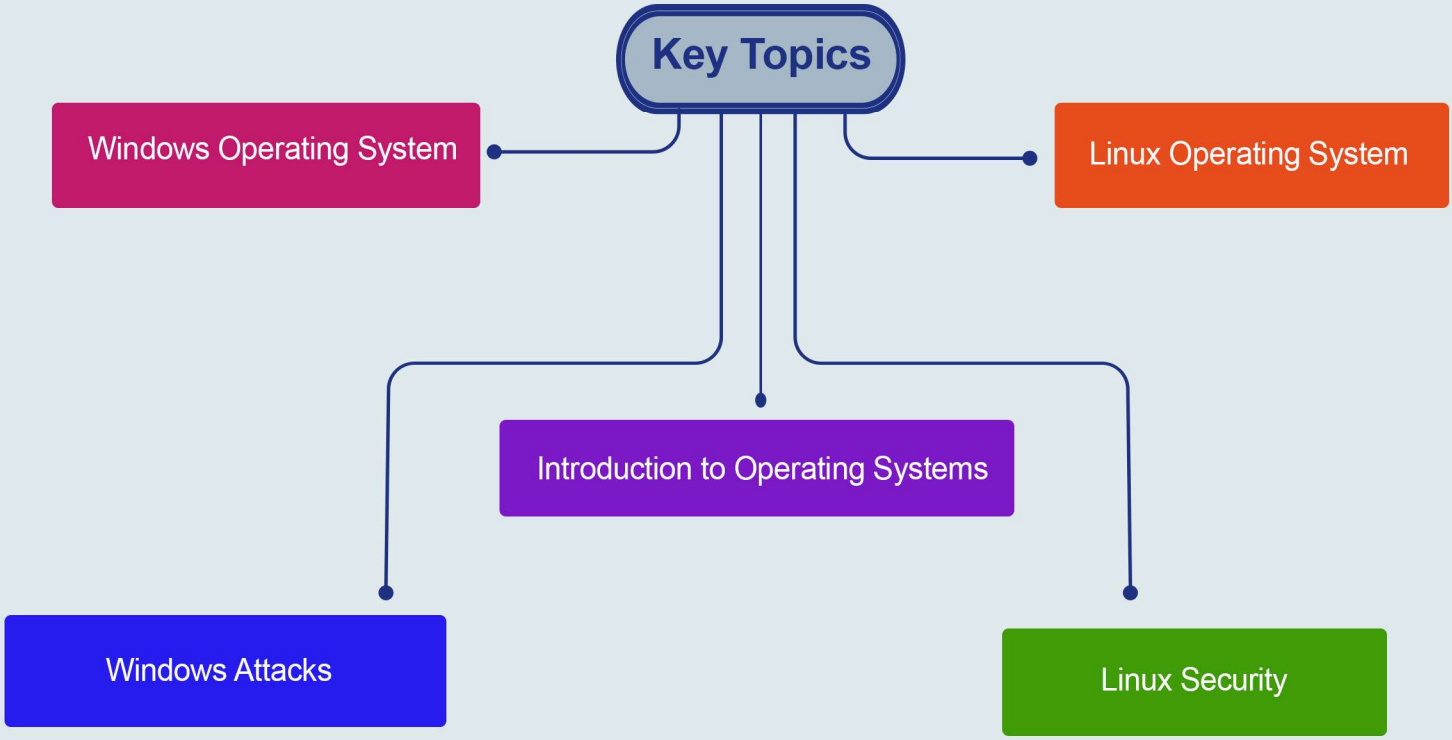
About the Course

Operating System (OS) is a program that works as a bridge between the computer hardware and the software. It manages the computer resources and allocates the resources to the software to run efficiently. In other word, the operating system is the physical environment where your application runs. Therefore, any vulnerability in the operating system could compromise the security of the application. OS security refers to specified steps or measures used to protect the OS from threats, viruses, worms, malware or remote hacker intrusions. OS security encompasses all preventive-control techniques, which safeguard any computer assets capable of being stolen, edited or deleted if OS security is compromised. In this course you learn how to secure OS.

Learning Objectives

Key Topics



Pre Requisites

A powerful knowledge about operating systems also taking the following course:

- Information Security Concepts & Principles Course
- Network Security Course

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files
- Operating Systems Security eBook

Who Should Attend

- Network Administrator
- Security Engineers
- CTOs
- System Administrators
- System Engineers
- Network Administrators
- Security Engineers
- System Administrators
- IT Managers
- Information Security Professionals
- Penetration Testers

Syllabus

Introduction to Operating Systems

- What is an Operating System
- 32-bit vs 64-bit Operating Systems

Windows Operating System

- Network Operating Systems
- Windows Server Architecture
- Windows in The Enterprise
- Windows Networking Options
- Using The MMC
- Domain Management
- User Profiles, Logon Scripts, and Variables Management
- Files and Folders Management
- Registry Management
- Protocol Management
- Service Management
- Drives and File Systems
- Active Directory Domain Services
- Group Policy
- Shares

Windows Attacks

- Overview of Windows Security
- Gathering System Information
- Password Attacks
- Active Directory – Escalation of Privilege
- Exchange Server – Mail Service Attacks
- Office – Macros and ActiveX
- Kernel Attacks

Syllabus

- Domain Controller Security
- Memory Attack

Windows Hardening

- Basic Security
- User Accounts
- Security Policies
- System Patches
- Operating System Minimization
- Logging and Monitoring
- System Integrity
- Access Control
- Protecting Local Data
- Securing Data in Transit
- File Security
- Securing the Registry
- Network Security
- Service Security

Linux Architecture

- Linux Directories
- Linux Users
- Linux Files
- Linux Process

Linux Security Concepts

- Check Local User Accounts and Group Accounts
- Check password security
- Startup files in /etc/rc.d
- Network services

Syllabus

- Critical network files
- NFS Security
- User security policy
- Securing root
- Password and Account Policy
- /etc/shadow and /etc/password files
- Cracking user passwords
- Group membership
- The wheel group
- User quotas
- List of File Systems
- Using lsof
- Determine disk usage
- UNIX file permission
- SUID and SGID files
- Umask
- Permissions on critical files and folders File integrity mechanisms

Linux/Unix Systems Attacks

- Memory Attacks and Overflows
- Stack and Heap Overflows
- Format String Attacks

Hardening Linux/Unix Systems

- Stack Protection
- Vulnerability Minimization
- Minimization vs. Patching
- OS Minimization
- Patching Strategies
- Boot-Time Configuration
- Reducing Services

Syllabus

- o systemd vs init
- o Email Configuration
- o Legacy Services
- o Encrypted Access
- o Session Hijacking Exploits
- o The Argument For Encryption
- o SSH Configuration
- o Host-Based Firewalls
- o IP Tables and Other Alternatives
- o Simple Single-Host Firewalls
- o Managing and Automating Rule Updates
- o Rootkits and Malicious Software
- o Backdoors and Rootkits
- o Kernel Rootkits
- o chkrootkit and rkhunter
- o File Integrity Assessment
- o Overview of AIDE
- o Basic Configuration
- o Typical Usage
- o Physical Attacks and Defenses
- o Known Attacks
- o Single User Mode Security
- o Boot Loader Passwords
- o User Access Controls
- o Password Threats and Defenses
- o User Access Controls
- o Environment Settings
- o Root Access Control With Sudo
- o Features and Common Uses
- o Configuration
- o Known Issues and Work-Arounds

Syllabus

- Warning Banners
- Suggested Content
- Implementation Issues
- Kernel Tuning For Security
- Network Tuning
- System Resource Limits
- Restricting Core Files
- Automating Tasks With SSH
- Public Key Authentication
- ssh-agent and Agent Forwarding
- AIDE Via SSH
- Conceptual Overview
- SSH Configuration
- Tools and Scripts
- Linux/Unix Logging Overview
- Syslog Configuration
- System Accounting
- Process Accounting
- Kernel-Level Auditing
- SSH Tunneling
- X11 Forwarding
- TCP Forwarding
- Reverse Tunneling Issues
- Centralized Logging With Syslog-NG
- Why You Care
- Basic Configuration
- Hints and Hacks for Tunneling Log Data
- Log Analysis Tools and Strategies

Hands-on Training

- Lab 1: Windows Server Secure Configuration
- Lab 2: Password Attack
- Lab 3: Domain Controller Attack
- Lab 4: Registry Security