

Google Cybersecurity Notes:

Description: Study notes for the Google Cybersecurity Professional Certificate.

Written By: Pedro Osorio Lopez.

About Me: www.linkedin.com/in/pedro-osorio-lópez-756809293

Index: These notes cover the eight courses from the Google Cybersecurity Certificate:

-Topic 1: Introduction to Cybersecurity (pages 2-4).

-Topic 2: How to Manage Security Risks & Threats (pages 5-9).

-Topic 3: Internet Networks & Network Security (pages 10-15).

-Topic 4: The Basics of Computing Security: Linux & SQL (pages 16-21).

-Topic 5: Cybersecurity Assets, Network Threats & Vulnerabilities (pages 22-27).

-Topic 6: Cybersecurity Detection & Response (pages 28-32).

-Topic 7: Fundamentals of Python for Cybersecurity (pages 33-37).

-Topic 8: How to Prepare for your Cybersecurity Career (pages 38-41).

References: <https://www.coursera.org/professional-certificates/google-cybersecurity>

Last Updated: November 14th, 2023.

Topic 1: Introduction to Cybersecurity.

-What is Cybersecurity:

*Cybersecurity is the practice of ensuring the integrity, confidentiality, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.

*Treat Actors: Persons or groups that present a risk. Can be internal (from inside a company, on purpose or by accident, or external).

*Benefits of security: Protection against threats, meet regulatory compliance, improve business productivity, and reduce expenses.

*Common job titles: Security/cybersecurity analyst (protect systems, installing prevention software, conducting periodic audits, etc), security operations Center (SOC) analyst, and information security analyst.



-Core Skills for cybersecurity professionals:

*Communication (describe tasks, procedures, etc to people that may not necessarily have their technical background).

*Collaboration: Working with project managers, ethical hackers, security analysts, etc in a team.

*Analysis: Being able to analyze complex situations.

*Problem solving: Identifying problems and diagnose the proper solutions.

-Technical skills for security analysts:

*Programming languages (automate tasks/identifying errors).

*Use Security Information and Event Management (SIEM) tools (alert that unknown users attempted to access a system).

*Note: PII (Personality Identifiable Information) is any information used to infer individual identities (ids, ips, etc) SPII (Sensitive PII) is a specific type of PII with stricter handling guidelines (SSN, Face ID, etc).

-History of Security:

*Computer Viruses: Malicious code written to interfere with computer ops and cause damage to data and software. Worms are viruses that can replicate without human intervention.


*Malware: Software designed to harm devices/networks. The Brain Malware (1986) created to prevent piracy, but ended up replicating globally. The Morris Worm (1988) created to assess the size of the internet by attaching itself to other computers, ended up replicating in them, crashing their systems.

*Digital Age: With the expansion of the high-speed internet, the numbers of computers attached to it increased dramatically. Physical disks were no longer required to spread viruses. Two notable attacks: The Love Letter Malware (2000) created to steal internet login credentials through emails


*Social engineering: Manipulation technique that exploits human error to gain private information, access. Ex: Phishing, which is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

*Equifax Breach: In 2017 attackers successfully infiltrated the credit reporting agency, stealing over 143 million customer records (40% of Americans). The company failed to detect security vulnerabilities prior to the attack.


The Equifax Breach – A Global Settlement



\$575,000,000+ settlement



Free credit monitoring and identity theft services



Strong **data security** requirements

Learn more: ftc.gov/Equifax

-Eight Security Domains:

*Security and Risk Management: Defines security goals and objectives, risk mitigation, compliance, business continuity, and the law.

*Asset Security: Secures digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data.

*Security Architecture and Engineering: Optimizes data security by ensuring effective tools, systems, and processes are in place.

*Communication and Network Security: Manage and secure physical networks and wireless communications.

*Identity and Access Management: Keeps data secure by ensuring users follow established policies to control and manage physical assets (items perceived as valuable by an organization), like office spaces, and logical assets, such as networks and applications.

*Security Assessment and Testing: Conducting security control testing, collecting, and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.

*Security Operations: Conducting investigations and implementing preventative measures.

*Software Development Security: Uses secure coding practices, which are a set of recommended guidelines that are used to create secure applications and services.

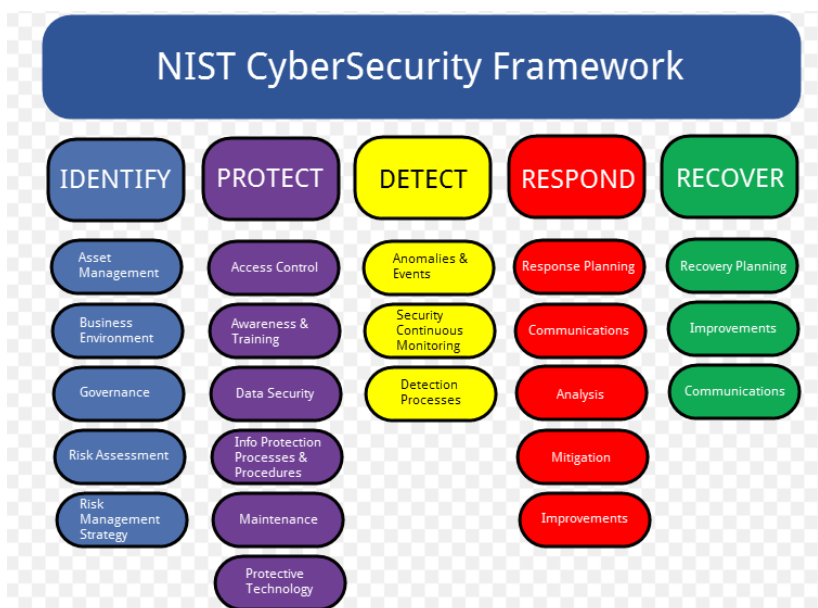
-Security frameworks and controls:

*Security frameworks: Guidelines used for building plans to help mitigate risk and threats to data and privacy. Their goals are protecting PII, securing financial information, identifying security weaknesses, managing organizational risks, and aligning security with business goals.

*Components of Security frameworks: Identifying and documenting security goals, setting guidelines to achieve security goals, implementing security processes, and monitoring and communicating results.

*Security controls: Safeguards designed to reduce specific security risks. The CIA triad is a foundational model that helps inform how organizations consider risk when setting up systems and security policies. Stands for confidentiality (only authorized users can access specific assets or data, integrity (data is correct, authentic, and reliable) and availability (data is accessible to those authorized to access it).

*NIST Cybersecurity Framework (CSF): Voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.



-Ethics for a cybersecurity professional:

*Security ethics: Guidelines for making appropriate decisions as a security professional.

*Ethical principles in security: Confidentiality, privacy protections (safeguarding personal information from unauthorized use) and laws (rules recognized by a community and enforced by a governing entity).

-Tools and programming languages used in cybersecurity:

*Security Information and Event Management (SIEM) tools (applications that collect and analyze log data to monitor critical activities in an organization, ex: SPLUNK and Chronicle), playbooks (manuals that provide details about any operational action), network protocol analyzers (tools designed to capture and analyze data traffic within a network, ex: TCP Dump, Wireshark), Linux OS, programming languages (SQL, used to create, interact with, and request information from a database; and Python, used to perform tasks that are repetitive and time-consuming, and require a high level of detail and accuracy).

*Logs: Record of events that occur within an organization's systems.

Topic 2: How to Manage Security Risks & Threats.

-CISSP:

*Security posture refers to an organization's ability to manage its defense of critical assets and data and react to change.

1. The first domain is **security and risk management**. There are several areas of focus for this domain: defining security goals and objectives, risk mitigation, compliance, business continuity, and legal regulations.

*Risk mitigation means having the right procedures and rules in place to quickly reduce the impact of a risk like a breach.

*Business continuity relates to an organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans.

2. The **asset security** domain is focused on securing digital and physical assets. Security analysts may need to store, maintain, and retain data by creating backups to ensure they are able to restore the environment if a security incident places the organization's data at risk.

3. The third domain is **security architecture and engineering**. This domain is focused on optimizing data security by ensuring effective tools, systems, and processes are in place to protect an organization's assets and data.

*Shared responsibility means that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security.

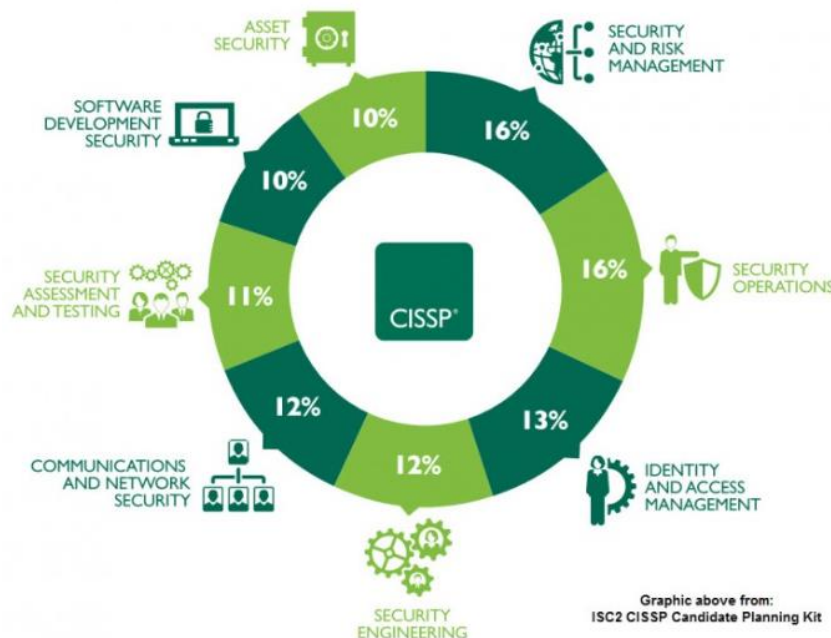
4. The fourth domain is **communication and network security**, which is mainly focused on managing and securing physical networks and wireless communications.

5. The fifth domain is **identity and access management**, or IAM. And it's focused on access and authorization to keep data secure by making sure users follow established policies to control and manage assets. Components of IAM: Identification, authentication, authorization, accountability.

6. The sixth security domain is **security assessment and testing**. This domain focuses on conducting security control testing, collecting, and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities.

7. Next, let's discuss **security operations**. The security operations domain is focused on conducting investigations and implementing preventative measures. Investigations begin once a security incident has been identified.

8. The eighth and final security domain is **software development security**. This domain focuses on using secure coding practices.



-Threats, risks, and vulnerabilities:

*A threat is any circumstance or event that can negatively impact assets.

*Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.

*A risk is anything that can impact the confidentiality, integrity, or availability of an asset. A low-risk asset is information that would not harm the organization's reputation or ongoing operations, and would not cause financial damage if compromised. A medium-risk asset might include information that's not available to the public and may cause some damage to the organization's finances, reputation, or ongoing operations. A high-risk asset is any information protected by regulations or laws, which if compromised, would have a severe negative impact on an organization's finances, ongoing operations, or reputation.

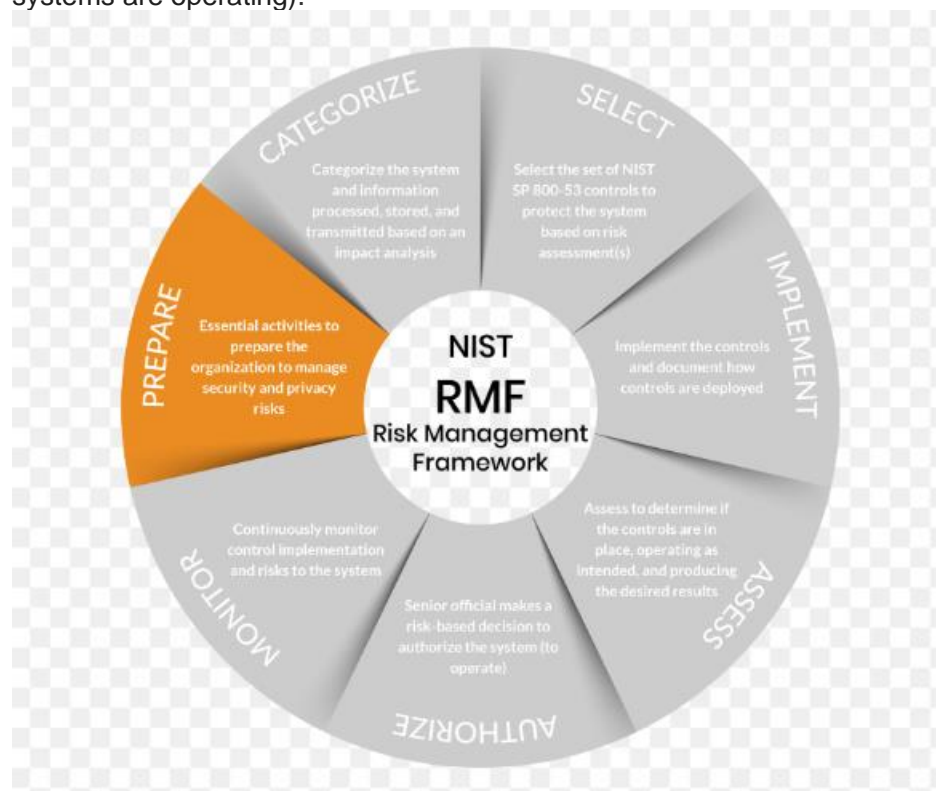
*A vulnerability is a weakness that can be exploited by a threat.

*Ransomware is a malicious attack where threat actors encrypt an organization's data then demand payment to restore access.

*The web is actually an interlinked network of online content that's made up of three layers: the surface web, the deep web, and the dark web.

*Key impacts of threats, risks, and vulnerabilities: financial, identity theft, damage to reputation.

*National Institute of Standards and Technology (NIST) Risk Management Framework (RMF): There are seven steps in the RMF: prepare (activities that are necessary to manage security and privacy risks before a breach occurs), categorize (develop risk management processes and tasks), select (Select means to choose, customize, and capture documentation of the controls that protect an organization), implement (security and privacy plans for the organization), assess (determine if established controls are implemented correctly), authorize (being accountable for the security and privacy risks that may exist in an organization), and monitor (Monitor means to be aware of how systems are operating).



-More about frameworks and controls:

*Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy, such as social engineering attacks and ransomware.

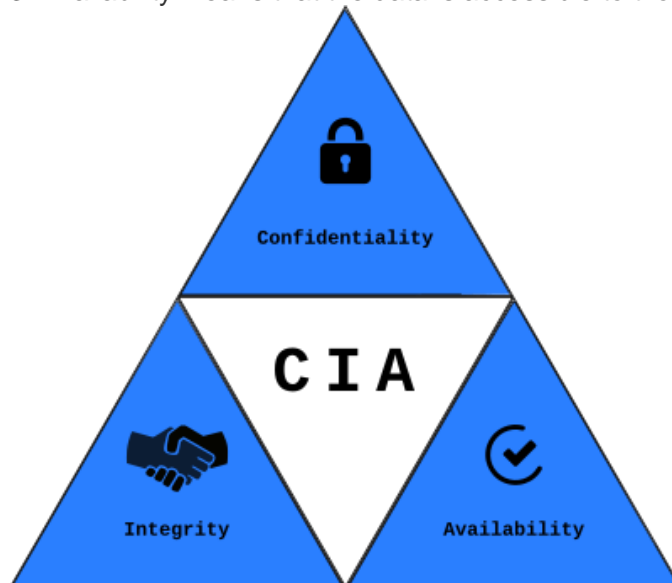
*Controls: Security controls are safeguards designed to reduce specific security risks. Three important types:

1. Encryption is the process of converting data from a readable format to an encoded format.
2. Authentication is the process of verifying who someone or something is. Biometrics are unique physical characteristics that can be used to verify a person's identity. Vishing is the exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
3. Authorization refers to the concept of granting access to specific resources within a system.

-The CIA triad: Confidentiality, integrity, and availability:

*The CIA triad is a model that helps inform how organizations consider risk when setting up systems and security policies.

1. Confidentiality means that only authorized users can access specific assets or data.
2. Integrity means that the data is correct, authentic, and reliable.
3. Availability means that the data is accessible to those who are authorized to access it.



-National Institute of Standards and Technology (NIST) frameworks:

*The NIST CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.

* NIST special publication, or SP 800-53: Provides a unified framework for protecting the security of information systems within the federal government, including the systems provided by private companies for federal government use.

*Five functions of the NIST CSF:

1. Identify, which is related to the management of cybersecurity risk and its effect on an organization's people and assets.
2. Protect, which is the strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats.
3. Detect, which means identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections.
4. Respond, which means making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.
5. Recover, which is the process of returning affected systems back to normal operation.

-OWASP (Open Web Applications Security Project) principles and security audits:

1. Minimize attack surface area. Attack surface refers to all the potential vulnerabilities a threat actor could exploit. 2. Principle of least privilege. Users have the least amount of access required to perform their everyday tasks. 3. Defense in depth: Organizations should have varying security controls that mitigate risks and threats. 4. Separation of duties: Critical actions should rely on multiple people, each of whom follow the principle of least privilege. 5. Keep security simple: Avoid unnecessarily complicated solutions. Complexity makes security difficult. 6. Fix Security issues correctly: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.

*A security audit is a review of an organization's security controls, policies, and procedures against a set of expectations. They can be internal or external (focus on internal here). The purposes of internal security audits are: Identify organizational risk, assess controls, and correct compliance issues. Common elements of internal audits:

1. Establishing the scope and goals.
2. Conducting a risk assessment.
3. Completing a controls assessment.
4. Assessing compliance.
5. Communicating results with stakeholders.

***Scope** refers to the specific criteria of an internal security audit.

***Goals** are an outline of the organization's security objectives, or what they want to achieve in order to improve their security posture.

***Audit questions:** What is the audit meant to achieve? Which assets are most at risk? Are current controls sufficient to protect those assets? What controls and compliance regulations need to be implemented?

***Controls:** administrative controls, technical controls, and physical controls.

***Compliance:** Does it meet GDPR/other necessary regulations?

***Stakeholder Communication:** In general, this type of communication summarizes the scope and goals of the audit. Then, it lists existing risks and notes how quickly those risks need to be addressed. Additionally, it identifies compliance regulations the organization needs to adhere to and provides recommendations for improving the organization's security posture.

-Security information and event management (SIEM) dashboards:

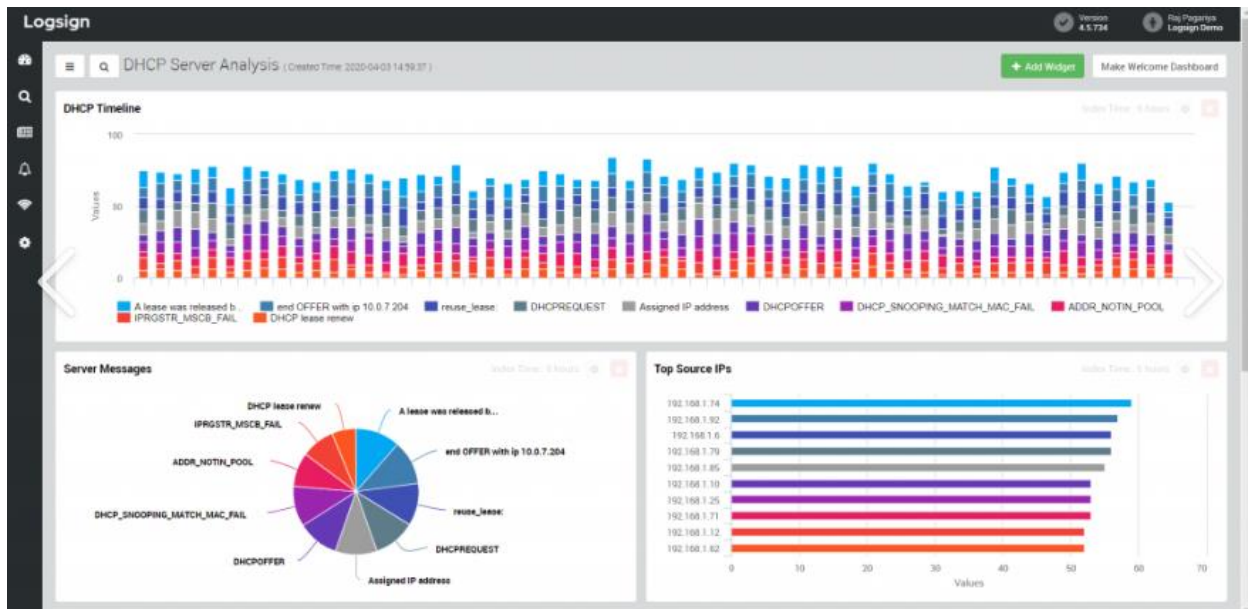
***Log:** Record of events that occur within an organization's systems and networks. Common log sources are:

1. Firewall log: Record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.
2. Network log: Record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.
3. Server log: Record of events related to services such as websites, emails, or file shares. It includes actions such as login, password, and username requests.

***Security information and event management (SIEM) tool:** application that collects and analyzes log data to monitor critical activities in an organization. It provides real-time visibility, event monitoring and analysis, and automated alerts. It also stores all log data in a centralized location.

***SIEM dashboards** help security analysts quickly and easily access their organization's security information as charts, graphs, or tables.

***Metrics** are key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application.



-SIEM Tools:

*Different types of SIEM tools: Self hosted, cloud hosted and hybrid.

*Splunk Enterprise is a self-hosted tool used to retain, analyze, and search an organization's log data to provide security information and alerts in real-time.

*Splunk Cloud is a cloud-hosted tool used to collect, search, and monitor log data.

*Chronicle is a cloud-native tool designed to retain, analyze, and search data.

-Phases of an incident response playbook:

*A playbook is a manual that provides details about any operational action. Playbooks also clarify what tools should be used in response to a security incident.

*Incident response is an organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach. Incident response playbook phases:

1. Preparation. Organizations must prepare to mitigate the likelihood, risk, and impact of a security incident by documenting procedures, establishing staffing plans, and educating users.
2. Detection and analysis. Detect and analyze events using defined processes and technology.
3. Containment. Prevent further damage and reduce the immediate impact of a security incident.
4. Eradication and recovery. Complete removal of an incident's artifacts so that an organization can return to normal operations.
5. Post incident activity. Documenting the incident, informing organizational leadership, and applying lessons learned to ensure that an organization is better prepared to handle future incidents.
6. Coordination. reporting incidents and sharing information, throughout the incident response process, based on the organization's established standards.

Topic 3: Internet Networks & Network Security.

-Introduction to networks:

*A network is a group of connected devices. The devices can communicate through cables or wireless connections.

*To find each other, devices use IP and MAC addresses,

*A local area network, or LAN, spans a small area like an office building, a school, or a home. A wide area network or WAN spans a large geographical area like a city, state, or country.

*A hub is a network device that broadcasts information to every device on the network.

*A switch makes connections between specific devices on a network by sending and receiving data between them.

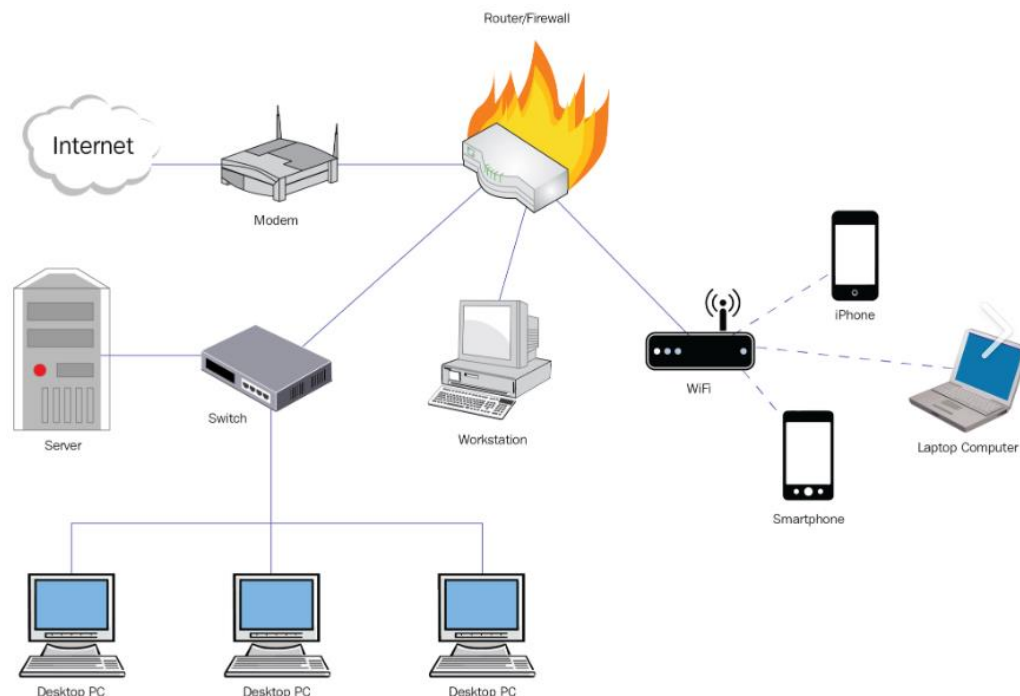
*A router is a network device that connects multiple networks together.

*A modem is a device that connects your router to the internet, and brings internet access to the LAN.

*Virtualization tools are pieces of software that perform network operations.

*Cloud computing is the practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices.

*Cloud service providers offer **cloud computing** to maintain applications. For example, they provide **on-demand storage** and **processing power** that their customers only pay as needed. They also provide business and web **analytics** that organizations can use to monitor their web traffic and sales.



-Network Communication:

*A data packet is a basic unit of information that travels from one device to another within a network.

*A data packet contains a **header** that includes the internet protocol address, the IP address, and the media access control, or MAC, address of the destination device. It also includes a protocol number that tells the receiving device what to do with the information in the packet. Then there's the **body** of the packet, which contains the message that needs to be transmitted to the receiving device. Finally, at the end of the packet, there's a **footer**, similar to a signature on a letter, the footer signals to the receiving device that the packet is finished.

*Bandwidth refers to the amount of data a device receives every second.

*You can calculate bandwidth by dividing the quantity of data by the time in seconds. Speed refers to the rate at which data packets are received or downloaded. Packet sniffing is the practice of capturing and inspecting data packets across the network.

***TCP**, or Transmission Control Protocol, is an internet communication protocol that allows two devices to form a connection and stream data. **IP** has a set of standards used for routing and addressing data packets as they travel between devices on a network. Included in the Internet Protocol (IP) is the IP address that functions as an address for each private network.

*A port is a software-based location that organizes the sending and receiving of data between devices on a network. Ex: Port 20 (Large file transfer), port 25 (email), port 443 (Secure internet communication).

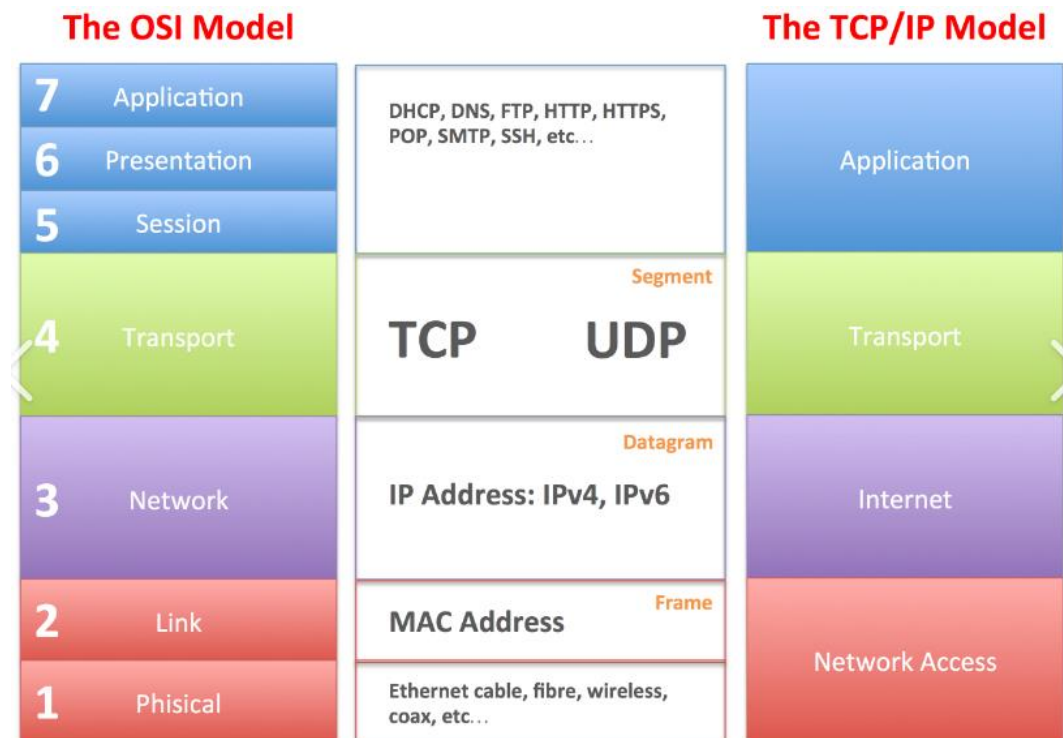
*The TCP/IP model is a framework that is used to visualize how data is organized and transmitted across the network. The TCP/IP model has four layers.

- 1) The network access layer deals with creation of data packets and their transmission across a network.
- 2) The internet layer is where IP addresses are attached to data packets to indicate the location of the sender and receiver.
- 3) The transport layer includes protocols to control the flow of traffic across a network.
- 4) Finally, at the application layer, protocols determine how the data packets will interact with receiving devices.

*An internet protocol address, or IP address, is a unique string of characters that identifies a location of a device on the internet. Each device on the internet has a unique IP address. Types:

- 1) IPv4 addresses are written as four, 1, 2, or 3-digit numbers separated by a decimal point.
- 2) IPv6 addresses are made up of 32 characters.

*A MAC address is a unique alphanumeric identifier that is assigned to each physical device on a network.



-Network protocols:

*Network protocols are a set of rules used by two or more devices on a network to describe the order of delivery and the structure of the data.

*Transmission Control Protocol (TCP) is an internet communication protocol that allows two devices to form a connection and stream data.

*The Address Resolution Protocol, or ARP, is used to determine the MAC address of the next router or device on the path. This ensures that the data gets to the right place.

*The Hypertext Transfer Protocol Secure, or HTTPS, is a network protocol that provides a secure method of communication between client and website servers. HTTPS encrypts data using the Secure Sockets Layer and Transport Layer Security, otherwise known as SSL/TLS.

*Domain Name System, or DNS, is a network protocol that translate internet domain names into IP addresses.

*IEEE 802.11, commonly known as Wi-Fi, is a set of standards that define communications for wireless LANs.

*WPA is a wireless security protocol for devices to connect to the internet.

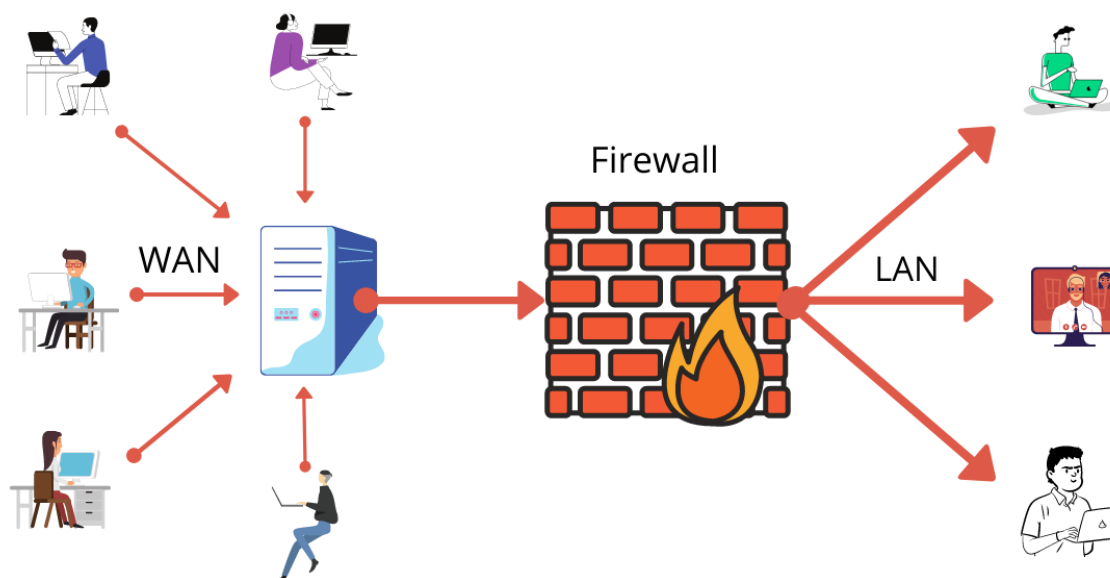
-Firewalls and network security measures:

*A firewall is a network security device that monitors traffic to and from your network. A firewall can use port filtering, which blocks or allows certain port numbers to limit unwanted communication.

*Three main types of firewalls: hardware (physical device that protects a server), software (program that protects a device) and cloud-based (software firewalls hosted by a cloud service provider).

*Stateful refers to a class of firewall that keeps track of information passing through it and proactively filters out threats. A stateless firewall only acts according to preconfigured rules set by the firewall administrator.

*A next generation firewall, or NGFW, provides even more security than a stateful firewall. Not only does an NGFW provide stateful inspection of incoming and outgoing traffic, but it also performs more in-depth security functions like deep packet inspection and intrusion protection.



*A virtual private network, also known as a VPN, is a network security service that changes your public IP address and hides your virtual location so that you can keep your data private when you're using a public network like the internet.

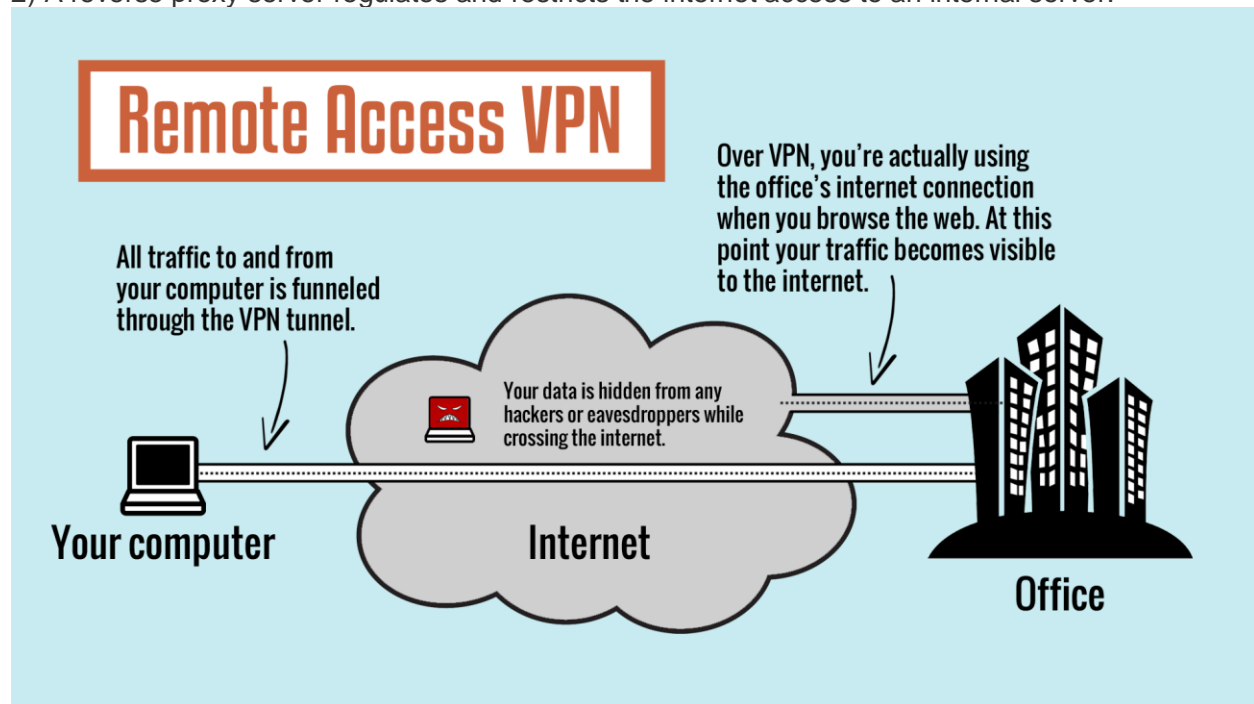
*Encapsulation is a process performed by a VPN service that protects your data by wrapping sensitive data in other data packets.

*Security zones are a segment of a network that protects the internal network from the internet. Two types of security zones. First, there's the uncontrolled zone, which is any network outside of the organization's control, like the internet. Then, there's the controlled zone, which is a subnet that protects the internal network from the uncontrolled zone.

*Areas in the controlled zone: On the outer layer is the demilitarized zone, or DMZ, which contains public-facing services that can access the internet. Then, there are the internal network and the restricted zone (ideally separated through firewalls to protect them in case the external layer is compromised; subnetting).

*A proxy server is a server that fulfills the request of a client by forwarding them on to other servers. There are different types of proxy servers:

- 1) A forward proxy server regulates and restricts a person with access to the internet.
- 2) A reverse proxy server regulates and restricts the internet access to an internal server.



-Secure networks against Denial of Service (DoS) attacks:

*A denial of service attack is an attack that targets a network or server and floods it with network traffic.

*A distributed denial of service attack, or DDoS, is a kind of DoS attack that uses multiple devices or servers in different locations to flood the target network with unwanted traffic.

*A SYN flood attack is a type of DoS attack that simulates the TCP connection and floods the server with SYN packets.

***ICMP** stands for Internet Control Message Protocol. ICMP is an internet protocol used by devices to tell each other about data transmission errors across the network. An **ICMP flood attack** is a type of DoS attack performed by an attacker repeatedly sending ICMP packets to a network server. A **ping of death attack** is a type of DoS attack that is caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64 kilobytes, the maximum size for a correctly formed ICMP packet.

-Network attack tactics and defense:

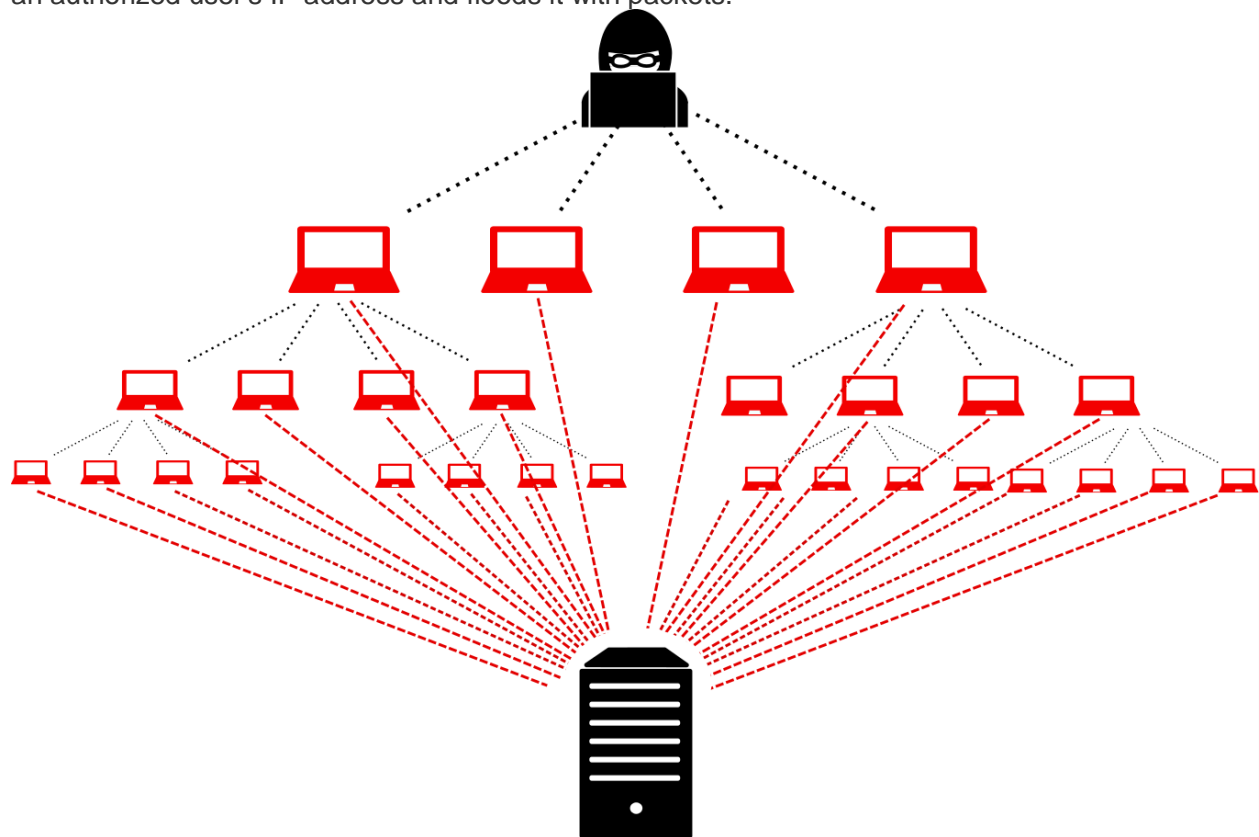
*Packet sniffing is the practice of using software tools to observe data as it moves across a network. Two types:

- 1) Passive packet sniffing is a type of attack where data packets are read in transit.
- 2) Active packet sniffing is a type of attack where data packets are manipulated in transit.

*Packages can be protected with VPNs, using HTTPS, etc.

*IP spoofing is a network attack performed when an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network. Some common types are:

- 1) An on-path attack is an attack where the malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit.
- 2) A replay attack is a network attack performed when a malicious actor intercepts a data packet in transit and delays it or repeats it at another time.
- 3) A smurf attack is a combination of a DDoS attack and an IP spoofing attack. The attacker sniffs an authorized user's IP address and floods it with packets.



-Security Hardening:

*Security hardening is the process of strengthening a system to reduce its vulnerability and attack surface.

*Security hardening can be conducted on any device or system that can be compromised, such as hardware, operating systems, applications, computer networks, and databases.

*Another important strategy for security hardening is to conduct regular **penetration testing**. A penetration test, also called a pen test, is a simulated attack that helps identify vulnerabilities in a system, network, website, application, and process.

*OS: Interface between the hardware and the user. It is very important to protect individually in a system, since one insecure OS could compromise the entire network. A **patch update** is a software and operating system, or OS, update that addresses security vulnerabilities within a program or product. Other OS hardening practices are **password policies** or **multi-factor authentication (MFA)**.

*A baseline configuration is a documented set of specifications within a system that is used as a basis for future builds, releases, and updates.

*Network Security Hardening: Include procedures like port filtering, network access privilege, and encryption. Typical tasks performed to protect networks are: Firewall rules maintenance, network log analysis, patch updates and server backups.

*Network log analysis is the process of examining network logs to identify events of interest.

*A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization.

*Network log and SIEM dashboard analysis are done regularly for maintenance.

*Other tasks are performed only once: Port filtering is a firewall function that blocks or allows certain port numbers to limit unwanted communication. Furthermore, patch updates should be done immediately when available, backups of important data, segmentation of security zones, and encryption of data.



*Network Security in the cloud: A cloud network is a collection of servers or computers that stores resources and data in a remote data center that can be accessed via the internet. One distinction between cloud network hardening and traditional network hardening is the use of a server baseline image for all server instances stored in the cloud. Similar to OS hardening, data and applications on a cloud network are kept separate depending on their service category.

Topic 4: The Basics of Computing Security: Linux & SQL.

-Introduction to operating systems:

*The operating system, or the OS as it's commonly called, is responsible for making the computer run as efficiently as possible while also making it easy to use. Hardware refers to the physical components of a computer.

*An application is a program that performs a specific task. When you do this, the application sends your request to the operating system. From there, the operating system interprets this request and directs it to the appropriate component of the computer's hardware.

*The OS is responsible for ensuring that each program is allocating and de-allocating resources. All this occurs in your computer at the same time so that your system functions efficiently. The user communicates with the operating system via an interface. A user interface is a program that allows a user to control the functions of the operating system. Two main user interfaces:

- 1) A GUI is a user interface that uses icons on the screen to manage different tasks on the computer. Basic GUI components are the start menu, task bar, and desktop.
- 2) In comparison, the command-line interface, or CLI, is a text-based user interface that uses commands to interact with the computer.



-Linux:

*Linux is an open-source operating system.

*The components of Linux include the user, applications, the shell, the Filesystem Hierarchy Standard, the kernel, and the hardware.

- 1) The user is the person interacting with the computer.
- 2) An application is a program that performs a specific task, such as a word processor or a calculator.
- 3) The shell is a command line interpreter.
- 4) Filesystem Hierarchy Standard, or FHS. It's the component of the Linux OS that organizes data.
- 5) The kernel is a component of the Linux OS that manages processes and memory.
- 6) Hardware refers to the physical components of a computer.

*There are different versions of Linux, called distributions. All distros are derived from another distro, but there are a few that are considered parent distributions. Red Hat® is the parent of CentOS, and Slackware® is the parent of SUSE®. Both Ubuntu and KALI LINUX™ are derived from Debian.

*KALI LINUX™ is a trademark of Offensive Security and is Debian derived. This open-source distro was made specifically with penetration testing and digital forensics in mind.

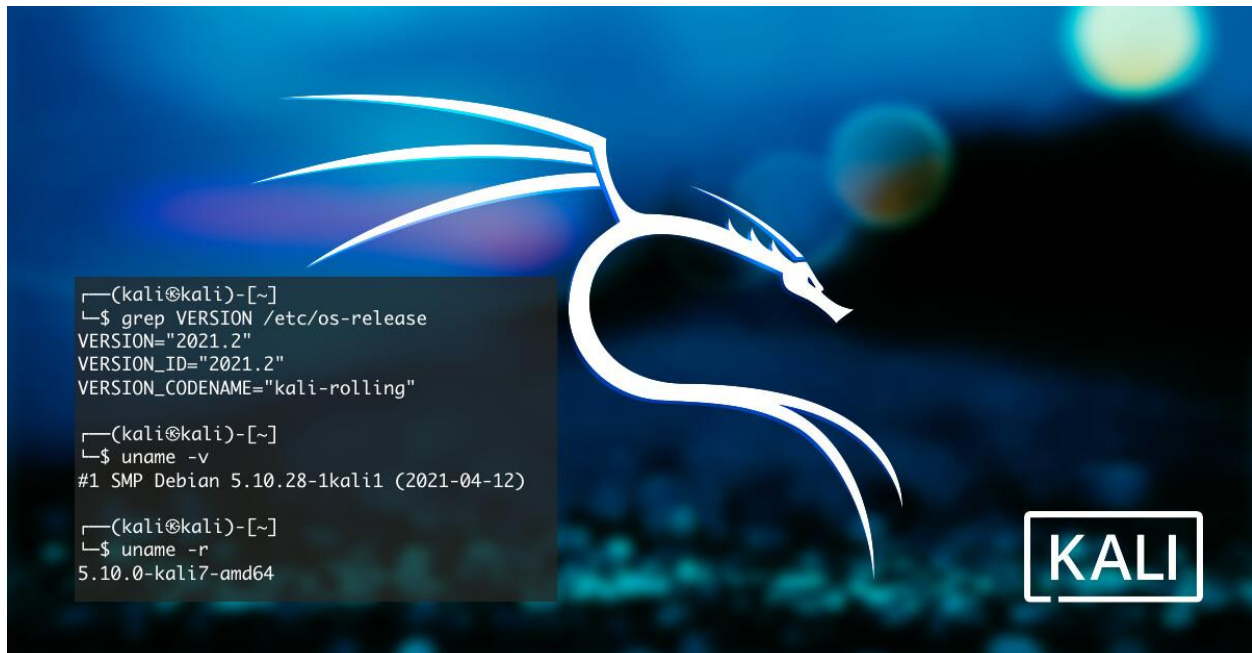
*A penetration test is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes.

*Some built in testing tools in KALI Linux: Metasploit can be used to look for and exploit vulnerabilities on machines. Burp Suite is another tool that helps to test for weaknesses in web applications. And finally, John the Ripper is a tool used to guess passwords.

*Digital forensics is the process of collecting and analyzing data to determine what has happened after an attack. Some digital forensics tools in KALI Linux are: tcpdump, wireshark and autopsy.

*When communicating with the shell: Standard input consists of information received by the OS via the command line. Standard output is the information returned by the OS through the shell.

*Echo is a Linux command that outputs a specified string of text. String data is data consisting of an ordered sequence of characters.



-Navigate the Linux Filesystem:

*As a security analyst, you will work with server logs and you'll need to know how to navigate, manage and analyze files remotely without a graphical user interface. In addition, you'll need to know how to verify and configure users and group access. You'll also need to give authorization and set file permissions.

*Bash is the default shell for most Linux distributions. A command is an instruction telling the computer to do something.

*The root directory is the highest level of directory in Linux. Is indicated with the symbol / Subdirectories branch off from the root tree.

*Core commands for navigating and reading files: pwd (prints working directory), ls (displays files and directories in wd), cd (navigates between directories).

*Showing file content: cat (displays the whole content), head (displays the first 10 lines), tail (opposite to head), less (displays one page at a time).

*Man (manual) gives information on a command. Whatis command displays a description of a command on a single line. Apropos searches the manual page descriptions for a specified string.

```

kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(kali@kali)-[~]
$ cd Documents
(kali@kali)-[~/Documents]
$ ..
(kali@kali)-[~]
$ man ping
(kali@kali)-[~]
$

```

Manage file content:

*The grep command searches a specified file and returns all lines in the file containing a specified string. Another command for searching is find, which searches for files/directories that meet specific criteria (find /home/analyst -name users).

*The piping | command sends a standard output of one command as standard input into another command for further processing. Ex: ls /home/analyst | grep users find every file/directory containing the word users in the home directory.

*mkdir/rmdir: Create/delete directory.

*touch/rm: Create/delete file.

*mv/cp: move/copy file or directory to a new location.

*nano is one of the main file editors in Linux.

```

(kali@kali)-[~]
$ cd Documents
(kali@kali)-[~/Documents]
$ mkdir pruebas
(kali@kali)-[~/Documents]
$ cd pruebas
(kali@kali)-[~/Documents/pruebas]
$ touch prueba1.txt
(kali@kali)-[~/Documents/pruebas]
$ touch prueba2.txt
(kali@kali)-[~/Documents/pruebas]
$ grep *.txt
(kali@kali)-[~/Documents/pruebas]
$ nano prueba1.txt
(kali@kali)-[~/Documents/pruebas]
$ grep Random *.txt
prueba1.txt:Random text
(kali@kali)-[~/Documents/pruebas]
$ rm *
zsh: sure you want to delete all 2 files in /home/kali/Documents/pruebas [yn]? y
(kali@kali)-[~/Documents/pruebas]
$ ls
(kali@kali)-[~/Documents/pruebas]
$ ..
(kali@kali)-[~/Documents]
$ rmdir pruebas

```

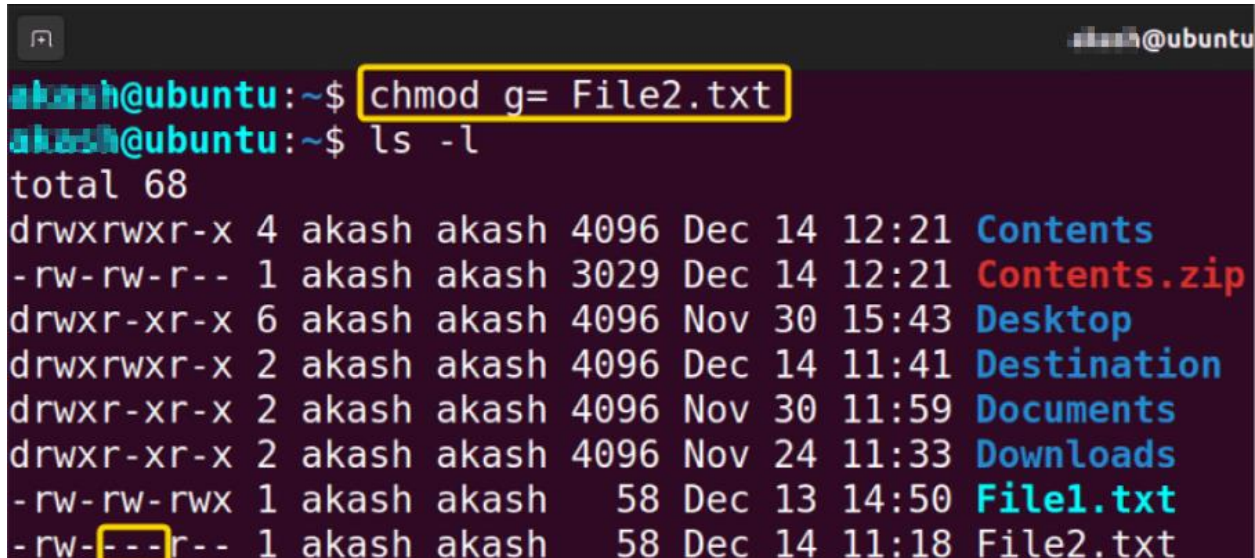

File Permissions and ownership:

*Permissions are the type of access granted for a file or directory. Authorization is the concept of granting access to specific resources in a system. Access should be granted in a need to know basis, using the principle of least privilege.

*Permissions can be read, write, or execute, given to users, groups or other. The first character of the permissions sequence is -(file) or d(directory).

*Options modify the behavior of the command. The options for a command can be a single letter or a full word. Entering ls -l displays permissions to files and directories. Using ls -a display hidden files.

*Chmod changes permissions in files and directories.



```

akash@ubuntu:~$ chmod g= File2.txt
akash@ubuntu:~$ ls -l
total 68
drwxrwxr-x 4 akash akash 4096 Dec 14 12:21 Contents
-rw-rw-r-- 1 akash akash 3029 Dec 14 12:21 Contents.zip
drwxr-xr-x 6 akash akash 4096 Nov 30 15:43 Desktop
drwxrwxr-x 2 akash akash 4096 Dec 14 11:41 Destination
drwxr-xr-x 2 akash akash 4096 Nov 30 11:59 Documents
drwxr-xr-x 2 akash akash 4096 Nov 24 11:33 Downloads
-rw-rw-rwx 1 akash akash 58 Dec 13 14:50 File1.txt
-rw----r-- 1 akash akash 58 Dec 14 11:18 File2.txt
  
```

Add and delete users:

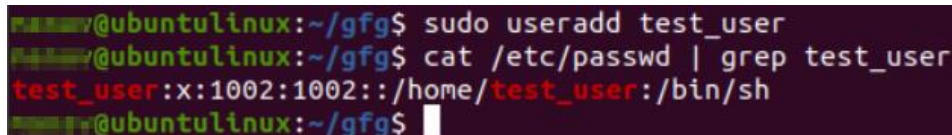
*Root users can create, modify, or delete any file and run any program.

*Sudo is a command that temporarily grants permissions to specific users. This provides more of a controlled approach compared to root, which runs every command with root privileges.

*Adduser/useradd adds a user to the system.

*Deluser/userdel deletes a user from the system.

*Other commands that can be used with sudo are chown (change ownership of a file or directory) and usermod (modify existing user accounts).



```

gfg@ubuntu:~/gfg$ sudo useradd test_user
gfg@ubuntu:~/gfg$ cat /etc/passwd | grep test_user
test_user:x:1002:1002::/home/test_user:/bin/sh
gfg@ubuntu:~/gfg$
  
```

Introduction to SQL and Databases:

* We can define a database as an organized collection of information or data. They can be used by multiple people simultaneously, store massive amounts of data and perform complex tasks while accessing data.

*A relational database is a structured database containing tables that are related to each other.

* The columns that relate two tables to each other are called keys. There are two types:

1) The primary key refers to a column where every row has a unique entry. The primary key must not have any duplicate values, or any null or empty values.

2) The second type of key is a foreign key. The foreign key is a column in a table that is a primary key in another table. Foreign keys, unlike primary keys, can have empty values and duplicates.

* SQL is a programming language used to create, interact with, and request information from a database.

* A log is a record of events that occur within an organization's systems. A common practice is using SQL to find relevant information in security logs.

* A query is a request for data from a database table or a combination of tables. Some important queries are: SELECT indicates which columns to return and FROM: which table to query.

* Syntax refers to the rules that determine what is correctly structured in a computing language. SELECT * shows all columns from a table. ORDER BY specifies a column to sort the entries.

* An operator is a symbol or keyword that represents an operation. An example of an operator would be the equal to operator. WHERE indicates the condition for a filter (ex: WHERE = 'USA'). Filter for 'US%' would return entries that start with USA (ex: where country LIKE 'US%').



```

1  SELECT *
2  FROM customers
3  WHERE favorite_website = 'techonthenet.com'
4  ORDER BY last_name ASC;

```

customer_id	last_name	first_name	favorite_website
4000	Jackson	Joe	techonthenet.com
9000	Johnson	Derek	techonthenet.com

More SQL filters and Joins:

* String data is data consisting of an ordered sequence of characters. Numeric data is data consisting of numbers, such as a count of log-in attempts.

* Some operators to use with numerical data include =, >, <, <>, >=, <=. BETWEEN and AND are operators that filters for numbers or dates within a range.

* To make a query with multiple conditions, we use operators such as AND, OR, NOT, etc. These operators can also be combined in a single query.

* Joining tables when querying a database: We need a shared column to join two tables (a primary key from the first table must be equal to the foreign key of the second one or vice versa).

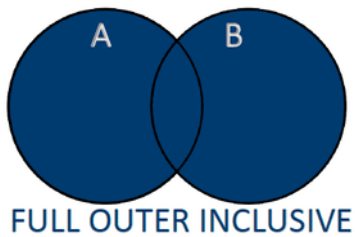
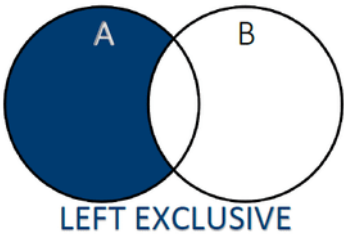
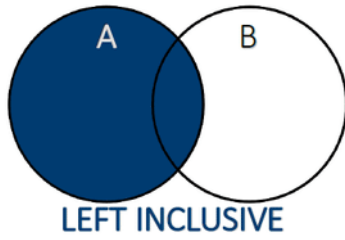
* An INNER JOIN returns rows matching on a specified column that exists in more than one table. Example syntax: INNER JOIN machines ON employees.employee_id = machines.employee_id.

* Outer joins combine two tables together; however, they don't necessarily need a match between columns to return a row. Which rows are returned depends on the type of join.

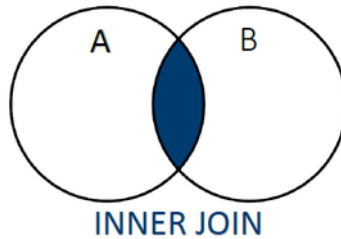
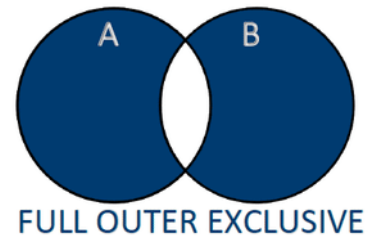
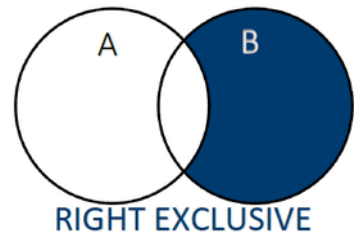
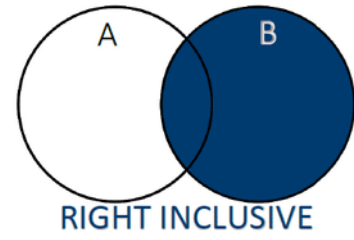
1) LEFT JOIN returns all of the records of the first table, but only returns rows of the second table that match on a specified column.

2) RIGHT JOIN returns all of the records of the second table but only returns rows from the first table that match on a specified column.

3) FULL OUTER JOIN returns all records from both tables.



SQL JOINS	
LEFT INCLUSIVE SELECT [Select List] FROM TableA A LEFT OUTER JOIN TableB B ON A.Key= B.Key	RIGHT INCLUSIVE SELECT [Select List] FROM TableA A RIGHT OUTER JOIN TableB B ON A.Key= B.Key
LEFT EXCLUSIVE SELECT [Select List] FROM TableA A LEFT OUTER JOIN TableB B ON A.Key= B.Key WHERE B.Key IS NULL	RIGHT EXCLUSIVE SELECT [Select List] FROM TableA A LEFT OUTER JOIN TableB B ON A.Key= B.Key WHERE A.Key IS NULL
FULL OUTER INCLUSIVE SELECT [Select List] FROM TableA A FULL OUTER JOIN TableB B ON A.Key = B.Key	FULL OUTER EXCLUSIVE SELECT [Select List] FROM TableA A FULL OUTER JOIN TableB B ON A.Key = B.Key WHERE A.Key IS NULL OR B.Key IS NULL
INNER JOIN SELECT [Select List] FROM TableA A INNER JOIN TableB B ON A.Key = B.Key	



Topic 5: Cybersecurity Assets, Network Threats & Vulnerabilities.

Asset Security:

*In security, a risk is anything that can impact the confidentiality, integrity, or availability of an asset.

*Security plans are based on the analysis of three elements: assets, threats, and vulnerabilities.

1) An asset is an item perceived as having value to an organization.

2) A threat is any circumstance or event that can negatively impact assets.

3) A vulnerability is a weakness that can be exploited by a threat.

*Asset management is the process of tracking assets and the risks that affects them. Asset management starts with having an asset inventory, a catalog of assets that need to be protected.

*Asset classification is the practice of labeling assets based on the sensitivity and importance to an organization. Assets can be public, internal-only, confidential, or restricted.

*Data is information that is translated, processed, or stored by a computer. Data in use is data being accessed by one or more users. Data in transit is data traveling from one point to another. Data at rest is data not currently being accessed.

*The main types of risk categories are: damage, disclosure, and loss of information. These risk categories must be addressed with security plans.

*Security plans consist of three basic elements: policies, standards, and procedures. A policy is a set of rules that reduce risk and protects information. Standards are references that inform how to set policies. Procedures are step-by-step instructions to perform a specific security task.

*Compliance is the process of adhering to internal standards and external regulations. Regulations are rules set by a government or other authority to control the way something is done.

*The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. Three main components: The **core** is basically a simplified version of the functions, or duties, of a security plan (identify, protect, detect, respond, and recover). **Tiers** provide security teams with a way to measure performance across each of the five functions of the core. **Profiles** provide insight into the current state of a security plan.



Security Controls:

*Security controls are safeguards designed to reduce specific security risks. Three types: Technical control types include the many technologies used to protect assets. Operational controls relate to maintaining the day-to-day security environment. Managerial controls are centered around how the other two reduce risk.

*Information privacy is the protection of unauthorized access and distribution of data. To maintain privacy, security controls are intended to limit access based on the user and situation. This is known as the principle of least privilege.

*A data owner is a person who decides who can access, edit, use, or destroy their information. A data custodian is anyone or anything that's responsible for the safe handling, transport, and storage of information. Steps of the data lifecycle: Collect, store, use, archive, destroy.

*Some notable privacy regulations: General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA).



*Personally identifiable information, or PII, is any information that can be used to infer an individual's identity. Cryptography is the process of transforming information into a form that unintended readers can't understand.

*An algorithm is a set of rules that solve a problem. Specifically in cryptography, a cipher is an algorithm that encrypts information. Cryptographic keys are used to decrypt ciphertext. A brute force attack is a trial-and-error process of discovering private information.

*Public key infrastructure, or PKI, is an encryption framework that secures the exchange of information online. Involves either asymmetric, symmetric encryption, or both. Asymmetric encryption involves the use of a public and private key pair for encryption and decryption of data. Symmetric encryption involves the use of a single secret key to exchange information.

*PKI is a two step process: Exchange of encrypted information and establishing trust using a system of digital certificates. A digital certificate is a file that verifies the identity of a public key holder.

*A hash function is an algorithm that produces a code that can't be decrypted. These produce a unique identifier known as hash values. In security, hashes are primarily used as a way to determine the integrity of files and applications.

*Non-repudiation is the concept that authenticity of information can't be denied.

*Access controls: The security controls that manage access, authorization, and accountability of information. The AAA framework includes **authentication** (can be by knowledge, ownership, or characteristic), **authorization** (idea that access to information only lasts as long as needed) and **accounting** (practice of monitoring the access logs of a system).

*Single sign-on, or SSO, is a technology that combines several different logins into one. Multi-factor authentication, or MFA, is a security measure, which requires a user to verify their identity in two or more ways to access a system or network.

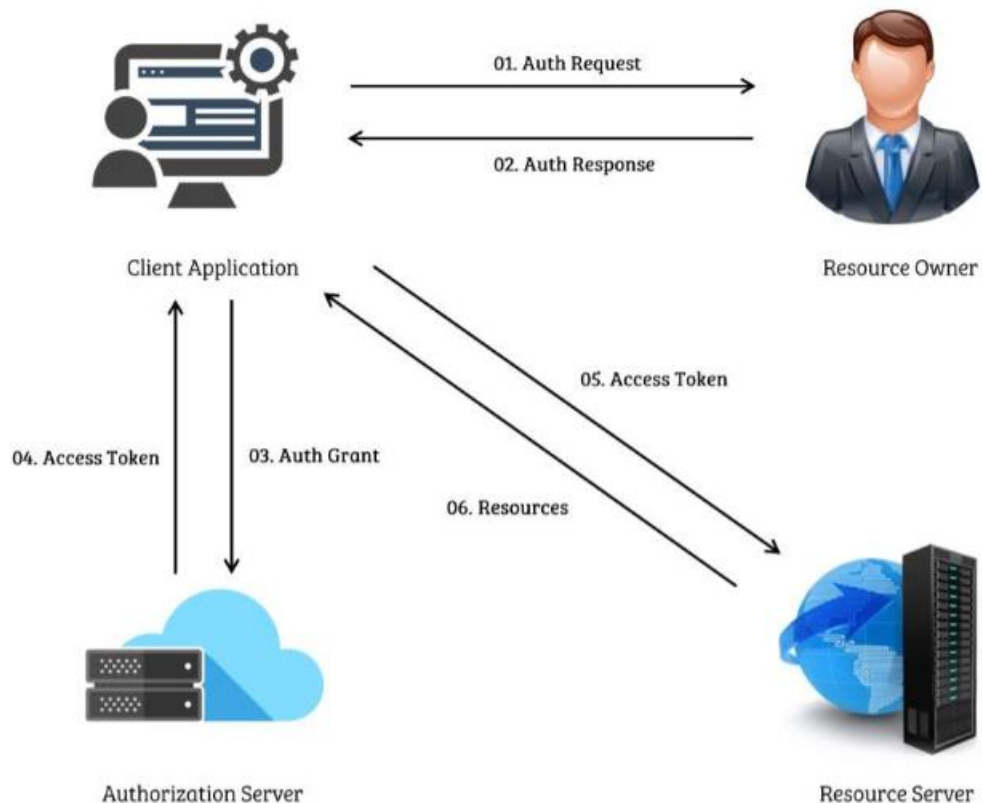
*Separation of duties is the principle that users should not be given levels of authorization that will allow them to misuse a system.

*HTTP Basic auth: Technology used to establish a user's request to access a server. Since this protocol is considered vulnerable, most websites today use HTTPS instead, which stands for hypertext transfer protocol secure. This protocol doesn't expose sensitive information, like access credentials, when communicating over the network.

*OAuth is an open-standard authorization protocol that shares designated access between applications. Uses Application Programming Interface (API) tokens to verify access, which are small blocks of encrypted code that contains information about a user.

*A session is a sequence of network HTTP basic auth requests and responses associated with the same user. Access logs are records of sessions (between a user accesses a system and leaves). Session IDs are attached to the user until they either close their browser or the session times out. A session cookie is a token that websites use to validate a session and determine how long that session should last.

*Session hijacking is an event when attackers obtain a legitimate user's session ID.



Attacks and Vulnerabilities:

*A vulnerability is a weakness that can be exploited by a threat. An exploit is a way of taking advantage of a vulnerability. Vulnerability management is the process of finding and patching vulnerabilities (identify them, consider potential exploits, prepare defenses against threats, and evaluate those defenses). A zero-day is an exploit that was previously unknown.

*Defense in depth is a layered approach to vulnerability management that reduces risk. The strategy consists of 5 layers: Perimeter layer (authentication; usernames/passwords), network layer

(authorization; firewalls), endpoint layer (devices that access the network; antivirus), application layer (interfaces used to interact with the technology; MFA), data layer (information to protect; PII).

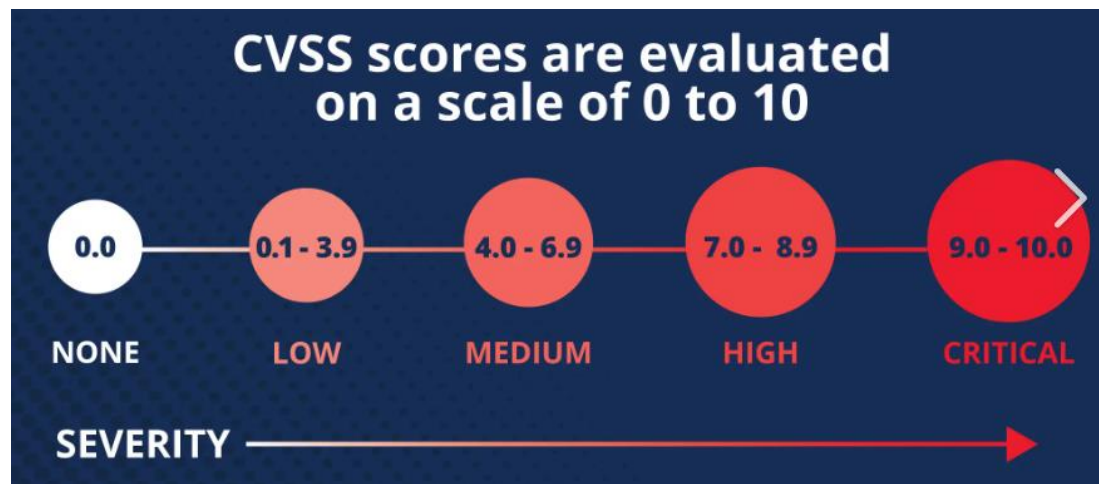
*An exposure is a mistake that can be exploited by a threat.

*The common vulnerabilities and exposures list, or CVE list, is an openly accessible dictionary of known vulnerabilities and exposures. The CVE list was originally created by MITRE corporation in 1999. MITRE is a collection of non-profit research and development centers. They're sponsored by the US government.

*Before a CVE can make it onto the CVE list, it first goes through a strict review process by a CVE Numbering Authority, or CNA. A CNA is an organization that volunteers to analyze and distribute information on eligible CVEs.

*The CVE list tests four criteria that a vulnerability must have before it's assigned an ID. First, it must be independent of other issues. Second, it must be recognized as a potential security risk by whoever reports it. Third, the vulnerability must be submitted with supporting evidence. And finally, the reported vulnerability can only affect one codebase.

*The NIST National Vulnerabilities Database uses what's known as the common vulnerability scoring system, or CVSS, which is a measurement system that scores the severity of a vulnerability.



*A vulnerability assessment is the internal review process of an organization's security systems. The vulnerability assessment is usually a 4 step process: identification (scanning tools and manual testing are used to find vulnerabilities), vulnerability analysis (each of the vulnerabilities that were identified are tested), risk assessment (during this step of the process, a score is assigned to each vulnerability) and remediation (the vulnerabilities that can impact the organization are addressed).

*An attack surface is all the potential vulnerabilities that a threat actor could exploit. Security hardening is the process of strengthening a system to reduce its vulnerabilities and attack surface. These can be physical (devices) or digital (webpages, cloud servers, etc).

*Attack vectors refer to the pathways attacker use to penetrate security defenses (ex: social media, usb drives, etc). To practice an attack mindset: first we identify the target, then we determine how the target can be accessed, evaluate attack vectors, and find the tools and methods of attack.

*Some ways of defending attack vectors: educating users, apply the principle of least privilege, use the right controls and tools, and build a diverse security team.

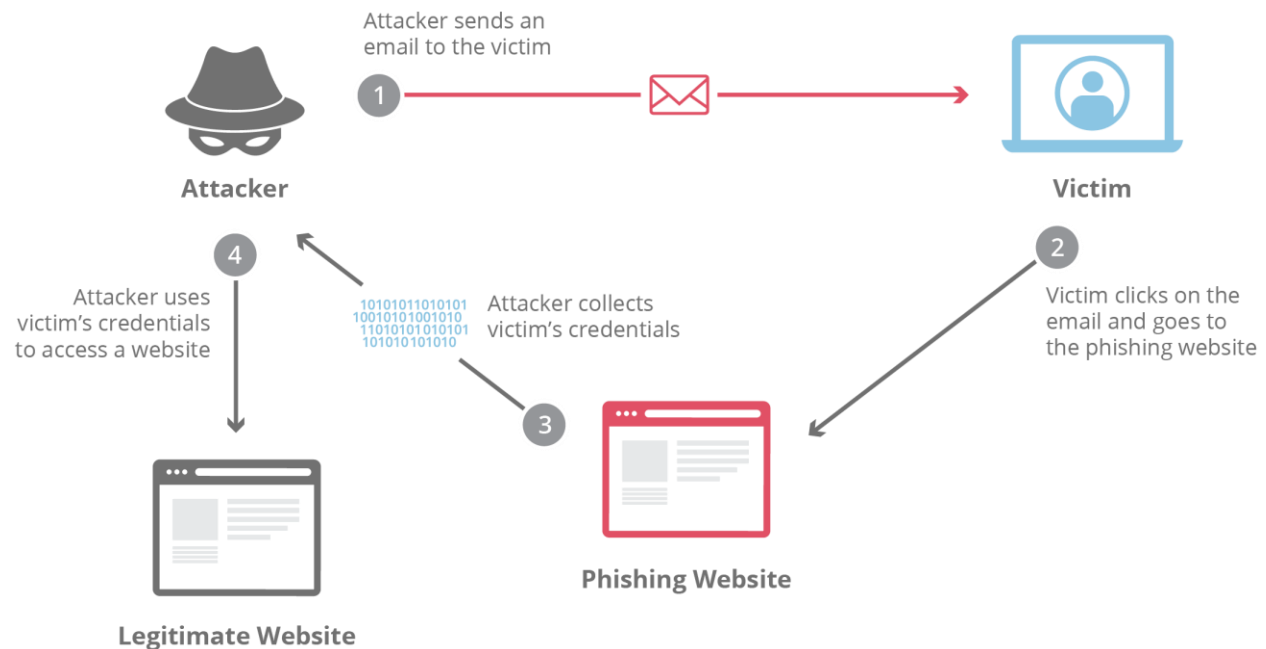
Social engineering, malwares, and threats:

*Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables. It usually consists of several stages: prepare, establish trust, use persuasion tactics, and disconnect from the target. Can be prevented by establishing managerial controls, staying informed of trends, and sharing your knowledge with others.

*Phishing is the use of digital communications to trick people into revealing sensitive data or deploying malicious software. Attackers who carry out these attacks commonly use phishing kits. A phishing kit is a collection of software tools needed to launch a phishing campaign. These include malicious attachments, fake data-collection forms, and fraudulent web links.

*Smishing is the use of text messages to obtain sensitive information or to impersonate a known source. Vishing is the exploitation of electronic voice communication to obtain sensitive information or impersonate a known source.

*Some phishing security measures are: anti-phishing policies, employees training resources, email filter and intrusion prevention systems.



*Malware is software designed to harm devices or networks. Five of the most common types of malware are a virus, worm, trojan, ransomware, and spyware.

*A virus is malicious code written to interfere with computer operations and cause damage to data and software.

*A worm is malware that can duplicate and spread itself across systems on its own.

*A trojan, or Trojan horse, is malware that looks like a legitimate file or program.

*Ransomware is a type of malicious attack where attackers encrypt an organization's data and demand payment to restore access.

*Spyware is malware that's used to gather and sell information without consent.

*Cryptojacking is a form of malware that installs software to illegally mine cryptocurrencies. Signs of this malware are slowdown, increased CPU usage, sudden system crashes, fast draining batteries and unusually high electricity cost.

*An intrusion detection system, or IDS, is an application that monitors system activity and alerts some possible intrusions.

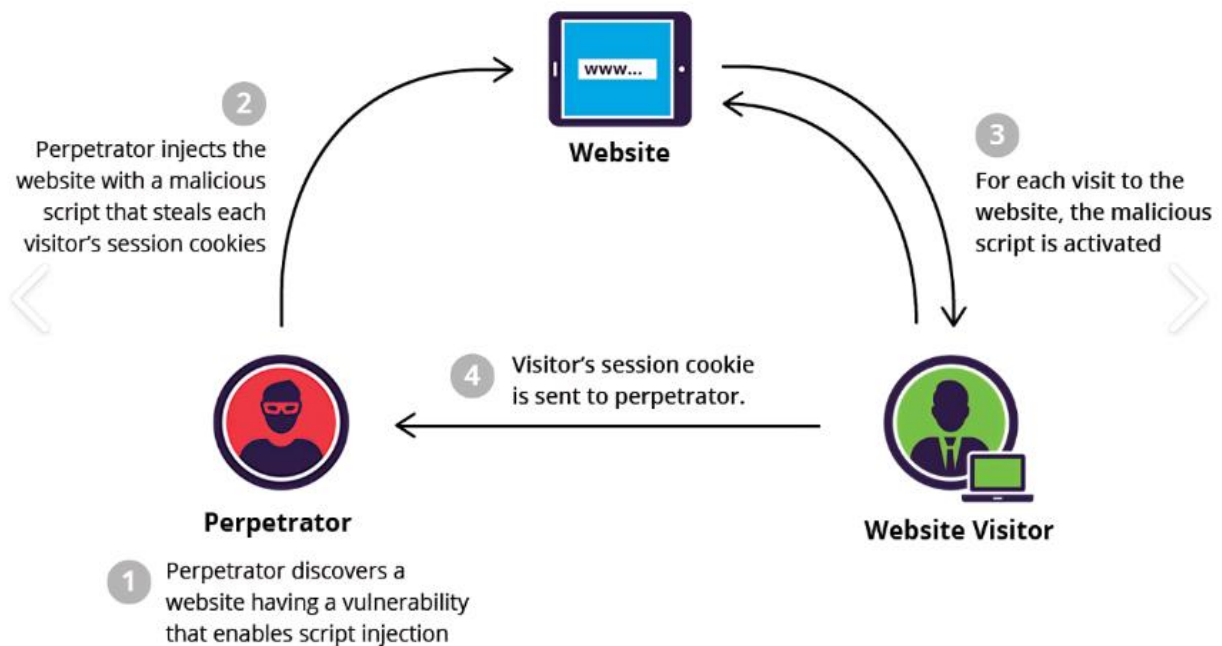
*Web-based exploits are malicious code or behavior that's used to take advantage of coding flaws in a web application.

*An injection attack is malicious code inserted into a vulnerable application. Cross site scripting, or XSS, is an injection attack that inserts code into a vulnerable website or web application. There are three main types of cross-site scripting attacks: reflected, stored, and DOM-based.

*A reflected XSS attack is an instance where a malicious script is sent to the server and activated during the server's response. A stored XSS attack is an instance when malicious script is injected

directly on the server. DOM stands for Document Object Model, which is basically the source code of a website. A DOM-based XSS attack is an instance when malicious script exists in the web page a browser loads.

*SQL is a programming language used to create, interact with, and request information from a database. A SQL injection is an attack that executes unexpected queries on a database. The best way to defend against SQL injection is code that will sanitize the input. A prepared statement is a coding technique that executes SQL statements before passing them on to the database.



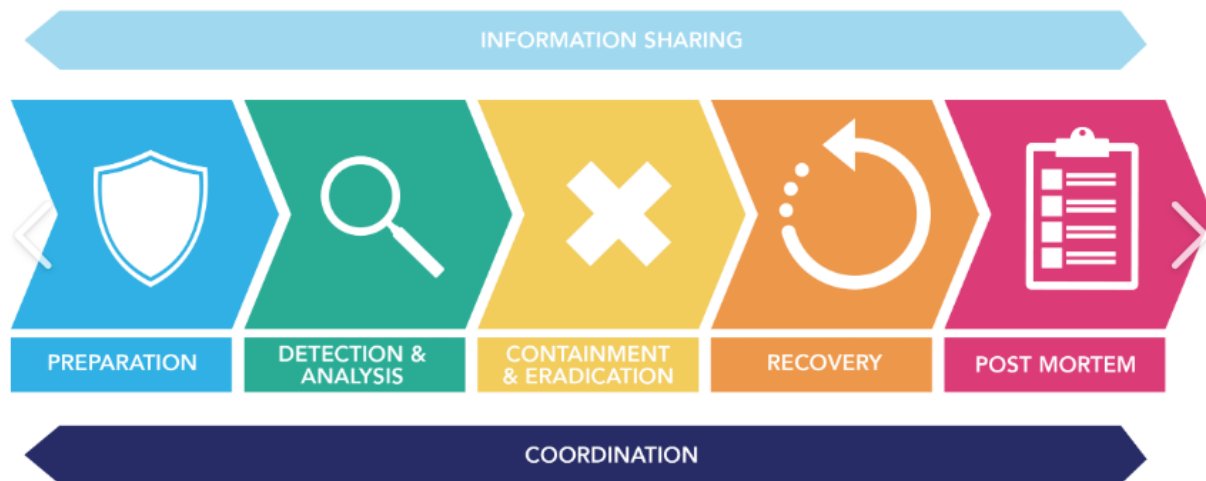
*Threat modeling is a process of identifying assets, their vulnerabilities, and how each is exposed to threats. Generally speaking, the process consists of six steps: define the scope of the model, identify threats, characterize the environment, analyze threats, mitigate risk, and evaluate findings.

*PASTA is a popular threat modeling framework that's used across many industries. PASTA is short for Process for Attack Simulation and Threat Analysis. Seven stages: Define business and security objectives, define the technical scope, decompose the application, analyze treats, analyze vulnerabilities, attack modeling, and analyze risk and impact.

Topic 6: Cybersecurity Detection & Response.

The Incident Response Lifecycle:

*In this course, we'll focus on the NIST CSF. To recall, the five core functions of the NIST CSF are: identify, protect, detect, respond, and recover. The NIST incident response lifecycle is another NIST framework with additional sub steps dedicated to incident response. It begins with preparation. Next, detection and analysis, and then containment, eradication and recovery, and finally post-incident activity.



*According to NIST, an incident is "an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

*It's important to understand that all security incidents are events, but not all events are security incidents. An event is an observable occurrence on a network, system, or device.

*The 5 Ws of an incident: who triggered the incident, what happened, when the incident took place, where the incident took place, and why the incident occurred.

*Computer security incident response teams, or CSIRTs, are a specialized group of security professionals that are trained in incident management and response. There are several roles in CSIRTs: security analyst, technical lead, and incident coordinator.

*Recall: Elements of a security plan are policies, standards, and procedures. The elements of an incident plan are: Incident response procedures, system information and other documents.

*An incident response plan is a document that outlines the procedures to take in each step of incident response.

*Different types of tools for incident response: Detection and management tools to monitor system activity to identify events that require investigation. Documentation tools to collect and compile evidence. Investigative tools for analyzing these events, like packet sniffers.

*Documentation is any form of recorded content that is used for a specific purpose. Types: These include playbooks, incident handler's journals, policies, plans, and final reports. A playbook is a manual that provides details about any operational action.

*Word processors are a common way to document. Some popular tools to use are Google Docs, OneNote, Evernote, and Notepad++. Ticketing systems like Jira can also be used to document and track incidents.

*An intrusion detection system is an application that monitors system and network activity, and produces alerts on possible intrusions. Some popular tools are Snort, Zeek, Kismet, Sagan, and Suricata.

*SIEM is a tool that collects and analyzes log data to monitor critical activities in an organization. First, SIEM tools collect and aggregate data. Next, SIEM tools normalize data. Finally, the normalized data gets analyzed according to configured rules.

*Security orchestration, automation, and response (SOAR) automates analysis and response to security events and incidents.

Network Traffic:

*Network data is the data that's transmitted between devices on a network. We can detect traffic abnormalities through observation to spot indicators of compromise, also known as IoC, which are observable evidence that suggests signs of a potential security incident.

*Data exfiltration, which is the unauthorized transmission of data from a system. There are several ways to protect from these types of attacks: prevent attacker access (MFA), monitor network activity (logins from IP addresses outside the network), protect the assets (properly catalog them) and detect and stop the exfiltration (network monitoring).

*Packets contain delivery information which is used to route it to its destination. A packet has multiple components. There's the header (with the IP address), which includes information like the type of network protocol and port being used. Next, there's the payload, which contains the actual data that's being delivered. And there's the footer, which signifies the end of the packet.

*A network protocol analyzer, or packet sniffer, is a tool designed to capture and analyze data traffic within a network. A packet capture, or P-cap, is a file containing data packets intercepted from an interface or network. Some network analyzer tools are Wireshark and tcpdump.

*Remember, the TCP/IP model is a framework that is used to visualize how data is organized and transmitted across a network. The internet layer accepts and delivers packets for the network. It's also the layer where the IP operates.

4-bit Version	4-bit Header Length	8-bit Type of Service (TOS)	16-bit Total Length (Bytes)	
16-bit Identification			3-bit Flags	13-bit Fragment Offset
8-bit Time to Live (TTL)		8-bit Protocol	16-bit Header Checksum	
32-bit Source IP Address				
32-bit Destination IP Address				
Options (if any)				
Payload				

Incident detection and verification:

*Analysis involves the investigation and validation of alerts. During the analysis process, analysts must apply their critical thinking and incident analysis skills to investigate and validate alerts.

*Challenges in the detection and analysis phase of the lifecycle: Impossible to detect everything, high volumes of alerts, etc.

*Benefits of documentation: transparency (relevant information can be accessed), standardization (This means that there's an established set of guidelines or standards that members of an organization can follow to complete a task or workflow) and clarity (provide detailed instructions prevent uncertainty and confusion during incident response).

*Chain of custody is the process of documenting evidence possession and control during an incident lifecycle. Broken chain of custody occurs when there are inconsistencies in the collection and logging of evidence in the chain of custody.

*Chain of custody establishes integrity, reliability, and accuracy of the evidence.

*A playbook is a manual that provides details about any operational action. There are three types: non-automated (requires step-by-step actions performed by an analyst), automated (Automated playbooks automate tasks in incident response processes) and semi-automated (combines a person's action with automation).

*Triage is the prioritizing of incidents according to their level of importance or urgency. The triage process consists in receiving and assessing, assigning priority, and collect and analyze.

*After an incident has been detected, it must be contained. Containment is the act of limiting and preventing additional damage caused by an incident.

*Once an incident has been contained, security teams work to remove all traces of the incident through eradication. Eradication involves the complete removal of the incident elements from all affected systems.

*Finally, the last step of this phase in the incident response lifecycle is recovery. Recovery is the process of returning affected systems back to normal operations.

*The post-incident activity phase entails the process of reviewing an incident to identify areas for improvement during incident handling. One of the critical forms of documentation that gets created is the final report. The final report is documentation that provides a comprehensive review of an incident.

*Some questions to ask during a lessons learned meeting: What happened? What time did it happen? Who discovered it? How did it get contained? What were the actions taken for recovery? What could have been done differently?



Logs, IDS, and SIEM tools:

*A log is a record of events that occur within an organization's systems. They include details on dates, times, locations, actions, and names

*Log analysis is the process of examining logs to identify events of interest. Main types of logs are: network, system, applications, security, and authentication.

*Commonly used log formats: syslog (includes a header, structured data, and a message), JavaScript Object Notation (JSON) (known for its simplicity and easy readability), extensible Markup Language, or XML (used for storing and transmitting data) and Comma Separated Values, or CSV (uses separators like commas to separate data values).

*Telemetry is the collection and transmission of data for analysis. Remember that IDS is an application that monitors activity and alerts on possible intrusions. An endpoint is any device connected on a network.

*A host-based intrusion detection system is an application that monitors the activity of the host on which it's installed. A network-based intrusion detection system collects and analyzes network traffic and network data. Signature analysis is a detection method used to find events of interest (specifies the rules that an IDS uses to monitor activity).

*Components of NIDS: Action (alert, pass, reject), header (include information such as source and destination IP addresses, source and destination ports, protocols, and traffic direction) and rule options (lets you customize signatures with additional parameters).

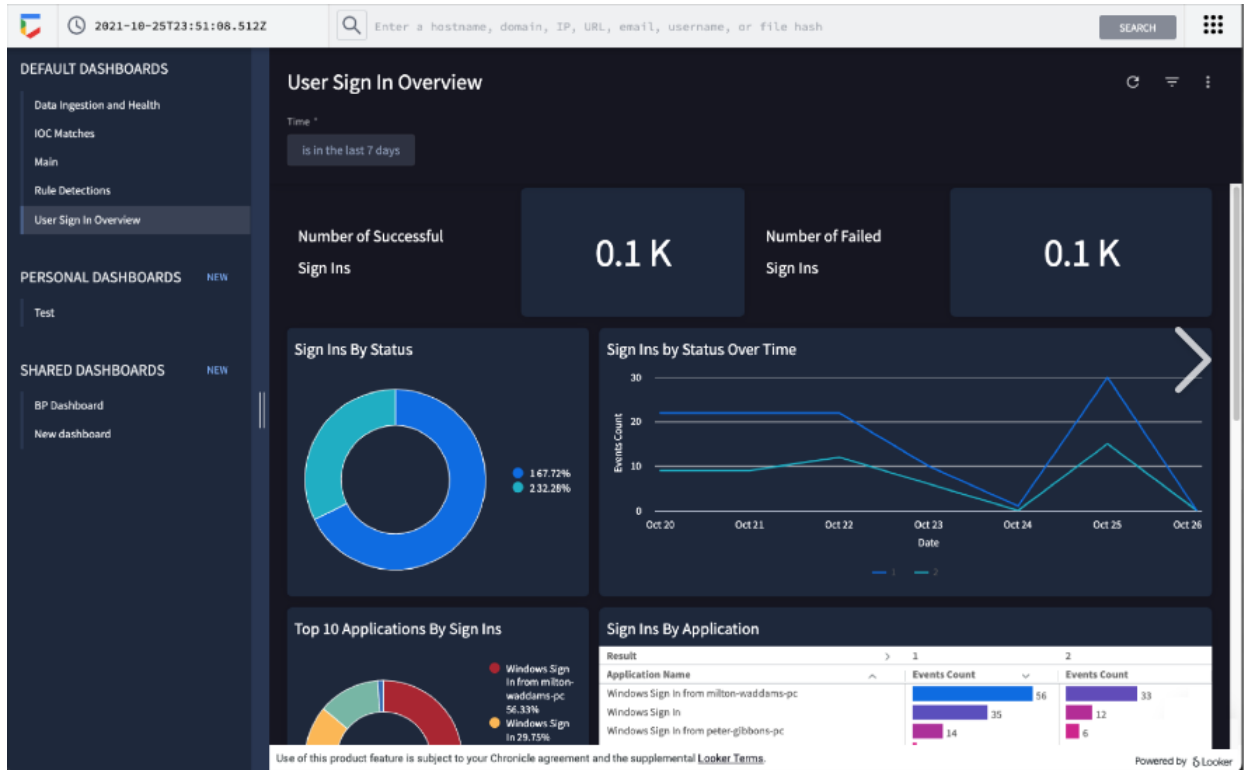
*Suricata is an open-source signature-based IDS used to examine signatures. In Suricata, alerts and events are output in a format known as EVE JSON. EVE stands for Extensible Event Format and JSON stands for JavaScript Object Notation. Suricata generates two log types: alert logs (contain information relevant to investigations) and network telemetry logs (contain information about network traffic flows).

```
{
  "configuration": {
    "name": "Default",
    "properties": {
      "property": [...]
    },
    "appenders": {
      "Console": {"name": "Console-Appender"...},
      "File": {"name": "File-Appender"...},
      "RollingFile": {"name": "RollingFile-Appender"...}
    },
    "loggers": {
      "logger": {"name": "guru.springframework.blog.log4j2json"...},
      "root": {"level": "debug"...}
    }
  }
}
```

*As a quick review, a SIEM is an application that collects and analyzes log data to monitor critical activities in an organization. First, SIEM tools **collect and process** enormous amounts of data generated by devices and systems from all over an environment. SIEM tools make it easy for security analysts to read and analyze data by **normalizing** it. Finally, SIEM tools **index** the data, so it can be accessed through search.

*Splunk is a data analysis platform. Splunk Enterprise Security provides SIEM solutions that let you search, analyze, and visualize security data. First, it collects data from different sources. That data gets processed and stored in an index. Then, it can be accessed in a variety of different ways, like through search. Splunk uses its own query language called Search Processing Language (SPL).

*Chronicle is Google Cloud's SIEM, which stores security data for search, analysis, and visualization. First, data gets forwarded to Chronicle. This data then gets normalized, or cleaned up, so it's easier to process and index. Finally, the data becomes available to be accessed through a search bar. Chronicle uses the YARA-L language to define rules for detection. The default method of search is using UDM search, which stands for Unified Data Model. It searches through normalized data. If you can't find the data you're looking for, you have the option of searching raw logs.



Topic 7: Fundamentals of Python for Cybersecurity

Introduction to Python:

*Programming is used to create a specific set of instructions for a computer to execute tasks.

*Python is considered to be a general-purpose language. This means that it can create a variety of different programs, and it isn't a specialized in any particular problem in fields such as web development and artificial intelligence. Python is typically used to build websites and perform data analysis. In security, the main reason we use Python is to automate our tasks.

*There are several advantages Python has as a programming language. Is user-friendly because it resembles human language. It requires less code, and it's easy to read. Python programmers also have the benefit of following standard guidelines to ensure consistency with the design and readability of code. Lastly, there's a large amount of online support.

*Python also has an extensive collection of built-in code that we can import and use to perform many different tasks.

*In Python, it's good practice to start with a comment. A comment is a note programmers make about the intention behind their code. Print outputs a specified object to the screen. Syntax refers to the rules that determine what is correctly structured in a computing language.

*A data type is a category for a particular type of data item. Main types are: string (sequence of characters), integer (numbers without decimal points), float (numbers with decimal points), Boolean (true or false) and list data (collection of data in sequential form).

*A variable is a container that stores data. To create a variable, you need a name for it. Then, you add an equals sign and then an object to store in it. Creating a variable is often called assignment. The type() function gives the type of a variable. Variables of different types can't be computed together. However, we can reassign the type of a variable for another.

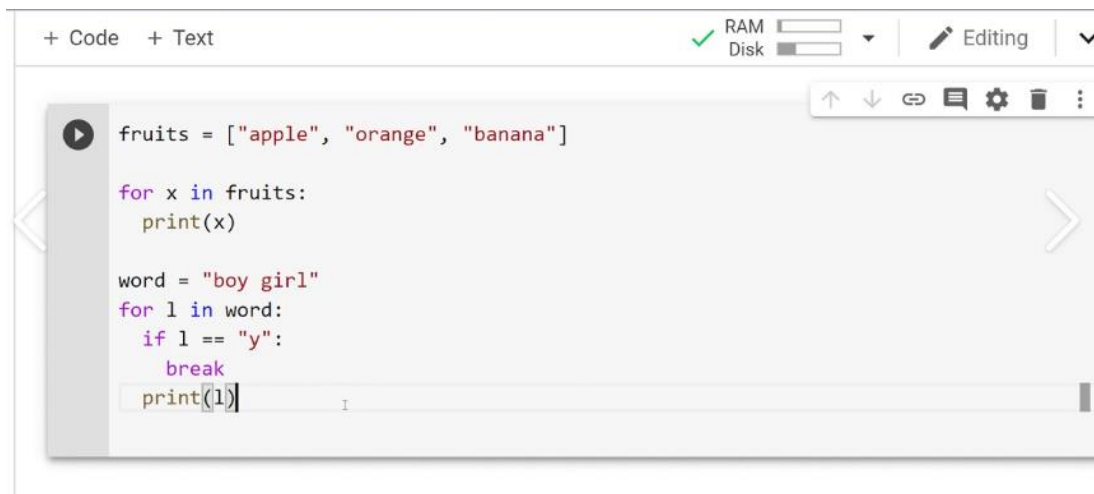
Name	Type	Description
Integers	int	Whole numbers, such as: 3 300 200
Floating point	float	Numbers with a decimal point: 2.3 4.6 100.0
Strings	str	Ordered sequence of characters: "hello" 'Sammy' "2000" "楽しい"
Lists	list	Ordered sequence of objects: [10,"hello",200.3]
Dictionaries	dict	Unordered Key:Value pairs: {"mykey": "value", "name": "Frankie"}
Tuples	tup	Ordered immutable sequence of objects: (10,"hello",200.3)
Sets	set	Unordered collection of unique objects: {"a","b"}
Booleans	bool	Logical value indicating True or False

*A conditional statement is a statement that evaluates code to determine if it meets a specified set of conditions. If (perform action if condition is meant) starts a conditional statement (use operators >, <, <=, >=, ==, !=). Else precedes a code section that only evaluates when all conditions that precede it within the conditional statement evaluate to False. Elif is equivalent to else if.

*An iterative statement is code that repeatedly executes a set of instructions. For loops repeat code for a specified sequence. While loops still repeatedly execute, but this repetition is based on a condition (better if you don't know the number of times to repeat in advance).

*When you want to exit a **for** or **while** loop based on a particular condition in an **if** statement being **True**, you can write a conditional statement in the body of the loop and write the keyword **break** in

the body of the conditional. When you want to skip an iteration based on a certain condition in an **if** statement being **True**, you can add the keyword **continue** in the body of a conditional statement within the loop.



```

+ Code + Text
RAM
Disk
Editing

fruits = ["apple", "orange", "banana"]

for x in fruits:
    print(x)

word = "boy girl"
for l in word:
    if l == "y":
        break
    print(l)

```

Functions:

*A function is a section of code that can be reused in a program. Built-in functions are functions that exist within Python and can be called directly. User-defined functions are functions that programmers design for their specific needs.

*Def is placed before a function name to define a function. After defining the function, a : is needed.

*In Python, a parameter is an object that is included in a function definition for use in that function. Parameters are accepted into a function through the parentheses after a function name. An argument is the data brought into a function when it is called.

*A return statement is a Python statement that executes inside a function and sends information back to the function call. Return is used to return information from a function.

*Recall that built-in functions are functions that exist within Python and can be called directly. First, print() outputs a specified object to the screen. Then, the type() function returns the data type of its input. The max() function returns the largest numeric input passed into it. The sorted() function sorts the components of a list.

*A library is a collection of modules that provide code users can access in their programs. A module is a Python file that contains additional functions, variables, classes, and any kind of runnable code.

*The Python Standard Library is an extensive collection of usable Python code that often comes packaged with Python. Some standard library modules are: re (for searching patterns) and csv (for working with CSV files). The Python Standard Library also contains glob and os modules for interacting with the command line as well as time and datetime for working with timestamps.

*External libraries can also be downloaded, such as BeautifulSoup (for parsing HTML website files) and NumPy for arrays and mathematical computations.

*A style guide is a manual that informs the writing, formatting, and design of documents. As it relates to programming, style guides are intended to help programmers follow similar conventions. PEP is short for Python Enhancement Proposals. PEP 8 provides programmers with suggestions related to syntax.

*A comment is a note programmers make about the intention behind their code. Indentation is a space added at the beginning of a line of code.

The screenshot shows a Python IDE window titled 'Python10.1.py'. The code is as follows:

```

1  #define a function
2  def func1():
3      print ("I am learning Python Function")
4
5  func1()
6  #print func1()
7  #print func1
8
9

```

Annotations on the code:

- Function definition:** Points to the `def func1():` line.
- Function Call:** Points to the `func1()` line.

The output console shows the following:

```

Run Python10.1
"C:\Users\DK\Desktop\Python code\Python Test\Python 10\Python10
10\Python10 Code\Python10.1.py"
I am learning Python Function

```

Annotation: **Function output** points to the output text.

Strings, algorithms, and regular expressions:

*String data is data consisting of an ordered sequence of characters. The string function `str()` is a function that converts the input object into a string. The length function `len()` is a function that returns the number of elements in an object. The string concatenation is the process of joining two strings together. Strings can be concatenated with the `+` operator.

*A method is a function that belongs to a specific data type. `Upper()` returns a copy of the string in all uppercase letters. `Lower()` does the same in all lowercase letters.

*The index is a number assigned to every element in a sequence that indicates its position. When taking a slice from a string, we specify where the slice starts and where the slice ends. So we provide two indices. The index method `.index()` finds the first occurrence of the input in a string and returns its location.

*Strings are immutable. In Python, "immutable" means that it cannot be changed after it's created and assigned a value. Let's break this down with an example.

String Indexing

"Ayushi bought a pen!"

-20	-19	-18	-17	-16	-15	-14	-13	-12	-11	-10	-9	-8	-7	-6	-5	-4	-3	-2	-1
A	y	u	s	h	i		b	o	u	g	h	t		a		p	e	n	!
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19

*Lists are useful because they allow you to store multiple pieces of data in a single variable. List concatenation is combining two lists into one by placing the elements of the second list directly after the elements of the first list. Unlike strings, lists are not immutable. `Inset(position, information)` adds an element in a specific position inside a list. `Remove(information)` removes the first occurrence of a specific element in a list. `Append(information)` adds input at the end of a list.

*An algorithm is a set of rules that solve a problem. Ex: extracting the first three digits from a list of IP addresses: 1. Use slicing to extract the first 3 digits from one IP address. 2. Use a loop to apply that solution to every IP address on the list.

```
my_list = [1, 2, 3, 4, 5, 6, 7, 8, 9, 2, 5, 2]
print(f'The list is - {my_list}')
print(f'The value 2 appears {my_list.count(2)} times in the list.')
```

Python_List_Operations x

```
C:\Users\User\PycharmProjects\First_Class\venv\Scripts\python.exe
C:/Users/User/PycharmProjects/First_Class/Python_List_Operations.py
The list is - [1, 2, 3, 4, 5, 6, 7, 8, 9, 2, 5, 2]
The value 2 appears 3 times in the list.
```

Process finished with `exit` code 0

*A regular expression, shortened to regex, is a sequence of characters that forms a pattern. The plus sign is a regular expression symbol that represents one or more occurrences of a specific character. The other building block we need is the `\w` symbol. This matches with any alphanumeric character, but it doesn't match symbols. Backslash is used before symbols that have meaning.

*`Re.findall()` returns a list of matches to a regular expression.

Python for automatization:

*Python can be used to check: whether several failed login attempts occurred within a short period of time, not established work zones or outside of regular working hours.

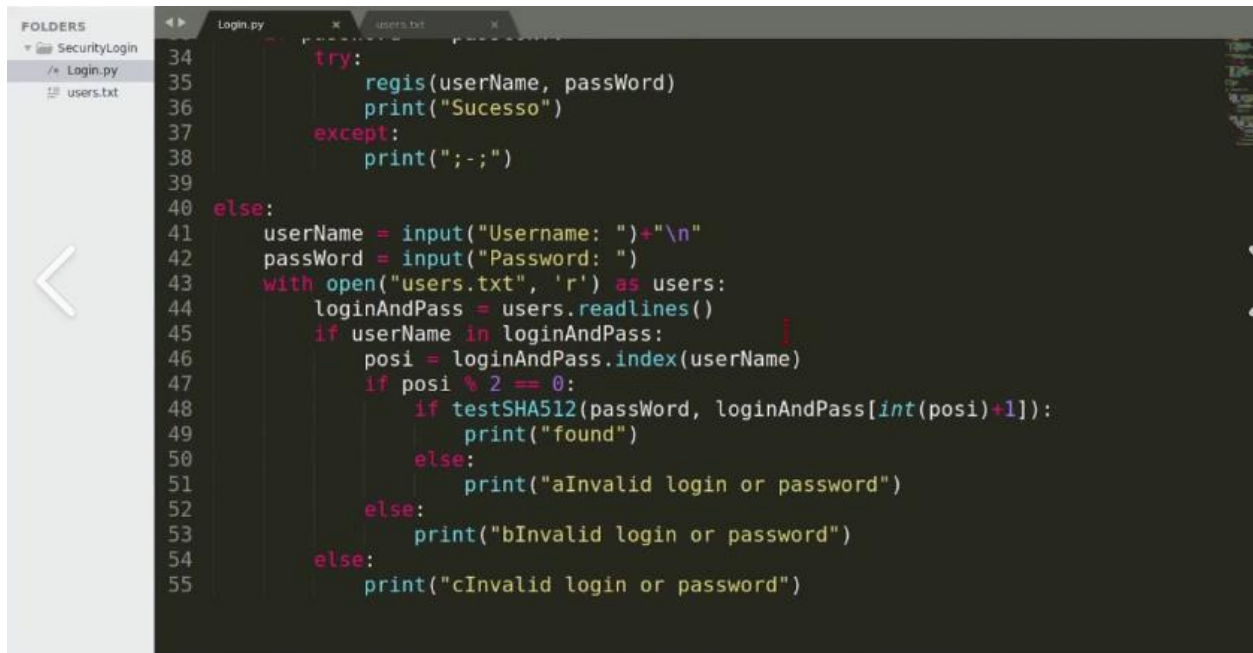
*For loops contribute to automatization by allowing to perform the same action a certain number of times.

*Cybersecurity-related information is often found in log files. Common formats for security logs are txt and csv documents.

*The `with` statement handles errors and manages external resources. Often used with `open(file or file path, what to do)`, which opens a file in Python. Ex: `with open("ip_addresses.txt", "r") as file:`
`file_text = file.read()` `print(file_text)` copies and prints the read file.

*Parsing is the process of converting data into a more readable format. The `split` method converts a string into a list. It does this by separating the string based on a specified character. The `join` method is the opposite to the `split` one.

*Debugging is the practice of identifying and fixing errors in code. Three types: syntax (invalid use of Python language), logic (may not create error messages, but display unintended results) and exception (different reasons, like a mathematically impossible operation, calling a function before defining it, etc) errors.



```
34     try:
35         regis(userName, passWord)
36         print("Sucesso")
37     except:
38         print(";-;")
39
40 else:
41     userName = input("Username: ")+"\n"
42     passWord = input("Password: ")
43     with open("users.txt", 'r') as users:
44         loginAndPass = users.readlines()
45         if userName in loginAndPass:
46             posi = loginAndPass.index(userName)
47             if posi % 2 == 0:
48                 if testSHA512(passWord, loginAndPass[int(posi)+1]):
49                     print("found")
50                 else:
51                     print("aInvalid login or password")
52             else:
53                 print("bInvalid login or password")
54         else:
55             print("cInvalid login or password")
```


Topic 8: How to Prepare for your Cybersecurity Career.

Event Incident Detection:

*A security mindset is the ability to evaluate risk and constantly seek out and identify the potential or actual breach of a system, application, or data.

*It's important to recognize that the assets and data you protect affect multiple levels of your organization.

*When a security event results in a data breach, it is categorized as a security incident. However, if the event is resolved without resulting in a breach, it's not considered an incident.

Incident Escalation:

*Incident escalation is the process of identifying a potential security incident, triaging it, and (if appropriate) handing it off to a more experienced team member.

*There are two essential skills that will help you identify security incidents that need to be escalated: attention to detail and an ability to follow an organization's escalation guidelines or processes.

*From the Chief Information Security Officer, also known as the CISO, to the engineering team, public relations team, and even the legal team, every member of the security team matters.

*A malware infection is the incident type that occurs when malicious software designed to disrupt a system infiltrates an organization's computers or network.

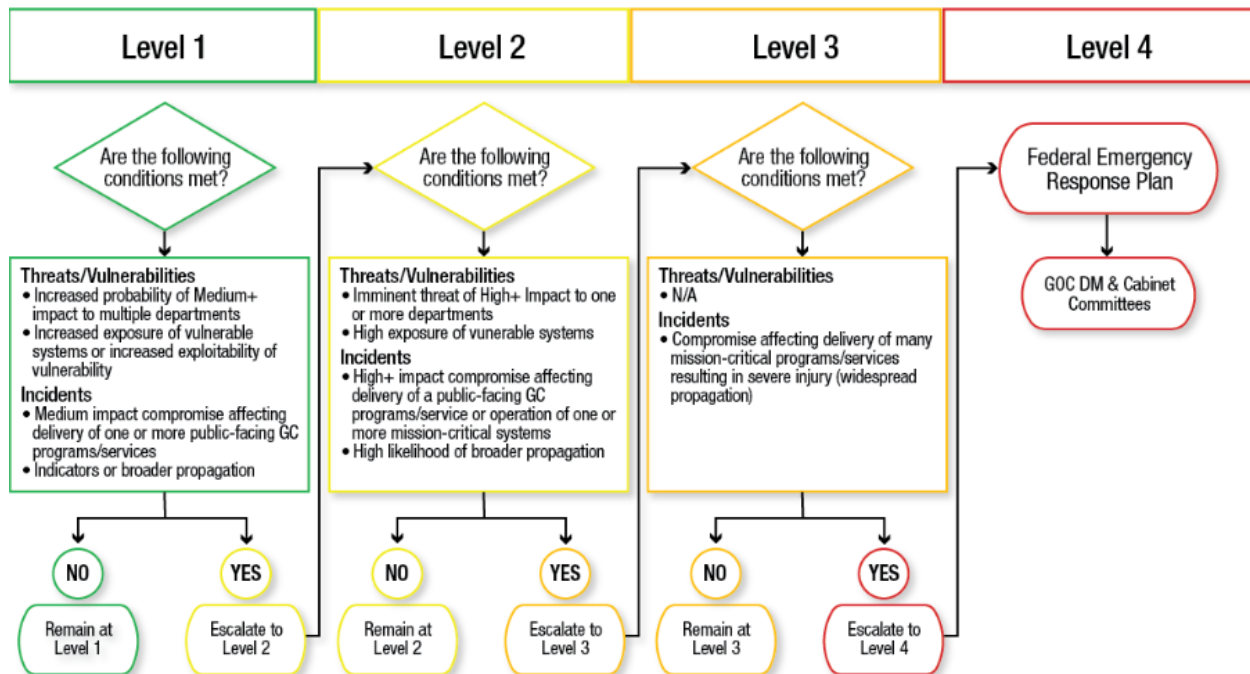
*Unauthorized access is an incident type that occurs when an individual gains digital or physical access to a system or application without permission. Brute force attacks, which use trial and error to compromise passwords, login credentials, and encryption keys.

*Improper usage is an incident type that occurs when an employee of an organization violates the organization's acceptable use policies.

*Small issues can become data breaches if not escalated properly. The impact of an attacker gaining unauthorized access to a manufacturing application or PII is far greater than a forgotten password.

*Each organization has its own process for handling security incidents. That process is known as an escalation policy, which is a set of actions that outline who should be notified when an incident alert occurs and how that incident should be handled.

*Attention to detail can make the difference between escalating an incident to the right or wrong person. It can also help you prioritize which incidents need to be escalated with more or less urgency.



Stakeholders, roles, and communication strategies:

*A stakeholder is defined as an individual or group that has an interest in the decisions or activities of an organization. We're going to focus on five of those stakeholders: risk managers; the Chief Executive Officer, also known as the CEO; the Chief Financial Officer, also known as the CFO; the Chief Information Security Officer, or CISO; and operation managers.

*Risk managers are important in an organization because they help identify risks and manage the response to security incidents. They also notify the legal department regarding regulatory issues that need to be addressed. Additionally, risk managers inform the organization's public relations team in case there is a need to publish public communications regarding an incident.

*Next, is the Chief Executive Officer, also known as the CEO. This is the highest ranking person in an organization. CEOs are responsible for financial and managerial decisions.

*Now, let's discuss the Chief Financial Officer, known as the CFO. CFOs are senior executives responsible for managing the financial operations of a company. They are concerned about security from a financial standpoint because of the potential costs of an incident to the business. They are also interested in the costs associated with tools and strategies that are necessary to combat security incidents.

*Another stakeholder with an interest in security is the Chief Information Security Officer, or CISO. CISOs are high-level executives responsible for developing an organization's security architecture and conducting risk analysis and system audits. They're also tasked with creating security and business continuity plans.

*Last, we have operations managers. Operations managers oversee security professionals to help identify and safeguard an organization from security threats. These individuals often work directly with analysts as the first line of defense when it comes to protecting the company from threats, risks, and vulnerabilities. They are also generally responsible for the daily maintenance of security operations.

*The security story details what the security challenge is, how it impacts the organization, and possible solutions to the issue. You can communicate the story we just discussed in various ways. Send an email, share a document, create a ticket, or even communicate through the use of a visual representation.

*Some scenarios are better expressed by using visual elements. Visuals are used to convey key details in the form of graphs, charts, videos, or other visual effects. Google Sheets and Apache OpenOffice are some programs that can be used to create visual dashboards.



Cybersecurity Resources:

*The OWASP top 10 is a globally recognized standard awareness document that lists the top 10 most critical security risks to web applications.

*Some interesting security websites and blogs are: CSO Online (provides news, analysis, and research on various security and risk management topics), Krebs on Security (in-depth security blog created by former Washington Post reporter, Brian Krebs), and Dark Reading (provides information about various security topics like analytics and application security, mobile and cloud security, as well as the Internet of Things, IOT).

*Social media is another great way to connect to other security professionals in the industry. A good example is connecting with professionals from the cybersecurity field in LinkedIn.

Find and prepare for cybersecurity jobs:

*A security analyst focuses on monitoring networks for security breaches, developing strategies to help secure an organization, and even researching IT security trends.

*Information security analyst: This role generally focuses on creating plans and implementing security measures to protect organizations' networks and systems.

*Security operations center analyst, also known as a SOC analyst, is another role you might find exciting focuses on ensuring security incidents are handled rapidly and efficiently by following established policies and procedures.

*A few well-known job sites in the United States and internationally are ZipRecruiter, Indeed, and Monster Jobs.

*Resume/CV: You can mention all that you've learned in this program on your resume, including programming languages, such as Python and SQL, and Linux line-command. You can also share your understanding of what it means to have a security mindset, your knowledge of standard frameworks and controls, like the NIST CSF and CIA Triad model, as well as your familiarity with how to use SIEM tools and packet sniffers.

*Transferable skills: could include being detail oriented, collaborative, and having strong written and verbal communication skills.

*Prepare for an interview: Review the job description and your resume, practice speaking about experiences and skills and dress professionally. Two parts of interview:

*Background interview: education, work experience, skills, abilities, etc.

*Technical interview: Python, SIEM tools, TCP/IP, etc. Answer confidently and concisely, be sincere.

*Pre-interview research: Mission, vision, core values, company culture, etc.

*Why you? Skills, experience, work ethic, goals, etc.

*Build rapport with interviewers: Rapport is a friendly relationship in which the people involved understand each other's ideas and communicate well with each other. Have questions prepared to the interviewer. After the interview, send a follow up email.

*Strategies to answer interview questions: The STAR (Situation, Task, Action, Result) method is a technique used to answer behavioral and situational interview questions. Just answering questions with confidence is also fine for other types of questions.

*An elevator pitch is a brief summary of your experience, skills, and background. Avoid rambling, sounding ingenuine, or speaking too quickly.

