**TOOLS**

**MOD2- Footprinting**

* **Netcraft:** Netcraft provides Internet security services, including anti-fraud and anti-phishing services, application testing, and PCI scanning.
* **Sublist3r:** Sublist3r is a Python script designed to enumerate the subdomains of websites using OSINT.
* **Harvester:** Harvester is a tool designed to be used in the early stages of a penetration test. It is used for open-source intelligence gathering and helps to determine a company's external threat landscape on the Internet.
* **Shodan:** It is a computer search engine that searches the Internet for connected devices It helps attackers to keep track of all the devices on the target network that are directly accessible from the Internet.
* **Censys:** It monitors the infrastructure and discovers unknown assets anywhere on the Internet. It provides a full view of every server and device exposed to the Internet. Attackers use this tool to monitor the target IT infrastructure to discover various devices connected to the Internet.
* **Sherlock:** attackers use Sherlock to search a vast number of social networking sites for a target username. This tool helps the attacker to locate the target user on various social networking sites along with the complete URL.
* **HTTrack:** It is an offline browser utility. It downloads a website from the Internet to a local directory and recursively builds all the directories including HTML, images, and other files from the web server on another computer.
* **Social Searcher:** It allows attackers to search for content in social networks in real time and provides deep analytics data.
* **eMailTrackerPro:** tracks the email.
* **Infoga:** Infoga is a tool used for gathering email account information (IP, hostname, country, etc.) from different public sources (search engines, pgp key servers, and Shodan), and it checks if an email was leaked using the haveibeenpwned.com API.
* **Maltego:** It is a program that can be used to determine the relationships and real-world links between people, groups of people, organizations, websites, Internet infrastructure, documents, etc.
* **Recon-ng:** It is a web reconnaissance framework with independent modules for database interaction that provides an environment in which open-source web-based reconnaissance can be conducted.
* **FOCA:** Fingerprinting Organizations with Collected Archives (FOCA) is a tool used mainly to find metadata and hidden information in the documents that its scans.
* **OSR Framework:** It includes applications related to username checking, DNS lookups, information leaks research, deep web search, and regular expression extraction.
* **OSINT Framework:** It is an open-source intelligence gathering framework that helps security professionals in performing automated footprinting and reconnaissance, OSINT research, and intelligence gathering.
* **BillCipher:** It is an information gathering tool for a website or IP address. It can work on any operating system that supports Python 2, Python 3, and Ruby.

**MOD3- Scanning Networks**

**Scanning Tools**

* **Nmap ("Network Mapper"):** It is a security scanner for network exploration and hacking. It allows you to discover hosts, ports, and services on a computer network, thus creating a "map" of the network.
* **Hping2/Hping3:** It is a command-line-oriented network scanning and packet crafting tool for the TCP/IP protocol that sends ICMP echo requests and supports TCP, UDP, ICMP, and raw-IP protocols. It performs network security auditing, firewall testing, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing.
* **Metasploit:** It is an open-source project that provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing. It provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
* **NetScanTools Pro:** It is an investigation tool that allows you to troubleshoot, monitor, discover, and detect devices on your network. Using this tool, you can easily gather information about the local LAN as well as Internet users, IP addresses, ports.
* **IP Scanner:** It for iOS scans your local area network to determine the identity of all its active machines and Internet devices.
* **Fing:** It is a mobile app for Android and iOS that scans and provides complete network information, such as IP address, MAC address, device vendor, and ISP location. It allows attackers to discover all devices connected to a Wi-Fi network along with their IP and MAC address as well as the name of the vendor/device manufacturer.
* **Network Scanner:** It is an Android mobile application that allows attackers to identify the active host in the range of possible addresses in a network.

**Ping Sweep Tools**

* **Angry IP scanner:** It is an IP address and port scanner. It can scan IP addresses in any range as well as any of their ports. It pings each IP address to check if it is alive.
* SolarWinds Engineer’s Toolset
* NetScanTools Pro
* Colasoft Ping Tool
* Visual Ping Tester
* OpUtils

**Proxy Tools**

* **Proxy Switcher:** It allows attackers to surf the Internet anonymously without disclosing their IP address.
* **CyberGhost VPN:** It hides the attacker's IP and replaces it with a selected IP, allowing him or her to surf anonymously and access blocked or censored content.
* **Shadowsocks:** It is a high-performance, cross-platform secured socks5 proxy for mobiles. It adopts bleeding-edge techniques with asynchronous I/O and event-driven programming.
* **ProxyDroid:** It is an app that can help you to set the proxy (http/socks4/socks5) on your Android devices. It supports HTTP/HTTPS/SOCKS4/SOCKS5 proxy and supports basic/NTLM/NTLMv2 authentication methods.

**Anonymizers**

* **Whonix:** It is a desktop OS designed for advanced security and privacy. It mitigates the threat of common attack vectors while maintaining usability.
* **Psiphon:** It is an open-source anonymizer software that allows attackers to surf the Internet through a secure proxy.
* **Orbot:** It is a proxy app that allows other apps to use the Internet more securely. It uses Tor to encrypt Internet traffic and then hides it by bouncing through a series of computers around the world.

**MOD4- Enumeration**

* **NetBIOS Enumerator:** It is an enumeration tool that shows how to use remote network support and to deal with some other web protocols, such as SMB.
* **Nmap:** Attackers use the Nmap Scripting Engine (NSE) for discovering NetBIOS shares on a network. The nbstat script of NSE allows attackers to retrieve the target’s NetBIOS names and MAC addresses.
* **Snmpcheck:** It is an open-source tool distributed under the GNU General Public License (GPL). Its goal is to automate the process of gathering information on any device with SNMP support.
* **SoftPerfect Network Scanner:** It can ping computers, scan ports, discover shared folders, and retrieve practically any information about network devices via Windows Management Instrumentation (WMI), SNMP, Hypertext Transfer Protocol (HTTP), SSH, and PowerShell.
* **Softerra LDAP Administrator:** It is an LDAP administration tool that works with LDAP servers such as Active Directory, Novell Directory Services, and Netscape/iPlanet. It browses and manages LDAP directories.
* **PRTG Network Monitor (NTP):** It monitors all systems, devices, traffic, and applications of IT infrastructure by using various technologies such as SNMP, WMI, and SSH.
* **RPCScan:** It communicates with RPC services and checks misconfigurations on NFS shares.
* **SuperEnum:** It includes a script “./superenum” that performs the basic enumeration of any open port.
* **NetScanTools Pro’s:** SMTP Email Generator tool tests the process of sending an email message through an SMTP server. Attackers use NetScanTools Pro for SMTP enumeration and extract all the email header parameters, including confirm/urgent flags.
* **smtp-user-enum:** It is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN, and RCPT TO commands.
* **LDNS-walk:** It enumerates the DNSSEC zone and obtains results on the DNS record files.
* **DNSRecon:** It is a zone enumeration tool that assists users in enumerating DNS records such as A, AAAA, and CNAME. It also performs NSEC zone enumeration to obtain DNS record files of a target domain.
* **PortQry utility:** It reports the port status of TCP and UDP ports on a selected target. Attackers can use the PortQry tool to perform TFTP enumeration. This utility reports the port status of target TCP and UDP ports on a local or remote computer.

**MOD5- Vulnerability Analysis**

* **Qualys VM:** It is a cloud-based service that gives immediate, global visibility into where IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps to continuously identify threats and monitor unexpected changes in a network before they turn into breaches.
* **Nessus Professional:** It is an assessment solution for identifying vulnerabilities, configuration issues, and malware that attackers use to penetrate networks. It performs vulnerability, configuration, and compliance assessment.
* **GFI LanGuard:** It scans for, detects, assesses, and rectifies security vulnerabilities in a network and its connected devices. This is done with minimal administrative effort. It scans the operating systems, virtual environments, and installed applications through vulnerability check databases.
* **OpenVAS:** It is a framework of several services and tools that offer a comprehensive and powerful vulnerability scanning and vulnerability management solution. The framework is part of Greenbone Network’s commercial vulnerability management solution. The actual security scanner is accompanied by a regularly updated feed of Network Vulnerability Tests (NVTs), over 50,000 in total.
* **Nikto:** It is an Open Source (GPL) web server scanner that performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files or programs, checks for outdated versions of over 1250 servers, and checks for version specific problems on over 270 servers.
* **Vulners scanner:** It is an android application that performs passive vulnerability detection based on a software version’s fingerprint.
* **SecurityMetrics Mobile:** It is a mobile defense tool that helps to identify mobile device vulnerabilities to protect customers’ sensitive data. It helps to avoid threats that originate from mobile malware, device theft, Wi-Fi network connectivity, data entry, etc.

**MOD6- System Hacking**

**Password Recovery Tools**

* **Elcomsoft Distributed Password Recovery application**: It allows attackers to break complex passwords, recover strong encryption keys, and unlock documents in a production environment.
* **Hashcat**
* **PCUnlocker**
* **pwdump7:** It is an application that dumps the password hashes (one-way functions orOWFs) from NT’s SAM database. pwdump extracts LM and NTLM password hashes of local user accounts from the Security Account Manager (SAM) database.

**Password Cracking Tools**

* **L0phtCrack:** It is a tool designed to audit passwords and recover applications. It recovers lost Microsoft Windows passwords with the help of a dictionary, hybrid, rainbow table, and brute-force attacks, and it also checks the strength of the password.
* **Ophcrack:** It is a Windows password-cracking tool that uses rainbow tables for cracking passwords. It comes with a graphical user interface (GUI) and runs on different OSs such as Windows, Linux/UNIX, etc.
* **RainbowCrack:** It cracks hashes with rainbow tables, using a time–memory trade-off algorithm. A traditional brute-force cracker cracks hash in a manner that is different from that followed by a time–memory-tradeoff hash cracker.
* **John the Ripper**
* **THC-Hydra**
* **Medusa**

**Tools to Detect LLMNR/NBT-NS Poisoning**

* **Vindicate:** It is an LLMNR/NBNS/mDNS spoofing detection toolkit for network administrators. Security professionals use this tool to detect name service spoofing. This tool helps them to quickly detect and isolate attackers on their network.
* **got-responded:** It helps security professionals to check for LLMNR/NBT-NS spoofing. This tool starts in the default mode and checks for both LLMNR and NBT-NS spoofing but does not send fake SMB credentials.
* **Respounder:** It detects the presence of a responder in the network. Security professionals use this tool to identify compromised machines before hackers exploit password hashes. This tool also helps security professionals to detect rogue hosts running responder on public Wi-Fi networks.

**Buffer Overflow Detection Tools**

* **OllyDbg:** It is a 32-bit assembler-level analyzing debugger for Microsoft® Windows®. Its emphasis on binary code analysis makes it particularly useful when the source is unavailable. It debugs multithread applications and attaches to running programs.
* Veracode
* Flawfinder
* Kiuwan
* Splint
* BOVSTT

**Privilege Escalation Tools**

* **BeRoot:** It is a post-exploitation tool to check common misconfigurations to find a way to escalate privilege.
* **linpostexp tool:** It obtains detailed information on the kernel, which can be used to escalate privileges on the target system.

**Tools for Defending against DLL and Dylib Hijacking**

* **Dependency Walker:** It is useful for troubleshooting system errors related to loading and executing modules. It detects many common application problems, such as missing modules, invalid modules, import/export mismatches, circular dependency errors, etc.
* **Dylib Hijack Scanner (DHS):** It is a simple utility that will scan your computer for applications that are either susceptible to dylib hijacking or have been hijacked.

**Tools for Detecting Spectre and Meltdown Vulnerabilities**

* **InSpectre:** It examines and discloses any Windows system’s hardware and software capability to prevent Meltdown and Spectre attacks. Detecting these vulnerabilities at an early stage helps security professionals to update system hardware, its BIOS, which reloads the updated processor firmware, and its OS to use the new processor features.
* **Spectre & Meltdown Checker:** It is a shell script to determine whether a system is vulnerable against various “speculative execution” CVEs. For Linux systems, the script will detect mitigations, including backported non-vanilla patches, regardless of the advertised kernel version number or the distribution.

**Tools for Executing Applications**

* **RemoteExec:** It remotely installs applications, executes programs/scripts, and updates files and folders on Windows systems throughout the network. This allows an attacker to modify the registry, change local admin passwords, disable local accounts, and copy/ update/delete files and folders.
* **Pupy**
* **PDQ Deploy**
* **Dameware Remote Support**
* **ManageEngine Desktop Central**
* **PsExec**

**Keyloggers**

* **KeyGrabber hardware** **keylogger:** It is an electronic device capable of capturing keystrokes from a PS/2 or USB keyboard. It comes in various forms, such as KeyGrabber USB, KeyGrabber PS/2, and KeyGrabber Nano Wi-Fi.
* **KeyCarbon**
* **Keyllama Keylogger**
* **Keyboard logger**
* **KeyGhost**
* **Spyrix Keylogger Free:** It is used for remote monitoring on a computer that includes recording of keystrokes, passwords, and screenshots. This keylogger is perfectly hidden from antivirus, anti-rootkit, and anti-spyware software.
* **REFOG Personal Monitor**
* **Elite Keylogger**
* **StaffCop Standard**
* **Spytector**
* **Refog Mac Keylogger:** It provides undetected surveillance and records all the keystrokes on the computer.

**Spyware Tools**

* **Spytech SpyAgent:** It is computer spy software that allows you to monitor everything users do on your computer—in total secrecy. SpyAgent provides a large array of essential computer monitoring features, as well as website, application, and chat client blocking, logging scheduling, and remote delivery of logs via email or FTP.
* **Power Spy:** It is PC-user activity-monitoring software. It runs and performs monitoring secretly in the background of a computer system. It logs all users on the system and users will not be aware of its existence.

**Desktop and Child-Monitoring Spyware**

* **ACTIVTrak**
* **Veriato Cerebral**
* **NetVizor**
* **SoftActivity Monitor**
* **SoftActivity TS Monitor**

**USB Spyware**

* **USB Analyzer**
* **USB Monitor**
* **USBDeview**
* **Advanced USB Port Monitor**
* **USB Monitor Pro**

**Audio Spyware**

* **Spy Voice Recorder**
* **Spy Audio Listening Device**
* **Spy USB Voice Recorder**
* **Voice Activated Flash Drive Voice Recorder**
* **Audio Spyware Snooper**

**Video Spyware**

* **Movavi Video Editor**
* **Free2X Webcam Recorder**
* **iSpy**
* **NET Video Spy**
* **Eyeline Video Surveillance Software**

**Cellphone Spyware**

* **Phone Spy**
* **XNSPY**
* **iKeyMonitor**
* **OneSpy**
* **TheTruthSpy**

**GPS Syware**

* **Spyera**
* **mSpy**
* **MOBILE SPY**
* **MobiStealth**
* **FlexiSPY**

**Anti-Keyloggers**

* **Zemana AntiLogger:** It is a software application that blocks attackers. It detects any attempts to modify your computer’s settings, record your activities, hook to your PC’s sensitive processes, or inject malicious code into your system.
* **GuardedID**
* **KeyScrambler**
* **Oxynger KeyShield**
* **Ghostpress**
* **SpyShelter Free Anti-Keylogger**

**Anti-Spyware**

* **SUPERAntiSpyware:** It is a software application that can detect and remove spyware, adware, Trojan horses, rogue security software, computer worms, rootkits, parasites, and other potentially harmful software applications.
* **Kaspersky Internet Security 2019**
* **SecureAnywhere Internet Security Complete**
* **adaware antivirus free**
* **MacScan**
* **Norton AntiVirus Plus**

**Rootkits**

* **LoJax:** It is a type of UEFI rootkit that is widely used by attackers to perform cyber-attacks. LoJax is created to inject malware into the system and is automatically executed whenever the system starts up. It exploits UEFI, which acts as an interface between the OS and the firmware.
* **Scranos:** It is a trojanized rootkit that masquerades as cracked software or a legitimateapplication, such as anti-malware, a video player, or an ebook reader, to infect systems and perform data exfiltration that damages the reputation of the target and steals intellectual property.
* **Horse Pill:** It is a proof of concept of a ramdisk-based containerizing rootkit. It resides inside “initrd,” and before the actual init starts running, it puts it into a mount and PID namespace that allows it to run covert processes and storage.
* **Necurs:** It is a kernel-mode driver component that can be used by an attacker (or added as a component to another malicious program) to perform unauthorized actions to take control of an OS, without alerting the system’s security mechanisms.

**Anti-Rootkits**

* **GMER:** It is an application that helps security professionals to detect and remove rootkits by scanning processes, threads, modules, services, files, disk sectors (MBR), ADSs, registry keys, driver hooking – SSDT, IDT, and IRP calls, and inline hooks.
* **Stinger**
* **Avast Free Antivirus**
* **TDSSKiller**
* **Malwarebytes Anti-Rootkit**
* **Rootkit Buster**

**NTFS Stream Detectors**

* **Stream Armor:** It is a tool used to discover hidden ADSs and clean them completely from your system. Its advanced auto analysis, coupled with an online threat verification mechanism, helps you eradicate any ADSs that may be present.
* **Stream Detector**
* **GMER**
* **ADS Manager**
* **ADS Scanner**
* **Streams**

**Whitespace Steganography**

* **Snow:** It is a program for concealing messages in text files by appending tabs and spaces to the ends of lines, and for extracting messages from files containing hidden messages. The user hides the data in the text file by appending sequences of up to seven spaces, interspersed with tabs.

**Image Steganography**

* **Openstego**
* **QuickStego**
* **SSuite Picsel**
* **CryptaPix**
* **gifshuffle**
* **PHP-Class Stream Steganography**

**Document Steganography**

* **StegoStick:** It is a steganographic tool that allows attackers to hide any file in any other file. It is based on image, audio, or video steganography, which hides any file or message in an image, audio/video or any other format.
* **StegJ**
* **Office XML**
* **SNOW**
* **Data Stash**
* **Texto**

**Video Steganography**

* **OmniHide PRO:** It allows you to hide any secret file within an innocuous image, video, music file, etc.
* **RT Steganography**
* **StegoStick**
* **OpenPuff**
* **MSU StegoVideo**

**Audio Steganography**

* **DeepSound:** It allows you to hide any secret data in audio files (WAV and FLAC). It also allows you to extract secret files directly from audio CD tracks. In addition, it can encrypt secret files, thereby enhancing security.
* **BitCrypt**
* **StegoStick**
* **MP3Stego**
* **QuickCrypto**
* **Spectrology**

**Folder Steganography**

* **GiliSoft File Lock Pro:** It restricts access to files, folders, and drivers by locking, hiding, or password-protecting them. Attackers can thus use this tool for these purposes. With this program, nobody can access or destroy the attacker’s data without a password.
* **Folder Lock**
* **Hide Folders 5**
* **Invisible Secrets 4**
* **Max Folder Secure**
* **QuickCrypto**

**Mobile Steganography**

* **Steganography Master:** It helps in hiding secret messages inside a photo. You can encode your message in a picture, then save or send it to any mobile user.
* **Stegais:** It can hide a message in a selected image from the photo library or in a photo taken by the camera.
* **SPY PIX**
* **Pixelknot: Hidden Messages**
* **Pocket Stego**

**Steganalysis**

* **zsteg tool:** It is used to detect stegano-hidden data in PNG and BMP image files.
* **StegoVeritas**
* **Stegextract**
* **StegoHuntTM**
* **Steganography Studio**
* **Virtual Steganographic Laboratory**

**Track-Covering Tools**

* **CCleaner:** It is a system optimization, privacy, and cleaning tool. It allows attackers to remove unused files and cleans traces of Internet browsing details from the target PC. With this tool, an attacker can very easily erase his/her tracks.
* **DBAN**
* **Privacy Eraser**
* **Wipe**
* **BleachBit**
* **ClearProg**

**MOD8- Sniffing**

* **Wireshark:** It lets you capture and interactively browse the traffic running on a computer network. This tool uses WinPcap to capture packets on its own supported networks. It captures live network traffic from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, and FDDI networks.
* **SteelCentral Packet Analyzer:** It provides a graphical console for high-speed packet analysis. This tool comes integrated with Riverbed AirPcap adapters to analyze and troubleshoot 802.11 wireless networks.
* **Capsa Network Analyzer:** It is a network-monitoring tool that captures all the data transmitted over the network and provides a wide range of analysis statistics in an intuitive and graphic way. The tool helps to analyze and troubleshoot the problem that has occurred (if any) in the network.
* **OmniPeek Network Analyzer:** It provides real-time visibility and expert analysis of eachpart of the target network. This tool will analyze, drill down, and fix performance bottlenecks across multiple network segments.
* **Observer Analyzer**
* **PRTG Network Monitor**
* **SolarWinds Deep Packet Inspection and Analysis**
* **Xplico**
* **Colasoft Packet Builder**
* **Sniffer Wicap:** It is a mobile network packet sniffer for ROOT ARM droids. It works on rooted Android mobile devices.
* **FaceNiff:** It is an Android app that can sniff and intercept web session profiles over a Wi-Fi connection to a mobile. This app works on rooted Android devices. The Wi-Fi connection should be over open, WEP, WPA-PSK, or WPA2-PSK networks while sniffing the sessions.
* **Packet Capture:** It is a network traffic sniffer app with SSL decryption. It is a powerful debugging tool, especially when developing an app.

**Promiscuous Detection Tools**

* **Nmap’s NSE script:** It allows you to check whether a system on a local Ethernet has its network card in promiscuous mode.
* **NetScanTools Pro:** It includes the Promiscuous Mode Scanner tool to scan your subnet for network interfaces listening for all Ethernet packets in promiscuous mode.

**MOD9- Social Engineering**

**Phishing Tools**

* **ShellPhish:** It is a phishing tool used to phish user credentials from various social networking platforms such as Instagram, Facebook, Twitter, and LinkedIn. It also displays the victim system’s public IP address, browser information, hostname, geolocation, and other information.
* **BLACKEYE**
* **PhishX**
* **Modlishka**
* **Trape**
* **Evilginx**

**Detecting Insider Threats**

**Deterrence Control**

* **DLP Tools:**
* **Symantec Data Loss Prevention**
* **SecureTrust Data Loss Prevention**
* **Check Point Data Loss Prevention**
* **IAM Tools:**
* **SailPoint IdentityIQ**
* **RSA SecurID Suite**
* **Core Access Assurance Suite**

**Detection Control**

* **IDS/IPS Tools:**
* **Check Point IPS Software Blade**
* **IBM Security Network Intrusion Prevention System**
* **AlienVault Unified Security Management**
* **Log Management Tools:**
* **SolarWinds Security Event Manager**
* **Splunk**
* **Loggly**
* **SIEM Tools:**
* **ArcSight ESM**
* **LogRhythm NextGen SIEM Platform**
* **SolarWinds Log & Event Manager**

**Anti-Phishing Tool**

* **Netcraft anti-phishing community:** It is a giant neighborhood watch scheme, empowering the most alert and most expert members to defend everyone within the community against phishing attacks.
* **PhishTank:** It is a collaborative clearinghouse for data and information about phishing on the Internet. It provides an open API for developers and researchers to integrate anti-phishing data into their applications.

**Social Engineering Tools**

* **Social-Engineer Toolkit (SET):** It is an open-source Python-driven tool aimed at penetration testing via social engineering. It is a generic exploit designed to perform advanced attacks against human elements to compromise a target and make them offer sensitive information.
* **SpeedPhish Framework (SPF)**
* **Gophish**
* **King Phisher**
* **LUCY**
* **MSI Simple Phish**
* **OhPhish:** It is a web-based portal for testing employees’ susceptibility to social engineering attacks. It is a phishing simulation tool that provides the organization with a platform to launch phishing simulation campaigns on its employees.

**MOD10- Denial-of-Service**

**DoS/DDoS Attack Tools**

* **Slowloris:** It is a DDoS attack tool used to perform layer-7 DDoS attacks to take down web infrastructure.
* **High Orbit Ion Cannon (HOIC):** It is a network stress and DoS/DDoS attack application written in 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.
* **Low Orbit Ion Cannon (LOIC**): is a network stress testing and DoS attack application. LOIC attacks can be called application-based DOS attacks because they primarily target web applications. LOIC can be used on a target site to flood the server with TCP packets, UDP packets, or HTTP requests with the intention of disrupting the service.
* **XOIC:** Itis a DOS attacking tool that performs a DOS attack on any server with an IP address, a user-selected port and a user-selected protocol.
* **HULK**
* **Tor’s Hammer**
* **Slowloris**
* **PyLoris**
* **R-U-Dead-Yet**
* **AnDOSid:** It allows the attacker to simulate a DoS attack (an HTTP POST flood attack to be precise) and DDoS attack on a web server from mobile phones.
* **Packets Generator app:** It allows attackers to generate network traffic including TCP SYN, UDP, and ICMP ping traffic.

**DoS/DDoS honeypot tools:**

* **KFSensor:** It is a Windows-based honeypot intrusion detection system (IDS). It acts as a honeypot designed to attract and detect hackers and worms by simulating vulnerable system services and Trojans.
* **SSHHiPot**
* **Artillery**

**DoS/DDoS Protection Tools**

* **FortiDDoS:** It provides comprehensive protection against DDoS attacks. It helps protect Internet infrastructure from threats and service disruptions by surgically removing network and application layer DDoS attacks while letting legitimate traffic flow without being impacted.
* **DDoS Protector:** It Check Point DDoS Protector blocks DDoS attacks with multi-layered protection.
* **Terabit DDoS Protection System (DPS):** It is a solution for the detection and subsequent treatment of DDoS attacks. Terabit DPS helps ensure the maximum availability of a network and eliminates any disruptions caused by DoS/DDoS attacks.
* **A10 Thunder Threat Protection System (TPS):** It ensures reliable access to key network services by detecting and blocking external threats such as DDoS and other cyber-attacks before they escalate into costly service outages.
* **Imperva Incapsula DDoS protection:** It quickly mitigates any size attack without disrupting legitimate traffic or increasing latency. It is designed to provide multiple DDoS protection options and supports unicast and anycast technologies to power a many-to-many defense methodology.
* **Anti DDoS Guardian**
* **DOSarrest’s DDoS protection service**
* **DDoS-GUARD**
* **Cloudflare**
* **F5**
* **Akamai provides DDoS protection for enterprises:** It regularly targeted by DDoS attacks. Akamai Kona Site Defender delivers multi-layered defense that effectively protects websites and web applications against the increasing threat, sophistication, and scale of DDoS attacks.
* **Kaspersky DDoS Protection Tool**
* **Stormwall PRO**
* **Corero Network Security**
* **Nexusguard**
* **BlockDoS**

**MOD11- Session Hijacking**

* **Burp Suite:** It is an integrated platform for the security testing of web applications. It allows attackers to inspect and modify traffic between a browser and target application.
* **OWASP ZAP**
* **bettercap**
* **netool toolkit**
* **WebSploit Framework**
* **Sslstrip**
* **DroidSheep tool:** It is used for session hijacking on Android devices connected to a common wireless network. It obtains the session ID of active users on the Wi-Fi network and uses it to access a website as an authorized user.
* **DroidSniff:** It is an Android app for security analysis in wireless networks that can capture Facebook, Twitter, LinkedIn, and other accounts. This tool is used for testing the security of user accounts. It identifies the poor security properties of network connections without encryption.
* **FaceNiff:** It is an Android app that allows a user to sniff and intercept web-session profiles over the WiFi network that the user’s mobile device is connected to.

**Session Hijacking Detection Tools**

* **AlienVault Unified Security Management (USM):** It offers powerful threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments.
* **Wireshark:** It allows users to capture and interactively browse the traffic on a network. This tool uses Winpcap to capture packets. Therefore, it can only capture packets on the networks supported by Winpcap.
* **Check Point IPS Software Blade**
* **LogRhythm**
* **SolarWinds Log & Event Manager**
* **IBM Security Network Intrusion Prevention System**

**Session Hijacking Prevention Tools**

* **Checkmarx CxSAST:** It is a unique source-code analysis solution that provides tools foridentifying, tracking, and repairing technical and logical flaws in source code, such as security vulnerabilities, compliance issues, and business logic problems.
* **Fiddler:** It is used for performing web-application security tests such as the decryption of HTTPS traffic and manipulation of requests using an MITM decryption technique. Fiddler is a web debugging proxy that logs all HTTP(S) traffic between a computer and the Internet.
* **Nessus**
* **Netsparker**
* **Wapiti**
* **WebWatchBot**

**MOD12- Evading IDS, Firewalls, and Honeypots**

**Intrusion Detection Tools**

* **Snort:** It is an open-source network intrusion detection system capable of performing real-time traffic analysis and packet logging on IP networks. It can perform protocol analysis and content searching/matching, and it is used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and OS fingerprinting attempts.
* **Suricata:** It is a robust network threat detection engine capable of real-time intrusion detection (IDS), inline intrusion prevention (IPS), network security monitoring (NSM), & offline pcap processing. It inspects network traffic using powerful and extensive rules and a signature language, and it provides powerful Lua scripting support for detection of complex threats.
* **AlienVault® OSSIMTM:** It is an open-Source Security Information and Event Management (SIEM), provides you with a feature-rich open-source SIEM complete with event collection, normalization, and correlation.
* **SolarWinds Security Event Manager**
* **OSSEC**
* **BroIDS/Zeek IDS**
* **Zimperium’s zIPSTM:** It is a mobile intrusion prevention system app that provides comprehensive protection for iOS and Android devices against mobile network, device, and application cyber-attacks. It can detect both known and unknown threats by analyzing the behavior of your mobile device.
* **Wifi Inspector:** It allows you to find all the devices connected to the network (via both wired and Wi-Fi connections, including consoles, TVs, PCs, tablets, and phones); it gives All relevant data such as the IP addresses, manufacturer names, device names, and MAC addresses of connected devices.
* **Wifi Intruder Detect:** It helps to find security leaks in the Wi-Fi network Internet connection. It allows you to detect an intruder who is accessing the network, Wi-Fi, or Internet connection without your consent.

**Intrusion Prevention Tools**

* **AlienVault USM:** It can perform threat detection, incident response, and compliance management across cloud, on-premises, and hybrid environments.

**Firewall Tools**

* **ZoneAlarm Free Firewall 2019:** It prevents attackers and intruders from accessing your system. It manages and monitors all incoming and outgoing traffic and shields the network.
* **ManageEngine Firewall Analyzer:** It is an agent-less log analytics and configurationmanagement software that helps network administrators to understand how the bandwidth is being used in their network.
* **pfSense**
* **Sophos XG Firewall**
* **Comodo Firewall**
* **Palo Alto Network Wildfire**
* **Mobiwol NoRoot Firewall:** It helps to take control of mobile apps, easily allow/block app connectivity, and block background app activity. It generates alerts when new apps access the Internet.
* **Mobile Privacy Shield’s Privacy Advisor:** It monitors application permissions, sorting them into three categories by the privacy-risk level.
* **NetPatch Firewall:** It is a full-featured advanced Android no-root firewall. It can be used tofully control a mobile device network. Using NetPatch Firewall, you can create network rules based on apps, IP addresses, domain names, etc.

**Honeypot Tools**

* **KFSensor:** It is a host-based IDS that acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans.
* **SPECTER:** It is a honeypot or deception system. It simulates a complete system and provides an appealing target to lure hackers away from production systems. It offers typical Internet services such as SMTP, FTP, POP3, HTTP, and TELNET, which appear perfectly normal to attackers.

**IDS/Firewall Evading Tools**

* **Traffic IQ Professional:** It is a tool that audits and validates the behavior of security devices by generating the standard application traffic or attack traffic between two virtual machines.
* **Nmap**
* **Metasploit**
* **Inundator**
* **IDS-Evasion**
* **Hyperion-2.0**

**Packet Fragment Generator Tools**

* **Colasoft Packet Builder:** It is used to create custom network packets and fragmenting packets. Attackers use this tool to create custom malicious packets and fragment them such that firewalls cannot detect them.
* **CommView**
* **NetScanTools Pro**
* **Ostinato**
* **WAN Killer**
* **WireEdit**

**Honeypot Detection Tools**

* **Send-Safe Honeypot Hunter:** It is a tool designed for checking lists of HTTPS and SOCKS proxies for "honey pots.“

**MOD13- Hacking Web Servers**

**Information Gathering tools**

* **WHOis.net:** It is designed to help perform a variety of whois lookup functions. It lets the user perform a domain whois search, whois IP lookup, and whois database search for relevant information on domain registration and availability.

**Web Server Footprinting Tools**

* **Netcraft:** It determines the OS of the queried host by examining in detail the network characteristics of the HTTP response received from the website. Netcraft identifies vulnerabilities in the web server via indirect methods; the fingerprinting of the OS, installed software, and configuration of that software.
* **Netcat:** It is a networking utility that reads and writes data across network connections by using the TCP/IP protocol. It is a reliable “back-end” tool used directly or driven by other programs and scripts. It is also a network debugging and exploration tool.
* **Telnet:** It is a client–server network protocol that is widely used on the Internet or LANs. It provides login sessions for a user on the Internet. A single terminal attached to another computer emulates the session by using Telnet.
* **Httprecon:** It is a tool for advanced web server fingerprinting. This tool performs banner-grabbing attacks, status code enumeration, and header ordering analysis on the target web server and provides accurate web server fingerprinting information.
* **Recon-ng**
* **Uniscan**
* **Nmap**
* **Ghost Eye**
* **Skipfish**

**Website Mirroring**

* **NCollector Studio:** It is a website mirroring tool used to download content from the web to a local computer. This tool enables users to crawl for specific file types, make any website available for offline browsing.
* **HTTrack Web Site Copier**
* **WebCopier Pro**
* **Website Ripper Copier**
* **WebRipper**
* **Cyotek WebCopy**

**Finding Default Credentials of Web Server**

* **cirt.net:** It is a lookup database for default passwords, credentials, and ports.

**Finding Default Content of Web Server**

* **Nikto:** It is a vulnerability scanner used extensively to identify potential vulnerabilities in web applications and web servers.

**Vulnerability Scanning Vulnerability**

* **Acunetix Web Vulnerability Scanner (WVS):** It scans websites and detects vulnerabilities. Acunetix WVS checks web applications for SQL injections, XSS.
* Fortify WebInspect
* Tenable.io
* ImmuniWeb
* Netsparker

**Session Hijacking**

* **Burp Suite:** It is a web security testing tool that can hijack session IDs in established sessions.
* **JHijack**
* **Ettercap**
* **CookieCatcher**
* **Cookie Cadger**

**Web Server Password Hacking**

* **Hashcat:** It is a cracker compatible with multiple OSs and platforms and can perform multi-hash (MD4, 5; SHA – 224, 256, 384, 512; RIPEMD-160; etc.), multi-device password cracking.
* **THC Hydra:** It is a parallelized login cracker that can attack numerous protocols. This tool is a proof-of-concept code that provides researchers and security consultants the possibility to demonstrate how easy it would be to gain unauthorized remote access to a system.
* **Ncrack**
* **Rainbow crack**
* **Wfuzz**
* **Wireshark**

**Web Server Attack Tools**

* **Metasploit:** It is a penetration-testing toolkit, exploit development platform, and research tool that includes hundreds of working remote exploits for various platforms. It performs fully automated exploitation of web servers by abusing known vulnerabilities.
* **Immunity’s CANVAS:** It provides penetration testers and security professionals with hundreds of exploits, an automated exploitation system, and a comprehensive, reliable exploit development framework.
* **THC Hydra**
* **HULK DoS**
* **MPack**
* **w3af**

**Patch Management Tools**

* **GFI LanGuard:** It scans the user’s network automatically as well as installs and manages security and non-security patches.
* **Symantec Client Management Suite**
* **Solarwinds Patch Manager**
* **Kaseya Patch Management**
* **Software Vulnerability Manager**
* **Ivanti Patch for Endpoint Manager**

**Web Server Security Tools**

* **Syhunt Hybrid scanner:** It automates web application security testing and guards the organization’s web infrastructure against web application security threats. Syhunt Dynamic crawls websites and detects XSS, directory transversal problems, fault injection, SQL injection, attempts to execute commands.
* **N-Stalker:** It is a web application security scanner that searches for vulnerabilities to attacks such as clickjacking, SQL injection, and XSS. It allows spider crawling throughout the application and the creation of web macros for form authentication.
* **Netsparker**
* **Burp Suite**
* **Wapiti**
* **WebScarab**
* **WPSec**
* **Tinfoil Security**
* **Skipfish**
* **Detectify**
* **Fortify on Demand**
* **OWASP Zed Attack Proxy (ZAP)**

**Web Server Security Scanners**

* **ScanMyServer:** It is used to find security vulnerabilities in a website or web server. It can generate comprehensive test reports and assist in fixing security problems that might exist in a company’s website or web server.
* **Qualys Community Edition**
* **Observatory**
* **WordPress Security Scan**
* **Web Vulnerability Scanner**
* **Nikto2**

**Web Server Malware Infection Monitoring Tools**

* **QualysGuard Malware Detection:** It allows organizations to proactively scan their websites for malware and provides automated alerts and in-depth reporting to enable prompt identification and resolution.
* **Sucuri SiteCheck**
* **SiteLock SMART**
* **Quttera**
* **Web Inspector**
* **SiteGuarding**

**Web Server Security Tools**

* **Fortify WebInspect:** It is an automated dynamic testing solution that discovers configuration issues as well as identifies and prioritizes security vulnerabilities in running applications.
* **Acunetix Web Vulnerability Scanner**
* **Retina Host Security Scanner**
* **NetIQ Secure Configuration Manager**
* **SAINT Security Suite**
* **Sophos Intercept X for Server**

**Web Server Pen Testing Tools**

* **CORE Impact:** It finds vulnerabilities in an organization’s web server. This tool allows a user to evaluate the security posture of a web server by using the same techniques currently employed by cyber criminals.
* **Immunity CANVAS**
* **Arachni**
* **WebSurgery**

**MOD14- Hacking Web Application**

**REST API Vulnerability Scanning**

* **Astra:** It is used to detect and exploit underlying vulnerabilities in a REST API. Astra can discover and test authentications such login and logout.
* **Fuzzapi**
* **w3af**
* **appspider**
* **Vooki**
* **OWASP ZAP**

**Web Shell Tools**

* **WSO Php Webshell:** It is a web shell that allows attackers to monitor running processes and execute remote commands to download, upload, erase, or edit files.
* **b374k**
* **C99**
* **China Chopper**
* **R57**
* **Pouya ASP Web Shell**

**Gaining Backdoor Access via Web Shell**

* **Weevely:** It is used to develop a backdoor shell and upload it to a target server to gain remote shell access. This tool also helps attackers in performing administrative tasks, maintaining persistence, and spreading backdoors across the target network.

**Web Shell Detection Tools**

* **Web Shell Detector:** It is a PHP/Python-based script that helps in scanning and discovering php/cgi(perl)/asp/aspx shells. It has a web shells signature database that helps in discovering the web shell”.
* **FireEye Network Security**
* **NeoPI**
* **AntiShell Web Shell Hunter**
* **Astra**

**Fuzz Testing Tools**

* **WSFuzzer**
* **WebScarab**
* **Burp Suite**
* **HCL AppScan® Standard**
* **Peach Fuzzer**

**Application Whitelisting and Blacklisting Tools**

* **Apility.io:** It is an anti-abuse API that helps security professionals to know if the IP address, domain, or email of a user is blacklisted. It is a collection of various tools delivered “as a service” to help security professionals.
* **AutoShun**
* **Cisco Umbrella**
* **Alexa Top Sites**
* **APT Groups and Operations**
* **NordVPN**

**Web Application Security Testing Tools**

* **Acunetix WVS:** It checks web applications for SQL injections, cross-site scripting, etc. It includes advanced penetration testing tools, such as HTTP Editor and HTTP Fuzzer.
* **N-Stalker Web App Security Scanner:** It checks for vulnerabilities such as SQL injection, XSS, and other known attacks.
* **Browser Exploitation Framework (BeEF):** It is an open-source penetration testing tool used to test and exploit web applications and browser-based vulnerabilities.
* **Metasploit**
* **PowerSploit**
* **Watcher Web Security Tool**
* **Netsparker**
* **Arachni**

**Web Application Firewalls**

* **dotDefenderTM:** It is a software-based WAF that protects your website from malicious attacks such as SQL injection, path traversal, cross-site scripting, and others that result in website defacement.
* ServerDefender VP
* HCL AppScan® Standard
* Radware’s AppWall
* Qualys WAF
* Barracuda Web Application Firewall

**MOD15- SQL Injection**

**SQL Injection tools**

* **Sqlmap:** It automates the process of detecting and exploiting SQL injection flaws and taking over database servers. It comes with a powerful detection engine, many niche features for advanced penetration testers, and a wide range of switches for database fingerprinting.
* **Mole:** It is an automatic SQL injection exploitation tool. Only by providing a vulnerable URL and a valid string on the site, it can detect the injection and exploit it using the union technique or a Boolean query-based technique.
* **Blisqy:** It exploits time-based blind SQL injection in HTTP-Headers (MySQL/MariaDB). This tool aids web security researchers in finding time-based blind SQL injection on HTTP Headers as well as exploitation of the same vulnerability.
* **blind-sql-bitshifting**
* **bsql**
* **NoSQLMap**
* **SQL Power Injector**
* **Tyrant SQL**
* **SQLi:** It is used to construct malicious queries with untrusted input and perform SQL injection attacks on Android applications.
* **Droidbug SQLi Spyder:** It is an SQL scanner engine that can be used to find and exploit various vulnerabilities such as simple SQL Injection, blind SQL injection, cross-site scripting (XSS)
* **Sqlmapchik:** It is a cross-platform sqlmap GUI for the sqlmap tool. It is primarily intended for use on mobile devices.

Wi-Fi Discovery Tools

* **inSSIDer Plus:** It is a Wi-Fi optimization and troubleshooting tool that scans for wireless networks with the user’s Wi-Fi adapter so that the user can visualize their signal strengths and the channels they are using.
* **NetSurveyor:** It is an 802.11 network discovery tool that gathers information about nearby wireless APs in real time and displays it in different diagnostic views and charts.
* **Wi-Fi Scanner**
* **Acrylic Wi-Fi Home**
* **WirelessMon**
* **Ekahau HeatMapper**

**Mobile-based Wi-Fi Discovery Tools**

* **WiFi Analyzer:** It is a Wi-Fi network optimization tool used to examine surrounding Wi-Fi networks, measure their signal strengths, and identify crowded channels.
* **OpenSignalMaps**
* **Network Signal Info Pro**
* **WiFi Manager**
* **Network Signal Info & WiFi Refresher**
* **WiFi Scanner**

**GPS Mapping Tools**

* **Maptitude mapping software** and a GPS receiver, attackers can track a victim’s location with a portable computer, collect field data, and create new or updated geographic files that mark map features.
* **Skyhook**
* **ExpertGPS**
* **GPS Visualizer**
* **Mapwel**
* **TrackMaker**

**Wi-Fi Hotspot Finder Tools**

* **Wi-Fi Finder:** It is an android mobile application that can be used for finding free or paid public Wi-Fi hotspots online or offline.
* **Homedale::Wi-Fi/WLAN Monitor**
* **Fing - Network Tools**
* **WiFi Finder - Free WiFi Map**
* **WiFi Map**
* **Find Wifi**

**MAC Spoofing Tools**

* **Technitium MAC Address Changer:** It allows a user to change (spoof) the MAC address of their NIC instantly. It has a simple user interface and provides information regarding each NIC in the machine.