



UNIVERSIDAD AUTÓNOMA DE CHIAPAS

Facultad de Contaduría y Administración, Campus I

Ingeniería y Desarrollo de Tecnologías de Software

Título: VPS con dominio

Materia: Análisis de vulnerabilidades

GILBERTO FARRERA LÓPEZ. A191017
CULEBRO LÓPEZ PAOLA A200176
GONZÁLEZ ÁLVAREZ BRAYAN ULISES A200116

Docente: Luis Gutierrez Alfaro

1. Servicio de VPS

En este caso usaremos un servicio de VPS de la empresa de “contabo” usando el perfil más accesible.

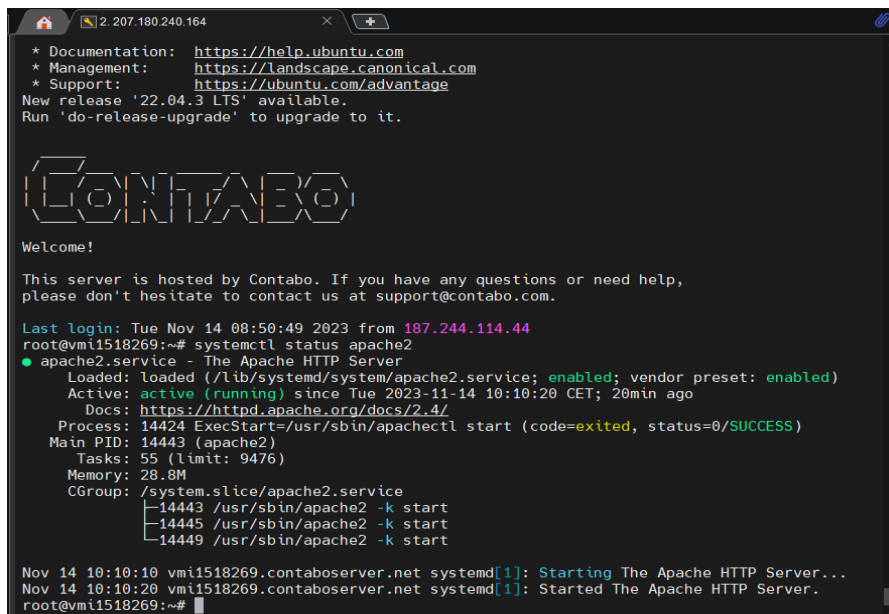
Con las siguientes especificaciones:

- 4 núcleos
- 8 gb de ram
- 200 gb ssd
- 1 snapshot
- 32 tb traffic

en este caso usaremos el sistema operativo “UBUNTU 20.04” y toda la conexión se hará por medio de SSH, lo cual instalaremos todas las dependencias del servidor en apache y usaremos la base de datos de “MARIADB”, aclarado este punto, comenzaremos con las instalaciones en este caso ya tenemos todas las configuraciones anteriores que aplicamos en el servidor local en ubuntu con el sitio de pruebas “DVWA”.

Se anexan imágenes para saber que las instalaciones son funcionales

Apache funcionando en contabo



```
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

CONTABO

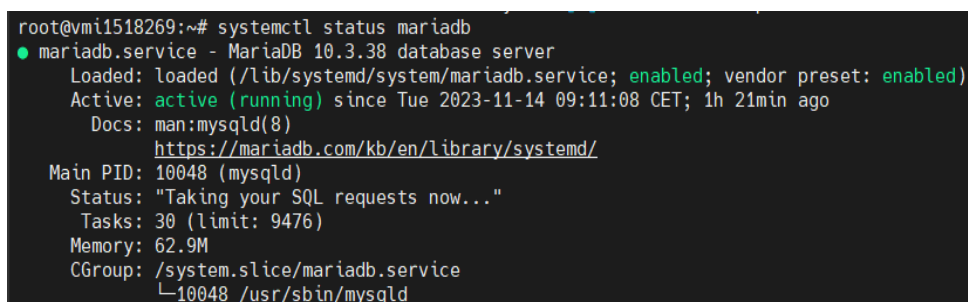
Welcome!

This server is hosted by Contabo. If you have any questions or need help,
please don't hesitate to contact us at support@contabo.com.

Last login: Tue Nov 14 08:50:49 2023 from 187.244.114.44
root@vml1518269:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-11-14 10:10:20 CET; 20min ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 14424 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
   Main PID: 14443 (apache2)
    Tasks: 55 (limit: 9476)
   Memory: 28.8M
   CGroup: /system.slice/apache2.service
           └─14443 /usr/sbin/apache2 -k start
             14445 /usr/sbin/apache2 -k start
             14449 /usr/sbin/apache2 -k start

Nov 14 10:10:10 vml1518269.contaboserver.net systemd[1]: Starting The Apache HTTP Server...
Nov 14 10:10:20 vml1518269.contaboserver.net systemd[1]: Started The Apache HTTP Server.
root@vml1518269:~#
```

Mariadb funcionando



```
root@vml1518269:~# systemctl status mariadb
● mariadb.service - MariaDB 10.3.38 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-11-14 09:11:08 CET; 1h 21min ago
     Docs: man:mysqld(8)
           https://mariadb.com/kb/en/library/systemd/
   Main PID: 10048 (mysqld)
    Status: "Taking your SQL requests now..."
   Tasks: 30 (limit: 9476)
   Memory: 62.9M
   CGroup: /system.slice/mariadb.service
           └─10048 /usr/sbin/mysqld
```

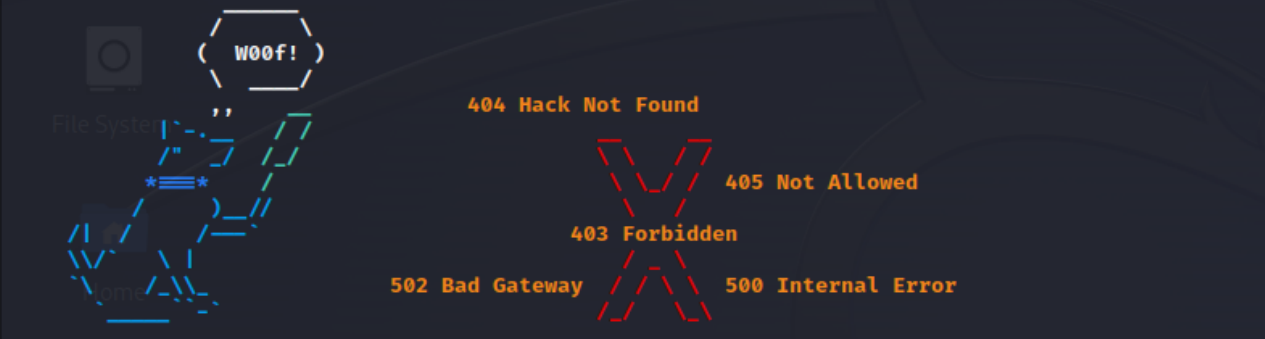
UFW activo

```
root@vmi1518269:~# ufw status numbered
Status: active

      To Action From
      --
[ 1] Apache Full ALLOW IN Anywhere
[ 2] 22 ALLOW IN Anywhere
[ 3] Apache Full (v6) ALLOW IN Anywhere (v6)
[ 4] 22 (v6) ALLOW IN Anywhere (v6)
```

Verificación de **MOD_SECURITY** por medio de Kali linux usando el comando “**wafw00f**”

```
File Actions Edit View Help
(gilberto@gilberto)-[~]
$ wafw00f http://207.180.240.164
```



The interface displays a large red 'X' in the center, indicating a detected security solution. Surrounding the 'X' are several HTTP error codes in orange text: 404 Hack Not Found, 405 Not Allowed, 403 Forbidden, 502 Bad Gateway, and 500 Internal Error. To the left of the 'X' is a stylized dog head icon with the text '(WOOF!)'. Below the 'X' is the text '~ WAFW00F : v2.2.0 ~' and 'The Web Application Firewall Fingerprinting Toolkit'.

```
[*] Checking http://207.180.240.164
[+] Generic Detection results:
[*] The site http://207.180.240.164 seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "403"
[~] Number of requests: 5
```

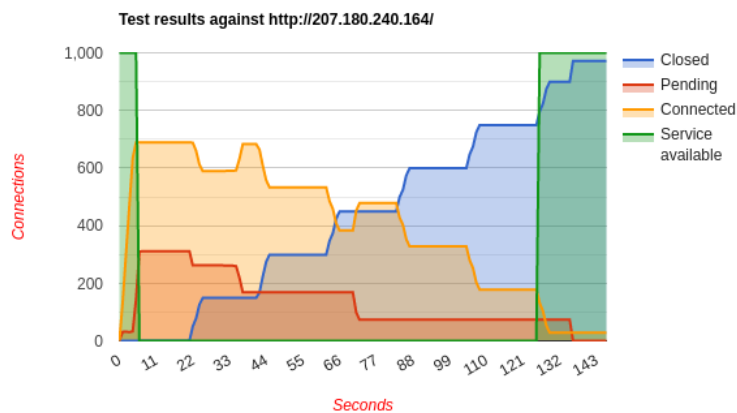
mod_evasive activo

```
root@vmi1518269:/var/www/html# apachectl -M | grep evasive
evasive20_module (shared)
```

prueba de slowhttptest (Sostenido a cambio)

Test parameters

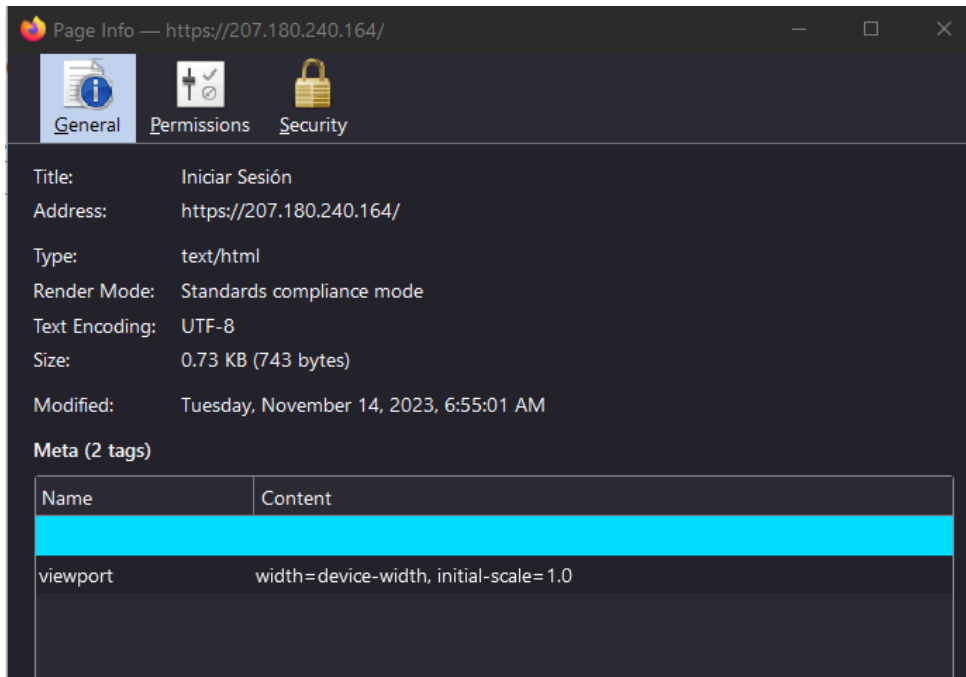
Test type	SLOW HEADERS
Number of connections	1000
Verb	GET
Content-Length header value	4096
Cookie	
Extra data max length	52
Interval between follow up data	10 seconds
Connections per seconds	200
Timeout for probe connection	3
Target test duration	240 seconds
Using proxy	no proxy



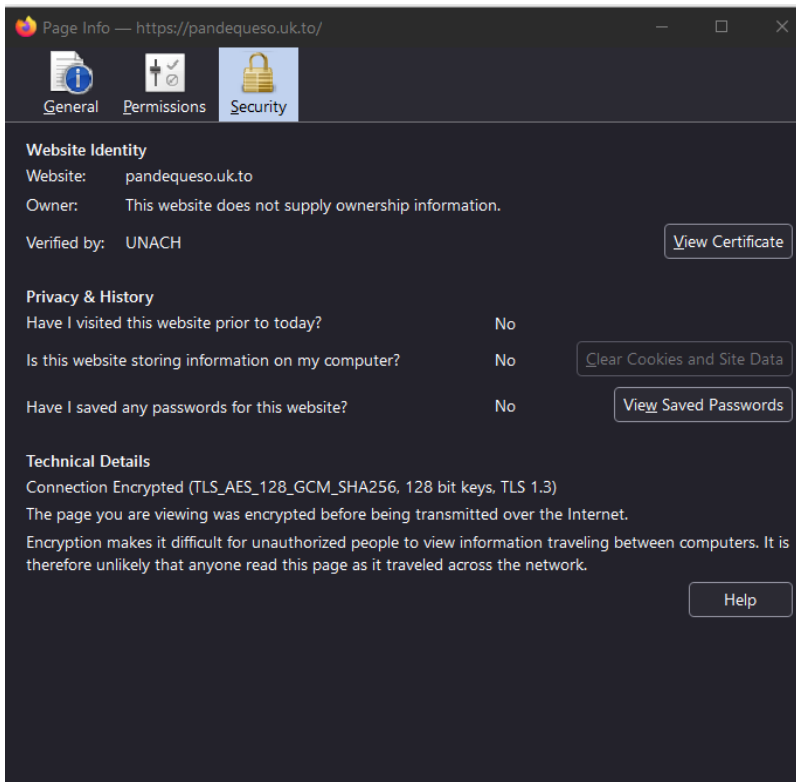
Fail2ban activo

```
root@vmi1518269:~# sudo systemctl enable fail2ban
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-s
Executing: /lib/systemd/systemd-sysv-install enable fail2ban
Created symlink /etc/systemd/system/multi-user.target.wants/fail2ban.service → /lib/systemd/
root@vmi1518269:~# sudo systemctl start fail2ban
root@vmi1518269:~# sudo systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2023-11-14 14:24:32 CET; 11s ago
     Docs: man:fail2ban(1)
  Main PID: 8541 (fail2ban-server)
    Tasks: 5 (limit: 9457)
   Memory: 13.7M
      CPU: 459ms
   CGroup: /system.slice/fail2ban.service
           └─8541 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

Certificado autofirmado por ubuntu activo



Domino de sitio web activo



conclusión

para concluir con este documento, primero llevo 8 horas sin moverme de la silla, pero al final funcionó el vps configurado con la seguridad que aplique en el dwwa, certificado SSL autofirmado por ubuntu y el nombre de dominio que obtuve de manera gratuita freedns con un simple registro de datos básico.

pero como se puede observar la práctica fue funcional y no mostró problemas al momento de ejecutarse, además en el caso del ataque Ddos falta ajustar la cantidad de datos para evitar un caída total del servidor, ya que este se puede recuperar pero se muestra lentitud en ciertos momentos.

Bueno debido al tiempo aun no agrego el front real al servidor pero agregue un login sin registros solo para las pruebas de protección.

Bibliográfica

<https://freedns.afraid.org/>

Sitio web → <https://pandqueso.uk.to/>

https://www.youtube.com/watch?v=8kdcLs_FbUI&t=553s&ab_channel=INNOVADOMOTICS

Servicio de VPS → <https://contabo.com/en/>