Semester	T.E. Semester VI – Computer Engineering
Subject	Cryptography and cyber security
Subject Professor In-charge	Prof. Amit Nerurkar
Assisting Teachers	Prof. Amit Nerurkar
Laboratory	M312B

Student Name	Deep Salunkhe
Roll Number	21102A0014
TE Division	A

Title:

Design and Implementation of DOS using Hping 3

Explanation:

1. **Denial of Service (DoS) Attack**:
    - In a DoS attack, a single source is used to flood a target with a large volume of traffic, thus consuming all available resources and making the service unavailable to legitimate users.
    - This attack can be launched using various methods, including sending a flood of TCP SYN packets, UDP packets, or ICMP (ping) requests to the target.
2. **Distributed Denial of Service (DDoS) Attack**:
    - DDoS attacks are more sophisticated and potent than DoS attacks as they involve multiple sources, often distributed across the internet, coordinated to flood the target simultaneously.
    - DDoS attacks typically leverage botnets, which are networks of compromised computers (often referred to as zombies) that can be remotely controlled by an attacker. These botnets are used to amplify the attack and make it more difficult to mitigate.
3. **Using hping3 for DoS/DDoS Attacks**:
    - hping3 is a command-line tool used for network testing and manipulation. It can be abused by attackers to launch DoS or DDoS attacks by sending crafted packets to a target.
    - hping3 can be used to send various types of packets, including TCP SYN, UDP, and ICMP packets, with custom payloads and rates.
    - Attackers can use hping3 to flood a target with packets, overwhelming its network bandwidth, exhausting its resources (such as CPU or memory), or exploiting vulnerabilities in the target's network stack.
    - hping3 can also be used to perform more sophisticated attacks, such as TCP SYN flooding, UDP flooding, ICMP flooding, and TCP ACK flooding.

4. **Mitigation and Prevention**:

   - Defending against DoS and DDoS attacks requires a combination of proactive measures and reactive strategies.
   - Proactive measures include implementing network security best practices, such as firewalls, intrusion detection/prevention systems (IDS/IPS), rate limiting, and filtering out malicious traffic.
   - Reactive strategies involve detecting and mitigating attacks in real-time using specialized DDoS mitigation appliances or cloud-based DDoS protection services.
   - Additionally, organizations should have incident response plans in place to quickly respond to and recover from DoS/DDoS attacks, including identifying the source of the attack and working with law enforcement if necessary.

Implementation:

DoS attack with hping3

dos.md Raw

DoS Attack with Hping3

Run the command: `hping3 --flood -S -V --rand-source http://stv.com`

Where:

1. `--flood` send packets as fast as possible
2. `-S` (Syn packet): legit TCP packet connection
3. `-V` verbose mode
4. `--rand-source` randomize the IP source address, like it's requested from different systems (sort of DDoS)

clhore commented on Feb 1, 2022

In this case the '-V' parameter is not really necessary since adding the '--flood' parameter disables it.

```
hping3: hping in flood mode, no replies will be shown
```

You can add the parameter '-d' or '--data' to be able to modify the weight of the sent data.
And if you wanted to use a single fake IP instead of multiple ones, you could use '-a' or '--spoof'.

Ej:

```
sudo hping3 --flood -S -d 2000 -a <fake_ip> <target_ip>
```

```
root@kali:~# ping -c 3 10.0.0.37
PING 10.0.0.37 (10.0.0.37) 56(84) bytes of data.
64 bytes from 10.0.0.37: icmp_seq=1 ttl=64 time=0.372 ms
64 bytes from 10.0.0.37: icmp_seq=2 ttl=64 time=0.236 ms
64 bytes from 10.0.0.37: icmp_seq=3 ttl=64 time=0.218 ms

--- 10.0.0.37 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 0.218/0.275/0.372/0.070 ms
root@kali:~#
```

```
root@kali:~# hping3 -S --flood --interface wlan0 --rand-source 10.0.0.37
```

```
root@kali:~# hping3 -S --flood --interface wlan0 --rand-source 10.0.0.37
HPING 10.0.0.37 (wlan0 10.0.0.37): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

246.99.62.66	10.0.0.37	TCP	54	1825→0 [SYN] Seq=0 Win=512 Len=0
152.246.145.17	10.0.0.37	TCP	54	1826→0 [SYN] Seq=0 Win=512 Len=0
17.160.192.51	10.0.0.37	TCP	54	1827→0 [SYN] Seq=0 Win=512 Len=0
217.195.51.84	10.0.0.37	TCP	54	1828→0 [SYN] Seq=0 Win=512 Len=0
1.86.43.188	10.0.0.37	TCP	54	1829→0 [SYN] Seq=0 Win=512 Len=0

Conclusion:

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are serious threats that disrupt online services by overwhelming their resources with malicious traffic. DoS attacks originate from a single source, while DDoS attacks involve multiple distributed sources, making them more potent and difficult to mitigate. Tools like hping3 can be misused by attackers to execute these attacks, although such actions are illegal and unethical. To defend against DoS and DDoS attacks, organizations should implement proactive measures like firewalls, intrusion detection/prevention systems, and rate limiting. Reactive strategies, such as real-time attack detection and mitigation, are also essential for minimizing the impact of attacks. Collaboration between network administrators, security professionals, and law enforcement agencies is crucial for identifying and prosecuting malicious actors. Ultimately, building resilient and secure networks is vital for safeguarding against the disruptive effects of DoS and DDoS attacks.