

LAB 1: Using INetSim on Kali Linux

Course Name: Malware Analysis and Reverse Engineering (IAM302)

Student Name: Nguyễn Trần Vinh – SE160258

Instructor Name: Mai Hoàng Đình

Lab Due Date: 7/1/2023

Purpose

We will use Kali Linux to simulate the Internet, and the Windows machine will be fooled by it.

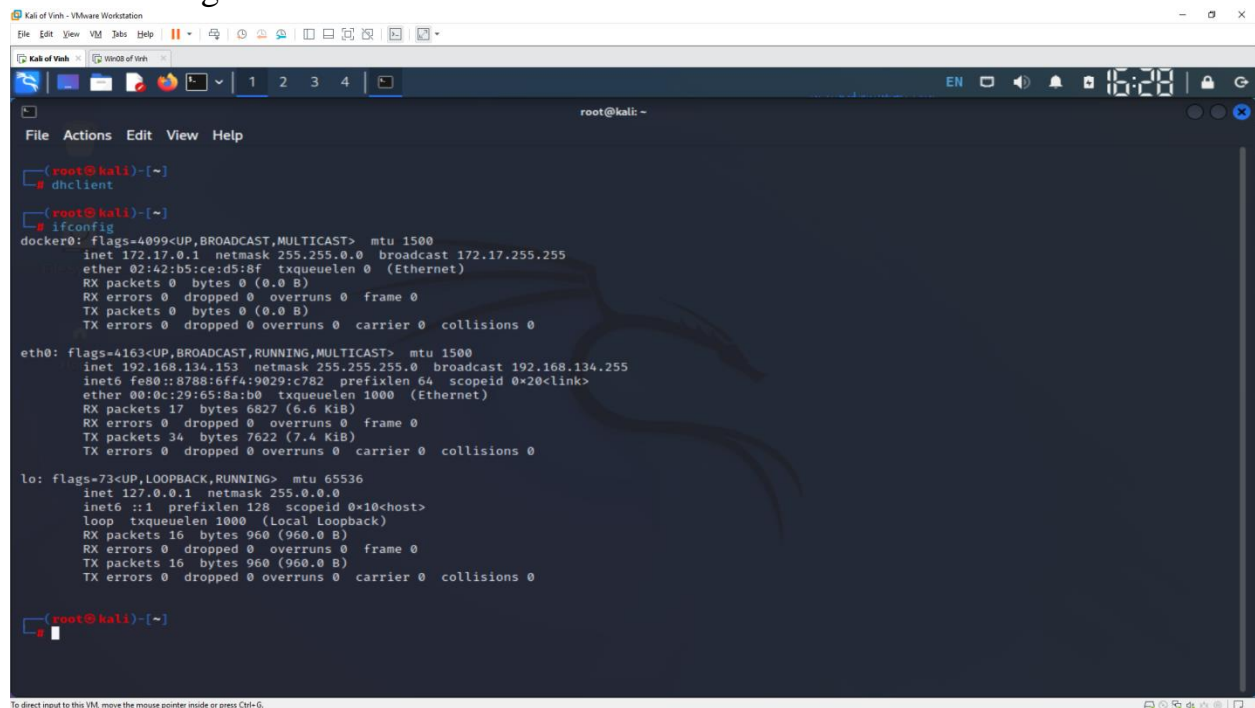
Getting the Virtual Machine 7-Zip Archive Files

The two files you need are:

- Kali Linux 32 bit VM PAE: Kali-Linux-2016.2-vm-i686.7z (or a later version)
- Windows 2008 Server: Win2008-Target.7z

Setting the Kali Linux VM to NAT Networking

- dhclient
- ifconfig



```
root@kali:~# dhclient
root@kali:~# ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:b5:ce:d5:8f txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

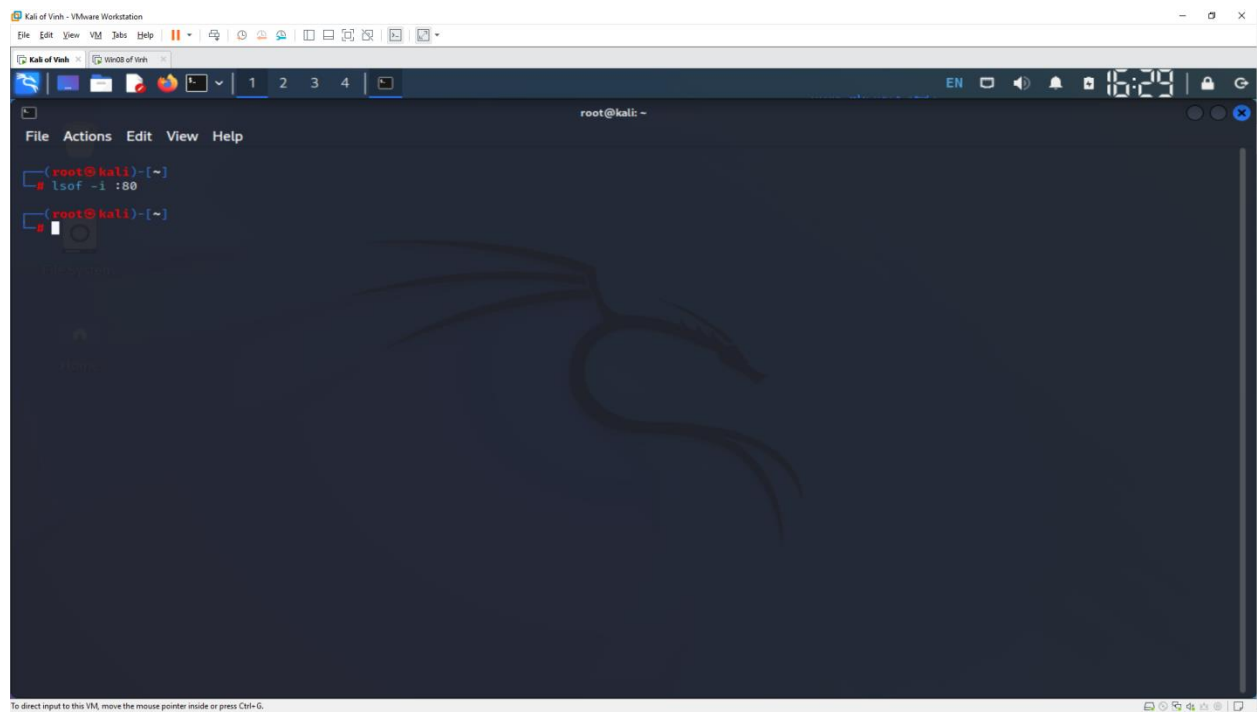
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.134.153 netmask 255.255.255.0 broadcast 192.168.134.255
    inet6 fe80::8788:6ff4:9029:c782 prefixlen 64 scopeid 0<20<link>
    ether 00:0c:29:65:8a:b0 txqueuelen 1000 (Ethernet)
    RX packets 17 bytes 6827 (6.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 7622 (7.4 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 16 bytes 960 (960.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 16 bytes 960 (960.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~#
```

Checking for a Web server

- lsof -i :80



Configuring inetsim

- dns_default_ip
- service_bind_address

```
Kali of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh x VMWare of Vinh x
1 2 3 4
EN 16:31
root@kali: ~
File Actions Edit View Help
GNU nano 7.0 /etc/inetsim/inetsim.conf *
start_service quotd_tcp
start_service quotd_udp
start_service chargen_tcp
start_service chargen_udp
start_service dummy_tcp
start_service dummy_udp

#####
# service_bind_address
#
# IP address to bind services to
#
# Syntax: service_bind_address <IP address>
#
# Default: 127.0.0.1
#
service_bind_address 0.0.0.0

#####
# service_run_as_user
#
# User to run services
#
# Syntax: service_run_as_user <username>
#
# Default: inetsim
#
service_run_as_user nobody

#####
# service_max_childs
#

#####
# Help
# Exit
# Write Out
# Read File
# Where Is
# Replace
# Cut
# Paste
# Execute
# Justify
# Location
# Go To Line
# M-U
# Undo
# M-E
# Redo
# M-A
# Set Mark
# M-C
# Copy
# M-J
# To Bracket
# M-W
# Where Was
```

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

```
Kali of Vinh - VMware Workstation
File Edit View VM Tabs Help
Kali of Vinh x VMWare of Vinh x
1 2 3 4
EN 16:33
root@kali: ~
File Actions Edit View Help
root@kali: ~ x kali@kali: ~ x
GNU nano 7.0 /etc/inetsim/inetsim.conf *
#
#dns_bind_port 53

#####
# dns_default_ip
#
# Default IP address to return with DNS replies
#
# Syntax: dns_default_ip <IP address>
#
# Default: 127.0.0.1
#
dns_default_ip 192.168.134.153

#####
# dns_default_hostname
#
# Default hostname to return with DNS replies
#
# Syntax: dns_default_hostname <hostname>
#
# Default: www
#
#dns_default_hostname somehost

#####
# dns_default_domainname
#
# Default domain name to return with DNS replies
#

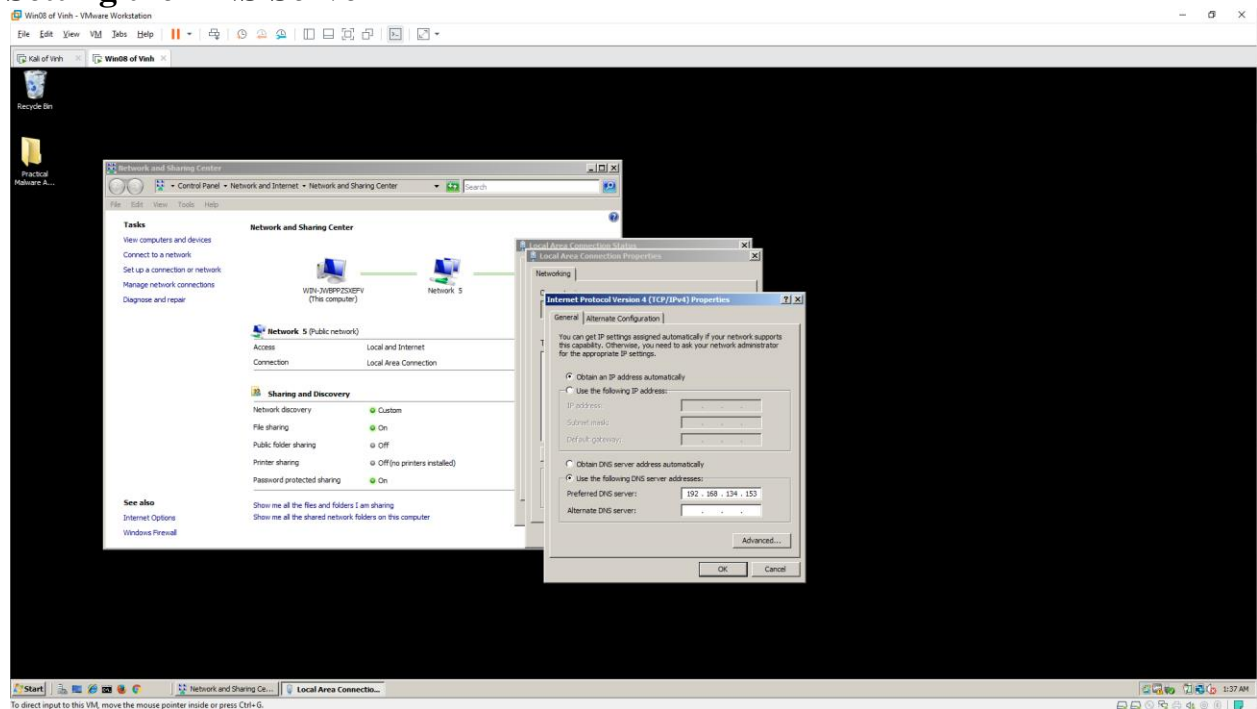
#####
# Help
# Exit
# Write Out
# Read File
# Where Is
# Replace
# Cut
# Paste
# Execute
# Justify
# Location
# Go To Line
# M-U
# Undo
# M-E
# Redo
# M-A
# Set Mark
# M-C
# Copy
# M-J
# To Bracket
# M-W
# Where Was
```

To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

```
Kali of Vinh - VMware Workstation
File Edit View VM Help
Kali of Vinh
root@kali: ~
File Actions Edit View Help
root@kali: ~ x kali@kali: ~ x
(root@kali)~# inetsim
INetSim 1.3.2 (2020-05-19) by Matthias Eckert & Thomas Hungenberg
Main logfile '/var/log/inetsim/main.log' does not exist. Trying to create it ...
Main logfile '/var/log/inetsim/main.log' successfully created.
Sub logfile '/var/log/inetsim/service.log' does not exist. Trying to create it ...
Sub logfile '/var/log/inetsim/service.log' successfully created.
Debug logfile '/var/log/inetsim/debug.log' does not exist. Trying to create it ...
Debug logfile '/var/log/inetsim/debug.log' successfully created.
Using log directory: /var/log/inetsim/
Using data directory: /var/lib/inetsim/
Using report directory: /var/log/inetsim/report/
Using configuration file: /etc/inetsim/inetsim.conf
Parsing configuration file.
Configuration file parsed successfully.
== INetSim main process started (PID 6503) ==
Session ID: 6503
Listening on: 0.0.0.0
Real Date/Time: 2023-01-07 04:35:50
Fake Date/Time: 2023-01-07 04:35:50 (Delta: 0 seconds)
Forking services ...
* dns_53_tcp_udp - started (PID 6505)
* echo_7_udp - started (PID 6525)
* echo_7_tcp - started (PID 6524)
* chargen_19_tcp - started (PID 6530)
* time_37_tcp - started (PID 6520)
* https_443_tcp - started (PID 6507)
* tftp_69_udp - started (PID 6514)
* daytime_13_tcp - started (PID 6522)
* ftps_990_tcp - started (PID 6513)
* irc_6667_tcp - started (PID 6515)
* pop3s_995_tcp - started (PID 6511)
* quotd_17_udp - started (PID 6529)
* time_37_udp - started (PID 6521)
* smtp_25_tcp - started (PID 6508)
```

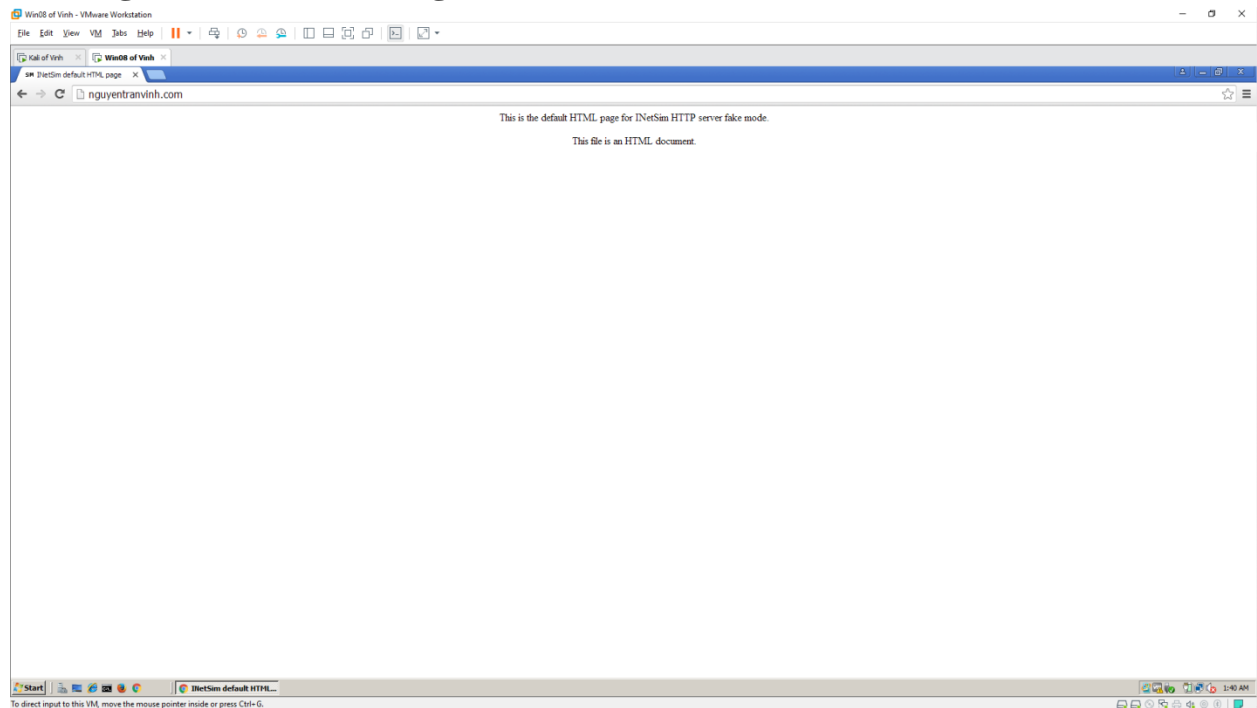
To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

Setting the DNS Server



To direct input to this VM, move the mouse pointer inside or press Ctrl-G.

Viewing an HTTP Web Page



Scanning

