PD
PENTEST DIARIES

PD
PENTEST DIARIES
HTTPS://WWW.SAKSHAMDIXIT.COM

KNOWLEDGE SHARE

PENTEST DIARIES

@pentestdiaries

4 Famous DoS method for Pentesting:

When pentesting servers, understanding various Denial of Service (DoS) methods is crucial for identifying vulnerabilities and assessing the resilience of the infrastructure. Here are four famous DoS methods commonly used in penetration testing:

Here are 4 famous DoS (Denial-of-Service) methods commonly used for pentesting servers:

1. UDP Flood:

- **Description: This method overwhelms the target server with a large volume of User Datagram Protocol (UDP) packets. UDP is a connectionless protocol, meaning the sender doesn't wait for confirmation from the receiver, making it efficient for flooding.**
- **Impact: The server's resources are consumed processing these packets, causing legitimate traffic to be dropped and the service to become unavailable.**
- **Tools: Tools like `hping3` or custom scripts can be used to generate UDP floods.**

2. SYN Flood:

- **Description: This method exploits the three-way handshake process in TCP connections. The attacker sends a large number of SYN (synchronization) packets, initiating connection requests but never completing the handshake. This leaves the server waiting for completion, consuming resources and preventing legitimate connections.**
- **Impact: Similar to a UDP flood, the server becomes overloaded with incomplete connection requests, rendering it unavailable to legitimate users.**
- **Tools: Tools like `slowloris` or custom scripts can be used to launch SYN floods.**

3. ICMP Flood (Ping Flood):

- **Description:** This method bombards the target server with ICMP (Internet Control Message Protocol) echo request packets (pings). While seemingly simple, a large volume of pings can overwhelm the server's resources.
- **Impact:** The server prioritizes responding to pings, neglecting other essential tasks and potentially becoming unresponsive to legitimate traffic.
- **Tools:** The `ping` command itself or tools like `hping3` can be used for ICMP floods.

4. HTTP Flood:

- **Description**: This method involves sending a large number of HTTP requests to the target server, like GET or POST requests. These requests can target specific pages or exploit vulnerabilities in the web server to maximize impact.
- **Impact:** The server becomes overloaded processing these requests, leading to slowdowns or crashes, preventing legitimate users from accessing the service.
- **Tools:** Tools like `ab` (ApacheBench) or custom scripts can be used to automate HTTP floods.

Important Note:

It's crucial to only perform DoS attacks with explicit permission on authorized systems during penetration testing. DoS attacks can disrupt legitimate operations and cause harm. Always act ethically and responsibly when pentesting.

These are just a few examples, and there are many other DoS methods available. Understanding these techniques can help penetration testers identify vulnerabilities in systems and recommend appropriate mitigation strategies.