

Reporte

Marzo 26, 2019

1 Resumen Ejecutivo

Se hizo el análisis del equipo proporcionado por medio de una herramienta para la identificación de los servicios que este provee. Dentro de estos servicios, los mas criticos fueron los siguientes: Servicio de base de datos, dos Servidores web y un Servicio para intercambio de archivos.

En uno de los servicios web se encontro que la contraseña para acceder a la administración de los contenidos era muy fácil (esta se encontraba en el top 100 de contraseñas mas usadas).

En el servicio para intercambio archivos, se encontró que cualquier persona con conocimientos de como usar el servicio puede hacer uso de este y manipular un archivo de acceso para poder entrar a la maquina con una cuenta que si bien no tiene muchos privilegios, en un futuro podría aprovecharse de un error para poder manipular contenido al que anteriormente tenía restringido.

2 Objetivo

Analizar el equipo proporcionado , encontrar y explotar las posibles vulnerabilidades en este y así poder dar recomendaciones para la solución de estos.

3 Alcance

Se proporciono un servidor al cual se le harán pruebas para obtener información acerca de este y obtener puertos abiertos y servicios asociados a este. Esto para obtener la mayor cantidad de información posible y proceder a atacar el objetivo.

4 Hallazgos

4.1 Wordpress

WORD01: Enumeración de usuarios

Impacto: 3.7

CVE: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N

WORD02: Uso de captcha fácil de romper

Impacto: 0.0

CVE: AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:N

WORD03: Uso de contraseñas débiles

Impacto: 7.7

CVE: AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L

Referencias de apoyo:

[https://www.owasp.org/index.php/Testing_for_Captcha_\(OWASP-AT-008\)](https://www.owasp.org/index.php/Testing_for_Captcha_(OWASP-AT-008))

https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

<https://es.wordpress.org/plugins/stop-user-enumeration/>

<https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy>

4.2 FTP

FTP01: Autenticación con sesión anónima

Impacto: 5.6

CVE: AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L

Referencias de apoyo:

<https://www.acunetix.com/vulnerabilities/web/ftp-anonymous-logins/>

5 Recomendaciones

5.1 WORD01

Se recomienda evitar mensajes muy descriptivos cuando un inicio de sesión falla, ya que esto indica que esto puede revelar información acerca de los usuarios que existen, y cambiarlo por mensajes menos descriptivos.

5.2 WORD02

Se recomienda cambiar el tipo de captcha por uno más complejo ya que los matemáticas son más fáciles de romper.

5.3 WORD03

Se recomienda usar contraseñas mas fuertes, el uso de frases como contraseña es buena medida.

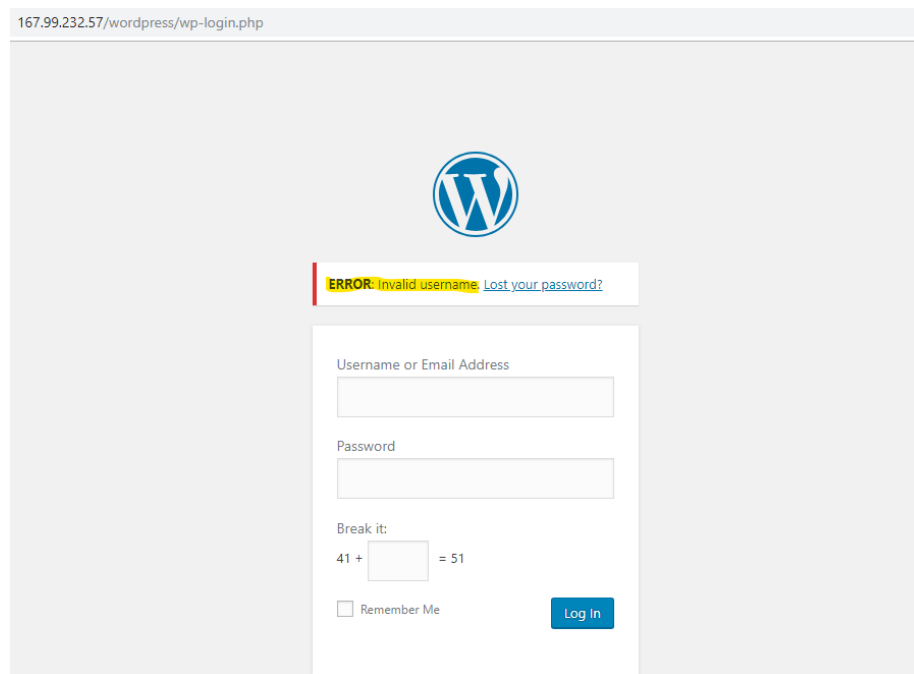
5.4 FTP01

Se recomienda desactivar la autenticación anonima, para que sólo los usuarios autorizados puedan usar el servicio.


6 Anexos

6.1 Wordpress

Se encontro que el CMS wordpress se encontraba corriendo en el servidor y a través de este se podía hacer enumeración de usuarios por medio del login:



167.99.232.57/wordpress/wp-login.php



ERROR Invalid username. [Lost your password?](#)

Username or Email Address

Password

Break it:
41 + = 51

☐ Remember Me

Figure 1: Enumeración de usuarios

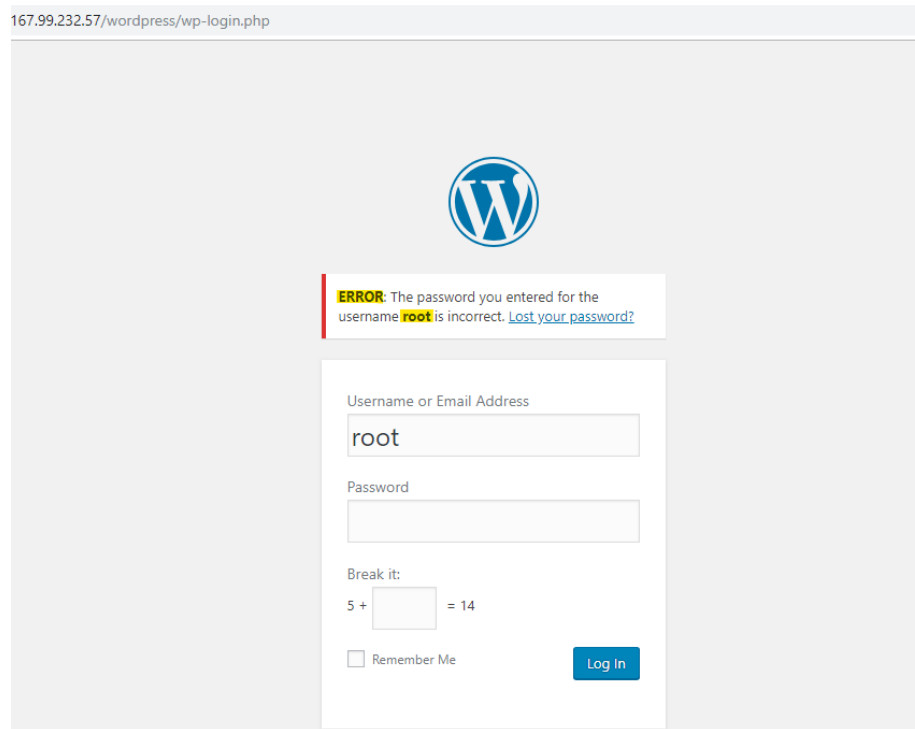


Figure 2: Enumeración de usuarios

Como se puede ver, en la segunda imagen se ingreso el usuario root, el cual es un usuario valido y nos dice que la contraseña para ese usuario no es válida, algo que no pasa en la primera imagen.

Sabiendo que existe el usuario root, con un ataque de fuerza bruta se podría obtener la contraseña, sin embargo, no puede ser un ataque trivial ya que el sitio cuenta con un captcha con una suma, solo bastó hacer un programa en python que procese la solicitud del sitio y resolver el captcha, una vez hecho esto, se uso el top 100 de contraseñas mas usadas y el resultado fue que se obtuvo la contraseña del usuario root:

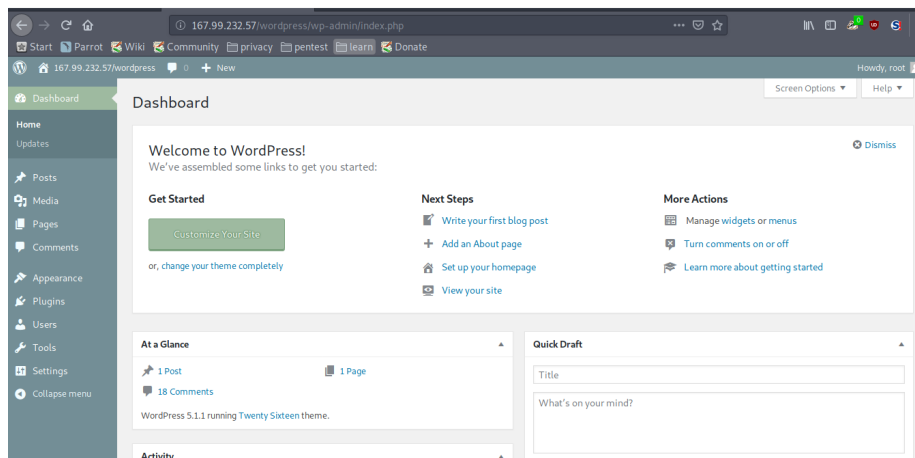


Figure 3: Obtención de acceso debido a contraseña débil

6.2 FTP

Se encontro el servicio FTP aceptando conexiones anónimas. Al listar los directorio se encontraron los siguientes directorios:

```
[iamc@parrot]~[~/Desktop/pentest]
$ftp 167.99.232.57
Connected to 167.99.232.57.
220 (vsFTPd 3.0.3)
Name (167.99.232.57:iamc): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  5 0 com/vulner 117 /sites/web/ 4096 Mar 24 03:11 .
drwxr-xr-x  5 0 org/wiki/W 117 /edia:10,000 4096 Mar 24 03:11 ..
drwx----- kove 2 112 m/quest 117 /43299777/ser 4096 Mar 24 17:07 .cache
drwx----- developer 3 112 a.org/e 117 /s/Web/HTTP/W 4096 Mar 24 03:08 .gnupg
drwx----- acune /vulner 117 /ities/network 4096 Mar 25 03:27 .ssh
226 Directory send OK.
ftp>
```

Figure 4: Autenticación anonima en FTP

A partir de esta información el directorio de interés es el .ssh, en el cual hay un archivo llamado authorized_keys en el cual se pueden añadir llaves para

conexiones por el servicio ssh. Procedí a crear un par de claves (pública y privada) y añadí la pública al archivo `authorized_keys` y procedí a conectarme como el usuario `ftp`:

```
[~]-[iamc@parrot]-[~/ssh]
$ssh ftp@167.99.232.57
Welcome to Ubuntu 18.04.2 LTS (GNU/Linux 4.15.0-46-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon Mar 25 06:34:16 UTC 2019
System load: 0.0 Processes: 122
Usage of /: 9.7% of 24.06GB Users logged in: 2
Memory usage: 78% IP address for eth0: 167.99.232.57
Swap usage: 0%

Get cloud support with Ubuntu Advantage Cloud Guest:
http://www.ubuntu.com/business/services/cloud

* Canonical Livepatch is available for installation.
Reduce system reboots and improve kernel security. Activate at:
https://ubuntu.com/livepatch

7 packages can be updated.
3 updates are security updates.

Last login: Mon Mar 25 06:16:27 2019 from 187.190.166.155
ftp@chaos:~$
```

Figure 5: Conexión SSH

Una vez dentro, procedí a listar a los usuarios del sistema:

```

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106::/home/syslog:/usr/sbin/nologin
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin
apt:x:104:65534::/nonexistent:/usr/sbin/nologin
lxd:x:105:65534::/var/lib/lxd:/bin/false
uuidd:x:106:110::/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112::/var/lib/landscape:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
mysql:x:111:116:MySQL Server,,,:/nonexistent:/bin/false
ubuntu:x:1000:1000:,,,:/home/ubuntu:/bin/bash
ftp:x:112:117:ftp daemon,,,:/srv/ftp:/bin/bash
xf938o:x:1001:1001:,,,:/home/xf938o:/bin/bash
ftp@chaos:~/.ssh$

```

Figure 6: Listando usuarios

Una mala configuración del servicio FTP produjo la obtención de una terminal mediante una conexión SSH con el usuario del servicio FTP (ftp) lo cual permite al atacante moverse a algunas partes del sistema y listar algunos archivos debido a que no es una cuenta privilegiada, sin embargo, si esto no es corregido, en un futuro podría salir alguna vulnerabilidad para el sistema en cuestion y el atacante puede aprovecharse de esta.