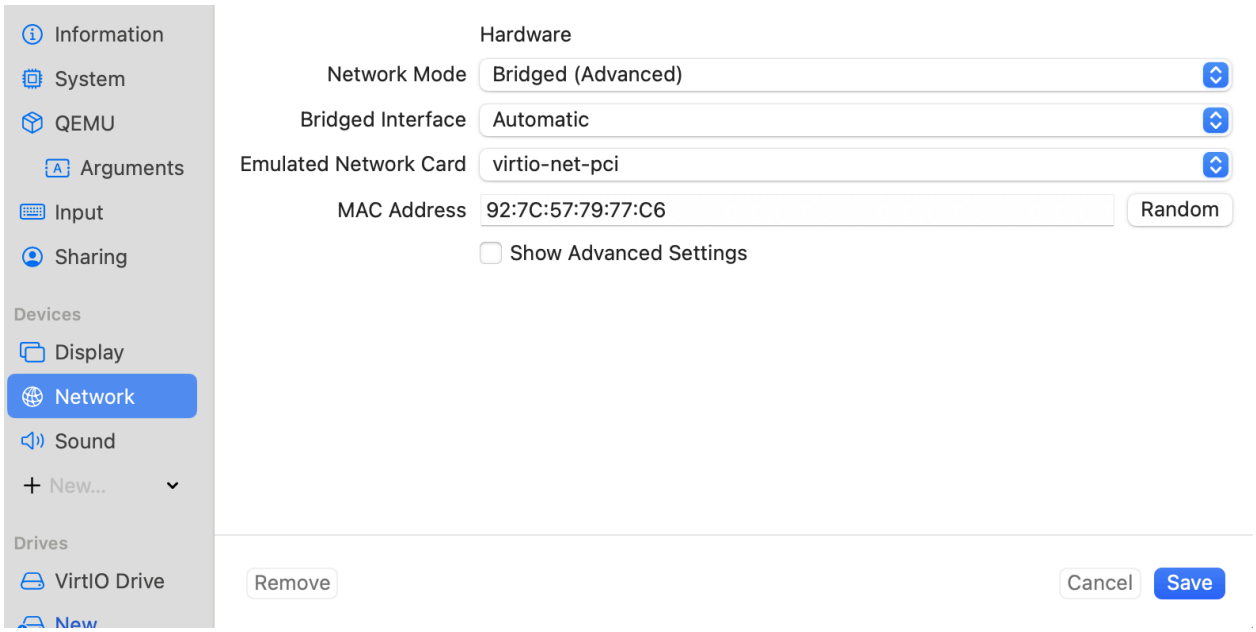
Parrot OS Ethical Hacking Lab Setup

Project Overview

This project demonstrates the successful installation and configuration of Parrot OS in VirtualBox with a focus on ethical hacking tools, including Nmap, Wireshark, and Metasploit. The project includes proper network configuration, the establishment of a secure lab environment, and documentation of all configurations and test executions.

1. Installation of Parrot OS in VirtualBox

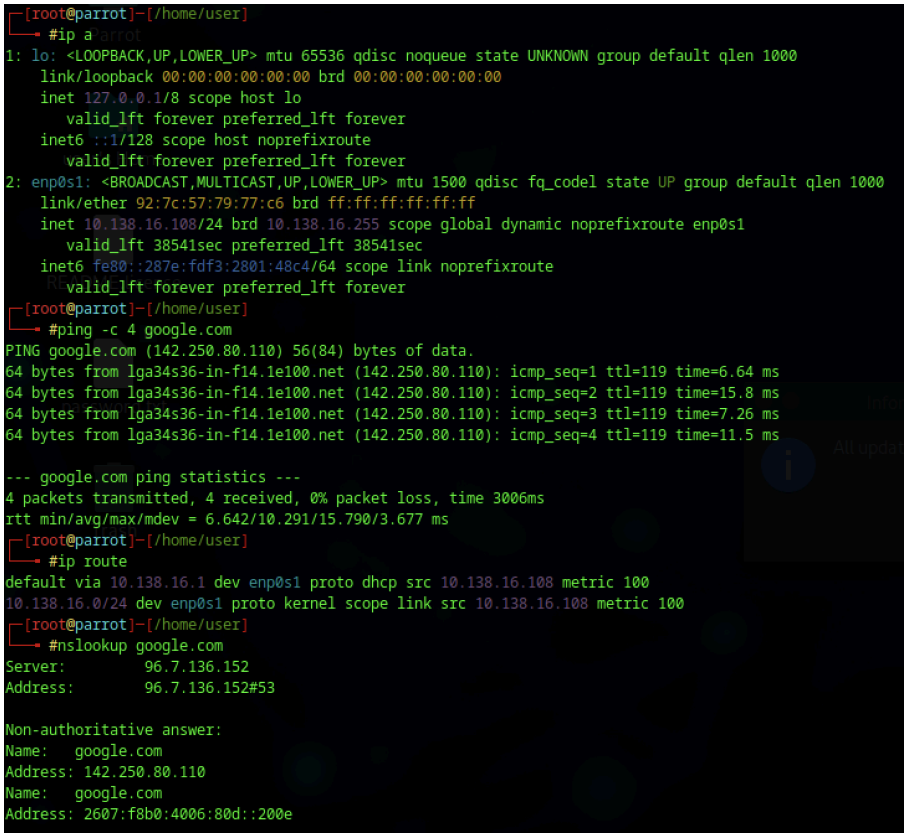
- Parrot OS was installed on VirtualBox using a bridged network adapter for internet access.
- Screenshot evidence of network configuration:



2. Network Configuration

- Network mode set to 'Bridged (Advanced)' with automatic bridged interface selection.
- Emulated Network Card: 'virtio-net-pci'.
- Proper IP address assigned via DHCP, as evidenced in terminal outputs.

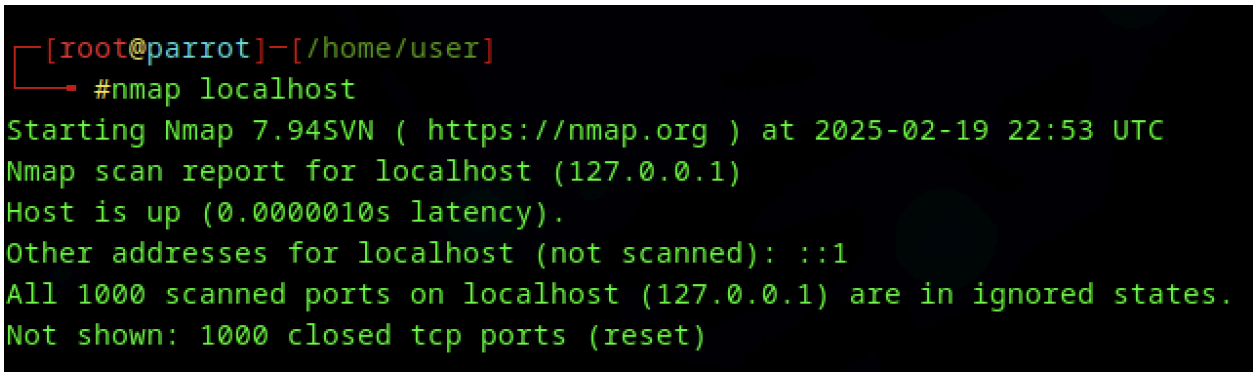
- Screenshot showing `ip a` and `ping google.com` command outputs:



3. Installation and Configuration of Ethical Hacking Tools

Nmap

- Scan of localhost showing all ports closed as expected.
- Screenshot of Nmap output:



Wireshark

- Wireshark installed and used to capture network traffic on interface `enp0s1`.
- Captured DNS traffic showing connected devices on the network.
- Screenshot of Wireshark in action:

Metasploit

- Metasploit framework installed and configured.
- Demonstrated a search for Windows exploits within the framework.
- Screenshot of Metasploit configuration:

4. Secure Lab Environment

- The VirtualBox environment is isolated from the host system by using bridged networking with no port forwarding.
- No sensitive host data exposed to the virtual machine.

5. Conclusion

This project successfully demonstrates the installation, configuration, and use of key ethical hacking tools in a controlled lab environment. The setup provides a strong foundation for further security testing and learning within an isolated and safe infrastructure.