

Module 4

What you'll learn

- Security hardening
- OS hardening
- Network hardening practices
- Cloud network hardening

Where security hardening occurs

- Devices
- Network
- Application
- Cloud infrastructure

Security analyst Responsibility

- Patch updates
- Backups

Security hardening

The process of strengthening a system to reduce its ~~st~~ vulnerability and attack surface

Attack Surface : All potential ~~st~~ vulnerability that a threat actor could exploit

Penetration Test : A simulated attack that helps identify vulnerability in system, network, website, applications and processes

OS hardening

OS hardening practice

Operating System (OS)

The interface between computer hardware and the user

Patch update

A software and operating system update that addresses security vulnerability within a program or product

Baseline configuration (baseline image)

A documented set of specification within a system that is used as a basis for future builds, releases and updates

Multi-factor authentication (MFA)

A security measure which requires a user to verify their identity in two or more ways to access a system or network

Categories of multifactor

- something you know
- something you have
- something unique about you

Network Hardening Practice

Network Security Hardening

- Port filtering
- Network access privilege
- Encryption

Task performed

- Firewall rules maintenance
- Network log analysis
- Patch updates
- Server backups

Network log analysis

The process of examining network logs to identify events of interest

Security Information and Event Management (SIEM)

An application that collects and analyzes log data to monitor critical activities in an organization

Port filtering

A firewall function that blocks or allows certain port numbers to limit unwanted communication

Cloud network

A collection of servers or computer that store resource and data in remote data center that can be accessed via the internet

DATE / /
PAGE

Raj