Talal Jawaid

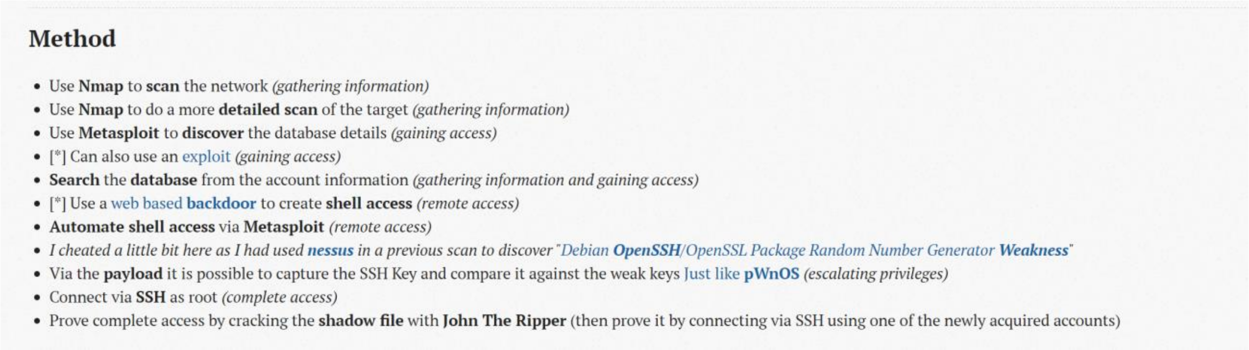
10/13/2019

CSC 154

Lab 2

Metasploit Tikiwiki exploit

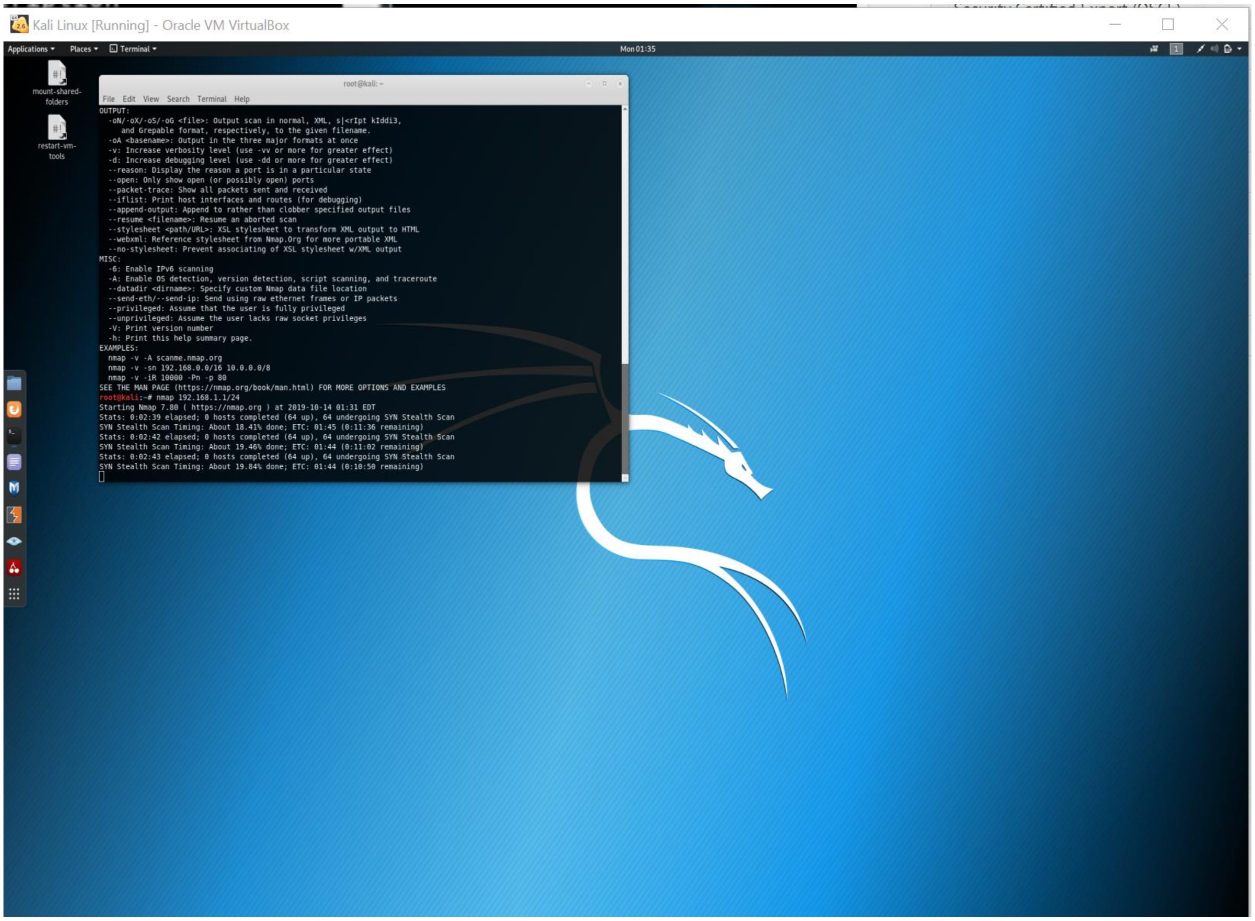
The entire method consists of this



Method

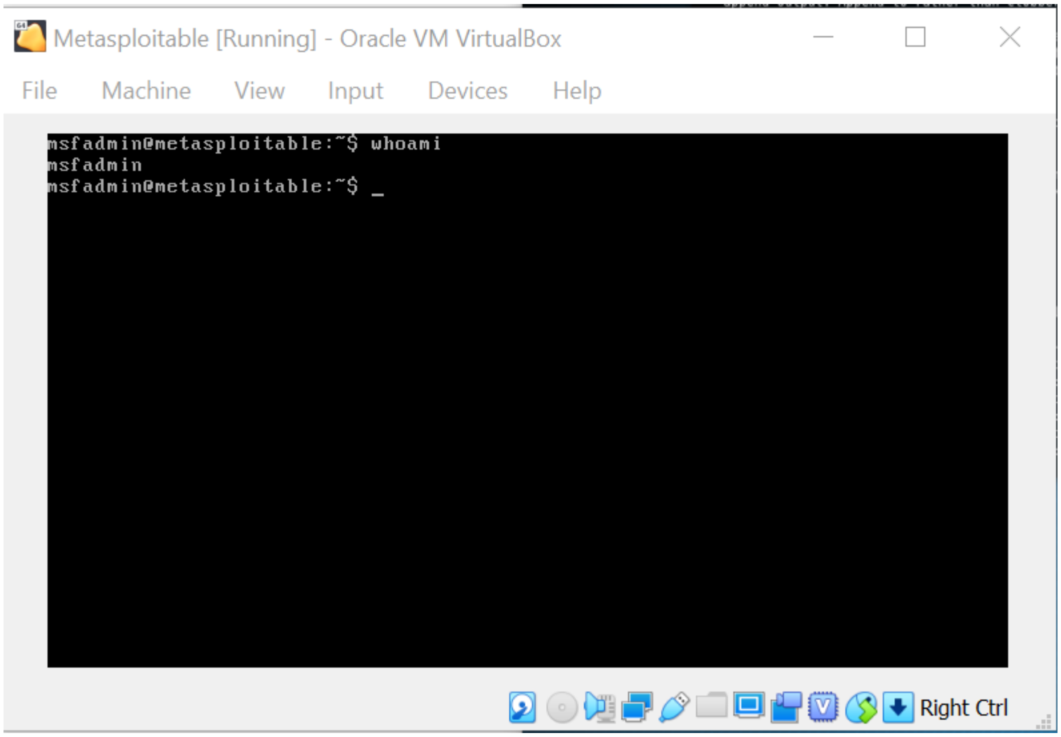
- Use **Nmap** to **scan** the network *(gathering information)*
- Use **Nmap** to do a more **detailed scan** of the target *(gathering information)*
- Use **Metasploit** to **discover** the database details *(gaining access)*
- [*] Can also use an exploit *(gaining access)*
- **Search** the **database** from the account information *(gathering information and gaining access)*
- [*] Use a web based **backdoor** to create **shell access** *(remote access)*
- **Automate shell access** via **Metasploit** *(remote access)*
- *I cheated a little bit here as I had used **nessus** in a previous scan to discover "Debian **OpenSSH**/OpenSSL Package Random Number Generator **Weakness**"*
- Via the **payload** it is possible to capture the SSH Key and compare it against the weak keys Just like **pWnOS** *(escalating privileges)*
- Connect via **SSH** as root *(complete access)*
- Prove complete access by cracking the **shadow file** with **John The Ripper** (then prove it by connecting via SSH using one of the newly acquired accounts)

1. First step is correctly setting up Kali Backtrack Linux on system



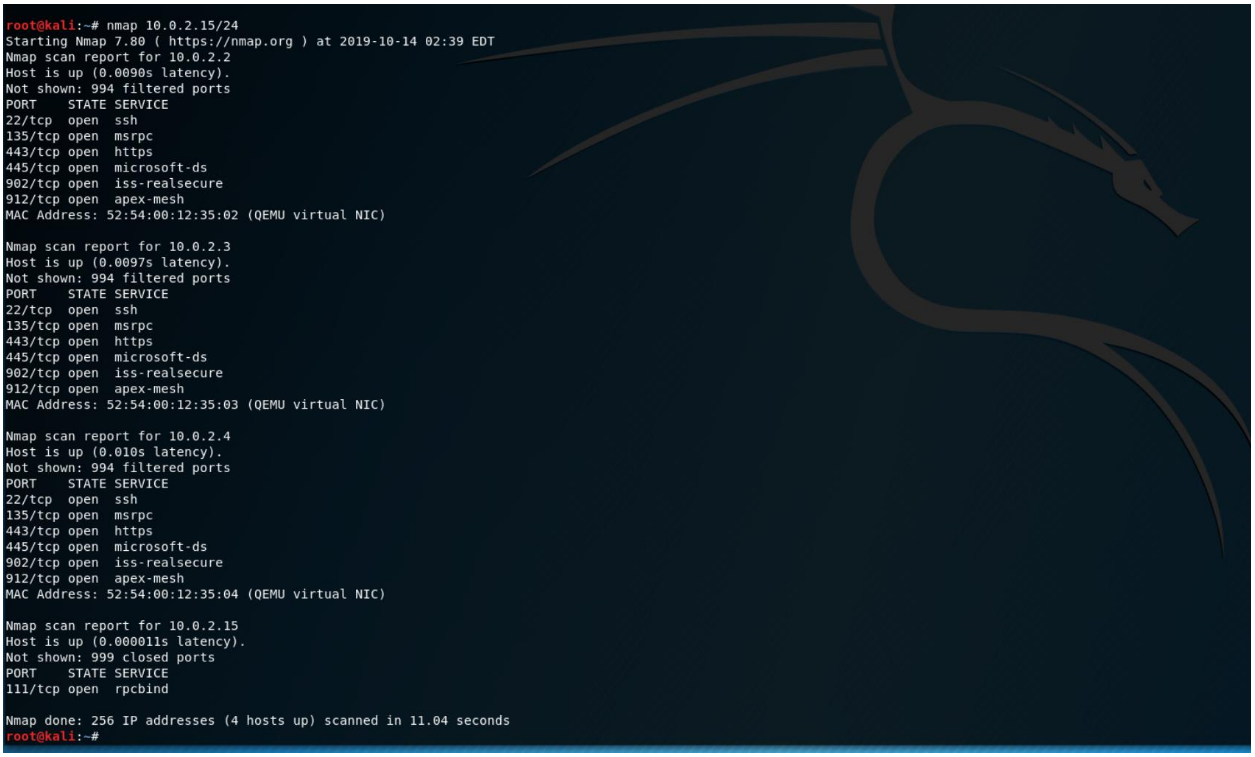
```
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
root@kali:~# nmap 192.168.1.1/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-14 01:31 EDT
Stats: 0:02:39 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.41% done; ETC: 01:45 (0:11:36 remaining)
Stats: 0:02:42 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.46% done; ETC: 01:44 (0:11:02 remaining)
Stats: 0:02:43 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 19.84% done; ETC: 01:44 (0:10:50 remaining)
```

2. Second step is to correctly set up Metasploit on Virtualbox



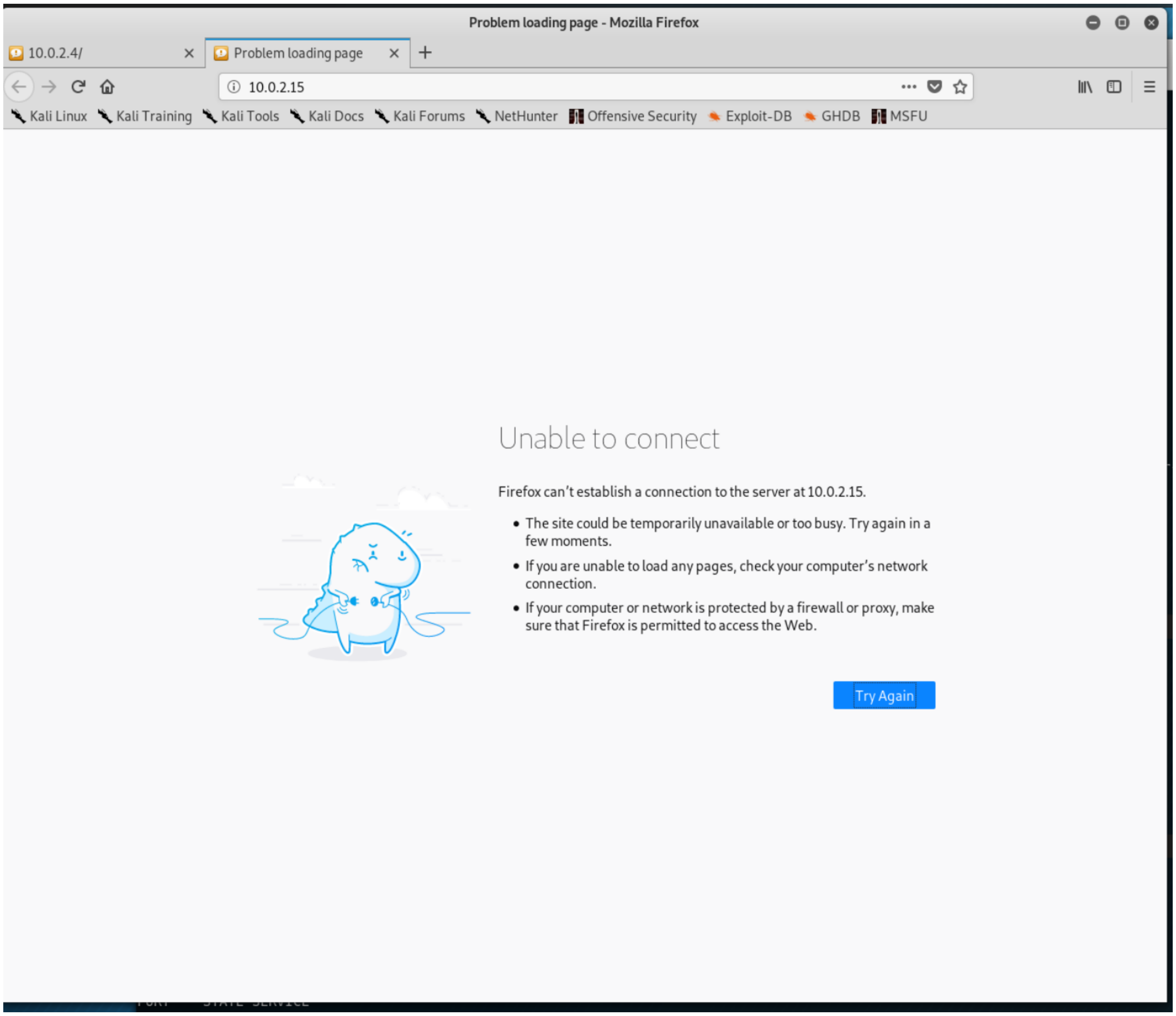
```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ _
```

3. Third step is to use Nmap to scan network through terminal on Kali



```
root@kali:~# nmap 10.0.2.15/24
Starting Nmap 7.80 ( https://nmap.org ) at 2019-10-14 02:39 EDT
Nmap scan report for 10.0.2.2
Host is up (0.0090s latency).
Not shown: 994 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
135/tcp open  msrpc
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 52:54:00:12:35:02 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.0097s latency).
Not shown: 994 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
135/tcp open  msrpc
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 52:54:00:12:35:03 (QEMU virtual NIC)

Nmap scan report for 10.0.2.4
Host is up (0.010s latency).
Not shown: 994 filtered ports
PORT    STATE SERVICE
22/tcp  open  ssh
135/tcp open  msrpc
443/tcp open  https
445/tcp open  microsoft-ds
902/tcp open  iss-realsecure
912/tcp open  apex-mesh
MAC Address: 52:54:00:12:35:04 (QEMU virtual NIC)

Nmap scan report for 10.0.2.15
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
111/tcp open  rpcbind

Nmap done: 256 IP addresses (4 hosts up) scanned in 11.04 seconds
root@kali:~#
```

4. Fourth step is to use firefox to confirm existence of the Metasploit server.

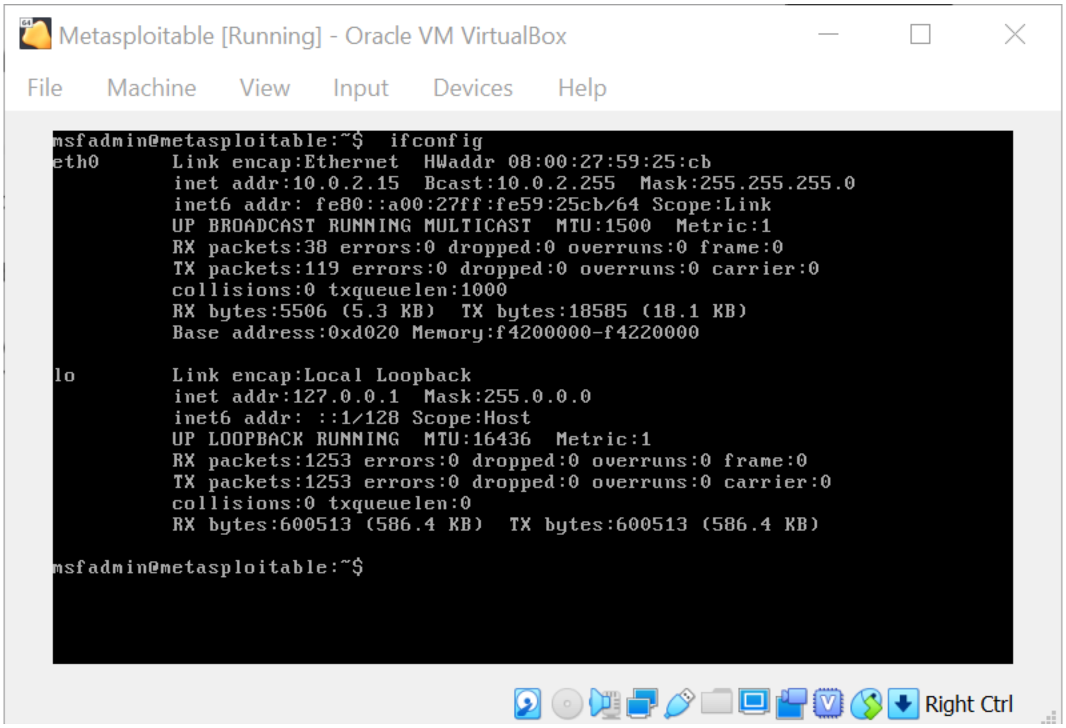


Unable to connect

Firefox can't establish a connection to the server at 10.0.2.15.

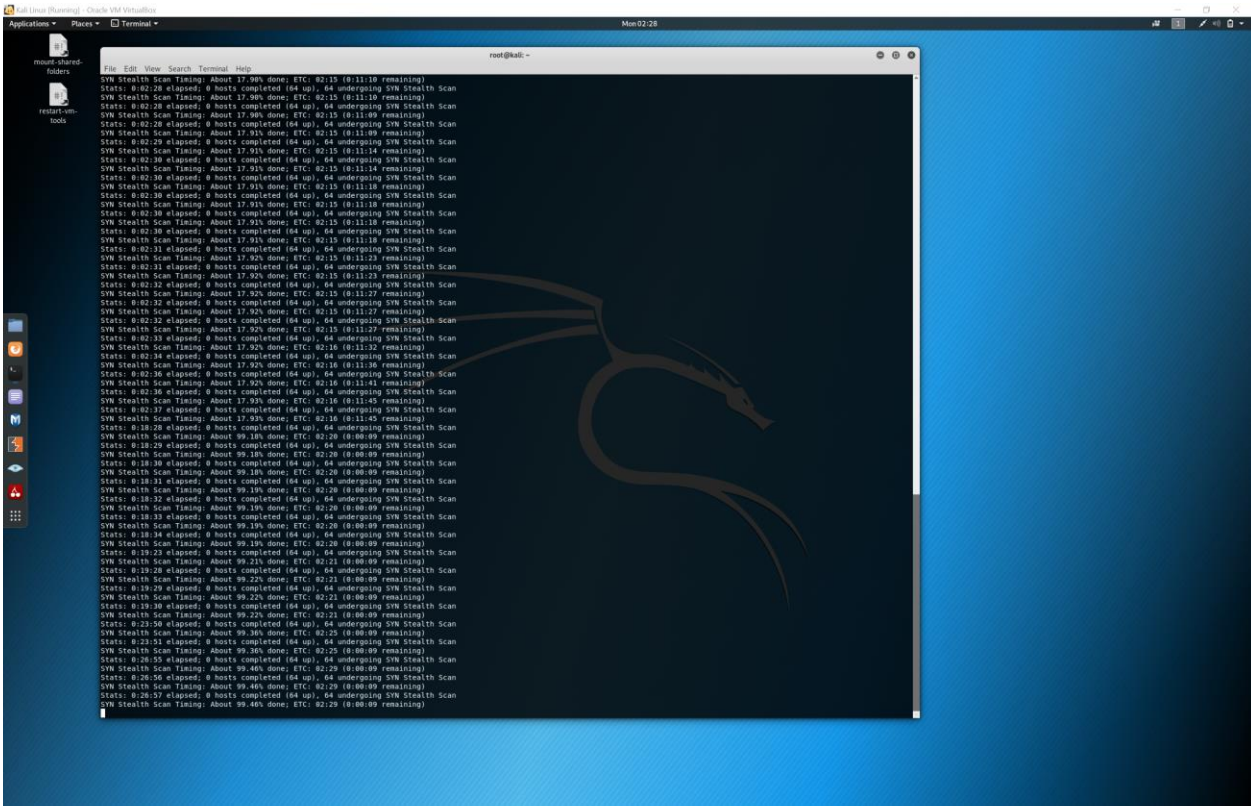
- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Weirdly, firefox was unable to connect to my Metasploit server, even though I had properly set it up through virtualbox network connections. I have attached screenshot of Metasploit server showing same ip address.



```
msfadmin@metasploitable:~$  ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:59:25:cb
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe59:25cb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:119 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5506 (5.3 KB)  TX bytes:18585 (18.1 KB)
          Base address:0xd020 Memory:f4200000-f4220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:1253 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1253 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:600513 (586.4 KB)  TX bytes:600513 (586.4 KB)

msfadmin@metasploitable:~$
```

5. Fifth step is to then compile and run the DirBuster file against the server.
6. You then use firefox to access the tikiwiki director
7. You then open up the Metasploit console and search for tikiwiki
8. You set the admin permissions for the tikiwiki file
9. You have to then go through and change the default SQL admin password.
10. After that, we use the web based backdoor to gain shell remote access.
11. We automate that shell access through use of our remote Metasploit access.
12. We then capture that SSH key being used to connect and compare it to known weak keys. Once we have the SSH key, we can connect as root and have full access to the system.



```
SYN Stealth Scan Timing: About 17.90% done; ETC: 02:15 (0:11:10 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.90% done; ETC: 02:15 (0:11:10 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.90% done; ETC: 02:15 (0:11:09 remaining)
Stats: 0:02:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.91% done; ETC: 02:15 (0:11:09 remaining)
Stats: 0:02:29 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.91% done; ETC: 02:15 (0:11:14 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.91% done; ETC: 02:15 (0:11:14 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.91% done; ETC: 02:15 (0:11:18 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.91% done; ETC: 02:15 (0:11:18 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.91% done; ETC: 02:15 (0:11:18 remaining)
Stats: 0:02:30 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.91% done; ETC: 02:15 (0:11:18 remaining)
Stats: 0:02:31 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.92% done; ETC: 02:15 (0:11:23 remaining)
Stats: 0:02:31 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.92% done; ETC: 02:15 (0:11:23 remaining)
Stats: 0:02:32 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.92% done; ETC: 02:15 (0:11:27 remaining)
Stats: 0:02:32 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.92% done; ETC: 02:15 (0:11:27 remaining)
Stats: 0:02:32 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.92% done; ETC: 02:15 (0:11:27 remaining)
Stats: 0:02:33 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.92% done; ETC: 02:16 (0:11:32 remaining)
Stats: 0:02:34 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.92% done; ETC: 02:16 (0:11:36 remaining)
Stats: 0:02:36 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.92% done; ETC: 02:16 (0:11:41 remaining)
Stats: 0:02:36 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.93% done; ETC: 02:16 (0:11:45 remaining)
Stats: 0:02:37 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 17.93% done; ETC: 02:16 (0:11:45 remaining)
Stats: 0:18:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.18% done; ETC: 02:20 (0:00:09 remaining)
Stats: 0:18:29 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.18% done; ETC: 02:20 (0:00:09 remaining)
Stats: 0:18:30 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.18% done; ETC: 02:20 (0:00:09 remaining)
Stats: 0:18:31 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.19% done; ETC: 02:20 (0:00:09 remaining)
Stats: 0:18:32 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.19% done; ETC: 02:20 (0:00:09 remaining)
Stats: 0:18:33 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.19% done; ETC: 02:20 (0:00:09 remaining)
Stats: 0:18:34 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.19% done; ETC: 02:20 (0:00:09 remaining)
Stats: 0:19:23 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.21% done; ETC: 02:21 (0:00:09 remaining)
Stats: 0:19:28 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.22% done; ETC: 02:21 (0:00:09 remaining)
Stats: 0:19:29 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.22% done; ETC: 02:21 (0:00:09 remaining)
Stats: 0:19:30 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.22% done; ETC: 02:21 (0:00:09 remaining)
Stats: 0:23:50 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.36% done; ETC: 02:25 (0:00:09 remaining)
Stats: 0:23:51 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.36% done; ETC: 02:25 (0:00:09 remaining)
Stats: 0:26:55 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.46% done; ETC: 02:29 (0:00:09 remaining)
Stats: 0:26:56 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.46% done; ETC: 02:29 (0:00:09 remaining)
Stats: 0:26:57 elapsed; 0 hosts completed (64 up), 64 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.46% done; ETC: 02:29 (0:00:09 remaining)
```

13.