Threat Actors

3.2.1

The Hacker

In the previous topic, you gained a high-level look at the current landscape of cybersecurity, including the types of threats and vulnerabilities that plague all network administrators and architects. In this topic, you will learn more details about particular types of threat actors.

Hacker is a common term used to describe a threat actor. Originally the term referred to someone who was a skilled computer expert such as a programmer and a hack was a clever solution. The term later evolved into what we know of it today.

As shown in the table, the terms white hat hacker, black hat hacker, and gray hat hacker are often used to describe a type of hacker.

Hacker Type	Description
White Hat Hackers	These are ethical hackers who use their programming skills for good, ethical, and legal purposes. White hat hackers may perform network penetration tests in an attempt to compromise networks and systems by using their knowledge of computer security systems to discover network vulnerabilities. Security vulnerabilities are reported to developers for them to fix before the vulnerabilities can be exploited.
Gray Hat Hackers	These are individuals who commit crimes and do arguably unethical things, but not for personal gain or to cause damage. Gray hat hackers may disclose a vulnerability to the affected organization after having compromised their network.
Black Hat Hackers	These are unethical criminals who compromise computer and network security for personal gain, or for malicious reasons, such as attacking networks.

Note: In this course, we will not use the term hacker outside of this module. We will use the term threat actor. The term threat actor includes hackers. But threat actor also includes any device, person, group, or nation state that is, intentionally or unintentionally, the source of an attack.

3.2.2

Evolution of Hackers

Hacking started in the 1960s with phone freaking, or phreaking, which refers to using audio frequencies to manipulate phone systems. At that time, telephone switches used various tones to indicate different functions. Early hackers realized that by mimicking a tone using a whistle, they could exploit the phone switches to make free long-distance calls.

In the mid-1980s, computer dial-up modems were used to connect computers to networks. Hackers wrote "war dialing" programs which dialed each telephone number in a given area in search of computers. When a computer was found, password-cracking programs were used to gain access.

The table displays modern hacking terms and a brief description of each.

Hacking Term	Description
Script Kiddies	These are teenagers or inexperienced hackers running existing scripts, tools, and exploits, to cause harm, but typically not for profit.
Vulnerability Broker	These are usually gray hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
Hacktivists	These are gray hat hackers who publicly protest organizations or governments by posting articles, videos, leaking sensitive information, and performing network attacks.
Cyber criminals	These are black hat hackers who are either self-employed or working for large cybercrime organizations.
State-Sponsored	These are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

3.2.3

Cyber Criminals

It is estimated that cyber criminals steal billions of dollars from consumers and businesses. Cyber criminals operate in an underground economy where they buy, sell, and trade attack toolkits, zero day exploit code, botnet services, banking Trojans, keyloggers, and much more. They also buy and sell the private information and intellectual property they steal. Cyber criminals target small businesses and consumers, as well as large enterprises and entire industries.

3.2.4

Hacktivists

Two examples of hacktivist groups are Anonymous and the Syrian Electronic Army. Although most hacktivist groups are not well organized, they can cause significant problems for governments and businesses. Hacktivists tend to rely on fairly basic, freely available tools.

3.2.5

State-Sponsored Hackers

State-sponsored hackers create advanced, customized attack code, often using previously undiscovered software vulnerabilities called zero-day vulnerabilities. An example of a state-sponsored attack involves the Stuxnet malware that was created to damage Iran's nuclear enrichment capabilities.

3.2.6

Check Your Understanding - Threat Actors

ⓘ Check your understanding of threat actors by choosing the BEST type of threat actor for each description.

1. Which type of hacker is described in the scenario: After hacking into ATM machines remotely using a laptop, I worked with ATM manufacturers to resolve the security vulnerabilities that I discovered.

   ○ White Hat
   ● Gray Hat
   ○ Black Hat

2. Which type of hacker is described in the scenario: From my laptop, I transferred $10 million to my bank account using victim account numbers and PINs after viewing recordings of victims entering the numbers.

   ○ White Hat
   ○ Gray Hat
   ● Black Hat

3. Which type of hacker is described in the scenario: My job is to identify weaknesses in my company's network .

   ● White Hat
   ○ Gray Hat
   ○ Black Hat

4. Which type of hacker is described in the scenario: I used malware to compromise several corporate systems to steal credit card information. I then sold that information to the highest bidder.

   ○ White Hat
   ○ Gray Hat
   ● Black Hat

5. Which type of hacker is described in the scenario: During my research for security exploits, I stumbled across a security vulnerability on a corporate network that I am authorized to access.

   ● White Hat
   ○ Gray Hat
   ○ Black Hat

6. Which type of hacker is described in the scenario It is my job to work with technology companies to fix a flaw with DNS.

   ● White Hat
   ○ Gray Hat
   ○ Black Hat

Check

Show Me

Reset

3.1 Current State of Cybersecurity

3.3 Threat Actor Tools