OS hardening practices

Hi there. In this video,
we'll discuss operating system, or OS, hardening and why it's
essential to keep the entire network secure.
The operating system is the interface between computer hardware and the user.
The OS is the first program loaded when a computer turns on.
The OS acts as an intermediary between software applications and the computer hardware.
It's important to secure the OS in each system because one insecure OS can
lead to a whole network being compromised.
There are many types of operating systems, and they all share similar security hardening practices.
Let's talk about some of those security hardening practices that are recommended to secure an OS.

Some OS hardening tasks are performed at regular intervals, like updates, backups, and keeping an up-to-date list of devices and authorized users.
Other tasks are performed only once as part of preliminary safety measures.
One example would be configuring a device setting to fit a secure encryption standard.
Let's begin with OS hardening tasks
that are performed at a regular interval, such as patch installation, also known as patch updates.

A patch update is a software and operating system, or OS, update that addresses security vulnerabilities within a program or product.
Now we'll discuss patch updates provided to the company by the OS software vendor.
With patch updates, the OS should be upgraded to its latest software version.
Sometimes patches are released to fix a security vulnerability in the software.
As soon as OS vendors publish a patch and the vulnerability fix, malicious actors know exactly where the vulnerability is in systems
running the out-of-date OS.
This is why it's important for organizations to run patch updates as soon as they are released.
For example, my team had to perform an emergency patch to address a recent vulnerability found in a commonly used programming library.
The library is used almost everywhere, so we had to quickly patch most of our servers and applications to fix the vulnerability.
The newly updated OS should be added to the baseline configuration, also called the baseline image.
A baseline configuration is a documented set of specifications within a system that is used as a basis for future builds,
releases, and updates.
For example, a baseline may contain a firewall rule with a list of allowed and disallowed network ports. If a security team suspects
unusual activity affecting the OS, they can compare the current configuration to the baseline and make sure that nothing has been changed.

Another hardening task performed regularly is hardware and software disposal.
This ensures that all old hardware is properly wiped and disposed of.
It's also a good idea to delete any unused software applications since some popular programming languages
have known vulnerabilities.
Removing unused software makes sure that there aren't any unnecessary vulnerabilities connected with the programs that the software uses.

The final OS hardening technique that we'll discuss is implementing a strong password policy.
Strong password policies require that passwords follow specific rules.
For example, an organization may set a password policy that requires a minimum of eight characters,
a capital letter, a number, and a symbol.
To discourage malicious actors, a password policy usually states that a user will lose access to the network after entering the wrong password a certain number of times in a row.
Some systems also require multi-factor authentication, or MFA.
MFA is a security measure which requires a user to verify their identity in two or more ways to access a system or network.
Ways of identifying yourself include something you know, like a password, something you have like an ID card, or something unique about you, like your fingerprint.

To review, OS hardening is a set of procedures that maintains OS security and improves it.
Security measures like access privileges and password policies frequently undergo regular security checks as part of OS hardening.
Coming up, we'll discuss network hardening practices.

Revision #2
Created 2023-07-03 07:25:11 UTC by naruzkurai
Updated 2023-07-03 10:48:50 UTC by naruzkurai