Coursera - Google Cybersecurity Professional Certificate

March 2025

COURSE 1 - Foundations in Cybersecurity **1**
MODULE 1 - Welcome to the Exciting World of Cybersecurity 1
MODULE 2 - The Evolution of Cybersecurity 1
MODULE 3 - Protect Against Threats, Risks, and Vulnerabilities 3
MODULE 4 - Cybersecurity Tools and Programming Languages 4
COURSE 2 - Play it Safe Manage Security and Risks **6**
MODULE 1 - Security Domains 6
MODULE 2 - Security Frameworks and Controls 7
MODULE 3 - Introduction to Cybersecurity Tools 9
MODULE 4 - Use Playbooks to Respond to Incidents 10
COURSE 3 - Connect and Protect: Networks and Network Security **11**
MODULE 1 - Network Architecture 11
MODULE 2 - Network Operations 14
MODULE 3 - Secure Against Network Intrusions 16
MODULE 4 - Security Hardening 17
COURSE 4 - Tools of the Trade: Linux and SQL **21**
MODULE 1 - Introduction to Operating Systems 21
MODULE 2 - The Linux Operating System 23
MODULE 3 - Linux Commands in the Bash Shell 24
MODULE 4 - Databases and SQL 24
COURSE 5 - Assets Threats and Vulnerabilities **25**
MODULE 1 - Introduction to Asset Security 25
MODULE 2 - Protect Organizational Assets 25
MODULE 3 - Vulnerabilities in Systems 25
MODULE 4 - Threats to Asset Security 25
COURSE 6 - Sound the Alarm: Detection and Response **26**
MODULE 1 - Introduction to Detection and Incident Response 26
MODULE 2 - Network Monitoring and Analysis 26
MODULE 3 - Incident Investigation and Response 26
MODULE 4 - Network Traffic and Logs Using IDS and SIEM Tools 26
COURSE 7 - Automate Cybersecurity Tasks with Python **27**
MODULE 1 - Introduction to Python 27
MODULE 2 - Write Effective Python Code 27
MODULE 3 - Work with Strings and Lists 27
MODULE 4 - Python in Practice 27
COURSE 8 - Put it to Work: Prepare for Cybersecurity Jobs **28**
MODULE 1 - Protect Data and Communicate Incidents 28
MODULE 2 - Escalate Incidents 28
MODULE 3 - Communicate Effectively to Influence Stakeholders 28
MODULE 4 - Engage with the Cybersecurity Community 28

COURSE 1 - Foundations in Cybersecurity

MODULE 1 - Welcome to the Exciting World of Cybersecurity

- **Cybersecurity -** The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation.
- **Responsibilities of a Security Analyst -** Protecting computer and network systems, installing prevention software, and conducting periodic security audits.
- **Personally identifiable information (PII) -** Information used to infer an individual's identity, such as their name, phone number or email address.
- **Sensitive personally identifiable information (SPII) -** A specific type of PII that falls under stricter handling guidelines such SSNs, medical records and bank account details.
- **Threat -** A threat refers to a potential danger or risk to an organization's systems, data, or operations. It can be an event, action, or condition that could exploit vulnerabilities to cause harm. For example, malware, phishing attacks, or natural disasters are all considered threats.
- **Threat Actor -** A threat actor is the entity or individual responsible for carrying out the threat. These actors can be humans, groups, or automated systems actively attempting to exploit vulnerabilities. Threat actors are categorized based on their intent, capability, and resources, such as hackers, insider threats, nation-states, or hacktivist groups.
- **Vulnerability -** A weakness that can be exploited by a threat. Examples include outdated software, poor access controls, weak passwords or misconfigurations.
- **Risk -** A risk is the likelihood of a threat exploiting a vulnerability and the potential impact of that event. It considers both the probability and consequences of harm occurring. Anything that can impact the confidentiality, integrity or availability of an asset is a risk. Both a vulnerability and threat must be present for there to be a risk.

MODULE 2 - The Evolution of Cybersecurity

- **Computer Virus -** A malicious code written to interfere with computer operations and cause damage to data and software. The virus attaches itself to programs or documents on a computer, then spreads and infects one or more computers in a network. Today, viruses are more commonly referred to as malware, which is software designed to harm devices or networks. The following are some of the most infamous viruses in history:
    - **Brain Virus -** The Brain Virus spread globally within months via pirated software. It infected computers, transferring itself to any disk inserted, and subsequently to new systems using those disks. Though not designed to destroy data or hardware, it severely disrupted productivity and business operations.
    - **Morris Worm -** Was invented to tally the number of computers connected to the internet but lacked a mechanism to avoid re-infecting systems. This led to

repeated installations, causing affected computers to crash due to memory overload. About 6,000 systems, or 10% of the internet at the time, were impacted, resulting in millions of dollars in damages and business disruptions. The incident prompted the creation of Computer Emergency Response Teams (CERTs®).
    - **Love Letter Malware -** The 2000 LoveLetter malware, created by Onel De Guzman, spread via an email titled "I Love You" with an attachment labeled "Love Letter For You." Opening the attachment triggered the malware, which collected passwords and spread to contacts in the user's address book. Exploiting trust, it infected 45 million computers and caused over $10 billion in damages, marking a pivotal early example of social engineering.
    - **Equifax Breach 2017 -** This breach exposed sensitive data of over 143 million individuals, affecting about 40% of Americans. Stolen information included Social Security numbers, birth dates, driver's license details, addresses, and credit card numbers. The breach resulted from Equifax's failure to address multiple known security vulnerabilities. The company later settled for over $575 million to resolve complaints and fines.
- **Phishing -** The use of digital communications to trick people into revealing sensitive data or deploying malicious software.
- **Most Common Phishing Attacks**
    - **Business Email Compromise -**
    - **Spear phishing -**
    - **Whaling -**
    - **Vishing -**
    - **Smishing -**
- **Malware -** Software designed to harm devices or networks. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.
- **Most Common Types of Malware**
    - **Viruses -** Malicious code written to interfere with computer systems.
    - **Worms -** Malware that can duplicate and spread itself across a system on its own.
    - **Ransomware** - When threat actors encrypt data and demand payment to restore.
    - **Spyware -** Malware that's used to gather and sell information without consent.
- **Social Engineering -** A manipulation technique that exploits human error to gain private information, access, or valuables. Can be avoided by regular internal training.
- **Most Common Types of Social Engineering Attacks**
    - **Social Media Phishing -** When a threat actor collects detailed info about their target from social media sites and then initiates an attack.
    - **Watering Hole Attack -** When a threat actor attacks a website that is frequently visited by a specific group of users.

    - **USB Baiting -** Is when a threat actor leaves a USB stick laying around that's full of malware and waits for someone to plug it into their computer.
    - **Physical Social Engineering Attack -** When a threat actor impersonates an employee, customer or vendor to obtain unauthorized access to a physical location.
- **Common Social Engineering Tactics -** Threat actors will use authority, intimidation, consensus/social proof, scarcity, familiarity, trust, and urgency to convince their victims into trusting them and giving them access to unauthorized spaces or information.
- **Eight CISSP Security Domains**
    - 1 - Security and risk management.
    - 2 - Asset security.
    - 3 - Security architecture and engineering.
    - 4 - Communication and network security.
    - 5 - Identity and access management.
    - 6 - Security assessment and testing.
    - 7 - Security operations.
    - 8 - Software development security.
- **Attack Types -** Password attack, social engineering attack, physical attack, supply chain attack, cryptographic attack.
- **Threat Actor Types**
    - **Advanced Persistent Threats -** A threat actor maintains unauthorized access to a system for an extended period of time.
    - **Insider Threats -** Staff members or vendors abuse their authorized access to obtain data that may harm an organization.
    - **Hacktivists -** Individuals or groups who use hacking techniques to promote political or social causes, usually targeting governments or corporations.

MODULE 3 - Protect Against Threats, Risks, and Vulnerabilities

- **Security Frameworks -** Structured guidelines for managing risks, protecting data, and ensuring privacy. They support an evolving security lifecycle, helping organizations manage risks, follow best practices, and meet regulatory requirements. Four core concepts of security frameworks are identifying/documenting security goals, setting guidelines to achieve security goals, implementing strong security processes and monitoring and communicating results.
    - **CIA Triad -** Confidentiality means only authorized users can access data. Integrity means the data is correct, authentic and reliable. Availability means data is accessible to those who are authorized to access it.
    - **NIST -** U.S.-based National Institute of Standards and Technology: the Cybersecurity Framework, also referred to as the NIST CSF. The NIST

Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk.
    - **FERC-NERC -** Regulations for U.S. power grid organizations, requiring preparation, mitigation, and reporting of security incidents under Critical Infrastructure Protection (CIP) standards.
    - **FedRAMP -** Standardizes security assessment and monitoring for cloud services in the U.S. federal sector.
    - **Center for Internet Security CIS -** A nonprofit providing security controls to protect systems and respond to incidents.
    - **General Data Protection Regulation GDPR -** E.U. regulation ensuring data privacy and transparency for E.U. residents, with strict breach notification rules.
    - **Payment Card Industry Data Security Standard PCI DSS -** International standard ensuring secure handling of credit card data to reduce fraud.
    - **Health Insurance Portability and Accountability Act HIPAA -** U.S. law protecting patient health information, requiring privacy, security, and breach notifications to prevent identity theft and fraud. Security pros often use HITRUST to ensure compliance.
    - **International Organization for Standardization ISO -** International standards for improving organizational processes, including technology, manufacturing, and management across borders.
    - **System and Organization Controls SOC 1 & 2 -** A series of reports that focus on an organization's user access policies at different organizational levels such as associate, supervisor, manager, executive, vendor and others.
    - **International Standpoint on Counterattacks -** States that you can only counter attack if: The counterattack will only affect the party that attacked first. The counterattack is a direct communication asking the initial attacker to stop. The counterattack does not escalate the situation. The counterattack effects can be reversed.

MODULE 4 - Cybersecurity Tools and Programming Languages

- **Logs -** A record of events that occur within an organization's systems. Examples of security-related logs include records of employees signing into their computers or accessing web-based services. Logs help security professionals identify vulnerabilities and potential security breaches.
- **Common Cybersecurity Tools**
    - **Playbooks -** Vary from one organization to the next, guide analysts in how to handle a security incident before, during, and after it has occurred.
    - **Packet Sniffer -** A tool designed to capture and analyze data traffic within a network. Common network protocol analyzers include tcpdump and Wireshark.

    - **Antivirus Software -** Detects and removes malware such as viruses, worms, and trojans.
    - **Firewall** - Monitors and controls incoming and outgoing network traffic based on predetermined security rules.
    - **Encryption Tools -** Protect data by converting it into a secure format, accessible only with a decryption key.
    - **Intrusion Detection/Prevention Systems (IDS/IPS) -** Monitors network traffic for suspicious activity and can block potential threats.
    - **Vulnerability Scanners -** Scans systems for security weaknesses that could be exploited by attackers. Ex Qualys, Tenable, Rapid7.
    - **Identity and Access Management (IAM) -** Manages user identities and controls access to resources based on roles and permissions.
    - **Endpoint Protection -** Secures end-user devices like laptops and mobile phones from malware and other security threats.
    - **Data Loss Prevention (DLP) -** Monitors and prevents the unauthorized sharing or loss of sensitive data.
    - **Backup and Disaster Recovery -** Tools for creating data backups and recovering from data loss or breaches.
- **Programming Languages used in Cybersecurity -** Organizations can use programming to create a specific set of instructions for a computer to execute tasks. Programming allows analysts to complete repetitive tasks and processes with a high degree of accuracy and efficiency. It also helps reduce the risk of human error, and can save hours or days compared to performing the work manually.
    - **Python -** Security professionals can use Python to automate tasks that are repetitive and time-consuming and that require a high level of detail and accuracy.
    - **SQL -** A programming language used to create, interact with, and request information from a database. A database is an organized collection of information or data. A security analyst would use SQL to filter through the data points to retrieve specific information.
- Order of volatility?

COURSE 2 - Play it Safe Manage Security and Risks

MODULE 1 - Security Domains

- **1 Security and Risk Management -** Defining security goals and objectives, risk mitigation, compliance, business continuity, and legal regulations.
- **2 Asset security -** The asset security domain is focused on securing digital and physical assets. It's also related to the storage, maintenance, retention, and destruction of data.
- **3 Security Architecture and Engineering -** Focuses on optimizing data security through effective tools, systems, and processes. A key concept, shared responsibility, involves everyone in the organization actively reducing risks and maintaining security by recognizing and reporting concerns.
- **4 Communication and Network Security -** Focused on managing and securing physical networks and wireless communications. Secure networks keep an organization's data and communications safe on-site, or in the cloud, or when connecting to services remotely.
- **5 Identity and Access Management -** Focused on access and authorization to keep data secure by making sure users follow established policies to control and manage assets. Ensuring user access is limited to what employees need. Basically, the goal of IAM is to reduce the overall risk to systems and data.
- **6 Security Assessment and Testing -** Focuses on conducting security control testing, collecting and analyzing data, and conducting security audits to monitor for risks, threats, and vulnerabilities. Security control testing can help an organization identify new and better ways to mitigate threats, risks, and vulnerabilities.
- **7 Security Operations -** Focused on conducting investigations and implementing preventative measures. Investigations begin once a security incident has been identified. This process requires a heightened sense of urgency in order to minimize potential risks to the organization.
- **8 Software Development Security -** Focuses on using secure coding practices. Ensuring that each phase of the software development lifecycle undergoes security reviews so that security can be fully integrated into the software product.
- **NIST Risk Management Framework Steps (RMF)**
    - **Prepare -** Establish a context for risk management, identify critical systems, resources, and stakeholders and define the organization’s risk management roles and responsibilities.
    - **Categorize -** Categorize the system based on the type of data it processes and its impact level (Low, Moderate, High).
    - **Select** - Identify and tailor security controls based on the system’s categorization.
    - **Implement -** Integrate the selected controls into the system during design, development, and deployment. Document control implementation detail
    - **Assess -** Evaluate the effectiveness of the implemented controls. Identify weaknesses and determine residual risk using guidance from NIST SP 800-53A.

    - **Authorize -**
    - **Monitor -** Continuously monitor the effectiveness of security controls. Identify and address changes in the system or environment that affect security posture. Report security status to stakeholders regularly.
- **Common Strategies Used to Manage Risks**
    - **Acceptance -** Accepting a risk to avoid disrupting business continuity.
    - **Avoidance -** Creating a plan to avoid the risk altogether.
    - **Transference -** Transferring risk to a third party to manage.
    - **Mitigation -** Lessening the impact of a known risk.

MODULE 2 - Security Frameworks and Controls

- **Security Frameworks -** Guidelines used for building plans to help mitigate risk and threats to data and privacy. Frameworks support organizations' ability to adhere to compliance laws and regulations.
- **Security Controls -** Safeguards designed to reduce specific security risks. Security controls are used alongside frameworks to lower risk and threats to data and privacy.
    - **Physical Controls -** Gates fences, locks, security guards, access badges, cctv.
    - **Technical Controls -** Firewalls, MFA, antivirus software.
    - **Administrative Controls -** Separation of duties, authorization, asset classification.
- **Encryption -** The process of converting readable data (plaintext) into an encoded format (ciphertext) to protect its confidentiality. Ciphertext is unreadable until it is decrypted back into plaintext. This ensures the confidentiality of sensitive information.
- **Authentication -** The process of verifying who someone or something is. A real-world example of authentication is logging into a website with your username and password. More advanced authentication is MFA or multi factor authentication.
- **Authorization -** The concept of granting access to specific resources within a system. Authorization is used to verify that a person has permission to access a resource.
- **CIA Triad -** A model that helps inform how organizations consider risk when setting up systems and security policies.
    - **Confidentiality -** Only authorized users can access specific assets or data. This can be achieved through encryption to protect data.
    - **Integrity -** Data is correct, authentic, and reliable. This can be achieved through hashing data to validate its integrity.
    - **Availability -** Data is accessible to those who are authorized to access it. This can be achieved through redundant systems, load balancing and ddos protection.
- **NIST Cybersecurity Framework (CFS) -** Provides specific guidance and direction for security professionals. This framework is used to develop plans to handle an incident appropriately and quickly to lower risk, protect an organization against a threat, and mitigate any potential vulnerabilities.

    - **Identify -** Related to the management of cybersecurity risk and its effect on an organization's people and assets. Such as monitoring systems and devices in your organization's internal network to identify potential security issues.
    - **Protect -** The strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats.
    - **Detect -** Identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections.
    - **Respond -** Make sure proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.
    - **Recover -** The process of returning affected systems back to normal operation.
- **Open Web Applications Security Project (OWASP) Principles**
    - **Minimize the Attack Surface Area -** Attack surface refers to all the potential vulnerabilities a threat actor could exploit.
    - **Principle of Least Privilege -** Users have the least amount of access required to perform their everyday tasks.
    - **Defense in Depth -** Organizations should have varying security controls that mitigate risks and threats.
    - **Separation of Duties -** Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
    - **Keep Security Simple -** Avoid unnecessarily complicated solutions. Complexity makes security difficult.
    - **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.
    - **Establish Secure Defaults -** This principle means that the optimal security state of an application is also its default state for users; it should take extra work to make the application insecure.
    - **Fail Securely -** When a control fails or stops, it should do so by defaulting to its most secure option. For example, when a firewall fails it should simply close all connections and block all new ones, rather than start accepting everything.
    - **Don’t Trust Services -** Many organizations work with third-party partners. These outside partners often have different security policies than the organization does. And the organization shouldn’t explicitly trust that their partners’ systems are secure. For example, if a third-party vendor tracks reward points for airline customers, the airline should ensure that the balance is accurate before sharing that information with their customers.
    - **Avoid Security by Obscurity -** The security of an application should not rely on keeping the source code secret. Its security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

- **Security Audit -** A review of an organization's security controls, policies, and procedures against a set of expectations. Internal security audits help security teams identify organizational risk, assess controls, and correct compliance issues.
    - **Establish the scope and goals of the audit -** Scope requires organizations to identify people, assets, policies, procedures, and technologies that might impact an organization's security posture.
    - **Conduct a risk assessment of the organization's assets -** Identify potential threats, risks, and vulnerabilities. Helps organizations consider what security measures should be implemented and monitored to ensure safety of assets.
    - **Complete a controls assessment -** Review an organization's existing assets, then evaluating potential risks to those assets, to ensure internal controls and processes are effective.
    - **Assess compliance -** Determining whether or not the organization is adhering to necessary compliance regulations. Compliance regulations are laws that organizations must follow to ensure private data remains secure.
    - **Communicate results to stakeholders -** Results and recommendations need to be communicated to stakeholders. In general, this type of communication summarizes the scope and goals of the audit.
- **Control Types -** As we learned previously there are three main control categories, administrative, technical and physical. Control types focus on the functional purpose of the control like what it aims to achieve in response to security risks.
    - **Preventative -** Aim to stop security incidents from occurring.
    - **Corrective -** Address and mitigate the security incident after it has occurred.
    - **Detective -** Identify or detect security incidents when they occur.
    - **Deterrent -** Discourage malicious activities by signaling consequences or making attacks more difficult.

MODULE 3 - Introduction to Cybersecurity Tools

- **Log Sources -** A log is a record of events that occur within an organization's systems and networks.
    - **Firewall Log -** A record of attempted or established connections for incoming traffic from the internet. It also includes outbound requests to the internet from within the network.
    - **Network Log -** A record of all computers and devices that enter and leave the network. It also records connections between devices and services on the network.
    - **Server Log -** A server log is a record of events related to services such as websites, emails, or file shares. It includes actions such as login, password, and username requests.
- **Metrics -** Key technical attributes such as response time, availability, and failure rate, which are used to assess the performance of a software application.

- **SIEM Tools -** An 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.
    - **Self Hosted -** Require organizations to install, operate, and maintain the tool using their own physical infrastructure, such as server capacity. These applications are then managed and maintained by the organization's IT department, rather than a third party vendor. Self-hosted SIEM tools are ideal when an organization is required to maintain physical control over confidential data. For example Splunk Enterprise.
    - **Cloud Hosted -** Maintained and managed by the SIEM providers, making them accessible through the internet. Cloud-hosted SIEM tools are ideal for organizations that don't want to invest in creating and maintaining their own infrastructure. For example Splunk Cloud.
- **Security orchestration, automation, and response (SOAR) -** A collection of applications, tools, and workflows that uses automation to respond to security events. Essentially, this means that handling common security-related incidents with the use of SIEM tools is expected to become a more streamlined process requiring less manual intervention. This frees up security analysts to handle more complex and uncommon incidents that, consequently, can’t be automated with a SOAR.

MODULE 4 - Use Playbooks to Respond to Incidents

- **Playbook -** A manual that provides details about any operational action. Playbooks also clarify what tools should be used in response to a security incident. In the security field, playbooks are essential. A playbook provides a predefined and up-to-date list of steps to perform when responding to an incident. Different types of security incidents have their own playbooks that detail who should take what action and when.
- **Incident Response Playbook Phases -** An organization's quick attempt to identify an attack, contain the damage, and correct the effects of a security breach.
    - **Preparation**
    - **Detection and Analysis**
    - **Containment**
    - **Eradication and Recovery**
    - **Post Incident Activity**
    - **Coordination**

COURSE 3 - Connect and Protect: Networks and Network Security

MODULE 1 - Network Architecture

- **Network -** A group of connected devices.
    - **LAN -** A local area network, or LAN, spans a small area like an office building, a school, or a home. For example, when a personal device like your cell phone or tablet connects to the WIFI in your house, they form a LAN. The LAN then connects to the internet.
    - **WAN -** A wide area network or WAN spans a large geographical area like a city, state, or country. You can think of the internet as one big WAN. An employee of a company in San Francisco can communicate and share resources with another employee in Dublin, Ireland over the WAN.
- **Network Devices**
    - **Hub -** broadcasts information to every device on the network. Think of a hub like a radio tower that broadcasts a signal to any radio tuned to the correct frequency.
    - **Switch -** A switch connects specific devices on a network by sending and receiving data between them. Unlike a hub, a switch is more intelligent, as it only forwards data to the intended device. This enhances security, controls traffic flow, and improves network performance.
    - **Router -** A network device that connects multiple networks is called a router. When a computer wants to send information to a device (like a tablet) on another network, the data first travels to the router. The router reads the destination address, forwards the data to the next network's router, and finally, the receiving router sends the data to the intended device.
    - **Modem -** A modem connects your router to the internet, providing internet access to the local network (LAN). When a computer wants to send data to a device on a different network, the data travels from the computer to the router, then through the modem to the internet. The recipient's modem receives the data, passes it to their router, and the router forwards it to the destination device.
    - **Firewall -** Firewalls are a line of defense that monitor traffic to and from your network. They can also restrict specific types of traffic. They typically reside between the secured internal network and untrusted outside network.
    - **Virtualization Tools -** Pieces of software that perform network operations. Virtualization tools carry out operations that would normally be completed by a hub, switch, router, or modem, and they are offered by Cloud service providers. These tools provide opportunities for cost savings and scalability. They are not physical like the other devices discussed above.
- **Cloud Computing -** the practice of using remote servers, applications, and network services that are hosted on the internet instead of on local physical devices. Cloud providers offer an alternative to traditional on-premise networks, and allow organizations

to have the benefits of the traditional network without storing the devices and managing the network on their own. Cloud service providers offer:
    - On demand storage
    - Processing power
    - Analytics
    - No need for companies to host their own infrastructure
    - Better reliability
    - Reduced cost
    - Scalability
- **CSPs provide three main categories of services**
    - Software as a service (SaaS)
    - Infrastructure as a service (IaaS)
    - Platform as a service (Paas)
- **Network Communication Terms**
    - **Data packet -** A data packet is a basic unit of information that travels from one device to another within a network.
    - **Bandwidth -** 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 -** The practice of capturing and inspecting data packets across the network.
    - **Port -** A software-based location that organizes the sending and receiving of data between devices on a network. Ports divide network traffic into segments based on the service they will perform between two devices.
- **TCP/IP Model -** Transmission Control Protocol and Internet Protocol. TCP/IP is the standard model used for network communication. TCP is for establishing a connection between two devices. The IP is for the set of standards used for routing and addressing the data packets. There are four layers to the TCP/IP Model.
    - **Network access layer -** Deals with creation of data packets and their transmission across a network. This includes hardware devices connected to physical cables and switches that direct data to its destination.
    - **Internet layer -** Where IP addresses are attached to data packets to indicate the location of the sender and receiver.
    - **Transport layer -** Includes protocols to control the flow of traffic across a network. These protocols permit or deny communication with other devices and include information about the status of the connection.
    - **Application layer -** Protocols determine how the data packets will interact with receiving devices. Functions that are organized at the application layer include file transfers and email services.

- **OSI Model**
    - **Application -** Provides end-user services and interfaces, enabling communication between software applications (e.g., HTTP, FTP).
    - **Presentation -** Translates, encrypts, and compresses data for application layer processing.
    - **Session -** Manages and maintains communication sessions between applications.
    - **Transport -** Ensures reliable data transfer with error recovery, segmentation, and flow control (e.g., TCP/UDP).
    - **Network -** Routes data packets between devices across different networks using logical addressing (e.g., IP addresses).
    - **Data Link -** Manages error detection, flow control, and MAC addressing for direct node-to-node communication.
    - **Physical -** Physical hardware that handles the transmission of raw binary data over physical media like cables and radio waves.
- **13 fields within the header of an IPv4 packet**
    - **Version (VER) -** This 4 bit component tells receiving devices what protocol the packet is using. The packet used in the illustration above is an IPv4 packet.
    - **IP Header Length (HLEN or IHL) -** HLEN is the packet's header length. This value indicates where the packet header ends and the data segment begins.
    - **Type of Service (ToS) -** Routers prioritize packets for delivery to maintain quality of service on the network. The ToS field provides the router with this information.
    - **Total Length -** This field communicates the total length of the entire IP packet, including the header and data. The maximum size of an IPv4 packet is 65,535 bytes.
    - **Identification -** IPv4 packets can be up to 65, 535 bytes, but most networks have a smaller limit. In these cases, the packets are divided, or fragmented, into smaller IP packets. The identification field provides a unique identifier for all the fragments of the original IP packet so that they can be reassembled once they reach their destination.
    - **Flags -** This field provides the routing device with more information about whether the original packet has been fragmented and if there are more fragments in transit.
    - **Fragmentation Offset -** The fragment offset field tells routing devices where in the original packet the fragment belongs.
    - **Time to Live (TTL) -** TTL prevents data packets from being forwarded by routers indefinitely. It contains a counter that is set by the source. The counter is decremented by one as it passes through each router along its path. When the TTL counter reaches zero, the router currently holding the packet will discard the packet and return an ICMP Time Exceeded error message to the sender.

- **Protocol -** The protocol field tells the receiving device which protocol will be used for the data portion of the packet.
- **Header Checksum -** The header checksum field contains a checksum that can be used to detect corruption of the IP header in transit. Corrupted packets are discarded.
- **Source IP Address -** The source IP address is the IPv4 address of the sending device.
- **Destination IP Address -** The destination IP address is the IPv4 address of the destination device.
- **Options -** The options field allows for security options to be applied to the packet if the HLEN value is greater than five. The field communicates these options to the routing devices.

MODULE 2 - Network Operations

- **Common Network Protocols -** A network protocol is a set of rules used by two or more devices on a network to describe the order of delivery and the structure of data. Network protocols serve as instructions that come with the information in the data packet.
  - **Communication Protocols -** Govern the exchange of information in network transmission. Dictate how the data is transmitted between devices.
    - Transmission Control Protocol (TCP)
    - User Datagram Protocol (UDP)
    - Hypertext Transfer Protocol (HTTP) - Port 80
    - Domain Name System (DNS) - Port 53
  - **Management Protocols -** Used for monitoring and managing activity on a network. Include protocols for error reporting and optimizing performance.
    - Simple Network Management Protocol (SNMP)
    - Internet Control Message Protocol (ICMP)
  - **Security Protocols -** Ensure that data is sent and received securely across a network by using encryption algorithms to protect data in transit.
    - Hypertext Transfer Protocol Secure (HTTPS) - Port 443
    - Secure File Transfer Protocol (SFTP) - TCP Port 22
- **Additional Network Protocols**
  - **DHCP -** UDP port 67 for servers, UDP port 68 for clients
  - **ARP -** None
  - **Telnet -** TCP port 23
  - **SSH -** TCP port 22
  - **POP3 -** TCP/UDP port 110 unencrypted, TCP/UDP port 995 encrypted
  - **IMAP -** TCP port 143 unencrypted, TCP port 993 encrypted
  - **SMTP -** TCP/UDP port 25 unencrypted
  - **SMTPS -** TCP/UDP port 587 encrypted

- **Wireless Security Protocols**
    - **WEP -** The earliest Wi-Fi security protocol, now considered weak due to vulnerabilities in its encryption.
    - **WPA -** Improved security over WEP, using TKIP encryption, but still vulnerable to attacks.
    - **WPA2 -** Stronger security with AES encryption, widely used but susceptible to some exploits like KRACK attacks.
    - **WPA3 -** The latest standard, offering improved encryption, protection against brute-force attacks, and stronger security for open networks.
- **Firewalls -** A network security device that monitors traffic to and from your network. It either allows traffic or it blocks it based on a defined set of security rules. A firewall can use port filtering, which blocks or allows certain port numbers to limit communication.
    - **Hardware Firewall -** Inspects each data packet before it's allowed to enter the network
    - **Software Firewall -** Performs the same functions as a hardware firewall, but it's not a physical device. Instead, it's a software program installed on a computer or on a server. If the software firewall is installed on a computer. Costs less and doesn't take up any extra space, but will add some processing burden.
    - **Cloud Based Firewalls -** Software firewalls hosted by a cloud service provider. Organizations can configure the firewall rules on the cloud service provider's interface, and the firewall will perform security operations on all incoming traffic before it reaches the organization’s onsite network.
    - **Stateful Firewalls -** Stateful refers to a class of firewall that keeps track of information passing through it and proactively filters out threats. Analyzes network traffic for characteristics and behavior that appear suspicious and stops them from entering the network.
    - **Stateless Firewalls -** Stateless refers to a class of firewall that operates based on predefined rules and does not keep track of information from data packets. Only acts according to preconfigured rules set by the firewall administrator.
    - **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.
- **VPN -** Virtual private networks 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. VPNs encapsulates your data in transit and the encryption is unhackable without a cryptographic key.
- **Security Zones -** Security zones are a segment of a network that protects the internal network from the internet. They are a part of a security technique called network segmentation that divides the network into segments.

    - **Uncontrolled Zone -** Any network outside of the organization's control.
    - **Controlled Zone**
        - **DMZ -** Acts as a network perimeter to the internal network and is situated between two firewalls.
        - **Internal Network -**
        - **Restricted Zone -** Protects highly confidential information that is only accessible to employees with certain privileges.
- **Subnetting -** Dividing a network within a network. Allows a subnet of devices to function as their own network and makes the network run more efficiently and creates additional security zones.
- **Proxy Servers -** A server that fulfills the request of a client by forwarding them on to other servers. The proxy server is a dedicated server that sits between the internet and the rest of the network. Can also be used to block unsafe websites that users aren't allowed to access. Proxy servers also use temporary memory to store data that's regularly requested by external servers.

MODULE 3 - Secure Against Network Intrusions

- **Common Network Attacks**
    - **Interception Attacks -** Malicious actors can use hardware or software tools to capture and inspect data in transit i.e. packet sniffing. They can also intercept network traffic and alter it or redirect it.
    - **Backdoor Attacks -** Backdoors are weaknesses intentionally left by programmers or system and network administrators that bypass normal access control mechanisms. Backdoors can also be installed later by attackers to ensure they have persistent access.
    - **DOS Attacks -** Targets a network or server and floods it with network traffic. The objective is to disrupt business operations by overloading an organization's network. The goal of the attack is to send so much information to a network device that it crashes or is unable to respond to legitimate users. A DDOS attack is similar to DOS but uses multiple devices from different locations to target the network, usually done through botnets.
        - **SYN Flood Attack -** Exploits the syn ack handshake process.
        - **ICMP Flood Attack -** Repeatedly sends ICMP packets to a server.
        - **Ping of Death -** Sends an oversized ICMP packet bigger than 64KB.
- **Network Protocol Analyzers -** Also called a packet sniffer or packet analyzer is a tool used to capture and analyze data traffic in a network. Some pieces of information you get from using a packet capture tool are: Timestamp, Source IP, Source Port, Destination IP, Destination Port. These tools help establish a baseline for network traffic patterns, detect and identify malicious traffic, create customized alerts to send when threats arise and locate unauthorized traffic. Some common network protocol analyzers are:

    - SolarWinds NetFlow Traffic Analyzer
    - ManageEngine OpManager
    - Azure Network Watcher
    - Wireshark
    - Tcpdump
- **Network Attack Tactics**
    - **Packet Sniffing -** The practice of using software tools to observe data as it moves across a network. May be used to analyze and capture packets when investigating ongoing incidents or when debugging network issues.
        - **Passive Packet Sniffing -** Data packets are read while in transit.
        - **Active Packet Sniffing -** Data packets are manipulated while in transit.
    - **How to Prevent Packet Sniffing**
        - Use a VPN.
        - Make sure the websites you visit use HTTPS.
        - Avoid using unprotected wifi.
    - **IP Spoofing -** When an attacker changes the source IP of a data packet to impersonate an authorized system and gain access to a network.
        - **On Path Attack -** When a malicious actor places themselves in the middle of an authorized connection to intercept or alter the data in transit. They sniff the packet information to learn the IP and MAC addresses of devices that are communicating and then pretend to be either of these devices.
        - **Replay Attack -** When a malicious actor intercepts a data packet in transit and delays it or repeats it at another time. A delayed packet can cause connection issues between target computers, or a malicious actor may take a network transmission that was sent by an authorized user and repeat it at a later time to impersonate the authorized user.
        - **Smurf Attack -** This 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. This overwhelms the target computer and can bring down a server or the entire network.
    - **How to Prevent IP Spoofing**
        - Ensure strong encryption so that your data cannot be read.
        - Create proper firewall rule configurations to reject certain IPs.

MODULE 4 - Security Hardening

- **Security Hardening -** The process of strengthening a system to reduce its vulnerability and attack surface.
- **Operating System Hardening -** The OS is the first program loaded when a computer turns on. It's important to secure the OS in each system because one insecure OS can lead to a whole network being compromised. The following are some ways to harden the OS.

    - **Patch Updates -** A software and operating system, or OS, update that addresses security vulnerabilities within a program or product. The OS should be upgraded to its latest version.
    - **Up-to-date Baseline OS -** A baseline configuration is a documented set of specifications within a system that is used as a basis for future builds, releases, and updates.
    - **Hardware and Software Disposal -** Ensure old hardware is properly wiped and disposed of. Delete any unused software applications as many popular programing languages have known vulnerabilities that will contribute to increasing your assets overall attack surface.
    - **Strong Password Policy -** Strong password policies require that passwords follow specific rules depending on the organization. It is also good to implement MFA for an added layer of security.
- **Brute Force Attacks -** A brute force attack is a trial-and-error process executed by an attacker to discover private information. OS hardening tactics can help prevent or counteract brute force attacks. The following are some tools and tactics used in the industry to help avoid cyber attacks.
    - **Virtual Machines -** Can be used to test and execute potentially malicious code in contained environments. Such as when investigating infected machines. But there is always a small risk that a malicious program can escape the virtual environment and affect the host system.
    - **Sandbox environments -** A type of testing environment that lets you excavate software/programs separate from your network. Usually used to test upgrades/patches/bug fixes for test environments before deploying to prod.
    - **Salting and Hashing -** Hashing maintains data integrity while salting adds more complexity to the hash value making it even more secure.
    - **MFA -** Multi Factor authentication requires users to verify their identity in two or more ways before they are allowed into a system. This adds an additional layer of security in case an attacker is able to compromise a password.
    - **CAPTCHA -** A way for computers to be able to tell humans and robots apart. It helps prevent brute force attacks.
    - **Password Policies -** Indicate how strong passwords should be and how often they must be updated to prevent successful password attacks.
- **Network Hardening -** Focuses on network-related security hardening, like port filtering, network access privileges, and encryption over networks. Some network hardening tasks are performed regularly, while others are performed once and then updated as needed. Some methods of network hardening include the following:
    - **Port Filtering -** A firewall function that blocks or allows certain port numbers to limit unwanted communication. Only needed ports are allowed.

    - **Network Access Privilege -** Use network segmentation to create isolated subnets for different departments in an organization. This helps ensure issues in a certain subnet do not spread to other subnets.
    - **Encryption -** All network communication should be encrypted using the latest encryption standards such as AES-256.
    - **Firewall Rules Maintenance -** Periodically review, update, and optimize firewall rules to ensure they remain effective and aligned with current security needs
    - **Network Log Analysis -** Examining network logs to identify events of interest, usually done by using a SIEM tool such as Splunk, Solarwinds or LogRhythm.
    - **Patch Updates -** Ensuring network systems have the latest upgrades installed.
    - **Server Backups -** Regularly create copies of critical server data, stored on a separate system or location, to enable recovery in case of a system failure, cyberattack, or accidental data deletion.
    - **IDS -** Sniff data packets in transit across the network and analyze them for the characteristics of known attacks. They review the packets for signatures of known attacks, and also for anomalies that could be the sign of malicious activity. Once an anomaly is detected the network admin is notified to investigate further. IDS is usually placed behind the firewall to limit the amount of data it has to analyze.
    - **IPS -** An application that monitors system activity for intrusive activity and takes action to stop the activity. It offers even more protection than an IDS because it actively stops anomalies when they are detected.
    - **SIEM -** Security information and event management systems are applications that collect and analyze log data to monitor critical activities in an organization. SIEM tools work in real time to report suspicious activity in a centralized dashboard. SIEM tools analyze network log data sourced from IDSs, IPSs, firewalls, VPNs, proxies, and DNS logs. They aggregate security event data so that it all appears in one place for security analysts to analyze.
- **Cloud Hardening -** 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. They host company data and applications using cloud computing to provide on-demand storage, processing power, and data analytics. Some things to consider in cloud security are:
    - **IAM -** Helps organizations manage digital identities in their environments. This service authorizes how users can use different cloud resources.
    - **Configuration -** Each individual cloud service needs to precisely be configured to uphold security compliance standards.
    - **Attack Surface -** CSPs often offer a multitude of different cloud services and applications. Each service/application carries its own set of risks and vulnerabilities and increases an organization's overall attack surface.
    - **Zero Day Attacks -** A zero day attack is an exploit that was previously unknown, usually a newly discovered vulnerability that doesn't have a solution yet.

- **Visibility and Tracking -** CSPs take responsibility for security in the cloud and don't allow organizations that use their services to monitor traffic on their servers. This can be a concern for organizations that are used to having full control and visibility over their network. CSPs do regular third party audits on their infrastructure to verify that their cloud security is up to standard.
- **Fast Paced Dynamic Environment -** CSPs work hard to stay up to date with technological advancements, this can be a potential challenge for their customers. Updates made by the CSP can affect connection configurations for their customers. For this reason organizations that use CSPs usually have to frequently update their IT processes.
- **Shared Responsibility Model -** States that the CSP must take responsibility for security involving the cloud infrastructures like the physical data centers, hypervisors and host operating systems. The company using the cloud service is responsible for their assets and the processes that they use to operate in the cloud. This model ensures that both the CSP and its users agree about where their responsibility for security begins and ends.
- **Hypervisors -** Isolates the host's hardware from the operating system, allowing the software environment to function independently of the underlying hardware. CSPs are responsible for managing the hypervisor and other virtualization components. Vulnerabilities in hypervisors can lead to VM escapes.
  - **Type 1 Hypervisor -** Run on the hardware of the host computer for example VMware's ESXi. CSPs commonly use this type.
  - **Type 2 Hypervisor -** Operate on the software of the host computer, for example VirtualBox.
- **Baselining -** A fixed reference point that can be used to compare changes made to a cloud environment. Examples of baselining in a cloud environment include:
  - Restricting access to the admin portal of the cloud environment.
  - Enabling password management.
  - Enabling file encryption.
  - Enabling threat detection services for SQL databases.
- **Cryptography -** Cryptography is applied to secure data that is processed and stored in a cloud environment. It uses encryption and security key management systems to provide data integrity and confidentiality.
  - **Cryptographic Erasure -** Involves destroying the encryption keys used to decrypt data, making it unreadable. This method is more effective than traditional data destruction, as it ensures all copies of the key are eliminated so nobody can access the data in the future.
- **Key Management -** Encryption relies on keeping the encryption keys secure. TMPs securely store passwords, certs and encryption keys. CloudHSMs provide secure storage for cryptographic keys and process cryptographic operations.

COURSE 4 - Tools of the Trade: Linux and SQL

MODULE 1 - Introduction to Operating Systems

- **Operating System -** The interface between the computer hardware and the user. The OS is responsible for making the computer run as efficiently as possible while also making it easy to use. Operating systems help humans and computers communicate and allow users to run multiple applications at once. Maintaining the security of an operating system is also critical for the security of a computer. The following are common operating systems.
    - **Windows -** Released in 1985 and is closed source.
    - **MacOS -** Released in 1984 and is partially open source.
    - **Linux -** Released in 1991 and is open source.
    - **Solaris -** Released in 1992 and is partially open source.
    - **ChromeOS -** Released in 2011 and is partially open source.
    - **Android -** Mobile OS released in 2008 and is open source.
    - **iOS -** Mobile OS released in 2007 and is partially open source.
- **Legacy Operating Systems -** An OS that is outdated but still being used. Some organizations still use legacy operating systems because software they rely on is not compatible with newer operating systems. These operating systems can be vulnerable to security issues because they're no longer supported or updated by their manufacturer.
- **Known Vulnerability Resources -** Listed below are some good resources to research known vulnerabilities. These are not only for operating system level vulnerabilities but also for software, hardware, cloud services, applications, and network devices.
    - **General Vulnerability Databases**
        - National Vulnerability Database (NVD)
        - Common Vulnerabilities and Exposures (CVE)
        - Exploit Database (Exploit-DB)
        - MITRE ATT&CK
        - Shodan Vulnerability Search
        - CISA Known Exploited Vulnerabilities Catalog
    - **Vendor-Specific Security Bulletins**
        - Cisco Security Advisories
        - Red Hat Security Advisories
        - Oracle Security Alerts
        - VMware Security Advisories
    - **Open Source & Linux**
        - Debian Security Tracker
        - Arch Linux Security Advisories
    - **Cloud & SaaS Platforms**
        - AWS Security Bulletins
        - Azure Security Center

    - **Browser & Application Security**
        - Mozilla Foundation Security Advisories
        - Chrome Security Releases
    - **Community and Crowd-Sourced Platforms**
        - HackerOne Vulnerability Database
        - GitHub Security Advisories
    - **Zero-day exploits**
        - Google Project Zero
        - Zero Day Initiative (ZDI)
- **How Operating Systems work**
    - **Booting the OS -** When you press the power button, you're interacting with the hardware. This boots the computer and brings up the operating system. Booting the computer means that a special microchip called a BIOS is activated. Then a special program called the bootloader is responsible for starting the operating system. Then the computer turns on.
    - **Completing a Task -** There is a four part process to executing a task.
        - **1) User -** The first part of the process is the user. The user initiates the process by having something they want to accomplish on the computer. Right now, you're a user! You've initiated the process of accessing this reading.
        - **2) Application -** The application is the software program that users interact with to complete a task. For example, if you want to calculate something, you would use the calculator application. If you want to write a report, you would use a word processing application. This is the second part of the process.
        - **3) Operating System -** The operating system receives the user's request from the application. It's the operating system's job to interpret the request and direct its flow. In order to complete the task, the operating system sends it on to applicable components of the hardware.
        - **4) Hardware -** The hardware is where all the processing is done to complete the tasks initiated by the user. For example, when a user wants to calculate a number, the CPU figures out the answer. As another example, when a user wants to save a file, another component of the hardware, the hard drive, handles this task. After the work is done by the hardware, it sends the output back through the operating system to the application so that it can display the results to the user.
- **Resource Allocation -** The OS is responsible for ensuring that each program is allocating and deallocating resources. The OS ensures the limited capacity of the computer system is used where it is needed most. You can see the resource allocation in the task manager.

- **Virtualization -** The process of using software to create virtual representations of various physical machines. Virtual machines don't exist physically, but operate like they do because their software simulates physical hardware. Virtual systems don't use dedicated physical hardware. They use software-defined versions of the physical hardware. Some of the benefits of using virtual machines are:
    - **Security -** VMs run in an isolated environment which adds a layer of security. A security professional can intentionally place malware on a VM to examine its effects and study how it works without harming other systems.
    - **Efficiency -** Multiple VMs can be hosted on the same physical machine, which allows for enhanced streamlining of security tasks.
- **User Interfaces -** 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 OS.
    - **GUI -** Uses icons on the screen to manage different tasks on the computer. Most operating systems can be used with a graphical user interface.
        - Has graphics and icons on the screen making it easier to navigate.
        - Can only perform one function at a time.
    - **CLI -** A text-based user interface that uses commands to interact with the computer. These commands communicate with the operating system and execute tasks like opening programs. Allows for more customization than GUI.
        - Only has text and looks similar to lines of code.
        - Can handle multiple requests at a time making it more efficient.
        - Maintains a history file to see what actions have been made.

MODULE 2 - The Linux Operating System

- **Components of the Linux Architecture**
    - **User -** The user is the person interacting with a computer. They initiate and manage computer tasks. Linux is a multi-user system, which means that multiple users can use the same resources at the same time.
    - **Application -** Applications are programs that perform specific tasks such as calculators or calendars. Some come preinstalled on your computer and others can be installed through a package manager tool.
    - **Shell -** The command-line interpreter. Everything entered into the shell is text based. The shell allows users to give commands to the kernel and receive responses from it.
    - **Filesystem Hierarchy Standard -**
    - **Kernel -**
    - **Hardware -**
-

MODULE 3 - Linux Commands in the Bash Shell

MODULE 4 - Databases and SQL

COURSE 5 - Assets Threats and Vulnerabilities

MODULE 1 - Introduction to Asset Security

MODULE 2 - Protect Organizational Assets

MODULE 3 - Vulnerabilities in Systems

MODULE 4 - Threats to Asset Security

COURSE 6 - Sound the Alarm: Detection and Response

MODULE 1 - Introduction to Detection and Incident Response

MODULE 2 - Network Monitoring and Analysis

MODULE 3 - Incident Investigation and Response

MODULE 4 - Network Traffic and Logs Using IDS and SIEM Tools

COURSE 7 - Automate Cybersecurity Tasks with Python

MODULE 1 - Introduction to Python

MODULE 2 - Write Effective Python Code

MODULE 3 - Work with Strings and Lists

MODULE 4 - Python in Practice

COURSE 8 - Put it to Work: Prepare for Cybersecurity Jobs

MODULE 1 - Protect Data and Communicate Incidents

MODULE 2 - Escalate Incidents

MODULE 3 - Communicate Effectively to Influence Stakeholders

MODULE 4 - Engage with the Cybersecurity Community

Other Notes

A Cybersecurity Professional's Toolkit		
Tool Category	**Purpose**	**Examples**
Network Security		• **Firewalls -** pfSense, Cisco ASA, Palo Alto Networks. • **IDS/IPS -** Snort, Suricata, Zeek. • **Network Scanners -** Nmap, Nessus.
Endpoint Security		• **Antivirus/Antimalware -** Windows Defender, CrowdStrike Falcon, Symantec. • **EDR -** SentinelOne, Carbon Black, Microsoft Defender for Endpoint.
IAM		• **SSO -** Okta, Azure AD, Ping Identity. • **MFA -** Google Authenticator, Duo Security. • **PAM -** CyberArk, BeyondTrust.
Vulnerability Management		• **Vulnerability Scanners -** Qualys, Nessus, Rapid7 InsightVM. • **Patch Management -** WSUS, Ivanti, ManageEngine Patch Manager.
Threat Intelligence and SIEM		• **SIEM -** Splunk, IBM QRadar, Microsoft Sentinel. • **Threat Intelligence Platforms -** MISP, Recorded Future, ThreatConnect.
Penetration Testing		• **Exploitation Frameworks -** Metasploit, Cobalt Strike. • **Password Crackers -** John the Ripper, Hashcat. • **Web Security Testing -** Burp Suite, OWASP ZAP.
Cloud Security		• **CSPM -** Prisma Cloud, Wiz, Dome9.

		• **CWPP -** Lacework, Aqua Security. • **CASB -** McAfee MVISION, Microsoft Defender for Cloud Apps.
Data Security and Encryption		• **Encryption Tools -** VeraCrypt, BitLocker, OpenSSL. • **DLP -** Symantec DLP, Forcepoint DLP.
SOAR		• **SOAR Platforms -** Splunk SOAR, Palo Alto Cortex XSOAR, IBM Resilient.
Forensics and Incident Response		• **Digital Forensics -** Autopsy, FTK, EnCase. • **Memory Analysis -** Volatility, Rekall.