Ethical Hacking Lab Setup Report

Introduction

This report documents the setup and configuration of an ethical hacking lab environment using Parrot OS in VirtualBox. The lab includes essential tools such as Nmap, Wireshark, and Metasploit, which are configured and tested for functionality. The report provides evidence of proper network configuration, tool installations, and successful test executions, ensuring a secure and isolated lab environment for ethical hacking practices.

Environment Setup

Parrot OS Installation in VirtualBox

Parrot OS was successfully installed and configured in VirtualBox. The following steps outline the installation process:

1. **Download Parrot OS**: The latest Parrot OS ISO was downloaded from the official website.
2. **VirtualBox Configuration**: A new virtual machine was created in VirtualBox with the following settings:
    - **Name**: Parrot OS
    - **Type**: Linux
    - **Version**: Debian (64-bit)
    - **Memory Size**: 2048 MB
    - **Hard Disk**: 20 GB dynamically allocated
3. **Network Configuration**: The network settings were configured to use Bridged Adapter for proper network connectivity.

Network Configuration

The network settings were configured to ensure proper connectivity and isolation within the lab environment. The following settings were applied:

- **Network Mode**: Bridged (Advanced)
- **Bridged Interface**: Automatic
- **Emulated Network Card**: virtio-net-pci
- **MAC Address**: 6A:BD:45:D1:80:7C

These settings ensure that the virtual machine can communicate with the host network while maintaining isolation for security purposes.

Tool Installation and Configuration

Nmap

Nmap was installed and configured to perform network scanning and discovery. The following command was used to install Nmap:

```
sudo apt-get install nmap
```

Functionality Test: A network scan was performed using Nmap to identify active hosts and open ports within the network. The scan results are shown in the screenshot below:

Wireshark

Wireshark was installed and configured to capture and analyze network traffic. The following command was used to install Wireshark:

```
sudo apt-get install wireshark
```

Functionality Test: Wireshark was used to capture network packets and analyze the traffic. The capture results are shown in the screenshot below:

Metasploit

Metasploit was installed and configured to perform penetration testing and exploit development. The following command was used to install Metasploit:

```
sudo apt-get install metasploit-framework
```

Functionality Test: Metasploit was used to perform a basic exploit test to demonstrate its functionality. The test results are shown in the screenshot below:

Secure Lab Environment

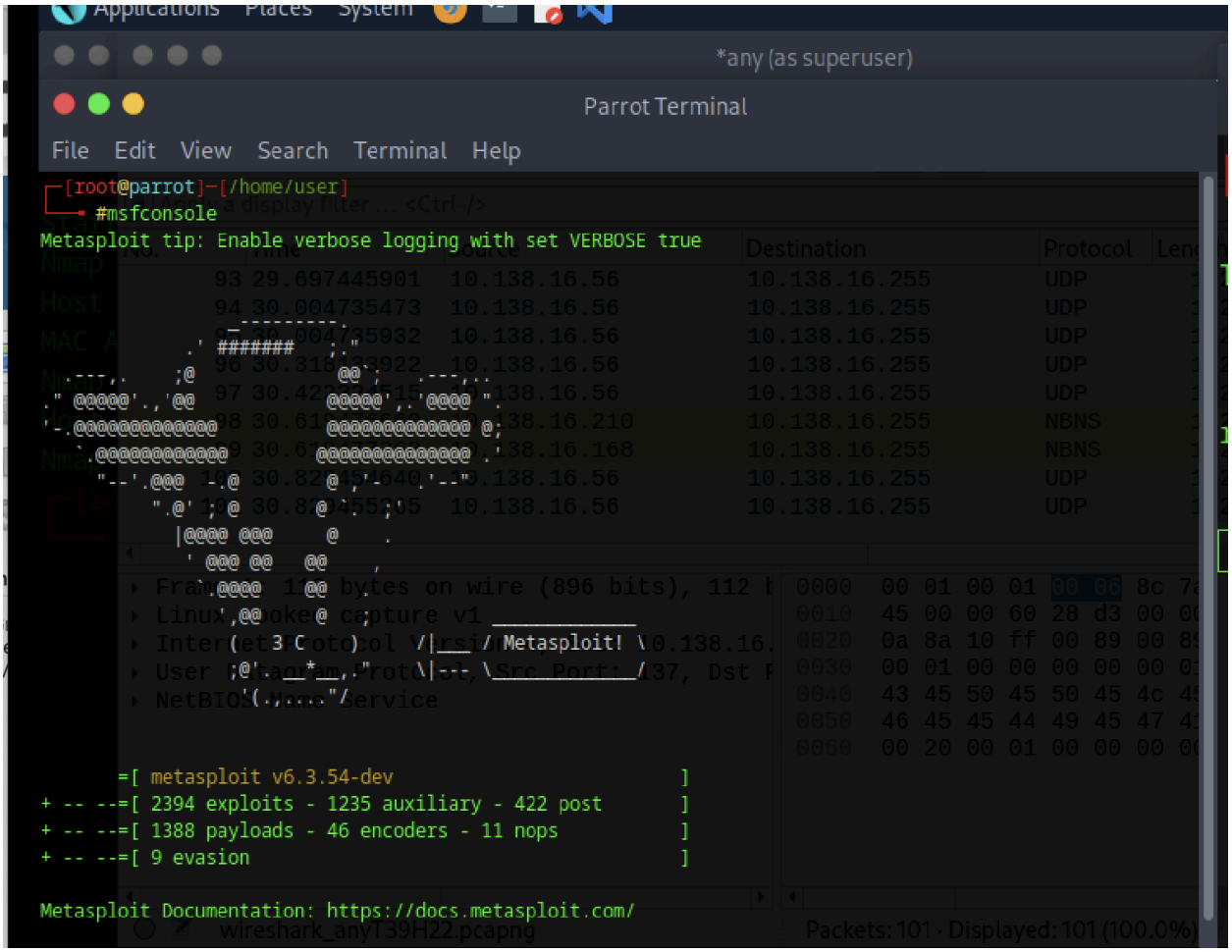
A secure lab environment was established with proper isolation to ensure that ethical hacking activities do not affect the host system or external networks. The following measures were taken:

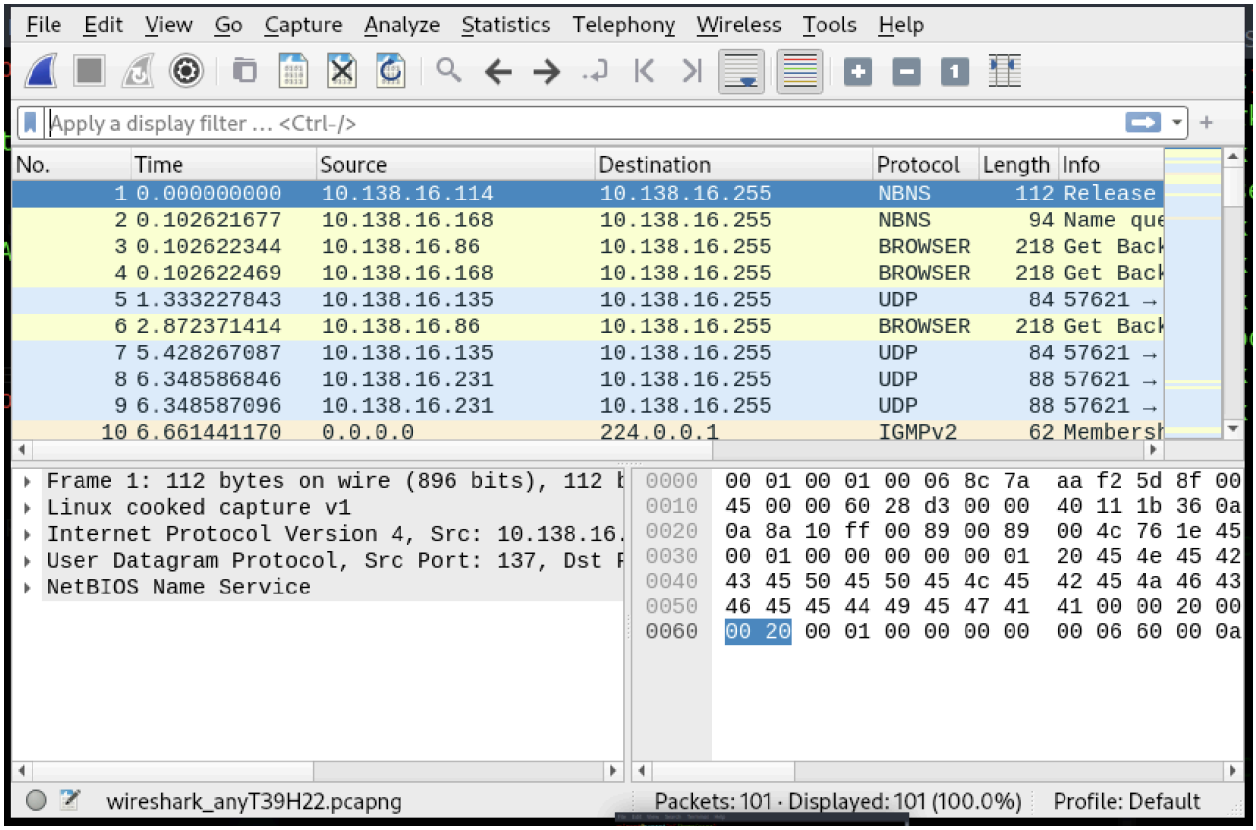
- **Network Isolation**: The virtual machine was configured to use a bridged network adapter to ensure isolation from the host network.
- **Firewall Configuration**: The virtual machine's firewall was configured to allow only necessary traffic and block unwanted connections.
- **Regular Updates**: The system and tools were regularly updated to patch any security vulnerabilities.

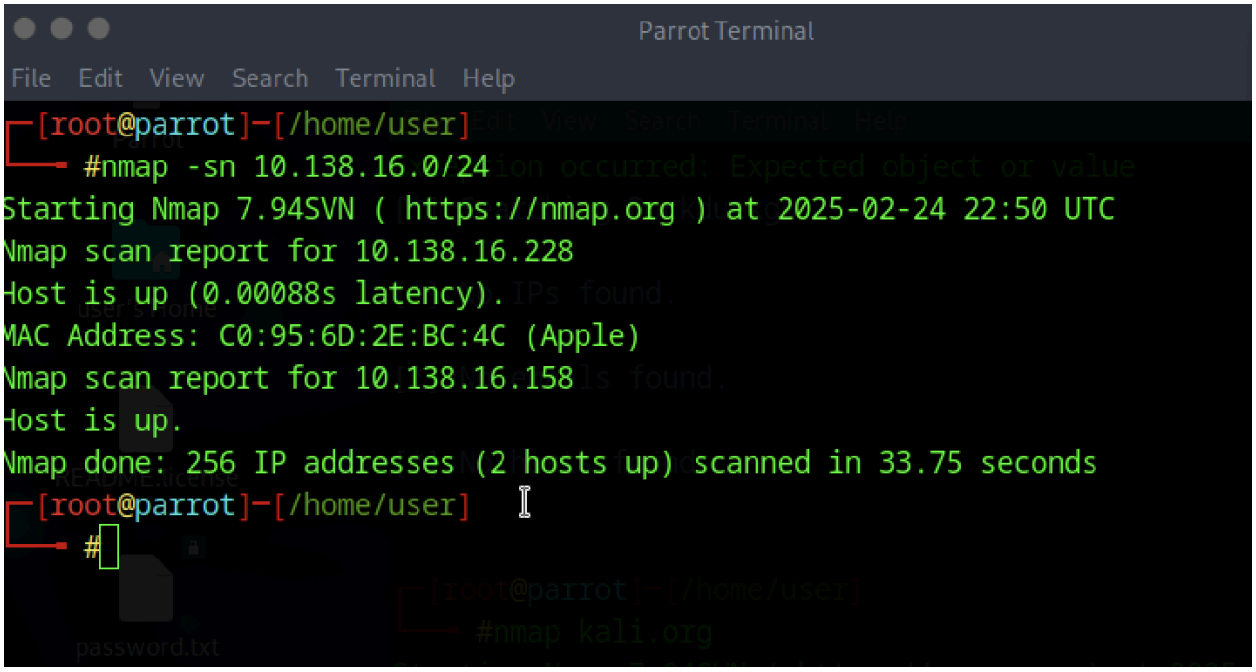
Documentation and Evidence

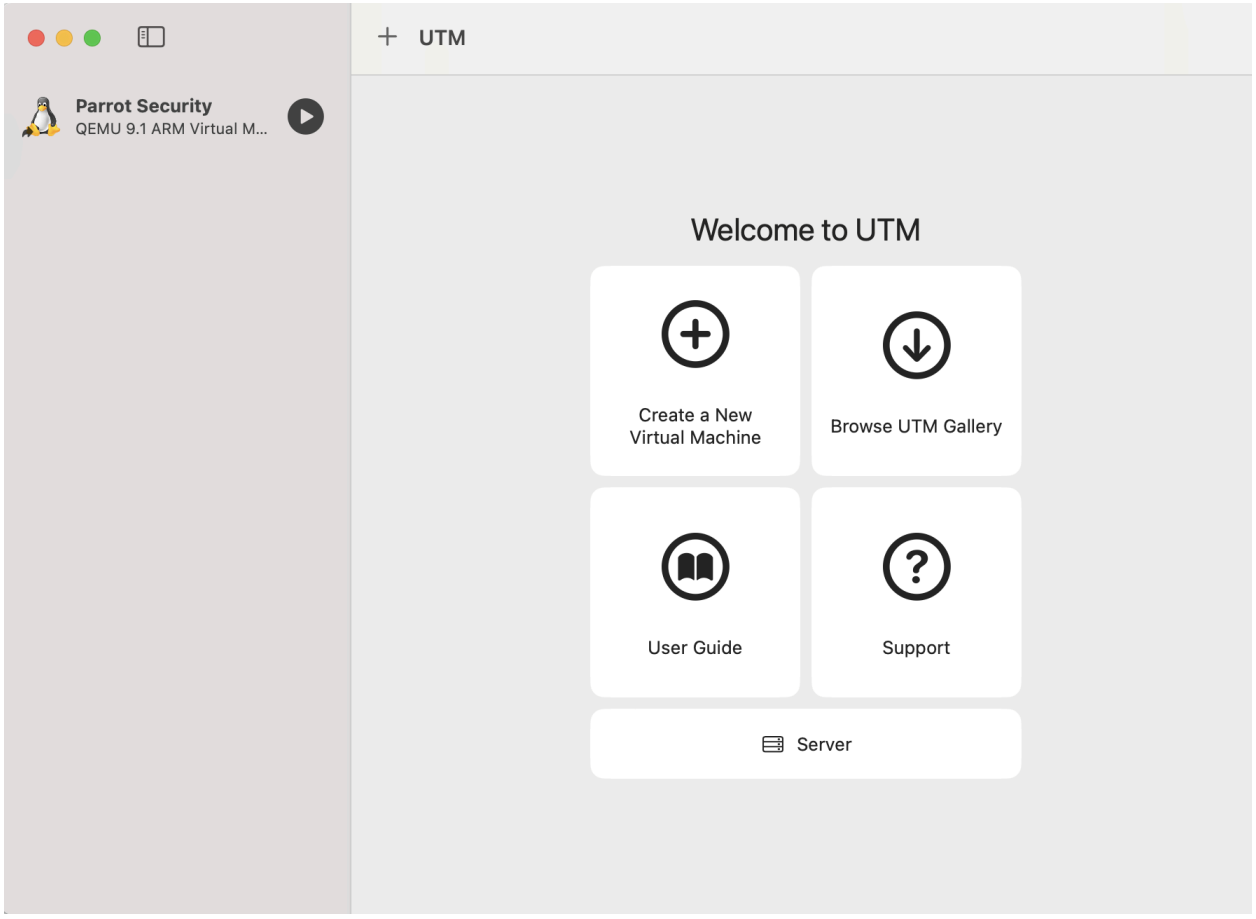
The report includes screenshots of tool configurations, network settings, and successful test executions. These screenshots provide evidence of proper installation, configuration, and functionality testing of the ethical hacking tools and network settings.

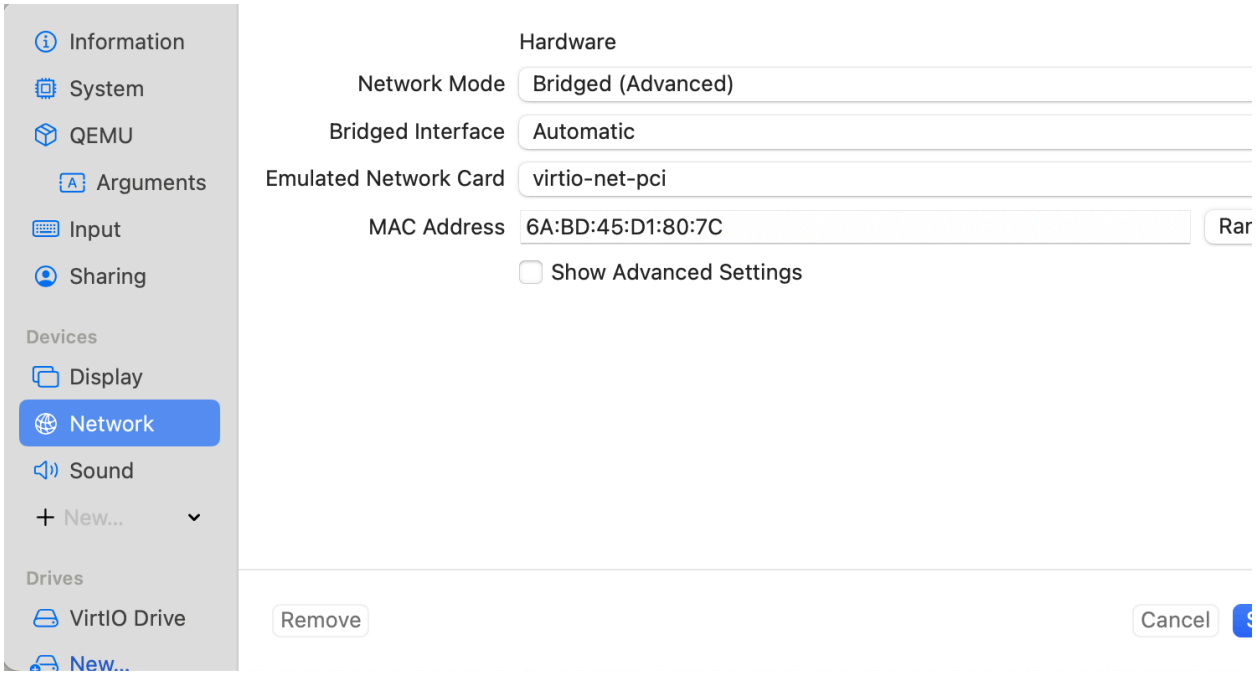
Screenshots




File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
No. Time Source Destination Protocol Length Info
1 0.000000000 10.138.16.114 10.138.16.255 NBNS 112 Release
2 0.102621677 10.138.16.168 10.138.16.255 NBNS 94 Name que
3 0.102622344 10.138.16.86 10.138.16.255 BROWSER 218 Get Back
4 0.102622469 10.138.16.168 10.138.16.255 BROWSER 218 Get Back
5 1.333227843 10.138.16.135 10.138.16.255 UDP 84 57621 →
6 2.872371414 10.138.16.86 10.138.16.255 BROWSER 218 Get Back
7 5.428267087 10.138.16.135 10.138.16.255 UDP 84 57621 →
8 6.348586846 10.138.16.231 10.138.16.255 UDP 88 57621 →
9 6.348587096 10.138.16.231 10.138.16.255 UDP 88 57621 →
10 6.661441170 0.0.0.0 224.0.0.1 IGMPv2 62 Membersh
Frame 1: 112 bytes on wire (896 bits), 112 b
Linux cooked capture v1
Internet Protocol Version 4, Src: 10.138.16.
User Datagram Protocol, Src Port: 137, Dst P
NetBIOS Name Service
0000 00 01 00 01 00 06 8c 7a aa f2 5d 8f 00
0010 45 00 00 60 28 d3 00 00 40 11 1b 36 0a
0020 0a 8a 10 ff 00 89 00 89 00 4c 76 1e 45
0030 00 01 00 00 00 00 00 01 20 45 4e 45 42
0040 43 45 50 45 50 45 4c 45 42 45 4a 46 43
0050 46 45 45 44 49 45 47 41 41 00 00 20 00
0060 00 20 00 01 00 00 00 00 00 06 60 00 0a
wireshark_anyT39H22.pcapng
Packets: 101 · Displayed: 101 (100.0%)
Profile: Default


Parrot Terminal
File Edit View Search Terminal Help
[root@parrot]-[/home/user]
#nmap -sn 10.138.16.0/24
Starting Nmap 7.94SVN (https://nmap.org) at 2025-02-24 22:50 UTC
Nmap scan report for 10.138.16.228
Host is up (0.00088s latency).
MAC Address: C0:95:6D:2E:BC:4C (Apple)
Nmap scan report for 10.138.16.158
Host is up.
Nmap done: 256 IP addresses (2 hosts up) scanned in 33.75 seconds
[root@parrot]-[/home/user]
#


UTM
Parrot Security
QEMU 9.1 ARM Virtual M...
Welcome to UTM
Create a New Virtual Machine
Browse UTM Gallery
User Guide
Support
Server


Information
System
QEMU
Arguments
Input
Sharing
Devices
Display
Network
Sound
New...
Drives
VirtIO Drive
New...
Hardware
Network Mode
Bridged (Advanced)
Bridged Interface
Automatic
Emulated Network Card
virtio-net-pci
MAC Address
6A:BD:45:D1:80:7C
Show Advanced Settings
Remove
Cancel

Conclusion

The ethical hacking lab environment was successfully set up and configured using Parrot OS in VirtualBox. Essential tools such as Nmap, Wireshark, and Metasploit were installed and configured, and their functionality was demonstrated through successful test executions. The lab environment was secured with proper isolation and regular updates to ensure a safe and effective ethical hacking practice.