Security Leaders 5.5 hours of content | Exam

1. Windows Fundamentals & Security

- Introduction to Windows and Enterprise Services
  - Active Directory
  - DHCP
  - File Server and Storage Services
  - WSUS (Windows Server Update Services)
- Workgroup vs Domain
  - User types in Windows
- Windows Security Architecture
  - LSA, SRM, SAM
- Deep Dive into Active Directory
  - BitLocker and Full Disk Encryption
- PowerShell and CMD
  - System Management & Automation
  - Use in Defense and Offense
- Access Control Lists (ACL)
  - ACE, DACL, Permissions and Practical Use
- Exam: Windows

2. Linux Fundamentals

- History of Linux and Linus Torvalds
- Security Differences Between Linux and Windows
- Linux File System Hierarchy (FSH)
  - Basic Structure
  - Directory Hierarchy
  - Permissions and Roles
- Basic Linux Commands (Demo)
- Exam: Linux

3. Linux Fundamentals

- Introduction to Networking
  - Basic Networking Concepts
  - Peer-to-Peer vs Client-Server
- Protocols and Models
  - OSI Model: Application, Presentation, Session, Transport, Network, Data Link, Physical
  - TCP/IP Model
  - TCP vs UDP
- Key Protocols:
  - ARP
  - ICMP
- Networking Devices:
  - Hub, Switch, Router
- Ports and Sockets
- Exam: Network Fundamentals

4. Information Security Essentials

- Introduction to Information Security
  - Threats to Individuals and Organizations
- Theoretical Models:
  - CIA Triad
  - IAAA Model
- Information Types and Information Systems
- Importance of Methodological Security Work
- Case Study
- Attacker Profile: Types of Hackers
- Exam: Information Security

5. Attack Techniques

- Malware Overview
  - Types of Common Malware
- Penetration Techniques
  - External and Internal
- Denial-of-Service (DoS) Attacks
- Data Protection and Maintenance in Organizations
- Exam: Attack Techniques

6. Network Security & Defensive Technologies

- Principles of Secure Architecture
- Cryptography Basics
- Defensive Systems:
  - WAF, IDS, IPS
  - VPN, Endpoint Security, DLP
- Extended Discussion on DLP
- Email Protection with DMARC
- Security Monitoring and Automation Systems:
  - SIEM
  - SOAR
- Exam: Network Security

7. Offensive Cybersecurity

- Understanding Security Vulnerabilities
- Introduction to Kali Linux
- Wi-Fi Network Attacks
- Brute Force Attacks
- Infrastructure Attacks
- Privilege Escalation Techniques
- Exam: Offensive Cyber Security

8. Course Summary

- Final Exam: Windows
- Recap and Key Takeaways