CHAPTER - 2	RECONNAISSANCE AND FOOTPRINTING
Netcraft	Website analyzing Server
Metagoofil	Command line interface that uses Google Hacks to find infomation in metatags (domain, Filetype)
Website Informer	online tool that gathers detailed information on a website such as a website's traffic rank, daily visitors rate, page views, etc. Website Informer discovers the main competitors of the website, reveals DNS servers used by the website, and also obtains the Whois record of the target website. https://website.informer.com
Web Mirroring | Website Cloning | Web Footprinting	HTTrack | Web Site Copier | NCollecteor Studio | Black Widow | Cyotek WebCopy | Web Ripper | Teleport Pro | Backstreet Browser
EmailTracerPro	Window Software that trace an Email back to its true point of Origin
eMailTackerPro | infoga | Mailtrack | PoliteMail	Allow to track an email and extract information
Whois	Gives Registration Information
SmartWhois	Windows GUI Software for Whois
Batch IP Converter	Batch IP Converter (http://www.sabsoft.com), etc. to extract additional target Whois information.
NsLookup	Perform DNS Queries
Dig	Unix Based Command Line Like nslookup : (zone transfer)
Reverse DNS Lookup	DNSRecon | Reverse IP Domian Check
traceroute / tracert (windows)	Find intermediary Servers
OSRFramework	Uses open source intelligence to get information about target usufy.py | mailfy.py | searchfy.py | domainfy.py | Phonefy.py | entify.py
Recon-ng	Web-Based open source reconnaissance framework with independent modules and database interaction, which provides an environment in which open source, web-based reconnaissance can be conducted.
Metasploit Framework	
theHarvester	Emails | Subdomains | Hosts | Employee Name | Open Ports | Banners
theHarvester & Email Spider	These tool collect publicy available email address of the target organization.
Sublist3r	Enumerates Subdomains
Pentest-Tools Find Subdomain	Online tool used for discovering SubDomain and IP address
DIRB	Find Subdirectories on Web Application
Maltego	Powerful OSINT Tools : IP address | Domain & Domain Name Schema | ServerSide Technology | SOA (Service Oriented Architecture) Info. | Name Server | Mail Exchange | Geo Location | Email and Phone
Social Engineering Framework (SEF)	Helps in generating Phishing attacks and Fake Emails
BuzzSumo	Advanced Social Search Engine Finds the Most Shared Content

CHAPTER - 2	RECONNAISSANCE AND FOOTPRINTING
Shodan	Hacker's Search Engine : lets you find connected devices(routers, server, IOT, etc) using a variety of filters.
Censys	Alternative of Shodan : search engine provides a full view of every server and device exposed to the internet.
Thingful	L
Fingerprinting Organization with Collected Archives (FOCA)	Tools that Reveals metadata and Hidden information in the document.
Intelius | pipl.com | Anywho | Beenverified | WhitePages | Peek You	Tools for People Search (People's Name | Address | contact details | Date of Birth | Photo | Videos | and so on..)
Reverse Image Search	Google Image Search | TinEye Reverse Image Search | Yahoo Image Search
Video Analysis Tools	Youtube DataViewer | EZGif | Google Videos | Yahoo videos | VideoReverser.com
Startpage, MetaGer	Meta Search Engines
NAPALM FTP Indexer , Global FTP Search Engine, FreewareWeb FTP File Search	FTP Search Engines to retrieve critical files and Directories about the target. Site : https://www.searchftps.net/ : https://globalfilesearch.com : http://www.freewareweb.com
Dark web browsers	Tor | Exonera Tor | freenet | Retroshare | GNUnet | I2P | OnionLand Search Engine
TOR Browser	It is used to access the deep and dark web where it act as a default VPN for the user and bounce the network IP address through several servers before interacting with the web.
Business Information	Opencorporates | CrunchBase : to gather important information about the target organization, such as their location, address, contact info, and employee database.
Alert Monitoring	Google Alerts | Twitter Alerts : help attackers to track mention of the organization's name, member name, website.
Online Reputation Management (ORM)	Trackur | Brand24 | Mention
Location Search on Social Media Sites	Followerwonk | Hootsuite | Sysomos Search for both geotagged and Non-geotagged info **Hootsuite** (https://hootsuite.com), **Sysomos** (https://www.sysomos.com), etc. to gather additional information related to the target company and its employees from social networking sites.
Followerwonk	Helps to explore and grow one's social graph by digging deeper into twitter analytics.
Sherlock | Social Searcher	**Social Searcher** (https://www.social-searcher.com), **UserRecon** (https://github.com), etc. to gather additional information related to the target company and its employees from social networking sites.
Sherlock	It is used to search a vast number of social networking sites for a target username.

CHAPTER - 2	RECONNAISSANCE AND FOOTPRINTING
Social Searcher	Allows you to search for a content in social network in real time and provide deep data analytics.
Web data Extractor | ParseHub | SpiderFoot	Web Spidering Tools : perform automated searches on the target websites and collect specified information, such as employee name, and Email address.
Extracting Web Links Tools	OctoParse | NetPeak Spider | Link Extractor
User-Directed Spidering	BurpSuite, WebScrab
Extracting Metadata	MetMagoofil | Exiftool
WebSite-Watcher | VisualPing	To Detect changes or Updates in targeted website, and they analyze the gathered information to detect underlying vulnerabilities in the target website.
Web-Stat | Alexa | Monitis	Web Traffic Monitoring Tools
Clicky	Find the Total Number of visitors browsing the website
Opentracker	Monitor Total number of Pages viewed by the user
Find IP Geolocation Information	IP2Location | IP Location Finder
Traceroute Tools	Path Analyzer Pro | VisualRoute
Path Analyzer Pro	it delivers network route tracing with performance tests, DNS, Whois, network Resolution to investigate network issue.
VisualRoute	It is a traceroute and network diagnostic tool that identifies the geographical location of routers, servers , and other IP address.
BillCipher	Information gathering tool for a website or ip Address
Recon-dog	It is an all in one tool for information gathering needs, which uses APIs to collect information about the target system.
Some Additional Footprinting Tool	TheHarvester | Th3Inspector | Raccoon | Orb | PENTMENU | Recon-Dog : to gather additional information related to the target company.
When did this company begin? How did it develop??	EDGAR Database, D & B Hoovers, LexisNexis, Business Wire
What are company's plans	MarketWatch, The wall street transcript, Alexa, Euromonitor
What expert opinion say about the company ?	SEMRush, AttentionMeter, ABI/Inform Global, SimilarWeb
Information Gathering using NNTP Usenet Newsgroups	Usenet Newsgroups, such as Newshosting and Eweka , to find the valuable information about the operating systems , software, web servers.

CHAPTER 3	SCANNING NETWORKS
Scanning Tools	Nmap | Hping2 /Hping3 | Metasploit | NetScanTools Pro | SolarWinds Port Scanner | PRTG Network Monitor | Unicornscan | Omnipeek Network Protocol.
Scanning Tool for Mobile	IP Scanner (iOS) | Fing (Android+iOS) | Network Scanner (Android)
Ping Sweep Tools	Angry IP Scanner | Solarwinds Engineer's Toolkit | NetScanTools Pro | Colasoft Ping tool | Visual Ping Tester | OpUtils | Pinkie
NetScanTools Pro	NetScanTools Pro assists attackers in automatically or manually listing IPv4/IPv6 , hostname, domain Names, and URLs.
Angry IP Scanner	Pings each ip address to check if any of these addresses are live. Then it optionally resolves hostnames, determine the MAC addresses, scan ports etc.
ServerMask	Tool to disable or change banner information
Anonymizers	Allows them to Bypass internet censors and evade certain IDS & firewall
Colasoft Packet Builder	Tool to create custom TCP Packets
Proxy Tools	Proxy Switcher | CyberGhost VPN | TOR | CCProxy | Burp Suite | Hotspot Shield |
Proxy Chains	Proxy Switcher | Proxy Workbench | Proxy Chains
Proxy Switcher	It allows you to surf anonymously on the internet without disclosing your IP address.
CyberGhost VPN	CyberGhost VPN hides your IP and replaces it with one of your choice, thus allowing you to surf anonymously.
Proxy Tools for Mobile	Shadowsocks | ProxyDroid | Proxy Manager |
Alkasir | Tails	Censorship Circumvention Tools
Whonix | Psiphon	Anonymizers
Psiphon	Open source Anonymizer software that allows the attacker to surf the internet through a secure proxy.
Anonymizers for mobile	Orbot | Psiphon | OpenDoor
Network Mapping Tools	OpManager | The Dude | NetSurveyor | NetBrain | Spiceworks Network Mapping Tool | Solarwinds Network Topology mapper
Network Topology Mapper	Network topology mapper discovers a network and produces a comprehensive network diagram. It display in-depth connection such as OSI Layer 2 and Layer 3 topology data.
Network Mapping Tools for Mobile	Scany | Network Analyzer | PortDroid Network Analysis
Vulnerability Scanner	Nessus | GFI LanGuard | Nikto | OpenVAS | wpscan | MBSA (Microsoft Baseline Security Analyzer) | Freescan | Qualys

CHAPTER - 4	ENUMERATION
NetBIOS Enumerator	NetBIOS Enumeration Tool : NetBIOS names, usernames, domain names, and MAC addresses
Nmap	Nmap's nbstat NSE script allows attacker to retrieve target's NetBIOS names and MAC address.
NetBIOS Enumeration Tool	Global Network Inventory | Advanced IP Scanner | Hyena | Nsauditor Network Security Auditor | Superscan
PsTools	Enumerating user account using the PsTools suite helps to control and mange remote systems from the command line.
Enumerating User Account	PsTools (PsExec | PsFile | PsGetSid | PsKill | PsInfo | PsList | PsLoggedOn | PsLogList | PsPasswd | PsShutdown)
Net View Utility	Enumerate Shared Resources
Snmpcheck	Snmpcheck allows one to enumerate the SNMP Device and place the output in a very human-readable and friendly format
Softperfect Network Scanner	Discover shared folders and retrieves practically any information about network device via WMI, SNMP, HTTP, SSH and Powershell
Other SNMP Enum tools	Network Performance Monitor | OpUtils | PRTG Network Monitor | Engineer's Toolkitset
Softerra LDAP Enumeration	Provides Various features essential for LDAP development, deployment, and administration of directories.
Other LDAP Enum Tools	LDAP Admin Tool | LDAP Account Manager | LDAP Search | JXplorer | Active Directory Explorer (AD Explorer)
AD Explorer	Active Directory Explorer (AD Explorer) is an advanced Active Directory (AD) viewer and editor. It can be used to navigate an AD database easily, define favorite locations, view object properties and attributes without having to open dialog boxes, edit permissions, view an object's schema, and execute sophisticated searches that can be saved and re-executed.
ntptrace	Traces a chain of NTP servers back to the primary Sources
ntpdc	Monitors Operations of the NTP Daemon, ntpd
ntpq	Monitors NTP daemon operation and determines performance
Other NTP Enum Tools	PRTG Network Monitor | Nmap | Wireshark | udp-proto-scanner | NTP Server Scanner
PRTG Network Monitor	It includes SNTP sensor monitor, a simple network time protocol (SNTP) server that shows the response time of the server and the time difference in comparison to the local system time.
rpcinfo -p <ip>	scan the ip address for an open NFS ports and NFS Service running on it
showmount -e <IP>	List the shared files and directories
RPCScan	RPCScan Communicates with RPC Service and check misconfiguration on NFS shares
SuperEnum	It includes a script that does the basic enumeration of any open port
Netscantools Pro	Netscantools Pro's SMTP Email Generator tool tests the process of sending an email message through an SMTP server

CHAPTER - 4	ENUMERATION
smtp-user-enum	Enumerating OS-level user accounts on solaris via smtp server Enumeration is done using VRFY, EXPN and RCTP TO commands
DNS Zone Transfer list	Nslookup | dig | DNSRecon
DNSSEC Zone Walking Tools	LDNS | DNSRecon | nsec3map | nsec3walker | DNSWalk
Professional Toolset, DNS Records	
LDNS-walk	Enumerates the DNSSEC zone and obtain result on the DNS record Files
ike-scan	IPSec Enumeration : Enumerate Sensitive Information including encryption, hashing algo, authentication type, key distribution algorithm
RPC Enumeration Tools	nmap | NetScanTools Pro | RPCScan
Unix, Linux User Enumeration	rusers | rwho | finger
SMB Enumeration	Nmap | SMBMap | enum4linux | nullinux
FTP Enumeration Tool	Metasploit (auxiliary/scanner/ftp/ftp_version)
TFTP Enumeration Tools	PortQry | Nmap
PortQry	This Utility reports the port status of TCP and UDP ports on a selected Target
IPv6 Enumeration Tools	Enyx | IPv6 Hackit
Enyx	Enum tool that fetches the IPv6 address of a machine through SNMP
IPv6 Hackit	Hackit is a scanning tool that provides a list of active IPv6 hosts. It can perform TCP Port scanning and identify AAAA IPv6 host records.

CHAPTER - 5	VULNERABILITY ANALYSIS
Website for Vulnerability Research	1. Microsoft Vulnerability Research(MSVR) | 2. Security Magazines | 3. Security Focus | 4. Dark Reading | 5. PenTest Magazines | 6. Help Net Security | 7. Security Tracker | Hacker Storm
Common Vulnerability Scoring System	CVSS provides an Open Framework for communicating the characteristics and impact of IT Vulnerability
Qualys Vulnerability Management	Cloud-Based Service vulnerability assessment tool
Nessus Professional	Identifying the Vulnerability, Configuring Issues, and Malwares
GFI Languard	Scan, Detect, assesses, and rectify security Vuln in network and connected Devices
OpenVAS	A framework of several services and tools offering a comprehensive and powerful vuln scanning and Vuln management solution.
Nikto	A web server assessment tools that examines a web server to discover potential problems and security vulnerability.

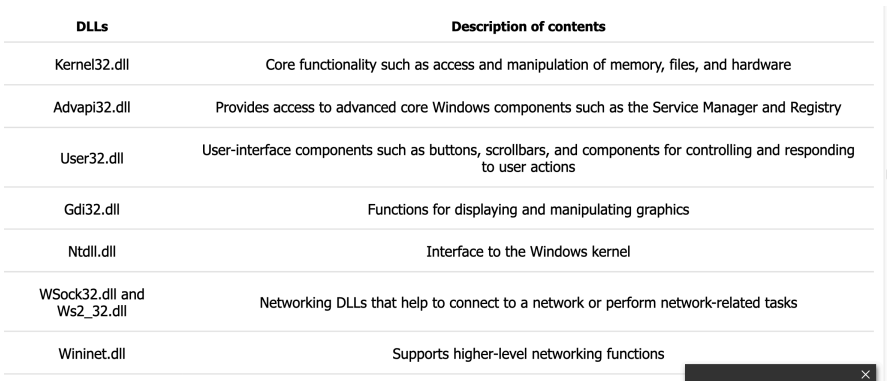
CHAPTER - 5	VULNERABILITY ANALYSIS
Other Vulnerability Assessment Tools	Qualys Freescan | Acuetix Free Scan | Nexpose | Network Security Scanner | SAINT | Microsoft Baseline Security Analyzer | Core Impact Pro
Vulners Scanner	An Android app that performs passive vulnerability detection based on the fingerprint of the software version.
Security Metrics Mobile	An Android app that complies with PCI SSC guidelines to generate a scan report

CHAPTER - 6	SYSTEM HACKING
Online Tools to Search Default Password	https://www.fortypoundhead.com https://cirt.net https://defaultpassword.us https://defaultpassword.in https://routerpasswords.com https://default-password.info
Mimikatz Rebeus Windows Credentials Attacks	Allow attacker to pass kerberos TGT to other computers and sign in using the victim's ticket. It also helps in extracting plaintext passwords, hashes, PIN codes, and kerberos tickets from memory
Responder	It is an LLMNR, NBT-NS and MDNS poisoner.
rtgen	Tool to create a rainbow table
RainbowCrack	RainbowCrack cracks hashes with rainbow tables. It uses a time-memory tradeoff algorithm.
Password Recovery Toolkit (PRTK)	Attackers uses PRTK which is equipped with DNA tools, to perform this attack
	It Breaks complex passwords, recovers strong encryotion keys and unlock documents in a production environment.
Password Recovery Tools	PRTK, Passware Kit Forensics, hashcat, Windows Password Recovery Tool, Hashcat, Windows Password Recovery Tools, PCUnlocker
pwdump7	Extract LM and NTLM password hashes of local user accounts from Security Account Manager (SAM).
Tools to Extract the password hashes	Mimikatz, Powershell Empire, DSInternals Powershell, Ntdsxtract
L0phtCrack, ophcrack	Password Cracking Tools
L0phtCrack	It is a tool design to audit passwords and recover application
ophcrack	It is window password cracker based on rainbow tables. It comes with a graphical user interface and runs on multiple platform
Password Cracking Tools	RainbowCrack, John the Ripper, hashcat, THC-Hydra, Medusa
Vindicate	Vindicate is an LLMNR/NBNS/mDNS Spoofing Detection Toolkit to detect name service spoofing. It is designed to detect the use of hacking tool such as Responder, Inveigh, NBNSpoof, and metasploit's LLMNR, NBNS, and mDNS Spoofer.

CHAPTER - 6	SYSTEM HACKING
got-responded	This helps security professional to check for both LLMNR/NBT-NS spoofing
Respounder	Respounder detects the presence of a responder in the network. This tools also helps security Professional to detect rogue hosts running responder on public Wi-Fi network
Exploit Sites	Attackers search for an exploit based on the OS and software application on exploit sites such as SecurityFocus (https://securityfocus.com) and Exploit Database (https://exploit-db.com)
OpenStego	It is a steganography application that provides the Data Hiding, Watermarking.
Image Steganography tools	QuickStego | SSuitePicsel | CryptaPix | gifshuffle | PHP-Class Stream Steganography
Document Steganography tools	StegoStick | StegJ | Office XML | SNOW | Data Stash | Texto
OmniHide Pro	It hides the files within another file. Any file can be hidden with common image/music/video/document formats. The output will work in the same way as the original source file does.
Video steganography tools	RT steganography | StegoStick | OpenPuff | MSU StegoVideo
Deep Sound	Hides Secret data in audio files - wave and Flac. It enables the extraction of secret files directly from audio CD Track.
Audio steganography tools	BitCrypt | StegoStick | MP3Stego | QuickCrypto | Spectrology
GiliSoft File lock pro	It locks files, Folders and Drives, hides files, folder and Drives to make them invisible or password protected files, folder and Drives
Folder steganography tools	Folder Lock | Hide Folder 5 | Invisible Secret 4 | Max Folder Secure | QuickCrypto
Spam Mimic	It is a Email/Spam steganography tools that encodes the secret message into an innocent-looking spam email.
Steganography tools for MOBILE	steganography master | Stegais | SPY Fix | PixelKnot | Pocket Stego | steganography image | steganography
Zsteg (steganography detection tool)	It is used to detect stegano-hidden data in PNG and BMP image File
steganography Detection Tools	StehoVeritas | Stegextract | StegoHunt | steganography Studio | Vitural steganography Laboratory (VSL)
Auditpol.exe	It is a command line utility tool to change audit security settings at the category and sub category levels. It is used to enable or disable security auditing on local or remote systems, and to adjust the audit criteria. **Enabling system auditing:** **C:\>auditpol /set /category:"system","account logon" / success:enable /failure:enable** **Disabling system auditing:** **C:\>auditpol /set /category:"system","account logon" / success:disable /failure:disable** **auditpol /get /category:***

CHAPTER - 6	SYSTEM HACKING
Clear_Event_Viewer_Logs.bat	Utility to clear the security, System and application logs
Clear-EventLog	Command to clear all the powershell events logs from remote or local computers.
wevutil	Utility to clear event logs related to the system, application and security
Cipher.exe	It is an in-built windows command-line tools that can be used to securely delete data by overwriting it to avoid their recovery in the future. To overwrite deleted files in a specific folder : cipher /w:<drive letter>:\<folder name> To overwrite all the deleted files in the given drive : cipher /w:<drive letter>
CCleaner	CCleaner cleans traces of temporary files, log files, registry files, memory dump, and your online activities such as your internet history.
Other Track Covering Tools	DBAN | Privacy Eraser | Wipe | BleachBit | ClearProg
Fatrat	It is an exploitation tool that compiles malware with a popular payload that can then be executed on Windows, Android, and Mac OSes. The software offers an easy way to create backdoors and payloads that can bypass most anti-viruses.
beroot.exe	**BeRoot** Project is a post exploitation tool to check common misconfigurations to find a way to escalate our privilege
Some another escalation	**run post/windows/gather/smart_hashdump** **getsystem -t 1** : uses the service - Named Pipe Impersonation (In memory/Admin) Technique.
Timestomp	**Timestomp** is a post-exploitation module available in **Meterpreter** that can be used to modify the MACE(Modified, Accessed, Created, Entry) values of files.
Power Spy	It is a computer activity monitoring software that allows you to secretly log all users on a PC while they are unaware.you can remotely receive log reports on any device via email or FTP. You can check these reports as soon as you receive them or at any convenient time. You can also directly check logs using the log viewer on the monitored PC.
Spytech/SpyAgent	It is a powerful piece of computer spy software that allows you to monitor everything users do on a computer—in complete stealth mode. SpyAgent provides a large array of essential computer monitoring features as well as website, application, and chat-client blocking, lockdown scheduling, and the remote delivery of logs via email or FTP.
Spyware Tools	ACTIVTrak | Veriato Cerebral | NetVizor | SoftActivity Monitor

CHAPTER - 7	MALWARE THREAT
Tools to create Covert Channel	Ghost Tunnel V2 | ELECTRICFISH -a | North Korean tunneling tools
Ghost Tunnel V2	**GhostTunnel** is a covert backdoor transmission method that can be used in an isolated environment.
Exploit Kit or Crimeware toolkit	It is a platform to deliver exploits and payloads such as trojans, spyware , backdoors,bots and buffer overflow scripts to the target system. Exploit kits comes with pre-written exploit codes.
Dharma	Ransomware that attacks victims through email campaign
Ransomware Families	Cerber, CTB-Locker, Sodinokibi, BitPaymer, CryptXXX, Cryptobit Ransomware, Crypto Locker Ransomware, Crypto Defence Ransomware, Cryto Wall Ransomware.
DELmE's Batch Virus Maker	DELmE batch virus maker creates viruses that can perform tasks such as Deleting files on a hard disk drive, disabling admin privileges , clearing the registry, and killing tasks.
Virus Maker Tools	JPS Virus Maker, Bhavesh Virus Maker SKW, Deadly Virus Maker, SonicBat Batch Virus Maker, TeraBIT Virus maker, Andreinick05's Batch Virus Maker.
JPS Virus Maker	It is used to create its own customized virus.
Internet Worm Maker Thing	It is an open source tool used to create worms that can infect victim's drives ,files show messages , and disable antivus software.
Other Worm Maker tools	Batch Worm Generator, C++ Worm Generator
SwayzCryptor	SwayzCryptor is an encrypter (or "crypter") that allows users to encrypt their program's source code.
Remote Access Trojans	njRAT, ProRat, Theef, MoSucker
HashMyFiles	This produces the hash value of file using MD5, SHA1, CRC32, SHA-256, SHA-512, and SHA-384 algorithm.
File Fingerprinting Tools	Mimkatz, Hashtab, Hashcalc, hashdeep, MD5Sums
Local or Online Malware Scanning Tools	Hybrid Analysis, Cuckoo Sandbox, Jotti, Valkyrie Sandbox, Online Scanner.
VirusTotal	Free service that analyzes suspicious files and URLs and Facilitates , the detection of viruses, worms, Trojans etc
BinText	It is a text extractor that can extract text from any kind of file and has the ability to find Plain ASCII text , unicode text and resource strings, thus providing useful information for each item.
String Searching Text	Bintext, FLOSS, Strings, Free EXE DLL, FileSeek , Hex Workshop
PEid	The PEid tool provide details about the window executable files. It can identify signatures associated with over 600 different packers and compilers.
Packaging/Obfuscation Tools	Macro_Pack, UPX, ASPack
PE Explorer	PE Explorer lets you open, view, and edit a variety of different 32-bit windows executable file types (also called as PE files) ranging from the common, such as EXE, DLL, and ActiveX Controls.

CHAPTER - 7	MALWARE THREAT
PE Extraction Tools	Portable Executable Scanner (pescan), Resource Hacker, PEView
Some of the standard DLL's	
Dependency Walker	Dependency walker lists all the dependent modules of an executable file and buils hierarchical tree diagrams, IT also record all the functions of each module exports and calls.
Dependency Checking tools	Dependency-Check, Snyk, Hakiri, RetireJS
IDA	IDA is a windows, linux , MAcOS, hosted multi-processor dissassembler nd debugger that can debug through instruction tracing , Function Tracing , and Read and Write Execute Tracing Features .
OllyDbg	OllyDbg is a debugger that emphasizes binary code analysis, which is useful when source code is unavailable. It traces registers, recognizes procedures, API calls switches, tables, constants, and strings, and locates routines from object files and libraries.
Disassembling and Debugging Tools	Ghidra, Radare2, OllyDbg, WinDbg, ProcDump.
Port Monitoring Tools	Netstat, TCPView, Port Monitor, CurrPorts, TCP Port Monitoring, PortExpert, PRTG's Network Monitor
Process Monitor	The Process Monitor shows the real-time file system, registry, and process/thread activity.
Process. Monitoring Tools	Process Explorer, OpManager, Monit, ESET SysInspector, System Explorer.
Jv16 PowerTools	It is a registry cleaner used to find registry errors and unneeded registry junk. It also helps in detecting registry entries created by the malware.
Registry Monitoring Tools	Regshot, Reg Organizer, Registry Viewer, RegScanner, Registrar Registry Manager.
Windows Service Manager(SrvMan)	To trace malicious services initiated by the malware
Windows Startup Program Monitoring Tools	Autorun Organizer, Quick Startup, StartEd Pro, Chameleon Startup Manager
Windows Service Monitoring Tools	Advanced Windows service manager, Process Hacker, Netwrix Service Monitor, Anvir Task Manager, Service+
Installation Monitoring Tools	Mirekusoft Install Monitor, SysAnalyzer, Advanced Uninstaller Pro, REVO UNINSTALLER PRO, Comodo Program Manager
Mirekusoft Install Monitor	monitors what gets placed on your system and allows you to uninstall it completely.

CHAPTER - 7	MALWARE THREAT
Splunk	It is a SIEM tool that can automatically collect all the events logs from all the system present in the network
Log Analysis Tool	ManageEngine Event Log Analyzer, Loggly, SolarWinds Log & Event Manager (LEM), Netwrix Event Log Manager
PA File Sight	It audit who is deleting files, moving files, or reading files . It also detects users copying files and optionally blocks access
File and Folder Integrity Checking Tools	Tripwire File Integrity and Change Manager, Netwrix Auditor, Verisys, CSP File Integrity Checker, NNT Change Tracker.
DriverView	DriverView utility displays a list of all the device drivers currently loaded on the system along with information such as load address of the driver, description, version, and product name
Device Driver Monitoring Tools	Driver Booster, Driver Reviver, Driver Easy, Driver Fusion, Driver Genius
SolarWinds NetFlow Traffic Analyzer	NetFlow Traffic Analyzer collects traffic data, correlates it into a useable format, and presents it to the user in a web-based interface for monitoring network traffic.
Network Activity Monitoring Tools	Casa Network Analyzer, Wireshark, PRTG Network Monitor,GFI LanGuard, NetFort LANGuardian
DNSQuerySniffer	DNSquerySniffer is a network sniffer utility that shows the DNS queries sent on your system.
DNS Monitoring / Resolution Tools	DNSstuff, DNS Lookup Tools, Sonar Lite
Kaspersky Internet Security	This provide the protection against trojans, viruses, spyware, ransomware, phishing, and Dangerous websites.
Other Anti Trojan Software	McAfee Livesafe, Symantec Norton Security Premium etc

CHAPTER 8	SNIFFING
macof	macof is a Unix and Linux tool that is a part of the dsniff collection. It floods the local network with random MAC addresses and IP addresses, causing some switches to fail and open in repeating mode, thereby facilitating sniffing.
DHCP Starvation Attack tools	Yersinia, Hyenae, dhcpstarv, Gobbler, DHCPig
Yersinia	Yersinia is a network tool designed to take advantage of weaknesses in different network protocols such as DHCP. It pretends to be a solid framework for analyzing and testing the deployed networks and systems
Arpspoof	arpspoof redirects packets from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies. This is an extremely effective way of sniffing traffic on a switch.
Cain & Abel	Cain & Abel is a password recovery tool that allows the recovery of passwords by sniffing the network and cracking encrypted passwords. The ARP poisoning feature of the Cain & Abel tool involves sending free spoofed ARPs to the network's host victims. This spoofed ARP can make it easier to attack a middleman.
TMAC & SMAC	Technitium MAC Address Changer (TMAC),

CHAPTER 8	SNIFFING
OmniPeek Network Analyzer	OmniPeek Network Analyzer provides real-time visibility and expert analysis of each part of the target network. It performs analysis, drills down, and fixes performance bottlenecks across multiple network segments. It includes analytic plug-ins that provide targeted visualization and search abilities
SteelCentral Packet Analyzer	SteelCentral Packet Analyzer provides a graphical console for high-speed packet analysis. It captures terabytes of packet data traversing the network, reads it, and displays it in a GUI. It can analyze multi-gigabyte recordings from locally presented trace files or on remote SteelCentral NetShark probes (physical, virtual, or embedded on SteelHeads), without a large file transfer, to identify anomalous network issues or diagnose and troubleshoot complex network and application performance issues down to the bit level.
ARP Spoofing Detection Tools	XArp, Capsa Netwrok Analyzer, ArpON, Arp Antispoofer, ARPStraw, shARP, Cain and Abel
XArp	XArp is a security application that detects ARP-based attacks. It detects critical network attacks that firewalls cannot cover. It uses advanced techniques to detect ARP attacks like ARP spoofing. This application screens the whole subnet for ARP attacks using different security levels and fine-tuning possibilities. A local network that is subject to ARP attacks inspects every ARP packet and reports attacks against remote machines.
NetScanTool Pro	This tool has also the capability to detect promiscuous mode
Sniffing tools	Wireshark, Outlook Express,
Promiscuous Detection Tools	Nmap , NetScan Tools Pro ,

CHAPTER 9	SOCIAL ENGINEERING
Social Engineering Toolkit (SET)	It is an Open-Source python driven tool aimed at penetration testing around Social Engineering
Other Social Eng. Tools	SpeedFish Framework, gophish, King Phisher, LUCY, MSI Simple Phish
Audit Organization's Security for Phishing Attacks using OhPhish	OhPhish is a web-based portal for testing employees' susceptibility to social engineering attacks. It is a phishing simulation tool that provides an organization with a platform to launch phishing simulation campaigns on its employees. The platform captures the responses and provides MIS reports and trends (on a real-time basis) that can be tracked according to the user, department, or designation.
Shellphish	It is a phishing tool used to obtain user credentials for various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. It can also provide the victim system's public IP address, browser information, hostname, and geolocation
Detect Phishing Using Netcraft	Netcraft anti-phishing community is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks. The Netcraft Extension provides updated and extensive information about sites that users visit regularly; it also blocks dangerous sites. This information helps users to make an informed choice about the integrity of those sites.

CHAPTER 9	SOCIAL ENGINEERING
Detect Phishing using PhishTank	PhishTank is a free community site on which anyone can submit, verify, track, and share phishing data. As the official website notes, “it is a collaborative clearing house for data and information about phishing on the Internet.” PhishTank provides an open API for developers and researchers to integrate anti-phishing data into their applications.

CHAPTER 10	DENIAL OF SERVICE
DOS Attack Tools	Metasploit(auxiliary/dos/tcp/syn), hping3 (hping3 -S (Target IP Address) -a (Spoofable IP Address) -p 22 --flood) (hping3 -d 65538 -S -p 21 --flood (Target IP Address),
High Orbit Ion Cannon (HOIC)	HOIC (High Orbit Ion Cannon) is a network stress and DoS/DDoS attack application. This tool is written in the BASIC language. It is designed to attack up to 256 target URLs simultaneously. It sends HTTP, POST, and GET requests to a computer that uses lulz inspired GUIs. It offers a high-speed multi-threaded HTTP Flood; a built-in scripting system allows the deployment of “boosters,” which are scripts designed to thwart DDoS countermeasures and increase DoS output.
Low Orbit Ion Cannon (LOIC)	LOIC (Low Orbit Ion Cannon) is a network stress testing and DoS attack application. We can also call it an application-based DOS attack as it mostly targets web applications. We can use LOIC on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service of a particular host.
Anti DDoS Guardian	It is a DDoS attack protection tool. It protects IIS servers, Apache serves, game servers, Camfrog servers, mail servers, FTP servers, VOIP PBX, and SIP servers and other systems. Anti DDoS Guardian monitors each incoming and outgoing packet in Real-Time. It displays the local address, remote address, and other information of each network flow. Anti DDoS Guardian limits network flow number, client bandwidth, client concurrent TCP connection number, and TCP connection rate. It also limits the UDP bandwidth, UDP connection rate, and UDP packet rate.
Other DoS Attack Tools	Imperva Incapsula DDoS Protection, DOSarrest’s DDoS protection service, DDoS-GUARD, Cloudflare
KFSensor	KFSensor acts as a honeypot, designed to attract and detect hackers and worms by simulating Vulnerable system service and Trojans.

CHAPTER 11	SESSION HIJACKING
BurpSuite	Burp Suite allows an attacker to inspect and modify the traffic between the browser and target application.

CHAPTER 11	SESSION HIJACKING
Other Session Hijacking Tools	OWASP ZAP, bettercap, netool toolkit, WebSploit Framework, sslstrip
Zed Attack Proxy (ZAP)	Zed Attack Proxy (ZAP) is an integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. It is designed to be used by people with a wide range of security experience, and as such is ideal for developers and functional testers who are new to penetration testing.
Session hijacking tools for mobile phones	DroidSheep, DroidSniff, FaceNiff
Bettercap	This tool is also used for sniffing and arpspoofing, sslstrip and many other tools.

CHAPTER 12	EVADING IDS, FIREWALLS AND HONEYPOTS
Honeypot Tools	KFSensors, SPECTER
KFSensor	It is a Host Based Intrusion Detection System(IDS) that act as a honeypot to attract and detect hackers and worms by simulating vulnerable system Services and Trojans.
SPECTER	It is honeypot based IDS that offers common internet services such as SMTP, FTP, POP3, HTTP and TELNET which appear perfectly normal to the attacker but in fact are traps.
Honeyd	Honeypot tools
Snort	Open source network intrusion detection system capable of performing real time traffic analysis and packet logging on ip network.
ZoneAlarm FREE FIREWALL 2019	It blocks attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network from hackers, malware, and other online threats that put network privacy at risk, and monitors programs for suspicious behavior spotting and stopping new attacks that bypass traditional anti-virus protection.
firewalls	ManageEngine Firewall Analyzer, pfSense, Sophos XG Firewall, Comodo Firewall, to block access to a particular website or IP address.
HoneyBOT	HoneyBOT is a medium interaction honeypot for windows. A honeybot creates a safe environment to capture and interact with unsolicited traffic on a network
HTTP Tunneling	HTTHost, HTTPort HTTPort intercepts the ftp request to the localhost and tunnels through it. HTTHost is installed in the remote machine

CHAPTER 13	HACKING WEB SERVERS
Skipfish	Skipfish is an active web application (deployed on a webserver) security reconnaissance tool. It prepares an interactive sitemap for the targeted site by carrying out a recursive crawl and dictionary-based probes.
Httprecon	httprecon is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on its target web server
ID Serve	ID Serve is a simple Internet server identification utility. 1. HTTP Server Identification 2. Non-HTTP Server Identification 3. Reverse DNS Lookup
Netcat and Telnet	Manual Type of Banner Grabbing
Uniscan	Uniscan is a versatile server fingerprinting tool that not only performs simple commands like ping, traceroute, and nslookup, but also does static, dynamic, and stress checks on a web server. Apart from scanning websites, uniscan also performs automated Bing and Google searches on provided IPs. Uniscan takes all of this data and combines them into a comprehensive report file for the user

CHAPTER - 14	HACKING WEB APPLICATIONS
Whois Lookup Tools	Whois Lookup Tools
DNS Interrogation	Toolset, DNSRecon, DNS Records, Domain Dossier,
WhatWeb	WhatWeb identifies websites and recognizes web technologies, including content management systems (CMS), blogging platforms, statistics and analytics packages, JavaScript libraries, web servers, and embedded devices. It also identifies version numbers, email addresses, account IDs, web framework modules, SQL errors, and more.
OWASP ZAP	Integrated penetration testing tool for finding vulnerabilities in web applications. It offers automated scanners as well as a set of tools that allow you to find security vulnerabilities manually. ZAP provides functionality for a range of skill levels—from developers to testers new to security testing, to security testing specialists.
Load Balancing Tools	Dig, lbd : these tool will detect load balancer in site
Vega	Vega is a web application scanner used to test the security of web applications. It helps you to find and validate SQL Injection, XSS, inadvertently disclosed sensitive information, and other vulnerabilities
Web application vulnerability tools	Vega, WPScan Vulnerability Database, Arachni, Appspider, Uniscan
Weevely	Weevely encodes the payload with a key phrase so that no one else can use it to access the target system

CHAPTER - 15	SQL INJECTION
Sqlmap	Sqlmap automates the process of detecting and exploiting SQL Injection Flaws and taking over the database servers.
Mole	MOLE is SQL injection Exploitation tools that detects the injection and exploits it only by providing a Vulnerable URL and a valid string on the site.
SQL injection tools	Mole, Blisqy, blind-sql-bitshifting, bsql, NoSQLMap
Damn Small SQLi Scanner(DSSS)	It is a fully functional SQL injection vulnerability scanner that supports GET and POST parameters. DSSS scans web applications for various SQL injection vulnerabilities.
SQL injection Detection	Acunetix Web Vulnerability Scanner, Snort, Burp Suite, w3af, Netsparker Web Application Security Scanner

CHAPTER 16	HACKING WIRELESS NETWORK
Technitium MAC address Changer	This allow you to change (spoof) the MAC address of your Network Interface Card (NIC)
Wireshark	Wireshark is a network protocol sniffer and analyzer
Wireless Traffic Analyzers	AirMagnet WiFi Analyzer PRO, SteelCentral Packet Analyzer, Omnipeek Network Protocol Analyzer, CommView for Wi-Fi, Capsa Portable Network Analyzer
Aircrack-ng	Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP, and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless networks.
Wi-Fi hacking tools	Elcomsoft Wireless Security Auditor Portable Penetrator WepCrackGui Pyrit WepAttack

CHAPTER 17	HACKING MOBILE PLATFORM
Kingoroot	Rooting software for android
DroidSheep	It is a simple android tool for web session hijacking (Sidejacking)
FaceSniff	Android app that allow you to sniff and intercept web sessions profiles over the Wi-Fi that your mobiles is connected to. It is possible only when Wi-Fi is not using EAP and over any private network.
Other Android Sniffing Tools	Packet Capture, tPacketCapture, Android PCAP, Sniffer Wicap 2 Demo, TestelDroid
Google Find My Device	Locate a lost android device
iOS	iOS

CHAPTER 17	HACKING MOBILE PLATFORM
Hexxa Plus	It is a Jailbreak Repo Extractor for iOS 13.2 that allow you to install themes,tweaks and apps.
iOS Device Tracking Tools	Find my iPhone, Phonty, SpyBubble, Prey Find my Phone tracker GPS, iHound, FollowMee GPS Location Tracker
Source Code analysis tools	z3A Advanced App Analysis, Kiuwan, Appium, Selendroid, Bitbar, Infer
z3A Advanced App Analysis	It allows to identify security and privacy risks across various iOS and Android application.
Reverse Engineering Tools	ApkTool, Frida, JEB, APK studio, objection, Bytecode Viewer
ApkTool	It is used for reverse engineering third party, closed, binary Android apps. It can decode resources to nearly original form and rebuild them after making some modification.
Low Orbit Ion Cannon (LOIC)	Low Orbit Ion Cannon (LOIC) is an open-source network stress testing and Denial-of-Service (DoS) attack application.
Android Debug Bridge (ADB) Using PhoneSploit	Android Debug Bridge (ADB) is a versatile command-line tool that lets you communicate with a device. ADB facilitates a variety of device actions such as installing and debugging apps, and provides access to a Unix shell that you can use to run several different commands on a device.
Android Hacking Tools	NetCut, drozer, zANTI, Network Spoofer, DroidSheep
Online Android Analyzers	Online Android Analyzers allow you to scan Android APK packages and perform security analyses to detect vulnerabilities in particular apps.
online Android analyzers	Sixo Online APK Analyzer, DeGuard, AVC UnDroid, SandDroid, Apktool, Apprisk Scanner
Quixxi Vulnerability Scanner	Quixxi is an intelligent and integrated end-to-end mobile app security solution. This powerful tool is for developers to protect and monitor any mobile apps in minutes
Android vulnerability scanners	X-Ray, Vulners Scanner, Shellshock Vulnerability Scan, Yaazhini, and Quick Android Review Kit (QARK)
Malwarebytes Security	Malwarebytes is an antimalware mobile tool that provides protection against malware, ransomware, and other growing threats to Android devices. It blocks, detects, and removes adware and malware; conducts privacy audits for all apps; and ensures safer browsing.
mobile antivirus and anti-spyware tools	AntiSpy Mobile, Spyware Detector - Anti Spy Privacy Scanner, iAmNotified - Anti Spy System, and Privacy Scanner (AntiSpy) Free

CHAPTER 18	IoT AND OT HACKING
Shodan	
Wireshark	open-source packet analyzer

CHAPTER 19	CLOUD COMPUTING
Container Vulnerability Scanner	Trivy, Clair, Dadga
Findsubdomains, Robtex	Tools to identify subdomains related to the target buckets
lazys3	lazys3 is a Ruby script tool that is used to brute-force AWS S3 buckets using different permutations. This tool obtains the publicly accessible S3 buckets and also allows you to search the S3 buckets of a specific company by entering the company name.
S3Scanner	Attacker use S3Scanner to identify open S3 buckets of cloud services such as Amazon Web services and retrieve their content for some malicious purpose.
S3 bucket enumeration tools	S3Inspector, s3-buckets-bruteforcer, Mass3, Bucket Finder, s3recon
GCPBucketBrute	It is a script based tool that allow attacker to enumerate google storage bucket, detemine what kind of access they have for them, and check whether they can be privilege escalated
AWS pwn	It is a AWS hacking tool that includes various automated scripts for hacking phase such as reconnaissance, escalating privilege, maintaining access, clearing tracks
AWS command line interface (CLI)	It is a unified tool for managing AWS services. With just one tool to download and configure, you can control multiple AWS services from the command line and automate them through scripts.

CHAPTER 20	CRYPTOGRAPHY
Onlinemd5	Onlinemd5 generates and checks file integrity using secure time-proven algorithms such as MD5, SHA-1, and SHA-256. One can create checksums (digital fingerprints) of files and verify their integrity using this online tool.
MD5 Calculator	MD5 Calculator is a simple application that calculates the MD5 hash of a given file.
MD5 and MD6 hash calculators	MD6 Hash Generator, All Hash Generator, HashCalc
Hash Calculators for Mobile	Hash Tools, Hash Droid, MD5 Checker, Hash Checker, hashr - checksum & Hash Digest Calculator, Hash Calculator, Hash Calc
HashCalc	HashCalc enables you to compute multiple hashes, checksums, and HMACs for files, text, and hex strings. It supports the Secure Hash Algorithm family: MD2, MD4, MD5, SHA1, SHA2 (SHA256, SHA384, SHA512), RIPEMD160, PANAMA, TIGER, CRC32, ADLER32, and the hash used in the peer-to-peer file sharing applications, eDonkey and eMule.
HashMyFiles	HashMyFiles is a small utility that allows you to calculate the MD5 and SHA1 hashes of one or more files in your system
Cryptography Tools	BCTextEncoder, AcCrypt, Microsoft Cryptography Tools, Concealer, CryptoForge, SensiGuard, Advanced Encryption Package 2017, Challenger
CryptoForge	CryptoForge is a file encryption software for personal and professional data security. It allows you to protect the privacy of sensitive files, folders, or email messages by encrypting them with strong encryption algorithms.

CHAPTER 20	CRYPTOGRAPHY
BCTextEncoder	Encrypts confidential text in your message Uses strong symmetric and public-key algorithms for data encryption
Cryptography Tools for Mobile	Secret Space Encryptor, Secure Everything, Crypto, Encrypt File Free, EgoSecure Encryption Anywhere , Cipher Sender
Some popular CAs	Comodo, IdenTrust, Symantec, GoDaddy
OpenSSL	OpenSSL is an open-source cryptography toolkit implementing SSL v2/v3 and TLS v1 network protocols and the related cryptography standards required by them
additional cryptography toolkits	Keyczar, wolfSSL, AES Crypto Toolkit, RELIC, PyCrypto
Email Encryption Tools	RMail, Virtru, ZixMail, Egress Secure Email and File Transfer, Proofpoint Email Protection, Paubox
RMail	RMail is an email security tool that provides open tracking, delivery proof, email encryption, electronic signatures, large file transfer functionality, etc.
Disk Encryption Tools	VeraCrypt , Symantec Drive Encryption, BitLocker Drive Encryption
VeraCrypt	VeraCrypt is a software for establishing and maintaining an on-the-fly-encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted immediately before it is saved and decrypted immediately after it is loaded, without any user intervention.
Symantec Drive Encryption	Symantec Drive Encryption provides full disk encryption for all data (user files, swap files, system files, etc.) on desktops, laptops, and removable media
BitLocker Drive Encryption	BitLocker provides offline data and operating system protection for your computer . It helps protect your data from theft or unauthorized viewing by encrypting the entire Windows volume
Rohos	Rohos Disk Encryption creates hidden and password-protected partitions on a computer or USB flash drive, and password protects/locks access to your Internet applications.
Additional disk encryption tools	FinalCrypt, Seqrite Encryption Manager, FileVault, Gillsoft Full Disk Encryption, Rohos Disk Encryption
Cryptanalysis Tools	CrypTool, Cryptosense, RsaCtfTool, Msieve, Cryptol , CryptoBench
CrypTool	CrypTool is a e-learning program in the area of cryptography and cryptanalysis It consists of e-learning software (CT1, CT2, JCT, and CTO)
Online MD5 Decryption Tools	MD5 Decoder, CrackStation, md5hashing, MD5 Decryption