

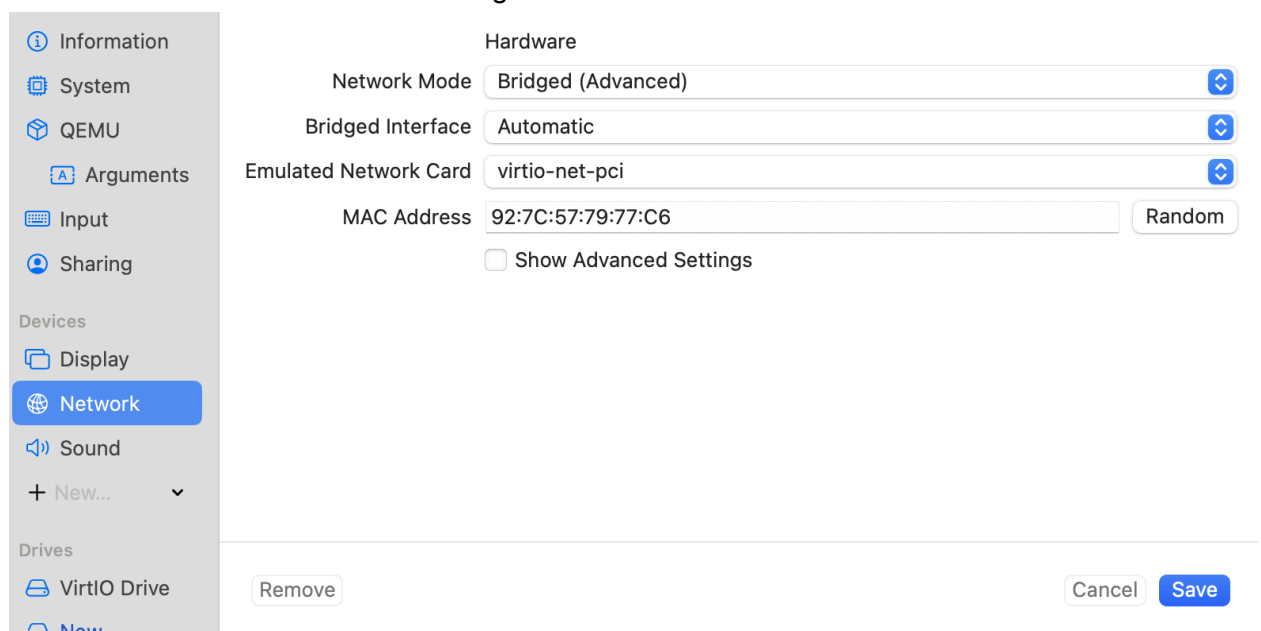
Parrot OS Ethical Hacking Lab Setup

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:

```
[root@parrot]~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 92:7c:57:79:c6:ff brd ff:ff:ff:ff:ff:ff
    inet 10.138.16.108/24 brd 10.138.16.255 scope global dynamic noprefixroute enp0s1
        valid_lft 38541sec preferred_lft 38541sec
    inet6 fe80::287e:fd3:2801:48c4/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

[root@parrot]~# ping -c 4 google.com
PING google.com (142.250.80.110) 56(84) bytes of data:
64 bytes from lga34s36-in-f14.1e100.net (142.250.80.110): icmp_seq=1 ttl=119 time=6.64 ms
64 bytes from lga34s36-in-f14.1e100.net (142.250.80.110): icmp_seq=2 ttl=119 time=15.8 ms
64 bytes from lga34s36-in-f14.1e100.net (142.250.80.110): icmp_seq=3 ttl=119 time=7.26 ms
64 bytes from lga34s36-in-f14.1e100.net (142.250.80.110): icmp_seq=4 ttl=119 time=11.5 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 6.642/10.291/15.790/3.677 ms

[root@parrot]~# ip route
default via 10.138.16.1 dev enp0s1 proto dhcp src 10.138.16.108 metric 100
10.138.16.0/24 dev enp0s1 proto kernel scope link src 10.138.16.108 metric 100

[root@parrot]~# nslookup google.com
Server:          96.7.136.152
Address:         96.7.136.152#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.80.110
Name:   google.com
Address: 2607:f8b0:4006:80d::200e
```

3. Installation and Configuration of Ethical Hacking Tools

Nmap

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

```
[root@parrot]~# nmap localhost
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-19 22:53 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000010s latency).
Other addresses for localhost (not scanned): ::1
All 1000 scanned ports on localhost (127.0.0.1) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

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:

```

[~root@parrot:~/home/user]
→ #shark -i
Running as user "root" and group "root". This could be dangerous.
1. enp0s1
2. any
3. lo (Loopback)
4. bluetooth-monitor
5. niflog
6. nifqueue
7. dbus-system
8. dbus-session
9. ciscodump (Cisco remote capture)
10. dsniffnet (DisplayPort AUX channel monitor capture)
11. randpkt (Random packet generator)
12. sdjournal (systemd Journal Export)
13. sshdump (SSH remote capture)
14. udpsnoop (UDP Listener remote capture)
15. wifidump (Wi-Fi remote capture)
[~root@parrot:~/home/user]
→ #shark -i enp0s1
Running as user "root" and group "root". This could be dangerous.
Capturing on 'enp0s1'
** (tshark:2421) 22:57:46.281864 [Main MESSAGE] -- Capture started.
** (tshark:2421) 22:57:46.281931 [Main MESSAGE] -- File: "/tmp/wireshark_enp0s1Q8B712.pcapng"
1 0.000000000 10.138.16.106 -> 224.0.0.251 MDNS 105 Standard query 0x6470 PTR SA's MacBook Air._companion-link._tcp.local, "QM" question
2 0.000000166 10.138.16.106 -> 224.0.0.251 MDNS 167 M-SEARCH * HTTP/1.1
3 0.102177010 10.138.16.86 -> 224.0.0.251 MDNS 126 Standard query response 0x0000 NSEC, cache flush SA's MacBook Air._companion-link._tcp.local
4 0.206576970 10.138.16.102 -> 229.255.255.250 SSDP 167 M-SEARCH * HTTP/1.1
5 0.306482006 10.138.16.128 -> 224.0.0.251 MDNS 79 Standard query 0x1c01 PTR _arduino._tcp.local, "QM" question
6 0.407215499 10.138.16.162 -> 224.0.0.251 MDNS 452 Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question
8 DEP-Pad_KX4YV1Cm6._companion-link._tcp.local PTR DAEDMAC50._companion-link._tcp.local PTR SA55._companion-link._tcp.local PTR Justin's MacBook Pro._companion-link._tcp.local PTR Alex's MacBook Air._companion-link._tcp.local PTR SA's MacBook Air._companion-link._tcp.local PTR Marybel's MacBook Air._companion-link._tcp.local PTR SA's MacBook Air (2)._companion-link._tcp.local PTR Isabel Newman laptop._companion-link._tcp.local PTR SA's MacBook Air._companion-link._tcp.local PTR DAEDMAC34._companion-link._tcp.local
7 0.407215999 10.138.16.230 -> 224.0.0.251 MDNS 850 Standard query 0x0000 PTR lb._dns-sd._udp.local, "QM" question PTR _airport._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question PTR _uic._companion-link._tcp.local, "QM" question PTR _app._tcp.local, "QM" question PTR _uscan._tcp.local, "QM" question PTR _ippush._tcp.local, "QM" question PTR _ptp._tcp.local, "QM" question PTR _pdl-datastream._tcp.local, "QM" question PTR _scanner._tcp.local, "QM" question PTR _printer._tcp.local, "QM" question PTR _ipps._tcp.local, "QM" question PTR _afpovertcp._tcp.local, "QM" question PTR _adisk._tcp.local, "QM" question PTR HP OfficeJet Pro 9130e Series [CD316E]_uscan._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_uscan._tcp.local PTR HP OfficeJet Pro 9130e Series [CD316E]_ipp._tcp.local PTR HP OfficeJet Pro 9130e Series [E7A3BF]_ipp._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_uscan._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_scanner._tcp.local PTR HP OfficeJet Pro 9130e Series [CD316E]_pdl-datastream._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_pdl-datastream._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_scanner._tcp.local PTR HP OfficeJet Pro 9130e Series [CD316E]_ipps._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_ipps._tcp.local
8 0.407216882 10.138.16.106 -> 224.0.0.251 MDNS 96 Standard query 0x474c PTR DAEDMAC34._companion-link._tcp.local, "QM" question
9 0.512827768 10.138.16.106 -> 224.0.0.251 MDNS 114 Standard query 0x4741 PTR HP OfficeJet Pro 8020 series [E7A3BF]_ipps._tcp.local, "QM" question
10 0.615700412 10.138.16.76 -> 224.0.0.251 MDNS 129 Standard query 0x0000 NSEC, cache flush HP OfficeJet Pro 8020 series [E7A3BF]_ipps._tcp.local
11 0.338177442 10.138.16.162 -> 224.0.0.251 MDNS 452 Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question PTR _uic._companion-link._tcp.local, "QM" question PTR _app._tcp.local, "QM" question PTR _uscan._tcp.local, "QM" question PTR _ippush._tcp.local, "QM" question PTR _ptp._tcp.local, "QM" question PTR _pdl-datastream._tcp.local, "QM" question PTR _scanner._tcp.local, "QM" question PTR _printer._tcp.local, "QM" question PTR _ipps._tcp.local, "QM" question PTR _afpovertcp._tcp.local, "QM" question PTR _adisk._tcp.local, "QM" question PTR HP OfficeJet Pro 9130e Series [CD316E]_uscan._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_uscan._tcp.local PTR HP OfficeJet Pro 9130e Series [CD316E]_ipp._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_pdl-datastream._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_scanner._tcp.local PTR HP OfficeJet Pro 9130e Series [CD316E]_ipps._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_ipps._tcp.local
8 DEP-Pad_KX4YV1Cm6._companion-link._tcp.local PTR DAEDMAC50._companion-link._tcp.local PTR SA55._companion-link._tcp.local PTR Justin's MacBook Pro._companion-link._tcp.local PTR Alex's MacBook Air._companion-link._tcp.local PTR SA's MacBook Air._companion-link._tcp.local PTR Marybel's MacBook Air._companion-link._tcp.local PTR SA's MacBook Air (2)._companion-link._tcp.local PTR Isabel Newman laptop._companion-link._tcp.local PTR SA's MacBook Air._companion-link._tcp.local PTR DAEDMAC34._companion-link._tcp.local
9 0.615700412 10.138.16.76 -> 224.0.0.251 MDNS 129 Standard query 0x0000 NSEC, cache flush HP OfficeJet Pro 8020 series [E7A3BF]_ipps._tcp.local
10 0.338177442 10.138.16.162 -> 224.0.0.251 MDNS 452 Standard query 0x0000 PTR _homekit._tcp.local, "QM" question PTR _rdlink._tcp.local, "QM" question PTR _uic._companion-link._tcp.local, "QM" question PTR _app._tcp.local, "QM" question PTR _uscan._tcp.local, "QM" question PTR _ippush._tcp.local, "QM" question PTR _ptp._tcp.local, "QM" question PTR _pdl-datastream._tcp.local, "QM" question PTR _scanner._tcp.local, "QM" question PTR _printer._tcp.local, "QM" question PTR _ipps._tcp.local, "QM" question PTR _afpovertcp._tcp.local, "QM" question PTR _adisk._tcp.local, "QM" question PTR HP OfficeJet Pro 9130e Series [CD316E]_uscan._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_uscan._tcp.local PTR HP OfficeJet Pro 9130e Series [CD316E]_ipp._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_pdl-datastream._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_scanner._tcp.local PTR HP OfficeJet Pro 9130e Series [CD316E]_ipps._tcp.local PTR HP OfficeJet Pro 8020 series [E7A3BF]_ipps._tcp.local

```

Metasploit

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

```
[root@parrot:/home/users] # cd /home/users
[parrot] # msfconsole
Metasploit tip: Search can apply complex filters such as search cve-2009
Type:exploit, see all the filters with help search

msf5 > search cve-2009

=====
# Name
-----
0  [redacted] /ftp/32bitftp_list_reply
1  [redacted] /ftp/threecftpsvc_long_mode
2  [redacted] /ftp/3cdemon_ftpt_user
3  [redacted] /scada/igss_misc
4  [redacted] /scada/igss_dataserver_rename
5  [redacted] /scada/igss_igssdataserver_listall
6  [redacted] /fileformat/a_pdf_wav_to_mp3
7  [redacted] /fileformat/asynclist_reply
8  [redacted] /scada/adb_server_exec
9  /fileformat/abcs_gsm_list
10 [redacted] /fileformat/acdsee_fotolatte_string
11 [redacted] /fileformat/acdsee_vpm
12 [redacted] /sip/aim_triton_csq
13 [redacted] /misc/ais_esel_server_rce

Disclosure Date Rank Check Description
-----
2010-10-12 good No 32bit FTP Client Stack Buffer Overflow
2006-11-27 great No 3CtFtpSvc TFTP Long Mode Buffer Overflow
2005-01-04 average Yes 3Com 3Cdemon 2.0 FTP Username Overflow
2011-03-24 excellent No 7-Techologies IGSS 9 Data Server/Collector Packet Handling vulnerability
2011-03-24 normal No 7-Techologies IGSS 9 IGSSDataServer.exe Remote Code Execution
2011-03-24 good No 7-Techologies IGSS IGSSDataServer.exe Stack Buffer Overflow
2010-08-17 normal No A-PDF WAV to MP3 v1.0.4 CSq Buffer Overflow
2010-10-12 good No AAASync V2.2.1.0 (Win32) Stack Buffer Overflow (LIST)
2013-04-05 excellent Yes ABM MicroSCADA server.exe Remote Code Execution
2013-06-30 normal No ABMS Audio Media Player LIST Buffer Overflow
2011-09-12 good No ACDSee Fotolatte P.LP File id Parameter Overflow
2007-11-23 good No ACDSee XPM File Section Buffer Overflow
2006-07-10 great No AIM Triton 1.0.4 CSq Buffer Overflow
2010-03-27 excellent Yes AIS Logistics ESEL-Server Unauth SQL Injection RCE
```

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.