VAPT

Module 01 (VAPT Concepts)

1] Introduction of VAPT
2] Types of Testings
3] CIA Triad
4] Types of Hackers
5] Cyber Security Laws
6] Cyber Security In Naval Defence Sectors
7] Risk Assessment
8] Disaster Recovery And Backups systems
9] VAPT Methodology And Phases
10] Incident Responce
11] Cyber Security Teams
12] types of teams Red,Blue And Purple
13] Information Warfare

Module 02 (Networking Concepts)

1] Introduction of Networking
2] Network Methodologies
3] Network Medias
4] Network Topologies
5] Ipv4 Vs Ipv6
6] OSI reference model
7] tcp 3 way handshake
8] firewalls and types
9] IDS/IPS
10] Honeypots

Module 03 (Linux And VAPT Lab-Setup)

1] About Linux OS And Windows OS
2] Linux File System
3] About Virtualization
4] Install and Setup Vm And Vbox
5] Install Linux On Vm and Vbox
6] Linux Basic Commands
7] Windows Basic Commands

Module 04 (Social Engineering Techniques)

1] Introduction of social engineering
2] Phishing , Vishing , Whaling
3] Tailgating and Piggy Backing
4] Pre Texting And Spams
5] Countermeasures About Social Engineering

Module 05 (Cryptography And Sytegnography)
==========
1] About Cryprography
2] Hash Algorithms
3] Symmetric and Asymmetric Encryption
4] About Stegenography
5] Invisible secret4 and steghide

Module 06 (Information Gathering)
==========

1] Cyber Threat Intelligance
2] Whois Information Gathering
3] DNS Information Gathering
4] Social Media Information Gathering
5] Compitive Intelligance
6] Email Harvesting And Check Pwned Status
7] Search Engine Information Gathering
8] Dark Web Investigation

Module 07 (Network Scanning)
==========

1] Introduction of network Scanners
2] Nmap Network Scanning tool
3] Finding Internal Ips
4] Scanning Versions and Ports
5] Aggresive Scanning
6] Hands On Nmap

Module 08 (Vulnerability Scanning)
==========

1] Introduction of Vulnerability Assessment.
2] Introduction of Risk Assessment.
3] Scanning System Vulnerability Using Nessus.
4] Scanning Web Vulnerability Using Nessus,Nikto,Uniscan,Burp,Zap.etc
5] Scanning Network Using Nmap And Nessus.
6] Scanning Vulnerability Using Nmap
7] Intranet Security Testing Tools

Module 09 (Web Application Testing)
==========

1] Introduction of WAPT
2] Introduction of OWASP
3] SPF
4] Identitiy Management and Session management
5] XSS Injection
6] SQL Injection
7] Web Application Firewall
8] Load Balancer
9] parameter Tempering

10] IDOR
11] Unwanted File Uploads
12] CSRF
13] Security Headers
14] Cookie Attributes
15] Weak Password Policies
16] Weak Encryption
17] Sensitive Directories via Fuzzing
18] Mitigation Of Vulnerabilities

Module 10 (Wireless Network Testing)
==========

1] about routers and version
2] routers security
3] Routers Vulnerabilities
4] Fake Access point and security
5] Wifi Password Cracking

Module 11 (System Hacking)
==========

1] About System Hacking
2] Windows Hacking
3] Linux Hacking
4] Android Hacking
5] Device Security And Security Controls
6] CTF

Module 12 (Mobile Application Testing)
==========

1] About MAPT
2] Static And Dynamic Security Testing
3] Mobile Application Security Framework
4] Code Review and XML Analysis

Module 13 (Frequency Hacking And Counter Measure)
==========

1] All About Frequency Hacking
2] RTSLDR Devices
3] Capture Frequency
4] Replay Frequency Attack

5] Countermesures Of Frequency Hacking
6] Fraday’s Concepts

Module 14 (Physical Security Assessment)
==========

1] evaluating the physical security controls implemented in naval
2] Implement access controls
3] Implement surveillance systems
4] Implement perimeter security
5] Implement physical intrusion detection mechanisms.