|  |  |
| --- | --- |
| 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:**

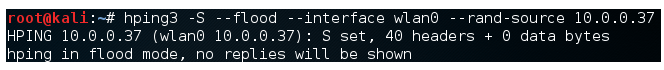
**A screenshot of a computer

Description automatically generated**

**A screenshot of a computer

Description automatically generated**

****

****

**A close-up of a grey background

Description automatically generated**

**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.