**TNE30024**

Deploying Secure Engineering Applications Online

**Tutorial 7 (week 10)**

**Distributed Denial of Service Attacks**

**Questions**

1. What is the difference between a direct attack and a reflector (or indirect) attack?
2. A)What is the following attack? Which host is attacking and which is being attacked?



|  |  |
| --- | --- |
| SADDR 192.103.5.3,SYN 2000  SADDR 192.103.5.5,SYN 2000  SADDR 192.103.5.7,SYN 2000 | SADDR 200.106.34.20,ACK 2001, SYN 3400  SADDR 200.106.34.20,ACK 2001, SYN 3400  SADDR 200.106.34.20,ACK 2001, SYN 3400 |

1. B) Is this a direct or reflector attack?

1. Draw a diagram showing how a TCP sequence number attack can be mounted as a reflector attack.

1. **Difference between a direct attack and a reflector (or indirect) attack**:

* **Direct Attack**: In a direct DDoS attack, the attacker directly sends malicious traffic to the target system (victim). The attacker's IP addresses are used to generate the requests, and these requests overwhelm the victim's resources, causing denial of service.
* **Reflector (or Indirect) Attack**: In a reflector attack, the attacker sends packets to third-party servers (reflectors) with the source IP address spoofed to appear as the target's IP. These third-party servers respond to the spoofed requests, unknowingly sending traffic to the target system, thus overwhelming it. The attacker remains anonymous in this case, as the actual traffic appears to come from the reflectors.

1. **A) What is the attack shown in the image? Which host is attacking and which is being attacked?**

* **Attack Shown**: The attack shown in the image is a SYN flood, which is a type of Denial-of-Service (DoS) attack. Multiple hosts with different IP addresses (192.103.5.3, 192.103.5.5, 192.103.5.7) are sending SYN requests to the target server (200.106.34.20) using port 2000.
  + The source IPs (192.103.x.x) are initiating TCP connection requests (SYN packets) with the target, overloading it.
* **Attacker**: The hosts with IP addresses **192.103.5.3, 192.103.5.5, and 192.103.5.7** are performing the attack.
* **Victim (being attacked)**: The host with IP **200.106.34.20** is being attacked.

1. **B) Is this a direct or reflector attack?**

* This is a **direct attack** because the attackers (with IP addresses 192.103.5.x) are directly sending SYN packets to the victim's IP (200.106.34.20).

1. **Diagram for a TCP sequence number attack mounted as a reflector attack**:

A TCP sequence number attack involves guessing the sequence numbers used in TCP packets to hijack an ongoing session. In a reflector attack, the attacker sends spoofed SYN packets to a third-party server, using the victim's IP as the source. The third-party server then sends SYN-ACK packets to the victim, who is overwhelmed by the traffic.

Here's how you can draw it:

1. **Step 1**: Attacker sends spoofed SYN packets to various reflectors (servers), using the victim's IP address as the source.
   * Reflector A ← SYN (Spoofed source: Victim IP)
   * Reflector B ← SYN (Spoofed source: Victim IP)
   * Reflector C ← SYN (Spoofed source: Victim IP)
2. **Step 2**: Each reflector responds with a SYN-ACK packet, thinking the victim is initiating the connection.
   * Reflector A → SYN-ACK → Victim
   * Reflector B → SYN-ACK → Victim
   * Reflector C → SYN-ACK → Victim
3. **Step 3**: The victim is overwhelmed by the incoming SYN-ACK responses from multiple reflectors, exhausting its resources and leading to a Denial of Service.