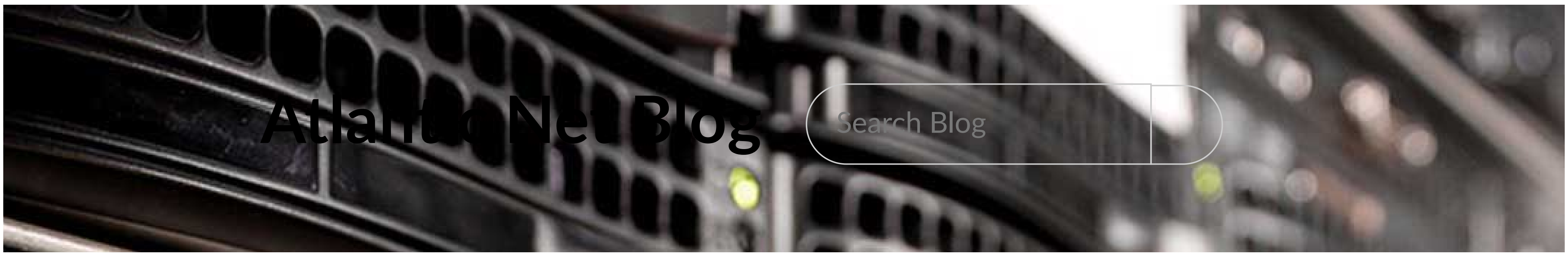


How to Install and Configure ModEvasive with Apache on Ubuntu 18.04

February 22, 2020 by Hitesh Jethva (https://www.atlantic.net/author/hitesh-jethva/) (511 posts) under VPS Hosting (https://www.atlantic.net/category/vps-hosting/)

0 Comments (https://www.atlantic.net/vps-hosting/how-to-install-and-configure-modevasive-with-apache-on-ubuntu-18-04/#disqus_thread)

(mailto:?subject=How to Install and Configure ModEvasive with Apache on Ubuntu 18.04&body=https://www.atlantic.net/vps-hosting/how-to-install-and-configure-modevasive-with-apache-on-ubuntu-18-04/)

(https://reddit.com/submit/?url=https://www.atlantic.net/vps-hosting/how-to-install-and-configure-modevasive-with-apache-on-ubuntu-18-04/&resubmit=true&title=How to Install and Configure ModEvasive with Apache on Ubuntu 18.04)

(https://news.ycombinator.com/submitlink?u=https://www.atlantic.net/vps-hosting/how-to-install-and-configure-modevasive-with-apache-on-ubuntu-18-04/&t=How to Install and Configure ModEvasive with Apache on Ubuntu 18.04)

Protecting your web server against different kinds of attacks is a crucial responsibility for any system administrator. ModEvasive is an Apache web server module that helps you to protect your web server in the event of DoS, DDoS, and brute-force attacks. These types of attacks cause the server to run out of memory, crashing your website.

The mod_evasive module works by creating a hash table of IP Addresses and URIs and monitoring for suspicious incoming server requests, such as:

- Making more than 100 concurrent connections per second.
- Requesting the same page several times per second.

If such a suspicious request occurs, the mod_evasive module sends a 403 error and blocks the IP address.

In this tutorial, we will show you how to install and configure mod_evasive with Apache on an Ubuntu 18.04 server.

Prerequisites

- A fresh Ubuntu 18.04 VPS (https://www.atlantic.net/vps-hosting/) on the Atlantic.Net Cloud Platform.

- A static IP address configured on your server.

Step 1 – Create Atlantic.Net Cloud Server

First, log in to your Atlantic.Net Cloud Server (https://cloud.atlantic.net/?page=userlogin). Create a new server (https://www.atlantic.net/cloud-hosting/how-to-create-new-atlantic-net-cloud-server/), choosing Ubuntu 18.04 as the operating system with at least 1GB RAM. Connect to your Cloud Server via SSH and log in using the credentials highlighted at the top of the page.

Once you are logged into your Ubuntu 18.04 server, run the following command to update your base system with the latest available packages.

```
apt-get update -y
```

Step 2 – Install mod_evasive

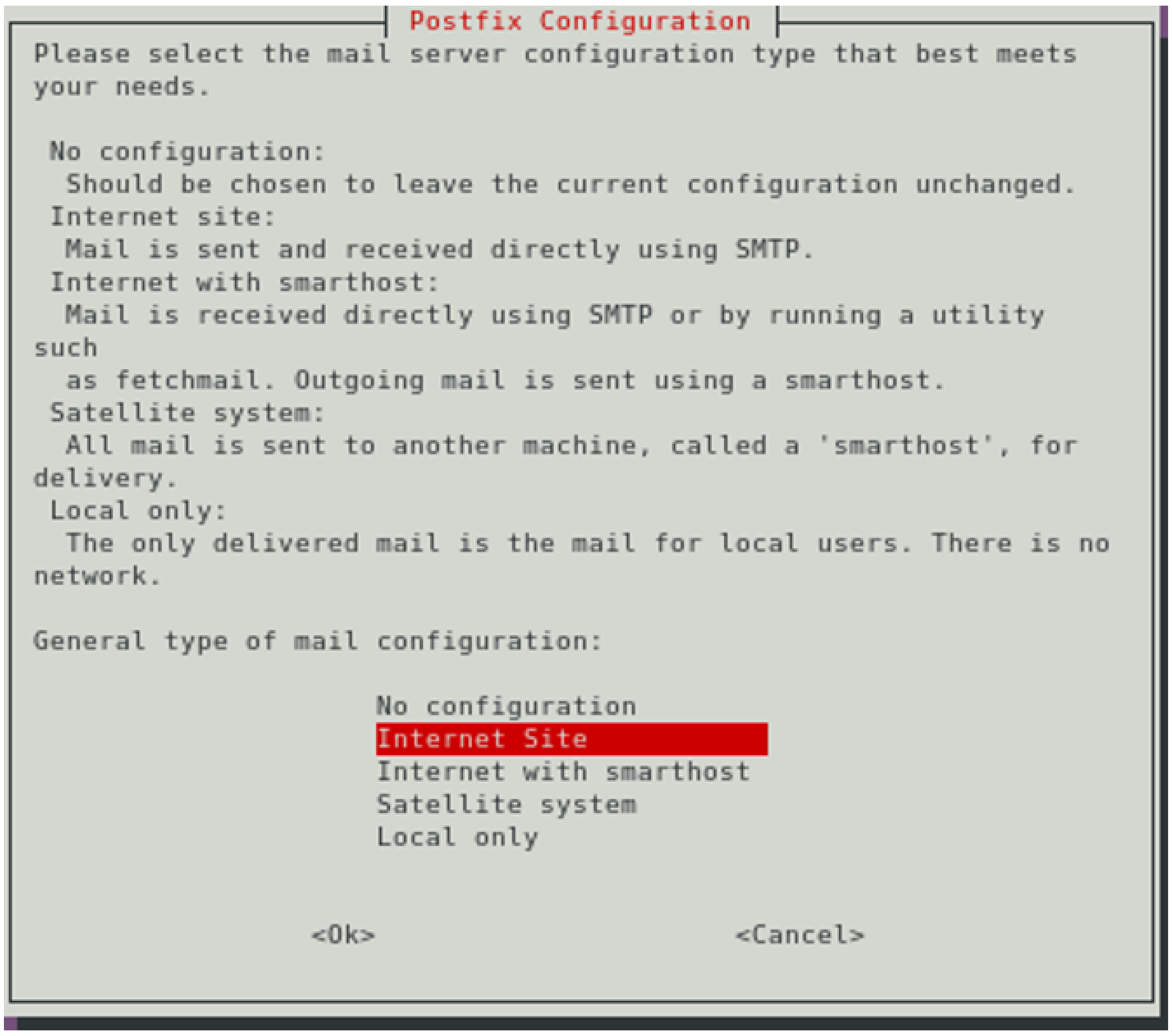
Before starting, Apache webserver needs to be installed on your server. If not installed, you can install it with the following command:

```
apt-get install apache2 apache2-utils -y
```

Once Apache web server is installed, you can install mod_evasive with the following command:

```
apt-get install libapache2-mod-evasive -y
```

During the installation, you will be asked to configure a Postfix mail server for email notification. You can choose your desired option to complete the installation. If you are unsure, just choose *local only* or *no configuration*.



```
Postfix Configuration
Please select the mail server configuration type that best meets
your needs.

 No configuration:
  Should be chosen to leave the current configuration unchanged.
 Internet site:
  Mail is sent and received directly using SMTP.
 Internet with smarthost:
  Mail is received directly using SMTP or by running a utility
such
  as fetchmail. Outgoing mail is sent using a smarthost.
 Satellite system:
  All mail is sent to another machine, called a 'smarthost', for
delivery.
 Local only:
  The only delivered mail is the mail for local users. There is no
network.

General type of mail configuration:

                     No configuration
                     Internet Site
                     Internet with smarthost
                     Satellite system
                     Local only


                 <Ok>                        <Cancel>
```

After installing mod_evasive, you can verify whether the mod_evasive module is enabled by running the following command:

```
apachectl -M | grep evasive
```

You should get the following output:

```
[Mon Jan 27 13:55:35.707317 2020] [so:warn] [pid 29031] AH01574: module
dav_module is already loaded, skipping
 evasive20_module (shared)
```

At this point, the mod_evasive module is installed and enabled. You can now proceed to the next step.

Step 3 – Configure mod_evasive

The default configuration file of mod_evasive is located at /etc/apache2/mods-enabled/evasive.conf. You will need to configure this file per your requirements.

You can open this file using the nano editor as shown below:

```
nano /etc/apache2/mods-enabled/evasive.conf
```

Change the file as shown below. We recommend amending DOSEmailNotify to the address you want the email sent to (if configured) and DOSSystemCommand – for example “su – richard -c ‘/sbin… %s …’”

```
<IfModule mod_evasive20.c>
    DOSHashTableSize    3097
    DOSPageCount        2
    DOSSiteCount        50
    DOSPageInterval     1
    DOSSiteInterval     1
    DOSBlockingPeriod   100
    DOSEmailNotify      root@ubuntu1804
    DOSSystemCommand    "su - someuser -c '/sbin/... %s ...'"
    DOSLogDir           "/var/log/mod_evasive"
</IfModule>
```

Save and close the file when you are finished.

A brief explanation of each option is shown below:

- **DOSHashTableSize**: mod_evasive uses this option to control the hash table size. It is recommended to increase this if you have a busy web server.
- **DOSPageCount**: This option specifies the threshold limit for the number of requests allowed to the same URI per second. Once the threshold limit has been exceeded, the client's IP address will be blacklisted.
- **DOSSiteCount**: This option specifies the limit on the total number of requests allowed to the same IP address.
- **DOSPageInterval**: This option specifies the page count interval.
- **DOSSiteInterval**: This option specifies the site count interval.
- **DOSBlockingPeriod** : This option defines the amount of time in seconds that a client will be blocked.
- **DOSEmailNotify**: This option sends an email to the specified address when an IP address has been blacklisted.
- **DOSSystemCommand**: Whenever an IP address has been blacklisted, the specified system command will be executed.
- **DOSLogDir**: This option defines the mod_evasive log directory.

Next, create a directory to store the mod_evasive log and change its ownership to www-data with the following command:

```
mkdir /var/log/mod_evasive
chown -R www-data:www-data /var/log/mod_evasive
```

Finally, restart the Apache service to implement the changes:

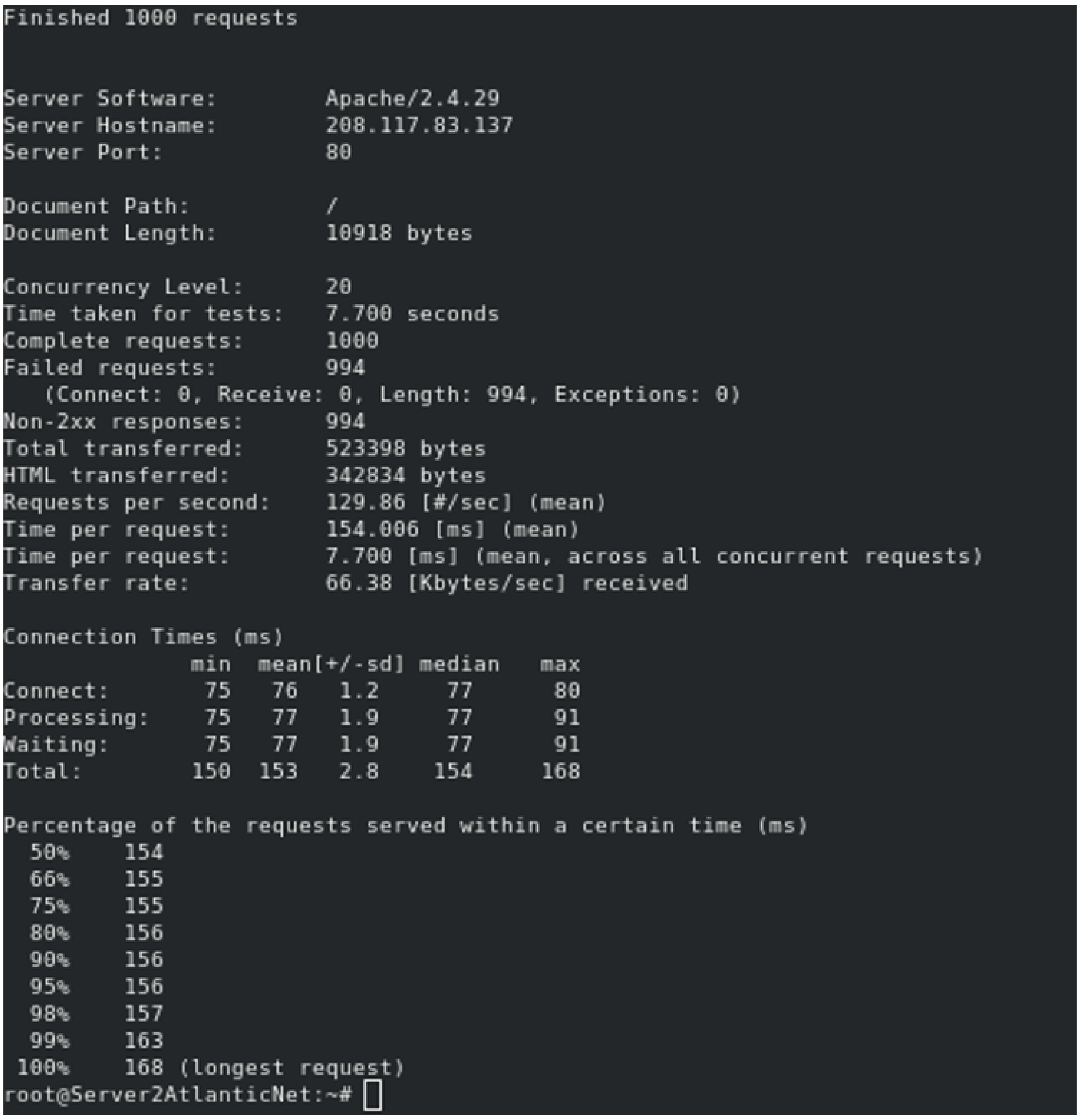
```
systemctl restart apache2
```

Step 4 – Test mod_evasive

At this point, the mod_evasive module is installed and configured. It's time to test whether the module is working correctly.

Go to the remote system and send a bulk page request to the server using the ab command:

```
ab -n 1000 -c 20 http://your-server-ip/
```



```
Finished 1000 requests


Server Software:        Apache/2.4.29
Server Hostname:        208.117.83.137
Server Port:            80

Document Path:          /
Document Length:        10918 bytes

Concurrency Level:      20
Time taken for tests:   7.700 seconds
Complete requests:      1000
Failed requests:        994
   (Connect: 0, Receive: 0, Length: 994, Exceptions: 0)
Non-2xx responses:      994
Total transferred:      523398 bytes
HTML transferred:       342834 bytes
Requests per second:    129.86 [#/sec] (mean)
Time per request:       154.006 [ms] (mean)
Time per request:       7.700 [ms] (mean, across all concurrent requests)
Transfer rate:          66.38 [Kbytes/sec] received

Connection Times (ms)
              min  mean[+/-sd] median   max
Connect:       75   76   1.2     77      80
Processing:    75   77   1.9     77      91
Waiting:       75   77   1.9     77      91
Total:        150  153   2.8    154     168

Percentage of the requests served within a certain time (ms)
  50%    154
  66%    155
  75%    155
  80%    156
  90%    156
  95%    156
  98%    157
  99%    163
 100%    168 (longest request)
root@Server2AtlanticNet:~#
```

This command will cause the equivalent of a DoS attack by sending 1000 page requests in 10 concurrent connections.

On the server, check the mail log by running the following command:

```
tail -15 /var/mail/root
```

You should see that the client IP address has been blacklisted by mod_evasive:

```
Received: by ubuntu1804 (Postfix, from userid 33)
            id B0C3EC1753; Mon, 27 Jan 2020 14:15:09 +0000 (UTC)
To: root@ubuntu1804
MIME-Version: 1.0
Content-Type: text/plain; charset="ANSI_X3.4-1968"
Content-Transfer-Encoding: 8bit
Message-Id: <20200127141509.B0C3EC1753@ubuntu1804>
Date: Mon, 27 Jan 2020 14:15:09 +0000 (UTC)
From: www-data <www-data@ubuntu1804>

To: root@ubuntu1804
Subject: HTTP BLACKLIST 103.250.161.100

mod_evasive HTTP Blacklisted 103.250.161.100
```

You can also test mod_evasive using the test.pl built-in script. You will need to modify this script to make it works.

You can edit the script as shown below:

```
nano /usr/share/doc/libapache2-mod-evasive/examples/test.pl
```

Find the following line:

```
print $SOCKET "GET /?$_ HTTP/1.0\n\n";
```

Replace it with the following:

```
print $SOCKET "GET /?$_ HTTP/1.0\r\nHost: 127.0.0.1\r\n\r\n";
```

Save and close the file when you are finished. Then, run the script using the perl command:

```
perl /usr/share/doc/libapache2-mod-evasive/examples/test.pl
```

If everything works correctly, you should get the following output:

```
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
HTTP/1.1 403 Forbidden
```

Conclusion

Congratulations! The mod_evasive module is now configured to protect your server against DDoS and Brute force attacks.

< Older post (https://www.atlantic.net/vps-hosting/how-to-install-and-configure-mariadb-galera-cluster-on-ubuntu-18-04/)

Newer post > (https://www.atlantic.net/vps-hosting/how-to-set-up-ssh-keys-on-ubuntu-18-04/)

ALSO ON **ATLANTIC.NET**

Getting Started with DNS Records
2 years ago · 2 comments
Atlantic.Net's Cloud Portal includes a DNS management module that …

Top 8 Cloud-Based Software Testing …
2 years ago · 2 comments
There is no shortage of good software testing tools on the market. Here's our …

Install OpenLiteSpeed, MariaDB, PHP8.0 on …
2 years ago · 1 comment
In this tutorial post, we will show you how to install Openlightspeed, …

Post-Pand Cybersecu
a year ago · 2
How have cy threats chan pandemic? E