PD
PENTEST DIARIES

PD
PENTEST DIARIES
HTTPS://WWW.SAKSHAMDIXIT.COM

# KNOWLEDGE • SHARE •

## PENTEST DIARIES

@pentestdiaries

# Leveraging Tools: Unveiling the Power of Kali Linux

## Penetration Testing and Vulnerability Assessment:

- **`Nmap` (Network Mapper):** A versatile network scanner used for reconnaissance, identifying machines on a network, open ports, and services running.

**Syntax:**

```
nmap <target IP>
```

- **`Aircrack-ng:`** A suite of tools for wireless network analysis and penetration testing, including password cracking for Wi-Fi networks.

**Syntax:**

```
airack-ng <interface> -w <wordlist.txt> <capture file>
```

- **`John the Ripper:`** A password cracking tool that supports various hashing algorithms used to crack stolen password hashes.

**Syntax:**

```
john --format=<hash format> <password hash>
```

## `Metasploit:`

1. **Launching Metasploit Framework**:
   - Open a terminal in Kali Linux and type `msfconsole` to launch the Metasploit Framework.
2. **Search for Modules**:
   - Once inside Metasploit, you can search for available modules using the `search` command. For example, type `search smb` to search for modules related to the Server Message Block (SMB) protocol.
3. **Selecting a Module**:
   - To use a specific module, you can select it using the `use` command followed by the module name. For example, `use exploit/windows/smb/ms08_067_netapi`.
4. **Viewing Module Options**:
   - You can view the options available for the selected module using the `show options` command. This displays the required and optional parameters that need to be configured before launching the exploit.
5. **Setting Module Options**:

- Set the required options for the module using the `set` command followed by the option name and its value. For example, `set RHOSTS target_ip` sets the remote host IP address.

6. **Running the Exploit**:
   - Once all required options are set, you can run the exploit using the `exploit` command. This will attempt to exploit the target system based on the specified parameters.


## Enumeration and Exploitation:

- **`Nessus` (Professional version requires a license):** A vulnerability scanner that identifies potential weaknesses in systems and applications.
- **`Nikto`:** A fast web server scanner that identifies outdated software, potentially dangerous scripts, and server configuration issues.

### Syntax:

```
nikto -h <target URL>
```

- **`sqlmap`:** An automated tool for exploiting SQL injection vulnerabilities in web applications.

### Syntax:

```
sqlmap -u <target URL> --dbs
```

## Social Engineering and Web Application Security:

- **`Social-Engineer Toolkit` (SET):** A collection of tools to automate social engineering attacks (used for educational purposes only with proper permission).
- **`WPScan`:** A vulnerability scanner specifically designed for WordPress websites to identify security weaknesses and outdated plugins.

### Syntax:

```
wpscan --url <target URL>
```

## Important Information:

- Ethical use is critical. Only use these tools on authorized systems with proper permission.
- Proficiency in Linux commands is essential for using these tools effectively.
- Many of these tools have complex syntax and capabilities. Consult their documentation for detailed usage instructions.