough available static IP addresses. Like hotels, who may have a static IP address but separate dynamic IP addresses for each room.

What is the Service Set Identifier? Or SSID?

- SSID is the name of a wireless network or wireless networks.
- SSID is the network name visible when devices are trying to connect to a wireless connection.
- The default SSID contains the manufacturers name and should be changed to prevent hackers using rainbow tables to hack into the network.

Passwords.

Passwords provide the first line of defence against unauthorized access to computer systems and personal information. The stronger the password, the more protected the computer will be from hackers and malicious software. Strong passwords should be maintained for all accounts on the computer.

Password elements to consider:

- Use a unique password for each important account (i.e., email and online banking). Do not use the same password across multiple accounts.
- Use a password at least 8 characters long. Passwords should consist of lowercase and uppercase letters, numbers, and symbols. Logically, a properly constructed long password will offer more protection than a short one.
- Do not use personal information such as names, age, date of birth, children's names, pet's names, or favourite colour or song when constructing passwords.
- Do not use consecutive keyboard combinations like qwerty or A S D F G.
- Look around to ensure no one is watching as the passwords are entered.
- Always log off or sign out if device is no longer being used for the day.
- Never enter passwords on computers, the user does not own or control. Malicious software may be installed to purposely steal passwords.
- Never enter passwords when connected to unsecured Wi-Fi connections (like at an airport or coffee shop). Hackers are able to intercept passwords and data over unsecured connections.
- Never disclose passwords.
- Change passwords regularly and avoid using same passwords over and over again.
- Never write down passwords.
- Always select "never" when an Internet browser asks for permission to remember passwords.