Wrap-up; Terms and definitions from Course 5, Week 3

Here we are at the end of this section! Can you believe it?
I had so much fun exploring the world of vulnerabilities.
I hope you felt the same.
More importantly, I hope you got a better sense of how complex a landscape the digital world is.
This environment is filled with gaps that attackers can use to gain unauthorized access to assets, making it a challenge to defend.
We've explored a lot of information this time around, so let's quickly recap what we've covered.
You learned about the vulnerability management process, starting with the defense-in-depth model.
You learned about the layers of this security framework and how each of them work together to build a stronger defense.
You then learned about the CVE list that's used to find cataloged vulnerabilities.
This is a great addition to your growing security toolbox.
After that, you learned of the attack surfaces that businesses protect.
We discussed physical and digital surfaces and the challenges of defending the cloud.
We finished up by exploring common attack vectors, where you learned how security teams use an attacker mindset to identify the security gaps that cyber criminals try to exploit.
Every one of the vulnerabilities that we've discussed so far is faced with a number of threats.
When we get back together, we're going to expand our attacker mindset even further by exploring specific type of attacks that cybercriminals commonly use.
We'll look at things like malware and the techniques attackers use to compromise defense systems.
By exploring how these tools and tactics work, you'll gain a clearer understanding of the threats they pose.
We'll then wrap up by investigating how security teams stop these threats from damaging our organizations' operations, their reputation, and most importantly, their customers and employees.
You've done a fantastic job getting to this point.
When you're ready, let's finish the journey together.
I'm looking forward to being back with you again.

Glossary terms from week 3

Advanced persistent threat (APT): An instance when a threat actor maintains unauthorized access to a system for an extended period of time

Attack surface: All the potential vulnerabilities that a threat actor could exploit

Attack tree: A diagram that maps threats to assets

Attack vector: The pathways attackers use to penetrate security defenses

Bug bounty: Programs that encourage freelance hackers to find and report vulnerabilities

Common Vulnerabilities and Exposures (CVE®) list: An openly accessible dictionary of known vulnerabilities and exposures

Common Vulnerability Scoring System (CVSS): A measurement system that scores the severity of a vulnerability

CVE Numbering Authority (CNA): An organization that volunteers to analyze and distribute information on eligible CVEs

Defense in depth: A layered approach to vulnerability management that reduces risk

Exploit: A way of taking advantage of a vulnerability

Exposure: A mistake that can be exploited by a threat

Hacker: Any person who uses computers to gain access to computer systems, networks, or data

MITRE: A collection of non-profit research and development centers

Security hardening: The process of strengthening a system to reduce its vulnerability and attack surface

Threat actor: Any person or group who presents a security risk

Vulnerability: A weakness that can be exploited by a threat

Vulnerability assessment: The internal review process of a company’s security systems

Vulnerability management: The process of finding and patching vulnerabilities

Vulnerability scanner: Software that automatically compares existing common vulnerabilities and exposures against the technologies on the network

Zero-day: An exploit that was previously unknown

Revision #2
Created 26 August 2023 08:51:25 by naruzkurai
Updated 26 August 2023 08:53:44 by naruzkurai