

## **FITZHUGH**

### **CSIA 440 – 3014 CYBER TEST & PENETRATION**

#### **SPRING 2020**

#### **Project 1**

#### **Objectives**

- Complete part one of a phased penetration test in a virtual lab environment.

#### **Problems**

For this scenario, assume you are working as a security engineer for Columbia Basin College (CBC).

Rebound Security (<http://reboundsecurity.info>) is a local company that makes a data-loss prevention appliance (Rebound\_DLP) that CBC has used for years.

By contract, this appliance is supported and updated by the vendor, but its security posture has never been assessed or tested.

For this class, you will assess the security of the appliance by performing a phased penetration test on Rebound\_DLP.

The CEO, Eric Robinson ([eric.robinson@reboundsecurity.info](mailto:eric.robinson@reboundsecurity.info)), is aware of this penetration test, but not really pleased about it. He tends to be a tad pompous and believe his company's appliance is unbreakable.

Let's see if his assertions are true.

#### **A. LAB SETUP**

For your virtualization software, you can use whatever solution you prefer. Most students use either VirtualBox, Parallels, VMWare Workstation, or VMWare Fusion.

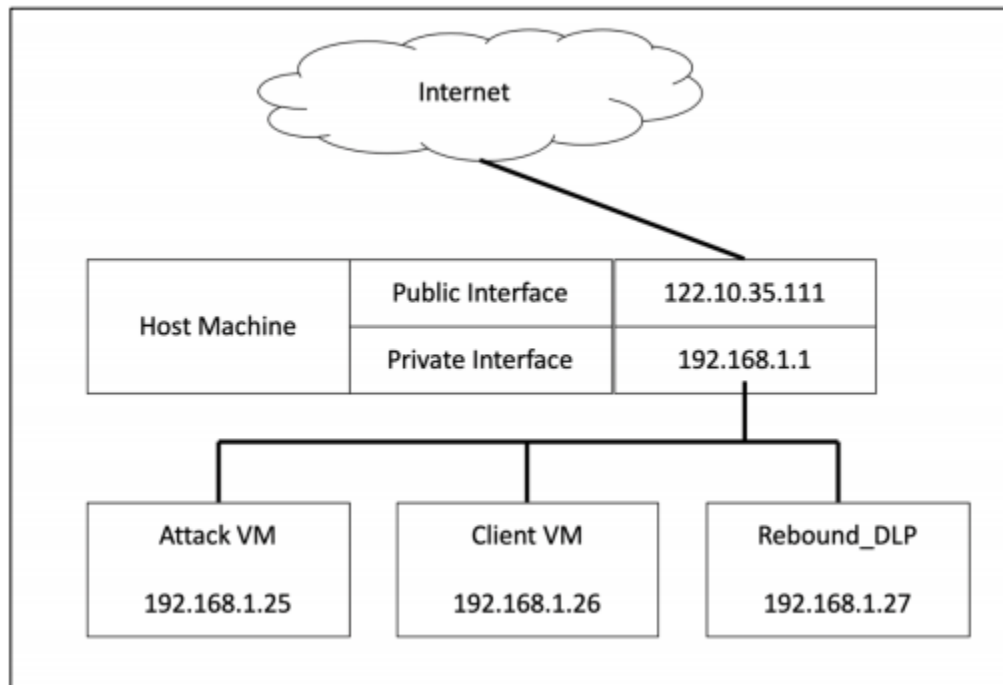
Be sure you understand the networking nuances of how you configure the virtual machines for whatever product you use.

The networking configuration should be of the "NAT" variety, such that the virtual machines are on the same virtual subnet and assigned IP addresses from the host machine. Internet access for the virtual machines may or may not be allowed, depending on our usage scenario, but this is relatively easy to configure either way.

You will need to create an environment with three virtual machines that are "NAT"-ed with the host:

1. Parrot Linux, Kali Linux, or another "Attack" system.
2. A "Client" system with a client operating system of your choice.
3. The "Rebound\_DLP" appliance (This will be provided by me).

Here is an example configuration. Your IP addresses will probably be different.



These are the known use cases (AND DATA FLOWS!) for this sample environment:

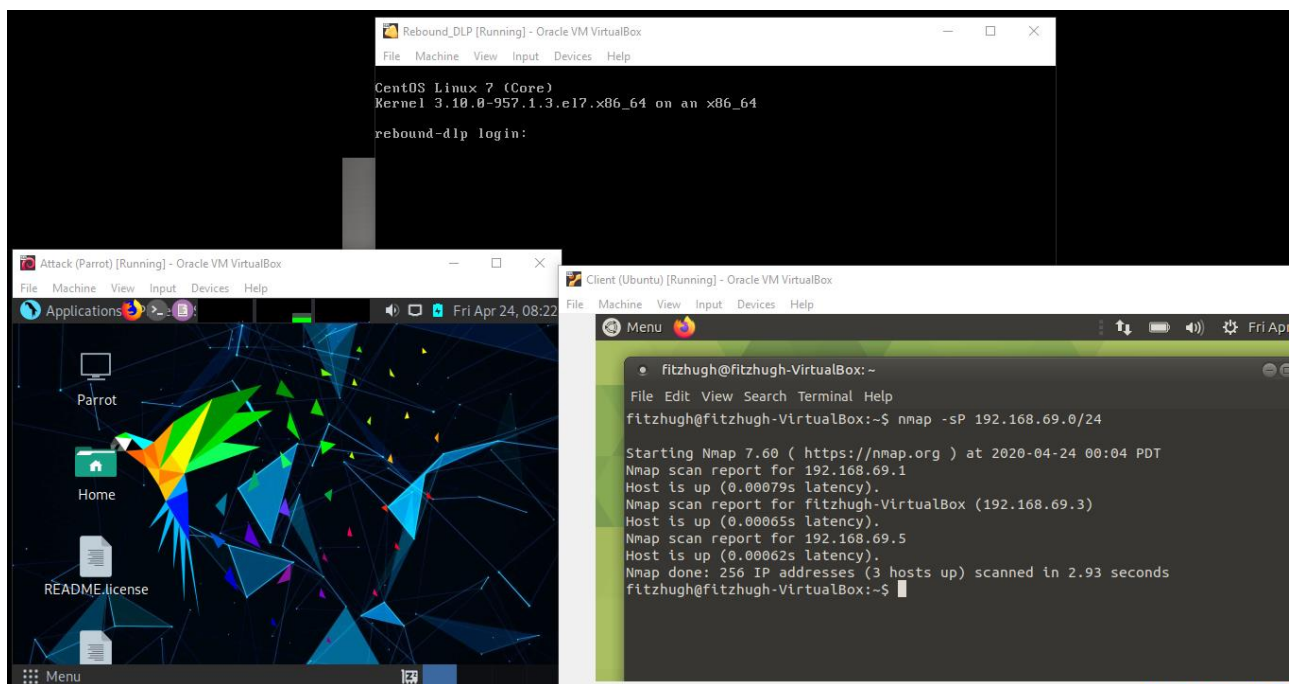
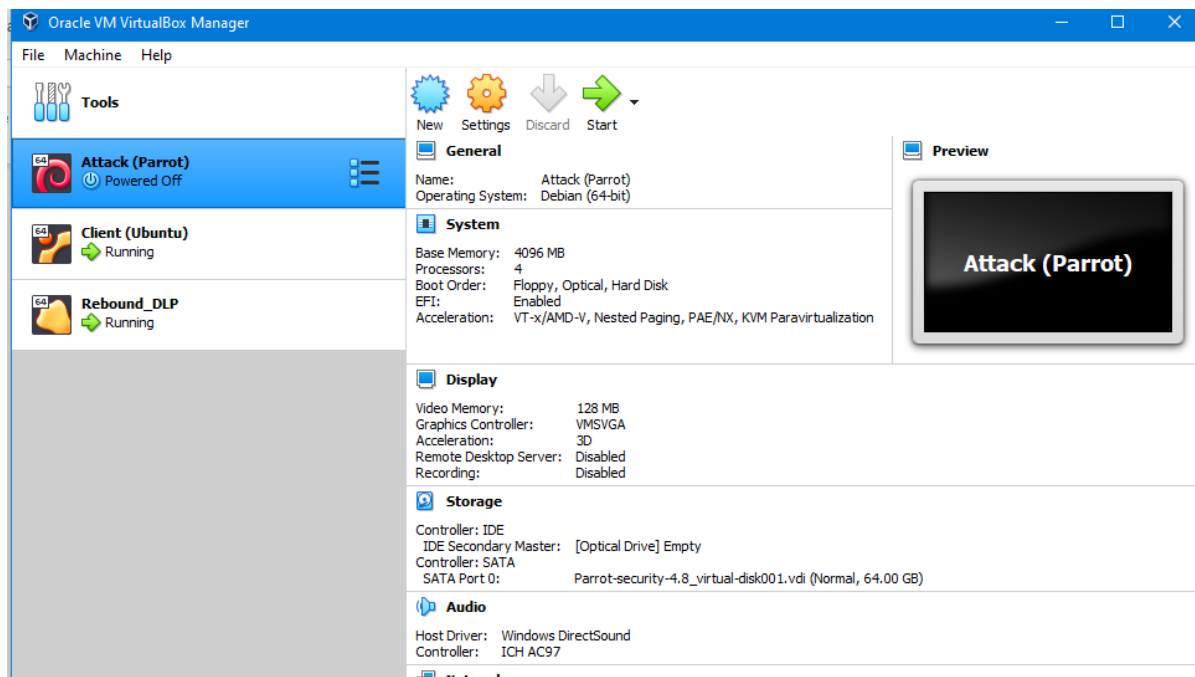
1. The "Client" system writes syslog events to the "Rebound\_DLP" appliance.
2. The "Client" system also uses a web browser to access the web application on "Rebound\_DLP".

**1. Create the virtual lab environment with three virtual machines.**

- a. Parrot Linux, Kali Linux, or another "Attack" system.
- b. A "Client" system with a client operating system of your choice.
- c. The "Rebound\_DLP" appliance.

Both the OVF (Rebound\_DLP.zip) and OVA (Rebound\_DLP.ova) versions of the Rebound\_DLP appliance are available at [https://drive.google.com/drive/folders/11smEhOAYgKURHQQJ1SVFNkN-2\\_OgL-0y](https://drive.google.com/drive/folders/11smEhOAYgKURHQQJ1SVFNkN-2_OgL-0y).

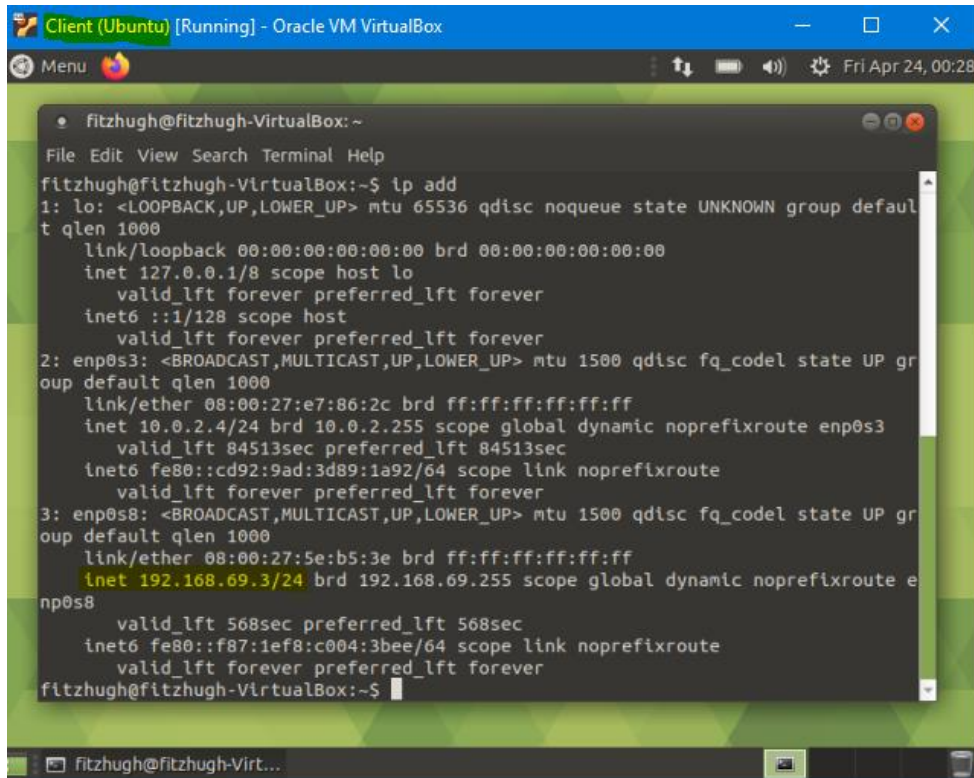
Below are screenshots showing my three virtual machines: Attack; Client; and Rebound\_DLP.



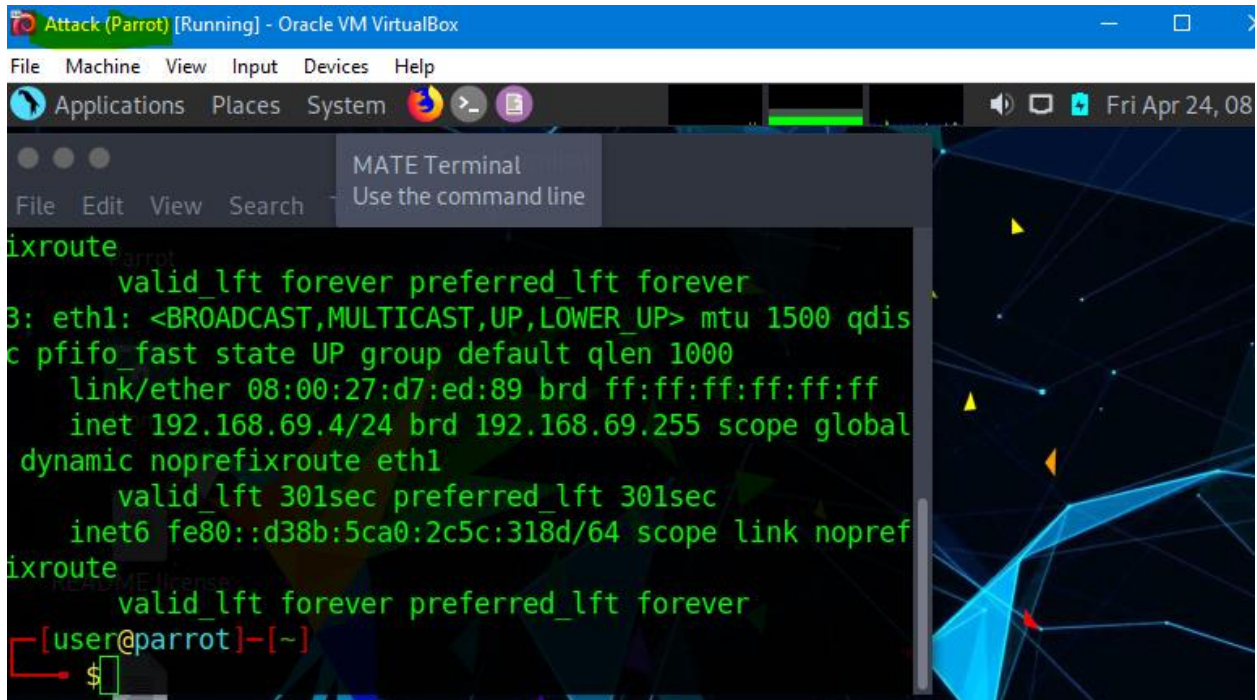
My machines are configured with a NAT adapter, which allows them to connect to the Internet, as well as a host-only network adapter, which allows them to communicate with each other and my host machine. I couldn't figure out how to allow my virtual machines to communicate with each other only using NAT on VirtualBox. This setup was what I was taught in my Unix Admin class, so that is what I will be using until told how to setup otherwise.

## 2. If possible, obtain the IP address for the "Rebound\_DLP" appliance. If not, explain why.

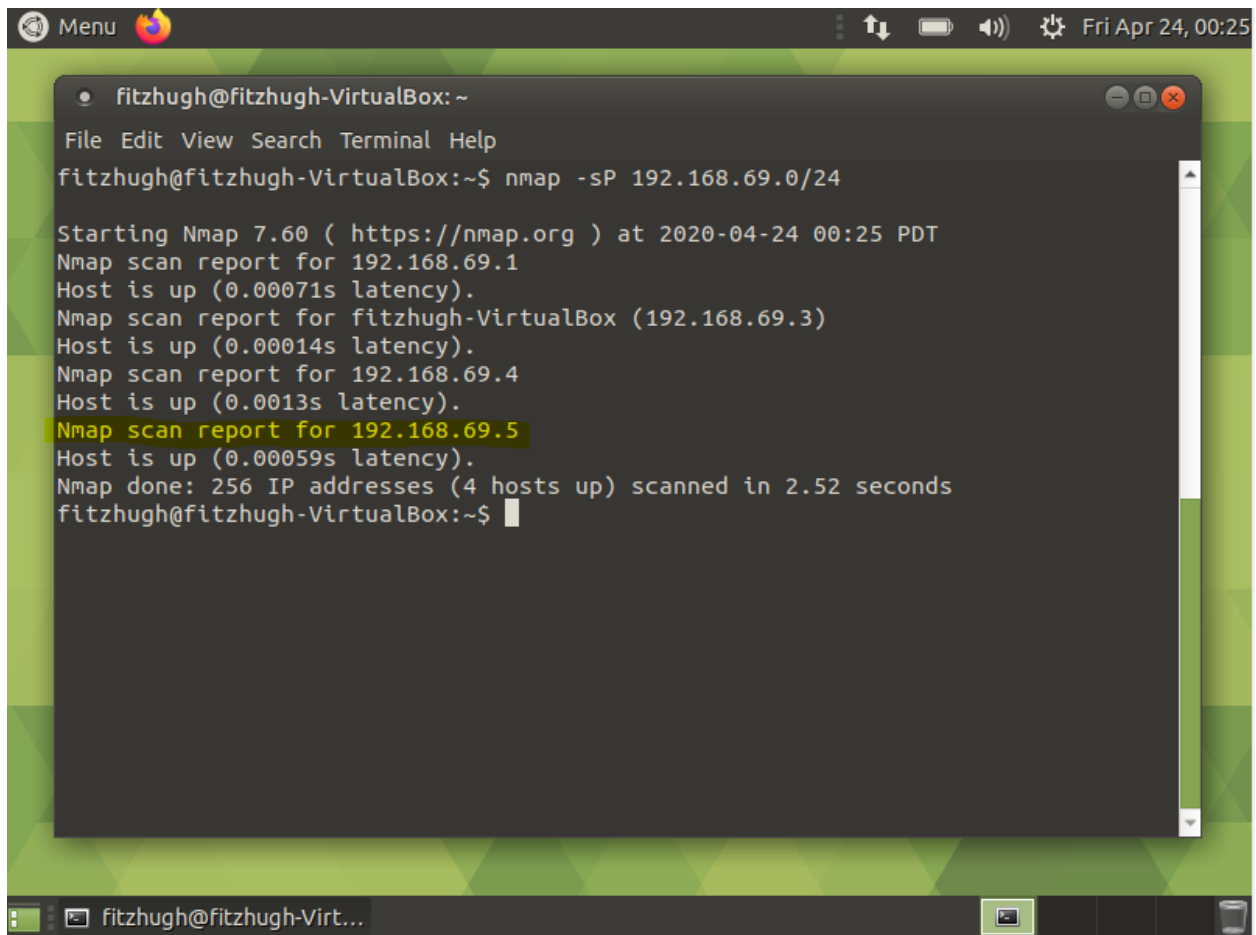
As I have the Rebound\_DLP appliance on my virtual network with my other machines, I am able to use nmap to discover the IP address for Rebound\_DLP. As seen in the screenshot below, I used nmap on my network. I had already run the command "ip add" on my Attack and Client machines to discover their IP addresses, which leaves the IP address for Rebound\_DLP as 192.168.69.5.



```
Client (Ubuntu) [Running] - Oracle VM VirtualBox
Menu
fitzhugh@fitzhugh-VirtualBox: ~
File Edit View Search Terminal Help
fitzhugh@fitzhugh-VirtualBox:~$ ip add
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
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:e7:86:2c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 84513sec preferred_lft 84513sec
    inet6 fe80::cd92:9ad:3d89:1a92/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:5e:b5:3e brd ff:ff:ff:ff:ff:ff
    inet 192.168.69.3/24 brd 192.168.69.255 scope global dynamic noprefixroute enp0s8
        valid_lft 568sec preferred_lft 568sec
    inet6 fe80::f87:1ef8:c004:3bee/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
fitzhugh@fitzhugh-VirtualBox:~$
```



```
Attack (Parrot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
MATE Terminal
Use the command line
ixroute
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:d7:ed:89 brd ff:ff:ff:ff:ff:ff
    inet 192.168.69.4/24 brd 192.168.69.255 scope global dynamic noprefixroute eth1
        valid_lft 301sec preferred_lft 301sec
    inet6 fe80::d38b:5ca0:2c5c:318d/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[user@parrot]-[~]
$
```

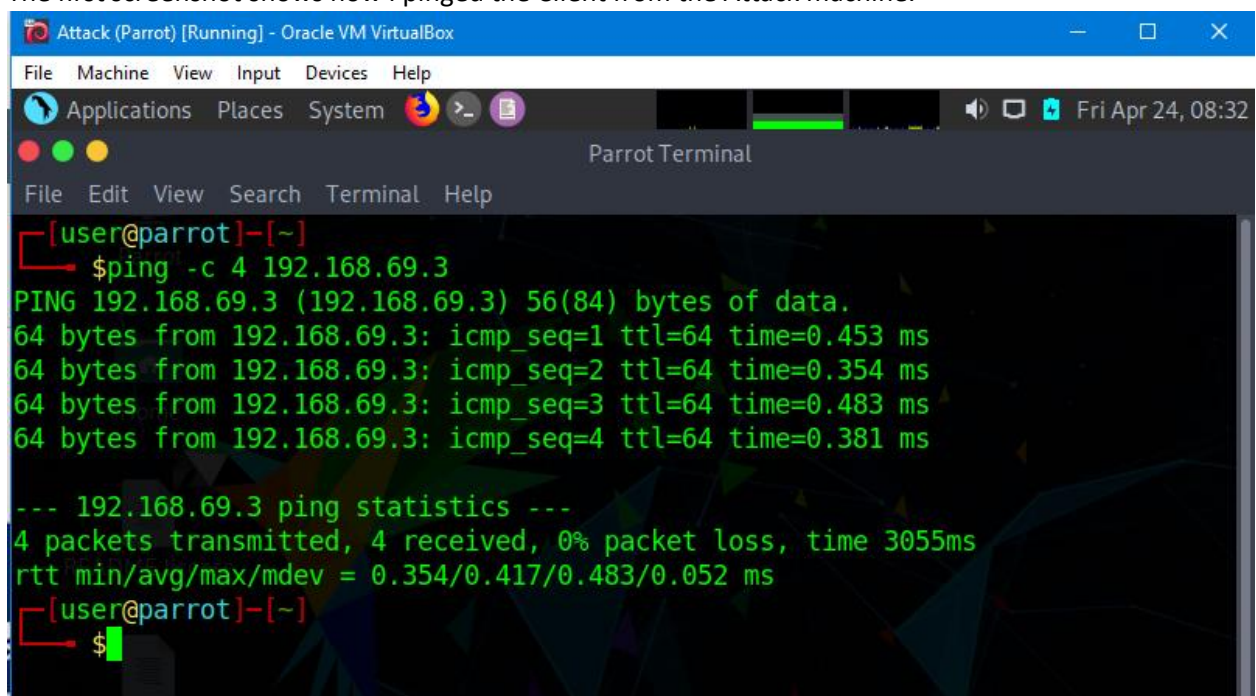


```
fitzhugh@fitzhugh-VirtualBox: ~
File Edit View Search Terminal Help
fitzhugh@fitzhugh-VirtualBox:~$ nmap -sP 192.168.69.0/24

Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-24 00:25 PDT
Nmap scan report for 192.168.69.1
Host is up (0.00071s latency).
Nmap scan report for fitzhugh-VirtualBox (192.168.69.3)
Host is up (0.00014s latency).
Nmap scan report for 192.168.69.4
Host is up (0.0013s latency).
Nmap scan report for 192.168.69.5
Host is up (0.00059s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.52 seconds
fitzhugh@fitzhugh-VirtualBox:~$
```

3. Ping the "Client" system from the "Attack" machine. If possible, ping the "Rebound\_DLP" system from the "Attack" machine.

The first screenshot shows how I pinged the Client from the Attack machine.

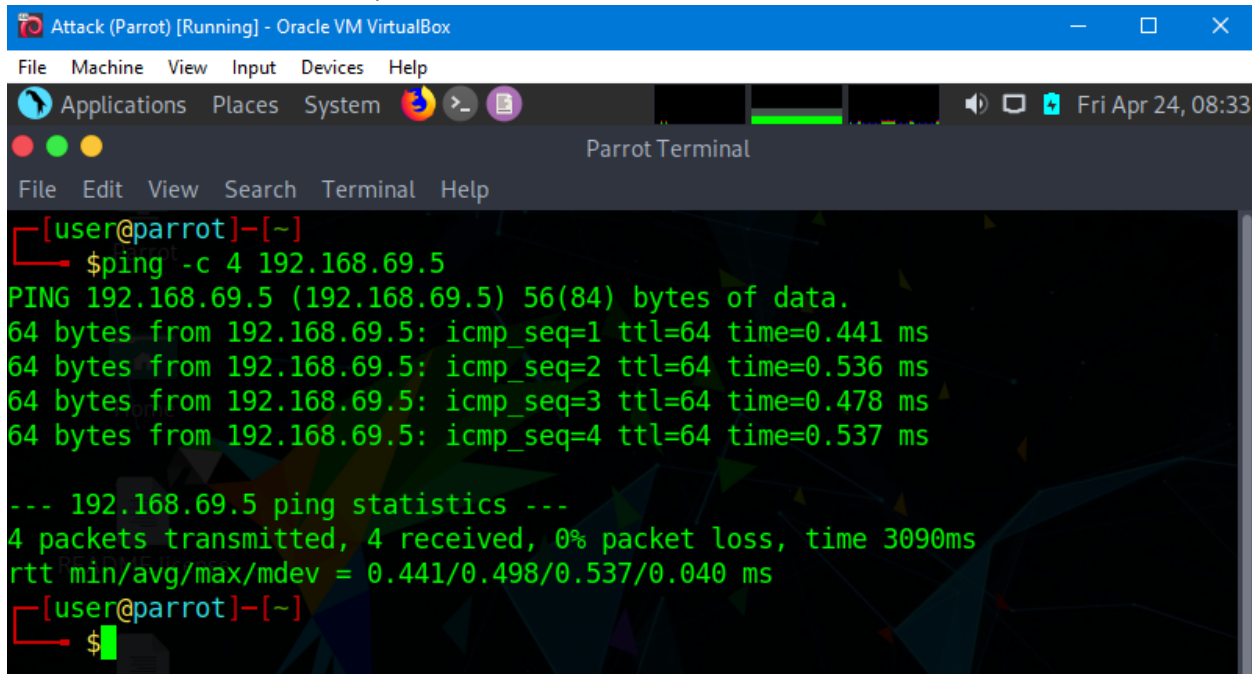


```
Attack (Parrot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]-[~]
$ ping -c 4 192.168.69.3
PING 192.168.69.3 (192.168.69.3) 56(84) bytes of data.
64 bytes from 192.168.69.3: icmp_seq=1 ttl=64 time=0.453 ms
64 bytes from 192.168.69.3: icmp_seq=2 ttl=64 time=0.354 ms
64 bytes from 192.168.69.3: icmp_seq=3 ttl=64 time=0.483 ms
64 bytes from 192.168.69.3: icmp_seq=4 ttl=64 time=0.381 ms

--- 192.168.69.3 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.354/0.417/0.483/0.052 ms
[user@parrot]-[~]
$
```



This second screenshot shows how I pinged the Rebound\_DLP from the Attack machine, using the IP address I discovered from nmap.



```
Attack (Parrot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help

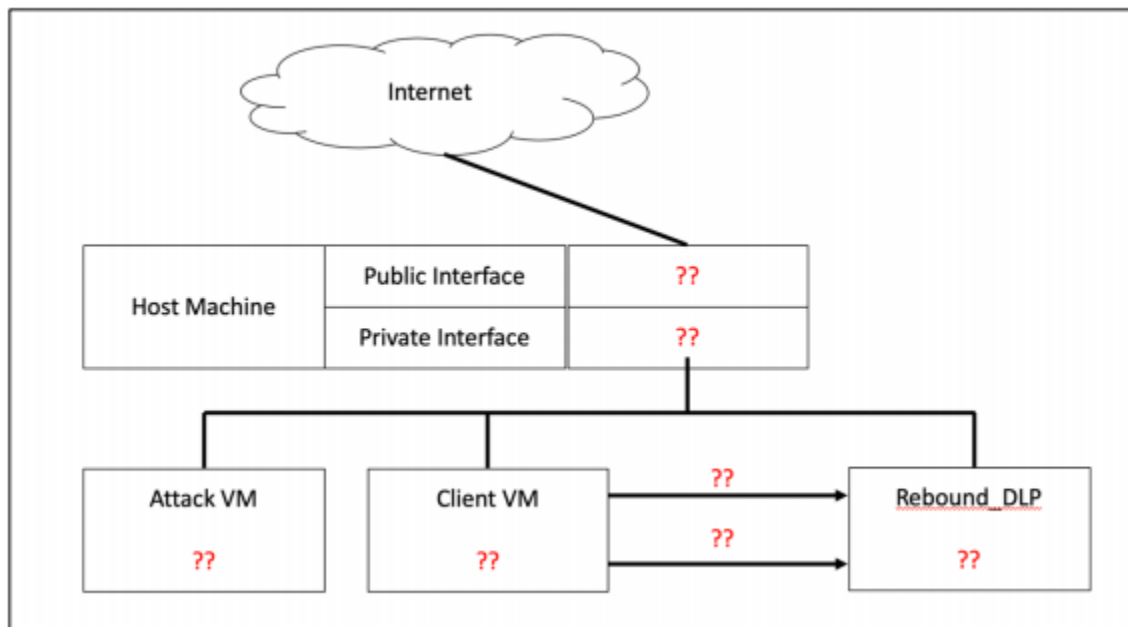
[user@parrot]-[~]
$ping -c 4 192.168.69.5
PING 192.168.69.5 (192.168.69.5) 56(84) bytes of data.
64 bytes from 192.168.69.5: icmp_seq=1 ttl=64 time=0.441 ms
64 bytes from 192.168.69.5: icmp_seq=2 ttl=64 time=0.536 ms
64 bytes from 192.168.69.5: icmp_seq=3 ttl=64 time=0.478 ms
64 bytes from 192.168.69.5: icmp_seq=4 ttl=64 time=0.537 ms

--- 192.168.69.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3090ms
rtt min/avg/max/mdev = 0.441/0.498/0.537/0.040 ms
[user@parrot]-[~]
$
```

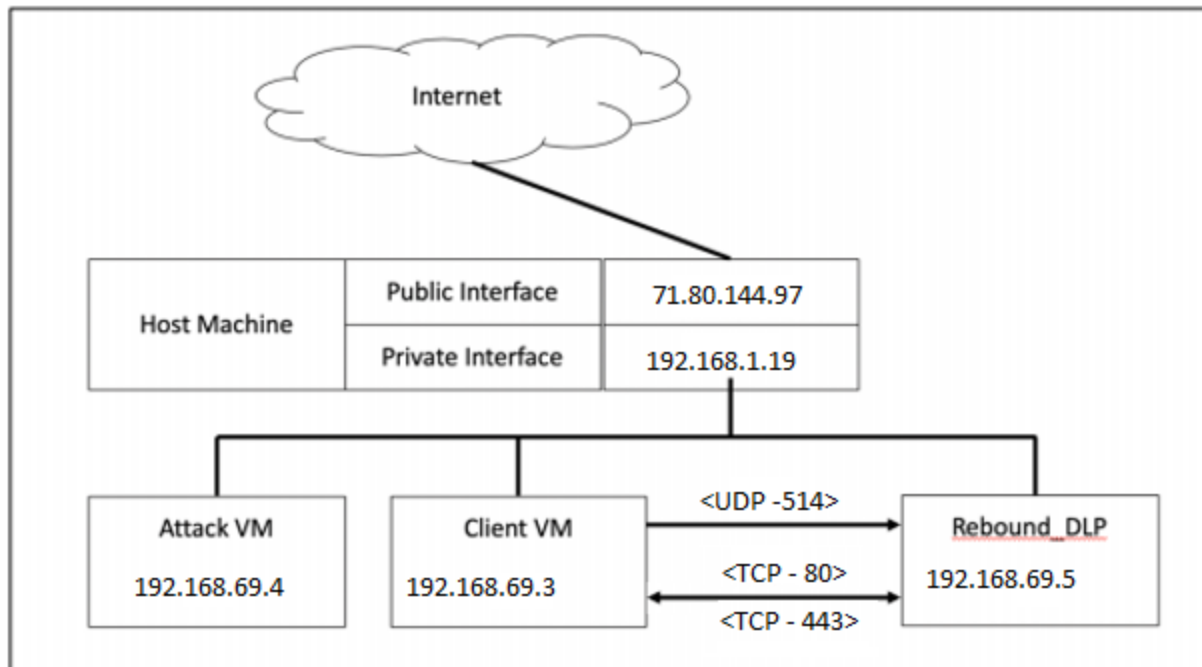
**4. Develop a system architecture diagram that shows the three systems, all known network addresses, and any known data flows.**

A data flow should capture all known protocols and ports used by that use case. For example, if “System1” uses Secure Shell to connect to “System2” then the data flow would be: <SSH – 22>.

Use the following as a template:



Below, is my system architecture diagram that shows my host machine, my three virtual machines, 5 of the known IP addresses, as well as the two data flows of how the Client connects to the Rebound\_DLP appliance (the two known data flows are listed above in Lab Setup).



5. Configure the "Client" system to write syslog events to the "Rebound\_DLP" appliance and send five syslog events.

a. HINT: You can do this in Linux with the 'logger' command. For Windows, you will need a 3rd party solution.

To configure the Client to write syslog events to Rebound\_DLP, I've configured Rsyslog as a client. I've added "`*.* @192.168.69.5:514`" to the end `/etc/rsyslog.conf`. This line will have log files sent to Rebound\_DLP over UDP using port 514. The second screenshot shows 5 syslog events sent.

```

fitzhugh@fitzhugh-VirtualBox: ~
File Edit View Search Terminal Help
#
# Set the default permissions for all log files.
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog
#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.* @192.168.69.5:514
fitzhugh@fitzhugh-VirtualBox:~$

```

```

fitzhugh@fitzhugh-VirtualBox: ~
File Edit View Search Terminal Help
fitzhugh@fitzhugh-VirtualBox:~$ logger "hello world"
fitzhugh@fitzhugh-VirtualBox:~$ logger "test"
fitzhugh@fitzhugh-VirtualBox:~$ logger "test2"
fitzhugh@fitzhugh-VirtualBox:~$ logger "hi"
fitzhugh@fitzhugh-VirtualBox:~$ logger "bye"
fitzhugh@fitzhugh-VirtualBox:~$

```

**6. Is there a way to confirm that the "Client" syslog data is being sent to the "Rebound\_DLP" appliance without actually accessing the appliance? Explain.**

Currently, there is no way to confirm that syslog data is being sent to Rebound\_DLP. This is because we are not able to access the appliance. Without accessing the client, we are not able to view the syslog folder to see what syslog data it contains.

## **B. RECONNAISSANCE**

First, let's perform some reconnaissance on the company website.

**7. Run "nslookup" on reboundsecurity.info. Where is this website hosted?**

Nslookup on reboundsecurity.info provides us with an IP address of 52.218.253.74. A whois on that IP address, as well as on reboundsecurity.info, tells us reboundsecurity.info is hosted through Amazon Technologies Inc server and registered through gandi.net; in Washington state.

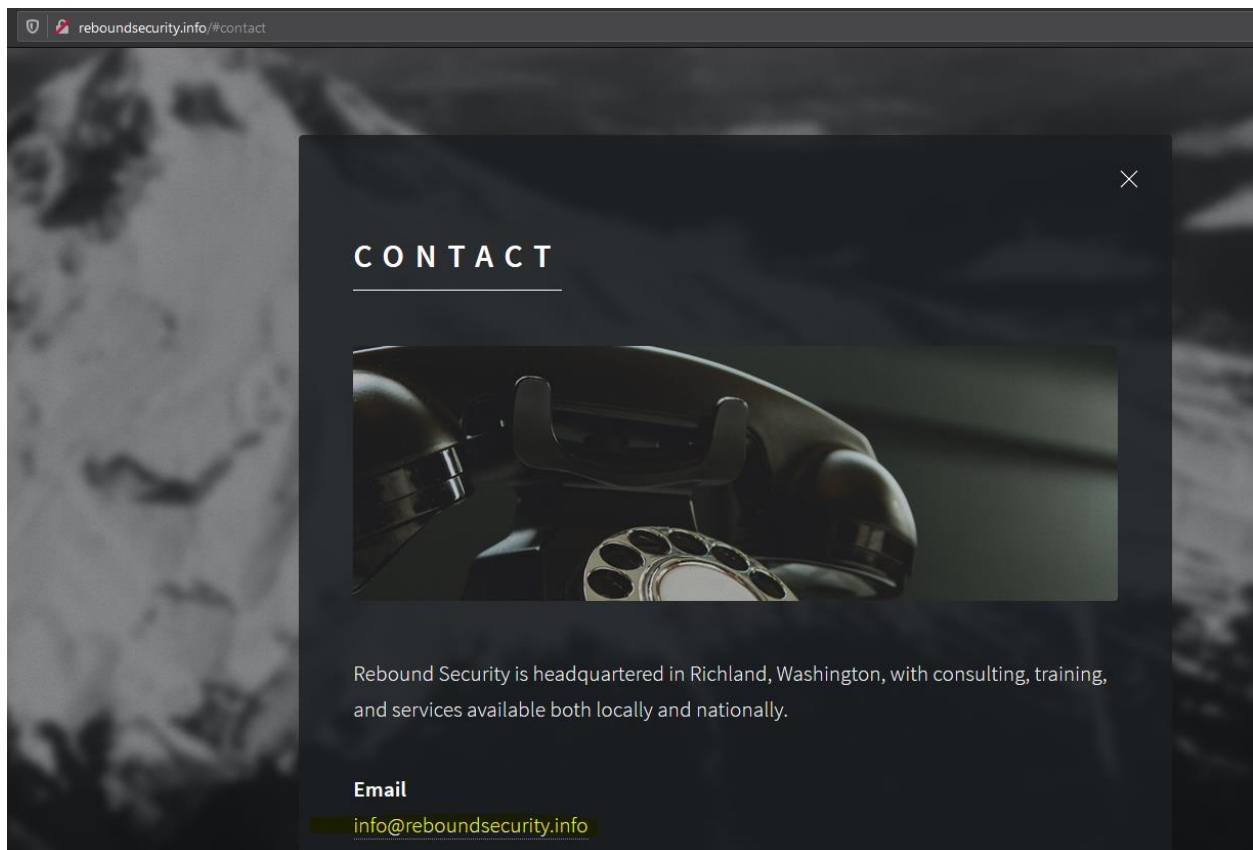
```
fitzhugh@fitzhugh-VirtualBox: ~  
File Edit View Search Terminal Help  
fitzhugh@fitzhugh-VirtualBox:~$ nslookup reboundsecurity.info  
Server:          127.0.0.53  
Address:         127.0.0.53#53  
  
Non-authoritative answer:  
Name:   reboundsecurity.info  
Address: 52.218.253.74  
  
fitzhugh@fitzhugh-VirtualBox:~$ whois 52.218.253.74  
  
#  
# ARIN WHOIS data and services are subject to the Terms of Use  
# available at: https://www.arin.net/resources/registry/whois/tou/  
#  
# If you see inaccuracies in the results, please report at  
# https://www.arin.net/resources/registry/whois/inaccuracy\_reporting/  
#  
# Copyright 1997-2020, American Registry for Internet Numbers, Ltd.  
#  
  
NetRange: 52.192.0.0 - 52.223.255.255  
CIDR: 52.192.0.0/11  
NetName: AT-88-Z  
NetHandle: NET-52-192-0-0-1  
Parent: NET52 (NET-52-0-0-0-0)  
NetType: Direct Allocation  
OriginAS:  
Organization: Amazon Technologies Inc. (AT-88-Z)  
RegDate: 2015-09-02  
Updated: 2015-09-02  
Ref: https://rdap.arin.net/registry/ip/52.192.0.0
```



```
fitzhugh@fitzhugh-VirtualBox:~$ whois reboundsecurity.info
Domain Name: REBOUNDSECURITY.INFO
Registry Domain ID: D503300000489763420-LRMS
Registrar WHOIS Server: whois.gandi.net
Registrar URL: https://www.gandi.net/whois
Updated Date: 2019-12-01T23:13:06Z
Creation Date: 2019-01-04T21:03:54Z
Registry Expiry Date: 2021-01-04T21:03:54Z
Registrar Registration Expiration Date:
Registrar: Gandi SAS
Registrar IANA ID: 81
Registrar Abuse Contact Email: abuse@support.gandi.net
Registrar Abuse Contact Phone: +33.170377661
Reseller:
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registrant Organization:
Registrant State/Province: WA
Registrant Country: US
Name Server: NS-1574.AWSDNS-04.CO.UK
Name Server: NS-189.AWSDNS-23.COM
Name Server: NS-612.AWSDNS-12.NET
Name Server: NS-1328.AWSDNS-38.ORG
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form is https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2020-04-25T02:43:34Z <<<
```

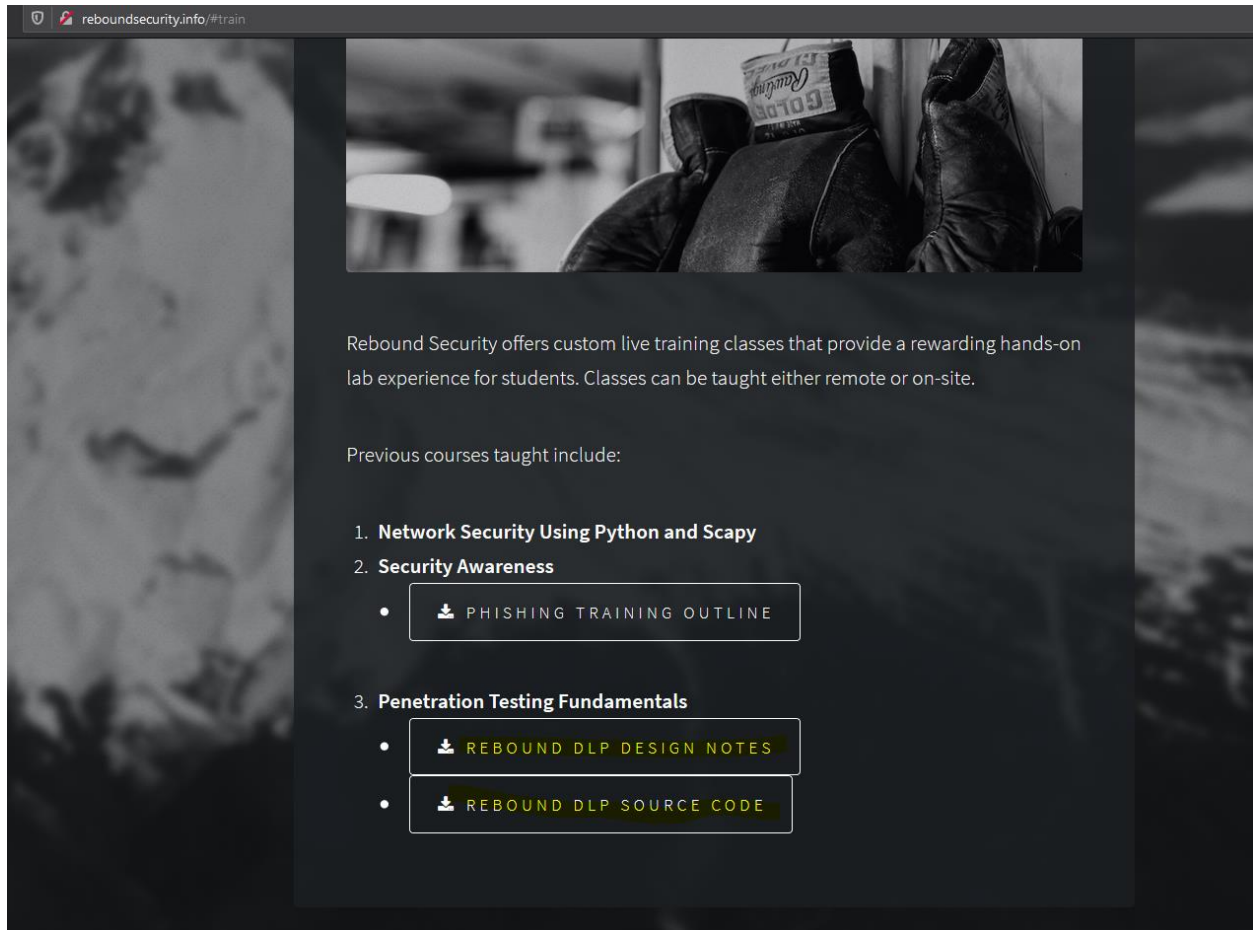
**8. Manually browse the reboundsecurity.info website and obtain the published contact email address. What is it?**

The contact email address is [info@reboundsecurity.info](mailto:info@reboundsecurity.info).



**9. There are two documents on the website that could be helpful for the penetration test. What are they?**

The two documents on the website that could be helpful for the penetration test are Rebound DLP Design Notes and Rebound DLP Source Code.



Analyze the source code document to obtain:

**10. The support account's email address.**

The email address is listed as username@reboundsecurity.info, so the support account's email address will be [support@reboundsecurity.info](mailto:support@reboundsecurity.info).

```
← → ↺ 🏠 reboundsecurity.info/train/dlp_web_src.txt

import random
import md5

def application(env, start_response):

    # DLP appliance support login:
    # username: support
    # email: username@reboundsecurity.info
    # password (!SHA2!): 275c38464deb2fa3a5cbb8f34debb109
    #
    #
    # Written by Fink-Nottle
    #

    # HTTP STATUS CODE
    status = '200 OK'
    MAXE = 75
    MAXW = 130

    # SET SOME METADATA
    product_name = 'Rebound DLP'
    product_version = '1.0.1'
```

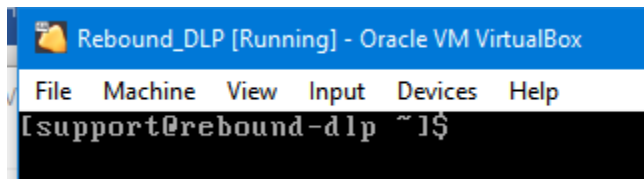
#### 11. The support account's password if possible. If not, describe why.

The hash for the support account's password is 275c38464deb2fa3a5cbb8f34debb109. It looks like it's hashed with SHA-2 from the (!SHA2!) listed before the password hash. I would not be able to determine what the password is using that hash if hashed with SHA-2 because SHA2 is secure and I do not have the time or the tools needed to try to crack it.

However, the top of the source code file also lists "import md5". If you run the password hash through a MD5 hash decoder, you get a password of "thirdday."

Found : **thirdday**  
(hash = 275c38464deb2fa3a5cbb8f34debb109)

Using the username "support" and the password found above, I was able to successfully log into the Rebound\_DLP appliance. The successful log in tells me that the password is hashed with MD5 and that the password is "thirdday."



Analyze the design notes document to obtain:

#### 12. The support engineer's email address.

The support engineer's email address is [parsloe@reboundsecurity.info](mailto:parsloe@reboundsecurity.info).

#### 4. Author Information

BY SIR GREGORY PARSLOE-PARSLOE

[parsloe@reboundsecurity.info](mailto:parsloe@reboundsecurity.info)

#### 13. What is metadata analysis and how important is it in penetration testing?

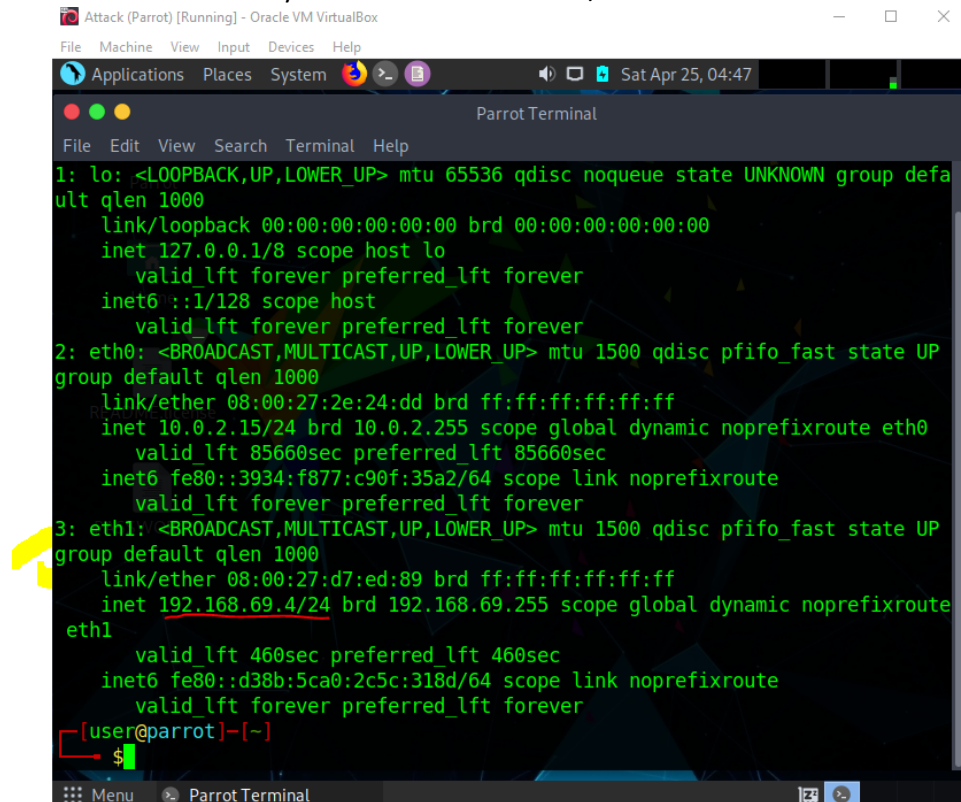
- a. HINT 1: It is very, very important.
- b. HINT 2: There is a reason I am asking this question now.

Metadata can be defined as information about a file such as author, the date & time of creation, where it was created, etc (One, pg. 194). Metadata analysis is analyzing the metadata on a file. This is important in penetration testing because we can gather personal information such as who created a file and what their email is. Such information can be used in a social engineering attack.

Now, let's complete some reconnaissance on the local appliance.

#### 14. Use your "Attack" system to get the /24 network address.

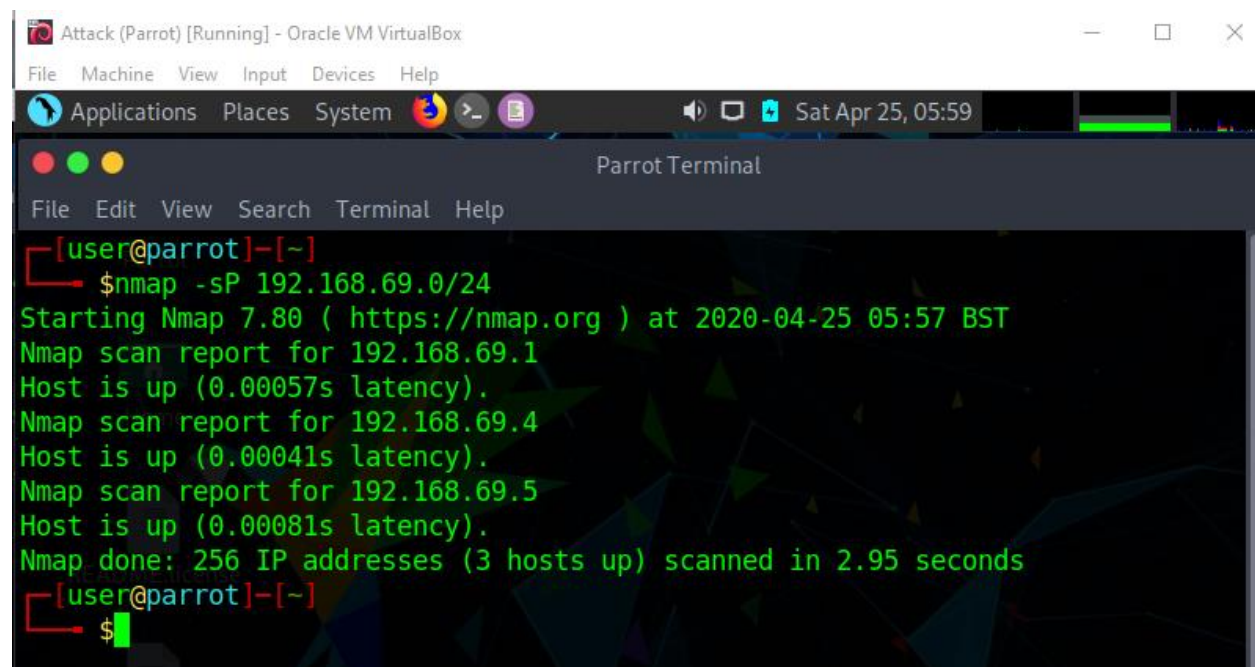
The /24 network address of my attack system is 192.168.69.4/24. It can be deduced that the /24 network address for my network is 192.168.69.0/24.



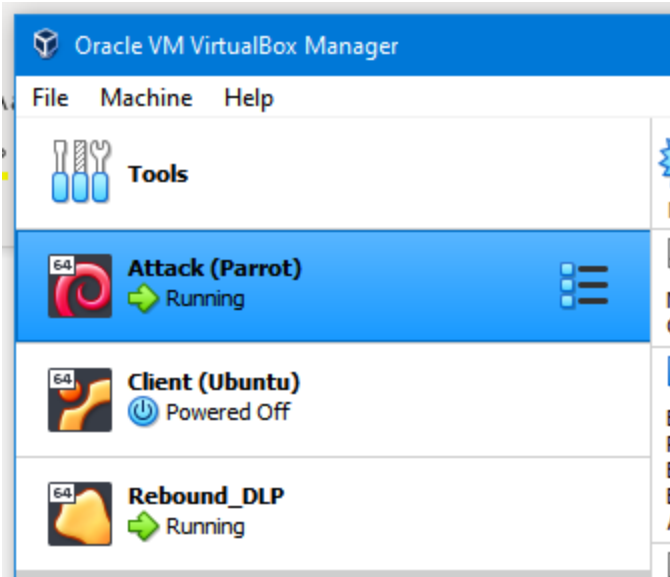
```
Attack (Parrot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
ult qlen 1000
  link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
  inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
  inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
  link/ether 08:00:27:2e:24:dd brd ff:ff:ff:ff:ff:ff
  inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
    valid_lft 85660sec preferred_lft 85660sec
  inet6 fe80::3934:f877:c90f:35a2/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
  link/ether 08:00:27:d7:ed:89 brd ff:ff:ff:ff:ff:ff
  inet 192.168.69.4/24 brd 192.168.69.255 scope global dynamic noprefixroute
    eth1
    valid_lft 460sec preferred_lft 460sec
  inet6 fe80::d38b:5ca0:2c5c:318d/64 scope link noprefixroute
    valid_lft forever preferred_lft forever
[user@parrot]~$
```

#### 15. Run a Nmap ping scan on the /24 network to see which hosts are "up".

Running nmap from my Attack machine on my /24 network shows there are two hosts up: 192.168.69.4 (Attack machine) and 192.168.69.5 (Rebound\_DLP). I can confirm this with Oracle, which shows my Attack machine and Rebound\_DLP as running.



```
Attack (Parrot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]~$ nmap -sP 192.168.69.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-25 05:57 BST
Nmap scan report for 192.168.69.1
Host is up (0.00057s latency).
Nmap scan report for 192.168.69.4
Host is up (0.00041s latency).
Nmap scan report for 192.168.69.5
Host is up (0.00081s latency).
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.95 seconds
[user@parrot]~$
```



16. For the "Rebound\_DLP" system, run a Nmap TCP full connect scan.

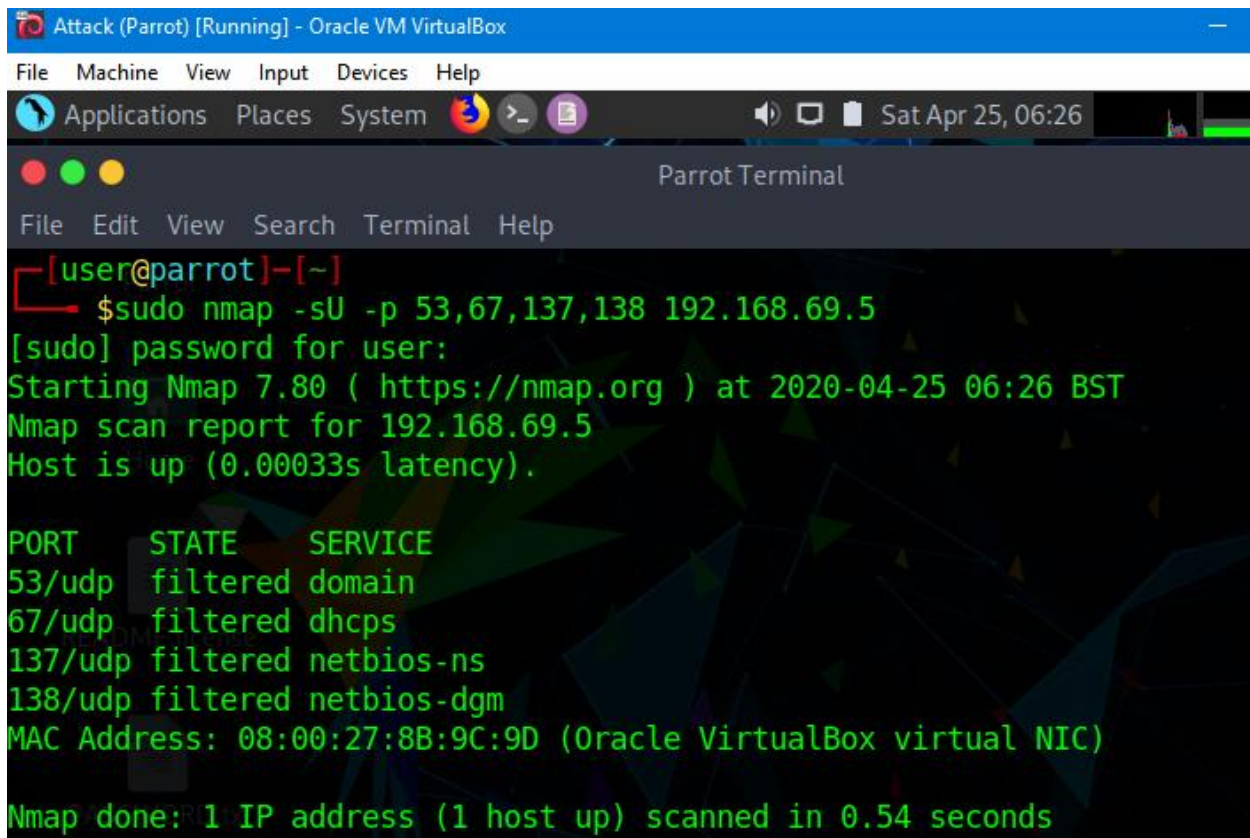
The results of running an nmap TCP full connect scan on Rebound\_DLP can be seen in the screenshot below. It found there were four open ports: 22/TCP, SSH; 80/TCP, HTTP; 443/TCP, HTTPS; and 514/TCP shell.

The screenshot shows a Parrot Terminal window titled 'Attack (Parrot) [Running] - Oracle VM VirtualBox'. The terminal has a menu bar with 'File', 'Edit', 'View', 'Search', 'Terminal', and 'Help'. The user is at the prompt '[user@parrot]-[~]' and has entered the command '\$nmap -sT 192.168.69.5'. The output of the scan is displayed in green text: 'Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-25 06:17 BST', 'Nmap scan report for 192.168.69.5', 'Host is up (0.0015s latency).', 'Not shown: 996 filtered ports', and a table of open ports. The table has three columns: 'PORT', 'STATE', and 'SERVICE'. The open ports are 22/tcp (ssh), 80/tcp (http), 443/tcp (https), and 514/tcp (shell). At the bottom, it says 'Nmap done: 1 IP address (1 host up) scanned in 8.21 seconds'. The user is now at the prompt '[user@parrot]-[~]' and has entered '\$' followed by a cursor.



17. For the "Rebound\_DLP" system, run a Nmap UDP scan for DNS, DHCP, and NetBIOS ports. What does their reported state mean?

The screenshot below shows the results for an nmap UDP scan for the DNS, DHCP and NetBIOS ports on Rebound\_DLP. All show a filtered state. According to nmap.org, filtered means nmap could not figure out if the port is open; this could be due to a firewall or router rules.



```
Attack (Parrot) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places System >_ Sat Apr 25, 06:26
Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]~$ sudo nmap -sU -p 53,67,137,138 192.168.69.5
[sudo] password for user:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-04-25 06:26 BST
Nmap scan report for 192.168.69.5
Host is up (0.00033s latency).

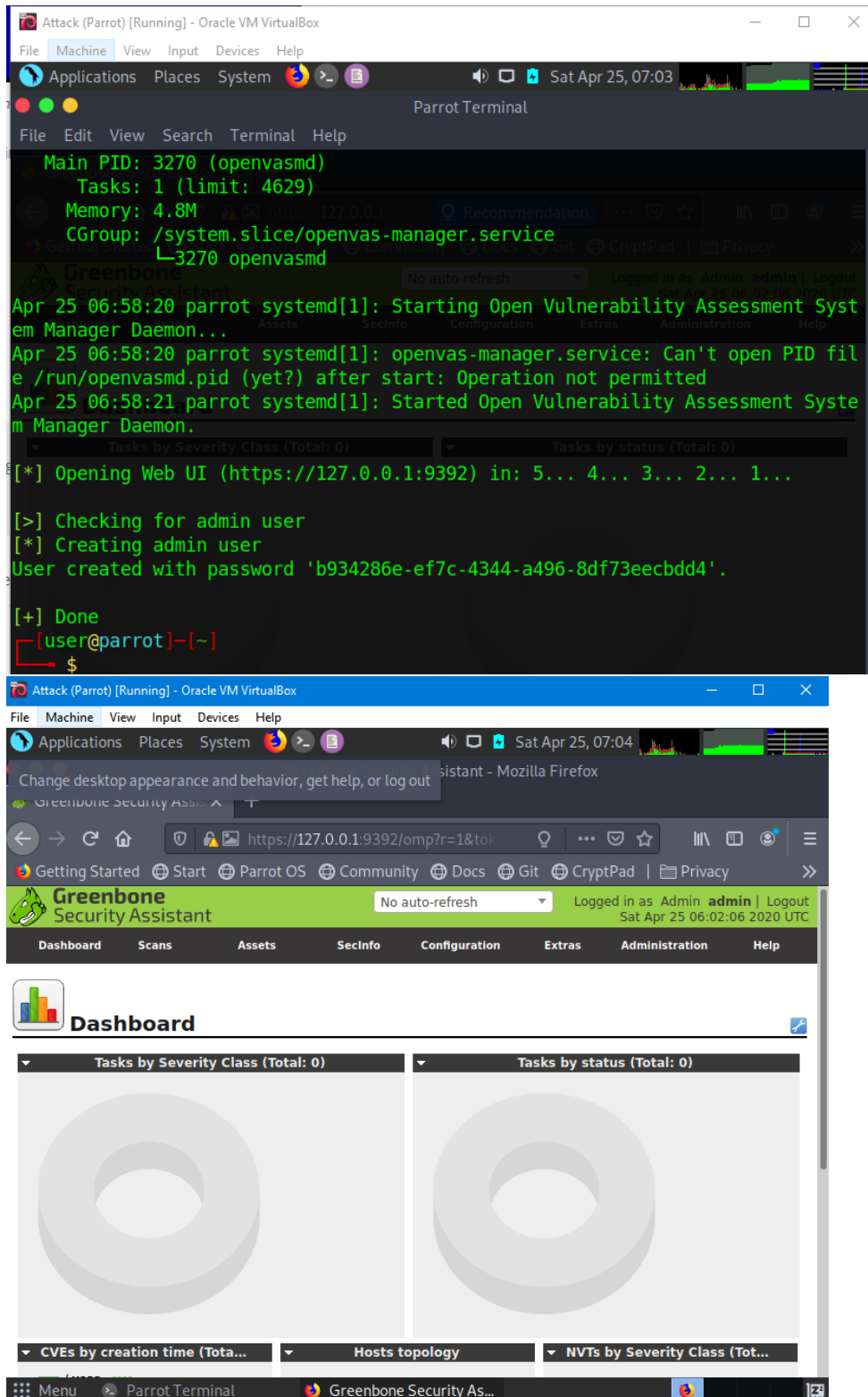
PORT      STATE      SERVICE
53/udp    filtered   domain
67/udp    filtered   dhcp
137/udp   filtered   netbios-ns
138/udp   filtered   netbios-dgm
MAC Address: 08:00:27:8B:9C:9D (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

## C. VULNERABILITY SCANNING

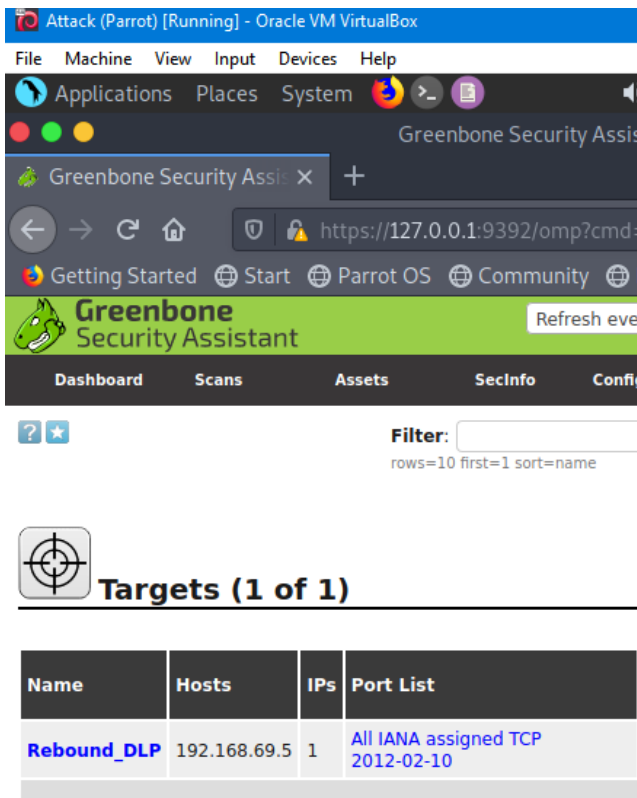
18. If needed, install OpenVAS on your "Attack" system. Confirm it is working properly by connecting to the OpenVAS Web Interface.

The first screenshot shows OpenVAS has finished installing on my Attack machine, while the second screenshot shows I have connected to the OpenVAS Web Interface.



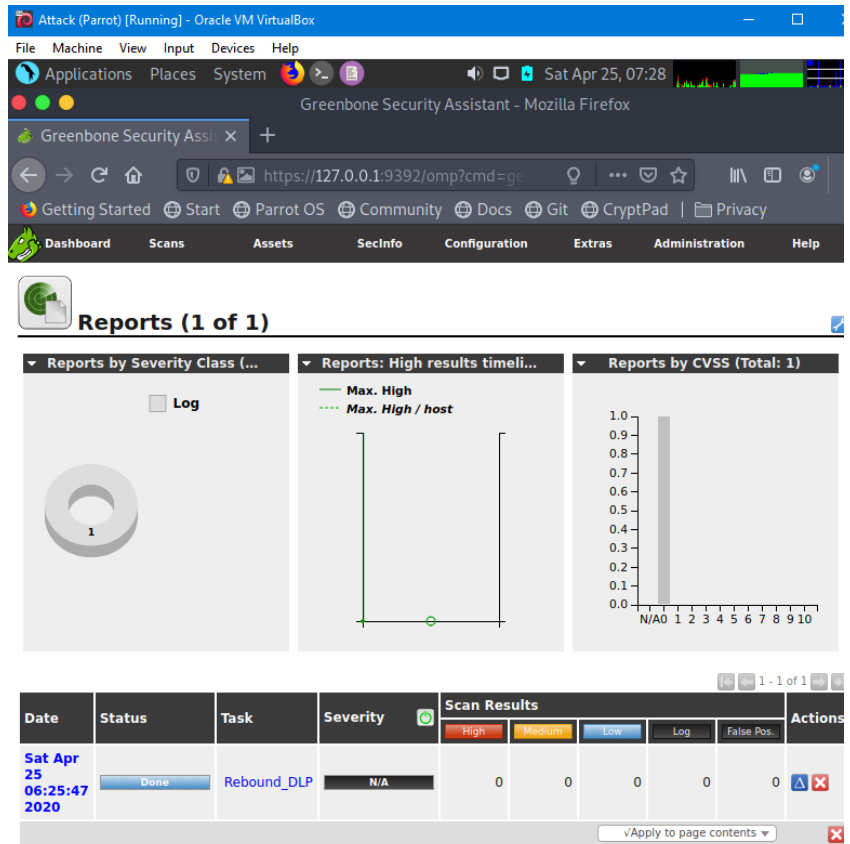
## 19. Run a non-credentialed scan of the "Rebound\_DLP" appliance and list the vulnerabilities reported.

The results of running a non-credentialed scan on Rebound\_DLP are in the screenshots below. It found no vulnerabilities. The first screenshot shows that I have made a target on OpenVAS with the IP address of Rebound\_DLP. The second screenshot shows how the scan from OpenVAS did not find any vulnerabilities. I can also see that the OpenVAS tool can find logs, as well.



The screenshot shows the Greenbone Security Assistant web interface. The 'Targets' section is active, displaying a table with one target:

Name	Hosts	IPs	Port List
Rebound_DLP	192.168.69.5	1	All IANA assigned TCP 2012-02-10



The screenshot shows the Greenbone Security Assistant web interface, specifically the 'Reports' section. It displays a summary of scan results for the target 'Rebound\_DLP'.

**Reports (1 of 1)**

- Reports by Severity Class (Log):** A donut chart showing 1 log.
- Reports: High results timeli...:** A line graph showing 'Max. High' and 'Max. High / host' results.
- Reports by CVSS (Total: 1):** A bar chart showing the distribution of CVSS scores.

**Scan Results Table:**

Date	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Sat Apr 25 06:25:47 2020	Done	Rebound_DLP	N/A	0	0	0	0	0	

## 20. What would you expect to see differently in the report if you had the ability to run a credentialed scan?

If I was able to run a credentialed scan, I would expect to be able to find vulnerabilities, as well as see the number of logs on the appliance. The video tutorial I was watching on Youtube, from I.T Security Labs, shows they were able to find a number of vulnerabilities, such as weak password, when running a credentialed scan.

## D. SOCIAL ENGINEERING

### 21. You need to obtain sudo credentials to the Rebound\_DLP appliance to continue your penetration test. Using social engineering techniques is one approach. Describe a \*technical\* way you could obtain sudo credentials.

A technical way to obtain sudo credentials for Rebound\_DLP could be session hijacking, such as session sniffing, to sniff credentials to log onto the server.

**22. Identify a specific social engineering motivation technique from the discussion notes that you will use. Then use online sources, and your own creativity, to write an example phishing email for use against Rebound Security.**

a. IMPORTANT: Your goal is to obtain sudo or root login credentials to the Rebound\_DLP appliance. You should craft your phishing email with this goal in mind.

b. You might find the resources at [http://reboundsecurity.info/train/Phishing\\_Training\\_Outline.txt](http://reboundsecurity.info/train/Phishing_Training_Outline.txt) helpful.

The phishing email I would use to gain sudo or root login credentials is as follows:

Hey Rebound Security Team!

I need sudo or root access to be able to view the yum.log for my application report. I'm not able to access it from my login. If you could, please, respond with the password. It will help me get this report finished in time!

Thanks,

Gussie Fink-Nottle

**23. List the email addresses you have obtained so far. Depending on your success (or lack thereof) so far, you may have as few as 0 or as many as 5 reboundsecurity.info email addresses.**

The emails I have obtained so far are:

- eric.robinson@reboundsecurity.info
- info@reboundsecurity.info
- username@reboundsecurity.info
- parsloe@reboundsecurity.info

**24. Send the example phishing email to all the reboundsecurity.info email addresses that have been discovered from the testing so far.**

a. HINT 1: Of all the email addresses you have obtained, only one specific email address will be successful with a 1)\*well-written\* and 2)\*targeted\* phishing email.

b. HINT 2: The CEO's email address is not that specific one as he is well-trained in phishing and probably won't succumb. However, you should still include it in your campaign.

The screenshot below shows my phishing email to all Rebound Security emails found so far.

Regarding Rebound\_DLP

Yahoo/Sent ★



Kia <redeyesyami@yahoo.com>

To: eric.robinson@reboundsecurity.info, info@reboundsecurity.info, username@reboundsecurity.info, parsloe@reboundsecurity.info



Sat, Apr 25 at 12:35 AM ★

Hey Rebound Security Team!

I need sudo or root access to be able to view the yum.log for my application report. I'm not able to access it from my login. If you could, please, respond with the password. It will help me get this report finished in time!

Thanks,

Gussie Fink-Nottle

I immediately got two response—there was a failure sending the email to both username@reboundsecurity.info and parsloe@reboundsecurity.info.

**25. What are "average" response rates for phishing emails out "in the wild"? Research this question and cite any references you use.**

According to SecurityIntelligence, the average response rate for phishing emails is 20%. According to CioSummits, the average response rate is 27%. These stats show that 1 out of 5, and even possibly 1 out of 4, people responds to a phishing email.

<https://securityintelligence.com/news/employee-training-lowers-susceptibility-to-phishing-emails-report-finds/>

<https://www.ciosummits.com/KnowBe4-Phishing-By-Industry-Benchmarking-Report.pdf>