Experiment 7: DOS Attack

<u>Aim:</u> Write the implementation of DOS attack

Theory:

A denial-of-service (DoS) attack is a type of cyber attack in which a malicious actor aims to render a computer or other device unavailable to its intended users by interrupting the device's normal functioning. DoS attacks typically function by overwhelming or flooding a targeted machine with requests until normal traffic is unable to be processed, resulting in denial-of-service to addition users. A DoS attack is characterized by using a single computer to launch the attack.

A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.

The primary focus of a DoS attack is to oversaturate the capacity of a targeted machine, resulting in denial-of-service to additional requests. The multiple attack vectors of DoS attacks can be grouped by their similarities.

An attack type in which a memory buffer overflow can cause a machine to consume all available hard disk space, memory, or CPU time. This form of exploit often results in sluggish behavior, system crashes, or other deleterious server behaviors, resulting in denial-of-service.

A few common historic DoS attacks include:

- Smurf attack a previously exploited DoS attack in which a malicious actor
 utilizes the broadcast address of vulnerable network by sending spoofed packets,
 resulting in the flooding of a targeted IP address.
- Ping flood this simple denial-of-service attack is based on overwhelming a target with ICMP (ping) packets. By inundating a target with more pings than it is able to respond to efficiently, denial-of-service can occur. This attack can also be used as a DDoS attack.
- Ping of Death often conflated with a ping flood attack, a ping of death attack involves sending a malformed packet to a targeted machine, resulting in deleterious behavior such as system crashes.

How can you tell if a computer is experiencing a DoS attack?

While it can be difficult to separate an attack from other network connectivity errors or heavy bandwidth consumption, some characteristics may indicate an attack is underway.

Indicators of a DoS attack include:

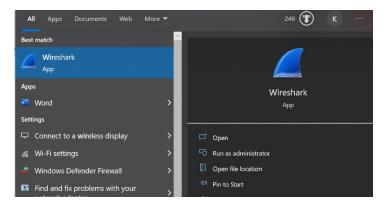
- Atypically slow network performance such as long load times for files or websites
- The inability to load a particular website such as your web property
- A sudden loss of connectivity across devices on the same network

The distinguishing difference between DDoS and DoS is the number of connections utilized in the attack. Some DoS attacks, such as "low and slow" attacks like Slowloris, derive their power in the simplicity and minimal requirements needed to them be effective.

DoS utilizes a single connection, while a DDoS attack utilizes many sources of attack traffic, often in the form of a botnet. Generally speaking, many of the attacks are fundamentally similar and can be attempted using one more many sources of malicious traffic. Learn how Cloudflare's DDoS protection stops denial-of-service attacks.

Implementation:

Step 1



Step 2

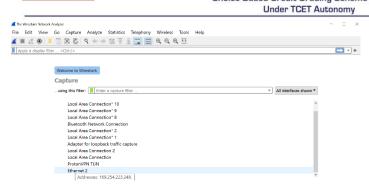


TCET DEPARTMENT OF COMPUTER ENGINEERING (COMP)

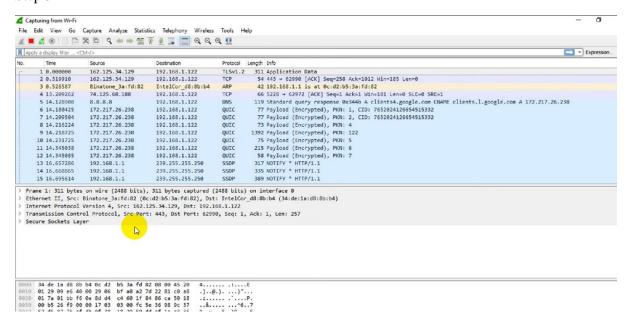
[Accredited by NBA for 3 years, 4th Cycle Accreditation w.e.f. 1st July 2022]



Choice Based Credit Grading Scheme (CBCGS)



Step 3



Step 4

				(22) (1)	
Time		Source	Destination		Length Info
	3.098145	192.168.1.120	224.0.0.251	MDNS	3 Standard query 0x0021 PTR _D2CA5178subgooglecasttcp.local, "QM" question PTR _googlecasttcp.local, "QM
185 134	4.508114	8.8.8.8	192.168.1.122	DNS	128 Standard query response 0xfc7d A cem.twimg.com CNAME wildcard.twimg.com A 104.244.46.167 A 104.244.46.71
186 134	4.521865	52.230.80.159	192.168.1.122	TLSv1.2	179 Application Data
187 134	4.643393	104.244.46.167	192.168.1.122	TCP	66 443 + 63238 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1440 SACK_PERM=1 WS=512
188 134	4.781763	104.244.46.167	192.168.1.122	TLSv1.2	1494 Server Hello
189 134	4.781823	104.244.46.167	192.168.1.122	TCP	1494 443 → 63238 [ACK] Seq=1441 Ack=179 Win=30720 Len=1440 [TCP segment of a reassembled PDU]
190 134	4.781952	104.244.46.167	192.168.1.122	TLSv1.2	1201 Certificate, Certificate Status, Server Key Exchange, Server Hello Done
191 134	4.939150	104.244.46.167	192.168.1.122	TLSv1.2	296 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
192 135	5.064189	104.244.46.167	192.168.1.122	TCP	1494 443 + 63238 [ACK] Seq=4270 Ack=456 Win=31744 Len=1440 [TCP segment of a reassembled PDU]
193 135	5.064245	104.244.46.167	192.168.1.122	TLSv1.2	1222 Application Data
194 137	7.800087	74.125.24.125	192.168.1.122	TCP	54 5222 + 62944 [ACK] Seq=54 Ack=213 Win=218 Len=0
195 138	8.538098	162.125.34.129	192.168.1.122	TLSv1.2	311 Application Data
196 138	8.850729	162.125.34.129	192.168.1.122	TCP	54 443 + 62990 [ACK] Seq=772 Ack=3034 Win=229 Len=0
197 139	9.156102	162.125.34.129	192.168.1.122	TCP	66 [TCP Dup ACK 196#1] 443 → 62990 [ACK] Seq=772 Ack=3034 Win=229 Len=0 SLE=2023 SRE=3034
Ethernet > Destin	II, Src: B		de:1a:d8:8b:b4)		s) on interface 0 d8:8b:b4 (34:de:la:d8:8b:b4)
Type:	IPv4 (0x08		168 1 1 Det: 239 255	255 250	
Type: Internet	IPv4 (0x080 Protocol V		168.1.1, Dst: 239.255	.255.250	

- 0000 34 de la d8 8b b4 ec d2 b5 3a fd 82 08 00 45 00 4......E.
 0010 01 6b 04 d3 00 00 04 11 ff 0b c0 a8 01 01 ef ff .k....

Step 5

```
roctmali:-# hping3 -S --flood -V www.xyz.com
using eth0, addr: 192.168.12.129, MTU: 1500
HPING www.xyz.com (eth0 184.169.138.0): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

Conclusion:

For Faculty Use:

Correction Parameters	Formative Assessment [40%]	Timely completion of Practical [40%]	Attendance/ Learning Attitude [20%]				
Marks Obtained							