

Nmap, network scanning

Learn how to use Nmap for network scanning and reconnaissance.

Category: Cyber Security · Duration: 1 day

WHO IT IS FOR

- Security engineers and system administrators
- Teams that want hands-on practice on real scenarios

In this course, you will gain a comprehensive understanding of Nmap and its techniques for network scanning. You will learn how to use Nmap to discover hosts, gather information about target systems, detect open ports and services, perform vulnerability scanning, and much more. Through hands-on exercises and real-world scenarios, you will develop the skills needed to conduct effective network reconnaissance and enhance the security of your infrastructure.

Prerequisites

Basic understanding of networking concepts.

Syllabus

- Introduction to network scanning
- Overview of Nmap and its features
- Host discovery and port scanning techniques
- Service and version detection
- Operating system detection
- Firewall evasion and techniques
- Scripting and automation with Nmap
- Advanced scanning techniques
- Vulnerability scanning and reporting
- Network mapping and reconnaissance
- Wireless network scanning
- Post-scanning analysis and reporting
- Securing network infrastructure using Nmap
- Case studies and real-world examples
- Nmap best practices

- Lab exercises and hands-on practice
- Q&A and group discussions
- Final assessment and certification preparation