Introduction to security hardening

I want to take a moment to congratulate you on your progress so far.
First, you learned about network operations.
Then, you learned about the tools and
protocols that help network systems function.
Next, you learned how vulnerabilities in
networks expose them to various security intrusions.

Now, we'll discuss security hardening.
Then, we'll learn about OS hardening, explore network hardening practices, and discuss cloud hardening practices.
Security hardening can be implemented in devices, networks,
applications, and cloud infrastructure.
Security analysts may perform tasks, such as patch updates and
backups, as part of security hardening.

We'll discuss these tasks as you progress through the course.
As a security analyst, hardening will play a major role in your day-to-day tasks,
which is why it's important for you to understand how it works.
I'm excited to accompany you on this journey.

Security hardening

Security analysts and the organizations they work with have to be
proactive about protecting systems from attack.
This is where security hardening comes in.
Security hardening is the process of strengthening a system to reduce its vulnerability and attack surface.
All the potential vulnerabilities that a threat actor could exploit
are referred to as a system's attack surface.

Let's use an example that compares a network to a house.
The attack surface would be all the doors and
windows that a robber could use to gain access to that house.
Just like putting locks on all the doors and windows in the house,
security hardening involves minimizing the attack surface or
potential vulnerabilities and keeping a network as secure as possible.

As part of security hardening, security analysts perform regular maintenance procedures to keep network devices and systems functioning securely and optimally.
Security hardening can be conducted on any device or system that can be compromised, such as hardware, operating systems, applications, computer networks, and databases.
Physical security is also a part of security hardening.
This may include securing a physical space with security cameras and security guards.

Some common types of hardening procedures include software updates, also called patches, and device application configuration changes.
These updates and changes are done to increase security and fix security vulnerabilities on a network.
An example of a security configuration change would be requiring longer passwords or more frequent password changes.
This makes it harder for a malicious actor to gain login credentials.
An example of a configuration check is updating the encryption standards for data that is stored in a database.
Keeping encryption up to date makes it harder for malicious actors to access the database.

Other examples of security hardening include removing or disabling unused applications and services, disabling unused ports, and reducing access permissions across devices and network.
Minimizing the number of applications, devices, ports, and access permissions makes network and device monitoring more efficient and reduces the overall attack surface, which is one of the best ways to secure an organization.

Another important strategy for security hardening is to conduct regular penetration testing.
A penetration test, also called a pen test, is a simulated attack that helps identify vulnerabilities in a system, network, website, application, and process.
Penetration testers document their findings in a report.
Depending on where the test fails, security teams can determine the type of security vulnerabilities that require fixing.
Organizations can then review these vulnerabilities and come up with a plan to fix them.

Coming up, you'll learn more about how security hardening is an essential aspect of securing networks.
It's a foundational part of network security that strengthens the network in order to reduce the number of successful attacks.

Revision #2
Created 2023-07-03 07:21:45 UTC by naruzkurai
Updated 2023-07-03 10:29:21 UTC by naruzkurai