* Threats, Vulnerabilities & Mitigations

**2.1 Threats Actors**

* **Threat actors**
  + Nation-state
  + Unskilled attacker
  + Hacktivist
  + Insider threat
  + Organized crime
  + Shadow IT
* **Attributes of actors**
  + Internal/external
  + Resources/funding
  + Level of sophistication/capability
* **Motivations**
  + Data exfiltration
  + Espionage
  + Service disruption
  + Blackmail
  + Financial gain
  + Philosophical/political beliefs
  + Ethical
  + Revenge
  + Disruption/chaos
  + War

What is a CyberCriminal:

* An individual or group who intends to exploit a network to gain access.
* CompTIA defines cybercriminals as **threat actors**.
* They are motivated by a variety of factors, including financial gain, political activism, or simply curiosity.
* They use techniques such as phishing, ransomware, and more to get access to their victims.

Types of CyberCriminals:

* **Hackers** use their technical skills to gain unauthorized access to a system.
  + **White hat** hackers work within the law and have permission to hack.
  + **Black hat** hackers are malicious and violate security for personal gain.
  + **Gray hat** hackers are in-between, they can find an opening and not exploit it.
* **Competitors** have other motivations (espionage, reputation, theft).
* **Script kiddies** (unskilled attackers) perform hacking without having the skills to do so on their own. They rely on pre-written code that they find online.
* **Hacktivists** (hacker + activist) are hackers who use their technical skills to promote a political, religious or social cause.
* **Criminal Syndicates** (Organized Crimes) target individuals, businesses, and governments. Their goal is extorting money.
* **Nation States** focus on national security, against external organizations.
* **Insiders** have authorized access to internal resources. They use their credentials to access resources and carry out malicious activities.
* **Shadow IT** refers to the use of IT systems without explicit approval from the organization's IT department. This can lead to data breaches as these unapproved systems are not subject to the same scrutiny.

Attributes of CyberCriminals:

* **Internal/External:**
  + Internal
    - Within the organization (employees, contractors)
    - Legitimate access
    - Motivated by revenge
  + External
    - Outside the organization
    - Hacktivists, Nation-states, Organized crimes
    - No legitimate access
* **Resources/Funding:**
  + Low Resources
    - Unskilled attackers and hacktivists
    - Rely on available tools and social engineering
    - Generally have low sophistication
  + High Resources
    - Nation-states and organized crimes
    - Have more complex and innovative techniques
    - Typically high sophistication

Motivations:

* **Financial Gain**: Stealing money or valuable information for monetary profit.
* **Data Exfiltration**: Unauthorized transfer to an external destination.
* **Espionage**: Spying to gather confidential or classified information.
* **Service** Disruption: Interrupting or disabling critical services.
* **Blackmail**: Threatening to reveal information or cause harm unless demands are met.
* **Beliefs**: Driven by ideological, philosophical, or political motivations.
* **Ethical**: Actions driven by a perceived sense of ethics or moral obligation.
* **Revenge**: Retaliatory actions driven by personal grudges or grievances.
* **Disruption/chaos**: Causing disorder and instability for its own sake.
* **War**: Cyber activities as part of broader military or geopolitical conflicts.

**2.2 Threat Vectors**

* **Message-based**
  + Email
  + Short Message Service (SMS)
  + Instant messaging (IM)
* **Image-based**
* **File-based**
* **Voice call**
* **Removable device**
* **Vulnerable software**
  + Client-based vs. Agentless
* **Unsupported systems and applications**
* **Unsecure networks**
  + Wireless
  + Wired
  + Bluetooth
* **Open service ports**
* **Default credentials**
* **Supply chain**
  + Managed service providers (MSPs)
  + Vendors
  + Suppliers
* **Human vectors/social engineering**
  + Phishing
  + Vishing
  + Smishing
  + Misinformation/disinformation
  + Impersonation
  + Business email compromise
  + Pretexting
  + Watering hole
  + Brand impersonation
  + Typosquatting

Threat Vectors:

The methods that attackers use to gain access.

They can be via images, files, internet, removable devices, software, or more.

* **MESSAGE BASED**
  + Email: Phishing
  + SMS (Smishing)
  + Instant Messages
* **IMAGE BASED**
  + Steganography
  + Malicious image
* **FILE BASED**
  + Malicious attachments
  + .exe, .doc, .pdf
* **VOICE CALL**
  + Vishing (voice phishing)
* **REMOVABLE DEVICE**
  + USB Drives
  + CDs, DVDs, Hard drives
* **VULNERABLE SOFTWARE**
  + Client-Based (software installed on user devices)
  + Agentless (Doesn't need software)
* **UNSUPPORTED APPS**
  + End-of-life apps
  + Security risks
* **UNSECURE NETWORKS**
  + Wi-Fi Attacks
  + Weak encryption
  + Rogue access points
  + Bluetooth attacks
* **OPEN SERVICES**
  + Network ports accessible
* **DEFAULT CREDENTIALS**
  + Pre-configured user names and passwords

UNSECURE NETWORKS

* **Wifi Security**
  + Wi-Fi security is important because Wi-Fi networks can be used to steal sensitive data.
  + Wi-Fi has secure protocols: **WPA2** & **WPA3** (Wi-Fi Protected Access 3).
  + **802.1X** is a protocol that is used to authenticate devices before they are allowed to access a network.
  + WEP and WPS are old Wi-Fi protocols that are unsecure and not used anymore.
* **Bluetooth Attacks**
  + **Bluejacking** allows people to send unsolicited messages to mobile devices over Bluetooth.
  + **Bluesnarfing** refers to unauthorized access to data on a device via Bluetooth.

OPEN SERVICES

* **Open Network Ports**
  + **SSH** (Secure Shell): protocol that allows you to remotely and securely connect to a computer. It uses port **22**.
  + **Telnet** is used to connect remotely to a computer. However, Telnet communication is not encrypted (unsafe). Telnet uses port **23**.

Supply Chain:

* A supply chain is a sequence of suppliers involved in delivering some product.
* The companies that make up your supply chain will have a different look on security than you do.
* It is important to make sure that all the companies involved in the supply chain are secure.

Target 2013 Sandal

* This is exactly what happened in **2013**.
* Target had over **40 million credit cards** compromised.
* Target had secured its perimeter, but not it’s **internal network**.
* The attacker decided to exploit the network of one of Target’s **HVAC providers** and steal its credentials. They gained access to the point of sale terminals and, from there, the credit card information.
* Target lost over **$200 million**

Social Engineering:

* A social engineering attack is a **psychological manipulation technique** used by cybercriminals to deceive individuals into revealing information.
* The **human fact**or in an organization is always the **weakest** link in terms of security, and the **easiest** way to hack a human is via social engineering.
* Some examples of social engineering attacks are:
  + **Phishing**: Sending malicious emails that appear to be from a legitimate source.
  + **Vishing**: Phishing via phone calls.
  + **Smishing**: Phishing via text messages (SMS).
  + **Tailgating**: Following someone into a secure area without authenticating.
  + **Impersonation**: Pretending to be someone you are not.
  + **Brand Impersonation**: Pretending to be a legitimate brand for fraudulent purposes.
  + **Pretexting**: Creating a fabricated scenario to obtain information.
  + **Baiting**: Offering something enticing like a fake reward, to trick individuals.
  + **Typosquatting**: Registering web names similar to popular websites.
  + **Business Email Compromise (BEC):** Compromise legitimate business emails.
  + **Watering Hole**: Attackers compromise websites frequented by their target victims.

**2.3 Vulnerability**

* **Application**
  + Memory injection
  + Buffer overflow
  + Race conditions
  + Time-of-check (TOC)
  + Time-of-use (TOU)
  + Malicious update
* **Operating system (OS)-based**
* **Web-based**
  + Structured Query Language injection (SQLi)
  + Cross-site scripting (XSS)
* **Hardware**
  + Firmware
  + End-of-life
  + Legacy
* **Virtualization**
  + Virtual machine (VM) escape
  + Resource reuse
* **Cloud-specific**
* **Supply chain**
  + Service provider
  + Hardware provider
  + Software provider
* **Cryptographic**
* **Misconfiguration**
* **Mobile device**
  + Side loading
  + Jailbreaking
* **Zero-day**

Threat, Vulnerability & Risk

* A **threat** is a potential danger to an organization.
* People, malware, natural disasters, etc.
* A **vulnerability** is a weakness in a system. Outdated systems, weak passwords, faulty software, etc.
* A **risk** is the probability that a threat will exploit a vulnerability.
* Our role in security is to reduce risk to a minimum.

Types of Vulnerabilities:

**Application Vulnerabilities**

* **Memory Injection**: Attackers able to manipulate the memory of an app to execute code. Can lead to data breaches and system compromise.
* **Buffer Overflow**: It occurs when an app receives more input than it expects, causing data to overwrite other memory spaces and applications to crash.
* **Race Conditions**: Occurs when the timing of actions impacts the app's behavior.
  + **Time-of-check, Time-of-use** (TOC/TOU): Happens when an attacker exploits the time gap between checking a condition and using the result.
  + Can lead to data inconsistency, unauthorized access, app crashing.
* **Malicious Update**: The distribution of software updates that contain malicious code.

**Web Based Vulnerabilities**

* **SQL Injection** **(SQLi)**: Malicious SQL statements are inserted into a query to manipulate a database.
* **Cross-Site Scripting** **(XSS)**: Injects (uploads) malicious scripts (code) into web pages viewed by other users. They eventually steal cookies, session tokens, steal data and financial information.

[Virtual Machine (VM)

* A virtual machine (VM) is a digital version of a physical computer. It is a file that behaves like an actual computer.
* It is a program that works like a separate computer (OS, apps, data, etc.)
* A VM is isolated from the host. This is suitable to run “risky” programs.
* The program that creates and manages VMs is called a **hypervisor** and the computer that is running the VM is called the **host**.]

**Virtualization**

* **VM escape**: Attackers are able to break out of the VM and interact directly with another VM or with the host OS.
* **Resource reuse**: Improper deprovisioning or reuse of resources in virtual environments.

**Hardware Vulnerabilities**

* **Firmware**: The software embedded in hardware devices to control functionality. It is different from regular software because it is not meant to be easily modified.
* **End-of-life**: Hardware that is no longer supported by the manufacturer.

**OS based**: Vulnerabilities within the OS that can be exploited to gain access. This can lead to privilege escalation (attackers gaining higher access levels), data breaches, disruption of services, full system compromise.

**Cloud-specific**: Vulnerabilities related to cloud environments (misconfigurations, multi-tenancy).

**Supply Chain**: Vulnerabilities introduced by vendors and 3 party providers.

**Cryptographic**: Vulnerabilities in cryptographic algorithms (weak keys, poor key management, outdated algorithms).

**Misconfiguration**: Weaknesses due to incorrect configuration of systems (default passwords, default configurations).

**Mobile device**: Weaknesses that can bypass mobile device security.

* **Sideloading**: Installing applications from untrusted sources bypassing official app stores
* **Jailbreaking:** Gaining access to the OS of devices

**Zero-Day Vulnerabilities**: Vulnerabilities that are not yet known by the software vendor and do not have available fixes.

What is Malware?

It is malicious software that is designed to harm a computer.

Most common malware:

* **Viruses**: Malware that can replicate and spread between computers.
* **Worms:** Malware that can self-replicate (propagate itself) within systems without user interaction.
* **Trojans**: Malware that appear to be legitimate software, but they contain malicious code.
* **Ransomware**: Malware that encrypts a victim's files and demands a ransom payment in order to decrypt them.
* **Backdoors**: Malware that provides another way of accessing a system to bypass security.
* **Rootkit**: Malware that gains admin control of a computer without being detected.
* **Keylogge**r: Malware that capturing keystrokes typed by a user.
* **Logic Bomb**: Malware set to execute harmful actions upon meeting specific conditions.
* **Spyware**: Malware that spies on you and steals your information.
* **Bloatware**: Pre-installed software that come with a new device but are often unnecessary. They consume significant memory, and power, slowing down the device's performance.

Network Attacks:

Most common network attacks:

* **DDoS Attacks**: A cyberattack that is designed to overwhelm a server with traffic from multiple locations, making it unavailable to users.
* **DNS Attacks**: Manipulating DNS records to redirect traffic from a legitimate site to a fraudulent one. An attacker alters the DNS entry for cybermuk.com to redirect users to a malicious IP address.
* **Wireless Attacks**:
  + **Rogue Access Points**: Unauthorized wireless access points set up to mimic legitimate ones.
  + **Evil Twins**: Creating a fake wireless network with a name similar to a legitimate one.
* **On-path Attacks (Man-in-the-middle**): Intercepting and potentially altering communication between two parties without their knowledge. Eavesdropping.
* **Credential Replay**: Attackers gain access to network packets, acquire data transferred
* previously, perform the same actions.
* **Malicious code**: Malicious software attached to legitimate files and spreads to other files (viruses, worms), encrypts (ransomware), gathers information (spyware).

Application Attacks:

Most common application attacks are:

* **Injection**: Injecting (adding) malicious commands, queries, code into a program.
  + Situations where an attacker adds data (untrusted) to a program.
  + Code injection is adding malicious code into an app (code).
  + It works because of poor programming.
* **Buffer Overflow**: It occurs when an app receives more input than it expects, causing data to overwrite other memory spaces and applications to crash.
* **Replay**: An attacker intercepts and retransmits a valid data transmission to gain access.
* **Privilege Escalation**: Exploiting vulnerabilities to gain higher access levels than intended.
* **Forgery:** An attack that tricks a user into performing actions on a web application without their consent.
* **Directory Traversal**: Attackers able to access files and directories outside the intended scope.

Cryptographic Attacks:

Most common cryptographic attacks are:

* **Downgrade**: An attacker forces a communication to use a less secure protocol, making it easier to compromise.
  + Example: Modifying web communication from TLS to SSL.
  + Exposes communications to vulnerabilities present in older, weaker protocols.
  + Easier to decrypt or manipulate data.
* **Collision**: An attack where two different inputs produce the same hash. This compromises integrity.
* **Birthday**: An attack that exploits the mathematics of the birthday problem in probability to find collisions in hash functions.

Password Attacks:

Most common password attacks are:

* **Brute-Force**: An attack where every possible combination of characters is tried.
* **Spraying**: Trying a password against many accounts, rather than trying many passwords against a single account.
  + This avoids triggering account lockout.

Indicators of Malicious Activity:

* **Account Lockout**: Multiple failed login account lockout.
* **Concurrent Usage**: Multiple simultaneous sessions from different locations or devices.
* **Blocked Content**: Access to certain websites or services being denied
* **Impossible Travel**: Login Attempts from geographically distant locations in a short time.
* **Resource Consumption**: Unusual or excessive use of CPU, memory or network bandwidth.
* **Resource Inaccessibility**: Legitimate users are unable to access resources they normally can.
* **Out-Of-Cycle Logging**: Logs generated outside normal business hours.
* **Missing Logs**: Unexplained absence of expected log entries.

Mitigation Techniques:

* **Segmentation**: Dividing a network into smaller, isolated sections to enhance security. Limits the spread of malware. Can be done by creating VLANs.
* **Access Control List (ACL**): A list of rules that determines who or what can access resources. ACLs on firewalls.
* **Application Allow List**: A list of approved apps that are permitted to run on a system.
* **Isolation**: Separating systems to prevent interactions that could lead to security issues.
  + For example, running a high-risk app in a VM isolated from the main network.
* **Patching**: Applying updates to software to fix vulnerabilities.
* **Encryption**: Converting data into a coded format to prevent unauthorized access.
* **Monitoring:** Continuously observing and analyzing networks. Using a SIEM tool like Splunk to have real-time monitoring.
* **Least Privilege**: Granting users the minimum level of access necessary to perform their duties.
* **Configuration Enforcement**: Ensuring systems are configured according to security best practices.
* **Decommissioning**: Safely disposing of outdated systems and devices.

Hardening Techniques:

* **Encryption**: Encrypting hard drives and networks to protect data at rest and in transit.
* **Host-based Firewalls**: Configuring firewalls on individual systems to control incoming and outgoing traffic.
* **Host-based Intrusion Prevention Systems (HIPS):** Monitoring and blocking malicious activities on **individual hosts**. Protects systems from attacks and unauthorized activities.
* **Disabling Unnecessary Services**: Shutting down unnecessary ports and protocols to reduce attack surfaces.
* **Changing Defaults:** Changing default passwords on systems to stronger passwords.
* **Removal of Unnecessary Software:** Uninstalling software that is not required for business operations.

Network Best Practices:

* Choose strong Wi-Fi passwords to prevent brute-force attacks.
* Change your passwords regularly.
* Enable WPA2 encryption.
* Be careful about what you're connecting to.
* Keep your software up to date.
* Use a firewall to protect from unauthorized access.
* Monitor your network.
* Educate your users.