Assets, Threats, and Vulnerabilities
Assets are things perceived to have value. They should be protected whether they are in use, in transit, or at rest. Data is a particularly important asset. We can track what assets we have via asset management, by listing them in an asset inventory. We can then use asset classification to keep track of what assets are, where they are, who owns them, and classify them as public, internal (or private), confidential, or restricted to help prioritize some assets over others.

Confidentiality is the idea that only authorized users can access specific assets or data. Integrity is the idea that only authorized users can access specific assets or data. Availability is the idea that only authorized users can access specific assets or data.

A risk is anything that can negatively impact the confidentiality, integrity, or availability of an asset. A higher likelihood and a greater impact mean a greater risk. A threat is any circumstance or event that can negatively impact assets. A vulnerability is a weakness that can be exploited by a threat. These can be either technical or human. Both threats and vulnerabilities are types of risks, but you need both a vulnerability and a threat actor to exploit it to create a security incident.

Authentication and Authorization
Authentication is the process of verifying who someone is (proving that someone is who they say they are, using something they know, have, or are; SSO and MFA are examples). Authorization is the concept of granting access to specific resources in a system. The principle of least privilege is the concept of granting only the minimal access and authorization required to complete a task or function. Separation of duties is the principle that users should not be given levels of authorization that would allow them to misuse a system.

Information privacy refers to the protection from unauthorized access and distribution of data. Information security (InfoSec) refers to the practice of keeping data in all states away from unauthorized users. Access controls are security controls that manage access, authorization, and accountability of information (AAA). Identity and access management (IAM) is a collection of processes and technologies that helps organizations manage digital identities in their environment. To this end, user provisioning is the process of creating and maintaining a user's digital identity.

Security Hardening and Documentation
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. Security posture is an organization’s ability to manage its defense of critical assets and data and react to change. Resilience is the ability to prepare for, respond to, and recover from disruptions. Security hardening is the process of

strengthening a system to reduce its vulnerability and attack surface. Security and vulnerability assessments can test how resilient current security controls are against threats.

A policy is a set of rules that reduces risks and protects information. Standards are references that inform how to set policies. Procedures are step-by-step instructions to perform a specific security task. Following a cybersecurity framework is voluntary; complying with federal regulations is mandatory. GDPR, PCI DSS, and HIPAA are regulations describing required protections of people's data. Security audits can be performed to determine compliance with these regulations and other policies.

Documentation is any form of recorded content that is used for a specific purpose and can help with transparency, standardization, and clarity. An incident response plan is a document that outlines the procedures to take in each step of incident response. A playbook is a manual that provides details about any operational action. A business continuity plan (BCP) is a document that outlines the procedures to sustain business operations during and after a significant disruption. A disaster recovery plan allows an organization's security team to outline the steps needed to minimize the impact of a security incident. An incident handler's journal is a form of documentation used in incident response that describes the incident, lists tools used by the attacker, and records the who, what, when, where, and why of the incident. Chain of custody is the process of documenting evidence possession and control during an incident lifecycle. The final report is documentation that provides a comprehensive review of the incident.

Incident Detection

An event is an observable occurrence on a network, system, or device. An incident is an event 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. Types include malware infection, unauthorized usage, and improper usage. Detection refers to the prompt discovery of security events and analysis involves the investigation and validation of alerts.

A log is a record of events that occur with an organization's systems. Types include network, system, application, security, and authentication. Telemetry is the collection and transmission of data for analysis. Indicators of Attack (IoA) are the series of observed events that indicate a real-time incident, whereas Indicators of Compromise (IoC) are observable evidence that suggests signs of a potential security incident. An Intrusion Detection System (IDS) is an application that monitors system (host-based) and network (network-based) activity and produces alerts on possible intrusions by detecting signatures or anomalies. An Intrusion Prevention System (IPS) is an application that monitors system activity for intrusions and takes action to stop the activity. An Endpoint Detection and Response (EDR) tool is an application that monitors

an endpoint (i.e. any device connected on a network) for malicious activity, and uses behavioral analysis and automation. A Security Information and Event Management (SIEM) tool is an application that collects and analyzes log data to monitor critical activities in an organization. A Security Orchestration, Automation, and Response (SOAR) tool/application/workflow uses automation to respond to security incidents. Other ways to detect incidents besides tools are through threat hunting, threat intelligence, and cyber deception (such as honeypots).

Incident Response

Incident escalation is the process of identifying a potential security incident, triaging it, and handing it off to a more experienced team member. Triage is the prioritizing of incidents according to their level of importance or urgency. Containment is the act of limiting and preventing additional damage caused by an incident. Eradication is the complete removal of the incident elements from all affected systems. Recovery is the process of returning affected systems back to normal operations. Serious breaches should be disclosed in a timely manner to affected employees, customers, and stakeholders as required.

Cybersecurity Roles

Computer Security Incident Response Teams (CSIRT) are a specialized group of security professionals that are trained in incident management and response, whose roles include security analyst, technical lead, and incident coordinator (but the exact structure varies by company). A Security Operations Center (SOC) is an organizational unit dedicated to monitoring networks, systems, and devices for security threats or attacks, either separate from or within a CSIRT, whose roles include SOC analyst, SOC lead, and SOC manager (but again the exact structure varies by company).

CISSP's 8 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

OWASP's Security Principles

Some of them include:

- Minimize attack surface area
- Principle of least privilege
- Defense in depth

- Separation of duties
- Keep security simple
- Fix security issues correctly
- Establish secure defaults
- Fail securely
- Don’t trust services
- Avoid security by obscurity

NIST CSF Core Functions

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover
6. Govern

NIST Incident Response Lifecycle

1. Preparation
2. Detection and analysis
3. Containment, eradication, and recovery
4. Post-incident activity

Defense in Depth Strategy

1. Perimeter layer, like authentication systems that validate user access
2. Network layer, which is made up of technologies like network firewalls and others
3. Endpoint layer, which describes devices on a network, like laptops, desktops, or servers
4. Application layer, which involves the software that users interact with
5. Data layer, which includes any information that’s stored (at rest), in transit, or in use

PASTA Threat Modelling Framework

Process for **A**ttack **S**imulation and **T**hreat **A**nalysis

1. Define business and security objectives
2. Define the technical scope
3. Decompose the application
4. Perform a threat analysis
5. Perform a vulnerability analysis
6. Conduct attack modeling
7. Analyze risk and impact

OWASP Top 10

A list of the 10 most common web vulnerabilities. Updated every few years, but some of the most common vulnerabilities to appear on this list are:

- Broken access control
- Cryptographic failures
- Injection
- Insecure design
- Security misconfiguration
- Vulnerable and outdated components
- Identification and authentication failures
- Software and data integrity failures
- Security logging and monitoring failures
- Server-side request forgery

Pyramid of Pain

1. Hash values- trivial
2. IP addresses- easy
3. Domain names- simple
4. Network artifacts- annoying
5. Host artifacts- annoying
6. Tools - challenging
7. TTPs - tough

Thinking like an attacker

A threat actor is any person or group who presents a security risk, intentional or unintentional. Types include competitors, state actors, criminal syndicates, insider threats, and shadow IT. An Advanced Persistent Threat (APT) refers to instances when a threat actor maintains unauthorized access to a system for an extended period of time.

A hacker is any person who uses computers to gain unauthorized access to computer systems, networks, or data. Types include unauthorized, authorized (aka ethical), and semi-authorized.

Attack vectors are the pathways attackers use to penetrate security defenses. Types include:

- Direct access
- Removable media
- Social media platforms
- Email
- Wireless networks on premises
- Cloud services
- Supply chains

Thinking like an attacker can help with threat modeling, which is the process of identifying assets, their vulnerabilities, and how each is exposed to threats. The red team conducts proactive simulations, assuming the role of an attacker by exploiting vulnerabilities and breaking through defenses. The blue team conducts reactive simulations, assuming the role of a defender responding to an attack.

To think like an attacker:

1. Identify a target
2. Determine how the target can be accessed
3. Evaluate attack vectors that can be exploited
4. Find the tools and methods of attack

A penetration test is a simulated attack that helps identify vulnerabilities in systems, networks, websites, applications, and processes. Digital forensics is the practice of collecting and analyzing data to determine what has happened after an attack.

Kali Linux is a distro that is designed for security testing. It should be used inside a virtual machine. It comes preinstalled with penetration testing tools including Metasploit, Burp Suite, and John the Ripper. It also comes with digital forensics tools including tcpdump, Wireshark, and Autopsy.

HackerOne is a community of ethical hackers where you can find active bug bounties to participate in.

Common attacks

- Emails- an email can be crafted to look like it comes from your company, when in fact it comes from someone impersonating an employee (this is the most common form of phishing). Don't click links or download files from suspicious-looking emails.
- USBs- if you lose own USB, losing it can leak potentially sensitive information, which could be used against you. If you find a random USB, don't plug it into your computer, as it can contain malware. If you decide to investigate it anyway, turn off Autoplay and only examine the USB's contents in an isolated virtual machine.
- Social engineering- a manipulation technique that exploits human error. Done by gathering intel about their target, tricking the target into trusting them, using persuasion tactics, and finally disconnecting from their target. Types include baiting, phishing, quid pro quo, tailgating, and watering hole. Learn more at OUCH! or Scamwatch.
- Phishing- the use of digital communications to trick people into revealing sensitive data or deploying malicious software (aka malware). They're often done using phishing kits, which use malicious attachments, fake data-collection forms, and fraudulent web links.

Types include email phishing, smishing, vishing, spear phishing, and whaling. Learn more at Phishing.org.

- Malware- software designed to harm devices or networks, often used to take control of the target's system without their knowledge or permission. Types include virus, worm, trojan, ransomware, scareware, spyware, cryptojacking, rootkit, and botnet. Learn more at INFOSEC's introductory course on malware analysis.
- Web-based exploits- malicious code or behavior that's used to take advantage of coding flaws in a web application. Examples include cross-site scripting (XSS), SQL injection, and cross-site request forgery (CSRF).
- Brute-force- a trial-and-error approach to systematically guess login info, credentials, and encryption keys. Types include simple brute force attack, dictionary attack, reverse brute force attack, credential stuffing (such as pass the hash), and exhaustive key search. Some common tools to conduct brute-force attacks include Aircrack-ng, Hashcat, John the Ripper, Ophcrack, and THC Hydra.

Common Vulnerabilities and Exposures (CVE) list

An openly accessible dictionary of known vulnerabilities and exposures (an exposure is a mistake that can be exploited by a threat), created by MITRE. The CVE Numbering Authority (CNA) reviews an eligible CVE before assigning it an ID, ensuring that the CVE meet these criteria:

- It's independent of other issues
- It's recognized as a potential security risk
- It's submitted with supporting evidence
- It only affects one codebase

NISTs National Vulnerability Database (NVD) then uses the Common Vulnerability Scoring System (CVSS) to score the severity of the vulnerability from 0 to 10. This is related to the vulnerability assessment process, whose steps are identification, vulnerability analysis, risk assessment, and remediation.

OSINT

Information refers to the collection of raw data or facts about a specific subject. Intelligence refers to the analysis of information to produce knowledge or insights that can be used to support decision-making. Crowdsourcing is the practice of gathering information using public input and collaboration. Open-source intelligence (OSINT) is the collection and analysis of information from publicly available sources to generate usable intelligence (such as gathering information related to threat actors, threats, vulnerabilities).

VirusTotal is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. You can check file hashes here.

MITRE ATT&CK® is a knowledge base of adversary tactics and techniques based on real-world observations.
MalwareBazaar is a free repository for malware samples. Malware samples are a great source of threat intelligence that can be used for research purposes.
OSINT Framework is a web-based interface where you can find OSINT tools for almost any kind of source or platform.
Have I been Pwned is a tool that can be used to search for breached email accounts.

Additional Security Resources
Some security websites and blogs include CSO Online, Krebs on Security, and Dark Reading.
The Cybersecurity & Infrastructure Security Agency (CISA) offers two cybersecurity mailing lists for you to join.

The Google Cybersecurity Certificate glossary provides many definitions for cybersecurity terms.

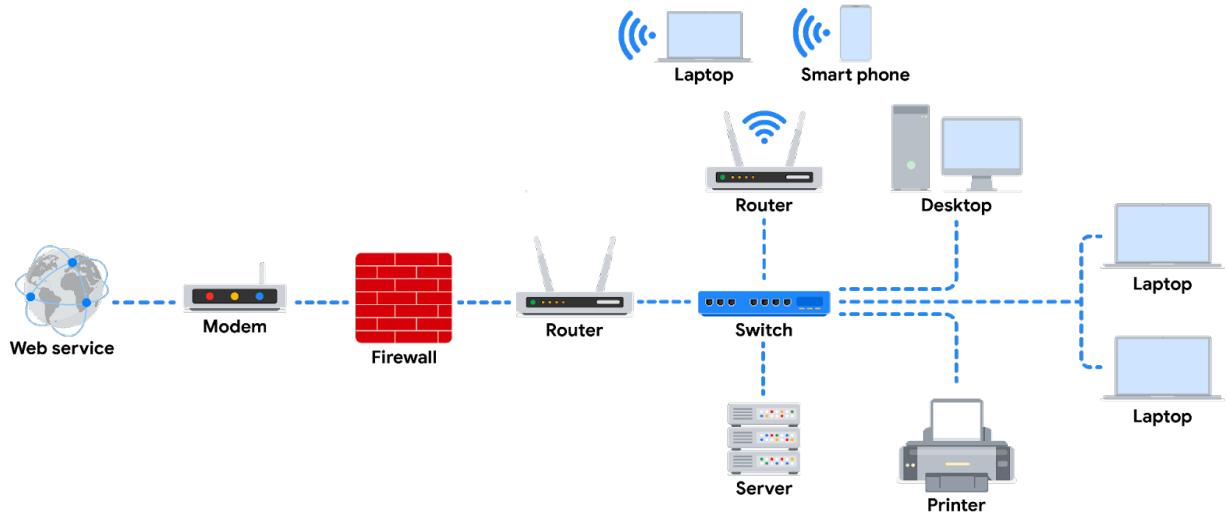
This is not part of the Google Cybersecurity Certificate course, but WolvSec is a cybersecurity club at the University of Michigan that has resources for beginners here.

You can follow Chief Information Security Officers (CISOs) on LinkedIn. You can also Google security associations conferences (such as BSides) in your area. You can also find others in the cybersecurity community on social media or LinkedIn.

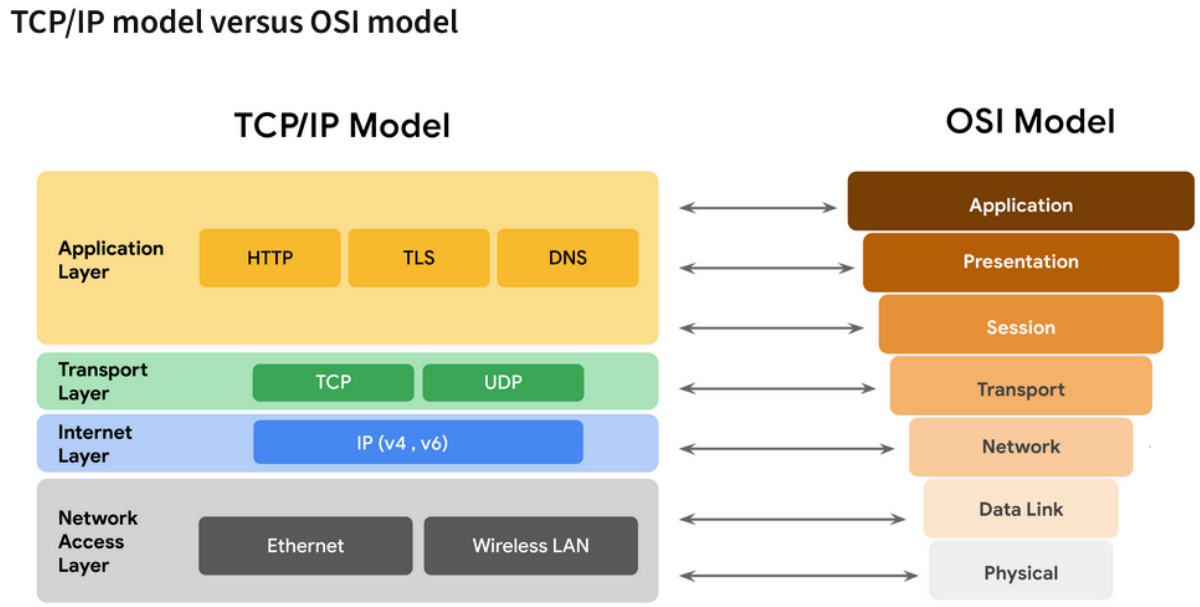
Network Structure
A network is a group of connected devices. Network traffic is the amount of data that moves across a network. Network data is the data that's transmitted between devices on a network.

Different network devices include:

- Hub- broadcasts information to every device on the network
- Switch- makes connections between specific devices on a network by sending and receiving data between them
- Router- connects multiple networks together
- Modem- connects your router to the internet and brings internet access to the LAN
- Firewall- monitors traffic to or from your network



Two common network models are the TCP/IP model and OSI model.



There are three main categories of network protocols:

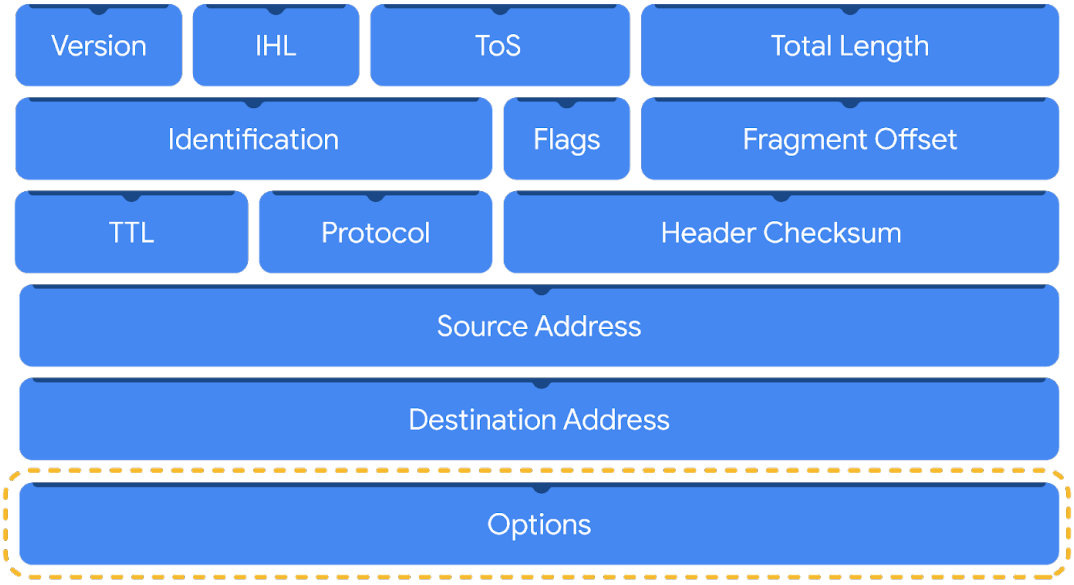
- Communication protocols
    - ex: DNS, HTTP, TCP, and UDP
- Management protocols
    - ex: SNMP (Simple Network Management Protocol) and ICMP (Internet Control Message Protocol)
- Security protocols
    - ex: HTTPS and SFTP

Here are other protocols.

Protocol	Port
DHCP	UDP port 67 (servers) UDP port 68 (clients)
ARP	none
Telnet	TCP port 23
SSH	TCP port 22
POP3	TCP/UDP port 110 (unencrypted) TCP/UDP port 995 (encrypted, SSL/TLS)
IMAP	TCP port 143 (unencrypted) TCP port 993 (encrypted, SSL/TLS)
SMTP	TCP/UDP Port 25 (unencrypted)
SMTPS	TCP/UDP port 587 (encrypted, TLS)

Wi-Fi is IEEE 802.11. Today it mostly uses the WPA2 and WPA3 protocols.

A data packet is a basic unit of information that travels from one device to another within a network. They contain a header, a payload, and may contain a footer. In more detail, an IPv4 packet header has the following structure.



Network attacks
Some common network attacks are:

- SYN flood- a type of DoS attack that simulates a TCP/IP connection and floods a server with SYN packets
- ICMP flood- a type of DoS attack performed by an attacker repeatedly sending ICMP request packets to a network server
- Ping of death- a type of DoS attack caused when a hacker pings a system by sending it an oversized ICMP packet that is bigger than 64KB
- On-path attack- an attack where a malicious actor places themselves in the middle of an authorized connection and intercepts or alters the data in transit

Also be aware of Command and Control (C2) and data exfiltration.

Network monitoring
Packet sniffing is the practice of capturing and inspecting data packets across a network. A packet capture (p-cap) is a file containing data packets intercepted from an interface or network. Packet captures can be viewed and further analyzed using a network protocol analyzer (aka packet sniffer). You can use tcpdump to capture (and read) packets. You can use Wireshark to filter a p-cap file to only show packets that come from a particular IP address, a particular MAC address, use a certain protocol, use a certain port, etc. IDSs like Suricata and SIEM tools like Splunk can alert you to IoCs in network logs.

Some related Bash commands include:

- **sudo tcpdump -i <network_interface> <options> <expressions>**
    - Example network interfaces include (run **sudo ifconfig** to see available network interfaces):
        - **any**
        - **eth0**
    - Example options include:
        - **-w <file>.pcap** writes sniffed network packets to **<file>.pcap**
        - **-r <file>.pcap** uses **<file>.pcap** as input rather than live network traffic
        - **-v**, **-vv**, and **-vvv** increase verbosity of output
        - **-n** doesn't resolve hostnames, **-nn** doesn't resolve hostnames and ports. Considered best practice because it prevents malicious actors from being alerted to an investigation
        - **-c <count>** specifies how many packets to capture
    - An example expression is **'ip and port 80'**
- **sudo suricata <options>**
    - Example options include:
        - **-r <file>.pcap** uses **<file>.pcap** as input rather than live network traffic

        - **-S <file>.rules** instructs Suricata to use the rules/signatures defined in **<file>.pcap** (Google how rules should be formatted)
        - **-k none** disables checksum checks
    - Output is written to eve.json

Network defense
Subnetting is the process of taking one large network and dividing it into several smaller, organized groups called subnets. Subnets can make the network more efficient and organized, allowing for distinct security zones within the network. Outside the network is the uncontrolled zone, while controlled zone is a subnet inside the network, which has the DMZ, internal network, and restricted network.

Firewalls can block connections on certain ports and filter out certain network activity. Forward proxy servers and reverse proxy servers can add another layer of security to the network.

VPNs are Virtual Private Networks that encrypt data packets (encapsulation) so proxy servers on the internet cannot read their raw data. There are two types of VPNs, remote access and site-to-site. There are two main VPN protocols, WireGuard and IPSec.

Encryption and hashing
Encryption is the process of converting data from a readable format to an encoded format using a key. There are two types, symmetric and asymmetric. Symmetric encryption requires just one key to encrypt and decrypt. Asymmetric encryption uses one public key to encrypt and another private key to decrypt.

Hashing converts data to a unique, fixed-length value. It is not meant to be decrypted. It helps with non-repudiation, which describes being unable to deny that information is authentic.

Some related Bash commands include:
- **tr** translates characters (useful for Caesar ciphers)
- **openssl** can encrypt or decrypt a file with a given cipher using a given key
- **sha256 <file>** hashes **<file>** using the SHA256 algorithm (which, as the name suggests, produces a 256-bit hash value)
- **cmp <file1> <file2>** returns the position of the first character at which **<file1>** and **<file2>** differ

String and pattern matching in Python
- **a.indexOf(b)** returns the index that **b** appears in **a**
- **re.findall(regex, str)** returns a list of all matches of **regex** in **str**. For example, **“\w+@\w+\.\w+”** would match all emails.

- **a+** matches one or more a's
- **a*** matches zero or more a's
- **a{3}** matches exactly three a's
- **a{1,3}** matches one, two, or three a's
- **\w** matches one alphanumeric character
- **\d** matches one digit
- **\b** matches one whitespace
- **.** matches one character