

MIT WORLD PEACE UNIVERSITY

Vulnerability Identification and Penetration Testing  
Third Year B. Tech, Semester 6

---

---

EXPLORING TOOLS FOR VULNERABILITY  
IDENTIFICATION AND PENETRATION TESTING

---

---

THEORY ASSIGNMENT 1

Prepared By

Krishnaraj Thadesar  
Cyber Security and Forensics  
Batch A1, PA 10

January 28, 2024

## Contents

## 1 Exploring Tool 1 - Hping (hping3)

### 1.1 Purpose of Tool

hping3 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies. It handles fragmentation and arbitrary packet body and size, and can be used to transfer files under supported protocols. Using hping3, you can test firewall rules, perform (spoofed) port scanning, test network performance using different protocols, do path MTU discovery, perform traceroute-like actions under different protocols, fingerprint remote operating systems, audit TCP/IP stacks, etc. hping3 is scriptable using the Tcl language.

### 1.2 Command 1 - Scanning

#### Syntax

```
$ sudo hping3 --scan ports -S target_ip
```

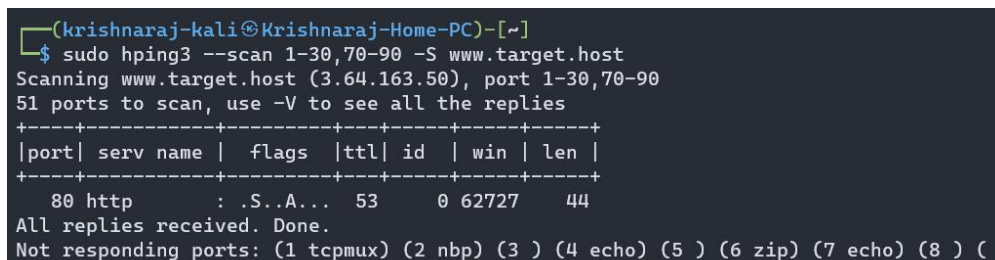
#### Command

```
$sudo hping3 --scan 1-30,70-90 -S www.target.host
```

#### Purpose

To scan for open ports on the target machine.

#### Output

A terminal window showing the execution of the hping3 scan command. The prompt is (krishnaraj-kali@Krishnaraj-Home-PC)-[~]. The command is \$ sudo hping3 --scan 1-30,70-90 -S www.target.host. The output shows the scanning process, including the target IP (3.64.163.50) and the port range (1-30,70-90). It indicates 51 ports to scan and shows a table of results for port 80 (http) which is open. The table has columns for port, serv name, flags, ttl, id, win, and len. The output for port 80 shows flags .S..A... and a len of 44. It also shows the number of replies received and a list of non-responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8 ) (9 ).

```
(krishnaraj-kali@Krishnaraj-Home-PC)-[~]
$ sudo hping3 --scan 1-30,70-90 -S www.target.host
Scanning www.target.host (3.64.163.50), port 1-30,70-90
51 ports to scan, use -V to see all the replies
+---+-----+-----+-----+-----+-----+
|port| serv name | flags  |ttl| id  | win | len |
+---+-----+-----+-----+-----+-----+
80 http      : .S..A... 53   0 62727 44
All replies received. Done.
Not responding ports: (1 tcpmux) (2 nbp) (3 ) (4 echo) (5 ) (6 zip) (7 echo) (8 ) (9 )
```

Figure 1: To scan open ports

### 1.3 Command 2 - Traceroute

#### Syntax

```
$ sudo hping3 --traceroute target_ip
```

#### Command

```
$sudo hping3 --traceroute krishnarajt.surge.sh
```

#### Purpose

To trace the route to the target machine.

## Output

```
(krishnaraj-kali@Krishnaraj-Home-PC)~$ sudo hping3 --traceroute krishnarajt.surge.sh
HPING krishnarajt.surge.sh (eth0 139.59.50.135): NO FLAGS are set, 40 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=172.25.144.1 name=Krishnaraj-Home-PC
hop=1 hoprtt=20.0 ms
hop=2 TTL 0 during transit from ip=192.168.1.1 name=UNKNOWN
hop=2 hoprtt=19.7 ms
^C
--- krishnarajt.surge.sh hping statistic ---
83 packets transmitted, 4 packets received, 96% packet loss
round-trip min/avg/max = 19.7/19.8/20.0 ms
```

Figure 2: To trace the route to the target machine

## 1.4 Command 3 - Flood

### Syntax

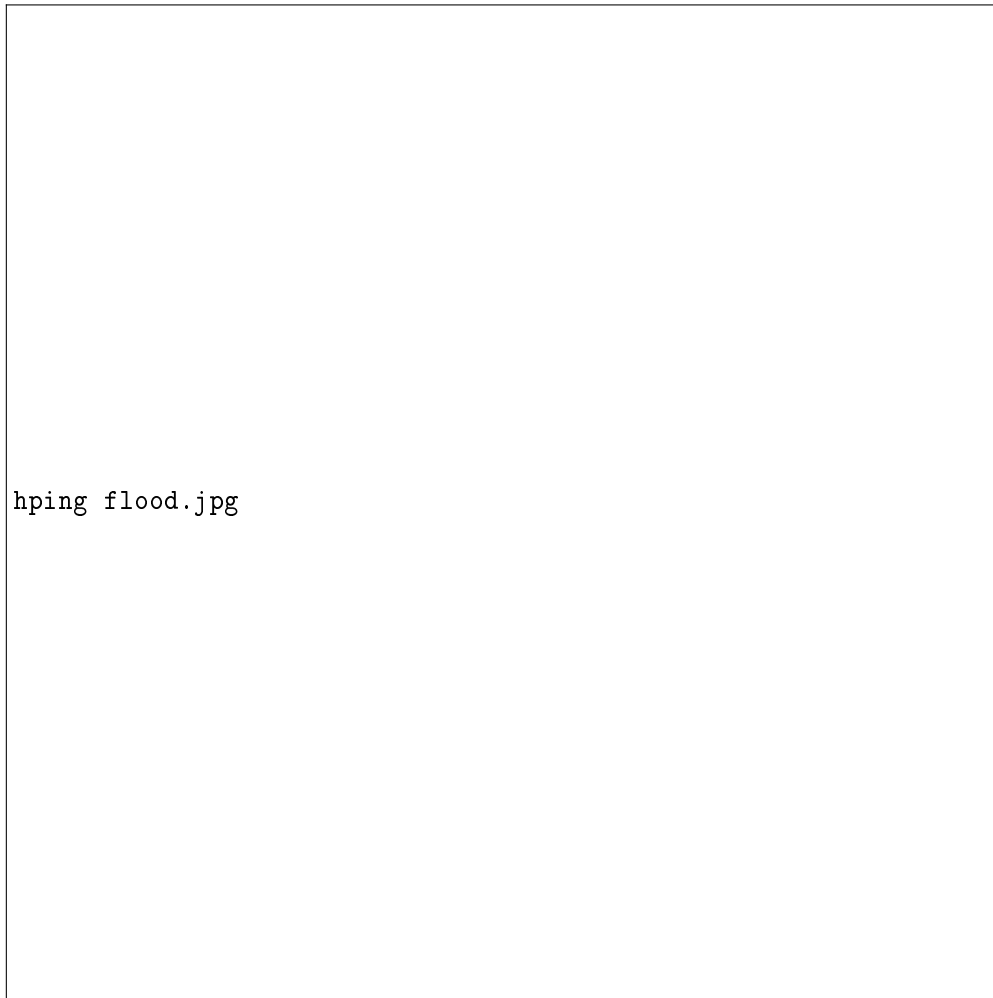
```
$ sudo hping3 --flood target_ip
```

### Command

```
$sudo hping3 --flood krishnarajt.surge.sh
```

### Purpose

To flood the target machine with packets.

**Output**

hping flood.jpg

Figure 3: To flood the target machine with packets

**1.5 Command 4 - Ping****Syntax**

```
$ sudo hping3 --icmp target_ip
```

**Command**

```
$sudo hping3 --icmp krishnarajt.surge.sh
```

**Purpose**

To ping the target machine.

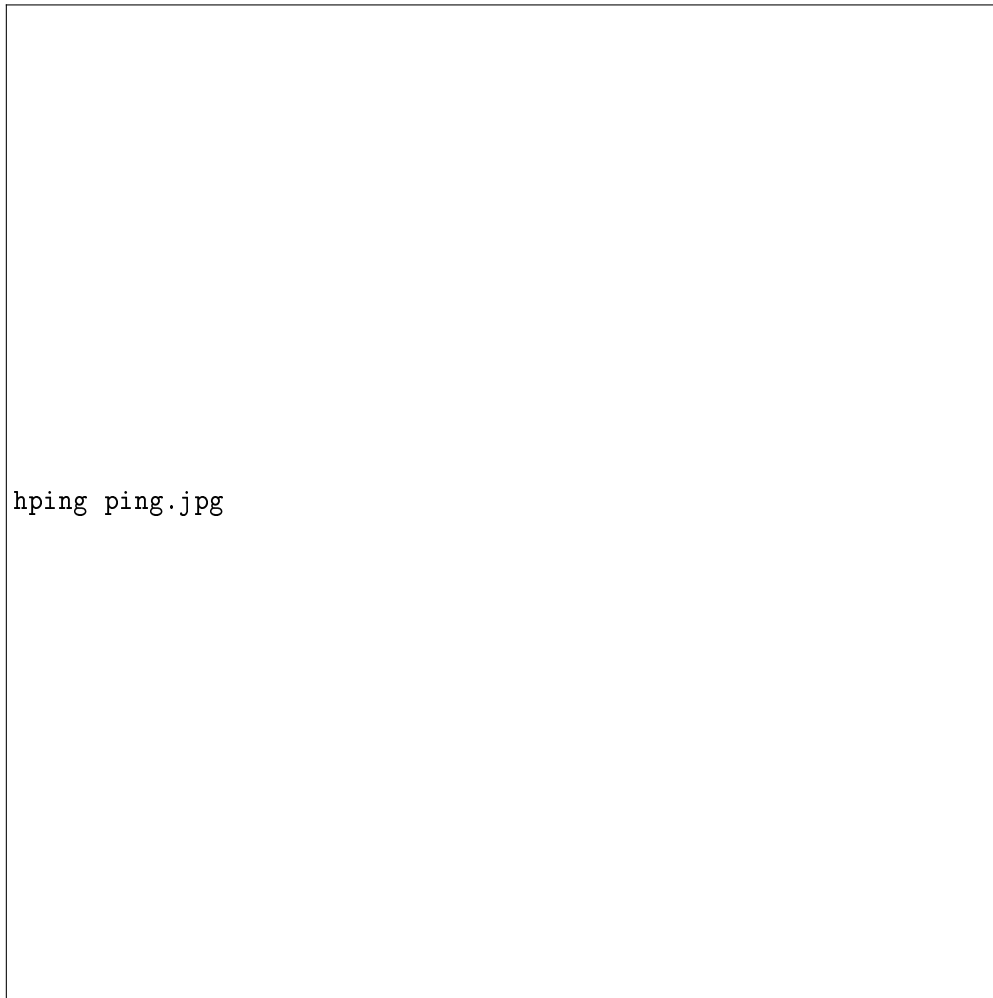
**Output**

Figure 4: To ping the target machine

**1.6 Command 5 - Syn Flood****Syntax**

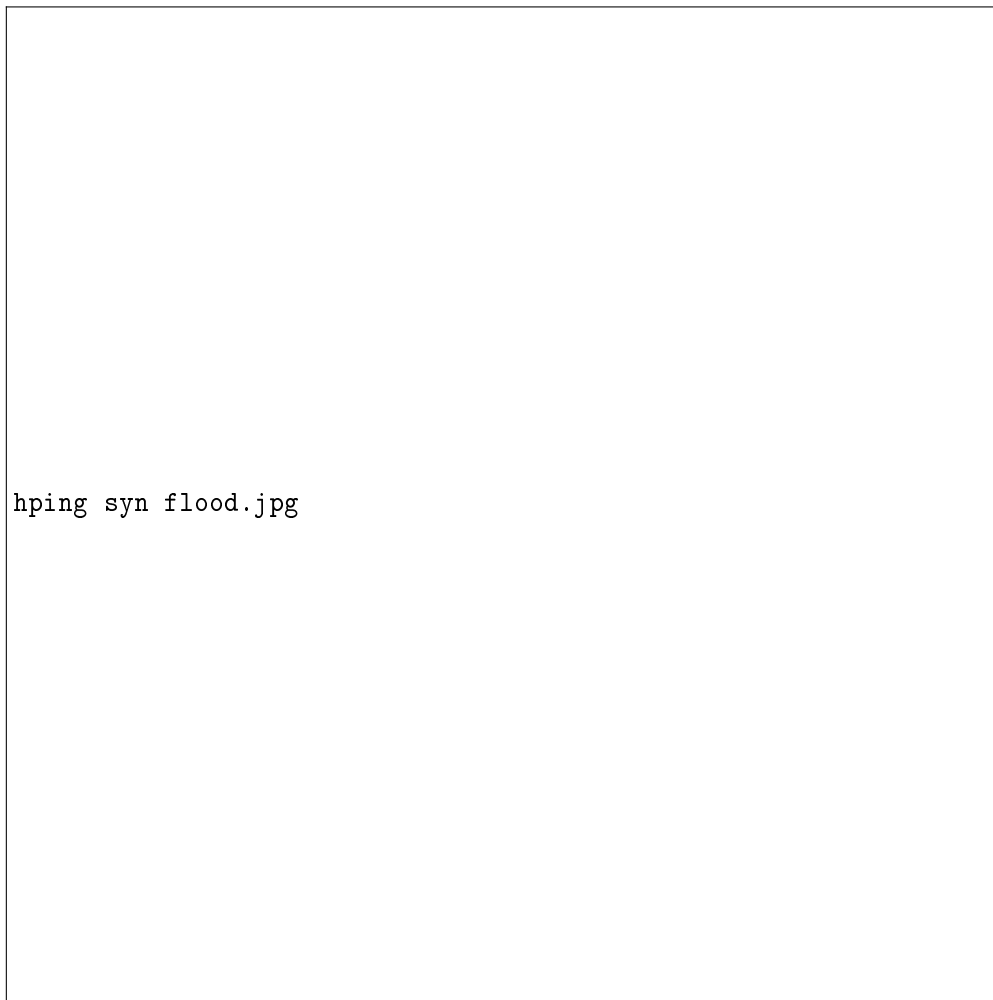
```
$ sudo hping3 --flood --rand-source -S target_ip
```

**Command**

```
$sudo hping3 --flood --rand-source -S krishnarajt.surge.sh
```

**Purpose**

To flood the target machine with SYN packets.

**Output**

hping syn flood.jpg

Figure 5: To flood the target machine with SYN packets

**1.7 Command 6 - UDP Flood****Syntax**

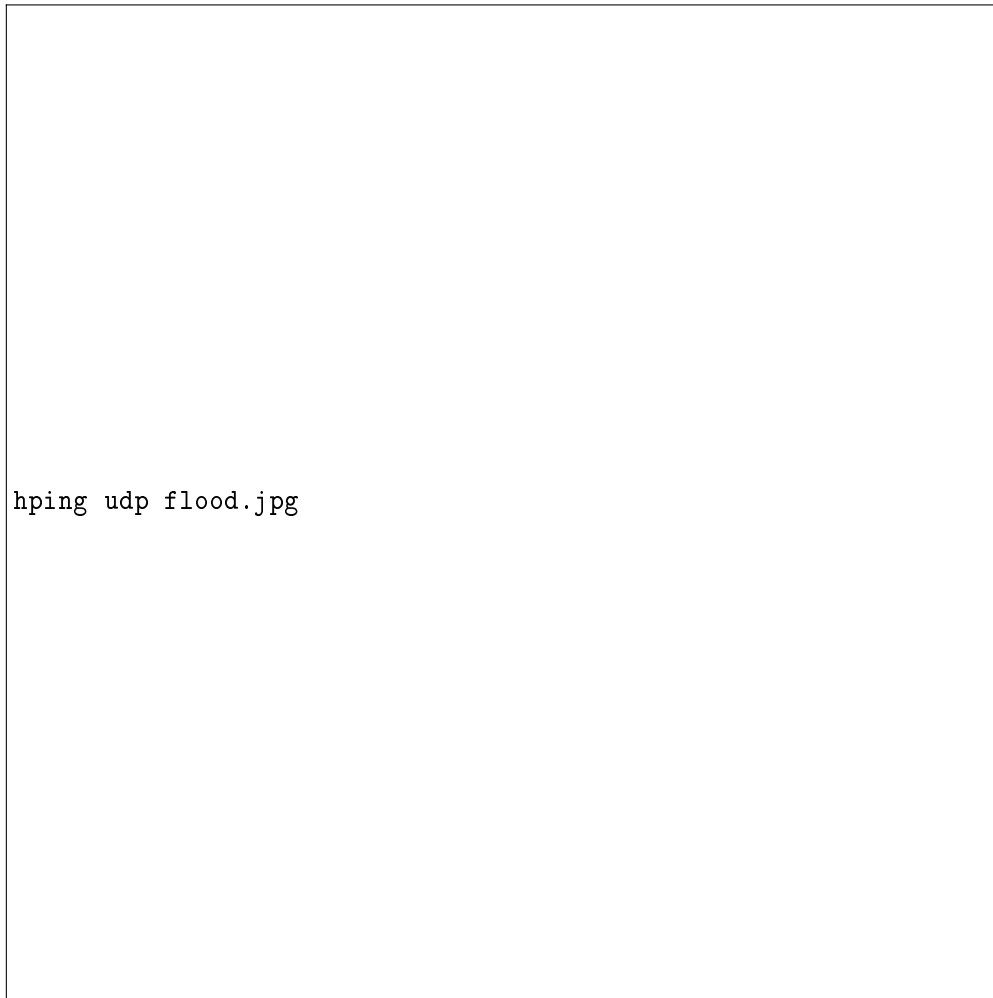
```
$ sudo hping3 --flood --rand-source -2 target_ip
```

**Command**

```
$sudo hping3 --flood --rand-source -2 krishnarajt.surge.sh
```

**Purpose**

To flood the target machine with UDP packets.

**Output**

hping udp flood.jpg

Figure 6: To flood the target machine with UDP packets

**1.8 Command 7 - TCP Flood****Syntax**

```
$ sudo hping3 --flood --rand-source -1 target_ip
```

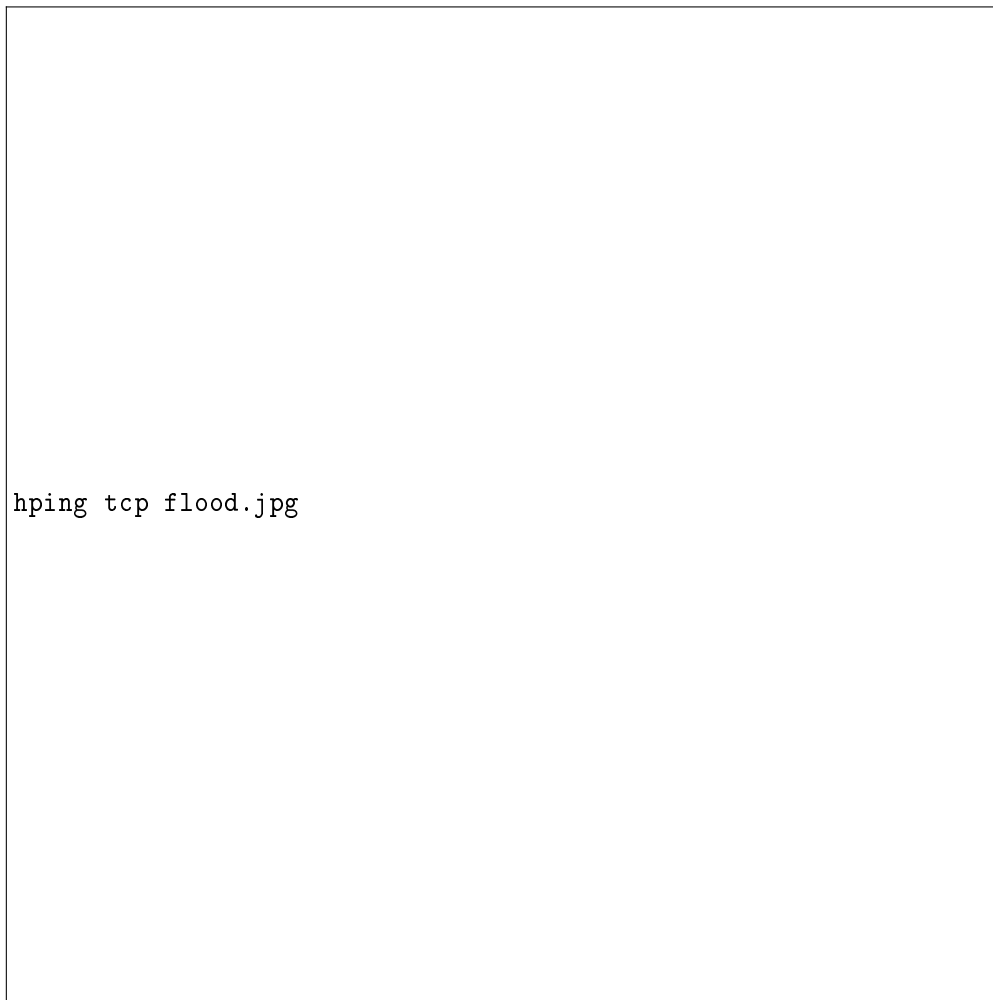
**Command**

```
$sudo hping3 --flood --rand-source -1 krishnarajt.surge.sh
```

**Purpose**

To flood the target machine with TCP packets.



**Output**

hping tcp flood.jpg

Figure 7: To flood the target machine with TCP packets

**1.9 Command 8 - HTTP Flood****Syntax**

```
$ sudo hping3 --flood --rand-source -F target_ip
```

**Command**

```
$sudo hping3 --flood --rand-source -F krishnarajt.surge.sh
```

**Purpose**

To flood the target machine with HTTP packets.

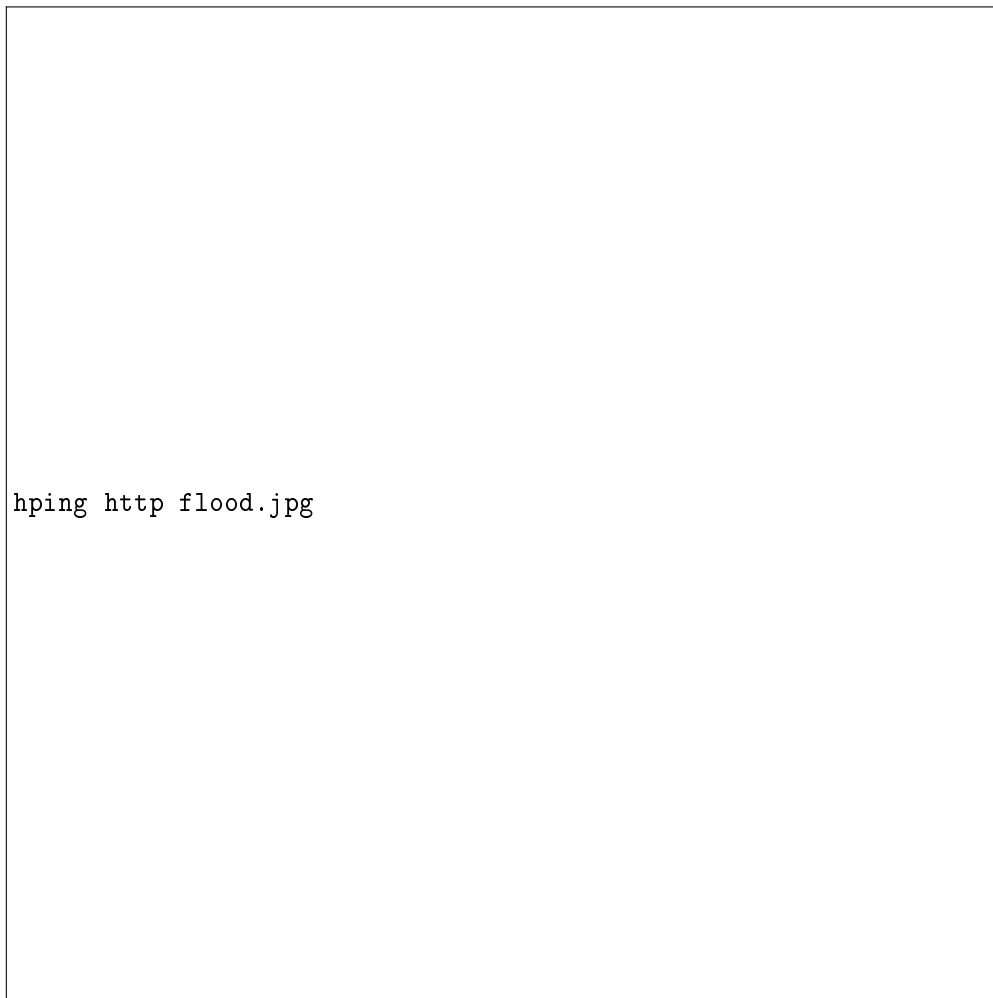
**Output**

Figure 8: To flood the target machine with HTTP packets

## **2 Exploring Tool 2 - p0f**

p0f is a tool that utilizes an array of sophisticated, purely passive traffic fingerprinting mechanisms to identify the players behind any incidental TCP/IP communications (often as little as a single normal SYN) without interfering in any way. Version 3 is a complete rewrite of the original codebase, incorporating a significant number of improvements to network-level fingerprinting, and introducing the ability to reason about application-level payloads (e.g., HTTP).

### **3 Exploring Tool 3 - httpprint**

### **4 Exploring Tool 4 - brutus**

### **5 Platform**

**Operating System:** Kali Linux Rolling on WSL

**IDEs or Text Editors Used:** Visual Studio Code

### **6 Conclusion**

Thus, we have successfully Explored several Tools for Vulnerability Identification and Penetration Testing.