

Prerequisites: Installed VirtualBox & Extension Pack .

1. Downloading Kali/Metasploitable2/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>

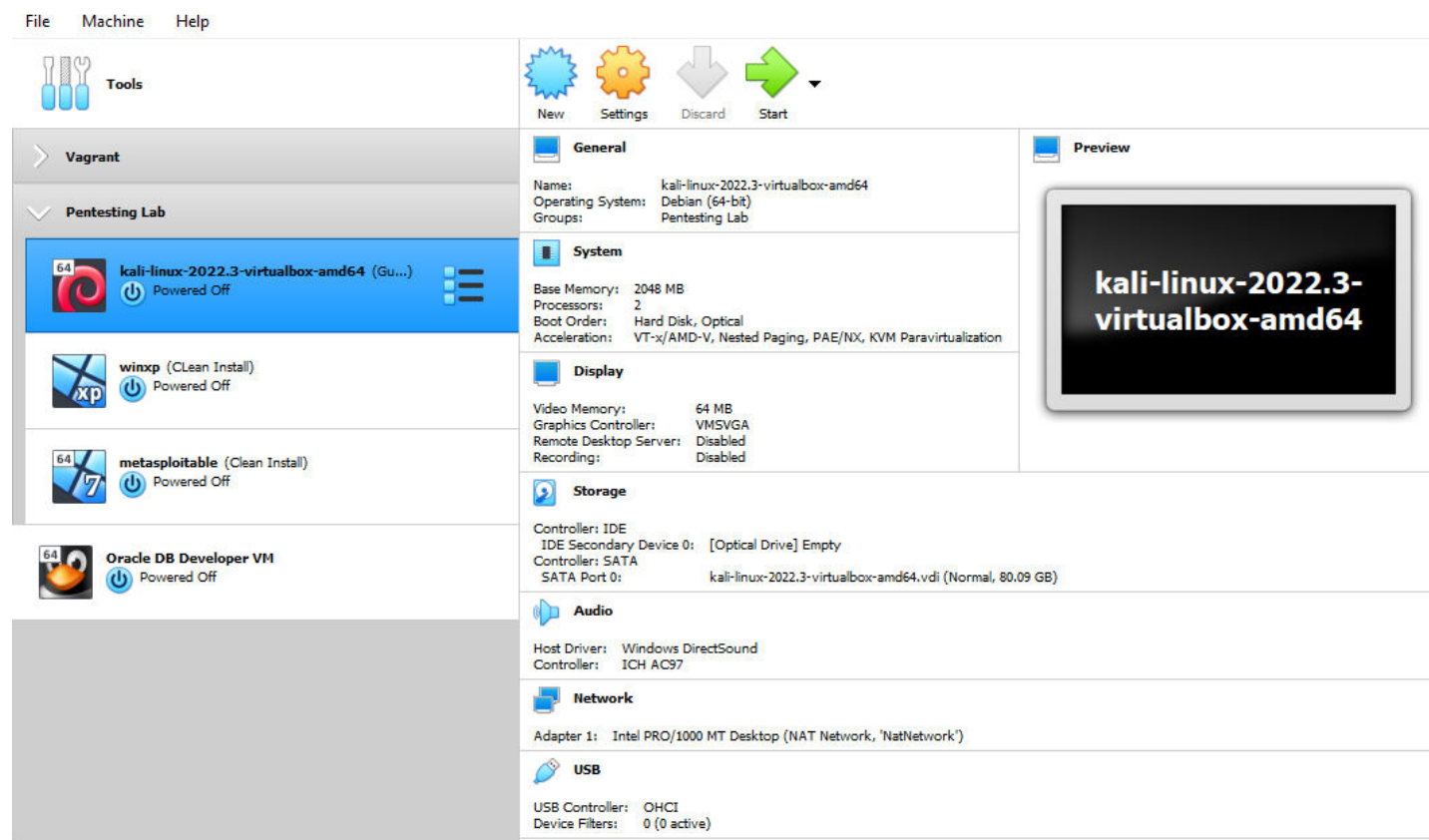
WindowsXP:

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 :

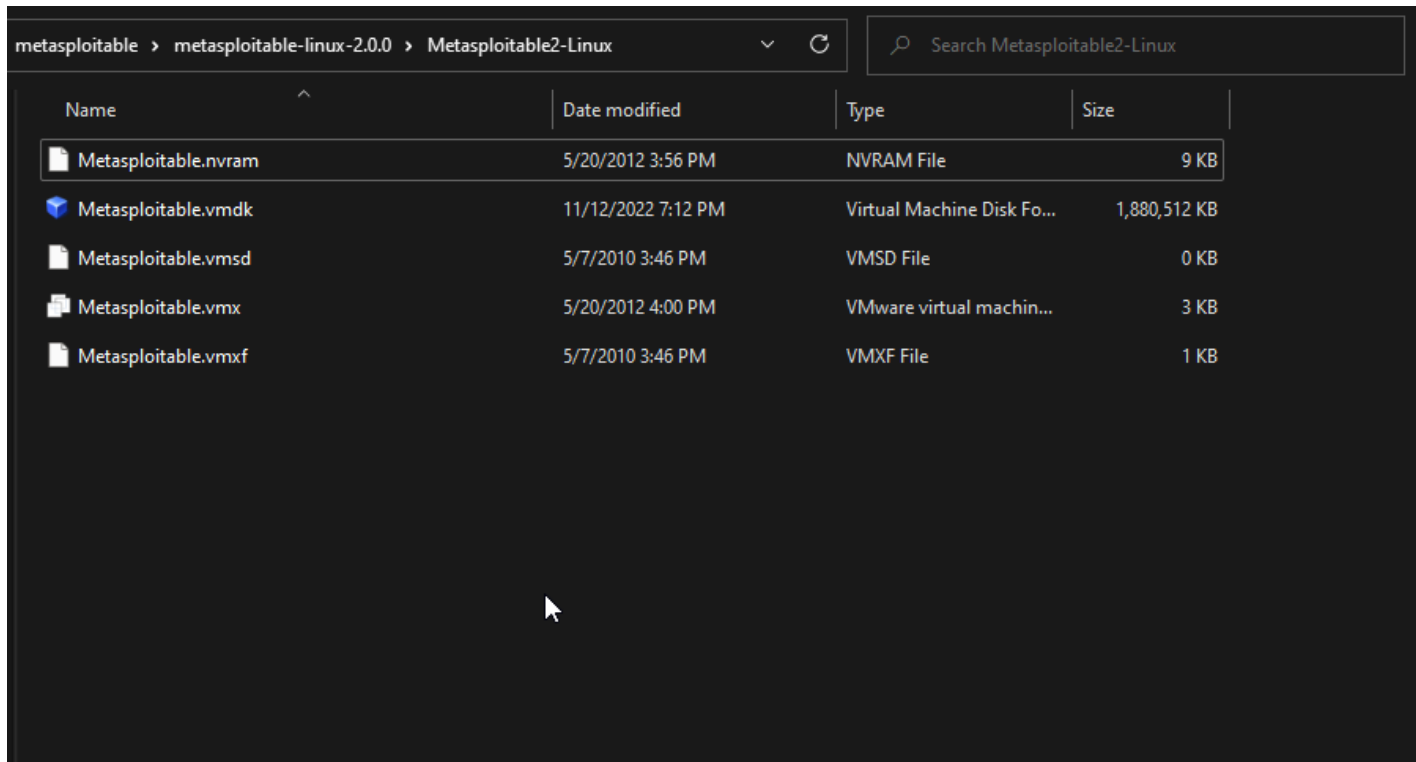
- Default Installation








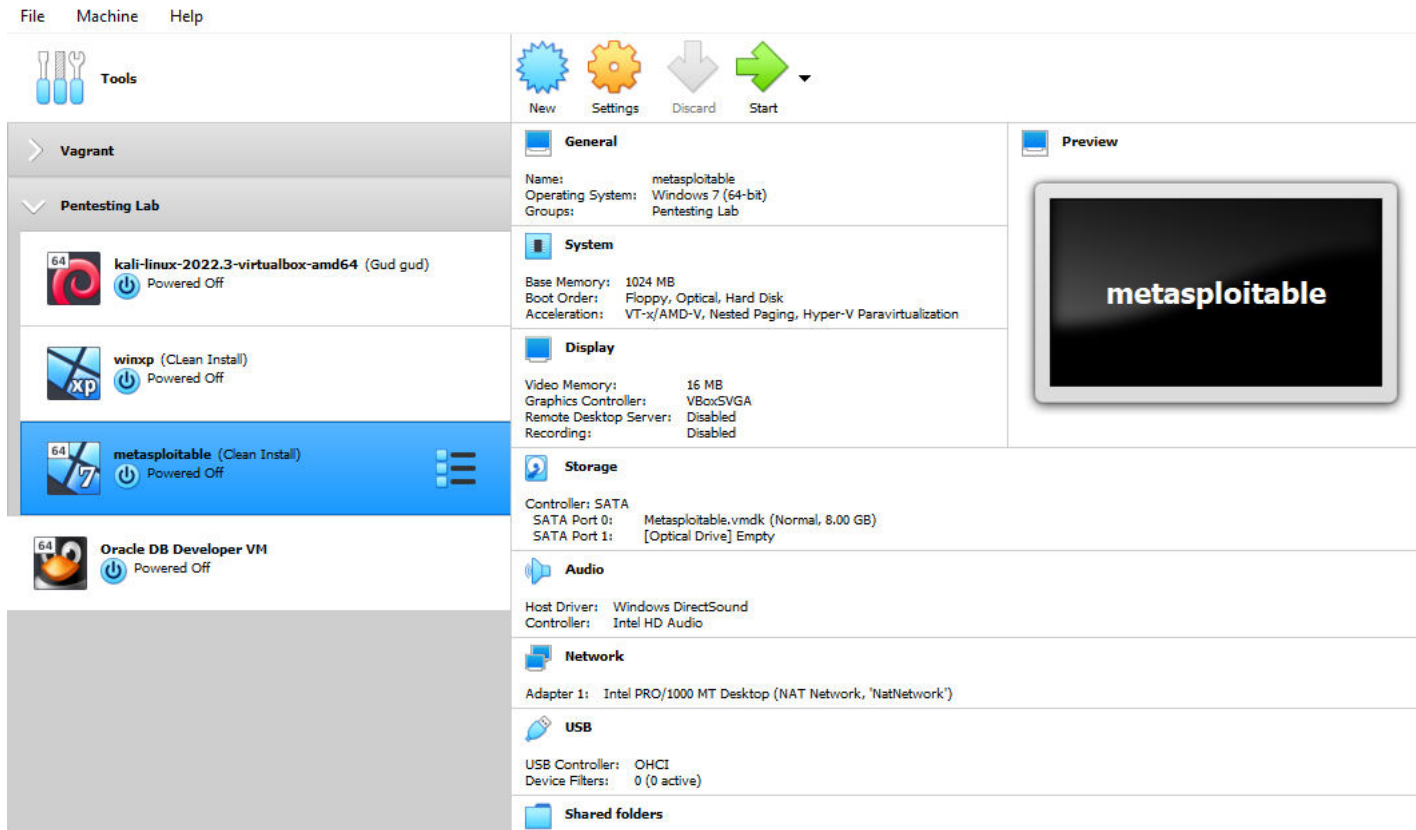
IMPORTANT!!

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 :



metasploitable > metasploitable-linux-2.0.0 > Metasploitable2-Linux				
Search Metasploitable2-Linux				
Name	Date modified	Type	Size	
 Metasploitable.nvram	5/20/2012 3:56 PM	NVRAM File	9 KB	
 Metasploitable.vmdk	11/12/2022 7:12 PM	Virtual Machine Disk Fo...	1,880,512 KB	
 Metasploitable.vmsd	5/7/2010 3:46 PM	VMSD File	0 KB	
 Metasploitable.vmx	5/20/2012 4:00 PM	VMware virtual machin...	3 KB	
 Metasploitable.vmx	5/7/2010 3:46 PM	VMXF File	1 KB	



IMPORTANT!!

For Windows XP :

- Same hardware specifications as below :



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



System



Display



Storage



Audio



Network



USB



Shared folders

Name: winxp
Operating System: Windows XP (32-bit)
Groups: Pentesting Lab

Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

Video Memory: 18 MB
Graphics Controller: VBoxVGA
Remote Desktop Server: Disabled
Recording: Disabled

Controller: IDE
IDE Primary Device 0: winxp.vdi (Normal, 10.00 GB)
IDE Secondary Device 0: [Optical Drive] VBoxGuestAdditions.iso (60.92 MB)

Host Driver: Windows DirectSound
Controller: ICH AC97

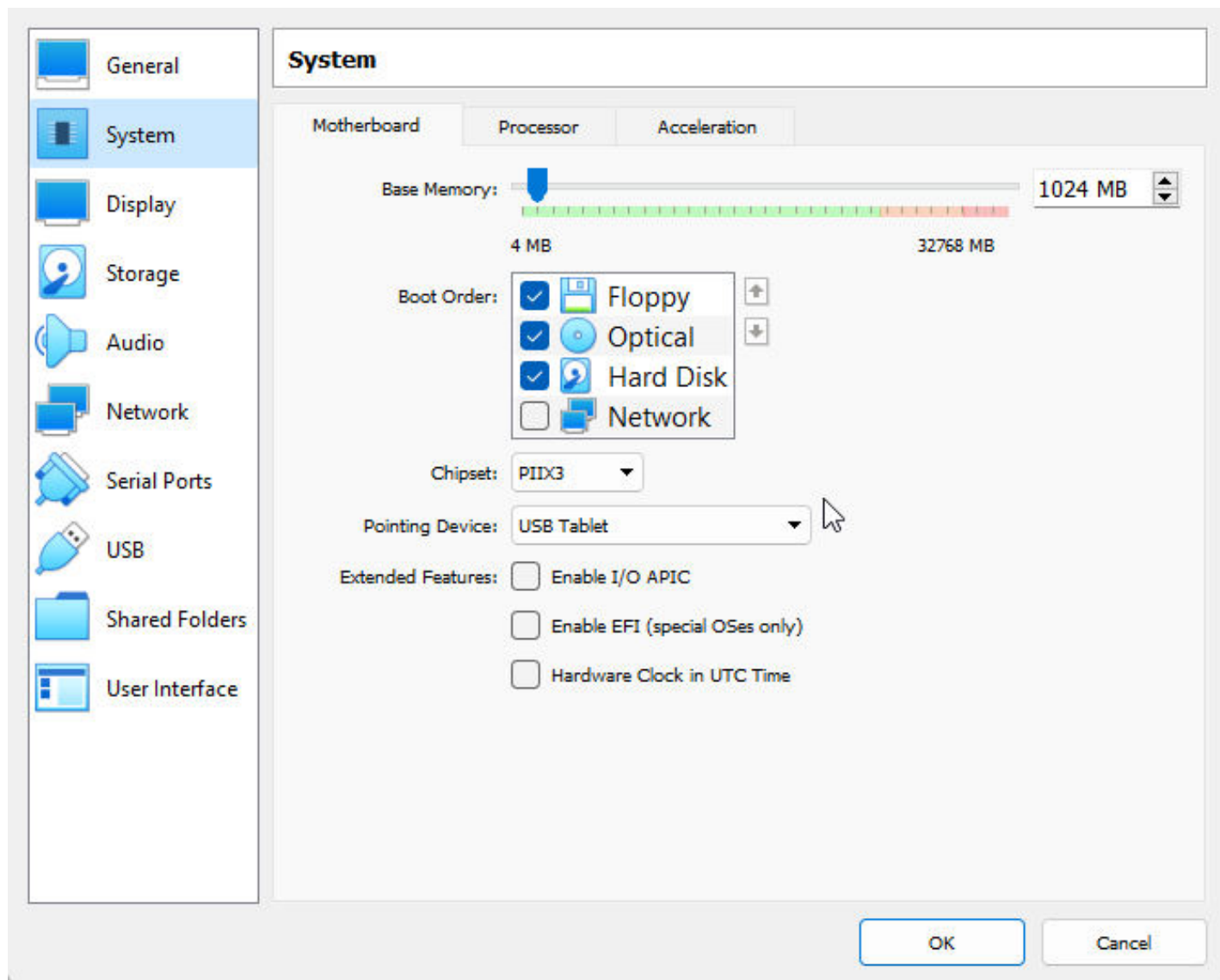
Adapter 1: Intel PRO/1000 T Server (NAT Network, 'NatNetwork')

USB Controller: OHCI
Device Filters: 0 (0 active)

Shared folders

Preview





- General
- System**
- Display
- Storage
- Audio
- Network
- Serial Ports
- USB
- Shared Folders
- User Interface

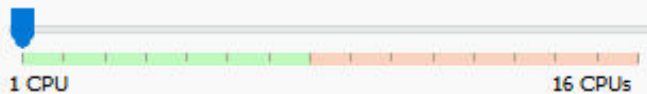
System

Motherboard

Processor

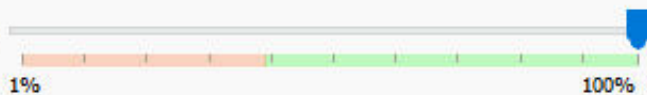
Acceleration

Processor(s):



1

Execution Cap:



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: 0 MB 128 MB 18 MB

Monitor Count: 1 8

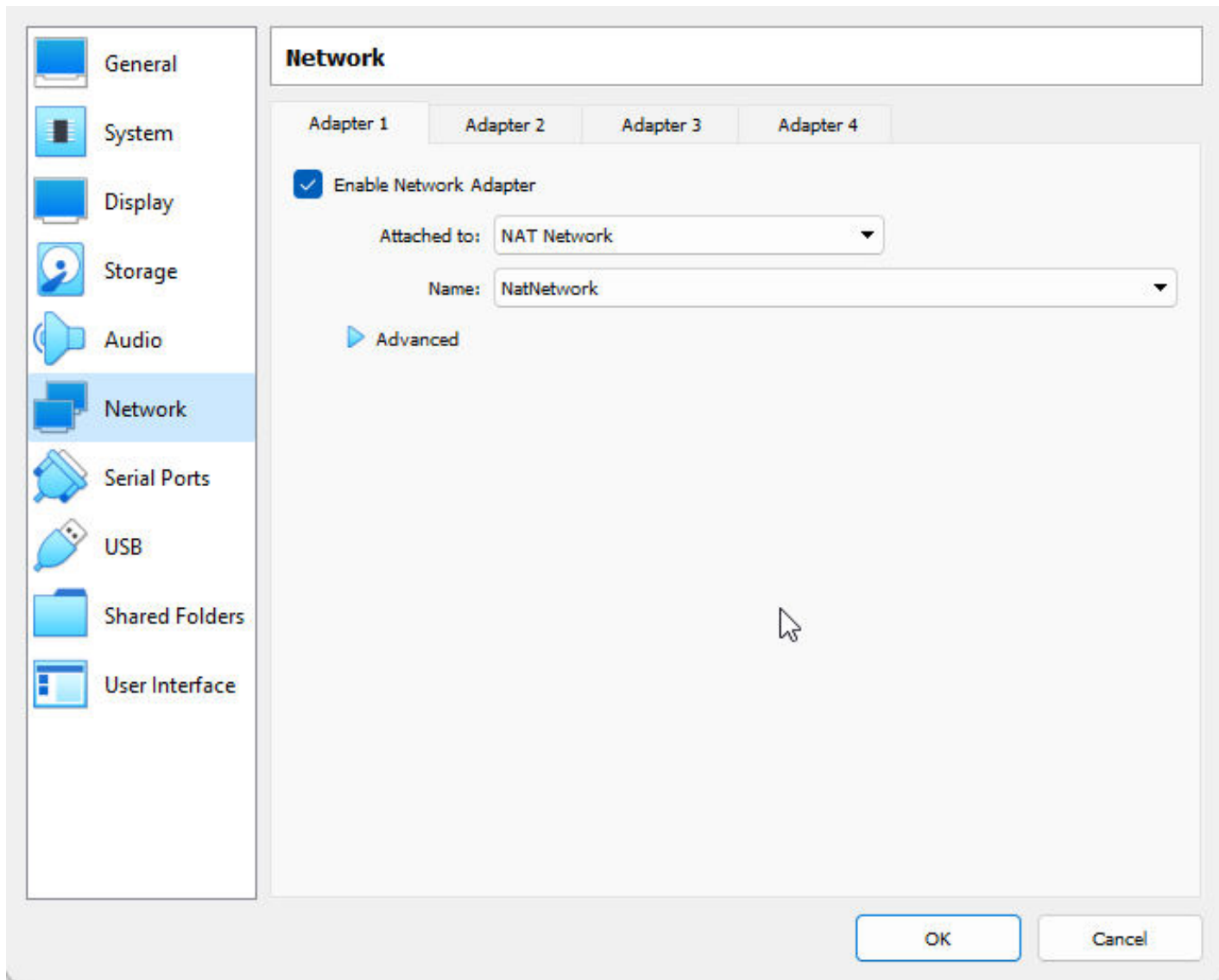
Scale Factor: All Monitors Min Max 100%

Graphics Controller: VBoxVGA

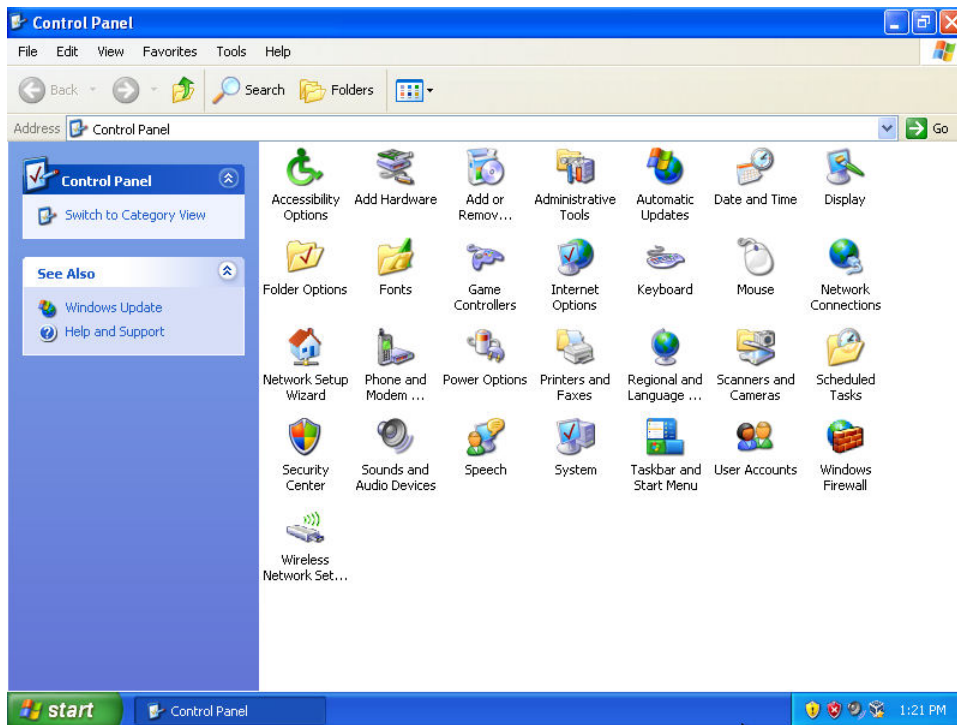
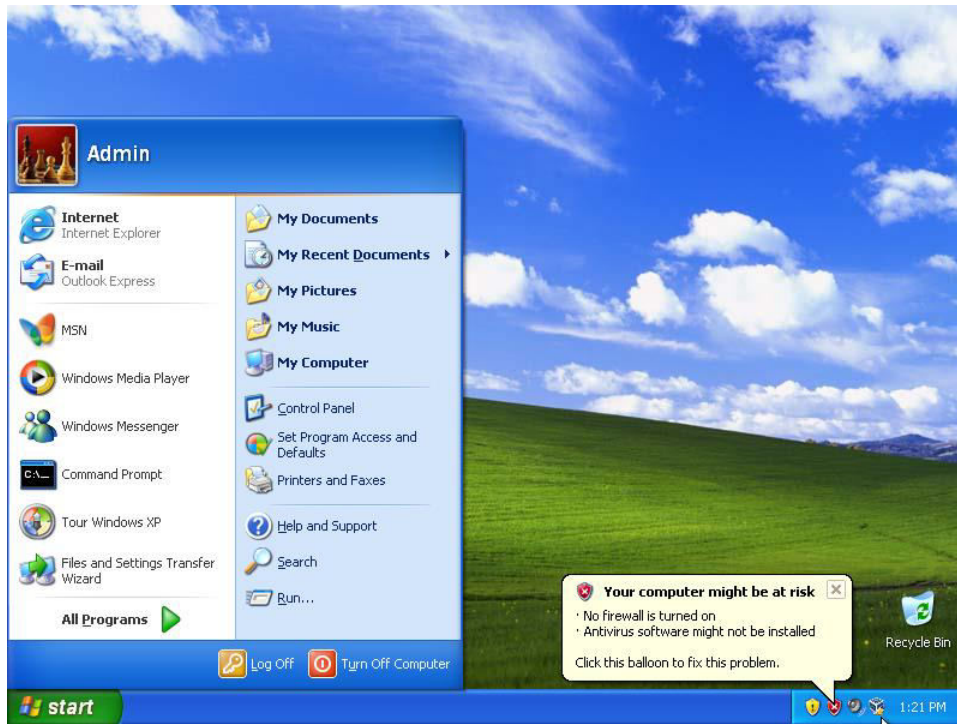
Acceleration: ☐ Enable 3D Acceleration

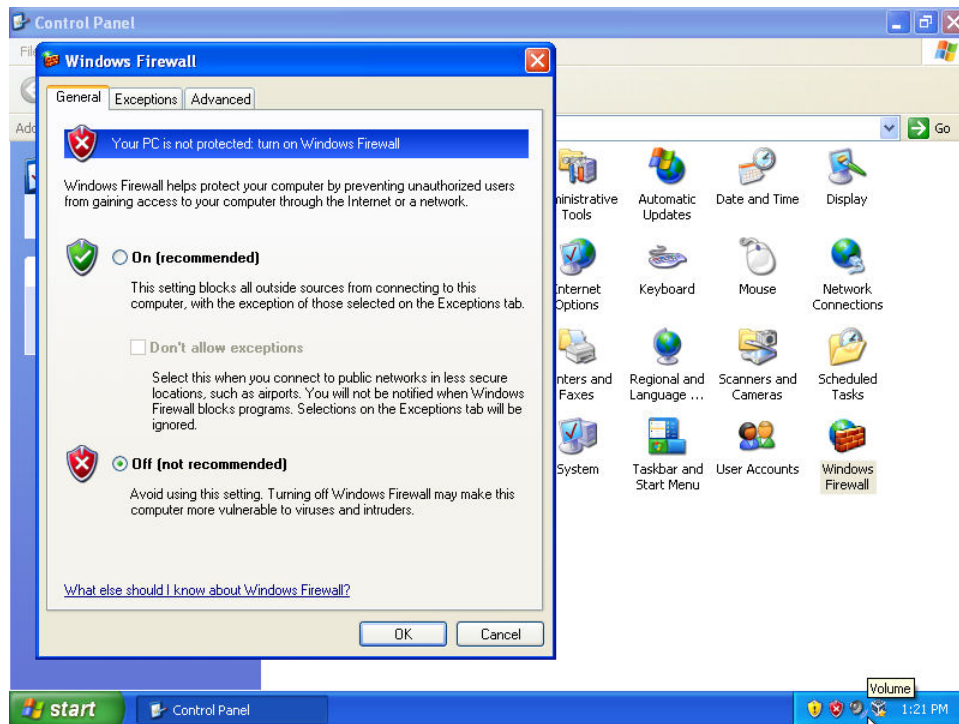
OK

Cancel



- Disabling Windows firewall .



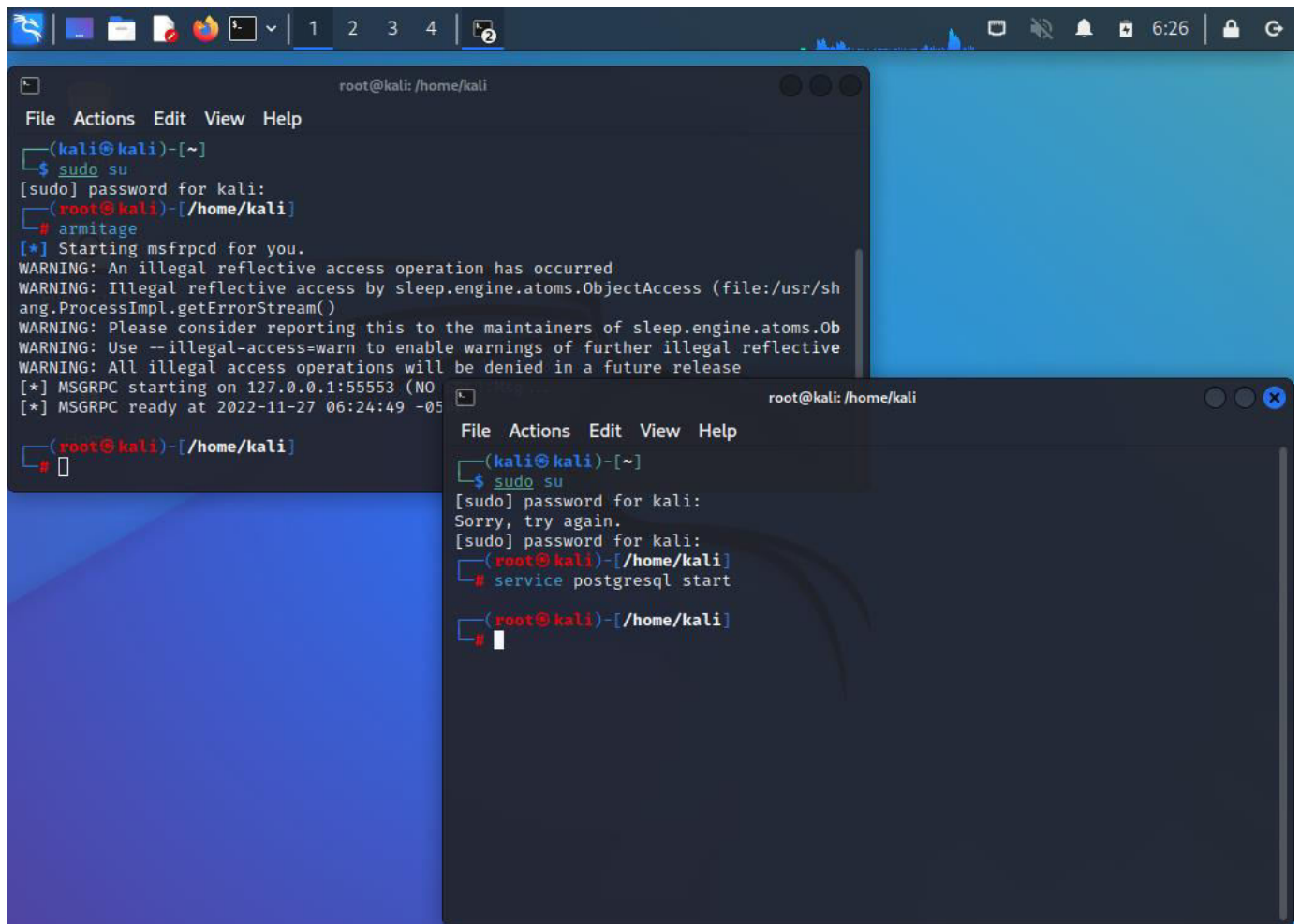


3. Updating and installing

On Kali VM :

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

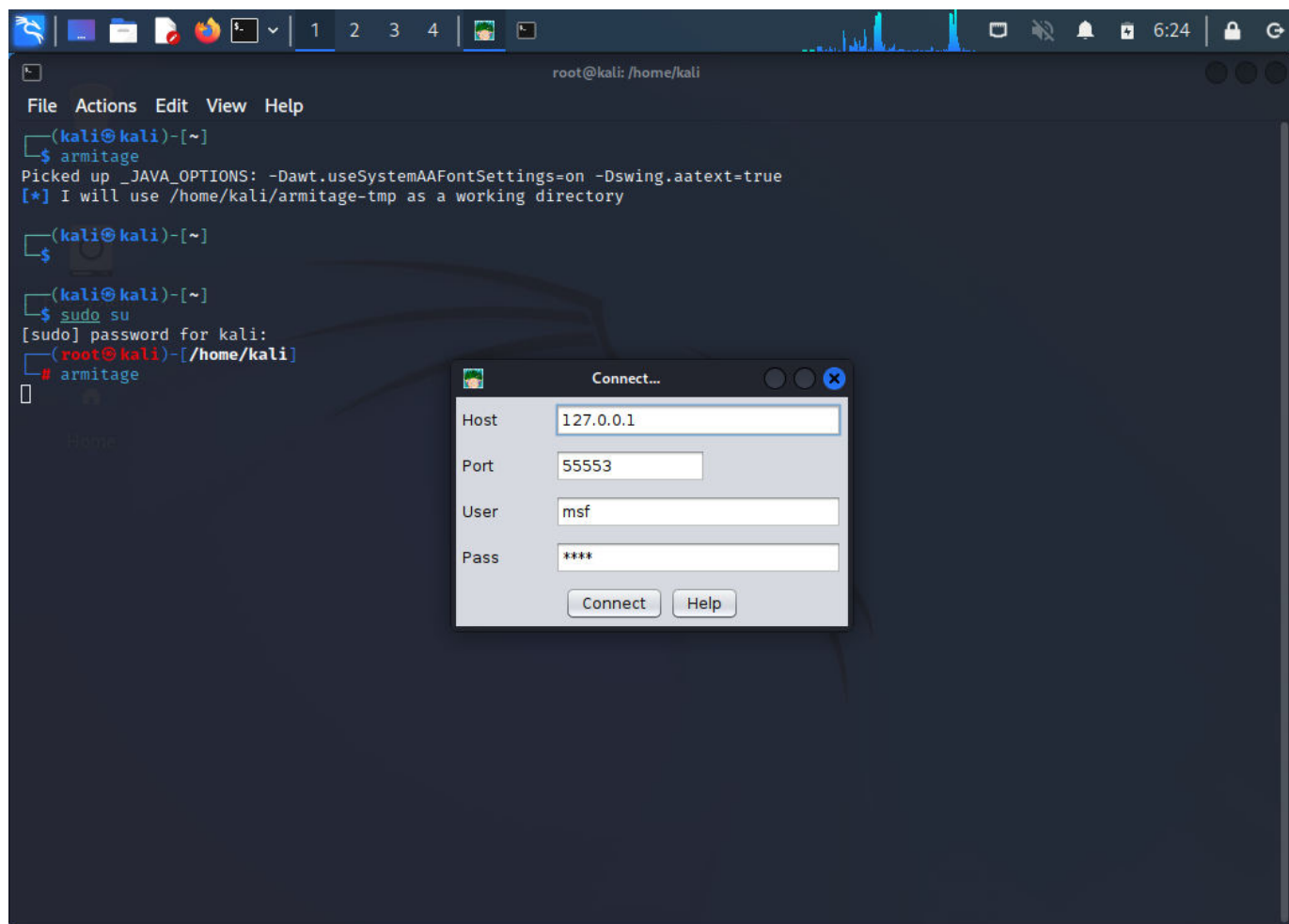
Start Postgres service.



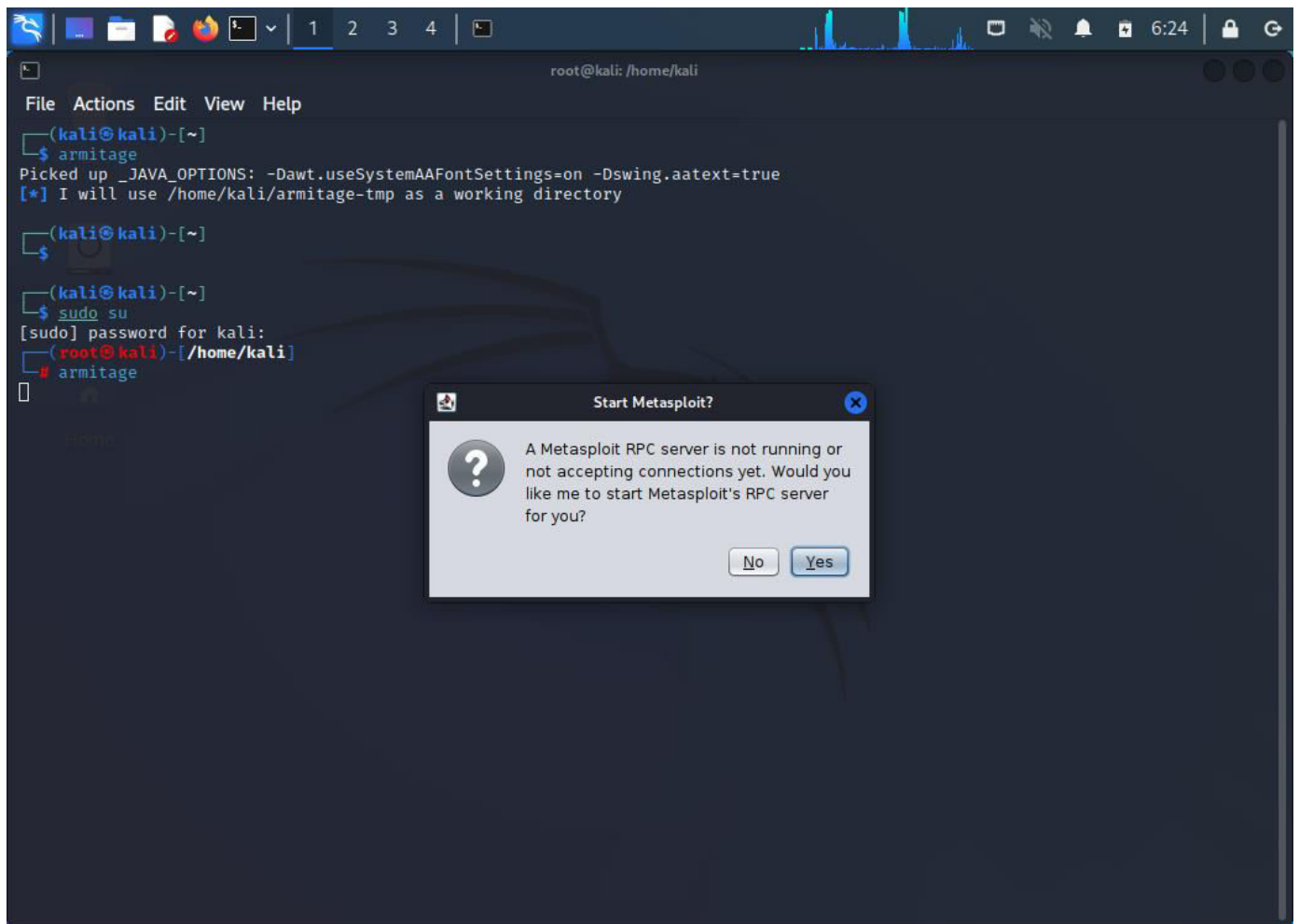
```
root@kali: /home/kali
File Actions Edit View Help
(kali@kali)-[~]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali]
# armitage
[*] Starting msfrpcd for you.
WARNING: An illegal reflective access operation has occurred
WARNING: Illegal reflective access by sleep.engine.atoms.ObjectAccess (file:/usr/share/ang.ProcessImpl.getErrorStream())
WARNING: Please consider reporting this to the maintainers of sleep.engine.atoms.ObjectAccess
WARNING: Use --illegal-access=warn to enable warnings of further illegal reflective access operations
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]
#
```

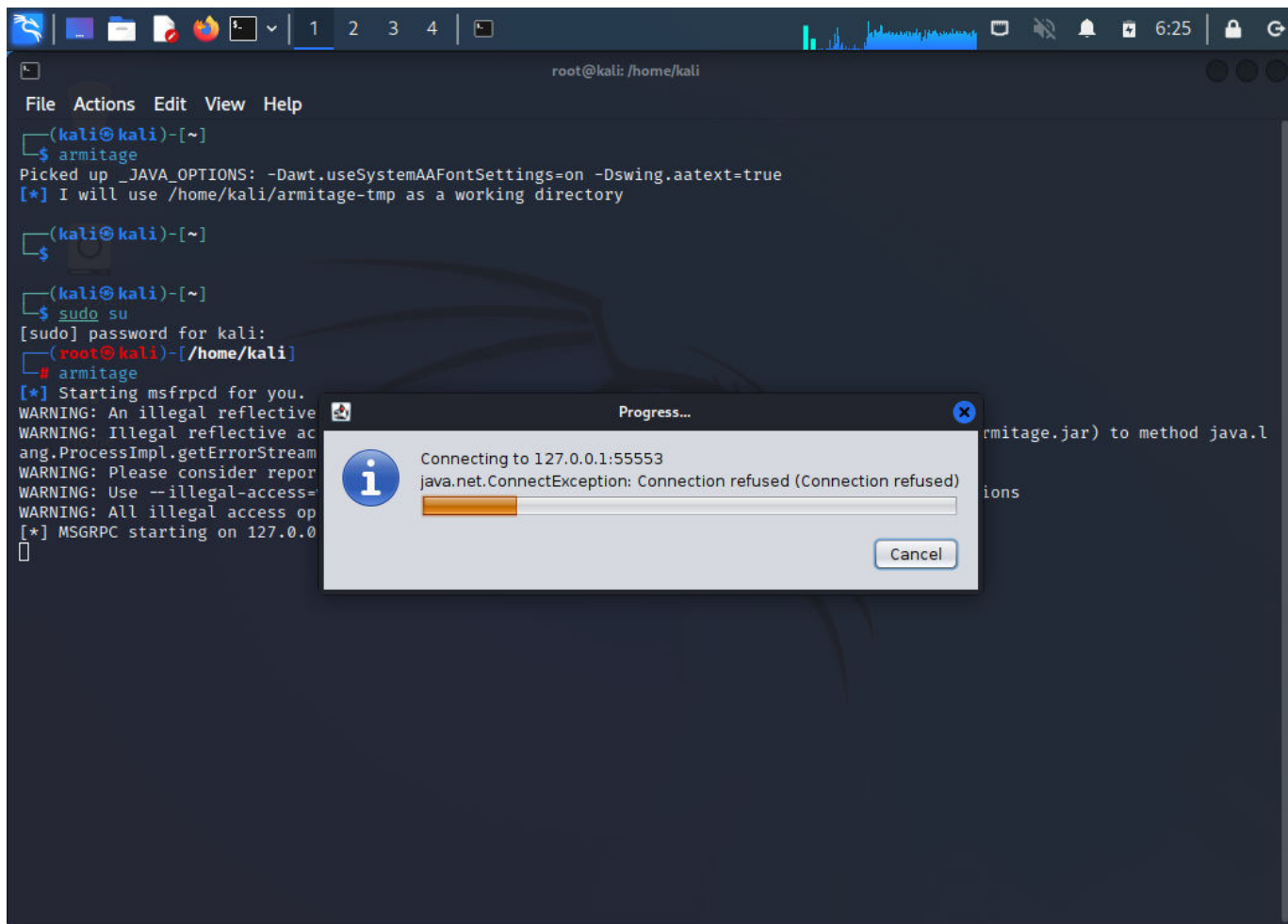
Connect.

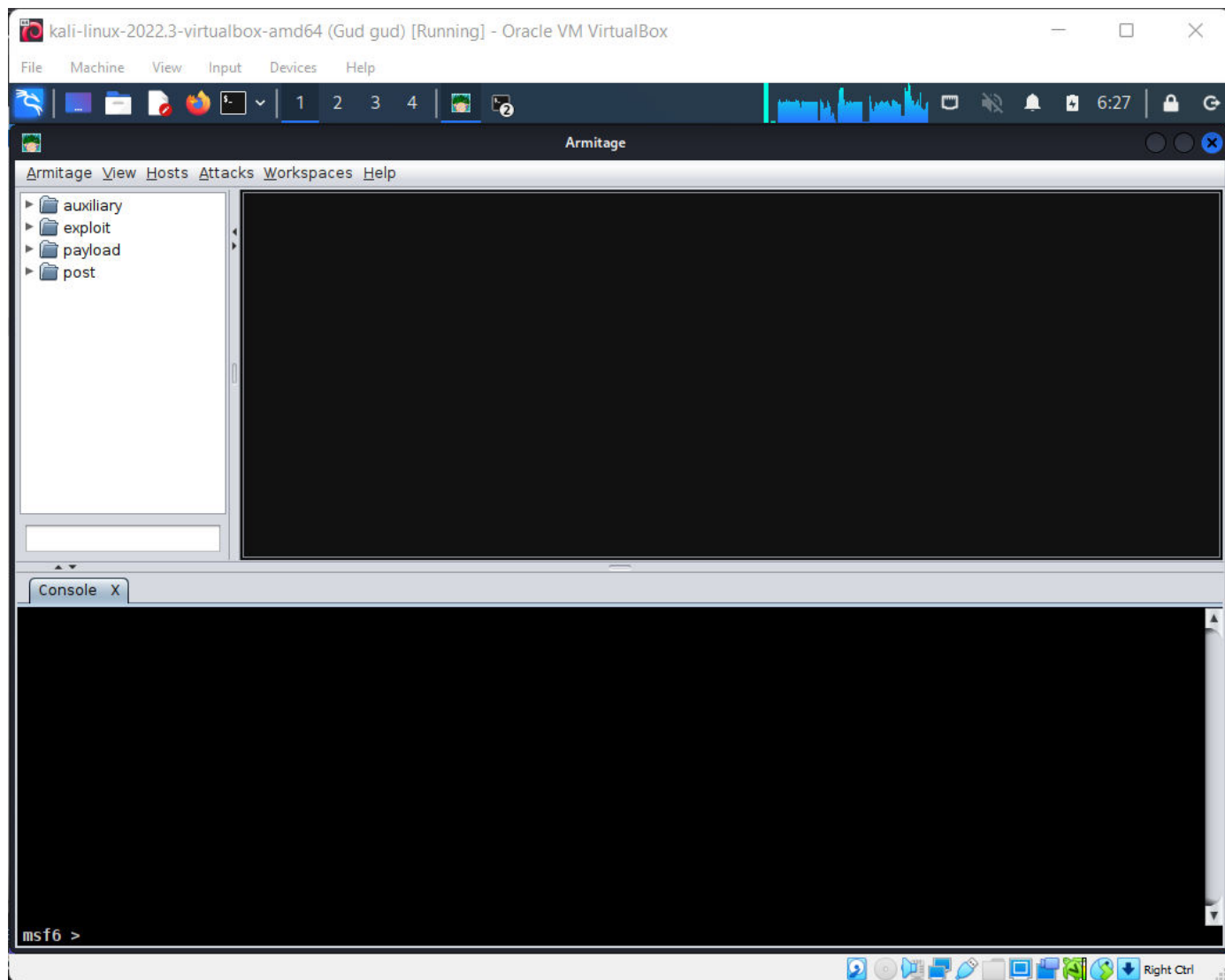


Yes.

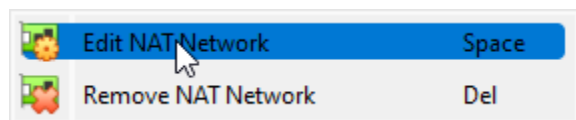
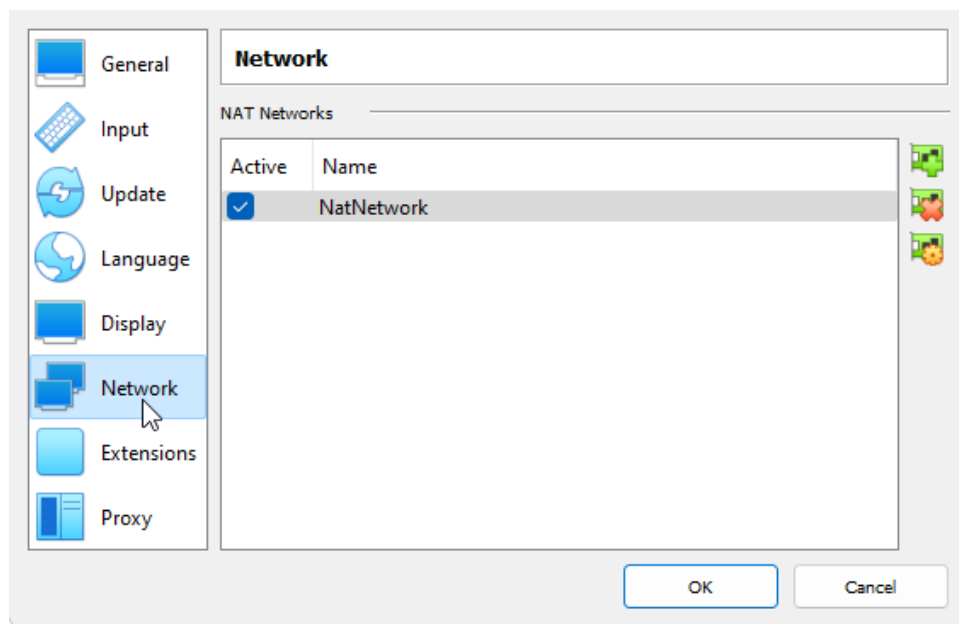
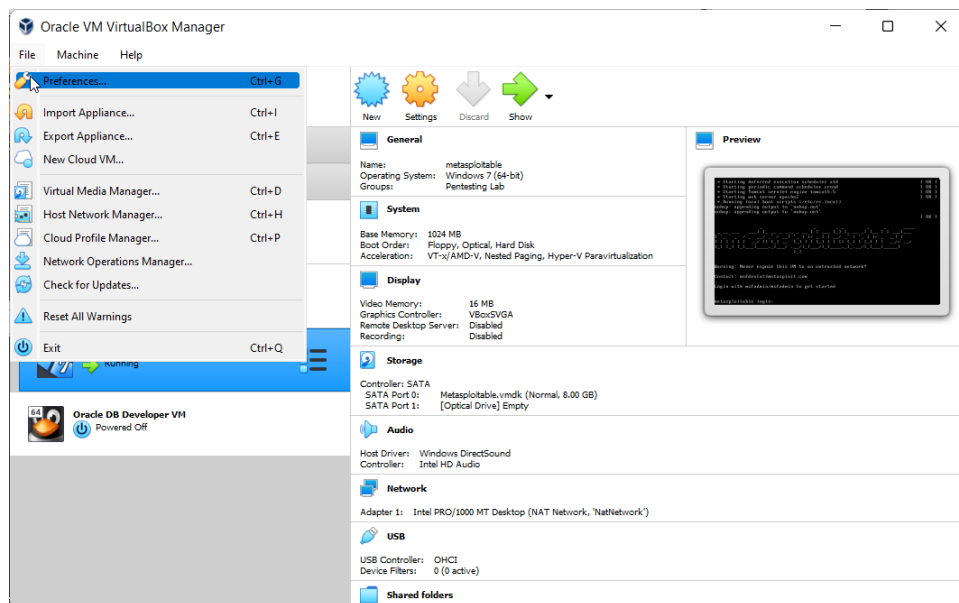


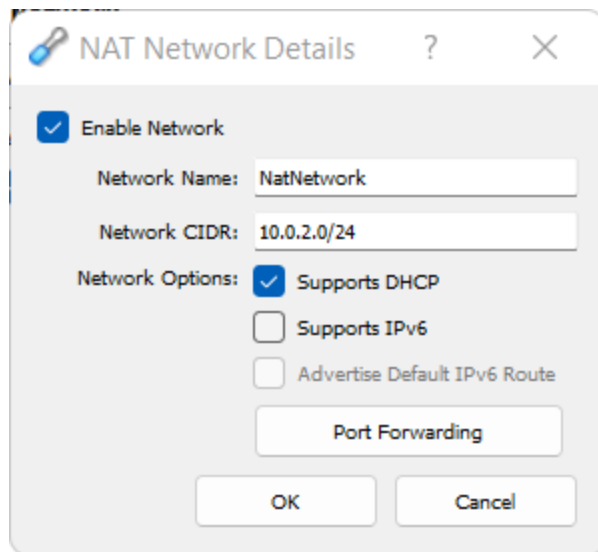
Wait





4. Network





The image shows a 'NAT Network Details' dialog box. It has a title bar with a lock icon, the text 'NAT Network Details', a question mark, and a close button. The main content area has a section 'Enable Network' with a checked checkbox. Below this are two text input fields: 'Network Name' with the value 'NatNetwork' and 'Network CIDR' with the value '10.0.2.0/24'. Under 'Network Options', there are three checkboxes: 'Supports DHCP' (checked), 'Supports IPv6' (unchecked), and 'Advertise Default IPv6 Route' (unchecked). A 'Port Forwarding' button is located below these options. At the bottom are 'OK' and 'Cancel' buttons.

NAT Network Details ? X

☒ Enable Network

Network Name: NatNetwork

Network CIDR: 10.0.2.0/24

Network Options: ☒ Supports DHCP

☐ Supports IPv6

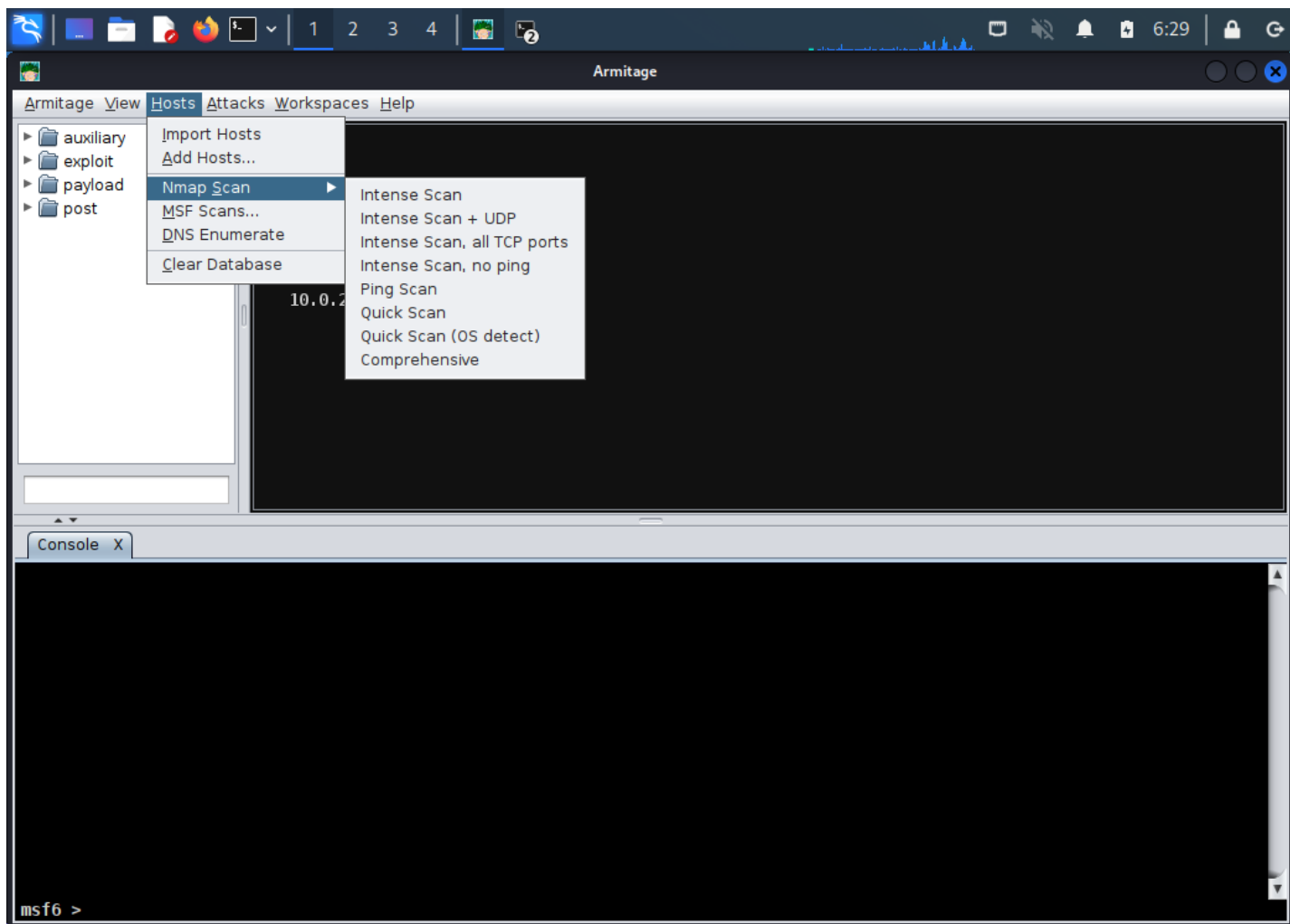
☐ Advertise Default IPv6 Route

Port Forwarding

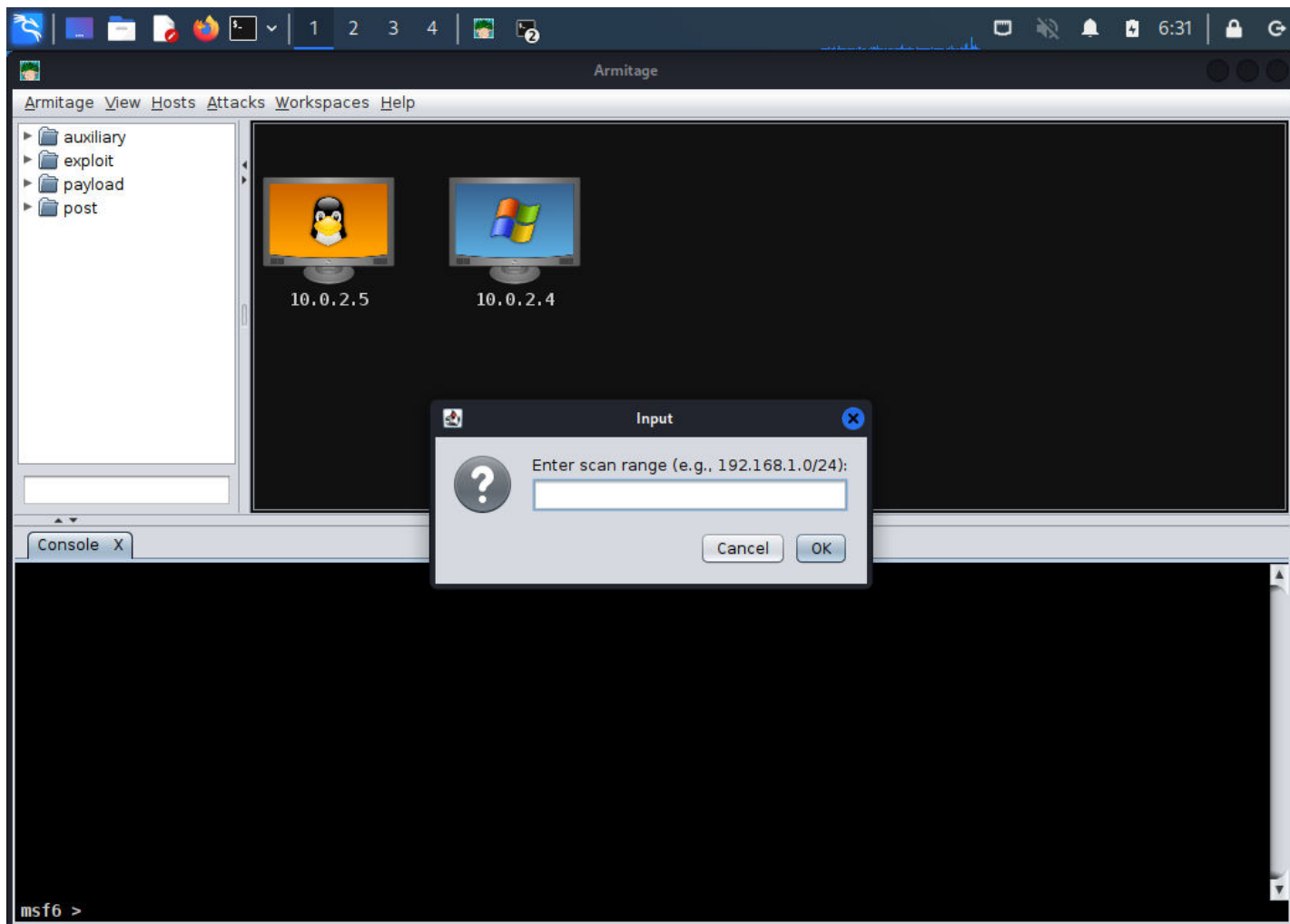
OK Cancel

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:

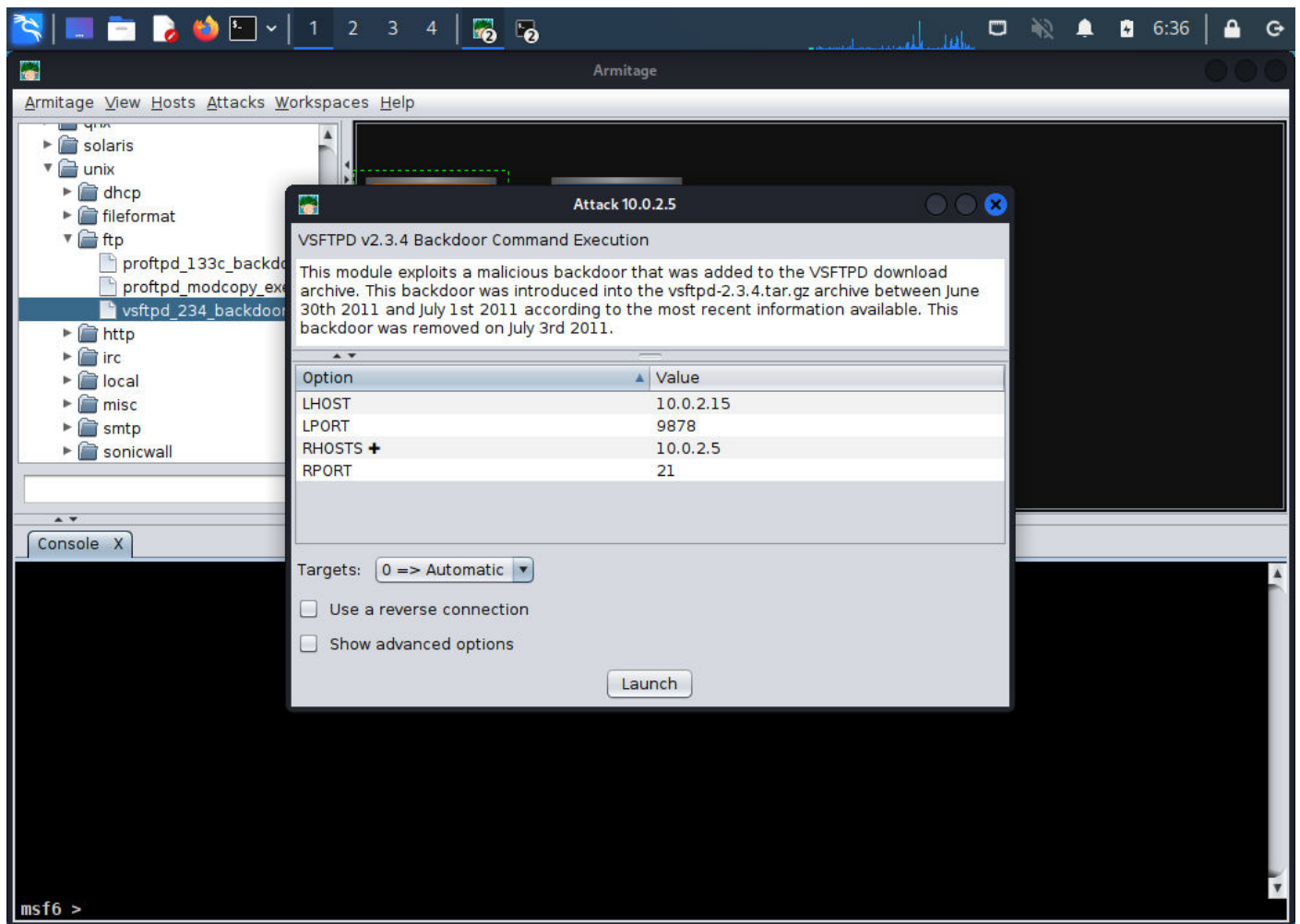
Exploit/windows/smb/ms08_067_netapi

For Linux :

Exploit/unix/ftp/vsftpd_234_backdoor

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

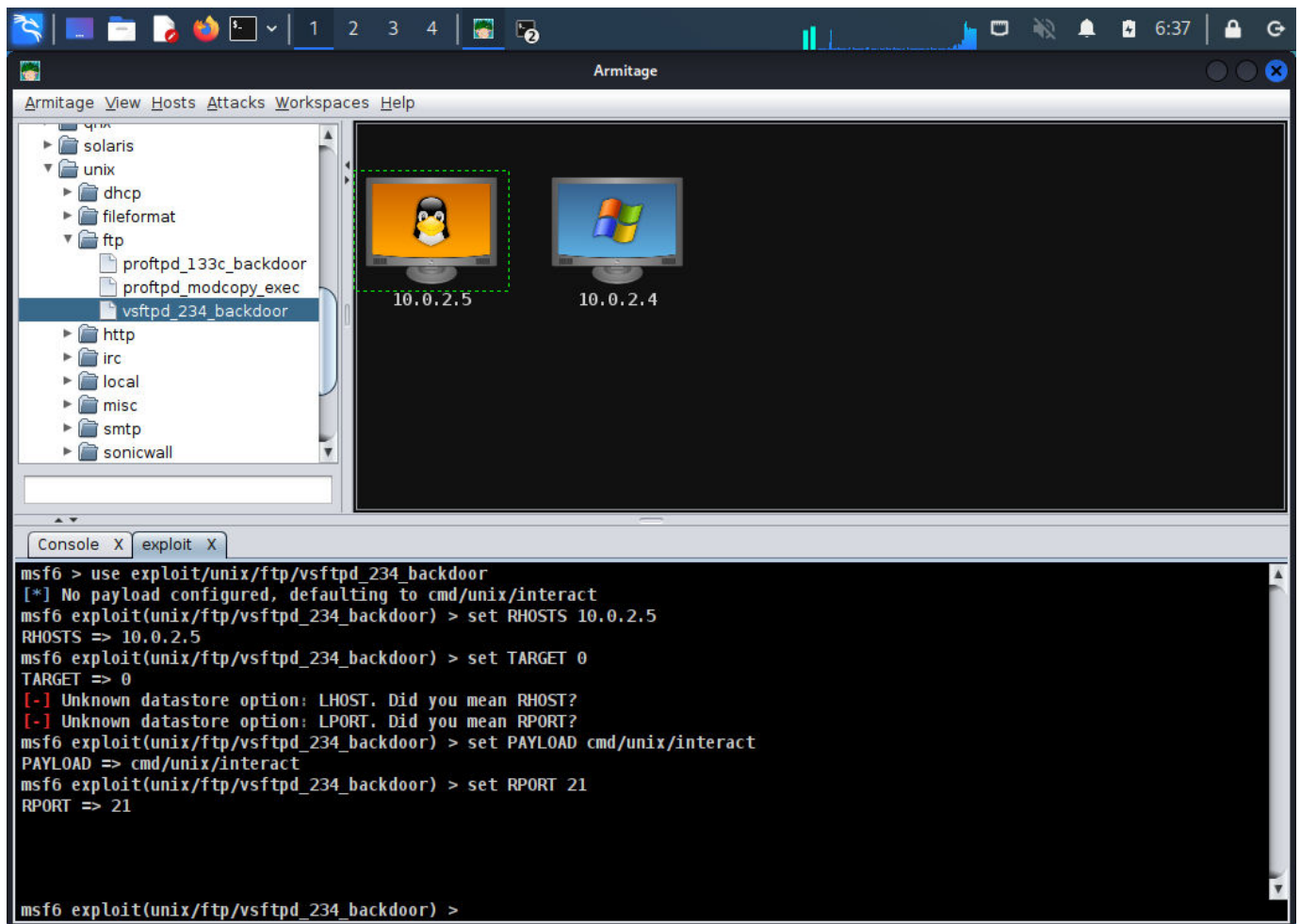
Linux

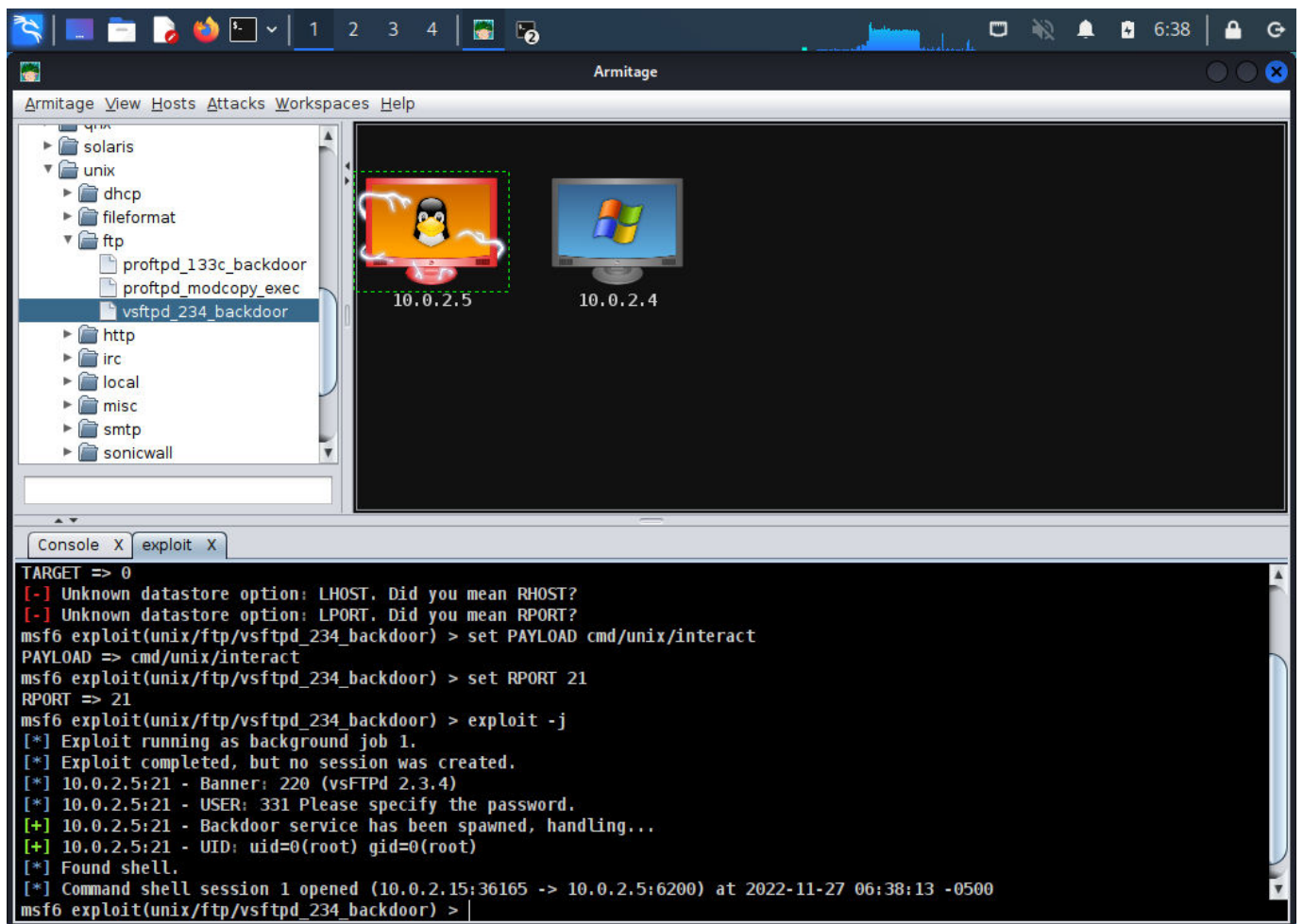


LHOST – KALI MACHINE

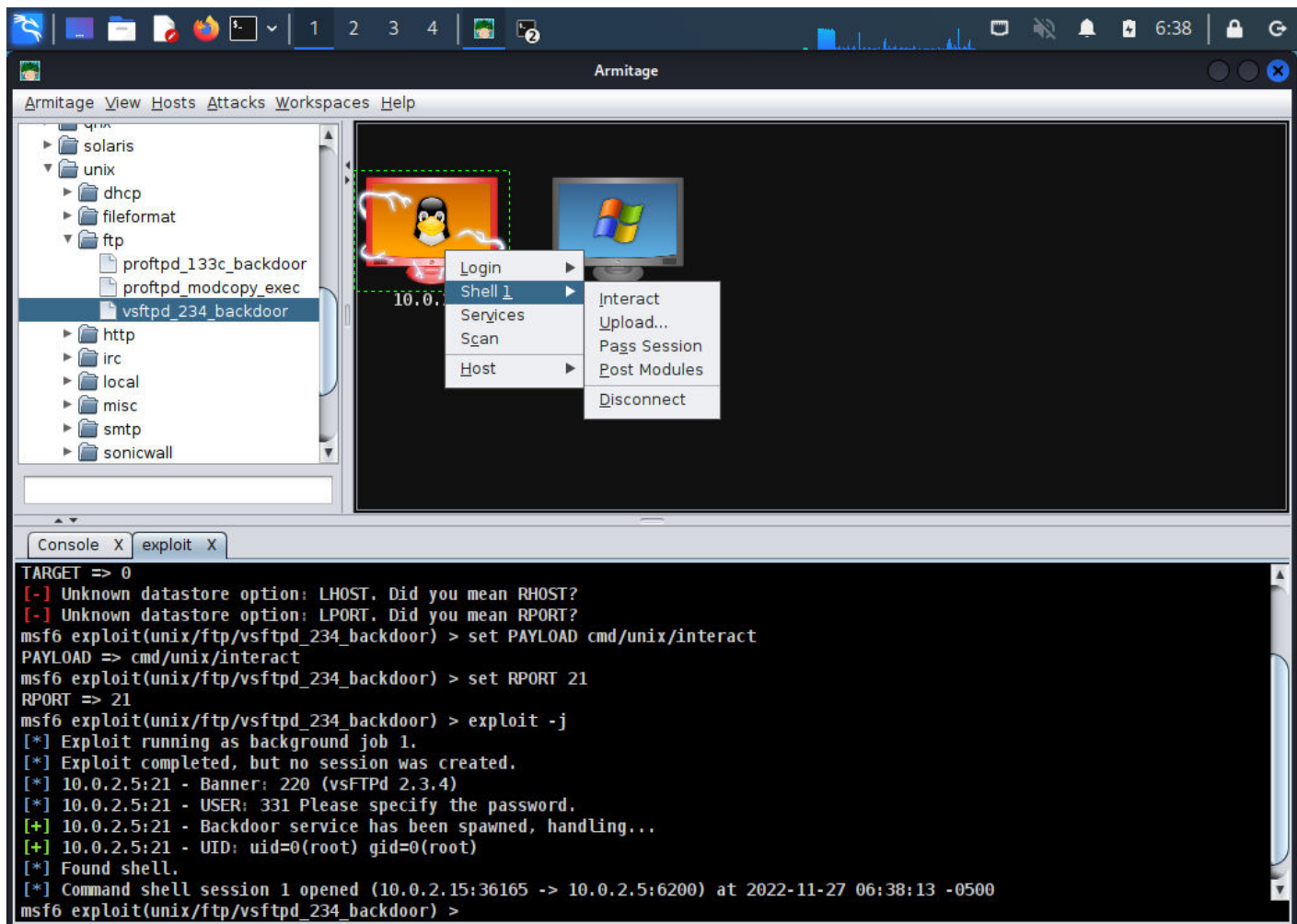
RHOST – LINUX MACHINE (METASPLOITABLE)

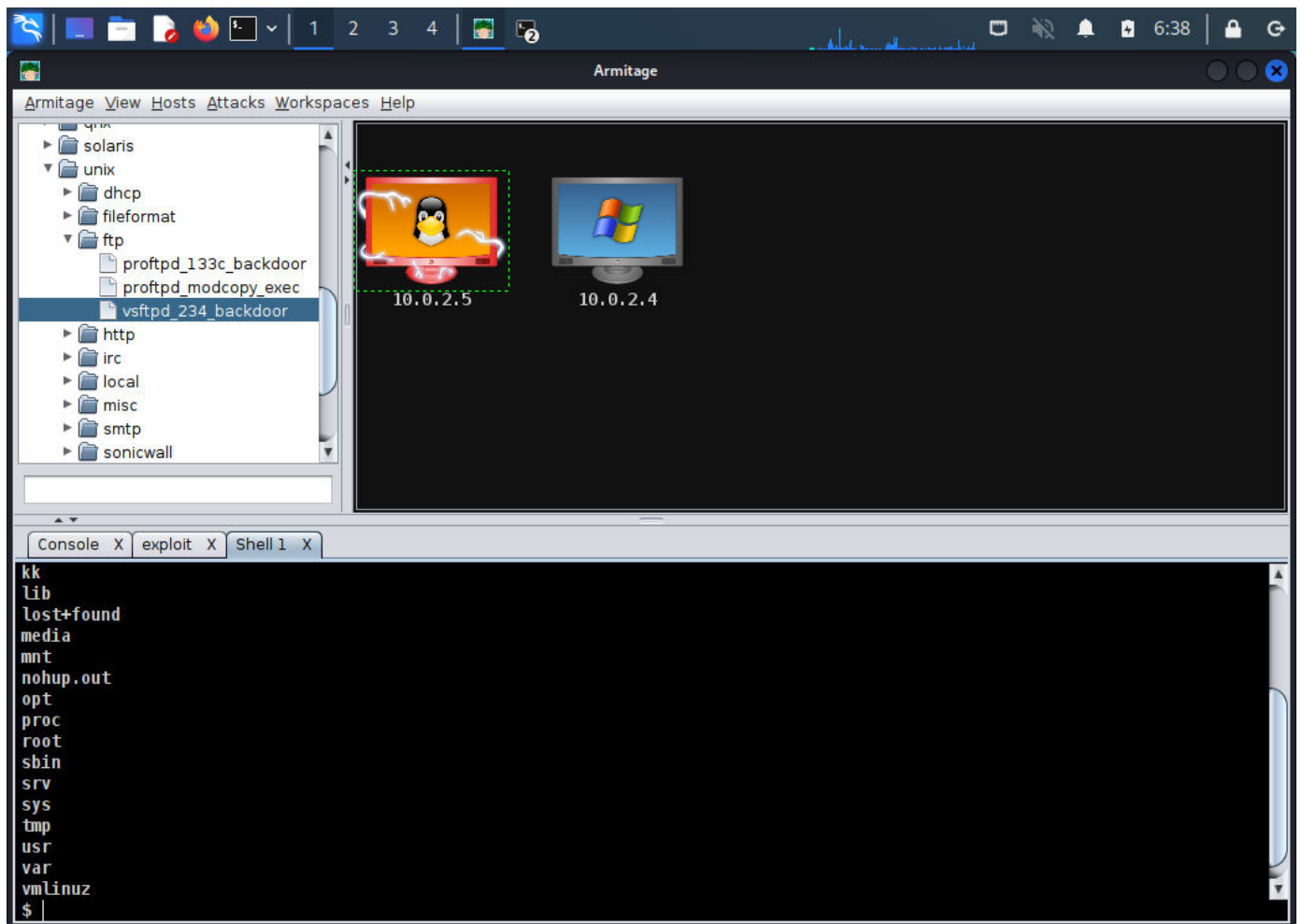
The exploit is ongoing .



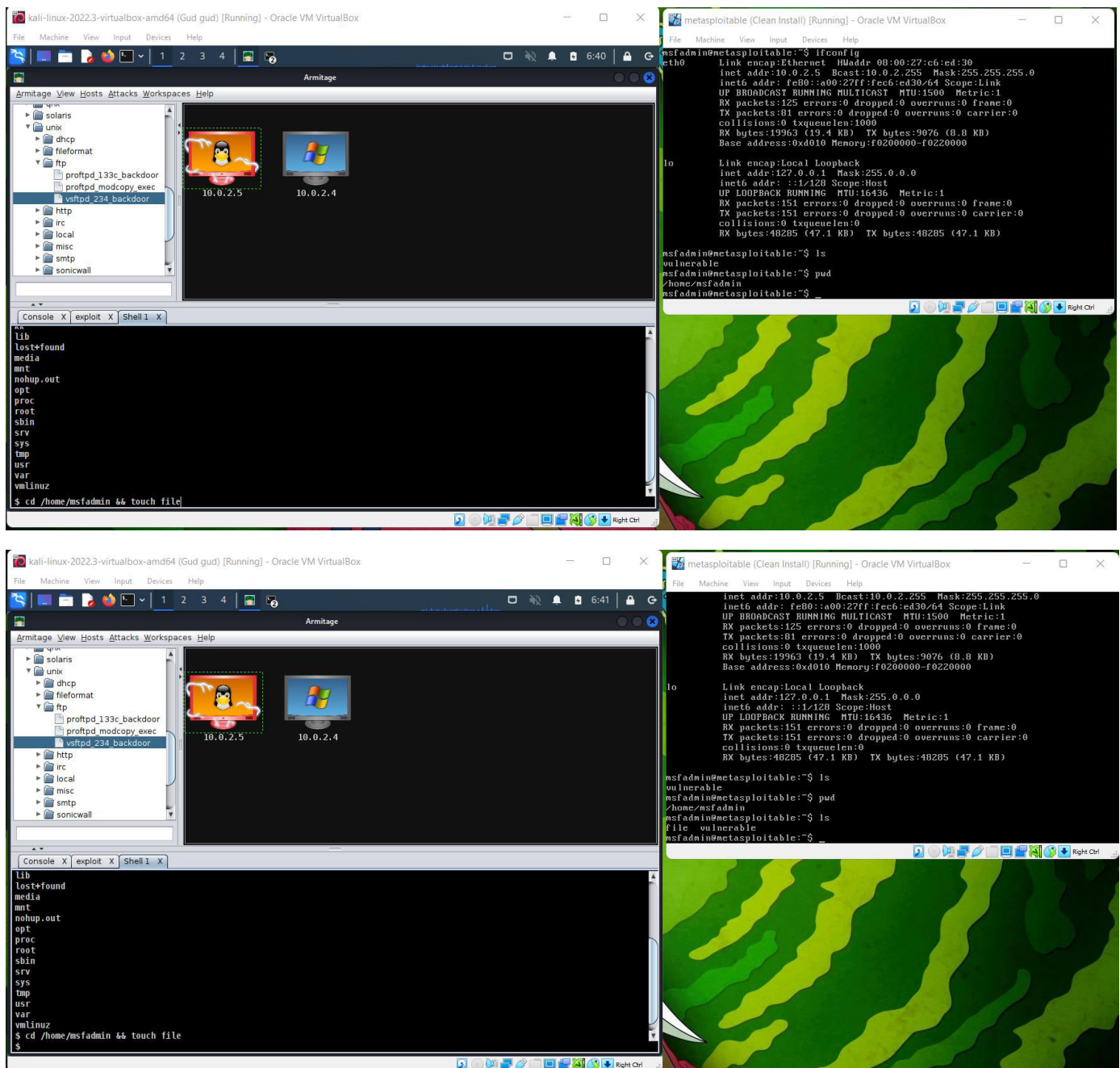


Interact with the found shell.

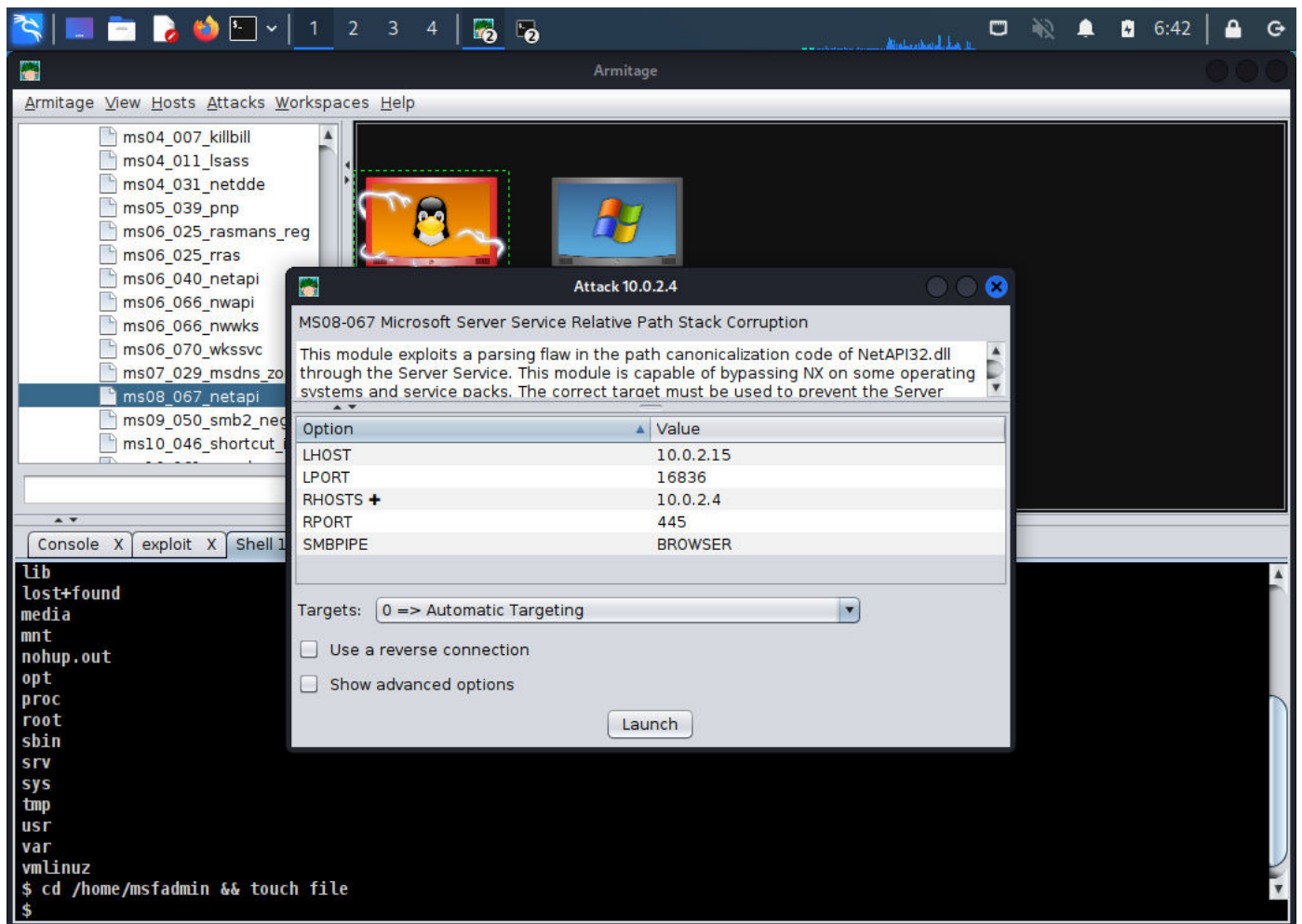


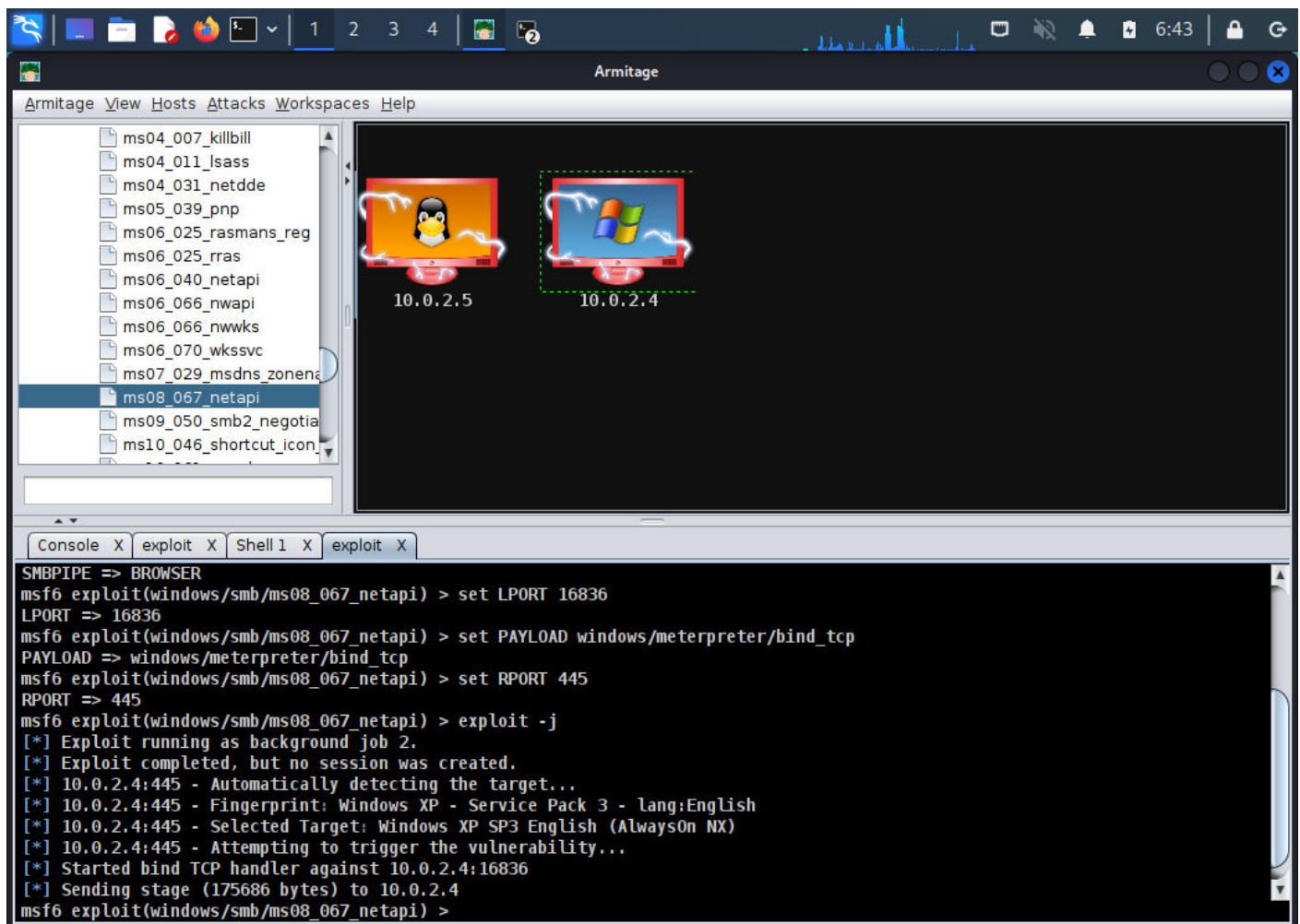


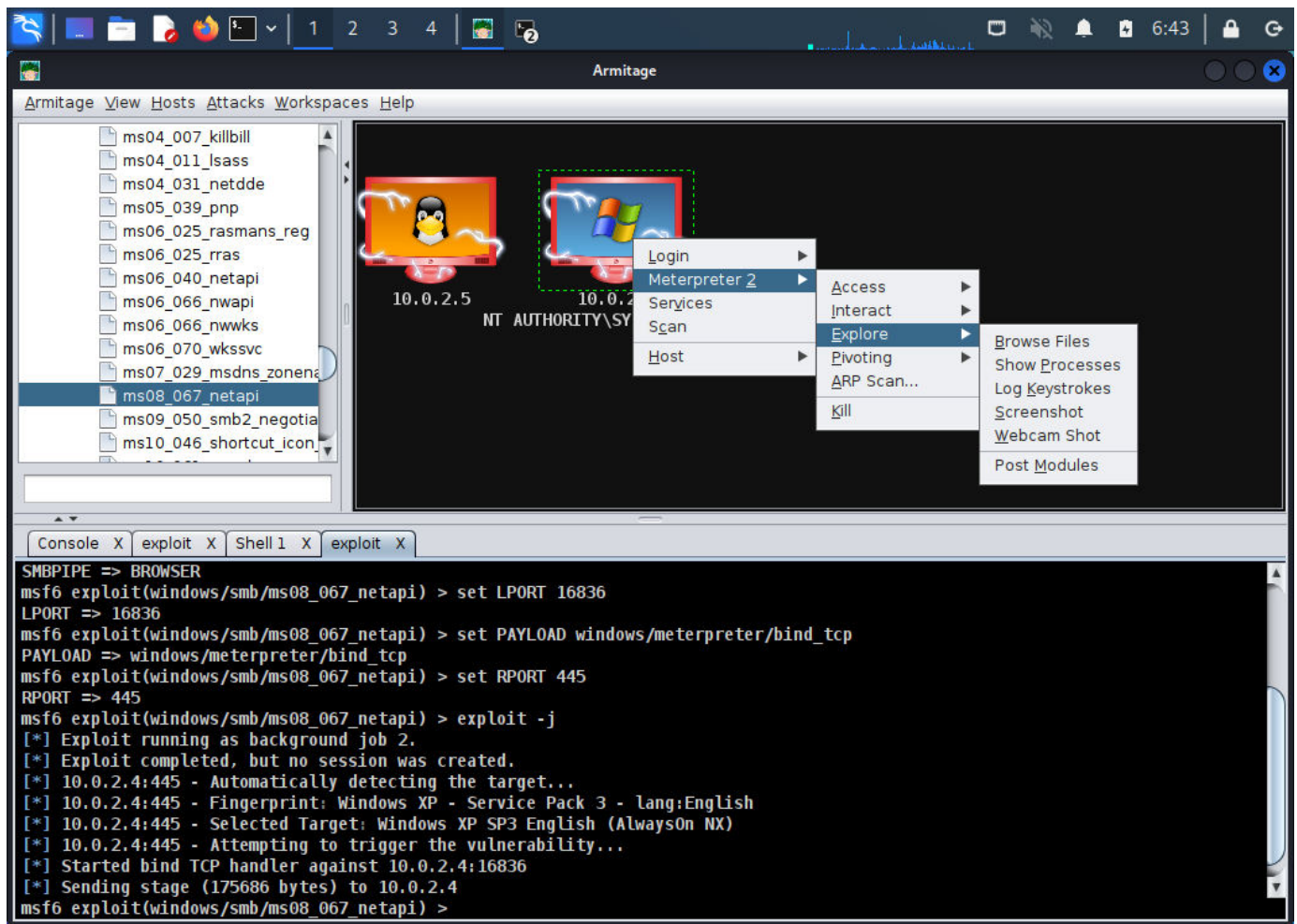
We will create , trough the shell , a file in /home/msfadmin , an we will print the directory contents from the metasploitable machine .



Windows







Let's take a screenshot:

