CYBER SECURITY – VAPT

INTRODUCTION TO CYBER SECURITY
Introduction to Ethical Hacking & Cyber Security
Types of Hackers
Kinds of Hackers
Phases of Hacking
Terminologies of Cyber Security
Active and Passive attack
White Box, Black Box, Grey Box Pen Test
Hacker VS Cracker
CIA Triad
Conclusion

BASICS OF NETWORKING
Introduction to Networks
Types of Networks
What is ISP
IPV4 & IPV6
Public and Private IP
Static and Private IP
Classifications of IP A,B,C,D and E
Network Ports
Proxies and VPNs
Anonymous IP Tracking
Network Environment with Different Tools
Conclusion

BUILDING VIRUTUAL LAB
Introduction to Virtualization
Installation of VMWare
Configuring XP OS in Virtual Machine
Configuring WIN 7 OS in Virtual Machine
Configuring KAIL LINUX OS in Virtual Machine
Installation of VMWare tools
Conclusion

GITHUB AND KALI
Introduction to Github
Adding the Git repos to Kali
What is Kali
Conclusion

SPOOFING ATTACK
Introduction to spoofing
Email Spoofing Attack
Email Header analysis
Call Spoofing Attack
MAC Spoofing Attack
SMS Spoofing Attack
Case Studies of Spoofing Attacks Prevention

ANTI VIRUS
Introduction to Anti Virus
Types of Anti Virus

How antivirus Detect Malware
Importance of Anti-Virus Updates
Conclusion

MALWARES
Types of Malwares
Crafting a virus
Attack & Prevention of Virus
Crafting a Worm
Attack & Prevention of Worm
Crafting a Backdoor
Hack Windows by Backdoor
Attack & Prevention Backdoor
Crafting a Trojan
Attack & Prevention of Trojan
Crafting a Keylogger
Attack & Prevention Keylogger
Crafting a Ransomware
Attack & Prevention Ransomware
Conclusion

DATA Recovery
How Data Stores in Memory
How Data Recovery Works
Recovering Lost Data
Clearing the Data recovery possibilities
Conclusion

GHDB
Introduction to GHDB
importance GHDB operators
Filtering the search engine results by operators
Retrieving the confidential info using operators
Finding vulnerable sites using operators
Conclusion

BASIC ATTACKS AND SECURITY
Introduction to Phishing
Phishing Attack (Facebook/Gmail Hacking)
prevention of Phishing
IDN Homograph Attack
DNS Poisoning Attack
Prevention

IDS, FIREWALL AND HONEYPOTS
Introduction
Working of IDS, Firewall, Honeypot system Detection of Honeypots
Countermeasures & Evading tools Conclusion

DENIAL OF SERVICE
Introduction to DoS & DDoS
Types of DoS Attack
Case Studies of DoS and DDoS

Protection Tools and Countermeasures Conclusion

STEGANOGRAPHY
Introduction to steganography
Types of steganography
Hiding files using steganography tools
Extracting hidden data from files
NTFS Alternate Data Streams
Conclusion

MOBILE HACKING
Introduction to architecture of various Mobile
Mobile Spy Using Malwares
Security Measures Conclusion

CRYTPOGRAPHY
Introduction to Encryption and Description
Data Encryption and Decryption using various tools
Conclusion

WIRELESS ATTACKS
Introduction to wireless architecture
Types of Wireless Networks
WPS vulnerability exploit
Packet-injection and monitor mode
Wi-Fi deauthentication
WEP/WPA hacking using Aircrack
Conclusion

CYBER LAWS AND SECURITY
Cyber Laws in India
Online Security Precautions Conclusion - End of the Session

VAPT

FOOTPRINTING AND RECONNAISSANCE
Introduction to Foot printing
Introduction to reconnaissance

Footprinting using search engines
Collecting info by cache
shodan search engine
exploit DB

Network Foot-Printing
Host availability check by Ping
Analyzing the target IP path by Trace root
NS-Lookup
Analyzing local and public network

Foot printing Who is
Gathering information of domain using Whois

Footprinting using DNS
Types of DNS records
DNS enumeration using tools

Email Footprinting
Email Header analysis by manually
Email Harvesting
Email header analysis by ETP
prevention of Email Harvesting

Social engineering
Introduction to Social Engineering
Eavesdropping
shoulder surfing
dumpster diving
impersonation on social media sites
Introduction to phishing
Phishing Attack SET Kit Attack
Analyzing the phishing attacker

Website Foot printing
Banner grabbing
Finding target key info by Shodan Reverse IP lookup
crawling
Way-back machine
Web mirroring
Robots.txt
Analyzing robots.txt
Analyzing the web technologies
Firewall analyzing

Google hacking/Google dorks
Hunting the vulnerable sites using dorks
Retrieving the confidential info using operators
Conclusion

Foot printing using social Network sites
analyzing the target profiles in social media
Gathering intelligence from Social Networking sites
Using OSINT tools to gather info about target
Competitive intelligence

Competitive Intelligence
Introduction to Competitive Intelligence
Techniques to gather info from target

SCANNING
Introduction to scanning
Types of Scanning
OSI layers
Methodologies of Scanning
Introduction to Nmap
Nmap Commands
Introduction to acunetix
Web vulnerability Scanning using acunetix
Introduction to nessus
Network vulnerability Scanning using nessus
application scanning using ZAP
Subdomain enumerations

GAINING ACCESS
Introduction to Gaining Access
Introduction to burp suit
Configuring burp with browser

Introduction Directory Traversal
Attacks of Directory Traversal
Prevention of Directory Traversal

Introduction Sql injection
Types of Sql injection Attacks of Sql injection
Error Based SQL injection Attack
Union Based SQL inaction attack
Boolean based blind sql injection attack
Prevention of Sql injection

Introduction to XSS
Types of XSS
Reflected XSS Attack
Stored XSS Attacks
Dom based XSS Attacks

LFI and RFI Attacks
IDOR
SPF record
URL redirection
Host Heder Attack
CSRF
Parameter tampering

Parameter brute forcing
OTP brute forcing
File uploading
Session hijacking
sub domain takeover
Security misconfiguration

MAINTINING ACCESS
Introduction to Web Malware shells
Shell uploading to the server Prevention

CLEARING TRACKS
Introduction to Clearing Tracks Hiding identity

Two CTF challenges
In this CTF challenges you will learn some more tools and techniques which are not covered in above.

Report Making on Security Vulnerabilities