

1. Introduction to Cyber Security

- What is Cyber Security?
- Why Cyber Security Matters
- CIA Triad (Confidentiality, Integrity & Availability)
- Types of Cyber Threats
- Malware, Ransomware & Phishing
- DDoS & Zero-Day Attacks
- Cyber Attack Lifecycle (Cyber Kill Chain)
- Security Controls (Preventive, Detective & Corrective)
- Authentication, Authorization & Accounting (AAA)
- Zero Trust Security Model
- Cyber Security Domains
- Security Operations Center (SOC) Overview
- Common Cyber Security Roles and Responsibilities
- Career Paths in Cyber Security
- Ethics & Legal Compliance (IT Act – India)
- Introduction to Cyber Security Tools

2. Networking Fundamentals for Security

- Network Basics and Terminology
- OSI & TCP/IP Models
- IP Addressing (IPv4 & IPv6)
- Subnetting Fundamentals
- MAC Address and ARP
- TCP vs UDP
- TCP Three-Way Handshake
- Common Network Ports
- Network Protocols (HTTP, HTTPS, FTP, SSH, DNS, DHCP, SMTP, POP3, IMAP)
- Routing and Switching Basics
- VLAN Fundamentals
- NAT (Network Address Translation)
- Network Devices (Router, Switch, Firewall, IDS/IPS)
- Packet Flow in a Network
- Introduction to Network Traffic Analysis using Wireshark
- Introduction to Network Attacks

3. Operating Systems & Security - Linux

- Introduction to Linux & Kali Linux
- Linux Installation and Virtual Machine Setup
- Linux File System Structure
- Linux Command Line Fundamentals
- File and Directory Management
- User & Group Management
- File & Directory Permissions
- Sudo and Privilege Escalation Concepts
- Package Management (apt, dpkg)
- Process & Service Management
- Network Configuration and Troubleshooting
- File Searching and Text Processing (find, grep, cat, less, head, tail)
- Compression and Archiving (tar, gzip, zip)
- SSH Basics and Secure Remote Access
- Bash Scripting Fundamentals
- Linux Security Best Practices

4. Windows Security

- Active Directory Basics
- Group Policy
- Windows Security Features
- Windows Defender & Firewall
- User Account Control (UAC)

5. Introduction to Ethical Hacking

- What is Ethical Hacking?
- Types of Hackers (White Hat, Black Hat & Grey Hat)
- Ethical Hacking Methodology
- Phases of Ethical Hacking
- Penetration Testing vs Ethical Hacking
- Vulnerability Assessment vs Penetration Testing (VAPT)
- Rules of Engagement and Scope
- Legal & Ethical Guidelines
- Responsible Disclosure
- Common Ethical Hacking Tools Overview

6. Reconnaissance & Information Gathering

- Active vs Passive Reconnaissance
- Domain & Network Footprinting
- Web Technology Fingerprinting
- OSINT Email & Username Enumeration
- Google Dorking
- WHOIS
- DNS Enumeration
- Subdomain Enumeration
- Automation in Information Gathering
- Security Tool Installation & Usage

7. Scanning Phase in Ethical Hacking

- TCP & UDP Essentials
- Installing vulnerable machine
- Network Discover Tool
- Nmap Scan Methods
- Host Discovery Techniques
- Port,Service & Version Detection
- Scanning Beyond IDS and Firewall
- Understanding Decoys and Packet Fragmentation
- Nmap Security Evasion Options
- Stealth & Obfuscation Techniques

8. Vulnerability Assessment

- Vulnerability Detection with Nmap NSE
- Manual Vulnerability Assessment
- Nessus Installation & Configuration
- Automated Vulnerability Detection

9. Exploitation & Gaining Access

- Metasploit Framework
- Reverse & Bind Shells
- FTP, Samba & Telnet Exploitation
- SSH Brute Force Testing
- Windows Exploitation Labs
- Exploit Search using Searchsploit
- Payload Concepts
- Meterpreter Payloads

10. Post Exploitation

- Meterpreter Fundamentals
- Privilege Escalation
- Persistence Techniques
- Post Exploitation Modules

11. Man-in-the-Middle Attacks

- ARP Spoofing
- Ettercap Password Sniffing
- ARP Cache Poisoning

12. Wireless Network Security

- Wireless Adapter Configuration and Monitor Mode
- Wireless Network Discovery and Packet Capture
- Wireless Traffic Analysis and Handshake Capture
- Handshake Processing and Password Audit Preparation
- Password Auditing with Hashcat and Aircrack-ng
- Custom Wordlist Generation with Crunch
- Wireless Security Best Practices and Practical Labs

13. Security Operations Center (SOC) & SIEM with Splunk

- Introduction to Security Operations Center (SOC)
- What is SIEM?
- Introduction to Wazuh (Open-Source SIEM & XDR)
- Wazuh Architecture and Components
- Wazuh Installation and Agent Configuration
- Splunk Architecture and Components
- Splunk Installation and Configuration
- Indexes, Sources, and Sourcetypes
- Data Ingestion and Log Management
- Search Processing Language (SPL) Fundamentals
- Creating Reports and Dashboards
- Alerts and Scheduled Searches
- Windows Event Log Analysis
- Linux Log Monitoring
- Firewall and Network Device Log Analysis
- File Integrity Monitoring (FIM) with Wazuh
- Vulnerability Detection with Wazuh
- Detecting Brute Force and Suspicious Login Attempts

- Basic Threat Hunting using Splunk and Wazuh
- SOC Investigation Workflow
- Hands-on Splunk and Wazuh Practical Labs

14. Android Security & Exploitation

- Android Security Concepts
- Android Meterpreter
- Malicious Payload Creation
- Identifying Malicious Applications

15. Security Reporting & Career Preparation

- Vulnerability Report Writing
- Executive & Technical Reports
- Risk Rating (CVSS Basics)
- Remediation Recommendations
- Resume Building
- LinkedIn Profile Optimization
- Interview Preparation
- Mock Interviews
- Capture The Flag (CTF) Practice
- Placement Assistance

Tools Covered

- Wireshark
- TCPdump
- Cisco Packet Tracer
- VirtualBox
- VMware
- Kali Linux
- Nmap
- Whois
- Google Dorks
- theHarvester
- Hunter.io
- Nessus
- Metasploit
- Burp Suite

- OWASP Juice Shop
- DVWA
- Aircrack-ng
- Hashcat
- Crunch
- Ettercap
- Splunk Enterprise
- Wazuh
- Sysmon

Course Objectives

- Understand Cyber Security & Ethical Hacking concepts
- Perform Penetration Testing & Vulnerability Assessments
- Identify and mitigate cyber threats
- Use industry-standard security tools
- Prepare for certifications such as CEH & CompTIA Security+

Prerequisites

Basic understanding of computers, networking, Windows, and Linux systems.

About SNIT

SNIT is a professional training institute dedicated to helping students build successful careers through Cyber Security, Cloud Computing, Networking, Digital Marketing, and Software Training programs. We provide certification-oriented training programs in partnership with leading technologies such as Cisco, Microsoft Azure, AWS, and Google. Students are also supported with placement assistance after successful course completion.

Document prepared for professional client presentation.