LESSON NOTES

CYBERSECURITY

Domain 2 - General Security Concepts

2.1.1 - Threat Actors

Lesson Overview:

Students will:

- Analyze threat actors and their motivations.

Guiding Question: What are threat actors and their motivations?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

2.1 - Compare and contrast common threat actors and motivations

- 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

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Threat Actors

Threat actors are groups of people who pose a threat to the security of software, data, or an organization's well-being. These groups or individuals each carry their own unique threat level and are driven by a range of motivations. Each threat actor group is characterized based on their level of skill and potential ability to cause damage to a business, organization, or government.

Script Kiddies

Script kiddies or ***unskilled attackers*** are the least sophisticated group of threat actors. These individuals are usually novice computer professionals with little expertise or knowledge. They often only perform attacks on vulnerabilities if there are already ready-made tools that they can simply point to a target and run. These individuals execute attacks that require a lower level of skill and are interested in making a name for themselves, vandalizing sites, or causing chaos. The term "script kiddie" is usually a negative label used by more sophisticated hackers to belittle one another or dismiss someone as not being knowledgeable.

Hacktivists

Hacktivists are usually groups of medium skilled professionals who perform exploits and attacks for a cause. They believe in a particular ideology and work to use technology, specifically exploiting their perceived opponent's technologies such as websites, social media profiles, and networks to cause disruption to the spread their message. Hacktivists are driven by their political, commercial, or economic message and are not often guided by a desire for money. Their end goal is to spread their message to a wider audience to raise awareness for their cause.

Organized Crime

Organized criminals, or criminal syndicates, use exploits to continue their organized crime business. This includes selling data on the dark web, hacking into various devices and accounts to spy on rival organized gangs or even the police, interrupting business until ransoms are paid, stealing trade secrets to sell to a company's competitor. These groups are fueled by money and the desire to gain power to continue their influence. These groups are very similar to the Mafia and organized crime gangs but instead of using physical violence, they perform many of their attacks online.

Nation States and APT

Nation states (state actors), or ***advanced persistent threats*** (APT), are very advanced government or military organizations that carry out cyberattacks to perform intelligence activities, disrupt an enemy nation's military movements, and defend the rights of their nation's citizens. These groups often have the full support of their nation's government, so there is almost no limit to the sophistication or reach of their exploits. It is argued that the Stuxnet malware was carried out by a nation-state or a collaboration of nation-states because of its sophistication. Nicknames have been given to different nation-states to identify them when speaking about their threat actor groups.

Insider Threats

Insider threats are actors that work within an organization to expose business secrets and data. They usually carry out low-level attacks, such as copying secrets to a USB drive or carrying out sensitive material in a briefcase. These threats are also almost wholly responsible for logic bombs and wholesale data removal that can cripple the organization's business. These threats can be difficult to detect because the actors are aware of the organization's weak points, thus they can exploit them with a greater chance of escaping unnoticed. Making them especially dangerous is they know right where to attack to cause the most damage. They have time on their side allowing them to look for and learn the most about the organization before executing their attack. Many times, these individuals act out of vengeance or spite because of something that has occurred to them on the job that they feel was unfair, such as not getting a raise or a promotion.

Competition

Competitors are any business or organization that operates within the same domain as another business. For example, both Netflix and Hulu operate within the streaming video business, and both Facebook and Twitter operate within the social media domain. Competitors attempt to steal secrets to undermine the profits of their competitors and drive customers to their businesses. Sometimes the sophistication of these attacks can be very high, but it mainly depends on the type of information they are after as well as the domain of the business.

Hackers

The term hacker is thrown around a lot, but a lot of people do not realize that there are different types of "hackers." A ***hacker*** can be defined as anyone who uses technology and its tools to bypass a normal operation to gain access to some system that they are not supposed to have. Previously, the intent of hackers varies based on what authorization they have. Unauthorized hackers, formerly known as black hat hackers, are malicious users who intend to cause damage and harm to their targets. Their work is typically illegal, and they intend to make profits or personal gains. Authorized hackers, formerly known as white hat hackers, find vulnerabilities and exploits in a system with the intent to patch them. While they are typically motivated by money, these hackers do not break the law, rather they get permission to try to break into a system to patch the holes and get paid for their work. Somewhere in between are the semi-authorized hackers, formerly known as grey hat hackers. They usually are breaking the law, but they are not doing it for malicious purposes. They might be breaking into a system just for the fun of it or to mess with the company and pull a prank.

Shadow IT

Shadow IT are part of larger organizations that do not follow the IT department rules and attempt to work around them. If a certain department has noticed that there is a problem with the security, they might implement security features in their specific department to better secure themselves. The IT department might also have certain features locked down, the shadow IT might find a way around the security and utilize these features without the IT department's consent. These shadow ITs run the risk of getting in trouble with their IT departments and/or the companies which could result in a person getting fired from their job.

Attributes of Actors

Threat actors can come from one of two places. ***Internal*** threat actors are those trusted insiders that have permission to be in the organization's network or information systems. These are users who already have authorized access or privileged knowledge about the information and systems on the network. ***External*** threat actors come from outside the organization or network. They do not have authorized access to the information or systems and don't have any special privileges to, or knowledge of the network.

Resources and ***funding*** can determine how well a threat actor can support their attack on a network either monetarily or with the needed equipment and software. While funding can be extremely important to an attacker, one of the most important factors that can determine whether an attacker is successful is their capability. The ***capability*** of an individual attacker can vary based on the type of attacker or their training. The ***level of sophistication*** is an important factor in determining the risk of a threat actor. Highly sophisticated threat actors are more likely to be successful when launching their attacks. Less sophisticated attackers will be more prone to failure when attempting an attack.

Motivations

Data exfiltration entails stealing sensitive or valuable data for various purposes, such as selling information on the black market, conducting corporate espionage, or obtaining intellectual property. ***Espionage*** is the act of gathering intelligence or sensitive information for political, economic, or military advantages. State-sponsored actors may engage in espionage for geopolitical reasons. ***Service disruptions*** involve disrupting the normal operation of systems, networks, or services. This may be done for various reasons, including causing chaos, gaining a competitive advantage, or achieving a political objective. ***Blackmail*** is extorting individuals, organizations, or governments by threatening to disclose sensitive information, compromise systems, or conduct damaging actions unless specific demands are met. The motivation for ***financial gain*** is to make money through cybercrime, such as stealing financial information, conducting ransom attacks, or engaging in fraudulent activities like identity theft and online scams. ***Philosophical/political beliefs*** encourage hacktivist groups to engage in cyber-attacks to promote a cause, express dissent, or further their beliefs. ***Ethical*** hackers often work to improve security by identifying and fixing weaknesses. Seeking ***revenge*** against individuals, organizations, or entities perceived to have wronged the threat actor may involve damaging their reputation, causing financial harm, or disrupting operations. Hackers may create disorder or chaos for various reasons, such as challenging the status quo, expressing discontent, or destabilizing systems for political or ideological purposes. Engaging in cyber warfare can be part of a broader military strategy. State-sponsored actors may target infrastructure or communication systems of other nations during times of conflict.