Network hardening practices

Earlier, you learned that OS hardening focuses on device safety and uses patch updates, secure configuration, and account access policies.
Now we'll focus on network hardening.
Network hardening focuses on network-related security hardening, like port filtering, network access privileges, and encryption over networks.
Certain network hardening tasks are performed regularly, while others are performed once and then updated as needed.

Some tasks that are regularly performed are firewall rules maintenance, network log analysis, patch updates, and server backups.
Earlier, you learned that a log is a record of events that occurs within an organization's systems.
Network log analysis is the process of examining network logs to identify events of interest.
Security teams use a log analyzer tool or a security information and event management tool, also known as a SIEM, to conduct network log analysis.
A SIEM tool is an application that collects and analyzes log data to monitor critical activities in an organization.
It gathers security data from a network and presents that data on a single dashboard.
The dashboard interface is sometimes called a single pane of glass.
A SIEM helps analysts to inspect, analyze, and react to security events across the network based on their priority.
Reports from the SIEM provide a list of new or ongoing network vulnerabilities and list them on a scale of priority from high to low, where high priority vulnerabilities have a much shorter deadline for mitigation.

Now that we've covered tasks that are performed regularly, let's examine tasks that are performed once.
These tasks include port filtering on firewalls, network access privileges, and encryption for communication, among many things.
Let's start with port filtering.
Port filtering can be formed over the network.
Port filtering is a firewall function that blocks or allows certain port numbers to limit unwanted communication.
A basic principle is that the only ports that are needed are the ones that are allowed.
Any port that isn't being used by the normal network operations should be disallowed.
This protects against port vulnerabilities.
Networks should be set up with the most up-to-date wireless protocols available and older wireless protocols should be disabled.
Security analysts also use network segmentation to create isolated subnets for different departments in an organization.
For example, they might make one for the marketing department and one for the finance department.

This is done so the issues in each subnet don't spread across the whole company and only specified users are given access to the part of the network that they require for their role.
Network segmentation may also be used to separate different security zones.
Any restricted zone on a network containing highly classified or confidential data should be separate from the rest of the network.
Lastly, all network communication should be
encrypted using the latest encryption standards.
Encryption standards are rules or methods used to conceal outgoing data and uncover or decrypt incoming data.
Data in restricted zones should have much higher encryption standards, which makes them more difficult to access.
You've learned about the most common hardening practices.
This knowledge will be useful as you complete the certificate program and it's essential to your career as a security analyst.

Revision #2
Created 2023-07-03 09:00:43 UTC by naruzkurai
Updated 2023-07-03 11:20:25 UTC by naruzkurai