

Web Attacks

Tools in Kali Linux

Module #33

Denial of Service (DoS) / Distributed DoS

Penetration Testing exercise is focused on identifying the gaps in security rather than harming a system.

This is a key feature that separates a real attacker from an authorized Penetration Tester. Real hackers don't follow the rules and are not concerned about interrupting business if it can improve their situation.

In some cases, a hacker is looking to create any form of negative impact on a target, including taking down critical systems. For this reason, it makes sense in some cases to test systems for the risk of Denial of Service (DoS) type attacks.

Denial of Service (DoS) / Distributed DoS

The most common DoS attack involves flooding a target with external communication requests.

This overload prevents the resource from responding to legitimate traffic, or slows its response so significantly that it is rendered unavailable. DoS attacks can target system resources (disk space, bandwidth, and so on), configuration information (remove route tables), state information (TCP session resetting), or anything that can harm system operation.

Denial of Service (DoS) / Distributed DoS

There are four major DoS/DDoS attack categories:

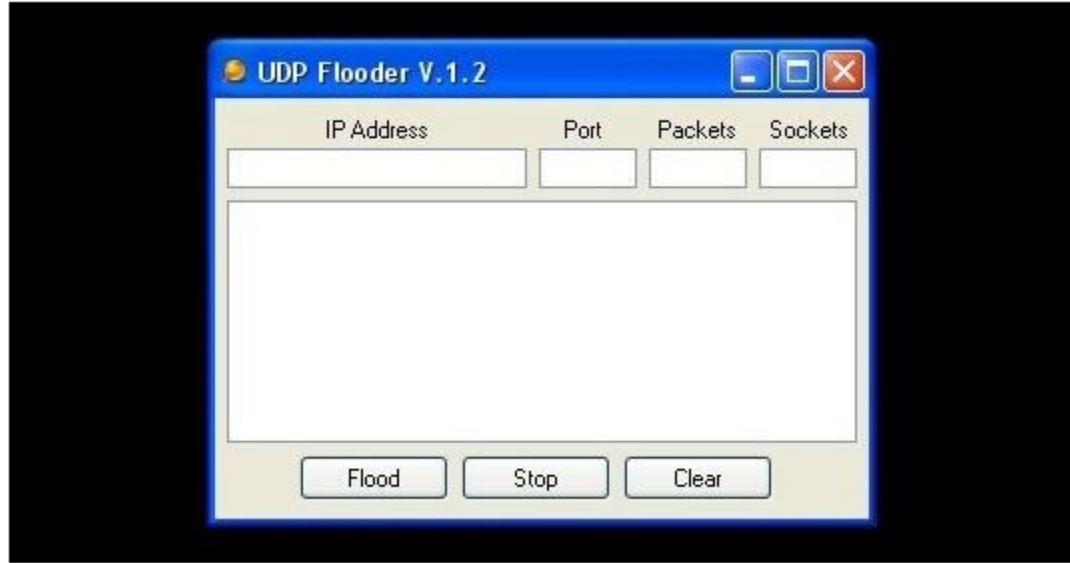
- **Volume Based Attacks:** It involves UDP floods, ICMP floods, and other spoofed packet-based floods. The purpose is to saturate the bandwidth of the victim website.
- **Protocol Attacks:** It consumes resources of servers or intermediate communication equipment, such as routers, firewalls, load balancers, and so on. Example: SYN flood.
- **Application Layer Attacks:** It leverages legitimate traffic to crash a web service. The examples include vulnerability exploitation.
- **Session Exhaustion:** Abusing session limitations by repeatedly establishing but not closing new sessions with the goal of consuming resources.

Denial of Service (DoS) / DDoS in Kali Linux

```
root@kali:/usr/share/metasploit-framework/modules/auxiliary/dos#  
cisco freebsd http misc pptp sap smtp ssl tcp windows  
dhcp hp mdns ntp samba scada solaris syslog upnp wireshark
```

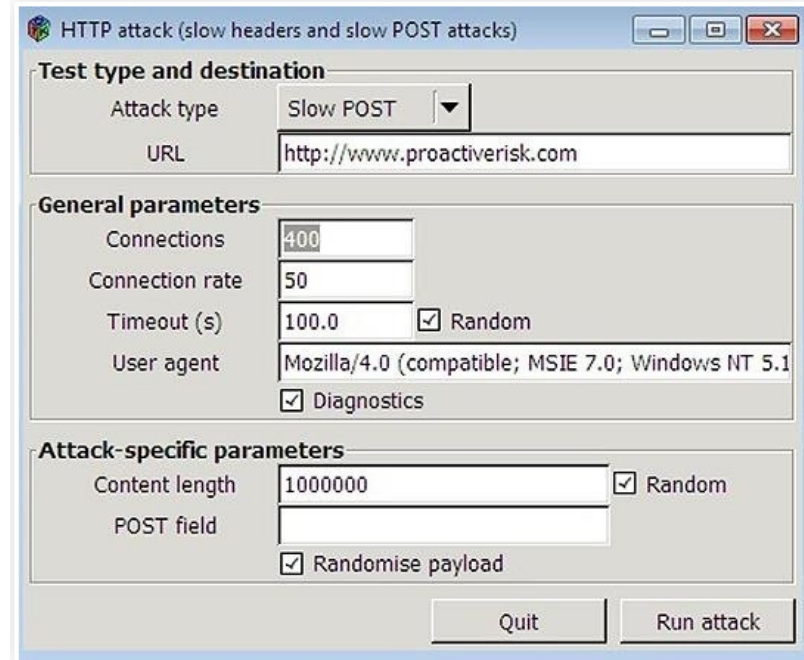
Important DoS tools: UDP Flooder

UDP Flooder does just as you would expect—it sends a flood of UDP packets to the target. It has been effectively used to knock gamers off their networks (online games primarily use UDP). You can download it at [SourceForge](#).



Important DoS tools: RUDY

R-U-Dead-Yet, or RUDY, takes a different approach to DoS-ing websites. It enables the user to select a form from the web app and then use that form to send a flood of POST requests. You can download it from Hybrid Security.



The screenshot shows the RUDY HTTP attack tool interface. It is titled "HTTP attack (slow headers and slow POST attacks)". The interface is divided into three main sections: "Test type and destination", "General parameters", and "Attack-specific parameters".

Test type and destination:

- Attack type: Slow POST (selected from a dropdown menu)
- URL: <http://www.proactiverisk.com>

General parameters:

- Connections: 400
- Connection rate: 50
- Timeout (s): 100.0 ☒ Random
- User agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1) ☒ Diagnostics

Attack-specific parameters:

- Content length: 1000000 ☒ Random
- POST field: (empty text box) ☒ Randomise payload

At the bottom right, there are two buttons: "Quit" and "Run attack".

Important DoS tools: Pyloris

Pyloris is another DoS tool, but with still a different strategy.

It allows the user to construct their own, unique HTTP request headers. It then attempts to keep open these TCP connections as long as possible in order to exhaust the connection queue.

When it does this, no legitimate connections can be made and new attempts to connect by other users will be dropped.

You can download it on SourceForge.

Thank You