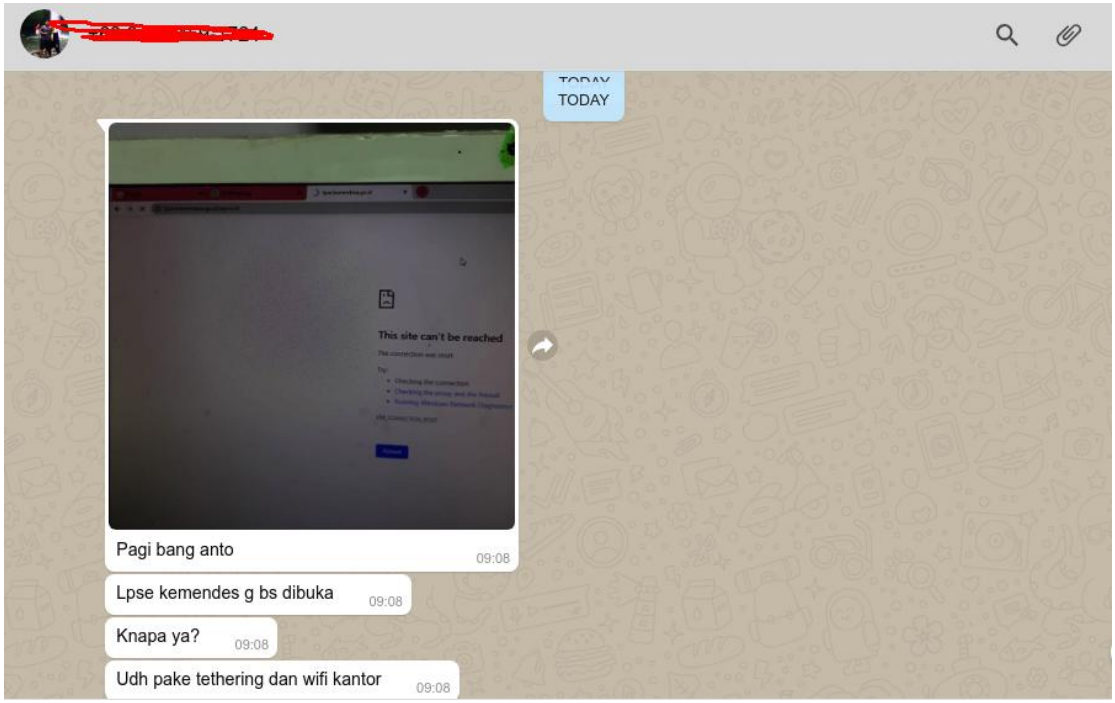
LAPORAN TROUBLESHOOT ERROR SERVER LPSE

1. Berawal dari laporan staf UKPBJ yang menyampaikan aplikasi LPSE tidak dapat diakses



2. Sysadmin melakukan pengecekan service pada server. Semua service berjalan normal

```
[root@appserv-kemendesa ~]# service httpd status
httpd (pid  28292) is running...
[root@appserv-kemendesa ~]# service postgresql-11 status
postgresql-11 (pid  5115) is running...
[root@appserv-kemendesa ~]# service spse4 status
spse4: unrecognized service
[root@appserv-kemendesa ~]# service iptables status
iptables: Firewall is not running.
[root@appserv-kemendesa ~]# sestatus
SELinux status:                 disabled
[root@appserv-kemendesa ~]#
```

3. Sysadmin melihat log error pada web server

```
'import site' failed; use -v for traceback
'import site' failed; use -v for traceback
[Mon Feb 24 10:04:02 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
[Mon Feb 24 10:04:02 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
[Mon Feb 24 10:04:02 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
[Mon Feb 24 10:04:02 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
[Mon Feb 24 10:04:02 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
'import site' failed; use -v for traceback
[Mon Feb 24 10:04:02 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
'import site' failed; use -v for traceback
[Mon Feb 24 10:04:02 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
[Mon Feb 24 10:04:02 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
'import site' failed; use -v for traceback
'import site' failed; use -v for traceback
'import site' failed; use -v for traceback
'import site' failed; use -v for traceback
'import site' failed; use -v for traceback
'import site' failed; use -v for traceback
[Mon Feb 24 10:04:04 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
'import site' failed; use -v for traceback
[Mon Feb 24 10:04:05 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
[Mon Feb 24 10:04:05 2020] [error] (24)Too many open files: apr_socket_accept: (client socket)
'import site' failed; use -v for traceback
'import site' failed; use -v for traceback
'import site' failed; use -v for traceback
[Mon Feb 24 10:04:09 2020] [warn] child process 28272 still did not exit, sending a SIGTERM
^Z
[2]+  Stopped                 tailf /var/log/httpd/error_log
[root@appserv-kemendesa spse]#
```

Dari error terbaca bahwa terdapat request file dalam jumlah besar dalam waktu bersamaan, terdapat limitasi dari konfigurasi default security server untuk membatasinya agar load CPU dan RAM tidak melonjak.

4. Sysadmin melakukan pengecekan trafik pada firewall untuk melihat request yang masuk ke server.

Destination	To Port	Application	Action	Rule	Session End Reason	Bytes	Bytes Sent	Bytes Received
36.66.117.19	80	incomplete	allow	LPSE_NEW	tcp-rst-from-server	1.4k	888	516
36.66.117.19	7547	incomplete	allow	Allow PING DMZ	tcp-rst-from-server	120	60	60
36.66.117.19	0	ping	allow	Inside_akses_DMZ_PRIVATE	aged-out	888	444	444
36.66.117.19	445	incomplete	allow	Allow PING DMZ	tcp-rst-from-server	374	194	180
36.66.117.19	80	incomplete	allow	LPSE_NEW	tcp-rst-from-server	1.5k	942	516
36.66.117.19	80	incomplete	allow	LPSE_NEW	tcp-rst-from-server	1.5k	942	516
36.66.117.19	445	incomplete	allow	Allow PING DMZ	tcp-rst-from-server	120	60	60
36.66.117.19	80	incomplete	allow	LPSE_NEW	tcp-rst-from-client	1.1k	810	330
36.66.117.19	0	ping	allow	Inside_akses_DMZ_PRIVATE	aged-out	888	444	444
36.66.117.19	80	web-browsing	allow	LPSE_NEW	tcp-rst-from-server	2.4k	1.8k	576
36.66.117.19	80	web-browsing	allow	LPSE_NEW	tcp-rst-from-server	4.6k	4.1k	576
36.66.117.19	7547	incomplete	allow	Allow PING DMZ	tcp-rst-from-server	120	60	60
36.66.117.19	0	ping	allow	Inside_akses_DMZ_PRIVATE	aged-out	888	444	444

Benar terdapat request dalam jumlah besar yang koneksinya di reset oleh server.

5. Sysadmin melakukan pengecekan threat pada firewall untuk melihat paket yang masuk ke server.

DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/qiqi.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/tyrant.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/ttt.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/rrr.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/nnn.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/shh.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/ack.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/yyy.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/ioi.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/bbr.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/app.php
DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW	medium	36.66.117.19/aap.php

23 05:03:10	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:03:09	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:03:06	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:03:01	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:58	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:56	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:56	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:56	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:55	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:54	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:49	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:48	vulnerability	PHP DIESCAN Information Disclosure Vulnerability	Outside-Telkom	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW
23 05:02:47	vulnerability	PHP DIESCAN Information	Outside-	DMZ	49.234.181.127		36.66.117.19	80	web-browsing	reset-server	LPSE_NEW

Server sedang diserang dengan metode Brute Force Scanner pada port 80.

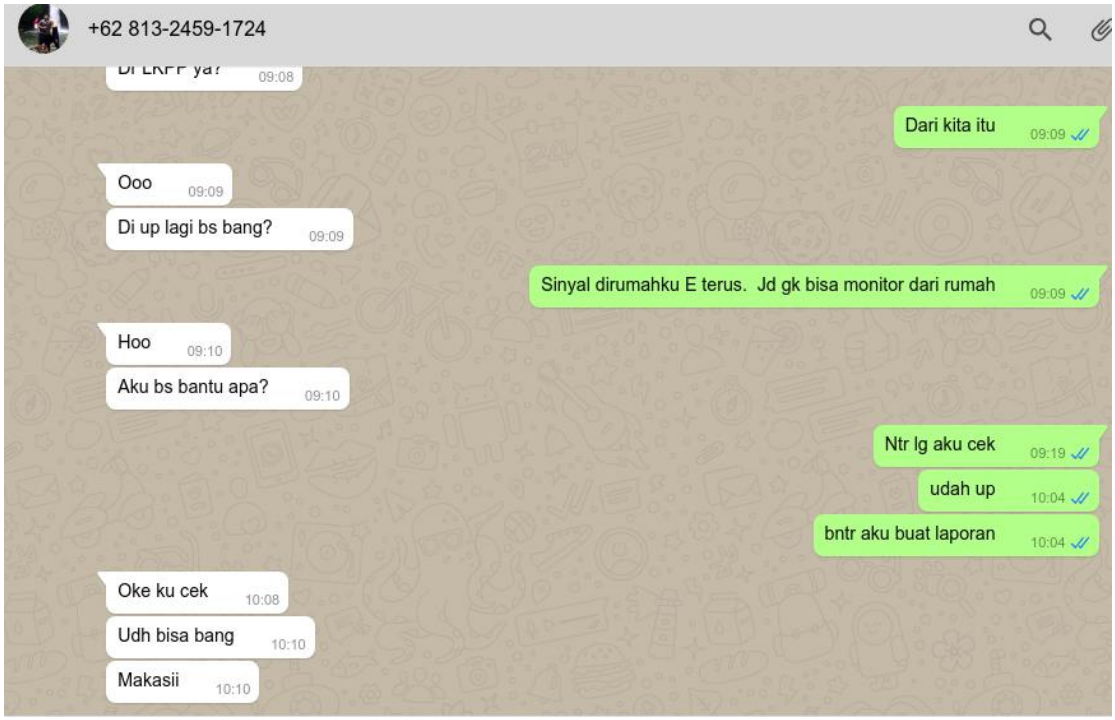
Dikarenakan server LPSE memiliki spesifikasi fisik CPU 16 core dan RAM 32 GB, sysadmin memutuskan untuk meng-allow trafik pada server. Dengan spesifikasi diatas, server diperkirakan mampu menahan script scanner.

```
1  [||              1.9%]   5  [|               0.5%]   9  [              0.0%]   13 [|              0.5%]
2  [|               1.4%]   6  [                0.0%]   10 [||            0.9%]   14 [               0.0%]
3  [|               0.5%]   7  [||              1.4%]   11 [              0.0%]   15 [               0.0%]
4  [                0.0%]   8  [                0.0%]   12 [              0.0%]   16 [               0.0%]
Mem[|||||||||||||||||||||||||||||||||5447/31720MB]   Tasks: 161, 433 thr; 1 running
Swp[||                              175/7847MB]   Load average: 0.08 0.02 0.01
                                                   Uptime: 119 days(!), 02:10:05
```

6. **Solving Problem.** Melakukan edit pada file `/etc/security/limits.conf`
Dan menambahkan pada baris akhir file tsb dengan :

```
ulimit -n 16384
```

7. Melakukan restart service web server.
8. Layanan kembali berjalan normal


+62 813-2459-1724
09:08
Dari kita itu 09:09
Ooo 09:09
Di up lagi bs bang? 09:09
Sinyal dirumahku E terus. Jd gk bisa monitor dari rumah 09:09
Hoo 09:10
Aku bs bantu apa? 09:10
Ntr lg aku cek 09:19
udah up 10:04
bntr aku buat laporan 10:04
Oke ku cek 10:08
Udh bisa bang 10:10
Makasii 10:10