2.1.2 Threat Agents Overview

Understanding the attributes and tactics associated with threat actors will help you better identify and defend against them.

Attribute	Description
Internal vs. External	- *Internal threats* are authorized individuals that exploit their inherent privileges to carry out an attack. This category includes employees (both current and former), janitors, security guards, and even customers. - *External threats* are any individuals or groups that attacks a network from the outside and seeks to gain unauthorized access to data.
Persistent vs. Non-Persistent	- *Persistent threats* seek to gain access to a network and remain there undetected. With this type of threat, the attacker will go to great lengths to hide their tracks and presence in the network. - *Non-persistent threats* are only concerned with getting into a system and stealing information. The attack is usually a one-time event, and the attacker typically doesn't care if their presence is noticed. An advanced persistent threat (APT) is a type of persistent threat carried out by a nation state. An APT has the goal of continually stealing information without being detected, and the tactics they use are much more advanced than a traditional persistent threat.
Open-Source Intelligence (OSINT)	Before carrying out an attack, a threat actor will typically gather open-source intelligence (OSINT) about their target. OSINT is information that is readily available to the public and doesn't require any type of malicious activity to obtain. Sources of OSINT include the following: - Media (newspapers, magazines, advertisements) - Internet (websites, blogs, social media) - Public government data (public reports, hearings, press conferences, speeches) - Professional and academic publications (journals, academic papers, dissertations)

The following table describes the different types of threat actors that you need to be aware of as a security professional:

Threat Actor	Description
Insider	An insider is any individual who has authorized access to an organization and either intentionally or unintentionally carries out an attack. The most common type of insider is a full-time employee; however, other inside actors include customers, janitors, security guards, and even former employees. Possible motives for an insider threat actor can include: - Becoming disgruntled with an employer - Being bribed by a competitor - Seeking personal financial gain Because insiders are one of the most dangerous and overlooked threats to an organization, you need to take the appropriate steps to protect against them. - Require mandatory vacations - Create and follow onboarding and off-boarding procedures - Employ the principal of least privilege - Have appropriate physical security controls in place - Require security awareness training which should be tailored for the role of the employee (role-based awareness training) - Data owner - System Administrator - System owner - User - Privileged user - Executive user Sometimes an employee can become an insider threat actor without them even knowing it. This is known as an unintentional insider threat actor. Proper security training can help protect against unintentional insider threat actors.
Script Kiddie	A script kiddie is an individual who carries out an attack by using scripts or programs written by more advanced hackers. Script kiddies typically lack the skills and sophistication of legitimate hackers. Script kiddies are usually motivated by the chance to impress their friends or garner attention in the hacking community. Because script kiddies lack knowledge and sophistication, their attacks often seek to exploit well-known vulnerabilities in systems. As such, defending against script kiddies involves keeping systems up-to-date and using standard security practices.

Hacktivist	A hacktivist is any individual whose attacks are politically motivated. Instead of seeking financial gain, hacktivists are looking to defame, shed light on, or cripple an organization or government. Often times, hacktivists work alone. Occasionally, they will create unified groups with like-minded hackers. For example, the website wikileaks.org is a repository of leaked government secrets, some of which have been obtain by hacktivists.
Organized Crime	An organized crime threat actor is a group of cybercriminals whose main goal is financial gain. Attacks carried out by organized crime groups can last several months and are very well-funded and extremely sophisticated. A common tactic used by organized crime is a targeted phishing campaign. Once access is gained, the group will either steal data and threaten to release it or use ransomware to hold data hostage. Due to the level of sophistication and amount of funding, attacks from organized crime groups are extremely hard to protect against. In a lot of cases, it's simply a matter of time until a data breach occurs or ransomware takes hold. Because of this, many companies that need immediate access to their data (such as hospitals and financial institutions) stockpile digital currency in case of an attack. Specific protections against organized crime threat actors include: ▪ Proper user security training ▪ Implementing email filtering systems ▪ Proper securing and storing of data backups In July 2017, an organized crime group hacked HBO's network and stole a purported 1.5 terabytes of data. The group then demanded HBO pay them a hefty ransom in bitcoins, or they would release the data to the public.
Nation State	A nation state is the most organized, well-funded, and dangerous type of threat actor. There are two primary motives for nation state attacks (also called state-sponsored attacks). ▪ **Obtaining information** – Some attacks seek to obtain sensitive information, such as government secrets. These attacks usually target organizations that have government contracts or the government systems themselves. Attacks motivated by information gathering are considered a type of APT, as the goal is to remain in the system undetected. ▪ **Crippling systems** – Some attacks seek to cripple their target's network or infrastructure. For example, an attack could target a city's power grid or water system. In 2010, a malicious computer worm called Stuxnet was discovered. The worm was designed to target industrial centrifuges used by the Iranian nuclear program. Stuxnet is thought to be a state-sponsored attack, as its code was so large and complex that it would have required huge amounts of funding and resources to create. Because nation states use so many different attack vectors and unknown exploits, defending against them involves building a comprehensive security approach that uses all aspects of threat prevention and protection.
Competitor	A competitor threat actor carries out attacks on behalf of an organization and targets competing companies. For example, a payment processing company could hire someone to carry out a DDoS attack on a competing payment processing company to force users to choose the attacker's product. The motive behind such attacks could be financial gain, competitor defamation, or even stealing industry secrets.

The term *hacker* is a catch-all term used to describe any individual who uses their technical knowledge to gain unauthorized access to an organization.

Common vulnerabilities exploited by threat actors:

Vulnerability	Impact
Improper Input Handling	Improper input handling may be the chief security vulnerability in today's software applications and web pages. It involves the improper validation, sanitization, and filtering, as well as encoding and decoding of input data. During application development, all inputs should be considered untrusted, especially external inputs that can be transferred in various formats.
Improper Error Handling	Improper handling of errors, especially by a website, can lead to other security problems. If an error message displays stack traces, database dumps, and error codes, an attacker can use this information to form a more customized offensive. Even error message that give limited details can reveal important clues to the inner workings of a website. For example, a message that says Access Denied lets an attacker know that a file exists, while a message that reads File Not Found does not.
Improperly Configured Accounts	Password length and complexity polices help prevent attackers from gaining unauthorized access. But there are other account configurations that can increase security. Attackers know the default domain, service, and device accounts, their default passwords, and the default privileges assigned to them. If these accounts are left enabled and unchanged, they can be an entry point for adversaries. Also, accounts should be configured with the least amount of permissions and privileges needed to perform their duties. It is better to give privileges later than to remove privileges after a security problem has occurred.
Vulnerable	Attacks on business processes have recently come into focus. Attackers target a business's unique processes and machines and

Business Processes	manipulate them for personal benefit. When they identify a weakness, they can alter a process to help them achieve their aims. For example, shipping companies working in the Belgian port of Antwerp were hacked by drug traffickers. They were able to modify the movement and location of containers, making it possible to move and retrieve illegal drugs.
Weak Cipher Suites and Implementations	To secure data that is transferred across external paths, TLS/SSL makes use of one or more cipher suites. Old and outdated cipher suites, especially those with documented vulnerabilities, can allow attackers access to secret data. Weak encryption keys are more likely to fail brute force attacks.
Improper Certificate and Key Management	Due to the proliferation and complexity of digital certificates used for identity and encryption, many organizations find it difficult to manage their certificates and cipher keys. Expiring certificates are a leading cause of system downtime. To better manage their certificates, organizations should track when certificates expire, their issuing CA, and their encryption key strengths.