

PROJ 3 : Using INetSim on Kali Linux

Prof. Alberto LaCava

CY -640

MALWARE ANALYSIS & DEFENSE

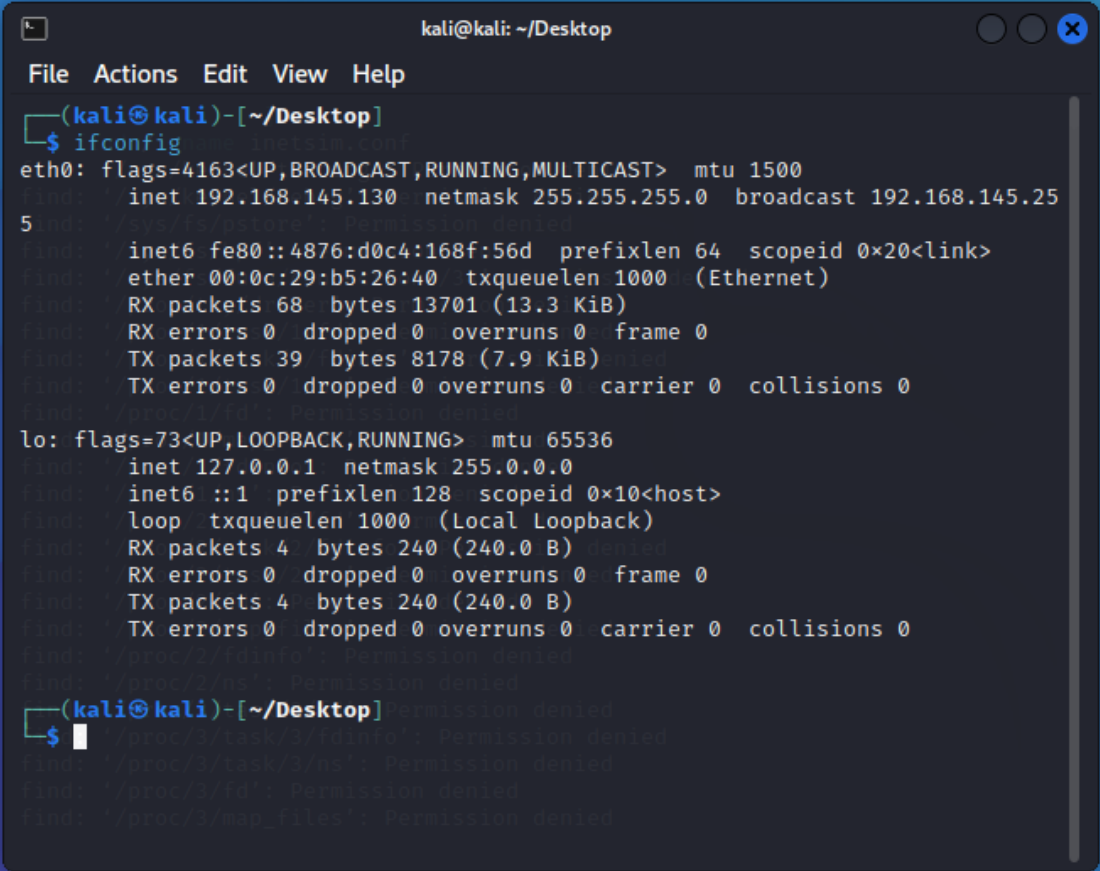
Nikhil Patel

09/20/2022

Introduction : In this lab, we will learn how to configure the INet on a Kali Linux virtual machine, as well as collect some packets using Zenmap.

Procedure :

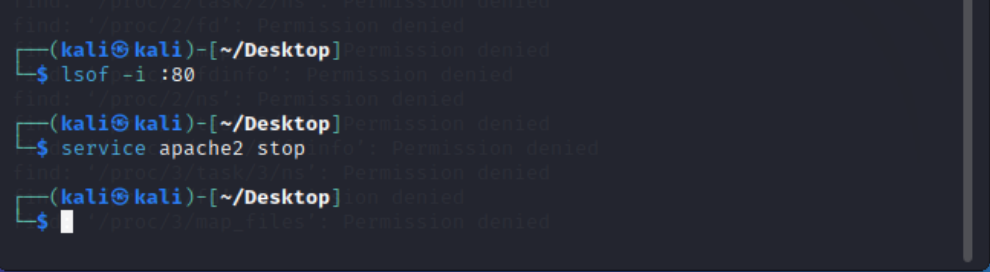
1. Open kali Linux 32 bit in a virtual machine.
2. Login using id as *root* and *toor*.
3. Now open the terminal and type *ifconfig* to find the ip address of the machine.



```
kali@kali: ~/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.145.130 netmask 255.255.255.0 broadcast 192.168.145.255
    ether 00:0c:29:b5:26:40 txqueuelen 1000 (Ethernet)
    RX packets 68 bytes 13701 (13.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 39 bytes 8178 (7.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

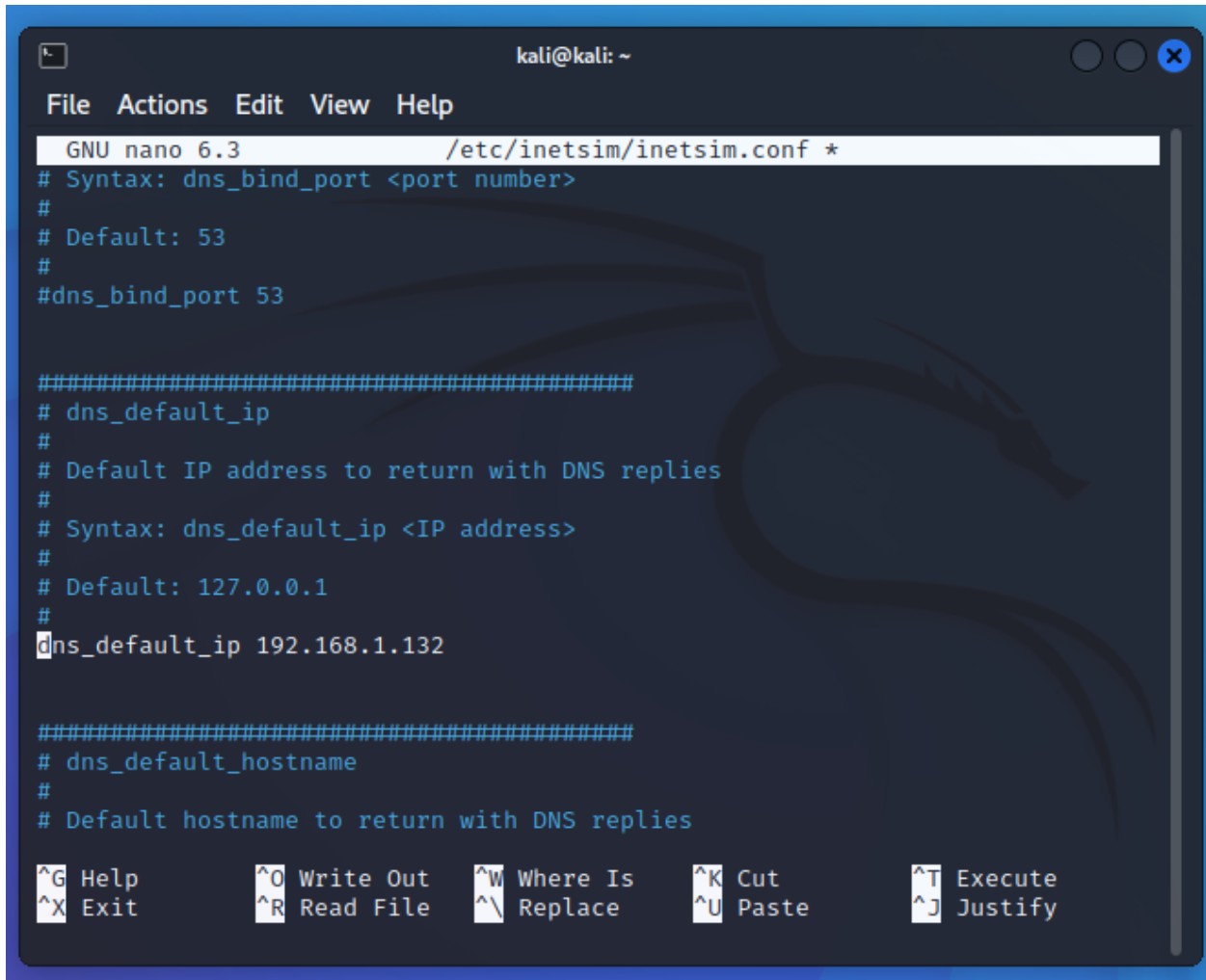
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

4. Now execute *lsof -i :80* and stop a apache server using *service apache2 stop*.



```
(kali@kali)-[~/Desktop]
$ lsof -i :80
service apache2 stop
```

5. Now we will configure inetsim. Execute `cp /etc/inetsim/intesim.conf /etc/inetsim/inetsim.conf.orig` followed by `nano /etc/inetsim/inetsim.conf`.
6. You will see the notepad has been launched now search for `#service_bind_address 10.10.10.1` and remove # from the line and proceed.
7. Now we will look for `#dns_default_ip 10.10.10.1` to `dns_default_ip 192.168.1.132`.



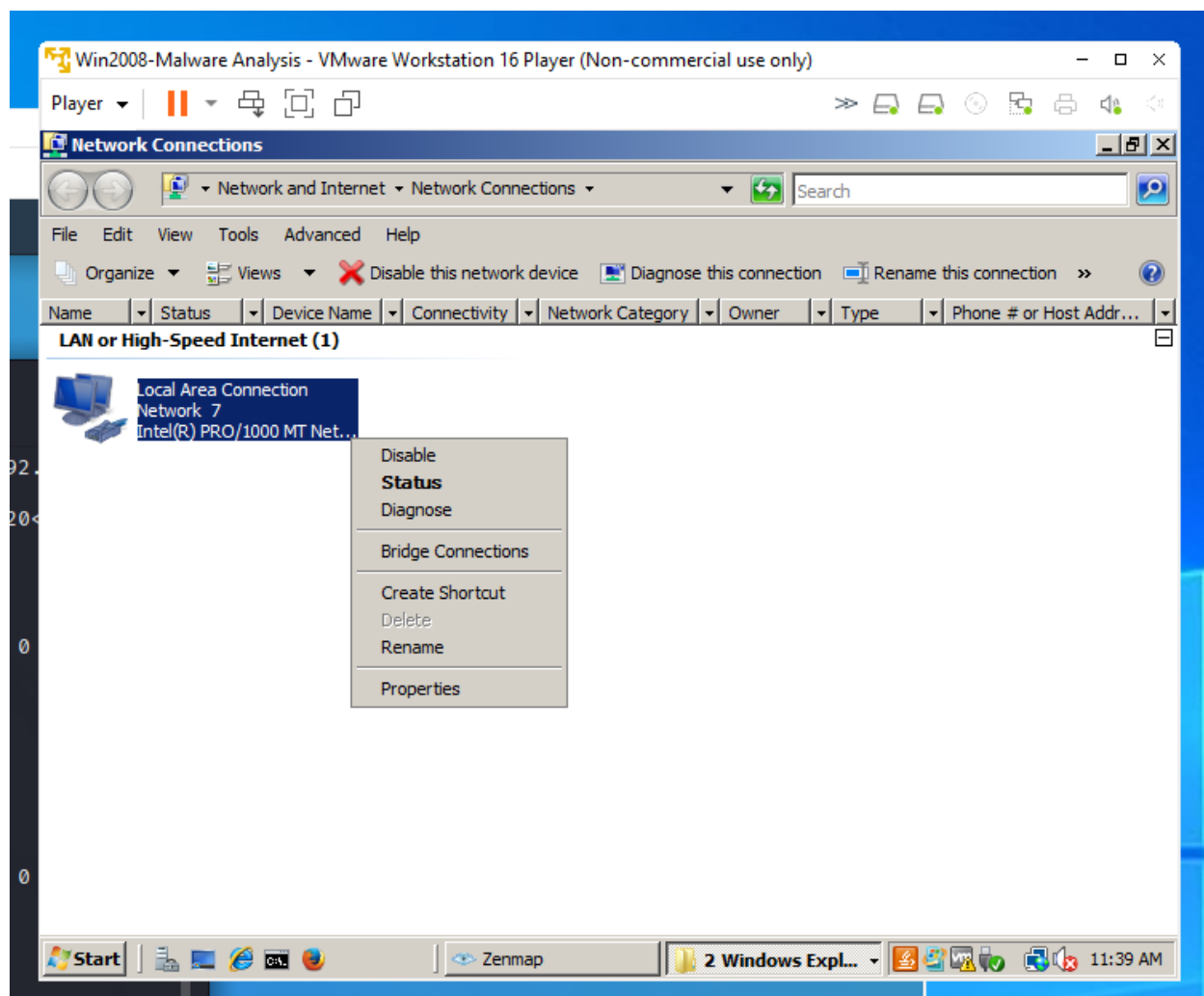
```
kali@kali: ~
File Actions Edit View Help
GNU nano 6.3 /etc/inetsim/inetsim.conf *
# Syntax: dns_bind_port <port number>
#
# Default: 53
#
#dns_bind_port 53

#####
# 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 192.168.1.132

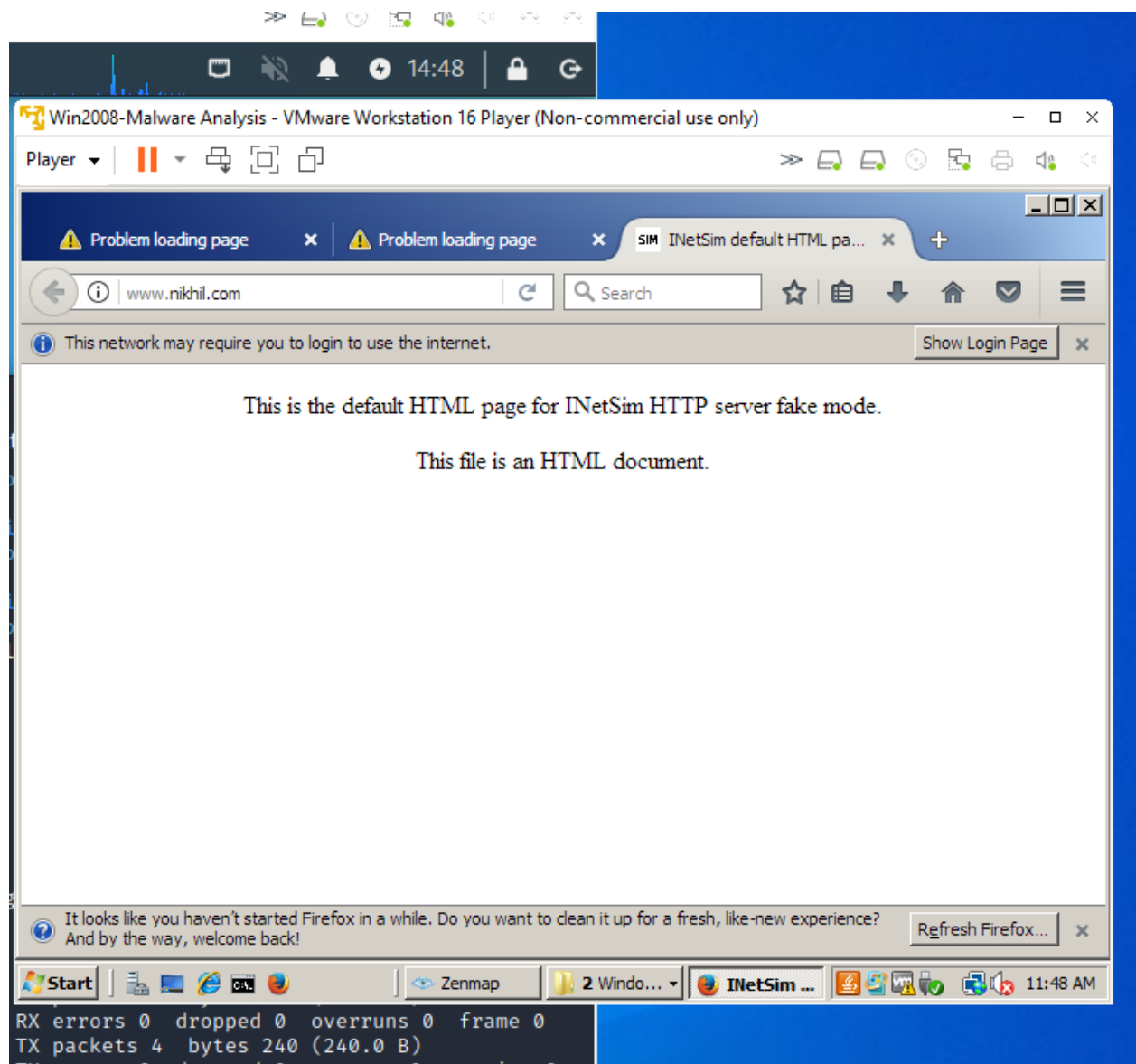
#####
# dns_default_hostname
#
# Default hostname to return with DNS replies

^G Help      ^O Write Out  ^W Where Is   ^K Cut        ^T Execute
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify
```

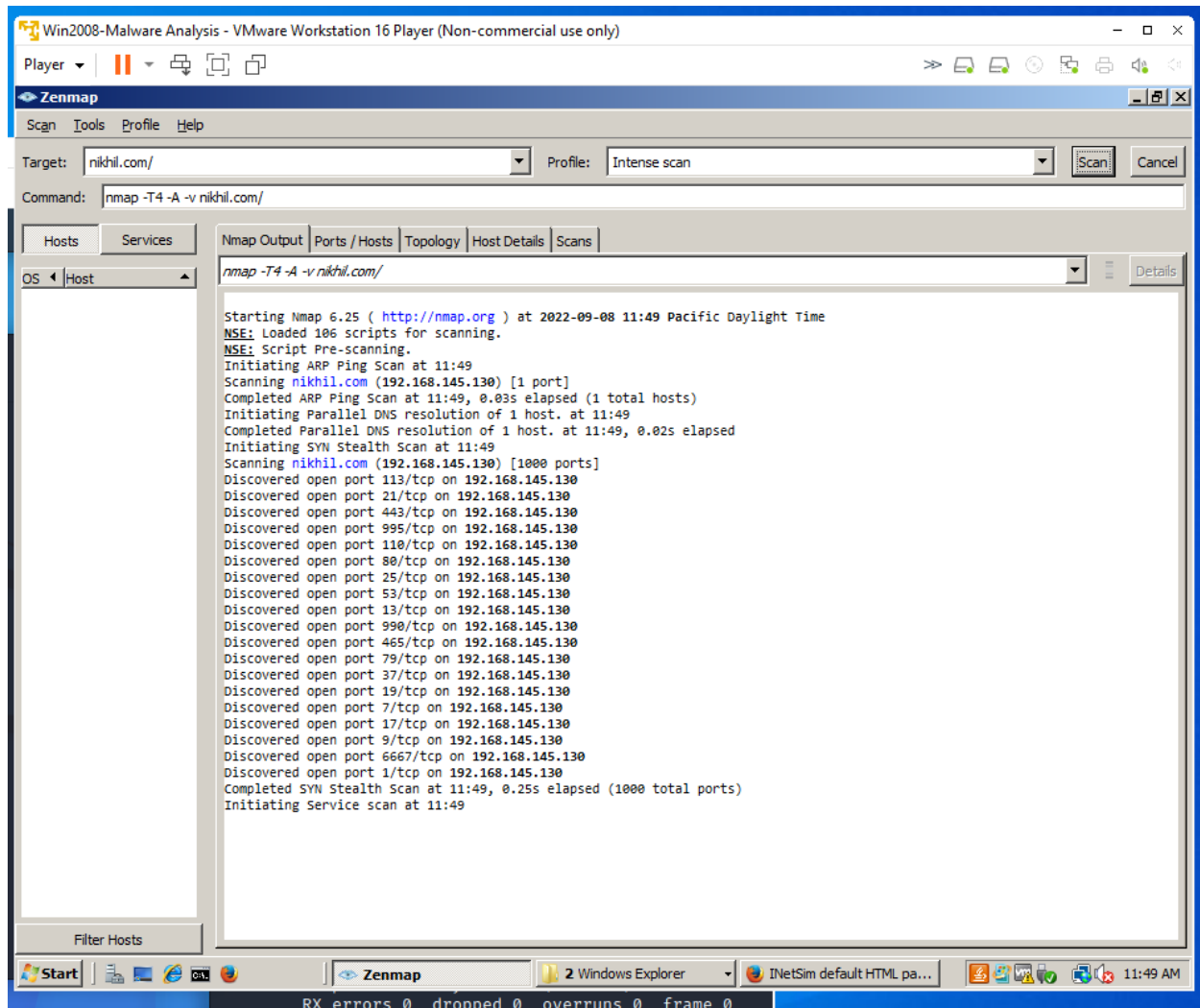
8. Press `ctrl + x`, `y` and hit `enter` to save the file.
9. Now open a terminal and type `"inetsim"`.
10. Type `"ifconfig eth0"` to find the ip address of the LAN.
11. Open Windows server 2008 login as admin as *Administrator & P@ssw0rd*.
12. Go to network and select properties.
13. Right click on *LAN*.
14. Double click on the IPV4 and new dns server to kali linux machine. Click ok and exit.



15. Go to the browser and type “<http://NIKHIL.com> “. You will see the INetSim default html page.



16. Now we will use zenmap to scan the website you have entered in the browser.
17. You see a long list of open ports is visible in the nmap window.
18. Take a screenshot of the field.



Conclusion : To end the experiment, I learnt how to link the Kali Linux VM to Windows Server 2012 for the INetSim. After that, we checked for open ports on the server and configured the DNS server in Windows using the IP address of the Kali Machine.