**AUDITORÍA DE UN NUEVO SOFTWARE**

Para realizar la auditoría del nuevo software desarrollado por el departamento de software de una empresa, primeramente se ha iniciado nuestra máquina con el sistema operativo **kali Linux**, se ha obtenido la IP para saber el en qué rango de IP estamos y seguidamente se ha buscado los equipos existentes en nuestra red hasta identificar el objetivo:

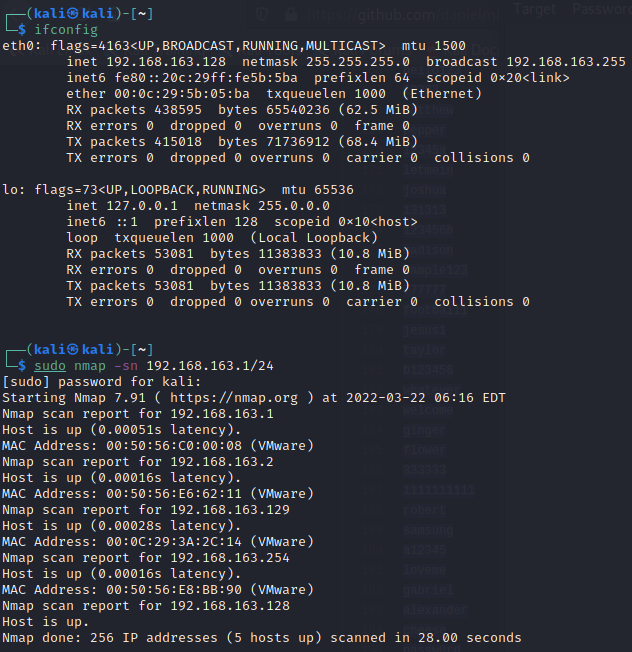


Figura 1 Identificar activos vivos.

Se han obtenido **4 IPs** sin contar la del mismo equipo que realiza el escaneo, de las cuales, la terminada en **.1** es el propio equipo físico donde se ejecuta la máquina virtual, la termina en **.2** es el la puerta de enlace o *gateway*, la terminada en **.254** es una dirección de *broadcast* por parte del sistema utilizado para virtualizar (VMware) y por último la terminada en **.129** es la máquina objetivo.

Una vez localizado el objetivo se han utilizado tanto el escáner de vulnerabilidades **Nessus** como el escáner **Nmap** obteniendo los siguientes resultados:

* **Vulnerabilidades de la versión del sistema operativo:**

## Campo 1: Descripción

**Sistema operativo Unix sin soporte**. Versión anterior, desactualizada y sin soporte de Ubuntu. Concretamente la versión Ubuntu 8.04. Lo cual implica fallos críticos de seguridad en esta versión del sistema operativo, a nivel de *kernel*.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **crítico**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

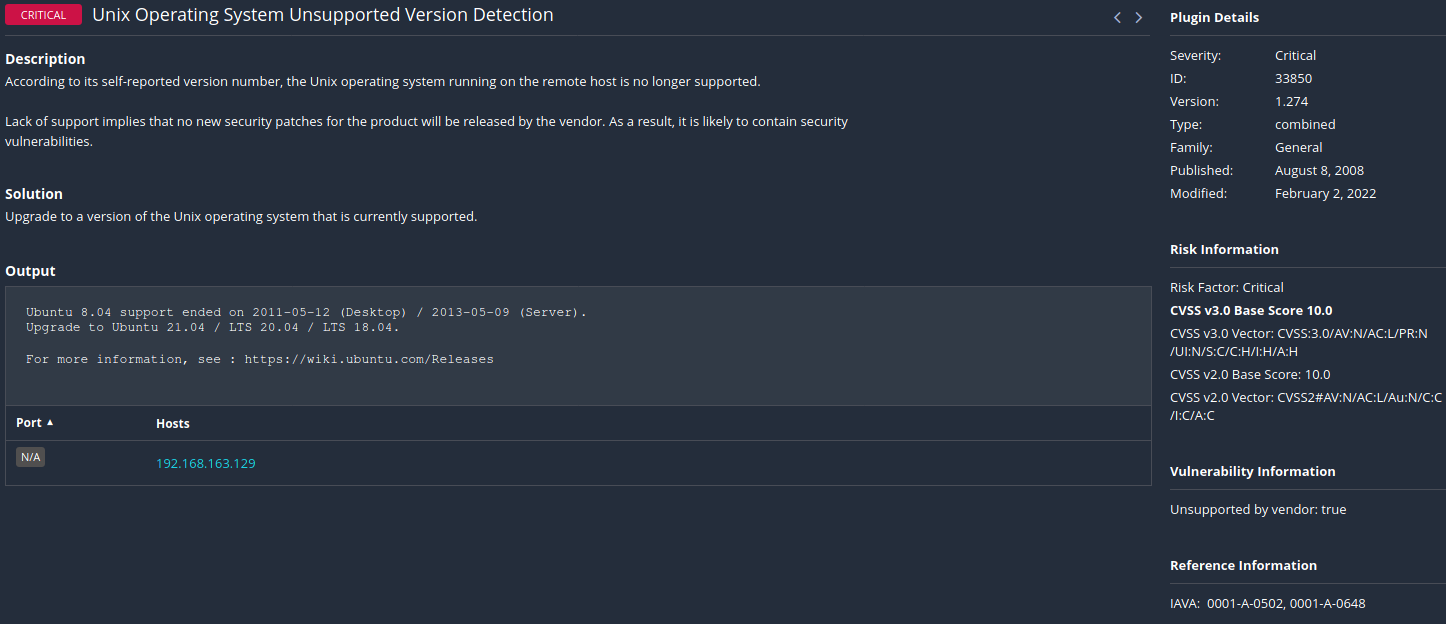
****

Figura 2 Vulnerabilidad por SO antiguo.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debe actualizar el sistema operativo a una versión con soporte o última versión existente de Ubuntu.

* **Vulnerabilidades del servidor web Apache puertos 80 y 8009:**

## Campo 1: Descripción

**Inyección de código en la comunicación por el conector AJP de Apache Tomcat**. Vulnerabilidad encontrada en el conector AJP de Apache Tomcat. Esta vulnerabilidad permitiría la lectura de ficheros de aplicaciones web en un servidor vulnerable y la inclusión o carga de ficheros maliciosos JavaServer Pages (JSP) dentro de distintos ficheros, con la posible ejecución remota de código, en el caso que el servidor permita la carga de ficheros.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **crítico**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

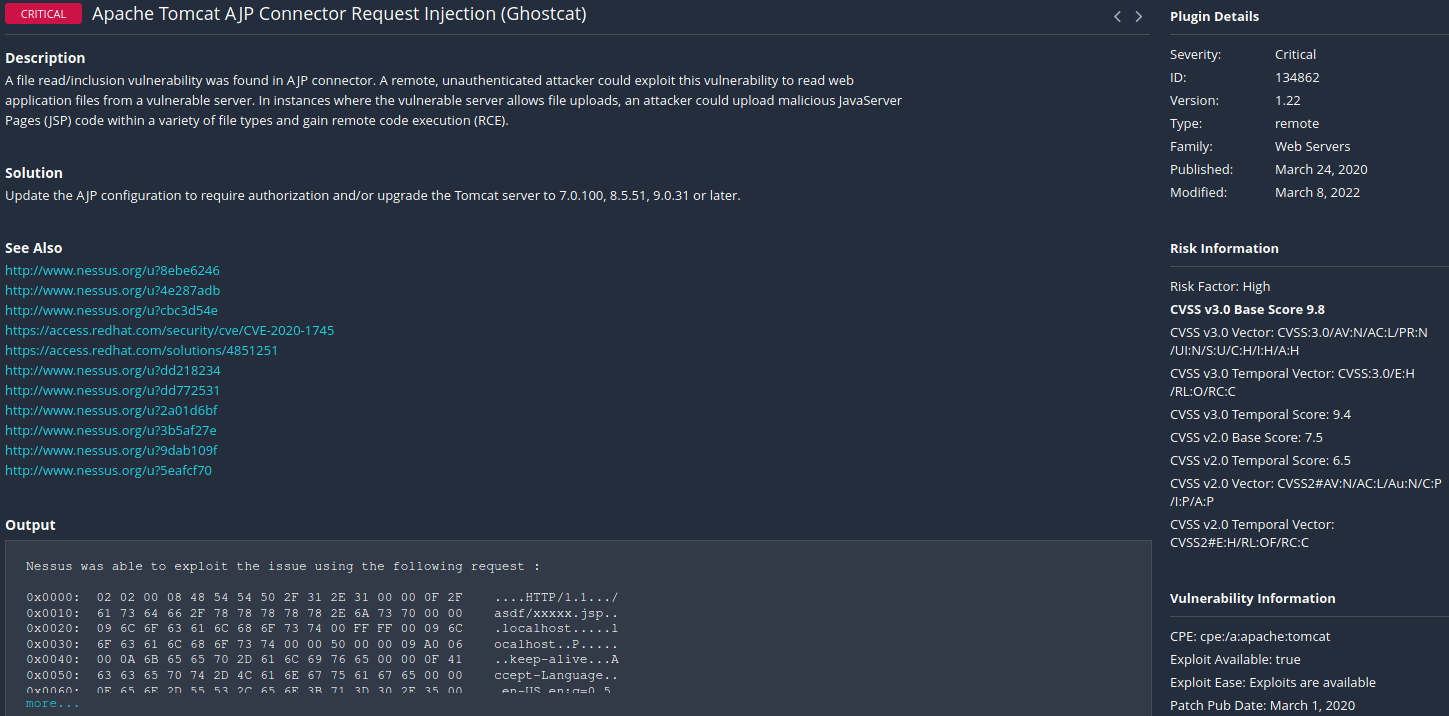
****

Figura 3 Vulnerabilidad conector AJP Tomcat.

Seguidamente se realizado la explotación de la vulnerabilidad utilizando la herramienta **Mestasploit**:

* Se ha buscado la vulnerabilidad por su referencia CVE: ***search cve-2020-1938***
* Se ha seleccionado el exploit: ***auxiliary/admin/http/tomcat\_ghostcat***
* Se configurado el exploit y se ha lanzado:

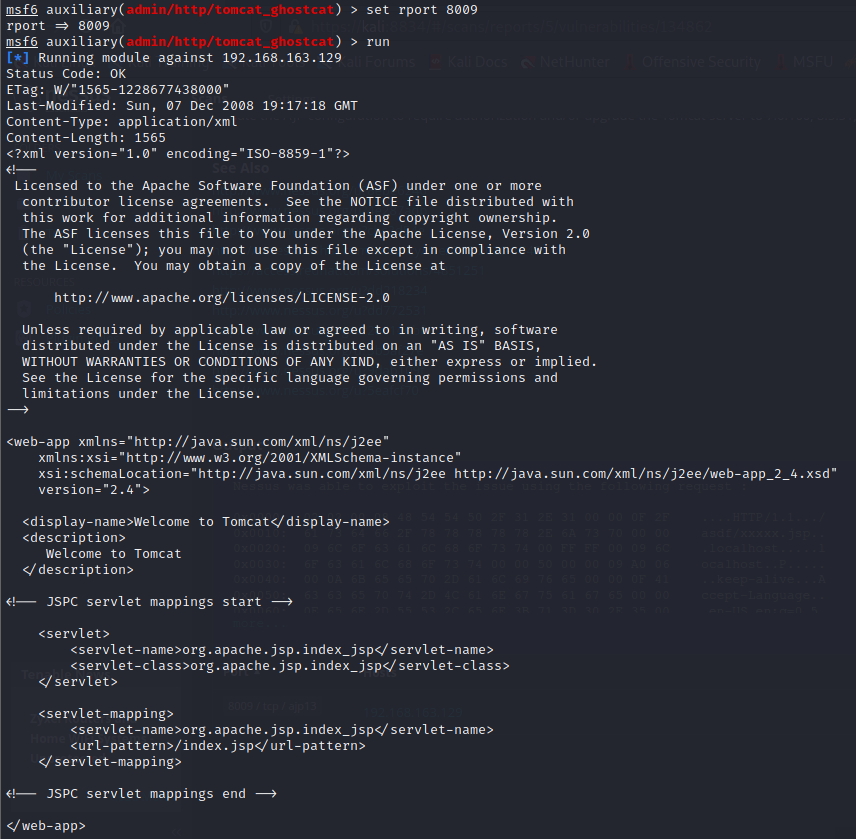


Figura 4 Lectura fichero aplicaciones web.

Mostrando la posibilidad de lectura de ficheros de aplicaciones web, en este caso la aplicación Apache.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería actualizar la configuración del conector AJP para que se requiera autenticación y actualizar la versión del servidor Tomcat a la 7.0.100, 9.5.51, 9.0.31 o posterior.

## Campo 1: Descripción

**Ejecución de comando arbitrario en el parámetro f de TikiWiki tiki-graph-formula.php.** Vulnerabilidad encontrada en la versión de TikiWiki instalada, la cual no resetea la variable ***f[]*** del script *tiki-graph-formula.php* antes de usarlo como una llamda de una función. Un posible atacante podría aprovechar este problema para ejecutar código arbitrario en el host remoto.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **alto**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

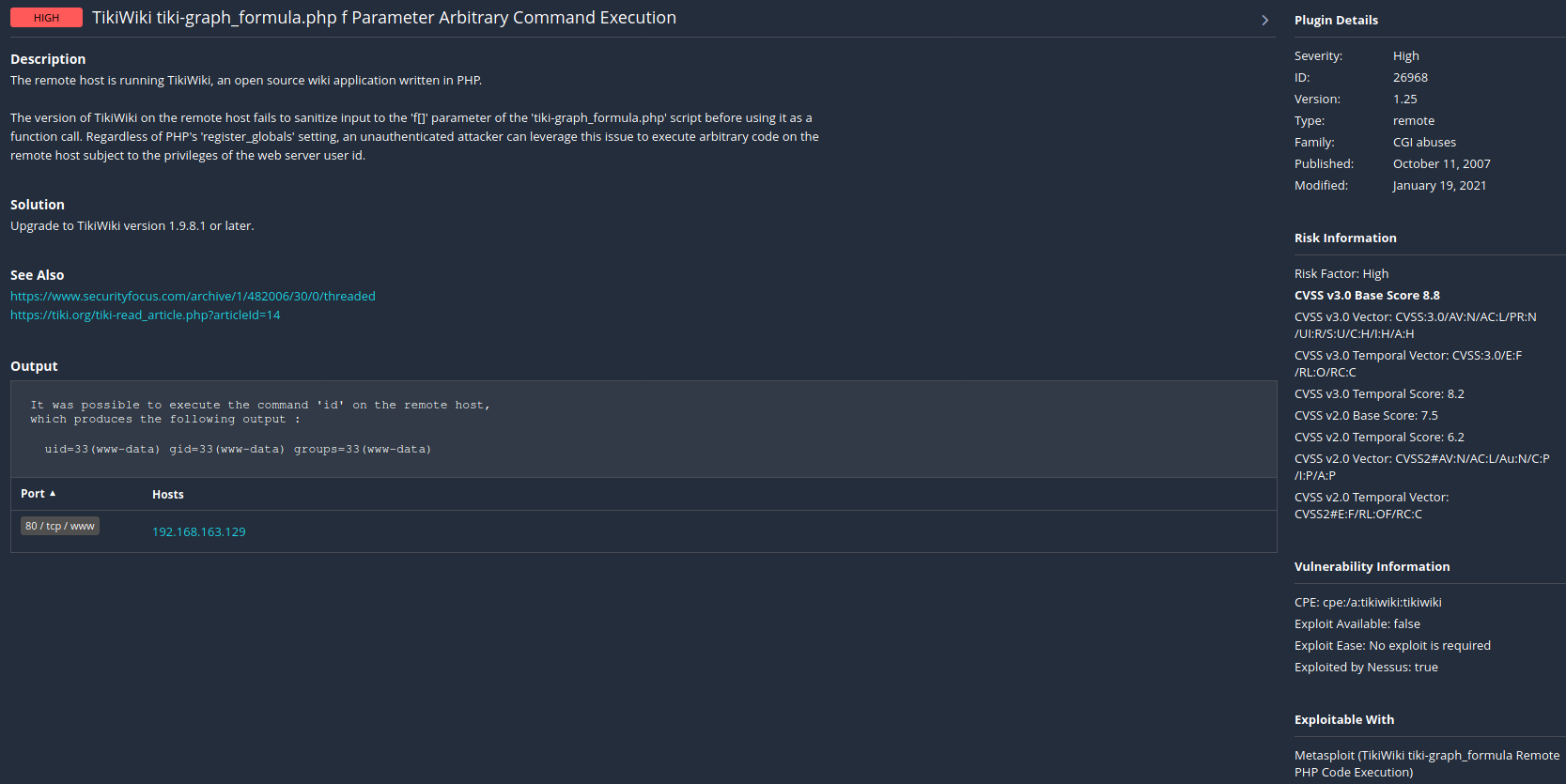


Figura 5 Vulnerabilidad en TikiWiki.

Seguidamente se realizado la explotación de la vulnerabilidad utilizando la herramienta **Mestasploit**:

* Se ha buscado la vulnerabilidad por su referencia CVE: ***search cve-2007-5423***
* Exploit seleccionado: ***exploit/unix/webapp/tikiwiki\_graph\_formula\_exec***
* Se ha configurado el exploit y se ha lanzado:

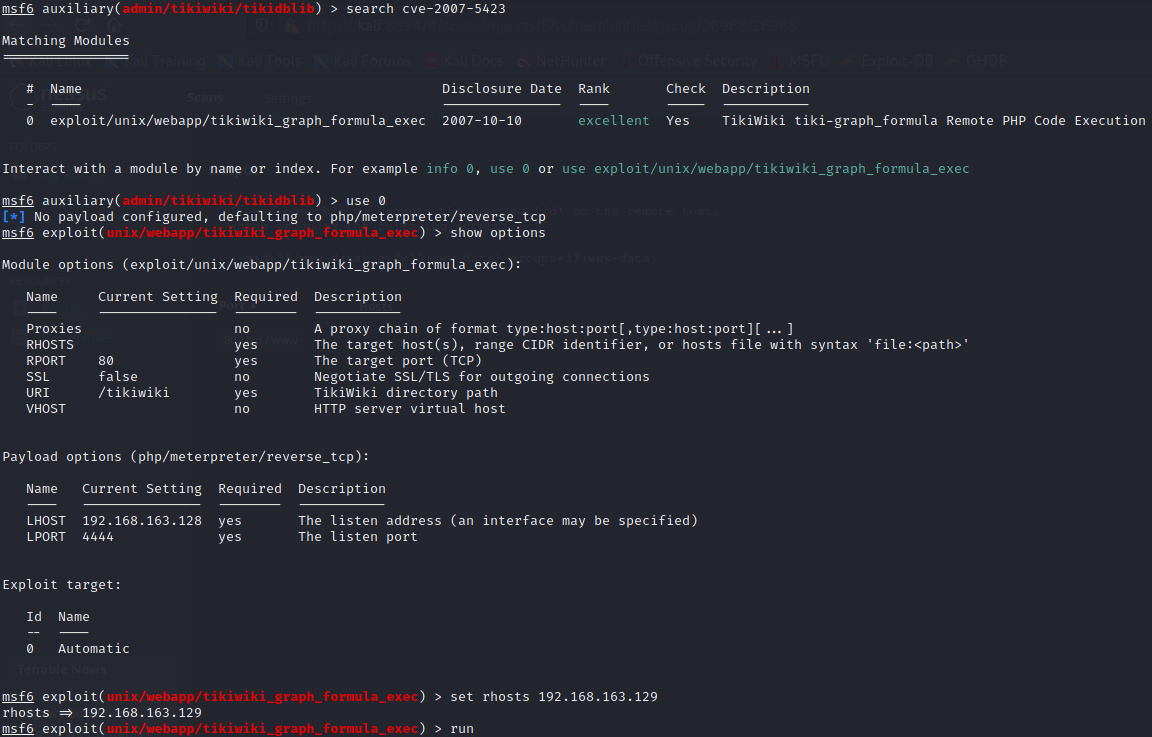


Figura 6 Explotación de la vulnerabilidad de TikiWiki.

Se ha podido observar la explotación de esta vulnerabilidad y la obtención de una sesión de **Meterpreter**:

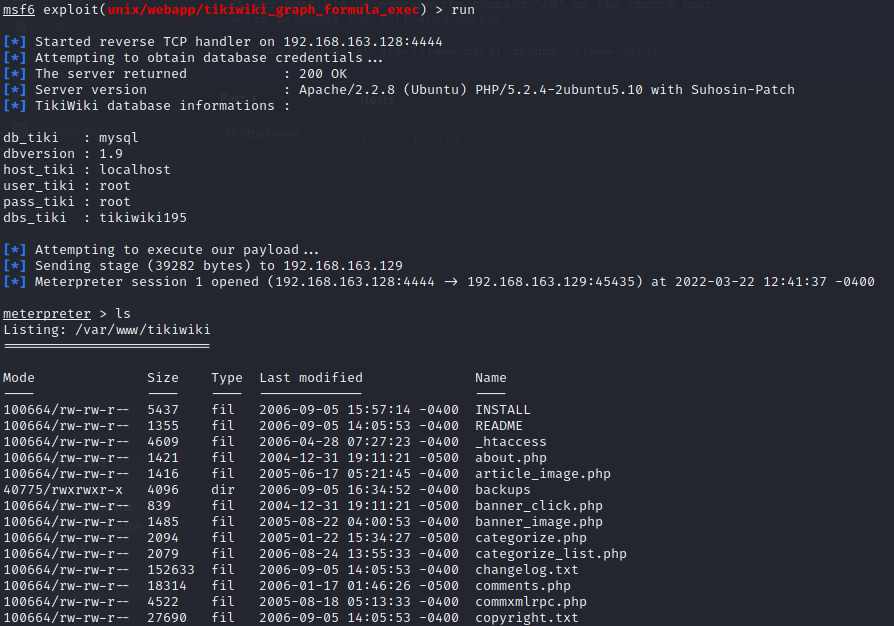


Figura 7 Sesión Meterpreter.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería actualizar la versión de TikiWiki a la versión 1.9.8.1 o superior.

## Campo 1: Descripción

**Divulgación de información de parametos en TikiWiki tiki-lastchanges.php si el parámetro sort\_mode está vacío.** Vulnerabilidad encontrada en la versión instalada de TikiWiki, la cual revela las credencias de la base de datos utilizada por la aplicación cuando se pasa un parámetro *sort\_mode* vavío al script *tiki-lastchanges.php*. Un atacante podría explotar este problema para extraer las credenciales de la base de datos.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

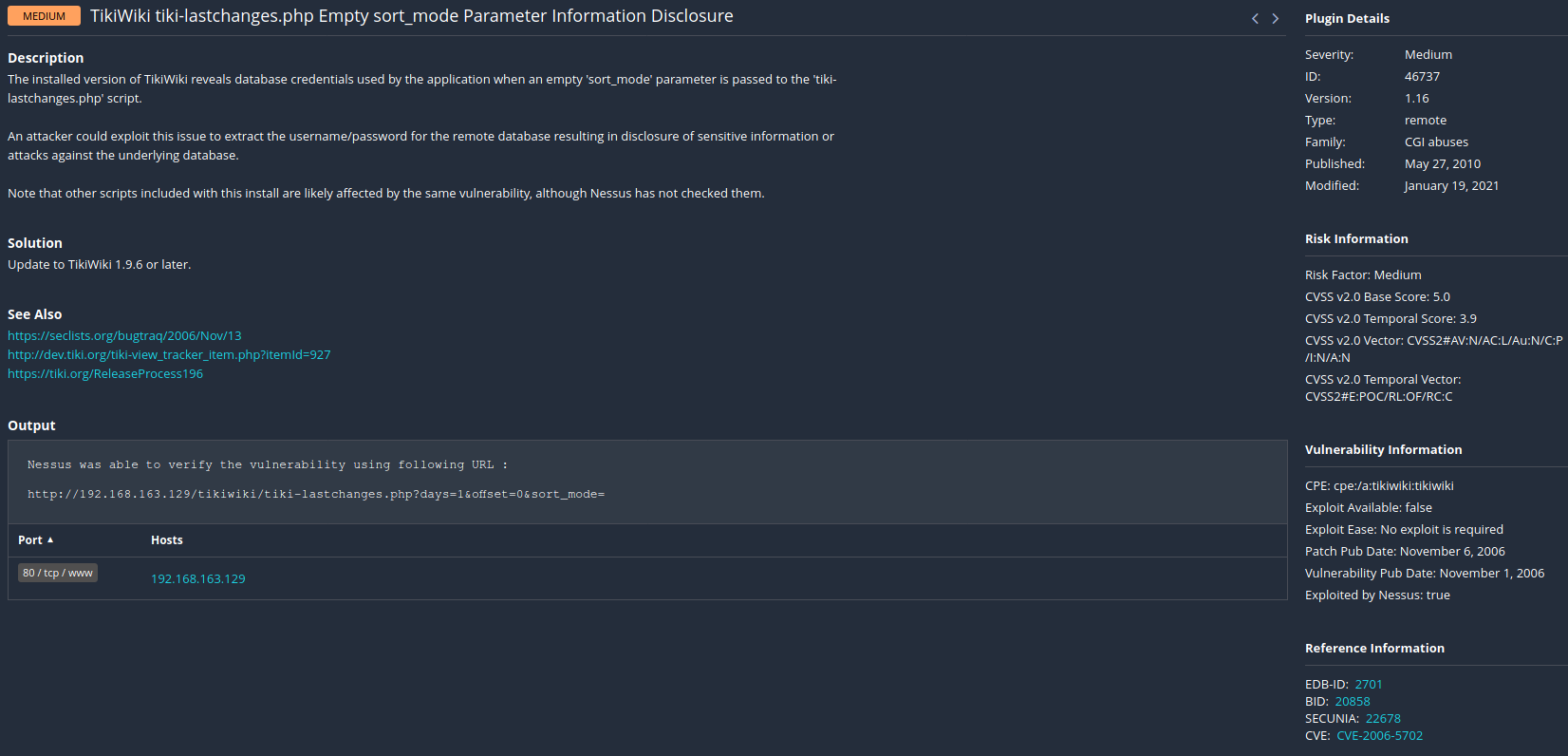


Figura Vulnerabilidad TikiWiki, credenciales.

Explotación realizada con la herramienta **Mestasploit**:

* Se ha buscado la vulnerabilidad por su referencia CVE: ***search cve-2006-5702***
* Se ha seleccionado el exploit: ***auxiliary/admin/tikiwiki/tikidblib***
* Se ha configurado el exploit y se ha lanzado:

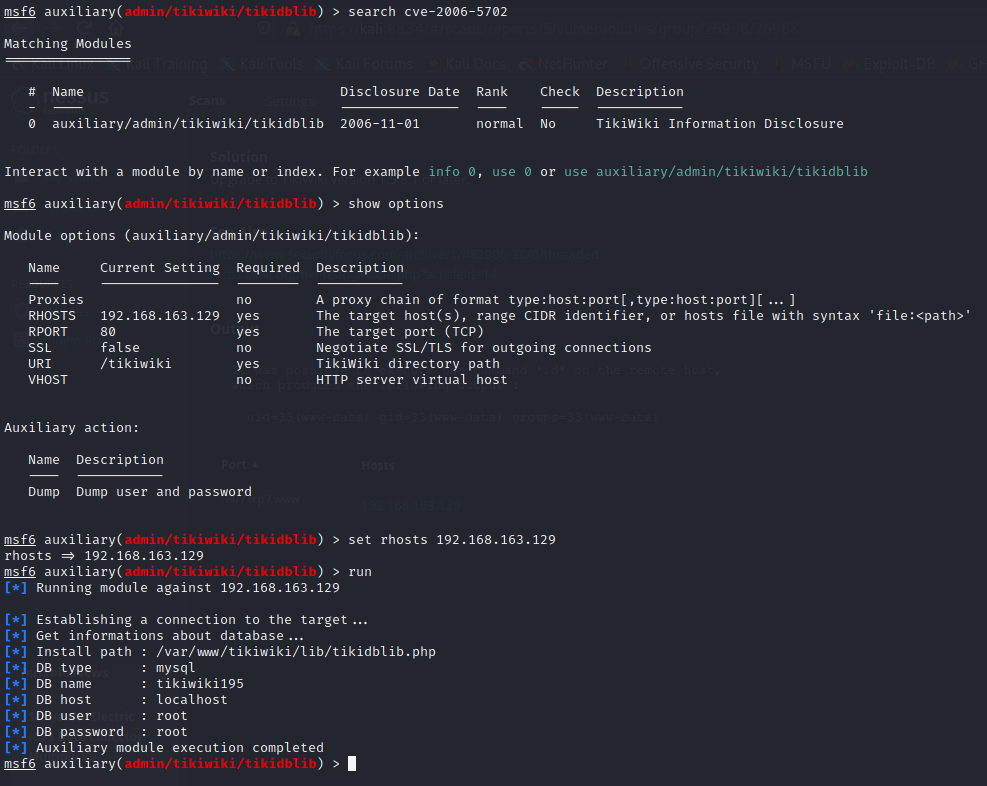


Figura 9 Explotación con Metasploit.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería actualizar la versión de TikiWiki a la versión 1.9.6 o superior.

## Campo 1: Descripción

**Métodos HTTP TRACE/TRACK permitidos**. Vulnerabilidad encontrada debido a que el servidor web permite los métodos de depuración TRACE/TRACK para depurar las conexiones del servidor web.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

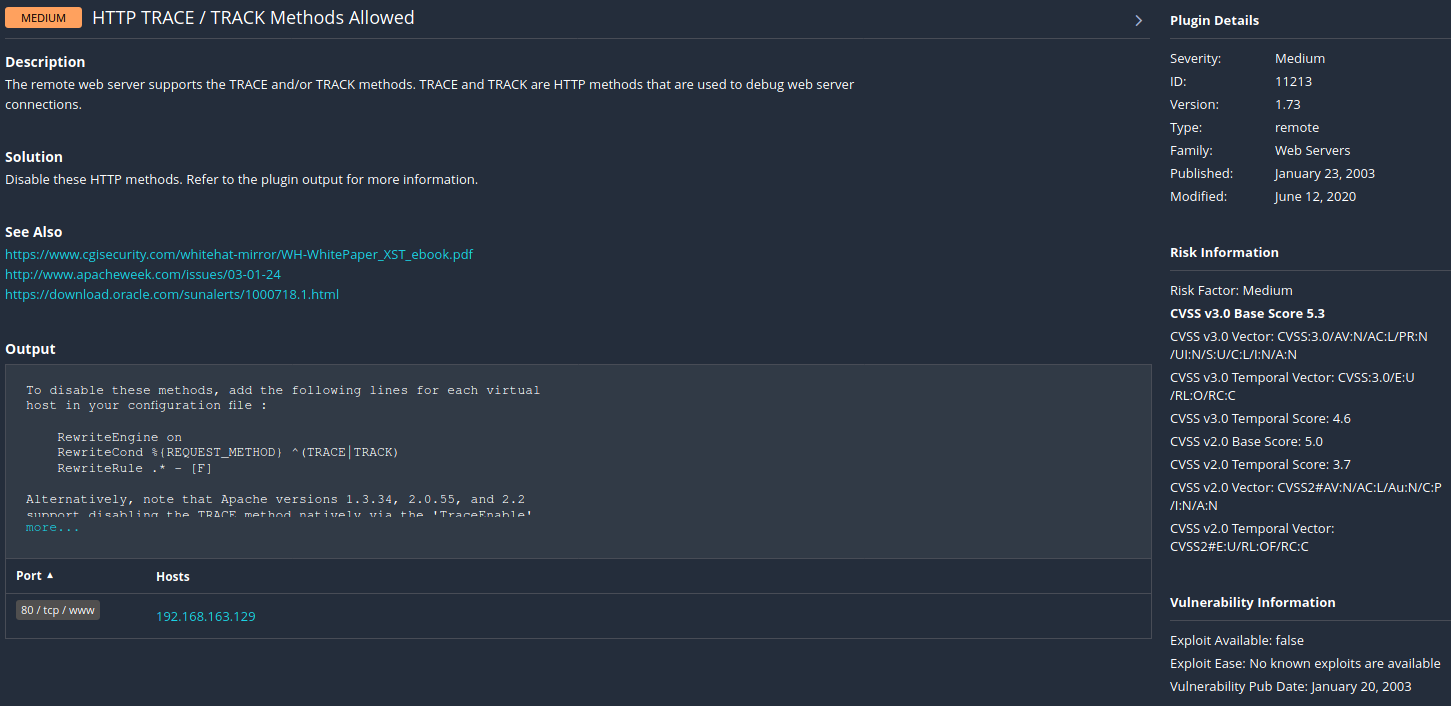


Figura 10 Métodos HTTP TRACE/TRACK permitidos.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería deshabilitar los métodos TRACE/TRACK de depuración web.

## Campo 1: Descripción

**Divulgación de información del encabezado ETag del servidor Apache**. Vulnerabilidad encontrada en el servidor web, ya que se puede obtener información confidencial del encabezado ETag, como el número de inodo de los archivos solicitados. Información que podría ayudar a un posible atacante.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

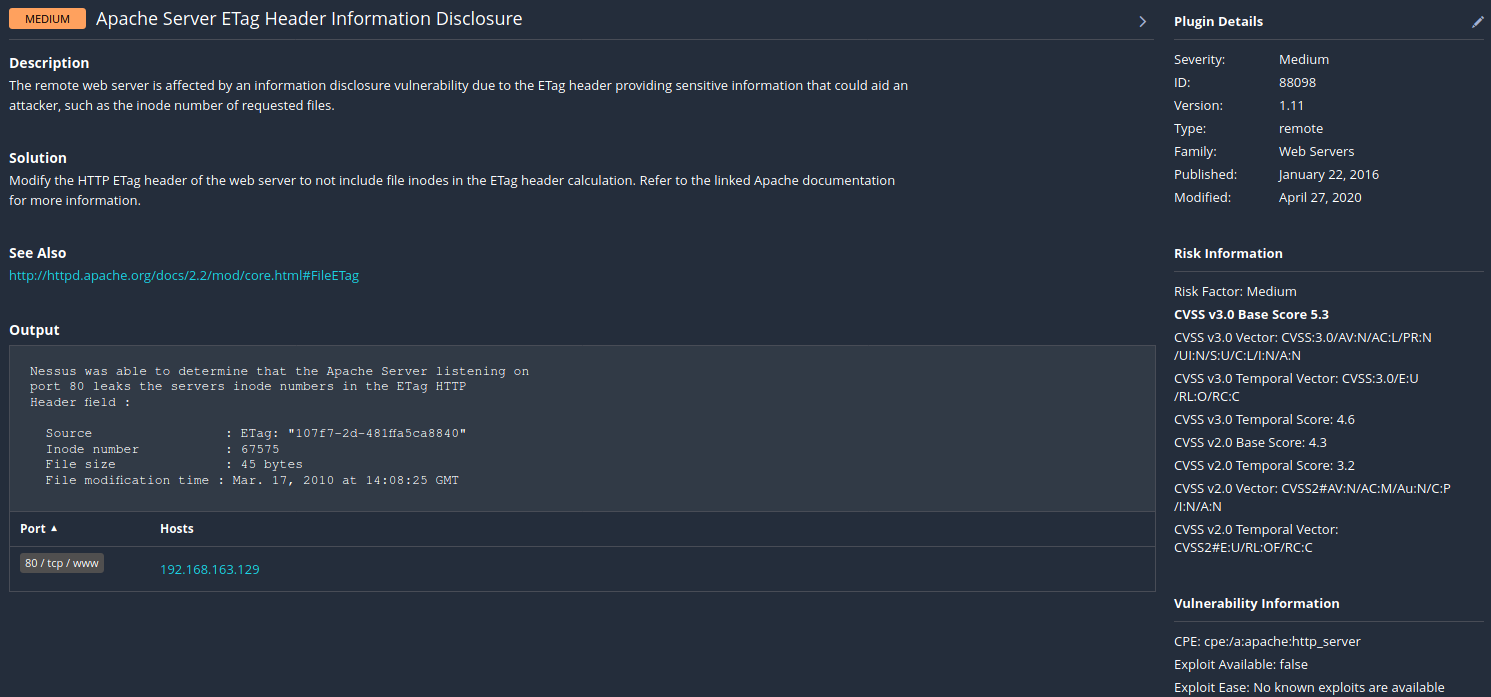


Figura 11 Divulgación de información confidencial del encabezado ETag.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería modificar el encabezado HTTP ETag del servidor web para no incluir inodos de archivo en el cálculo del encabezado ETag.

## Campo 1: Descripción

**Obtención de credenciales.** Vulnerabilidad encontrada por utilizar el mismo nombre del contenedor de servlets, tomcat.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con la herramienta **Nmap:**

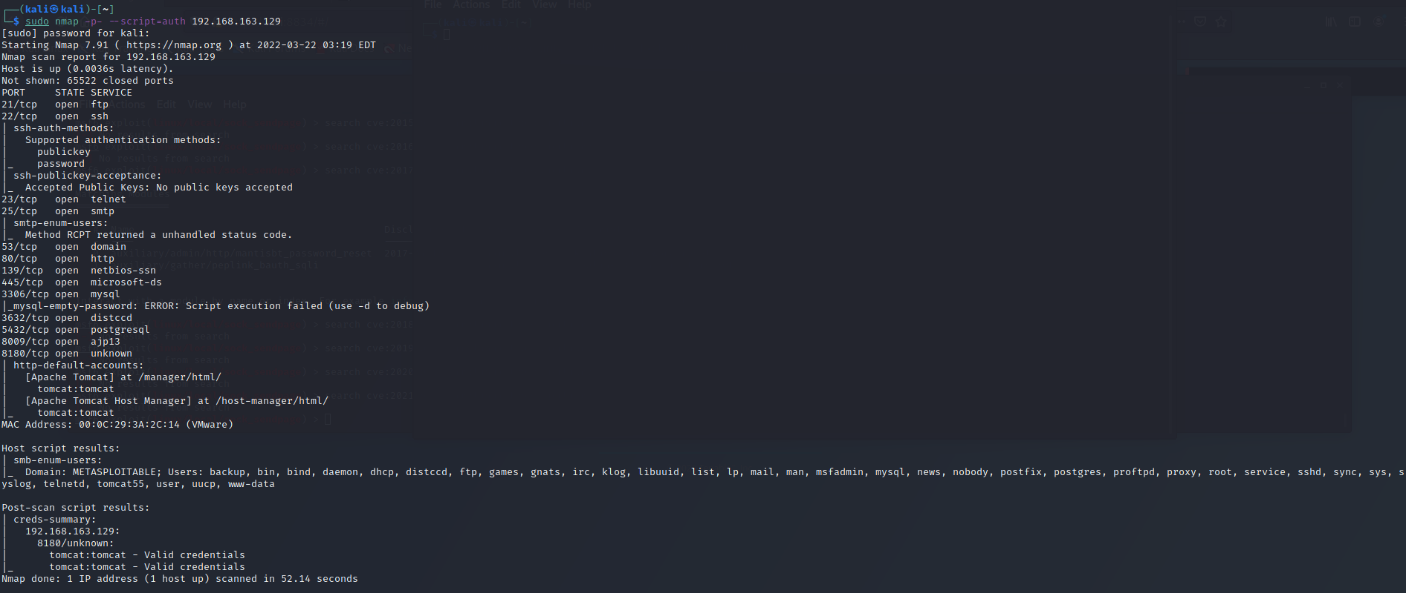


Figura 12 Obtención de posibles autenticaciones con Nmap.

Se ha lanzado un escaneo de todos los puertos con la utilización del script ***auth*** para comprobar una posible autenticación: ***sudo nmap –p- --script=auth 192.168.163.129***

Seguidamente se ha podido comprobar la autenticación abriendo una conexión por http con la máquina víctima y el puerto 8180:

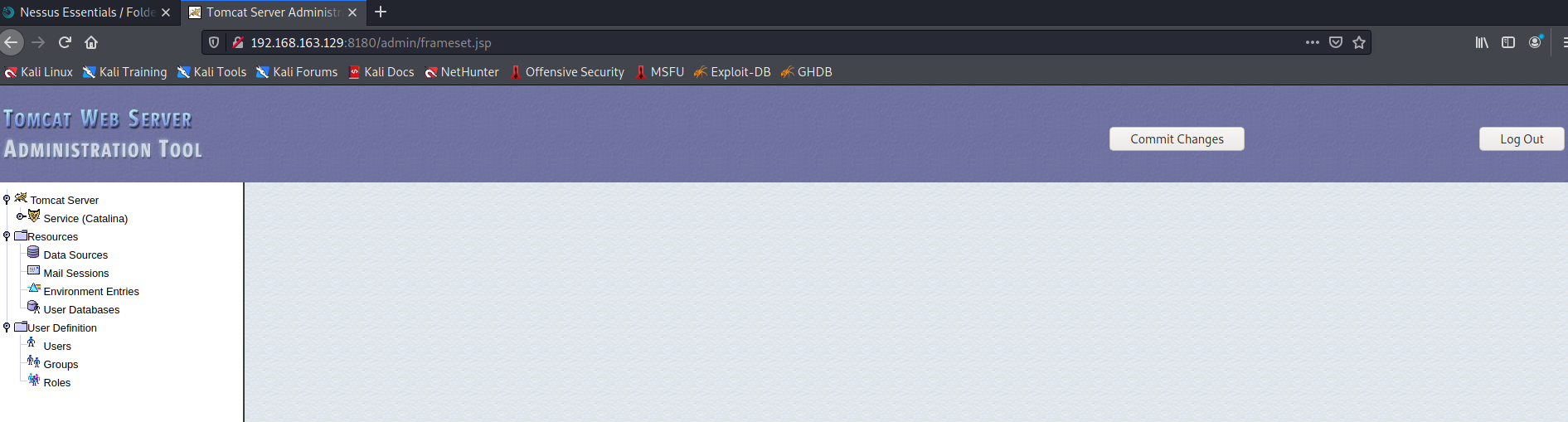


Figura 13 Autenticación administración Tomcat.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería modificar las credenciales de acceso a la herramienta Tomcat y utilizar unas credenciales más fuertes.

* **Vulnerabilidades software PostgreSQL (5432) y el protocolo SMTP (25):**

## Campo 1: Descripción

**Debilidad del generador de números aleatorios del paquete OpenSSH/OpenSSL de Debian**. Vulnerabilidad encontrada en el certificado x509 del protocolo SSL debido a un error en el generador de números aleatorios de la librería de OpenSSL de Ubuntu. El problema es debido a la falta de entropía en la versión utilizada de OpenSSL, lo cual permitiría a un posible atacante obtener fácilmente la clave privada de la conexión remota y utilizarla para descifrarla la comunicación.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **crítico**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

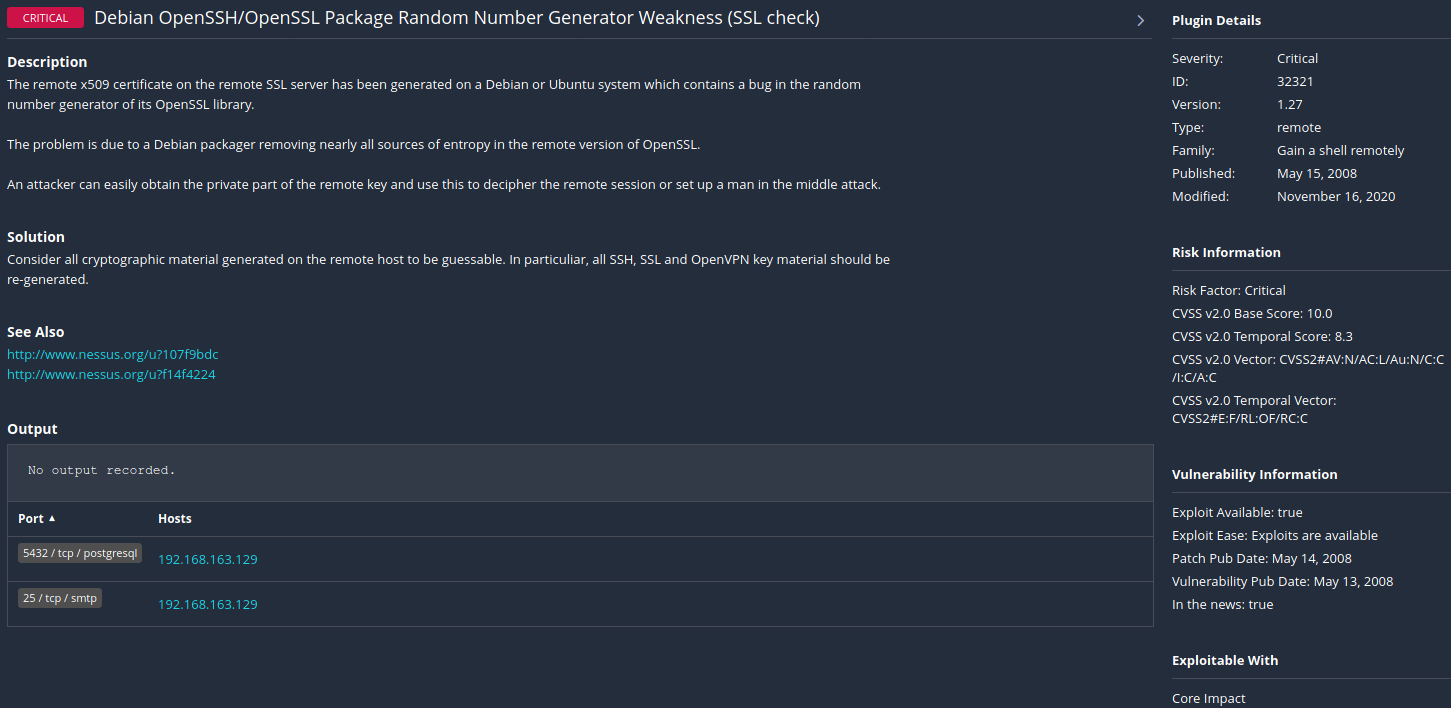
****

Figura 14 Debilidad en el generador de números aleatorios de OpenSSH/OpenSSL.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería regenerar todas las claves o contraseñas utilizadas para la comunicación remota, concretamente para los protocolos SSH, SSL y OpenVPN.

## Campo 1: Descripción

**Cifrado SSL de longitud menor a 112 bits o 3DES (fuerza media) soportado (SWEET32)**. Vulnerabilidad encontrada la el cifrado SSL el cual admite un cifrado de fuerza media con longitudes menores a 112 bits o 3DES. Implica una probabilidad más alta de descifrar una contraseña que al utilizar un cifrado de mayor fuerza.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **alto**.

## Campo 3: Explotación

Se ha obtenido esta vulnerabilidad con el escáner de vulnerabilidades **Nessus**:

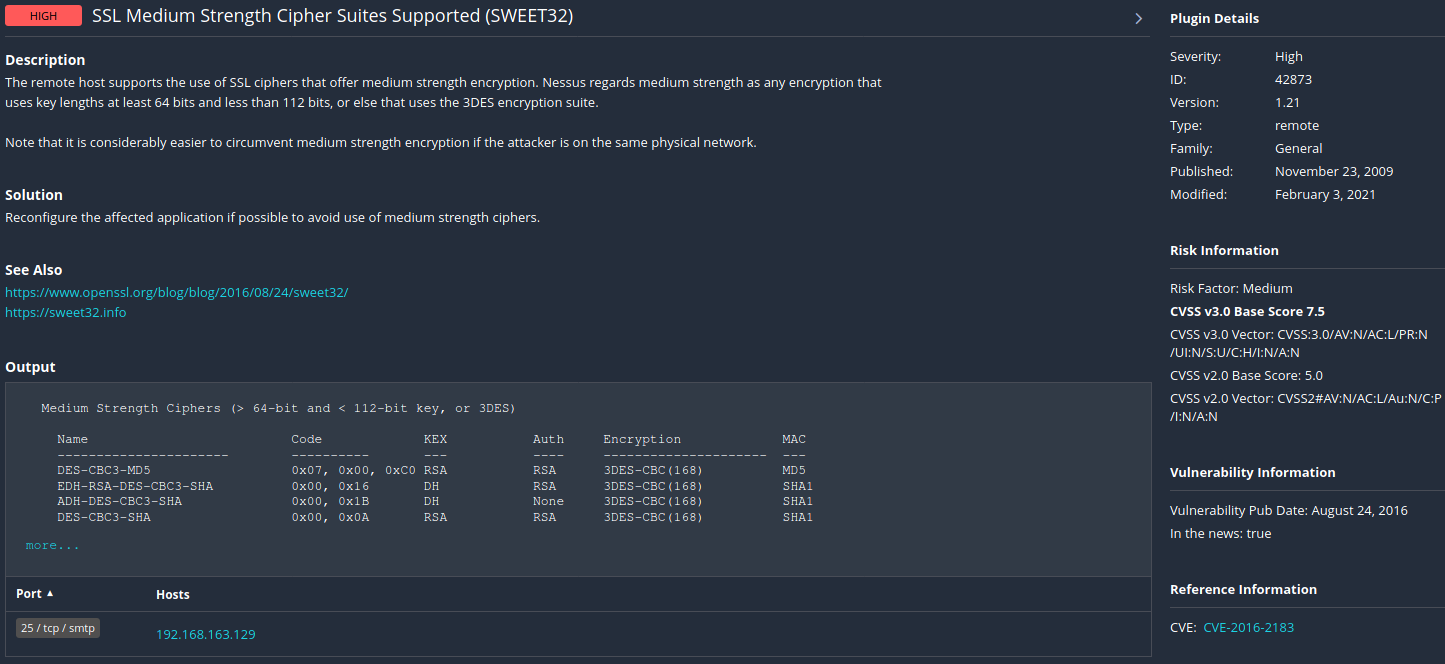
****

Figura 15 Cifrado de fuerza media en SSL.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería reconfigurar la aplicación afectada para solamente utilizar cifrados fuertes.

## Campo 1: Descripción

**Detección de las versiones 2 y 3 del protocolo SSL**. Vulnerabilidad encontrada en las versiones utilizadas para el cifrado de conexiones remotas. Tanto la versión 2 como la versión 3 tienen varios fallos de seguridad, como un esquema de relleno inseguro con cifrado CBC o esquemas inseguros de renegociación y reanudación de sesiones, que un posible atacante podría explotar y conseguir desencriptar la comunicación entre el servicio afectado y los clientes.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **alto**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

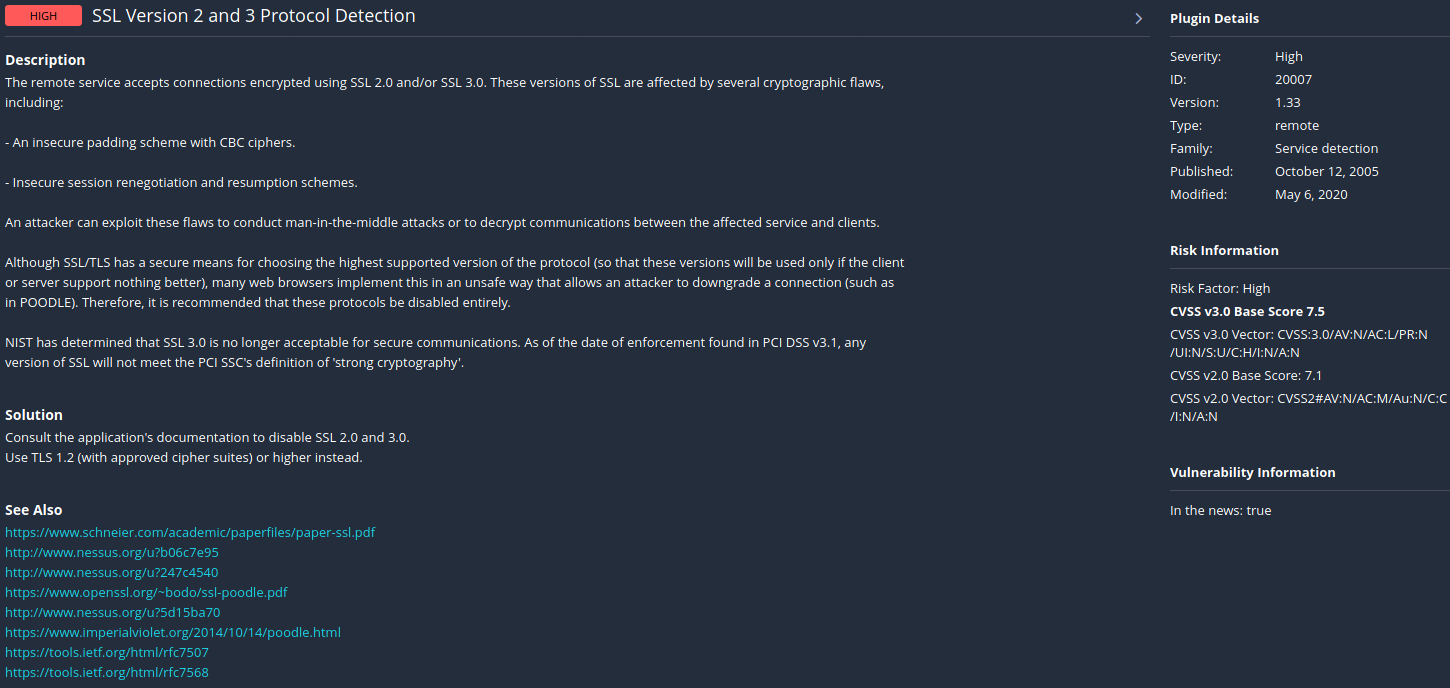
****

Figura 16 Versiones 2 y 3 de SSL.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería deshabilitar SSL 2.0 y 3.0 y utilizar en su lugar TLS 1.2 (con cifrados fuertes) o superior.

## Campo 1: Descripción

**Vulnerabilidad en el relleno del cifrado de Oracle en la versión SSLv3 (POODLE).** Vulnerabilidad existente en la versión 3 de SSL, la cual se debe a como maneja los bytes de relleno al descifrar mensajes cifrados mediante el cifrado de bloques. Un posible atacante que intercepta la conexión, podría descifrar un byte de un texto cifrado en tan solo 256 intentos en el caso de conseguir que una aplicación enviara repetidamente los mismos datos a través de nuevas conexiones SSLv3.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

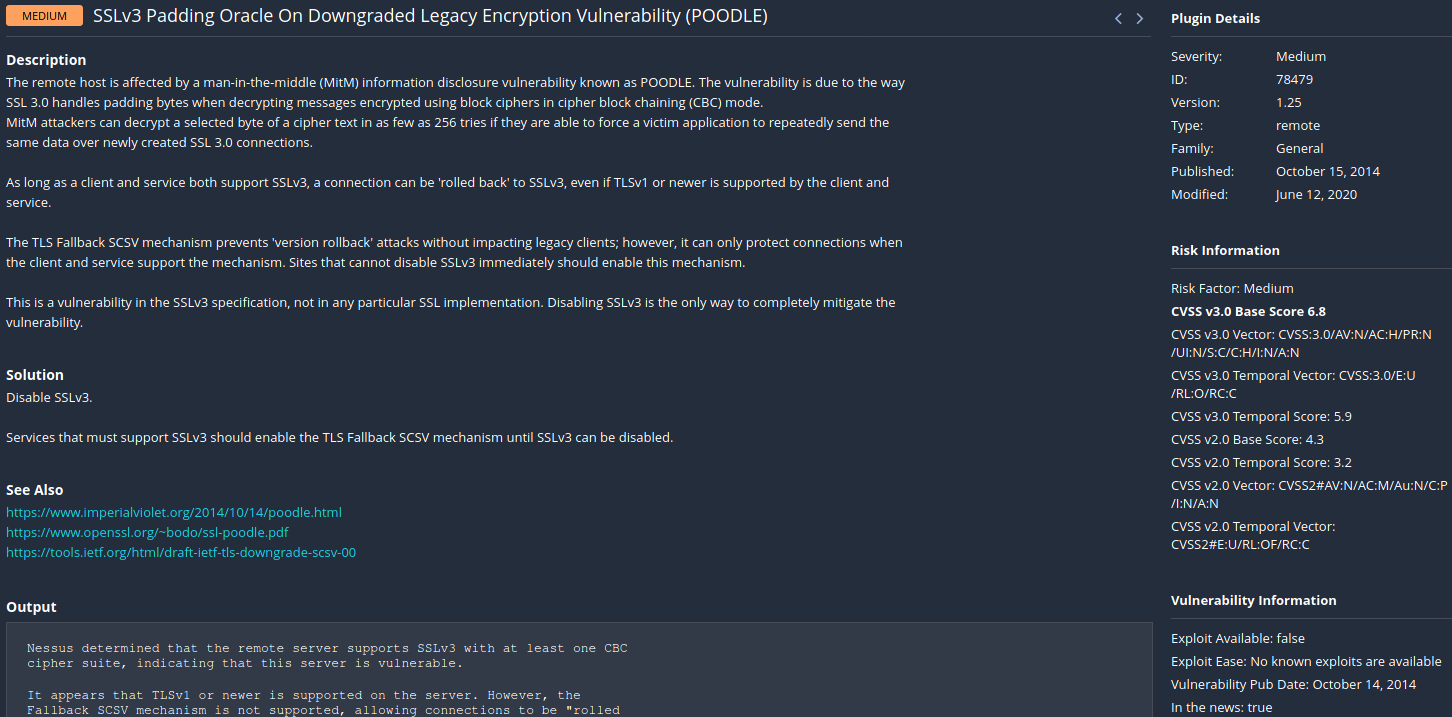
****

Figura 17 SSLv3 (POODLE).

Seguidamente se realizado una posible explotación de la vulnerabilidad utilizando la herramienta **Mestasploit**:

* Se ha buscado la vulnerabilidad por su referencia CVE: ***search cve-2014-3566***
* Se ha seleccionado el exploit: ***auxiliary/scanner/http/ssl\_version***
* Se configurado el exploit y se ha lanzado:

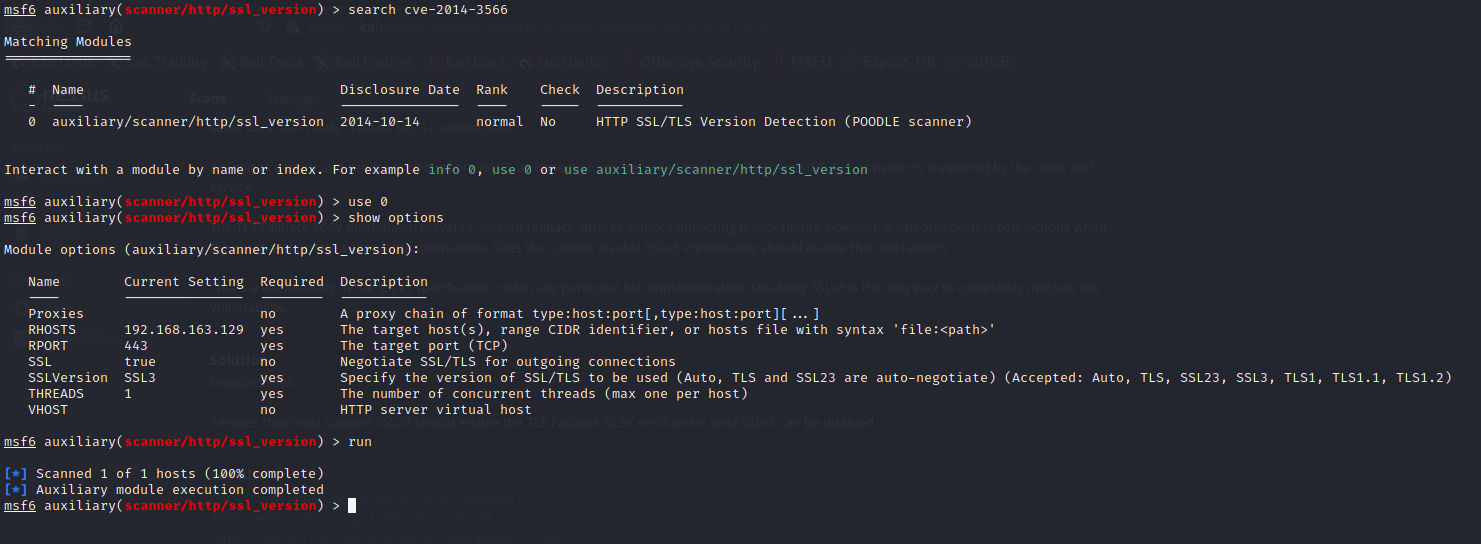


Figura 18 Explotación de la vulnerabilida POODLE.

En este caso se tendría que capturar el tráfico entre el host víctima y otra máquina de la misma red.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería deshabilitar SSLv3 y habilitar TLS Fallback SCSV en caso de no poder deshabilitar SSLv3.

## Campo 1: Descripción

**No se puede confiar en el certificado SSL**. Vulnerabilidad encontrada en la confianza del certificado SSL, la cual puede deberse a que no provenga de una autoridad de certificación pública conocida, que el certificado ya no sea válido o que la cadena de certificados contenga una firma que no coincide con la información del certificado o no se pueda verificar.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

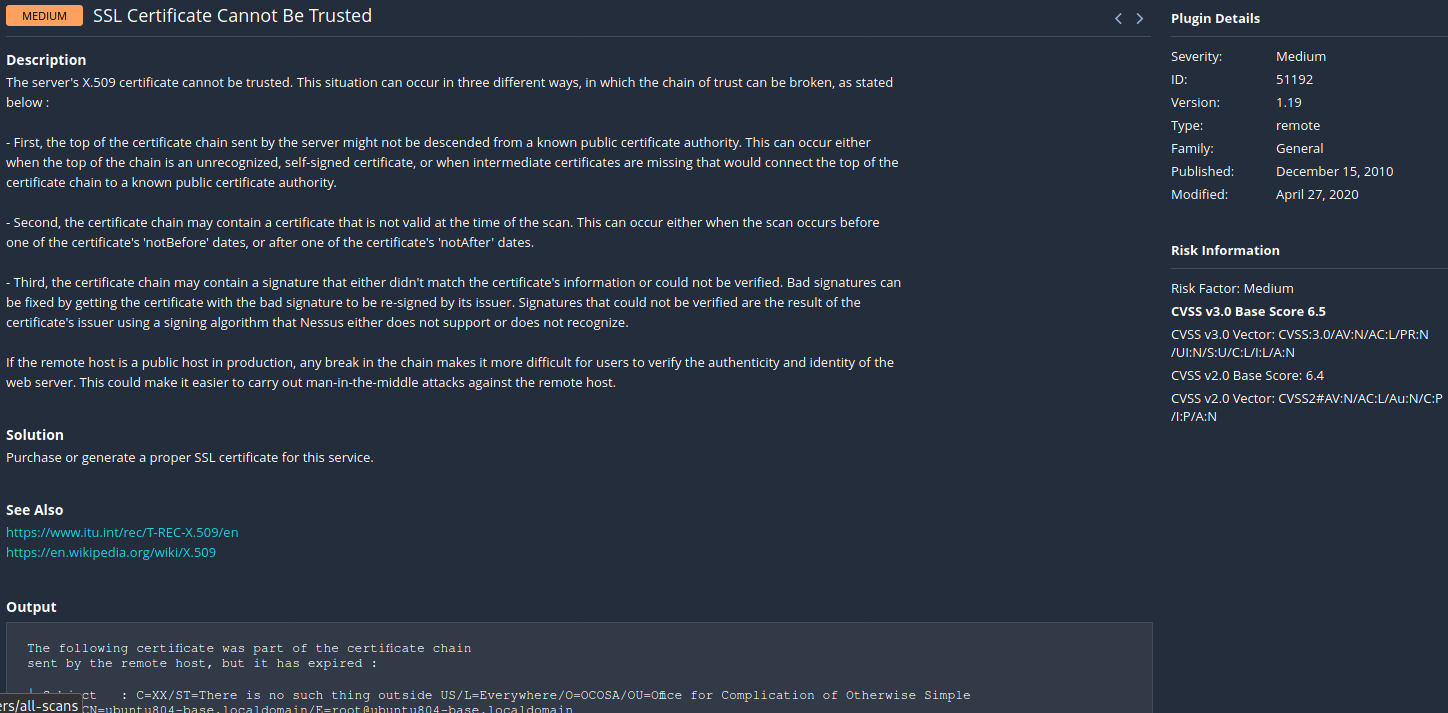
****

Figura 19 Certificado SSL inválido.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería comprar o generar un certificado SSL válido para este servicio.

## Campo 1: Descripción

**Certificado SSL autofirmado**. La cadena de certificados X.509 para este servicio no está firmada por una autoridad de certificación reconocida.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

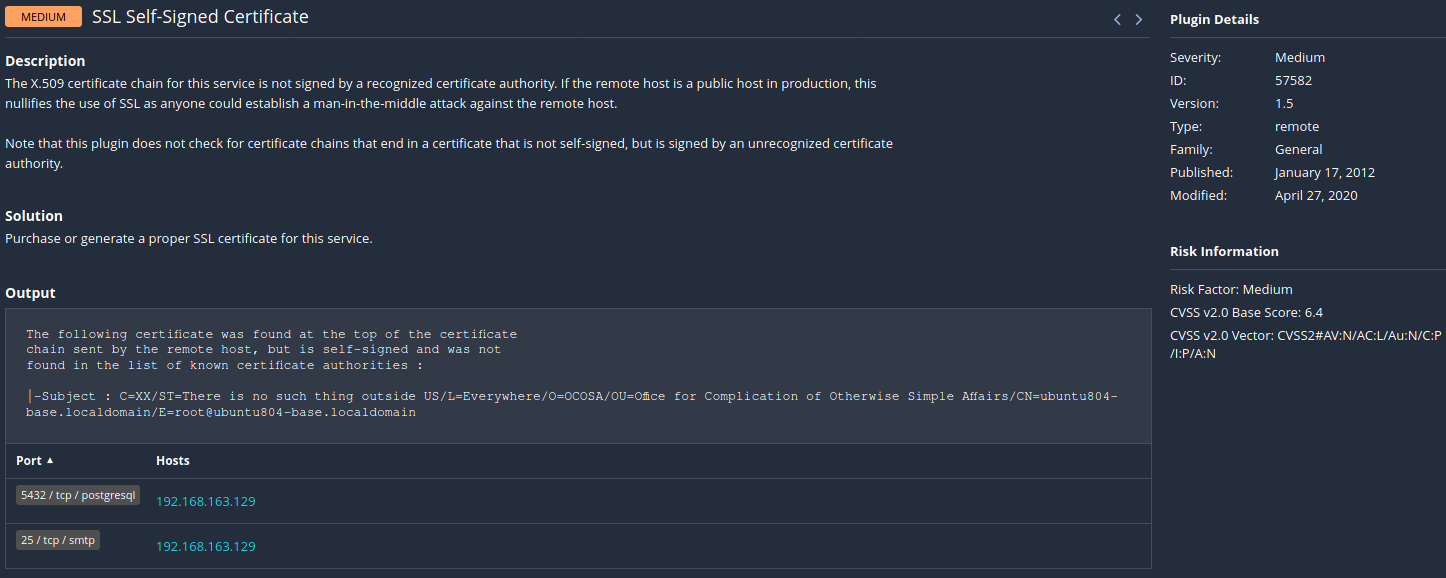
****

Figura 20 Certificado SSL autofirmado.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería comprar o generar un certificado SSL válido para este servicio.

## Campo 1: Descripción

**Cifrado SSL RC4 soportado (Bar Mitzvah)**. Vulnerabilidad en el uso del cifrado SSL RC4, el cual tiene problemas en la generación de flujo de bytes pseudoaleatorios con una disminución de su aleatoriedad. Un posible atacante podría descifrar los textos cifrados con este cifrado en el caso de obtener una gran cantidad (decenas de millones).

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

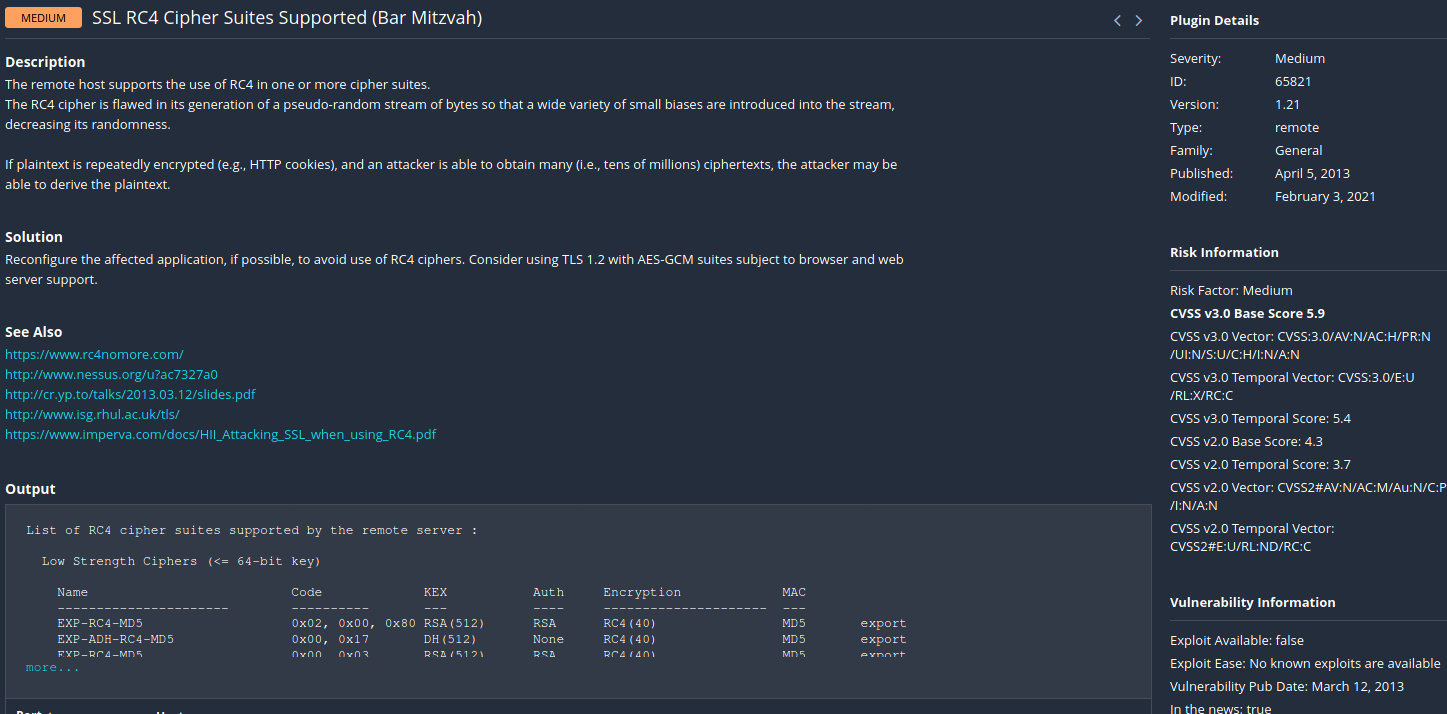
****

Figura 21 Cifrado SSL RC4 soportado.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería evitar el uso de cifrados RC4 y utilizar en su lugar TLS 1.2 con AES-GCM compatible con el navegador y servidor web.

## Campo 1: Descripción

**Certificado SSL caducado**. Vulnerabilidad encontrada en el certificado SSL por haber expirado, caducado.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

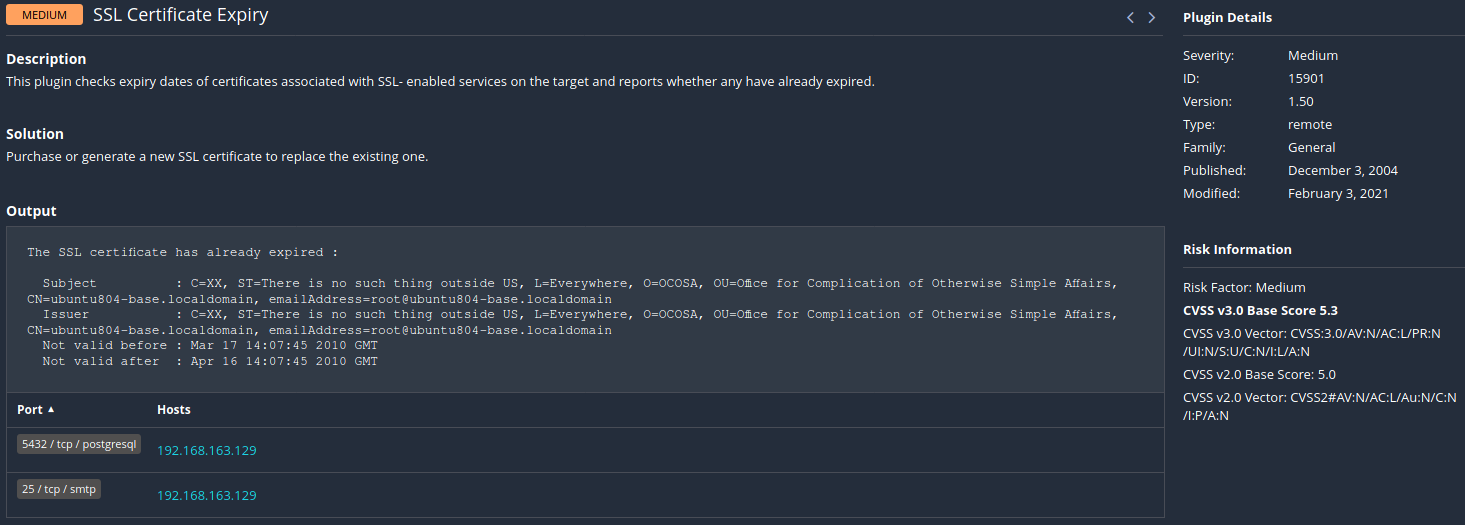
****

Figura 22 Certificado SSL caducado.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería comprar o generar un nuevo certificado SSL para reemplazar el existente.

## Campo 1: Descripción

**Certificado SSL con nombre de host incorrecto**. Vulnerabilidad encontrada en el atributo “*commonName*” (CN) del certificado SSL, donde se ha encontrado un nombre de máquina diferente.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

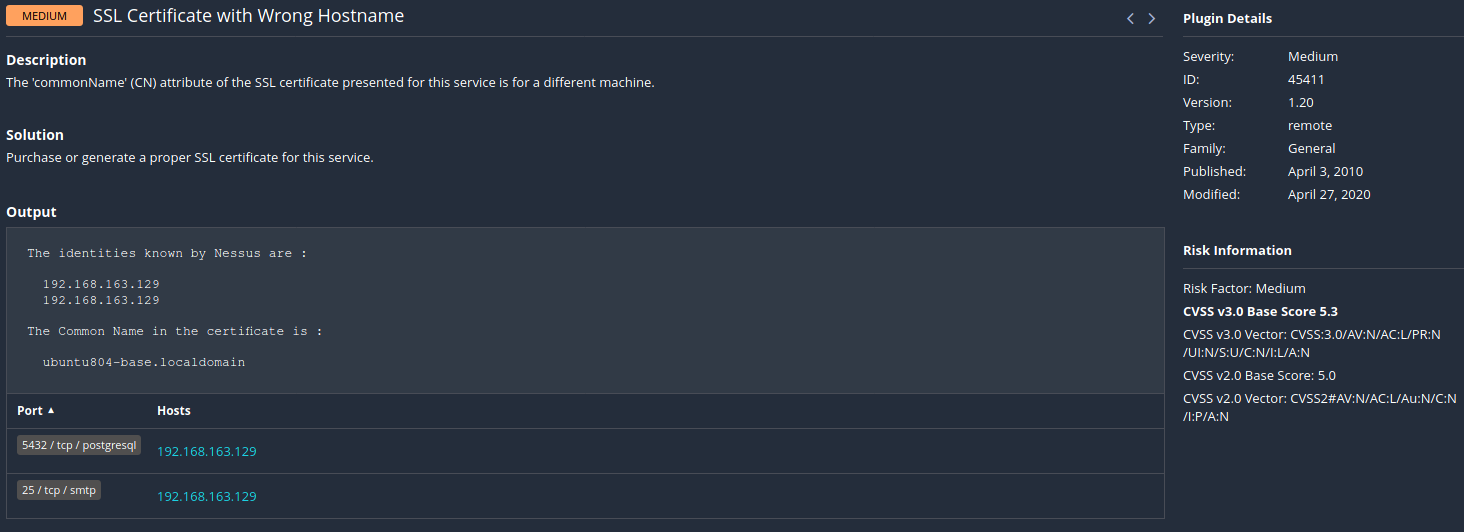
****

Figura 23 Certificado SSL con nombre de host incorrecto.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería comprar o generar un certificado SSL adecuado para este servicio.

## Campo 1: Descripción

**Cifrado débil SSL soportado**. Vulnerabilidad encontrada en el cifrado SSL, ya que admite un cifrado débil.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

****

Figura 24 Cifrado SSL débil soportado.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería configurar la aplicación afectada para evitar el uso de cifrados débiles.

## Campo 1: Descripción

**Cifrado SSL anónimo soportado**. Vulnerabilidad encontrada en el cifrado SSL, el cual admite el uso de cifrados SSL anónimos, lo cual permite que un administrador configure un servicio que encripta el tráfico sin tener que generar y configurar certificados SSL, no ofrece ninguna forma de verificar la identidad del host remoto y hace que el servicio sea vulnerable a un ataque de MiM.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

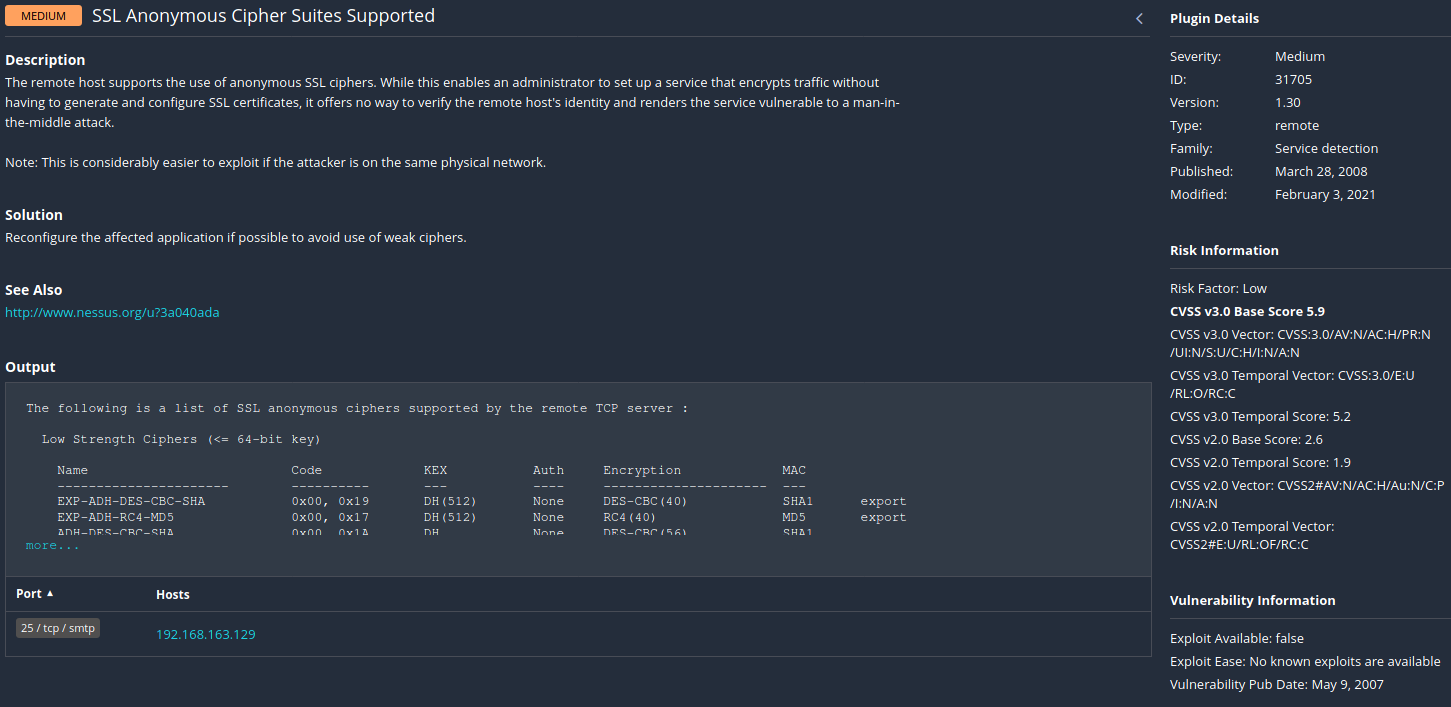
****

Figura 25 Cifrado SSL anónimo soportado.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería configurar la aplicación afectada si es posible, para evitar el uso de cifrados débiles.

## Campo 1: Descripción

**Versión 1.0 del protocolo TLS**. Vulnerabilidad encontrada en la versión instalada del protocolo TLS, versión 1.0 la cual tiene defectos de diseño criptográfico.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

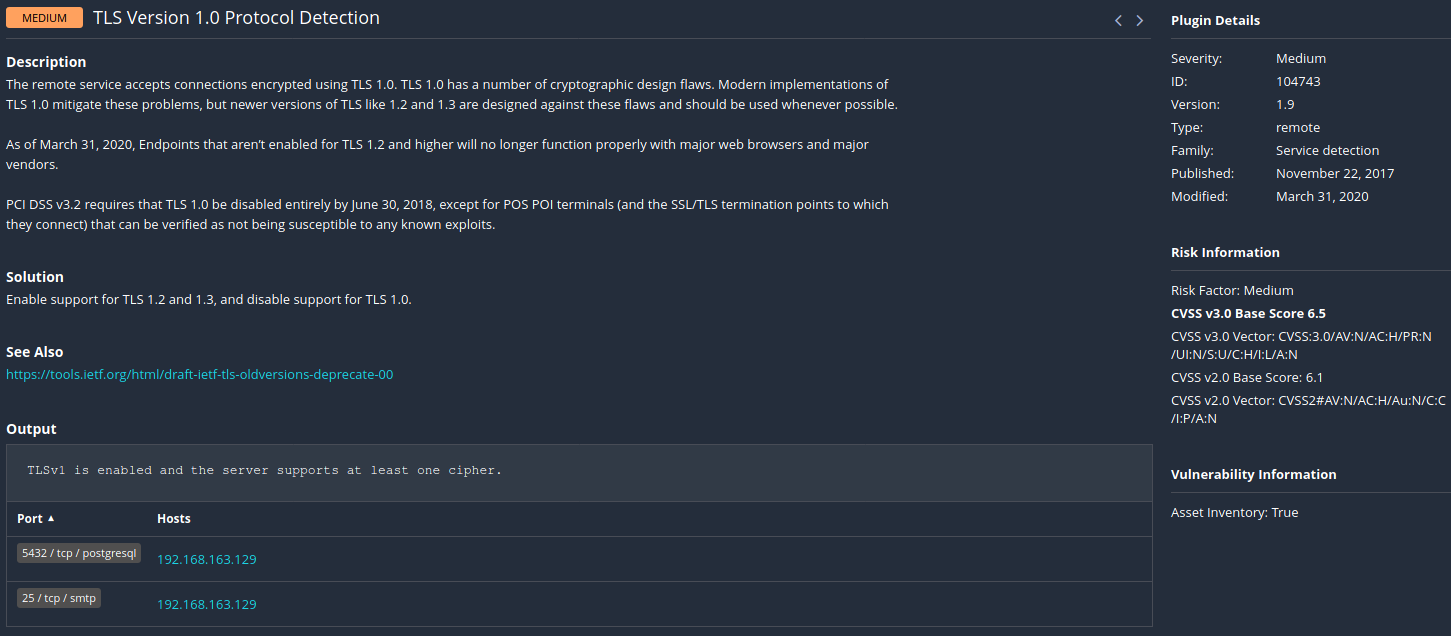
****

Figura 26 Versión 1.0 protocolo TLS.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería deshabilitar la compatibilidad con la versión 1.0 y habilitar la compatibilidad con las versiones de TLS 1.2 y 1.3.

## Campo 1: Descripción

**Vulnerabilidad de ataque SSL Drown (descifrado de RSA con un cifrado débil y obsoleto)**. Vulnerabilidad encontrada porque el equipo es compatible con la versión SSL2, la cual tiene un problema en la implementación y permite descifrar el tráfico TLS capturado. Un posible atacante (MiM) podría explotar este problema, para descifrar la conexión TLS utilizando el tráfico capturado previamente con una débil encriptación, junto con una serie de conexiones especialmente diseñadas a un servidor SSLv2 que usa la misma clave privada..

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

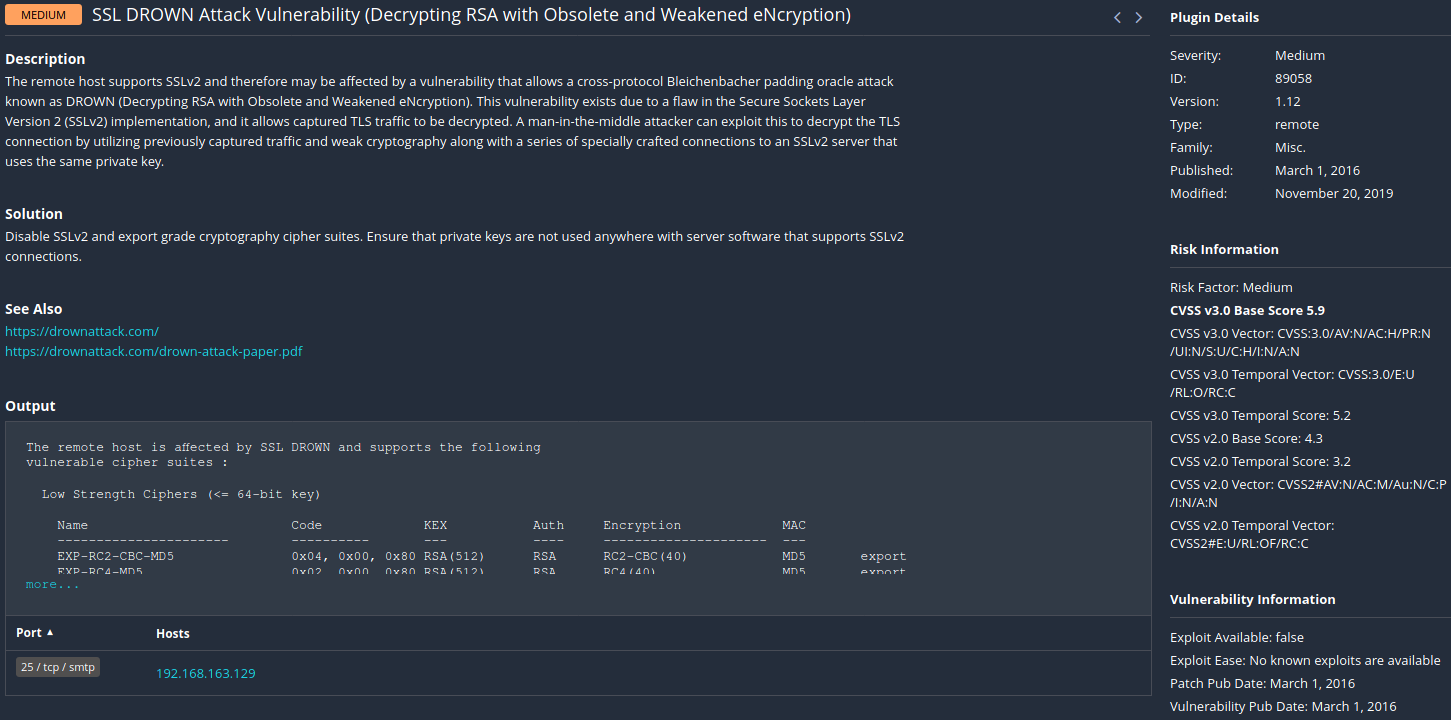
****

Figura 27 Vulnerabilidad en SSLv2 por ataque DROWN.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería deshabilitar SSLv2.

## Campo 1: Descripción

**Problema en la reanudación de sesión OpenSSL debido a una degradación del conjunto de cifrado (SSL\_OP\_NETSCAPE\_REUSE\_CIPHER\_CHANGE\_BUG)**. Vulnerabilidad encontrada en la versión de OpenSSL, debido a que permite reanudar la sesión con un cifrado débil que el utilizado cuando se inició la sesión. Un posible atacante que haya interceptado el inicio de sesión, podría manipular la memoria caché de la sesión de OpenSSL para hacer que las reanudaciones posteriores de esa sesión utilicen un cifrado más débil elegido por el atacante.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

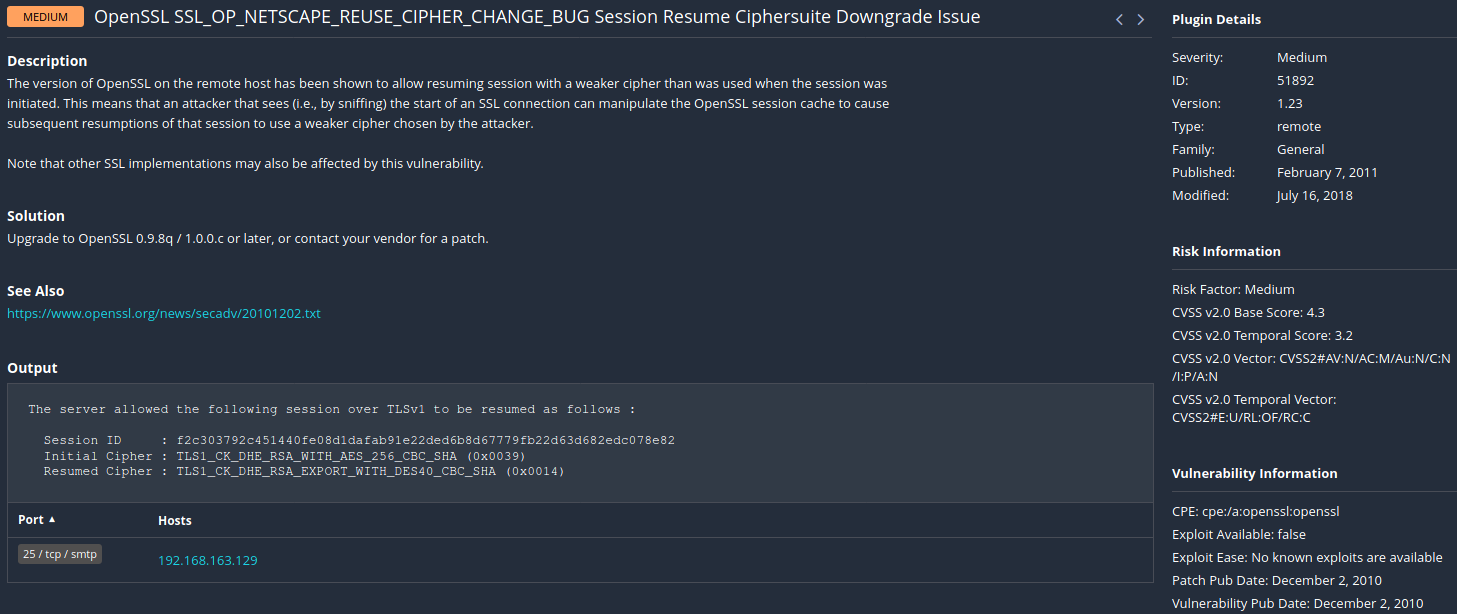


Figura 28 Vulnerabilidad OpenSSL reanudar sesión.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería actualizar la versión de OpenSSL a la 0.9.8q/1.0.0.co o buscar un parche para esta vulnerabilidad.

## Campo 1: Descripción

**Inyección de datos de texto sin formato en la renegociación del *handshakes* SSL/TLS***.* Vulnerabilidad encontrada en la encriptación TLS/SSL ya que permite que un cliente pueda reconectar de manera insegura después del protocolo de enlace inicial. Un posible atacante podría inyectar una cantidad arbitraria de texto sin formato al comienzo del flujo del protocolo de la aplicación, lo que podría facilitar los ataques intermediarios.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

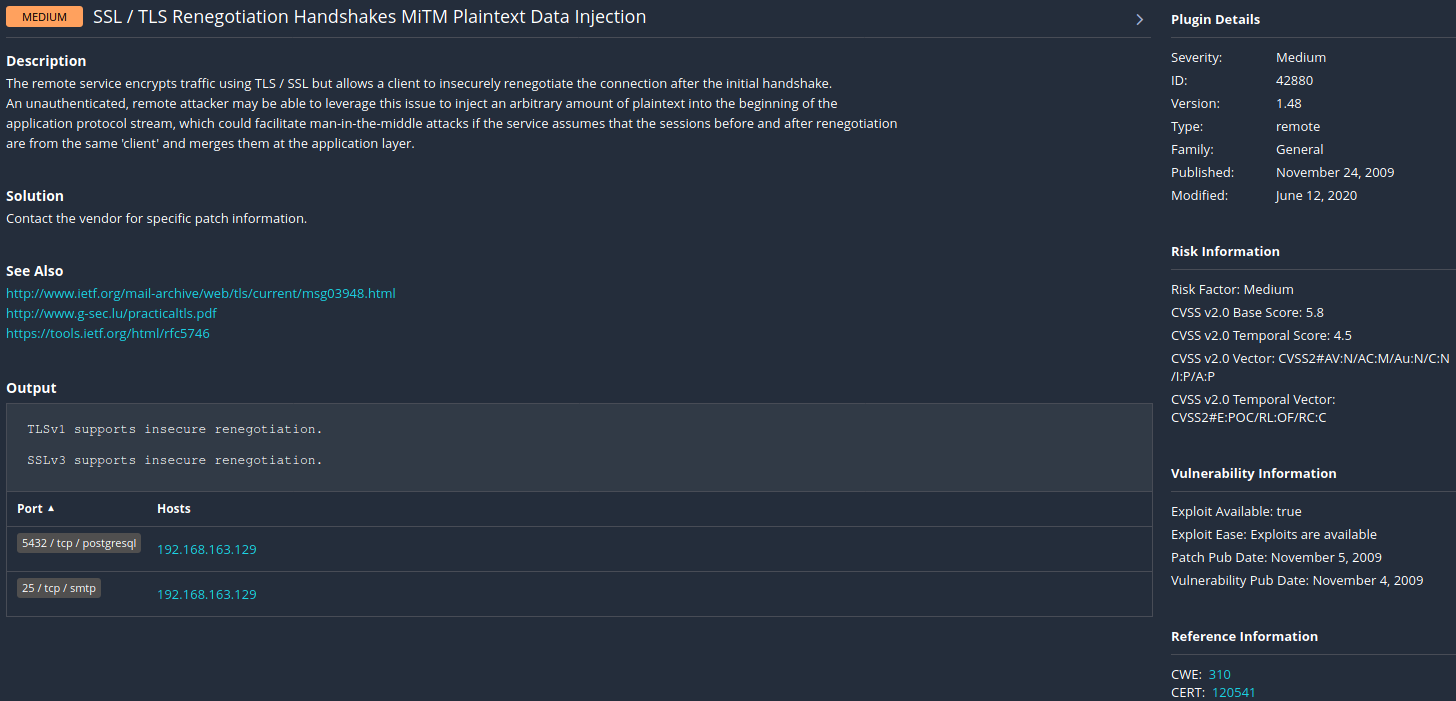


Figura 29 Inyección de código en la renegociación SSL/TLS.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería contactar con el proveedor para obtener información sobre un posible parche.

## Campo 1: Descripción

**Cifrado SSL/TLS EXPORT\_RSA <= 512-bit soportado (FREAK)**. Vulnerabilidad encontrada en el cifrado SSL/TLS el cual admite un cifrado EXPORT\_RSA con claves menores o iguales a 512 bits. El cual se puede obtener con un período corto de tiempo.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

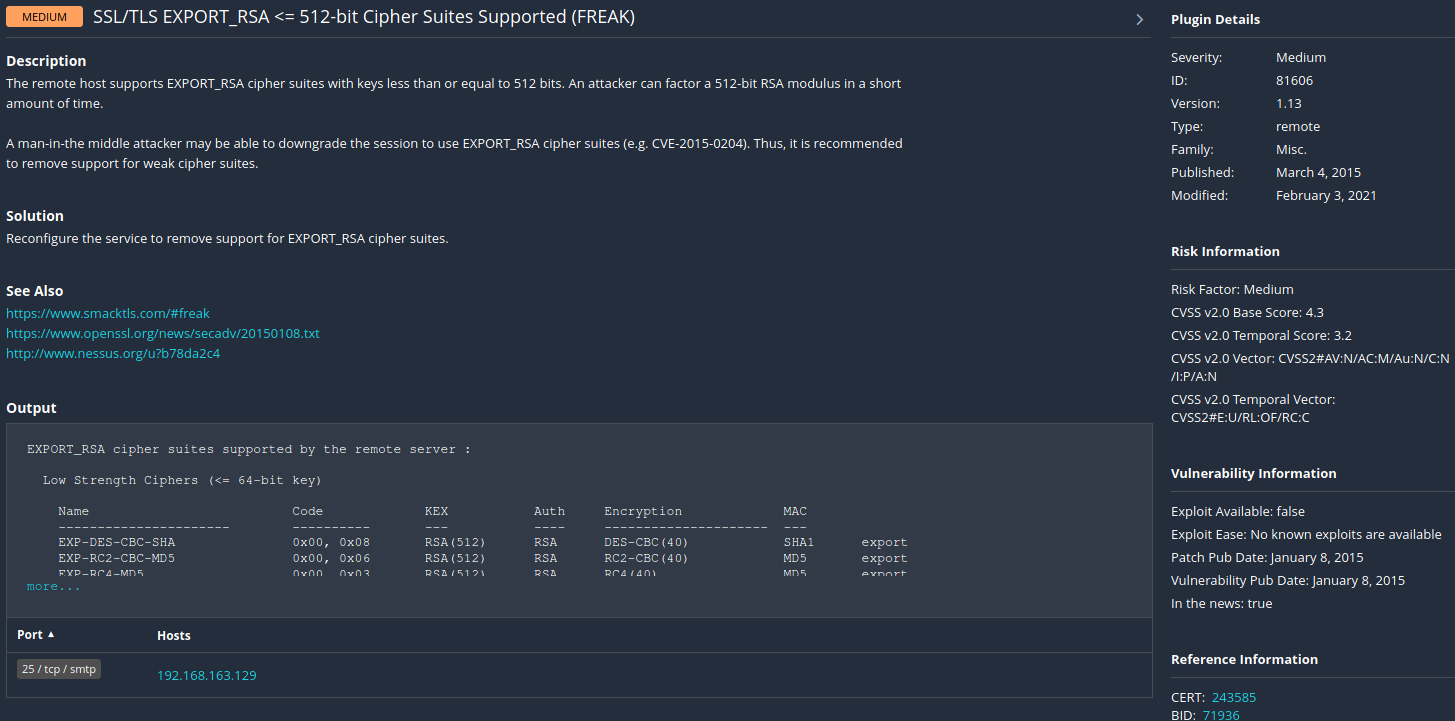


Figura 30 Cifrado SSL/TLS menor o igual a 512.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería eliminar la compatibilidad con el cifrado EXPORT\_RSA.

## Campo 1: Descripción

**Inyección de comandos de texto sin formato en el servicio SMTP STARTTLS**. Vulnerabilidad encontrada en el servicio remoto SMTP, STARTTLS, en el cual un usuario no autenticado podría inyectar comandos durante la fase del protocolo de texto sin formato que se ejecutará durante la fase del protocolo de texto cifrado. Un posible atacante podría explotar esta vulnerabilidad y robar el correo electrónico de la víctima o las credenciales SASL asociadas.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

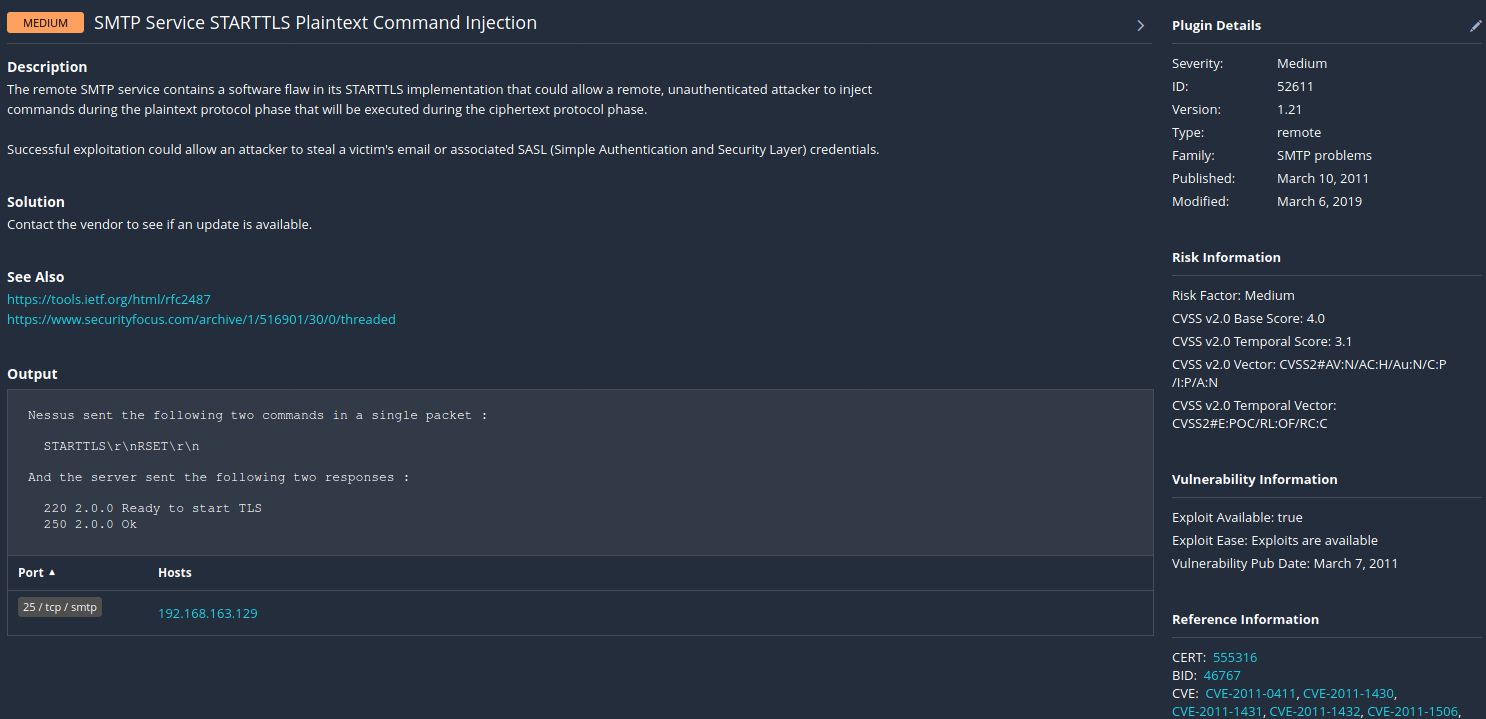


Figura 31 Inyección de código en el servicio SMTP STARTTLS.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería contactar con el proveedor para conseguir aplicar una actualización.

## Campo 1: Descripción

**Cifrados SSL/TLS EXPORT\_DHE <= 512 bits (Logjam) soportados**. Vulnerabilidad encontrada en los cifrados soportados, concretamente en la admisión del cifrado EXPORT\_DHE con claves menores o iguales a 512 bits, lo cual son cifrados débiles que pueden ser descifrados en poco tiempo por un posible atacante MiM.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **bajo**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

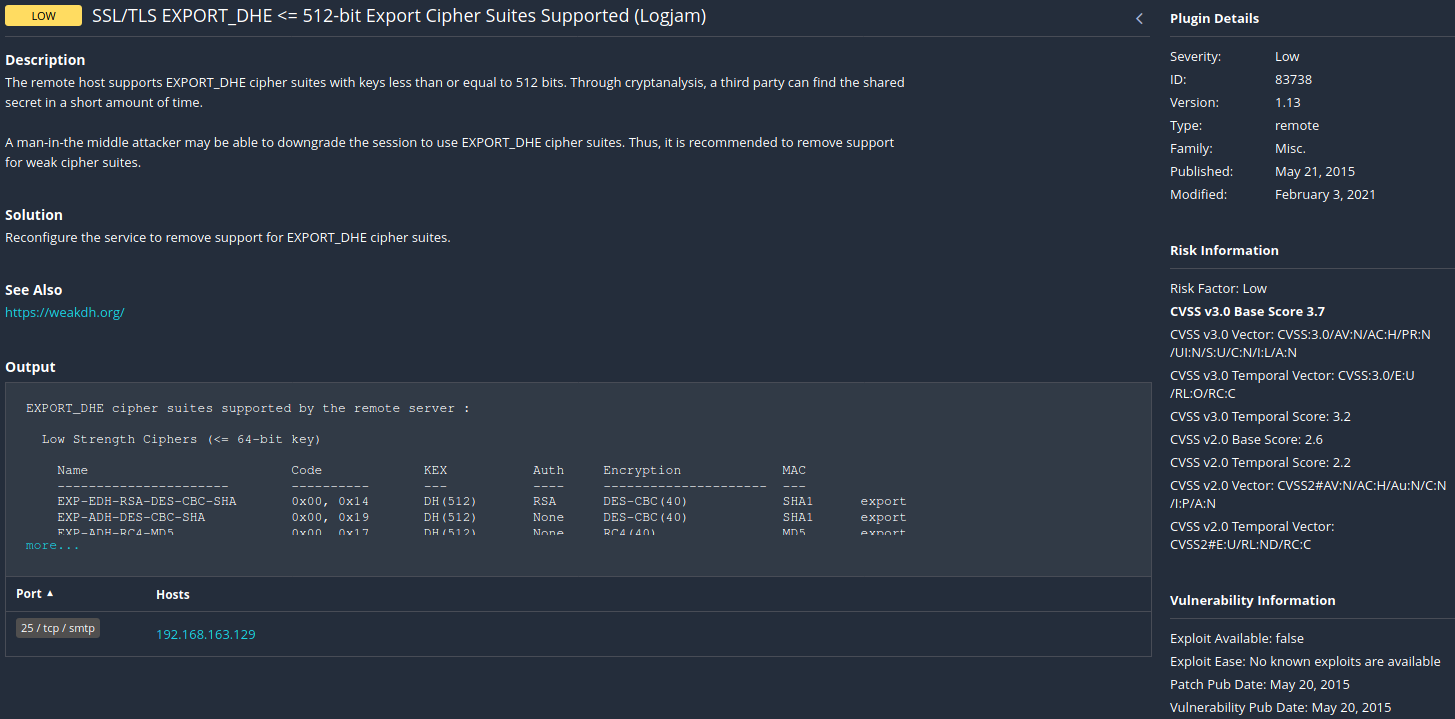


Figura Cifrados EXPORT\_DHE.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería configurar el servicio para eliminar la compatibilidad con el conjunto de cifrado EXPORT\_DHE.

* **Vulnerabilidades protocolo SSH puerto 22:**

## Campo 1: Descripción

**Debilidad del generador de números aleatorios del paquete OpenSSH/OpenSSL de Debian.** Vulnerabilidad encontrada en la clave de la conexión SSH debido a un error en el generador de números aleatorios de la librería de OpenSSL de Ubuntu. El problema es debido a la falta de entropía en la versión utilizada de OpenSSL, lo cual permitiría a un posible atacante obtener fácilmente la clave privada de la conexión remota y utilizarla para descifrarla la comunicación.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **crítico**.

## Campo 3: Explotación

Se ha obtenido esta vulnerabilidad con el escáner de vulnerabilidades **Nessus**:

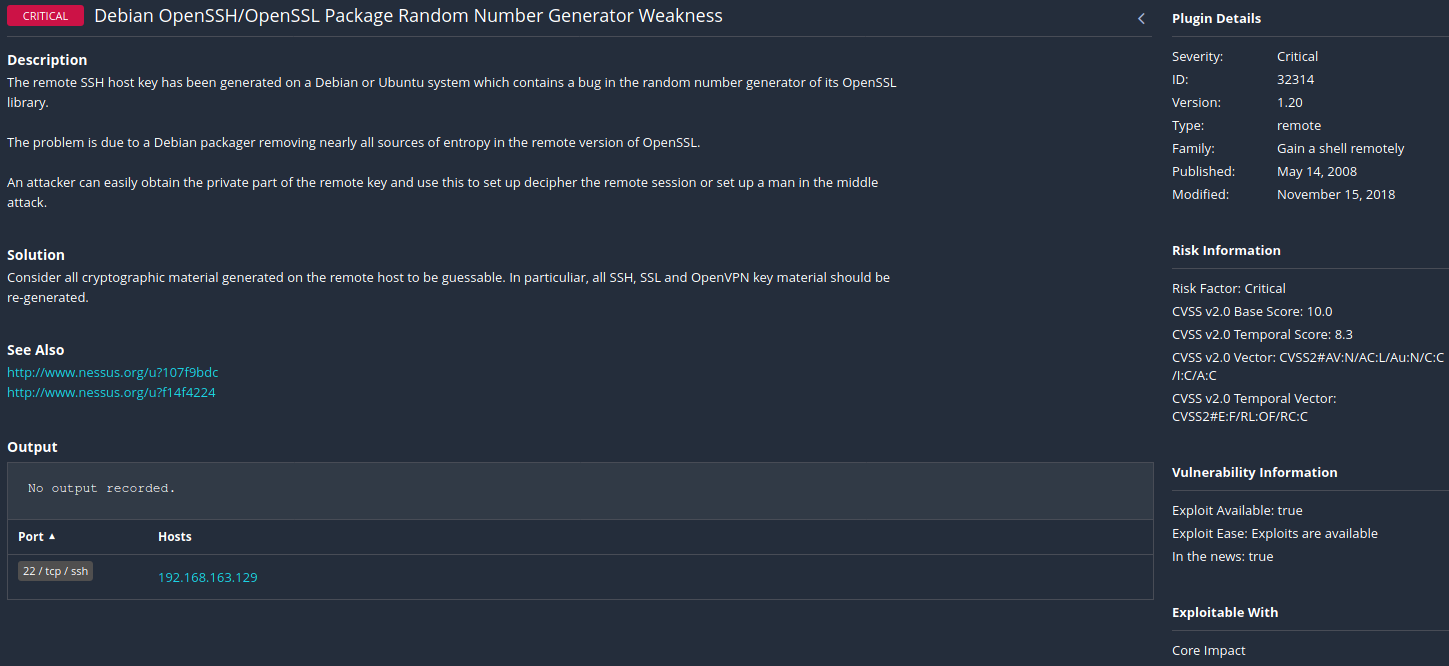
****

Figura 33 Vulnerabilidad encontrada en el generador de números aleatorios OpenSSH/SSL.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería regenerar todas las claves o contraseñas utilizadas para la comunicación remota, concretamente para los protocolos SSH, SSL y OpenVPN.

## Campo 1: Descripción

**Admisión de algoritmos débiles en el protocolo SSH**. Vulnerabilidad encontrada en la configuración del cifrado del servidor SSH, la cual está configurada para usar cifrado *Arcfour* o ningún cifrado. Según la RFC 4253 se desaconseja el uso de *Arcfour* debido a un problema con claves débiles.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

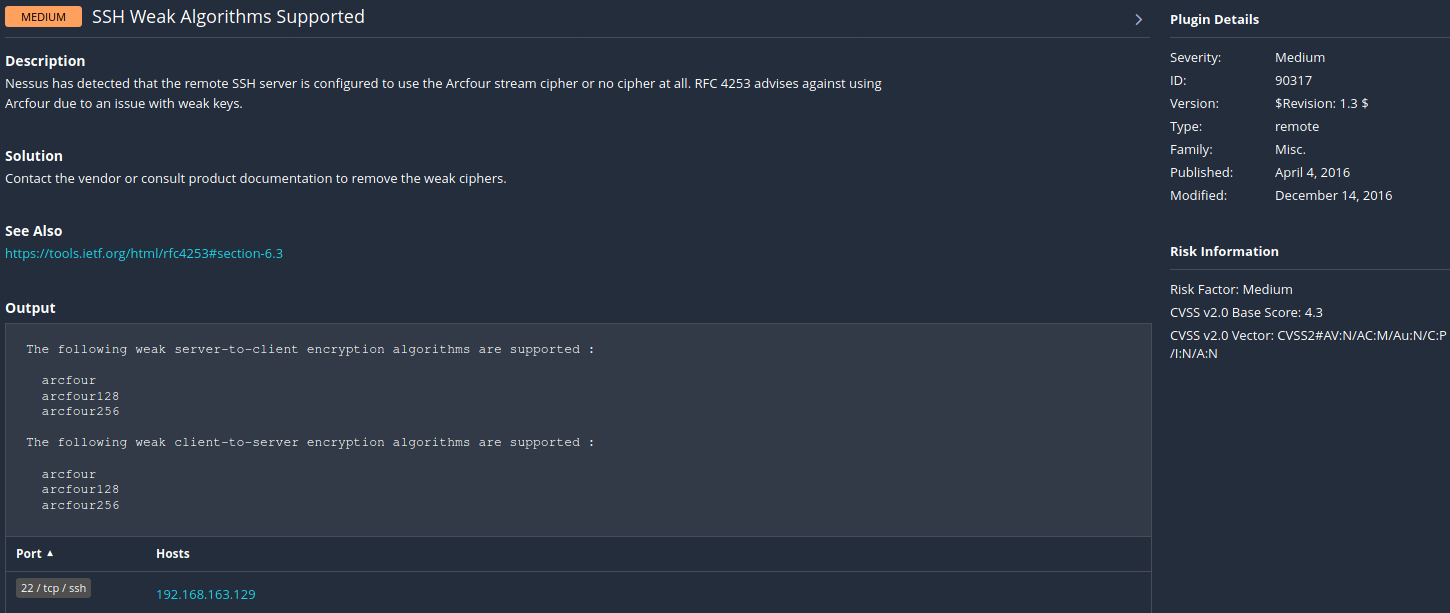


Figura 34 Algoritmos débiles soportados en SSL.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería contactar con el proveedor o consultar la documentación para eliminar los cifrados débiles.

## Campo 1: Descripción

**Algoritmo de intercambio de claves débiles SSH habilitado**. Vulnerabilidad encontrada en la configuración del servidor SSH, el cual está configurado para permitir el intercambio de claves que se consideran débiles.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **bajo**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

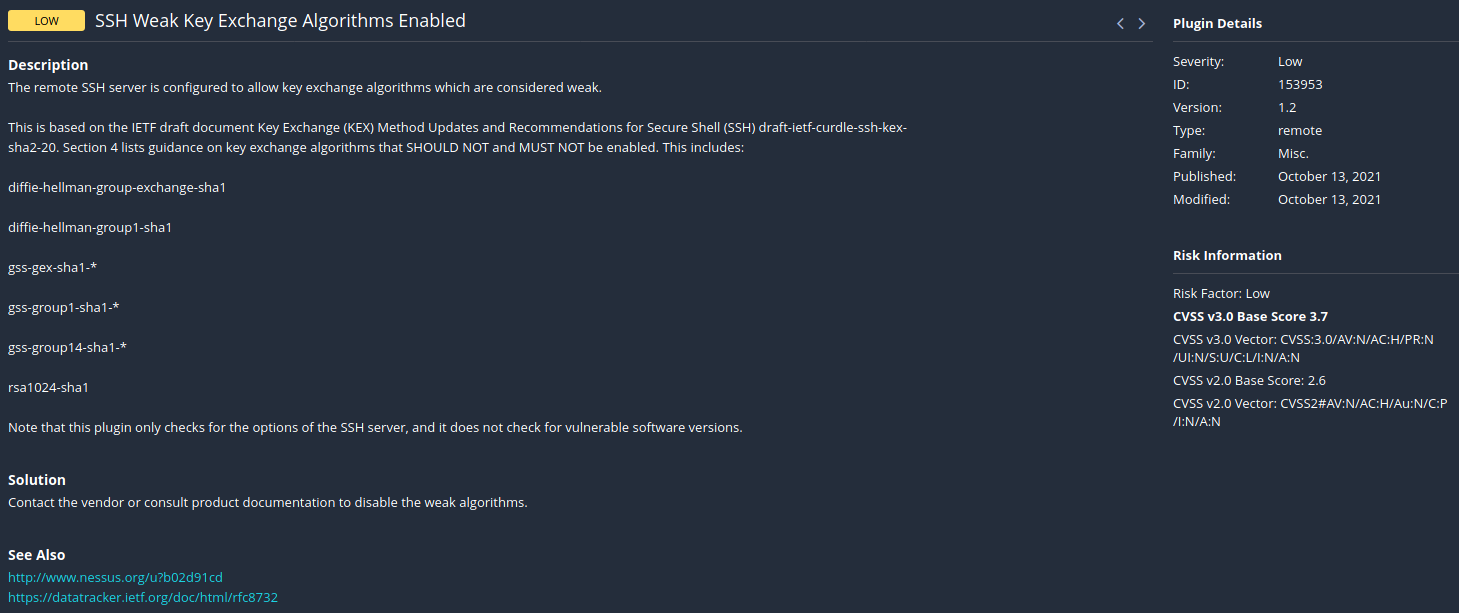


Figura 35 Algoritmo de intercambio de claves débiles SSH habilitado.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería contactar con el proveedor o consultar la documentación para deshabilitar los algoritmos débiles.

## Campo 1: Descripción

**Modos de cifrado CBC del servidor SSH habilitados**. Vulnerabilidad encontrada en la configuración del servidor SSH, el cual está configurado para admitir el cifrado *Cipher Block Chaining* (CBC), lo cual puede permitir que un posible atacante pueda recuperar el mensaje de texto sin formato del texto cifrado.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **bajo**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:



Figura Cifrado CBC servidor SSH.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería contactar con el proveedor o consultar la documentación para deshabilitar el cifrado en modo CBC y habilitar el cifrado en modo CTR o GCM.

## Campo 1: Descripción

**Algoritmos MAC débiles de SSH habilitados**. Vulnerabilidad encontrada en la configuración del servidor SSH, la cual permite algoritmos MD5 o MAC de 96 bits, los cuales se consideran débiles.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **bajo**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

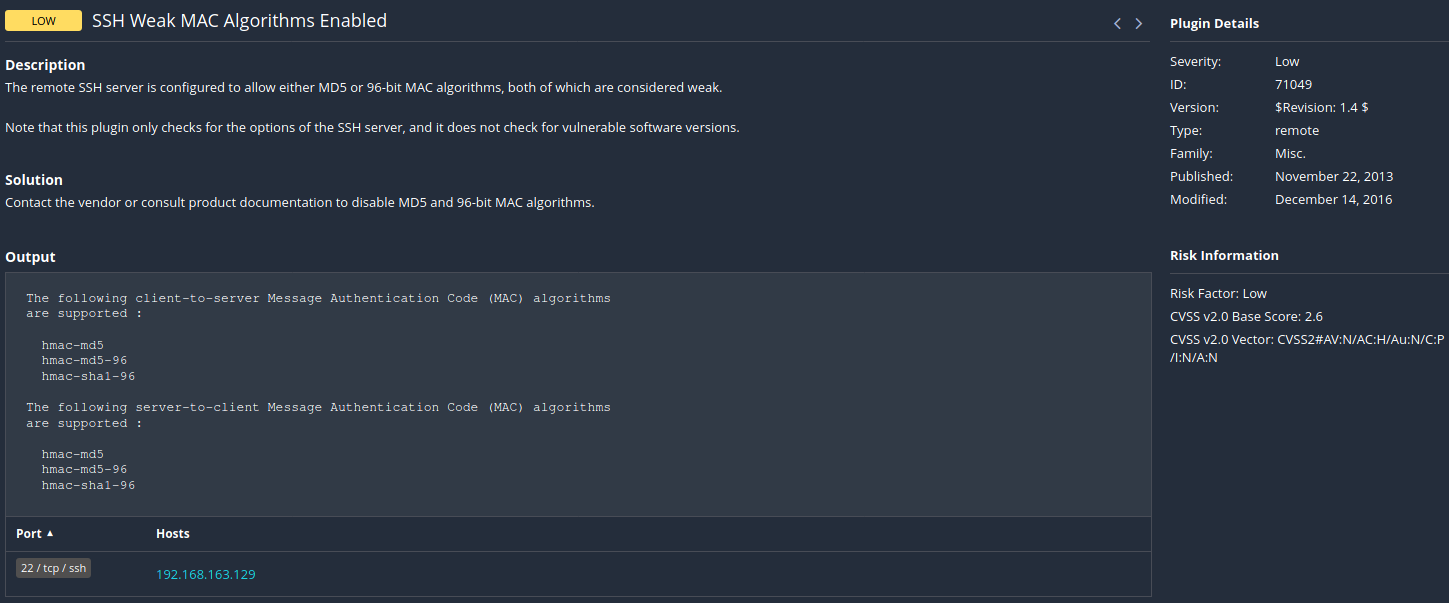


Figura Algoritmos MAC habilitados.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería contactar con el proveedor o consultar la documentación existente para deshabilitar los algoritmos MD5 y MAC de 96 bits.

## Campo 1: Descripción

**Obtención de credenciales con fuerza bruta**. Se ha obtenido las credenciales del protocolo de comunicación SSH **msfadmin**:**msfadmin**.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **alto**.

## Campo 3: Explotación

Vulnerabilidad obtenida primeramente gracias a la obtención de los usuarios con la herramienta **Nmap**, lanzando el script de autenticación:

***sudo nmap –p- --script=auth 192.168.163.129***

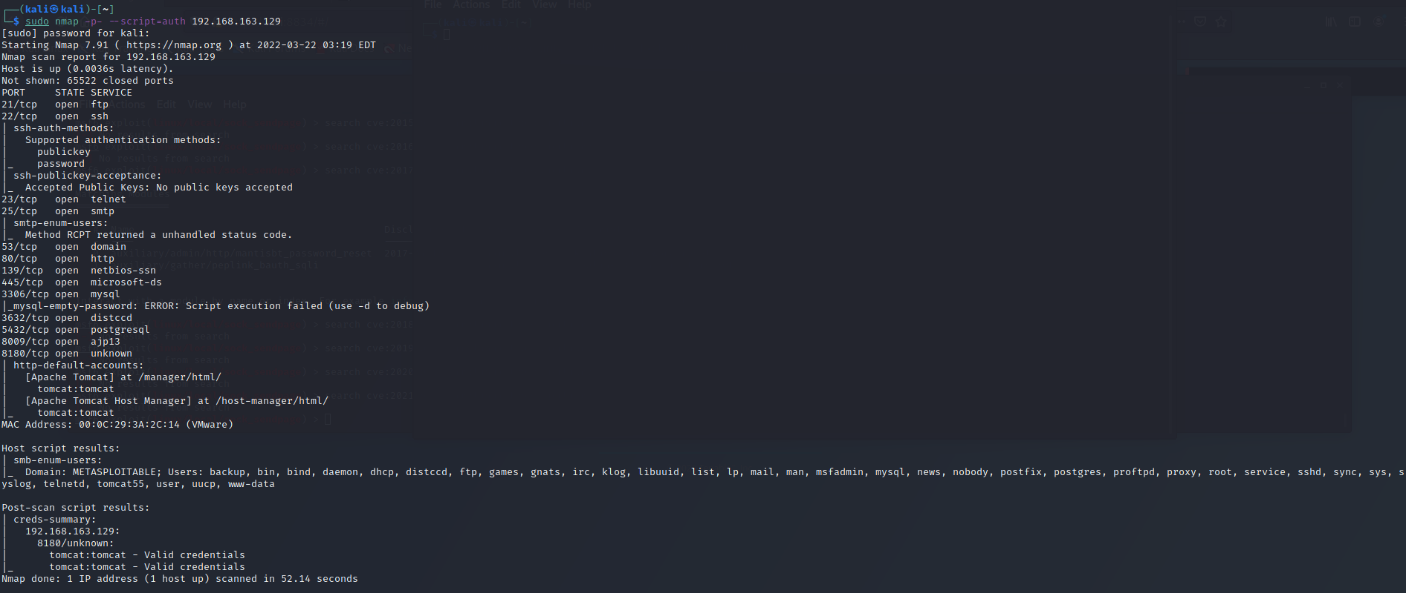


Figura 38 Usuarios.

Y seguidamente con ayuda de la herramienta **Hydra** y la generación del fichero de usuarios y contraseñas gracias a la información obtenida con **Nmap**:

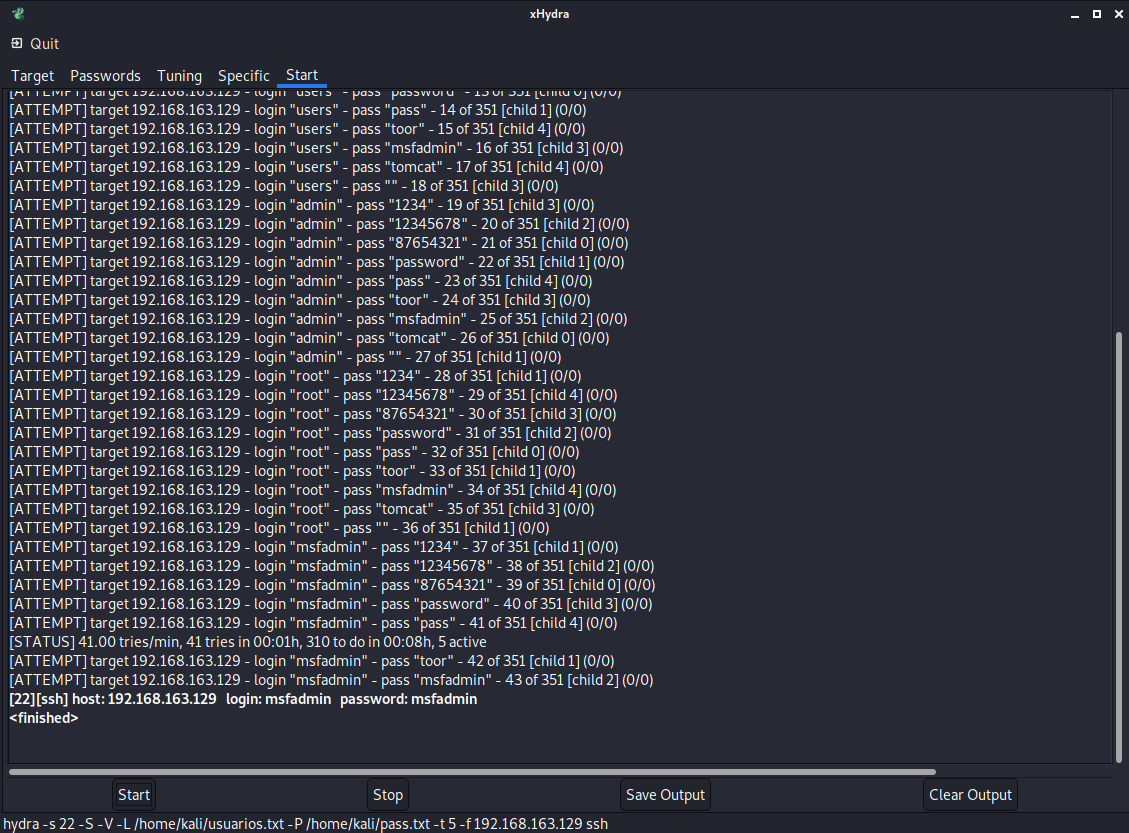
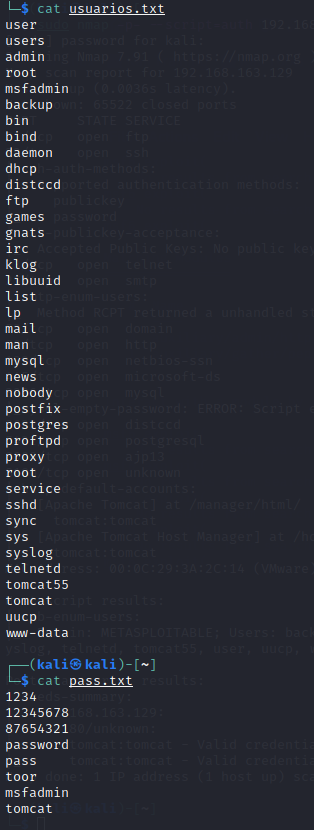


Figura 39 Fichero de usuarios/contraseñas y resultado con xHydra.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería generar usuarios y contraseñas más fuertes, con mayúsculas, minúsculas, números y caracteres. He intentar no utilizar palabras relacionadas con el mismo usuario.

* **Vulnerabilidades con el protocolo SMB puerto 445:**

## Campo 1: Descripción

**Vulnerabilidad Samba Badlock**. Vulnerabilidad encontrada en la versión de Samba, debido a un problema en la negociación del nivel de autenticación de los protocolos SAM y LSAD a través de RPC, conexión remota. Un posible atacante podría interceptar la comunicación entre servidor y cliente, afectar al nivel de autenticación y poder realizar comunicaciones Samba como obtener/modificar datos de seguridad confidenciales de la base de datos AD o deshabilitar servicios críticos.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **alto**.

## Campo 3: Explotación

Vulnerabilidad obtenida con la utilización del escáner de vulnerabilidades **Nessus**:

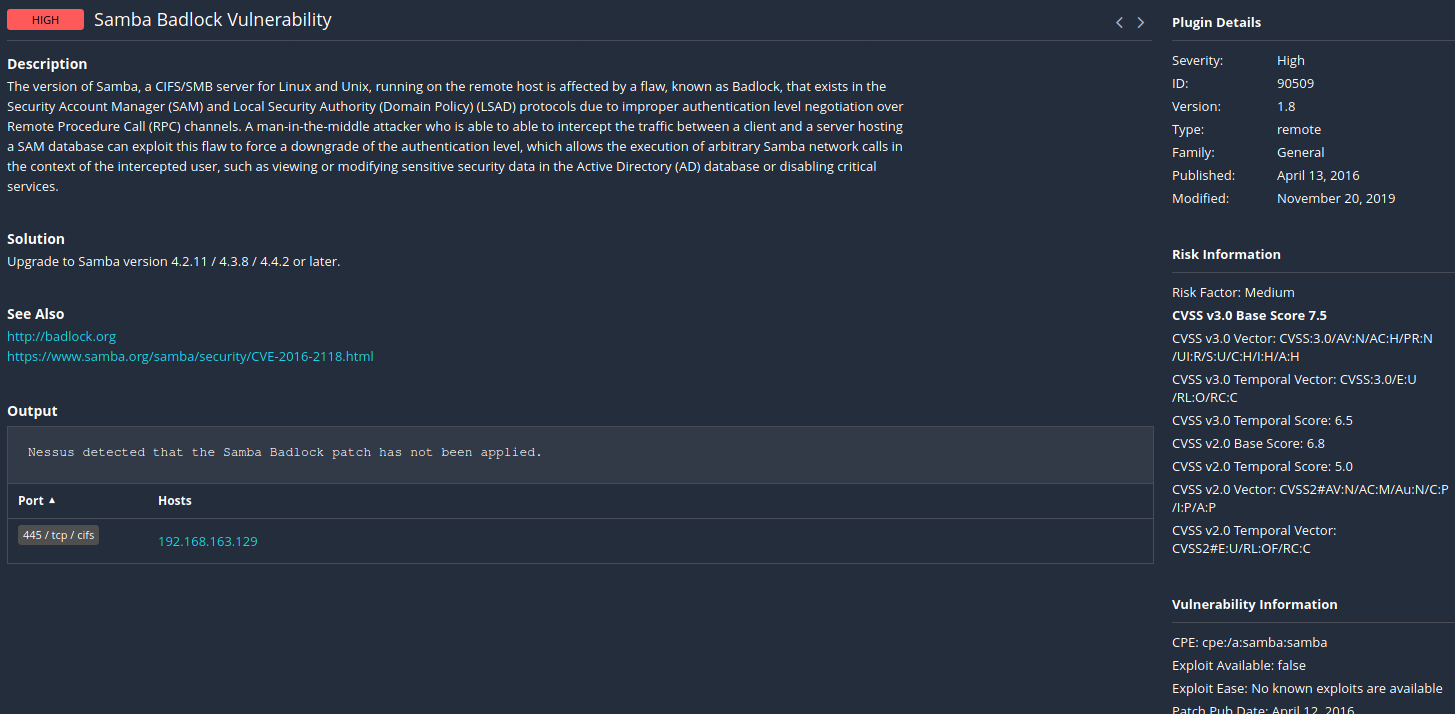
****

Figura 40 Vulnerabilidad Samba Badlock.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería actualizar la versión de Samba a la versión 4.2.11 / 4.3.8 / 4.4.2 o posterior.

## Campo 1: Descripción

**Firma SMB no requerida**. Vulnerabilidad encontrada en el servidor SMB por ser opcional firmar digitalmente la comunicación. Un posible atacante no autenticado podría aprovechar esto para realizar ataques MiM contra el servidor SMB.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

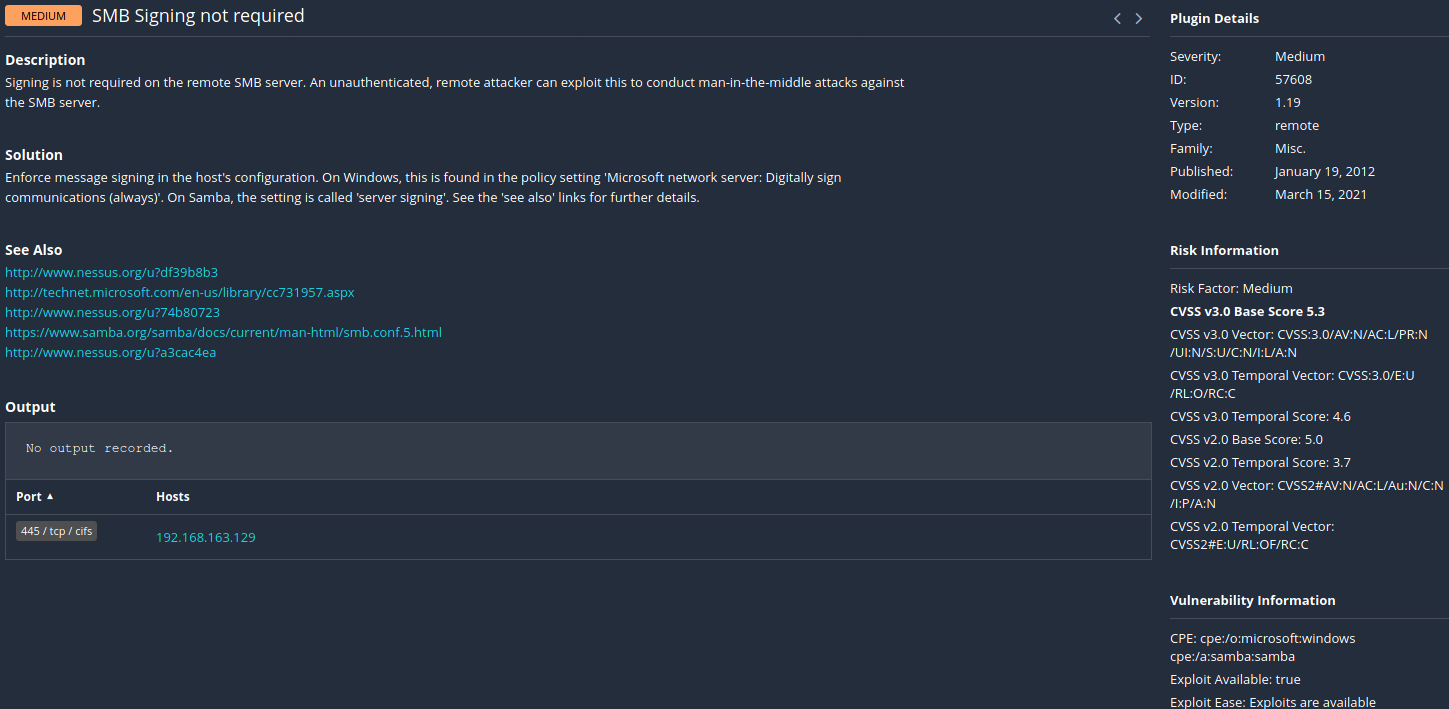
****

Figura 41 Firma SMB no requerida.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería modificar la configuración para firmar digitalmente las comunicaciones siempre.

* **Vulnerabilidades en el sistema de nombres de dominio (DNS) puerto 53:**

## Campo 1: Descripción

**Degradación del servicio ISC BIND/DoS reflejado**. Vulnerabilidad encontrada en la instancia de ISC BIND 9 ejecutada en el DNS, la cual está afectada por una degradación del rendimiento y DoS reflejado. Esto es debido a que BIND DNS no limita lo suficiente el número de recuperaciones que se pueden realizar mientras se procesa una respuesta. Un posible atacante no autenticado podría aprovechar esta vulnerabilidad para degradar el servicio o utilizarlo para un ataque reflejado.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **alto**.

## Campo 3: Explotación

Vulnerabilidad obtenida con la utilización del escáner de vulnerabilidades **Nessus**:

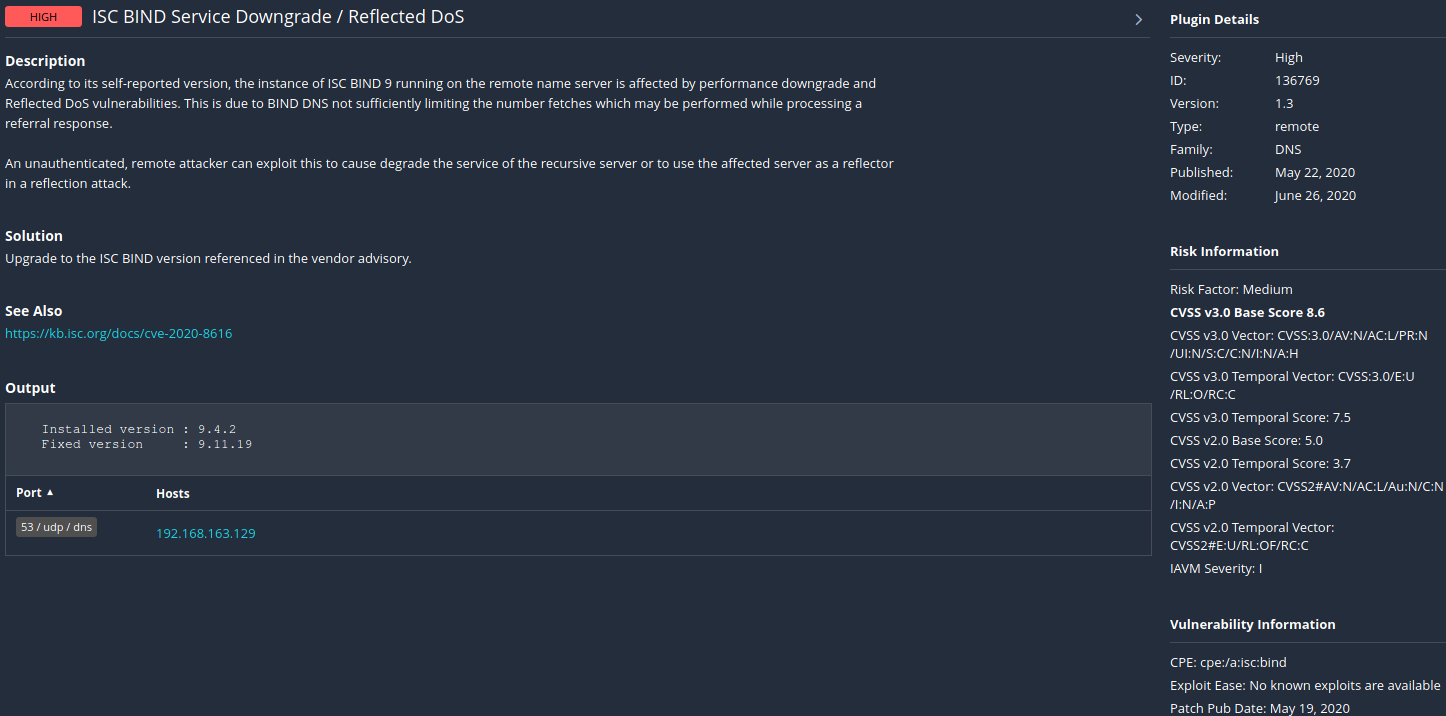
****

Figura 42 Degradación del servicio ISC BIND.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería actualizar la versión de ISC BIND a una versión con el problema solucionado, concretamente a la versión 9.11.19.

## Campo 1: Descripción

**Denegación de servicio en ISC BIND**. Vulnerabilidad encontrada en la versión instalada de ISC BIND 9.4.2, la cual podría ser explotada por un posible atacante, pudiendo hacer que el servicio dejase de responder.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **alto**.

## Campo 3: Explotación

Se ha obtenido esta vulnerabilidad con la utilización de la herramienta **Nessus**, un escáner de vulnerabilidades:

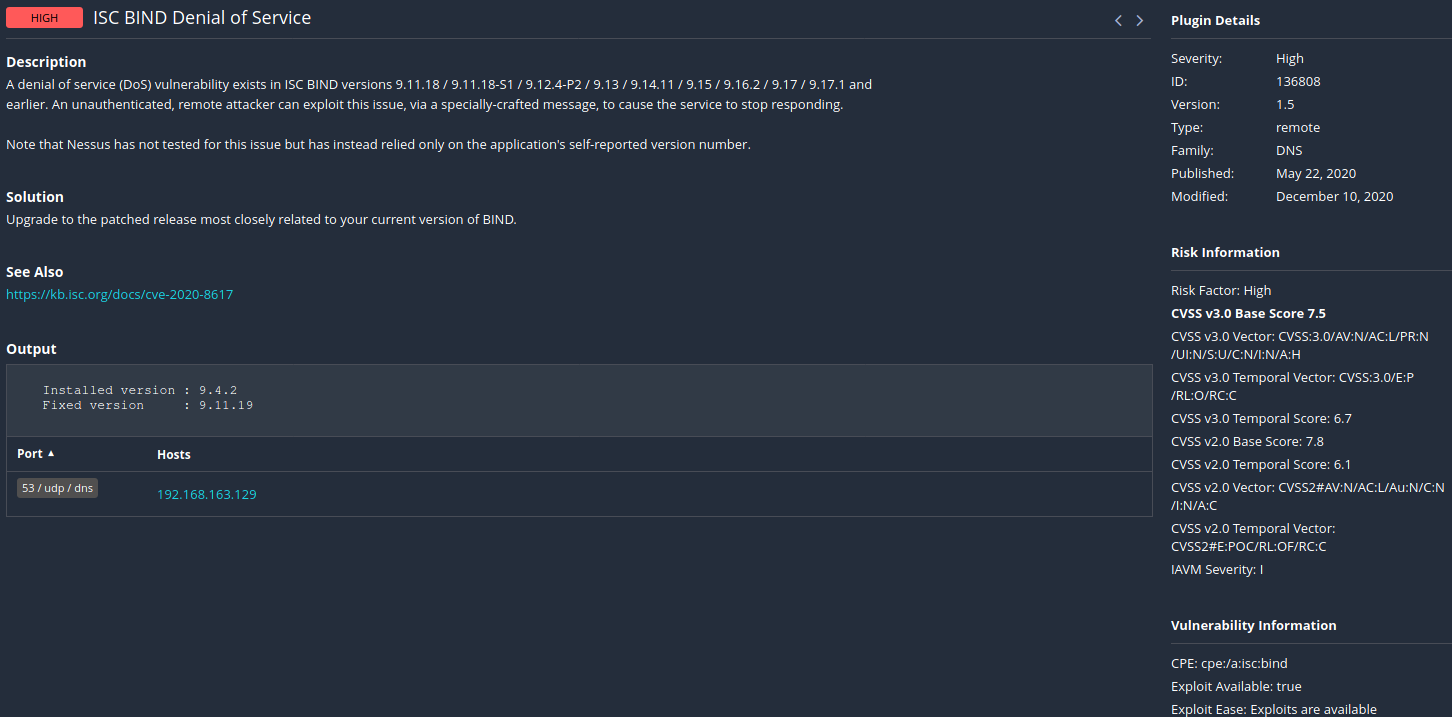
****

Figura 43 Denegación de sevicio en ISC BIND.

Seguidamente se realizado la explotación de la vulnerabilidad utilizando la herramienta **Mestasploit**:

* Se ha buscado la vulnerabilidad por su referencia CVE: ***search cve-2020-8617***
* Se ha seleccionado el exploit: ***auxiliary/dos/dns/bind\_tsig\_badtime***
* Se configurado el exploit y se ha lanzado:

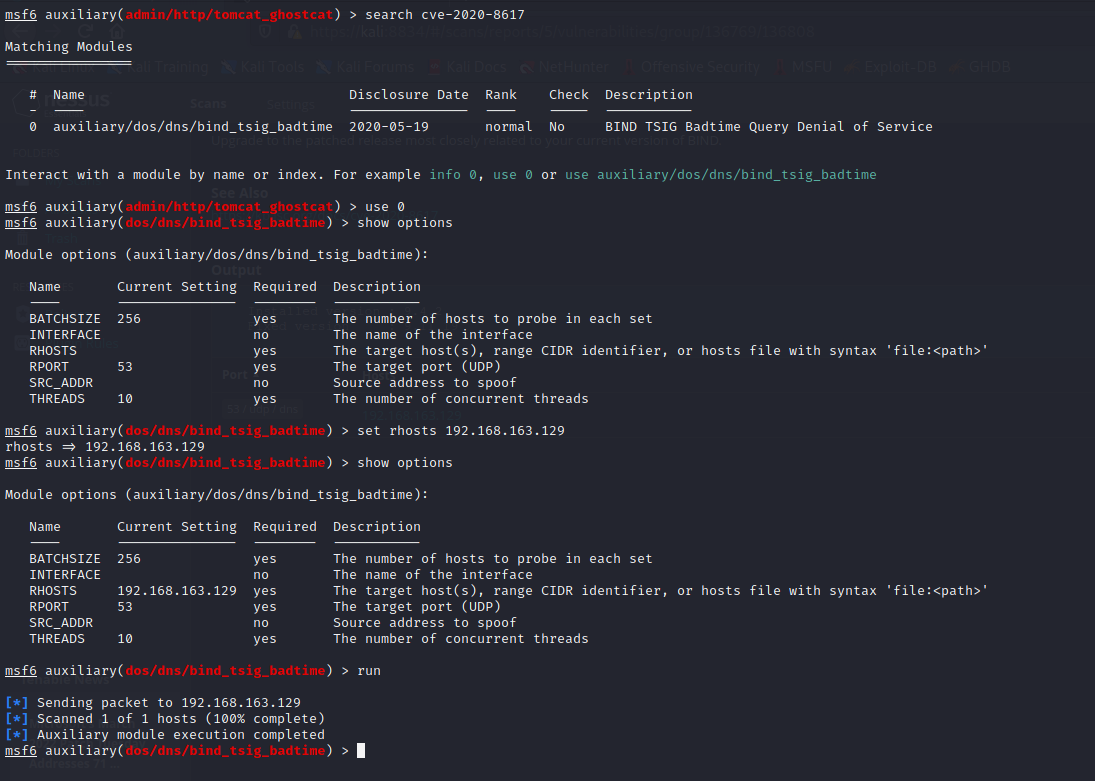


Figura 44 Explotación ISC BIND DoS.

El cual realizaría una denegación del servicio ISC BIND de la máquina víctima.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería actualizar la versión de ISC BIND a una versión con el problema solucionado, concretamente a la versión 9.11.19.

## Campo 1: Descripción

**Versión de ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 vulnerable a DoS**. Vulnerabilidad encontrada en la versión instalada de ISC BIND (9.4.3) la cual puede ser explotada por una denegación de servicio (DoS) debido a un problema de aserción al intentar verificar una respuesta truncada a una solicitud firmada por TSIG.

## Campo 2: Impacto

El peligro/impacto de explotar esta vulnerabilidad es **medio**.

## Campo 3: Explotación

Vulnerabilidad obtenida con el escáner de vulnerabilidades **Nessus**:

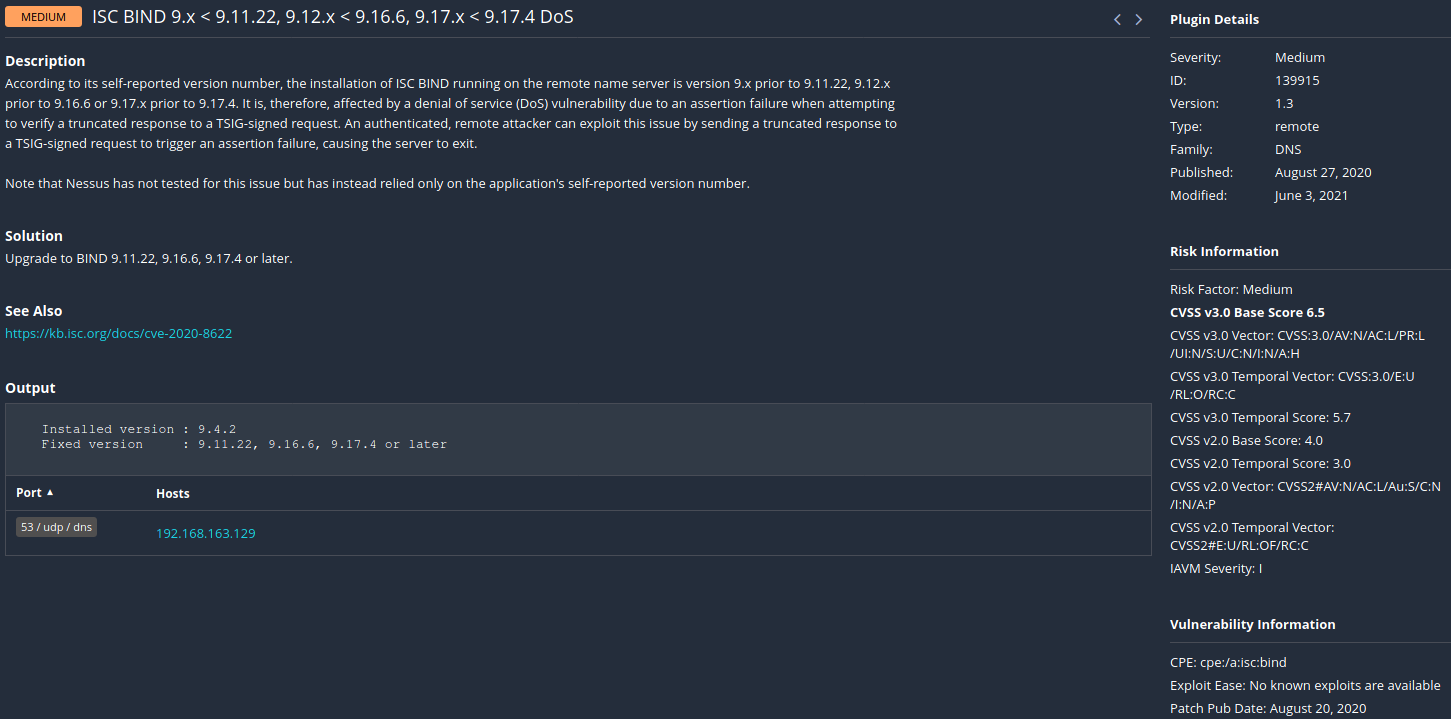
****

Figura 45 Versión de ISC BIND vulnerable a DoS.

## Campo 4: Mitigación

Para solucionar esta vulnerabilidad se debería actualizar ISC BIND a la versión 9.11.22, 9.16.6, 9.17.4 o posterior.