



Threat Guardians Private Limited

Modules:

- Network Security
- Security Threats and Trends
- Application Security
- OS Security
- Cryptography

Perquisites:

- Basics of Computer Networks
- Operating System (Linux / Windows)
- Bash script and Python

Module 1: Network Security

- Introduction
 - Introduction to Networking
 - Fundamental of Network Security
 - Features of Network Security
- Threat, Vulnerabilities, and attacks
 - Network Security Threats
 - Network Security Vulnerability and attacks
- Network Security Management
 - Data Privacy
- Network Management
 - Security Monitoring and Control
 - Security Best Practices

Module 2: Security Threats and Trends

- Malware and their types
- Botnet/ Trojan / Rootkit
- Cyber Warfare
 - Introductions to APT and Information Warfare
- Social Engineering
 - Introduction to Social Engineering
 - Countermeasure to address Social Engineering
- IoT Security

Module 3: Cryptography

- Introduction to Cryptography
 - Cryptography Fundamentals
 - Classical Encryption Techniques

- Types of Algorithms
 - Cryptographic Encryption Algorithms
 - Cryptographic Data Integrity Algorithm
- Key Management
 - Entity Authentication and Key Management
 - Key Distribution
- Application of Cryptography
 - Authentication Services
 - Infrastructural requirement for Security

Module 4: Application Security

- Introduction
 - Application Security Introduction
 - Application Security Goals
 - WebGoat /DVWA Demo
- Introduction to OWASP
 - OWASP top 10
 - Threat actor and more definitions (different attackers that threaten software and systems)
 - Défense in depth
 - Proxy tools
 - API Security
- Defences and Tools
- Session Management
- Security Scanning and Testing

Module 5: OS Security

- OS protection Fundamentals
- Understanding User accounts (Linux and Windows)
- File and Directory Permissions
 - Importance of File and Directory Permissions
 - Basic NT File System Permissions (Demo)
 - Understanding Linux Permissions
- File and Disk Encryption
 - Windows Encrypted File System (Demo)
 - Tools for encryption (*BitLocker / VeraCrypt etc.)
- Data Storage and Backups
 - Importance of Data Storage and Backups
 - Understanding of RAID (redundant array of independent disks)
 - Demo: Exploring Windows Backup
 - Demo: Linux Backup
 - Local vs. Cloud Storage and Backups
- Host Based Firewall
 - Introductions
 - Demo: Windows/Linux Firewall
 - 3rd Party Firewall

- Antivirus
 - Introduction to Antivirus
 - Demo: Windows Defender Antivirus
- Application and Execution Control
 - Fundamental of User Account Control (UAC)
 - Windows UAC
 - Demo: UAC setting in Windows
 - Demo: Windows App and Browser Control
 - Demo: Controlled Folder Access
- Update and Patching
 - Relevance of Patching
 - Demo: Windows and Linux updates
 - Why Software updates is important?
- OS Hardening
 - Securing the Boot Process
 - Demo: Checking Secure Boot Status in Windows
 - Demo: Disabling Unnecessary Services and Processes