***Toooolssssssss:-----***

**KALI LINUX**

Kali Linux is a free, open-source, Debian-based Linux distribution focused on cybersecurity.

It includes hundreds of pre-installed tools for ethical hacking, penetration testing, and forensics.

Widely used by professionals and students, it supports various platforms (VMs, ARM, cloud, etc.).

**OWASP**

OWASP (Open Web Application Security Project) is a non-profit organization promoting secure software.

It offers tools, resources, and documentation to help developers identify and fix security flaws.

Their flagship projects like the OWASP Top 10 guide secure development practices globally.

**OWASP ZAP**

OWASP ZAP (Zed Attack Proxy) is a free tool to detect web app vulnerabilities.

It scans web requests and responses to identify threats like XSS and SQLi.

Great for developers and testers, it integrates easily into CI/CD pipelines.

**METASPLOIT**

Metasploit is an open-source Ruby-based framework used for penetration testing.

It contains modules for exploiting vulnerabilities, post-exploitation, and privilege escalation.

Highly customizable, it supports payloads, exploits, scanners, and more.

**BURP SUITE**

Burp Suite is a powerful tool for testing the security of web applications.

It acts as a proxy to intercept and modify HTTP(S) traffic between browser and server.

It includes modules like Scanner, Repeater, and Intruder for manual and automated testing.

**ETTERCAP**

Ettercap is a tool for man in the middle attacks and traffic sniffing in local networks.

It supports active and passive dissection of many protocols for analysis and auditing.

Used to intercept credentials, inject malicious content, or monitor network communications.

**HYDRA**

Hydra is a fast and flexible login cracker for testing authentication vulnerabilities.

It uses brute-force or dictionary-based attacks against various services like FTP, SSH, HTTP.

Supports parallel attacks, customizable options, and is ideal for password strength audits.

**MOSQUITTO**

Mosquitto is an open-source MQTT broker designed for lightweight, low-bandwidth messaging.

It’s widely used in IoT environments to allow devices to publish and subscribe to data.

Supports authentication, encryption (TLS), and multiple client libraries.

**NMAP**

Nmap (Network Mapper) is a free tool used to scan networks and discover hosts and services.

It detects open ports, running services, OS versions, and potential vulnerabilities.

Useful for mapping network topology and performing security audits.

**SQLMAP**

SQLmap is a Python-based tool that automates detecting and exploiting SQL injection flaws.

It allows users to dump database content, gain shell access, or test DB security.

It supports multiple DBMSs (MySQL, MSSQL, PostgreSQL, etc.) and provides customizable options.

**SQLNINJA**

SQLninja is a penetration testing tool focused on exploiting SQL injection in MS SQL servers.

It provides methods to escalate privileges and gain shell access to the backend system.

Best used for automating attacks on ASP/ASP.NET apps using vulnerable MSSQL databases.

**NETCAT**

Netcat is a simple networking utility to read and write data across TCP or UDP connections.

It can be used for port scanning, transferring files, banner grabbing, or remote shells.

Known as the "Swiss Army Knife" of networking, it’s a go-to for debugging and scripting.

**MSFVENOM**

MSFvenom is a payload generator that is part of the Metasploit Framework.

It combines the functionality of msfpayload and msfencode to create customized shellcodes.

Used to bypass antivirus or firewall defenses by crafting tailored payloads.

**MICROSOFT THREAT MODEL**

Microsoft Threat Modeling Tool helps visualize system components, data flows, and boundaries.

It allows developers to identify potential threats early in the design phase.

Built on the STRIDE framework, it automates risk assessment and documentation.

**PYCHARM**

PyCharm is a Python-specific IDE developed by JetBrains.It offers smart code completion, debugging, virtual environments, and Git integration.

Excellent for Python developers working on apps, data science, automation, or web projects.

| **Tool** | **What It Is** | **Used For** | **Why/Purpose** | **Benefits/Features** | **Examples** |
| --- | --- | --- | --- | --- | --- |
| **Kali Linux** | Debian‑based Linux distro | Security testing, forensics, research | Pre‑loaded with security tools | Hundreds of tools, live/VM support, bleeding‑edge updates | Boot via USB/VM, use Nmap to scan networks |
| **OWASP ZAP** | Web app security scanner | Vulnerability scanning for web apps | Identify injection, XSS, misconfigurations | GUI, passive/active scan, spider, CI/CD, extensible via scripts | Scan login page for XSS, integrate in Jenkins pipeline |
| **Metasploit** | Exploit framework | Vulnerability exploitation, post‑exploitation | Test and validate security controls | Large exploit DB, Meterpreter, msfvenom, scripting | Exploit MS08‑067 vulnerability, pivot to internal network |
| **Burp Suite** | Web app proxy + scanner (proprietary freemium) | Web application penetration testing | Deep manual + automated testing | Interceptor proxy, scanner, repeater, intruder, session handling | Intercept login request, fuzz session tokens, brute‑force forms |
| **Ettercap** | MITM attack suite | ARP spoofing, sniffing, session hijacking | Intercept and manipulate network traffic | UI and CLI, plugin support, filtering capabilities | Redirect HTTP traffic, inject JavaScript, sniff credentials |
| **Hydra** | Network login cracker | Brute‑force logins (ssh, ftp, etc.) | Test strength of authentication mechanisms | Fast, parallel connections, many protocols | Test FTP login with dictionary, check SSH credentials |
| **Mosquitto** | MQTT message broker | IoT messaging between clients/brokers | Lightweight pub/sub for sensor or device comms | Small footprint, SSL/TLS, authentication support, open source | Devices publish temp readings, server distributes to subscriber apps |
| **Nmap** | Network mapper & port scanner | Discover hosts/ports/services | Map networks and detect running apps/systems | OS detection, service versions, scripts, stealth options | nmap -sS -O 192.168.1.0/24, NSE script to check vulnerabilities |
| **Netcat** | Networking swiss‑army knife | Port listening, transfers, tunneling | Quick manual network diagnostics and comms | TCP/UDP client/server, redirection, piping, portable | Chat between PCs, pipe shell to remote via nc -l -p 4444 -e /bin/sh |
| **Sqlmap** | Automated SQL injection tool | Discover & exploit SQL injection flaws | Automate detection/extraction of DB data | DB fingerprinting, data dump, shell upload, contrast SQLi types | Extract user tables with sqlmap -u "site.com?id=1" |
| **SQLNinja** | SQL injection exploitation tool (MSSQL focus) | Exploit MS SQL injection automatically | Gain shell access via SQLi on Windows MSSQL | OS shell via SQLi, session handling, privilege escalation | Exploit vulnerable MSSQL login to spawn shell |
| **msfvenom** | Payload generator (part of Metasploit) | Create custom payloads | Generate shellcode/payloads for testing | Formats for .exe, .elf, PHP, Python; encoder support | Create reverse‑TCP meterpreter payload in exe: msfvenom -p windows/meterpreter/reverse\_tcp … |
| **Microsoft Threat Modeling Tool** | Visual threat modeling software | Analyze and document system threats | Understand & mitigate security threats early | Diagramming, STRIDE taxonomy, automated threat reports | Model web app data flows, produce report on possible spoof/DoS threats |
| **Pycharm** | IDE for Python | Develop Python scripts, apps, tools | Boost developer productivity | Code completion, debugging, virtualenv, plugins, refactoring | Write and debug a Flask web app, automate sqlmap script |