	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Weekly Report for Internship

Roll No: TACO19108

Name of the Student: Ojus Jaiswal

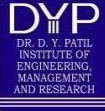
Name of the Company: T A L A K U N C H I Networks Pvt. Ltd.

Domain of Internship: Cyber Security (Ethical Hacking)

Name of the Internal Guide: Mrs. Nalini Jagtap

Name of the External Guide: Mrs. Poojitha Nandimandalam

Duration of Internship: 2 Months

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Week - VII

Dates: 21 February, 2022 to 27 February, 2022

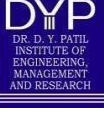
Description of work done till date:

In seventh week, we were given project no. 5 i.e., Exploiting Server Vulnerabilities. In this project we have to use tools and commands like SMTP Open Relay, Zone Transfer, NetBIOS Enumeration, Wireshark and DOS Attack. These tools can be used for brute forcing activities which will give us access to server, sniffing traffic and denying access to server. Once we gain access, we can use data present in system for our own benefits. That's why testing server is important as these vulnerabilities might be present and can be exploited and it is also possible to deny access to user.

We were first told to attend sessions from LMS which will cover basics regarding the topic. Then after completion of sessions from LMS, live hands-on lecture was conducted in which the instructor showed us practical implementation of project. Then doubt session was conducted for clearing our doubts and to check if we were facing any problem in project execution.

Student Sign

Internal Guide Sign

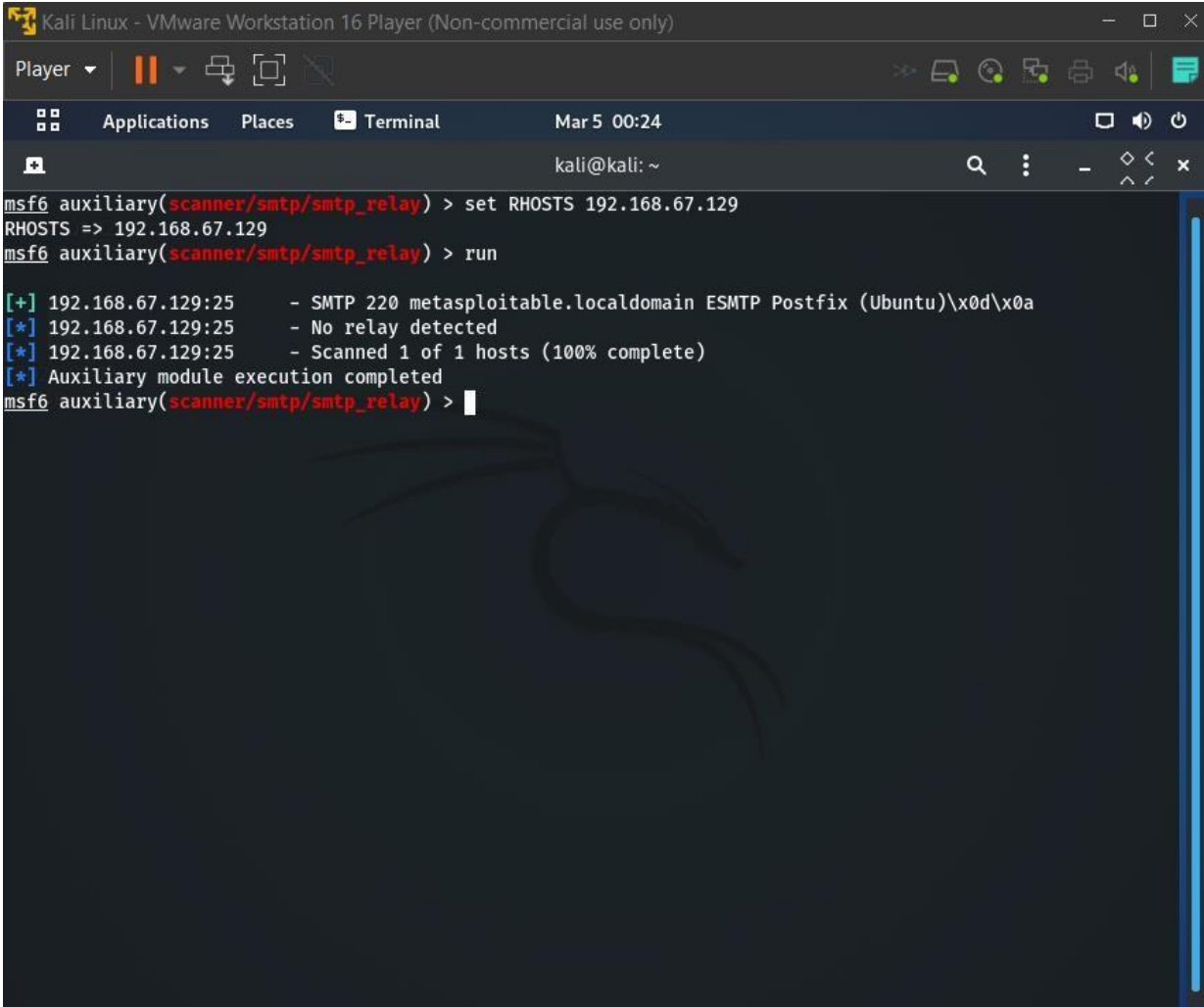
	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

Supporting Documents:

Internship Project 2 Exploiting Server Vulnerabilities

Task 1 :- Check for SMTP Open Relay

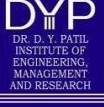
Solution :-



```

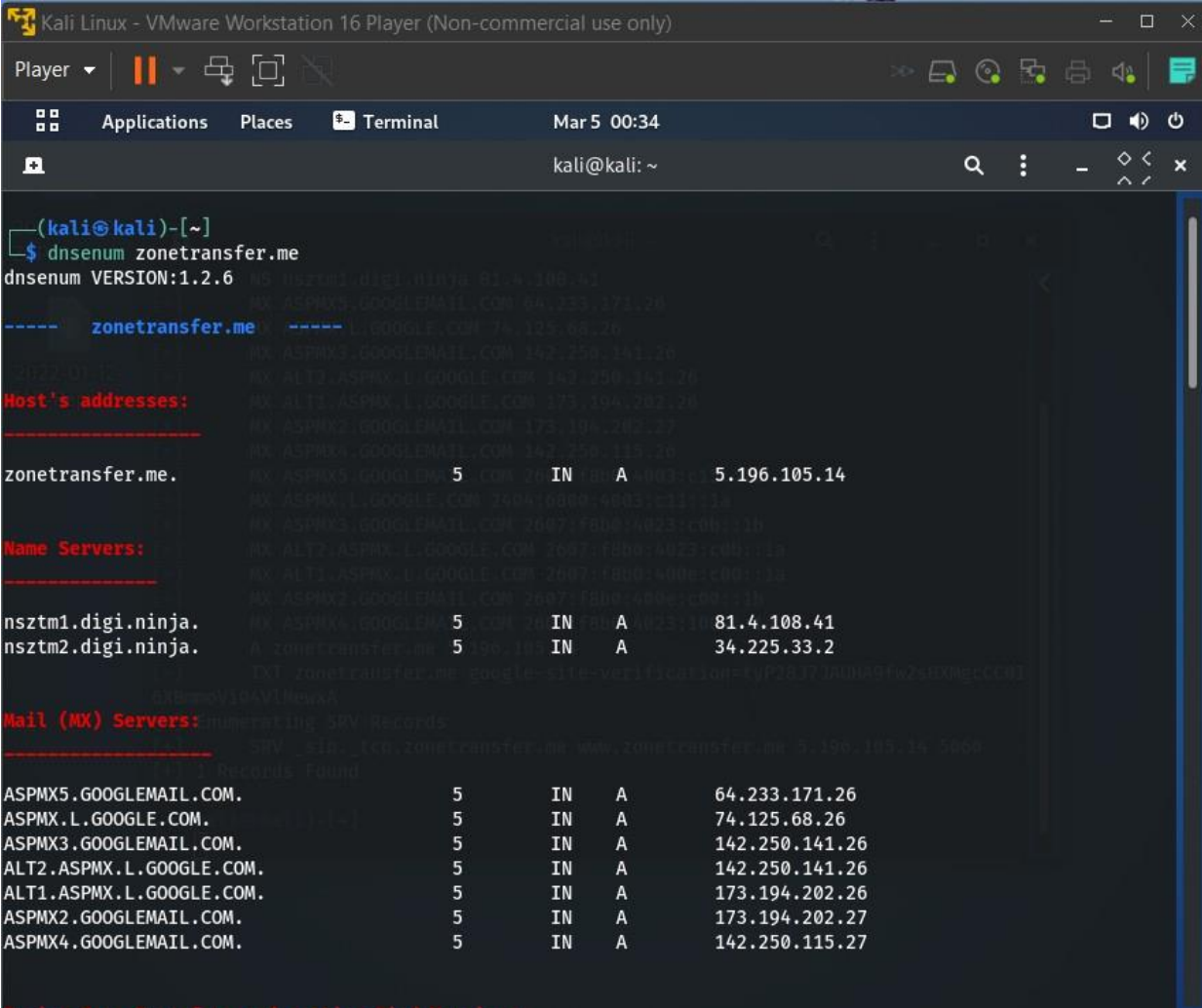
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | [Pause] [Full Screen] [Close] [Maximize] [Refresh] [Help]
Applications Places Terminal Mar 5 00:24
kali@kali: ~
msf6 auxiliary(scanner/smtp/smtp_relay) > set RHOSTS 192.168.67.129
RHOSTS => 192.168.67.129
msf6 auxiliary(scanner/smtp/smtp_relay) > run
[+] 192.168.67.129:25 - SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a
[*] 192.168.67.129:25 - No relay detected
[*] 192.168.67.129:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_relay) >

```

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022


Task 2 :- Check for Zone Transfers

Solution :-



```

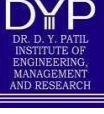
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | [Pause] [Full Screen] [Close]
Applications Places Terminal Mar 5 00:34
kali@kali: ~
(kali@kali)-[~]
$ dnstenum zonetransfer.me
dnstenum VERSION:1.2.6
----- zonetransfer.me -----
Host's addresses:
-----
zonetransfer.me.
Name Servers:
-----
nszstm1.digi.ninja.
nszstm2.digi.ninja.
Mail (MX) Servers:
-----
ASPMX5.GOOGLEMAIL.COM.
ASPMX.L.GOOGLE.COM.
ASPMX3.GOOGLEMAIL.COM.
ALT2.ASPMX.L.GOOGLE.COM.
ALT1.ASPMX.L.GOOGLE.COM.
ASPMX2.GOOGLEMAIL.COM.
ASPMX4.GOOGLEMAIL.COM.
  
```

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

```

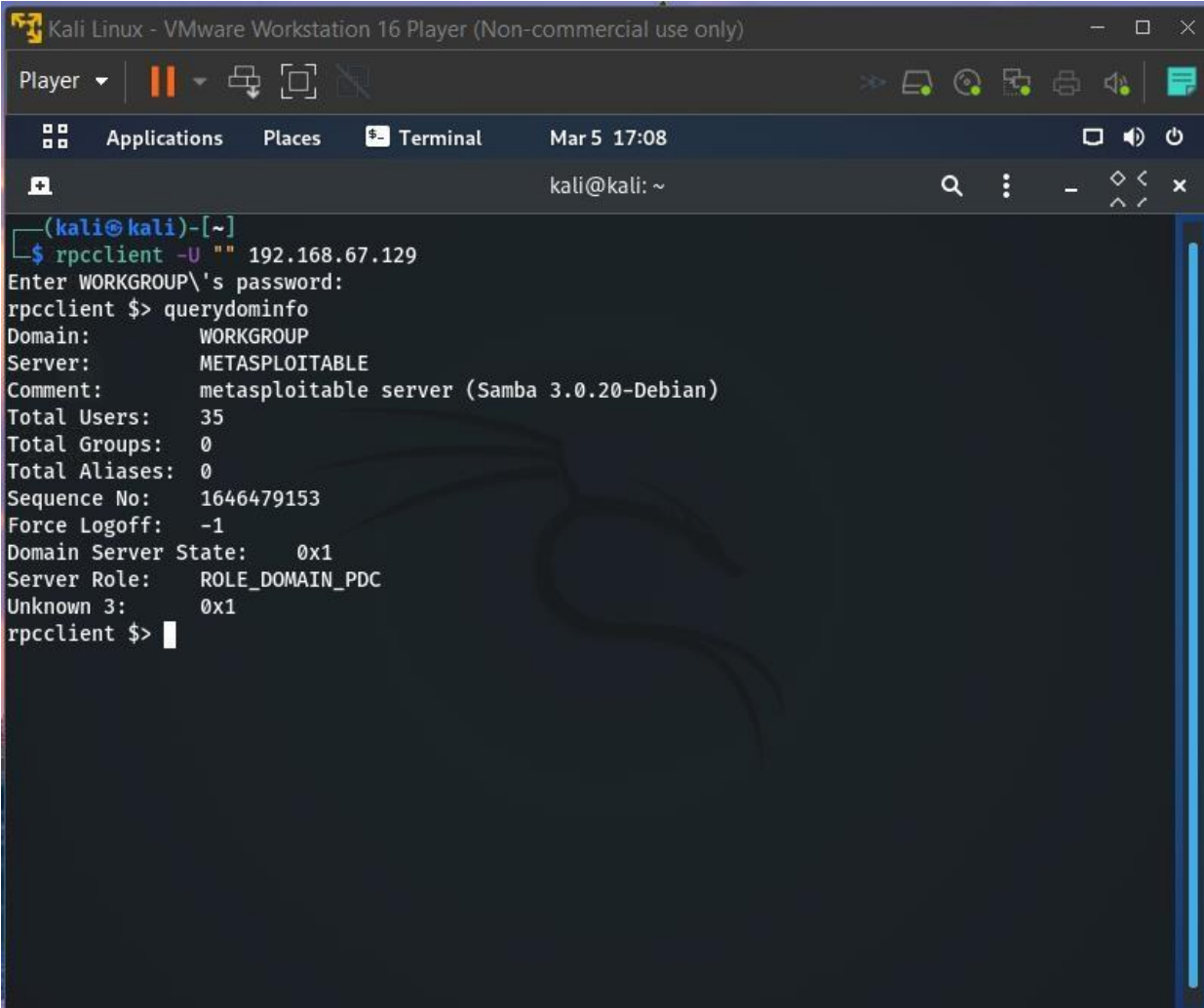
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminal Mar 5 00:34
kali@kali: ~
(kali@kali)-[~]
$ dnsrecon -d zonetransfer.me
[*] std: Performing General Enumeration against: zonetransfer.me...
[-] DNSSEC is not configured for zonetransfer.me
[*] SOA nsztml.digi.ninja 81.4.108.41
[*] NS nsztml.digi.ninja 34.225.33.2
[*] NS nsztml.digi.ninja 81.4.108.41
[*] MX ASPMX5.GOOGLEMAIL.COM 64.233.171.26
[*] MX ASPMX.L.GOOGLE.COM 74.125.68.26
[*] MX ASPMX3.GOOGLEMAIL.COM 142.250.141.26
[*] MX ALT2.ASPMX.L.GOOGLE.COM 142.250.141.26
[*] MX ALT1.ASPMX.L.GOOGLE.COM 173.194.202.26
[*] MX ASPMX2.GOOGLEMAIL.COM 173.194.202.27
[*] MX ASPMX4.GOOGLEMAIL.COM 142.250.115.26
[*] MX ASPMX5.GOOGLEMAIL.COM 2607:f8b0:4003:c15::1b
[*] MX ASPMX.L.GOOGLE.COM 2404:6800:4003:c11::1a
[*] MX ASPMX3.GOOGLEMAIL.COM 2607:f8b0:4023:c0b::1b
[*] MX ALT2.ASPMX.L.GOOGLE.COM 2607:f8b0:4023:c0b::1a
[*] MX ALT1.ASPMX.L.GOOGLE.COM 2607:f8b0:400e:c00::1a
[*] MX ASPMX2.GOOGLEMAIL.COM 2607:f8b0:400e:c00::1b
[*] MX ASPMX4.GOOGLEMAIL.COM 2607:f8b0:4023:1004::1a
[*] A zonetransfer.me 5.196.105.14
[*] TXT zonetransfer.me google-site-verification=typ28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VlMewxA
[*] Enumerating SRV Records
[+] SRV _sip._tcp.zonetransfer.me www.zonetransfer.me 5.196.105.14 5060
[+] 1 Records Found
(kali@kali)-[~]
$

```

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Task 3 :- Perform NetBIOS Enumeration

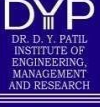
Solution :-

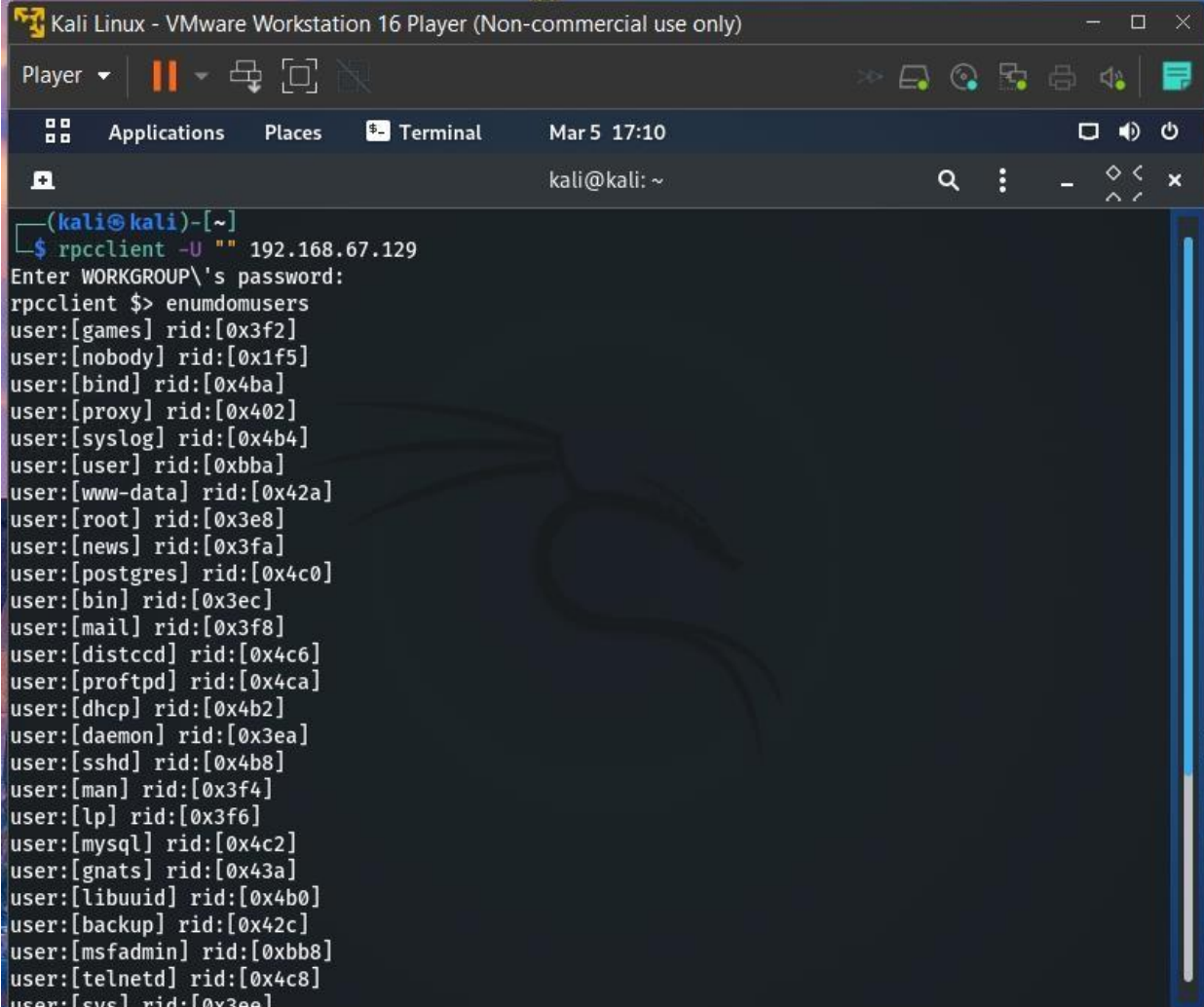


```

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | [Icons] | Mar 5 17:08
kali@kali: ~
(kali@kali)-[~]
$ rpcclient -U "" 192.168.67.129
Enter WORKGROUP\'s password:
rpcclient $> querydomaininfo
Domain:          WORKGROUP
Server:          METASPLOITABLE
Comment:         metasploitable server (Samba 3.0.20-Debian)
Total Users:     35
Total Groups:    0
Total Aliases:   0
Sequence No:     1646479153
Force Logoff:    -1
Domain Server State: 0x1
Server Role:     ROLE_DOMAIN_PDC
Unknown 3:       0x1
rpcclient $>

```

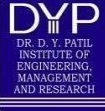
 <p>DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT AND RESEARCH</p>	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

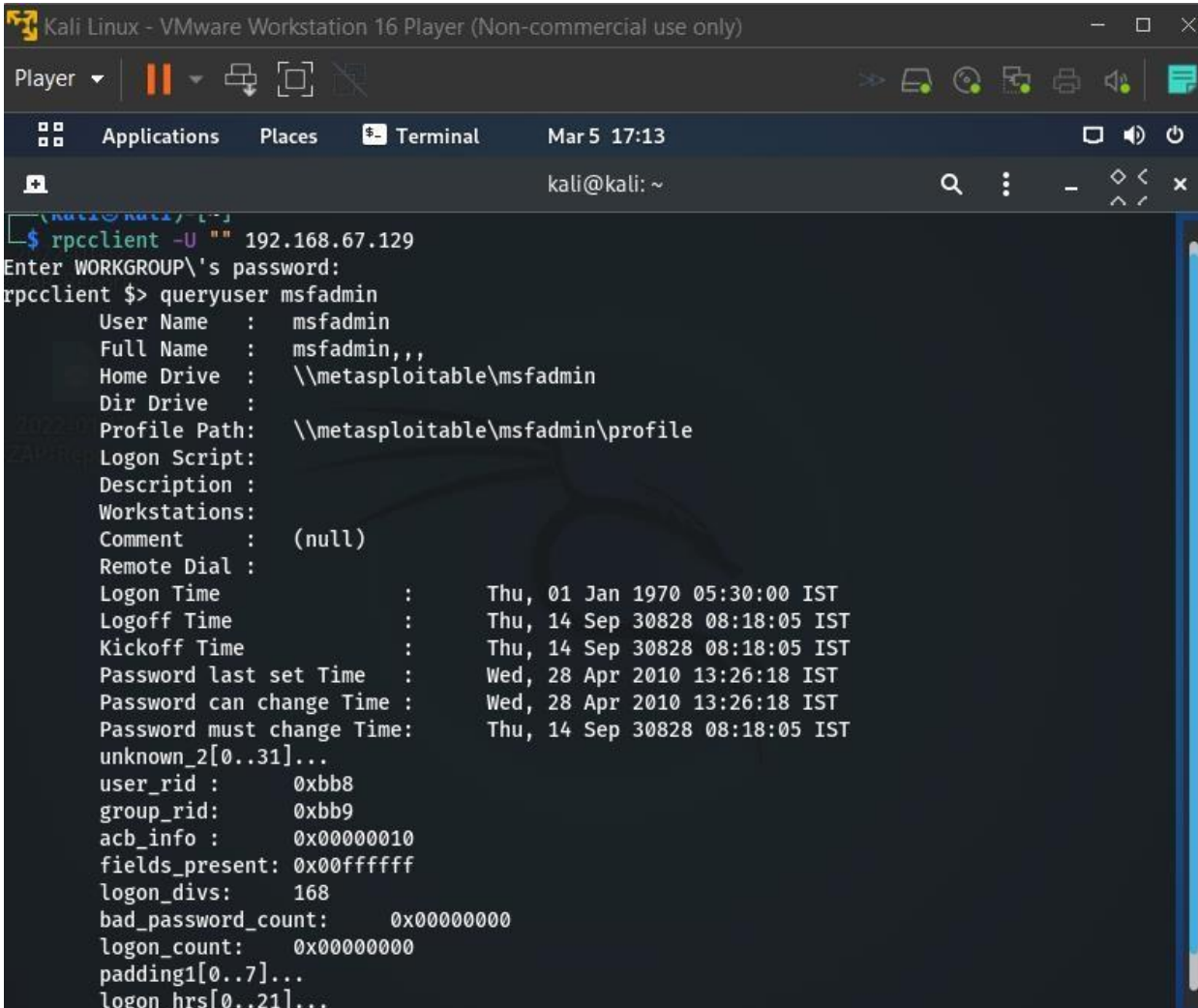


```

(kali@kali)-[~]
$ rpcclient -U "" 192.168.67.129
Enter WORKGROUP's password:
rpcclient $> enumdomusers
user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[svn] rid:[0x3ee]

```

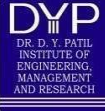

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022



```

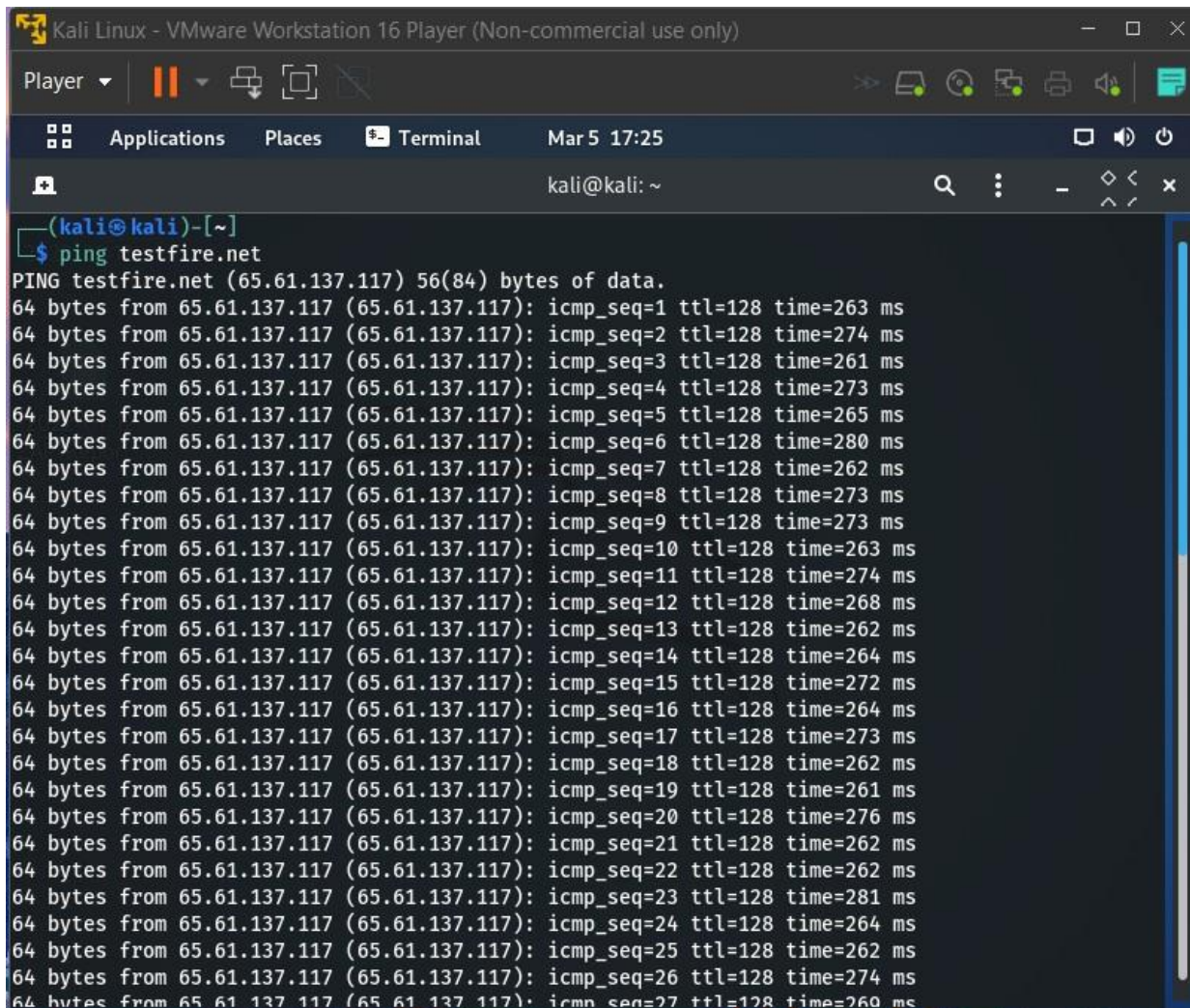
Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminal Mar 5 17:13
kali@kali: ~
kali@kali:~$ rpcclient -U "" 192.168.67.129
Enter WORKGROUP\'s password:
rpcclient $> queryuser msfadmin
User Name      : msfadmin
Full Name      : msfadmin,,,
Home Drive     : \\metasploitable\\msfadmin
Dir Drive      : 
Profile Path    : \\metasploitable\\msfadmin\\profile
Logon Script    : 
Description     : 
Workstations    : 
Comment        : (null)
Remote Dial    : 
Logon Time      : Thu, 01 Jan 1970 05:30:00 IST
Logoff Time     : Thu, 14 Sep 30828 08:18:05 IST
Kickoff Time    : Thu, 14 Sep 30828 08:18:05 IST
Password last set Time : Wed, 28 Apr 2010 13:26:18 IST
Password can change Time : Wed, 28 Apr 2010 13:26:18 IST
Password must change Time: Thu, 14 Sep 30828 08:18:05 IST
unknown_2[0..31]...
user_rid       : 0xbb8
group_rid      : 0xbb9
acb_info       : 0x00000010
fields_present : 0x00ffffff
logon_divs      : 168
bad_password_count: 0x00000000
logon_count     : 0x00000000
padding1[0..7]...
logon_hrs[0..21]...

```


	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Task 4 :- Sniff the data of any application using Wire-Shark


Solution :-



```

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player
Applications Places Terminal Mar 5 17:25
kali@kali: ~
(kali@kali)-[~]
$ ping testfire.net
PING testfire.net (65.61.137.117) 56(84) bytes of data.
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=1 ttl=128 time=263 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=2 ttl=128 time=274 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=3 ttl=128 time=261 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=4 ttl=128 time=273 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=5 ttl=128 time=265 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=6 ttl=128 time=280 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=7 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=8 ttl=128 time=273 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=9 ttl=128 time=273 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=10 ttl=128 time=263 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=11 ttl=128 time=274 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=12 ttl=128 time=268 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=13 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=14 ttl=128 time=264 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=15 ttl=128 time=272 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=16 ttl=128 time=264 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=17 ttl=128 time=273 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=18 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=19 ttl=128 time=261 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=20 ttl=128 time=276 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=21 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=22 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=23 ttl=128 time=281 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=24 ttl=128 time=264 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=25 ttl=128 time=262 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=26 ttl=128 time=274 ms
64 bytes from 65.61.137.117 (65.61.137.117): icmp_seq=27 ttl=128 time=260 ms

```

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player | Applications | Places | wireshark | Mar 5 17:28

*eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr == 65.61.137.117

No.	Time	Source	Destination	Protocol	Length	Info
3189	4.583209067	192.168.67.128	65.61.137.117	TCP	74	48020 → 80 [S
3190	4.810680873	192.168.67.128	65.61.137.117	TCP	74	48022 → 80 [S
3191	4.864838926	65.61.137.117	192.168.67.128	TCP	60	80 → 48020 [S
3192	4.864861612	192.168.67.128	65.61.137.117	TCP	54	48020 → 80 [A
3193	5.098134998	65.61.137.117	192.168.67.128	TCP	60	80 → 48022 [S

▶ Frame 3189: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface eth0, id

▶ Ethernet II, Src: VMware_fe:bc:3d (00:0c:29:fe:bc:3d), Dst: VMware_e7:87:11 (00:50:56:e7:87

▶ Internet Protocol Version 4, Src: 192.168.67.128, Dst: 65.61.137.117


▶ Transmission Control Protocol, Src Port: 48020, Dst Port: 80, Seq: 0, Len: 0

```

0000  00 50 56 e7 87 11 00 0c 29 fe bc 3d 08 00 45 00  .PV....).=.E.
0010  00 3c 11 96 40 00 40 06 5a 4b c0 a8 43 80 41 3d  .<.@.@.ZK.C.A=
0020  89 75 bb 94 00 50 2c 49 8a 98 00 00 00 00 a0 02  .u..P,I .....
0030  fa f0 cf 09 00 00 02 04 05 b4 04 02 08 0a 69 ae  .....i.
0040  bc bc 00 00 00 00 01 03 03 07                .....

```

wireshark_eth0102LI1.pcapng | Packets: 6631 · Displayed: 552 (8.3%) | Profile: Default

 <p>DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT AND RESEARCH</p>	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player ▾ | [Icons] | Applications Places wireshark Mar 5 17:35

Wireshark · Follow TCP Stream (tcp.stream eq 8) · eth0

File Edit

tcp.strea

No. 3189 3191 3192 3207 3208

GET / HTTP/1.1
Host: testfire.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1

HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=5CD0591B48158B07E459EC40B62070A5; Path=/; HttpOnly
Content-Type: text/html; charset=ISO-8859-1
Transfer-Encoding: chunked
Date: Sat, 05 Mar 2022 11:51:54 GMT

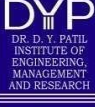
0000 00 2000
0010 00 2 client pkts, 5 server pkts, 3 turns.
0020 43
0030 fa

Entire conversation (16 kB) Show data as ASCII Stream 8

Find: Find Next

Filter Out This Stream Print Save as... Back Close Help

Profile: Default

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player | Applications | Places | wireshark | Mar 5 17:37

Wireshark · Packet 3207 · eth0

File Edit

tcp.stre

No. 3207

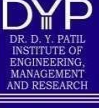
Frame 3207: 377 bytes on wire (3016 bits), 377 bytes captured (3016 b)
 Ethernet II, Src: VMware_fe:bc:3d (00:0c:29:fe:bc:3d), Dst: VMware_e7
 Internet Protocol Version 4, Src: 192.168.67.128, Dst: 65.61.137.117
 Transmission Control Protocol, Src Port: 48020, Dst Port: 80, Seq: 1,
 Hypertext Transfer Protocol

No.	Time	Source	Destination	Protocol	Length	Info
3207	0.000000	192.168.67.128	65.61.137.117	TCP	60	48020 → 80 [ACK] Seq=1

0000 00 50 56 e7 87 11 00 0c 29 fe bc 3d 08 00 45 00 ..PV.....)=
 0010 01 6b 11 98 40 00 40 06 59 1a c0 a8 43 80 41 3d ..k..@..Y..
 0020 89 75 bb 94 00 50 2c 49 8a 99 52 65 64 c7 50 18 ..u...P,I...Re
 0030 fa f0 d0 38 00 00 47 45 54 20 2f 20 48 54 54 50 ...8..GE T /
 0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 74 65 73 74 /1.1..Ho st:
 0050 66 69 72 65 2e 6e 65 74 0d 0a 55 73 65 72 2d 41 fire.net ..Us
 0060 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e gent: Mo zilla
 0070 30 20 28 58 31 31 3b 20 4c 69 6e 75 78 20 78 38 0 (X11; Linu
 0080 36 5f 36 34 3b 20 72 76 3a 39 31 2e 30 29 20 47 6_64; rv :91.

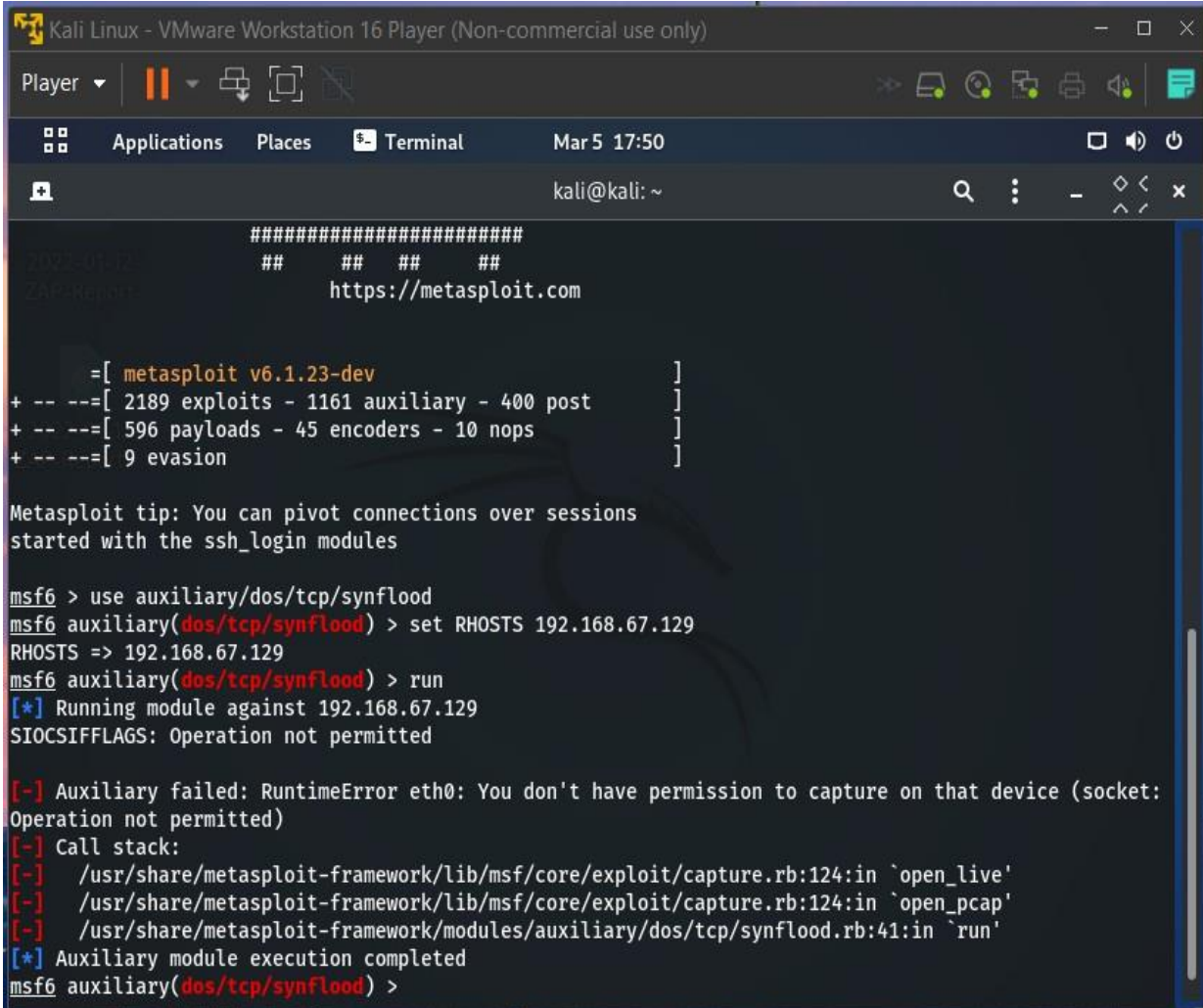
Close Help

wireshark_eth0102LI1.pcapng Packets: 7104 · Displayed: 23 (0.3%) Profile: Default

 <p>DR. D. Y. PATIL INSTITUTE OF ENGINEERING, MANAGEMENT AND RESEARCH</p>	<p align="center">Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune</p>		<p align="center">DI No.: ACAD/DI/72</p>
<p>Academic Year: 2021-22</p>	<p align="center">Weekly Report Format for Internship</p>		<p>Revision : 00 Dated : 20/11/2019</p>
<p align="center">Term – II</p>	<p align="center">Department : Computer Engineering</p>		<p>Date of Preparation : 3/01/2022</p>

Task 5 :- Perform DOS Attack using Metasploit framework

Solution :-



```

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)
Player | [Icons] | Mar 5 17:50
kali@kali: ~
#####
##  ##  ##  ##
https://metasploit.com

2022-01-12
ZAP-Report

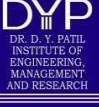
=[ metasploit v6.1.23-dev ]
+ -- ==[ 2189 exploits - 1161 auxiliary - 400 post ]
+ -- ==[ 596 payloads - 45 encoders - 10 nops ]
+ -- ==[ 9 evasion ]

Metasploit tip: You can pivot connections over sessions
started with the ssh_login modules

msf6 > use auxiliary/dos/tcp/synflood
msf6 auxiliary(dos/tcp/synflood) > set RHOSTS 192.168.67.129
RHOSTS => 192.168.67.129
msf6 auxiliary(dos/tcp/synflood) > run
[*] Running module against 192.168.67.129
SIOCSIFFLAGS: Operation not permitted

[-] Auxiliary failed: RuntimeError eth0: You don't have permission to capture on that device (socket:
Operation not permitted)
[-] Call stack:
[-] /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `open_live'
[-] /usr/share/metasploit-framework/lib/msf/core/exploit/capture.rb:124:in `open_pcap'
[-] /usr/share/metasploit-framework/modules/auxiliary/dos/tcp/synflood.rb:41:in `run'
[*] Auxiliary module execution completed
msf6 auxiliary(dos/tcp/synflood) >

```

	Dr D Y Patil Pratishthan's Dr. D.Y. Patil Institute of Engineering, Management and Research, Akurdi, Pune		DI No.: ACAD/DI/72
Academic Year: 2021-22	Weekly Report Format for Internship		Revision : 00 Dated : 20/11/2019
Term – II	Department : Computer Engineering		Date of Preparation : 3/01/2022

Kali Linux - VMware Workstation 16 Player (Non-commercial use only)

Player | Applications | Places | wireshark | Mar 5 17:52

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	192.168.67.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
2	1.004781355	192.168.67.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
3	2.005832057	192.168.67.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1
4	3.009387509	192.168.67.1	239.255.255.250	SSDP	215	M-SEARCH * HTTP/1.1

Frame 1: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits) on interface eth0, in packet 1
 Ethernet II, Src: VMware_c0:00:08 (00:50:56:c0:00:08), Dst: IPv4mcast_7f:ff:fa (01:00:5e:7f:ff:fa)
 Internet Protocol Version 4, Src: 192.168.67.1, Dst: 239.255.255.250
 User Datagram Protocol, Src Port: 54004, Dst Port: 1900
 Simple Service Discovery Protocol

```

0000  01 00 5e 7f ff fa 00 50 56 c0 00 08 08 00 45 00  ..^...P.V....E.
0010  00 c9 be c1 00 00 01 11 06 bf c0 a8 43 01 ef ff  .....C...
0020  ff fa d2 f4 07 6c 00 b5 f0 33 4d 2d 53 45 41 52  ....l...3M-SEAR
0030  43 48 20 2a 20 48 54 54 50 2f 31 2e 31 0d 0a 48  CH * HTTP/1.1..H
0040  4f 53 54 3a 20 32 33 39 2e 32 35 35 2e 32 35 35  OST: 239 .255.255
0050  2e 32 35 30 3a 31 39 30 30 0d 0a 4d 41 4e 3a 20  .250:190 0..MAN:
0060  22 73 73 64 70 3a 64 69 73 63 6f 76 65 72 22 0d  "ssdp:discover".
  
```

eth0: <live capture in progress> Packets: 4 · Displayed: 4 (100.0%) Profile: Default