**ISL Tools**

1. Kali Linux
2. OWASP ZAP
3. Metasploit
4. Burpsuite
5. Ettercap
6. Hydra
7. Mosquitto
8. N-map
9. Netcat
10. Sql map
11. Sql ninja
12. MSF Venom
13. MS threat model
14. PyCharm

**Kali Linux**

Kali Linux is a free open source Linux distro that is used for ethical hacking, pentesting and other cybersecurity tasks. It comes with many pre-installed security tools that are used for vulnerability scanning, network analysis, password cracking, digital forensics etc. Some of these tools are going to be discussed below.

**OWASP ZAP**

ZAP – Zed Attack Proxy

ZAP is an open source security software written in Java and is used to detect vulnerabilities present on any web server and try to remove them.

**Features:**

* Passive Scanner – Vulnerability Detected without getting in contact target machine
* Automated Scanner - Vulnerability Detected without getting in contact target machine (Easily detected by admin)
* Proxy Server - Server that acts as a mediator for clients who want to go through the request and want to alter them.

**Metasploit Framework**

An Exploitation framework for developing and executing exploit code. Used to simulate attacks by exploiting known vulnerabilities to test system defences. It is developed in Ruby and contains hundreds of pre-built exploits. It also allows for customization of these exploits and payloads and integrates with other tools like Nmap.

**Burpsuite**

A popular web application security testing tool used for finding vulnerabilities in websites.

It intercepts traffic and acts as a proxy between your browser and the web server. Burp Suite’s main feature is the Proxy. The Proxy enables Burp to act as an intermediary between the client (web browser) and the server hosting the web application. By placing itself between these two components, Burp will be able to intercept all exchanges and requests made between the web browser and the server. After intercepting these requests, they can be modified

**Ettercap**

Ettercap is an open source tools that is used for sniffing network traffic, intercepting data, and performing MITM attacks to analyze or manipulate communications between devices.

**Sniffing** : Watching the data that moves around on your network. (Like being a spy in the network)

**Spoofing:** Pretending to be another device on the network. (How attackers might trick the device)

**Hydra**

A tool that is used for brute-forcing password cracking. Hydra operates by systematically testing combinations of usernames and passwords until the correct pair is discovered. The steps in it’s operation are :

* **Protocol Selection:** Hydra allows targeting specific services (such as **SSH, FTP, or HTTP**) depending on the selected protocol.
* **Use of Password Lists:** The tool uses dictionary files (wordlists) containing common or customized passwords to increase the chances of success.
* **Parallelized Attacks:** Hydra can launch multiple connection attempts simultaneously, significantly speeding up the brute-forcing process.

**Mosquitto**

MQTT is a standards-based messaging protocol, or set of rules, used for machine-to-machine communication. Smart sensors, wearables, and other Internet of Things (IoT) devices typically have to transmit and receive data over a resource-constrained network with limited bandwidth. These IoT devices use MQTT for data transmission.

**Nmap**

**Nmap** is Linux command-line tool for network exploration and security auditing.

Used for Network scanning and discovery

Used to find devices on a network, discover open ports, and identify services running on them.

**Netcat**

Netcat is used for reading and writing data across network connections using either TCP or UDP protocols.

The following tasks can be done easily with Netcat:

* Connect to a port of a target host.
* Listen to a certain port for any inbound connections.
* Send data across client and server once the connection is established.
* Transfer files across the network once the connection is established.
* Can execute programs and scripts of the client on the server and vice versa.
* Can Provide remote shell access of server to a client where shell commands can be executed.

**SQL map**

Sqlmap is an open-source penetration testing tool used to find and exploit SQL injection problems and take control of database systems.

SQL injection usually occurs when you ask a user for input, like their username/userid, and instead of a name/id, the user gives you an SQL statement that you will **unknowingly** run on your database.

When a malicious user successfully completes an SQL injection attack, it can have any of the following impacts:

* **Exposes Sensitive Company Data**: Using SQL injection, attackers can retrieve and alter data, which risks exposing sensitive company data stored on the SQL server.
* **Compromise Users’ Privacy**: Depending on the data stored on the SQL server, an attack can expose private user data, such as credit card numbers.
* **Give an attacker access to your system**: If a database user has administrative privileges, an attacker can gain access to the system using malicious code. To protect against this kind of vulnerability, create a database user with the least possible privileges.

**SQL Ninja**

SQL ninja exploits web applications that use Microsoft SQL Server as a database backend. Its focus is on getting a running shell on the remote host. SQL ninja doesn't find an SQL injection in the first place, but automates the exploitation process once one has been discovered.

Sqlninja is a tool targeted to exploit SQL Injection vulnerabilities on a web application that uses Microsoft SQL Server as its back-end.  
Its main goal is to provide a remote access on the vulnerable DB server, even in a very hostile environment. It should be used by penetration testers to help and automate the process of taking over a DB Server when a SQL Injection vulnerability has been discovered.

**msfvenom**

**msfvenom** is a tool that's part of the **Metasploit Framework**, used to generate payloads for penetration testing and ethical hacking. msfvenom combines two older tools (msfpayload and msfencode) into one. It helps you create custom payloads — pieces of code that run on a target machine after an exploit succeeds.

**Functionality:**

* Generate payloads in various formats (executables, scripts, shellcode, etc.).
* Encode payloads to evade antivirus detection.
* Customize payloads with options like IP addresses, ports, and commands.

**MS threat model**

**MS threat model provides a systematic** way to identify, assess, and address potential security threats in software or systems during their design and development phases. Microsoft has popularized a specific methodology and toolset using the **STRIDE** model:

* **S**poofing identity — Pretending to be something or someone else.
* **T**ampering with data — Unauthorized modification of data.
* **R**epudiation — Users denying having performed an action.
* **I**nformation disclosure — Exposure of information to unauthorized parties.
* **D**enial of service — Disrupting or degrading service availability.
* **E**levation of privilege — Gaining unauthorized higher-level permissions.

**PyCharm**

PyCharm is considered to be one of the most integrated Python IDEs, offering a range of modules and tools which make coding a lot faster and easier for programmers. PyCharm can be used for code analysis, debugging, and testing, among other things.

Some core features of PyCharm:

1. Smart Code Editor
2. Code Analysis & Refactoring
3. Debugging and Testing
4. Project and Environment Management
5. Version Control Integration
6. Web Development Support
7. Database Tools
8. Scientific Tools