

CIBER SEGURIDAD

Informe Ejecutivo
y Técnico



HERRAMIENTAS ANALIZADAS:
METASPLOITABLE 3
WINDOWSPOITABLE 3

Índice

Informe Ejecutivo

01 Introducción

02 Alcance

03 Vulnerabilidades encontradas

04 Soluciones o recomendaciones

Informe Técnico

01 Introducción

02 Alcance

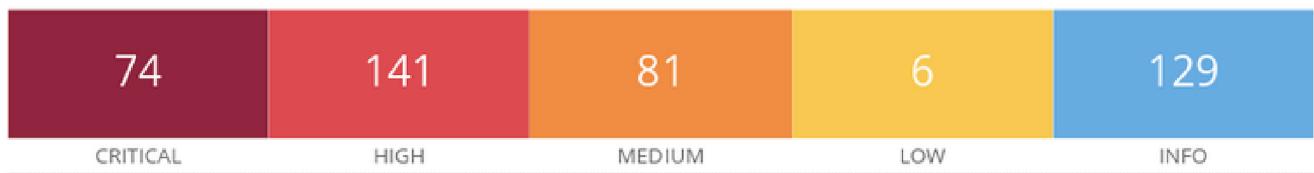
03 Vulnerabilidades encontradas

04 Recomendaciones

INFORME EJECUTIVO

1 - Introducción

En el análisis realizado a la primer host de la herramienta experimental (Metasploitable 3) expuesta para el estudio mediante White Box se han encontrado el siguiente número de vulnerabilidades ordenadas de mayor a menor según su criticidad. Detallamos la fecha y la hora de la realización de la prueba, el nombre del host, su IP, su dirección MAC y su sistema operativo actual.



Scan Information

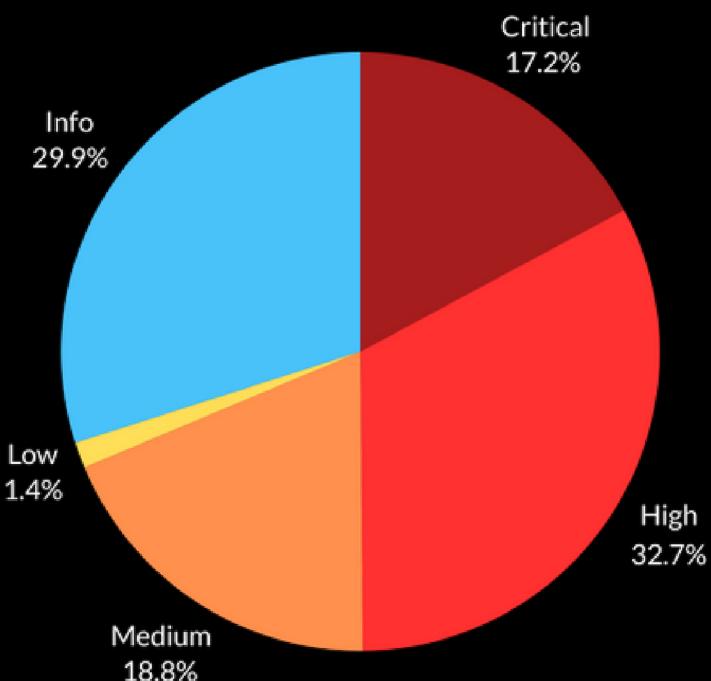
Start time: Mon Jun 24 12:44:13 2024
End time: Mon Jun 24 12:53:10 2024

Host Information

Netbios Name: METASPLOITABLE3-UB1404
IP: 10.0.2.9
MAC Address: 08:00:27:16:62:D7 96:65:CC:C8:5E:8C 02:42:82:8E:4E:ED
OS: Linux Kernel 3.13.0-24-generic on Ubuntu 14.04

CRITICIDAD DE LAS VULNERABILIDADES ENCONTRADAS

17,2%
Critical



Desglose de vulnerabilidades encontradas:

- 74 Critical
- 141 High
- 81 Medium
- 6 Low
- 129 Info

IP: 10.0.2.9 - MAC ADDRESS:08:00:27:16:62:D7
OS: LINUX KERNEL 3.13.0-24-GENERIC ON UBUNTU 14.04

JOSEJIMENEZCIBERSECURITY.COM

A continuación se muestra una tabla con el análisis de puertos abiertos encontrados del primer host de la herramienta experimental (Metasploitable 3) con Nmap.

Detallamos en la imagen los puertos abiertos, el estado, el servicio y la versión de ellos.

Puerto	Estado	Servicio	Versión
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 ((Ubuntu))
445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X
631/tcp	open	ipp	CUPS 1.7
3000/tcp	closed		
3306/tcp	open	mysql	MySQL
3500/tcp	open	http	WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp	open	irc	UnrealIRCd
8080/tcp	open	http	Jetty 8.1.7.v20120910
8181/tcp	closed	intermapper	

A continuación les mostramos los datos recabados mediante el estudio de vulnerabilidades con Nessus del segundo host de la herramienta experimental (Windowsploitable 3).

Detallamos la fecha y la hora de la realización de la prueba con Nessus, el nombre del host, su IP, su dirección MAC y su sistema operativo actual.

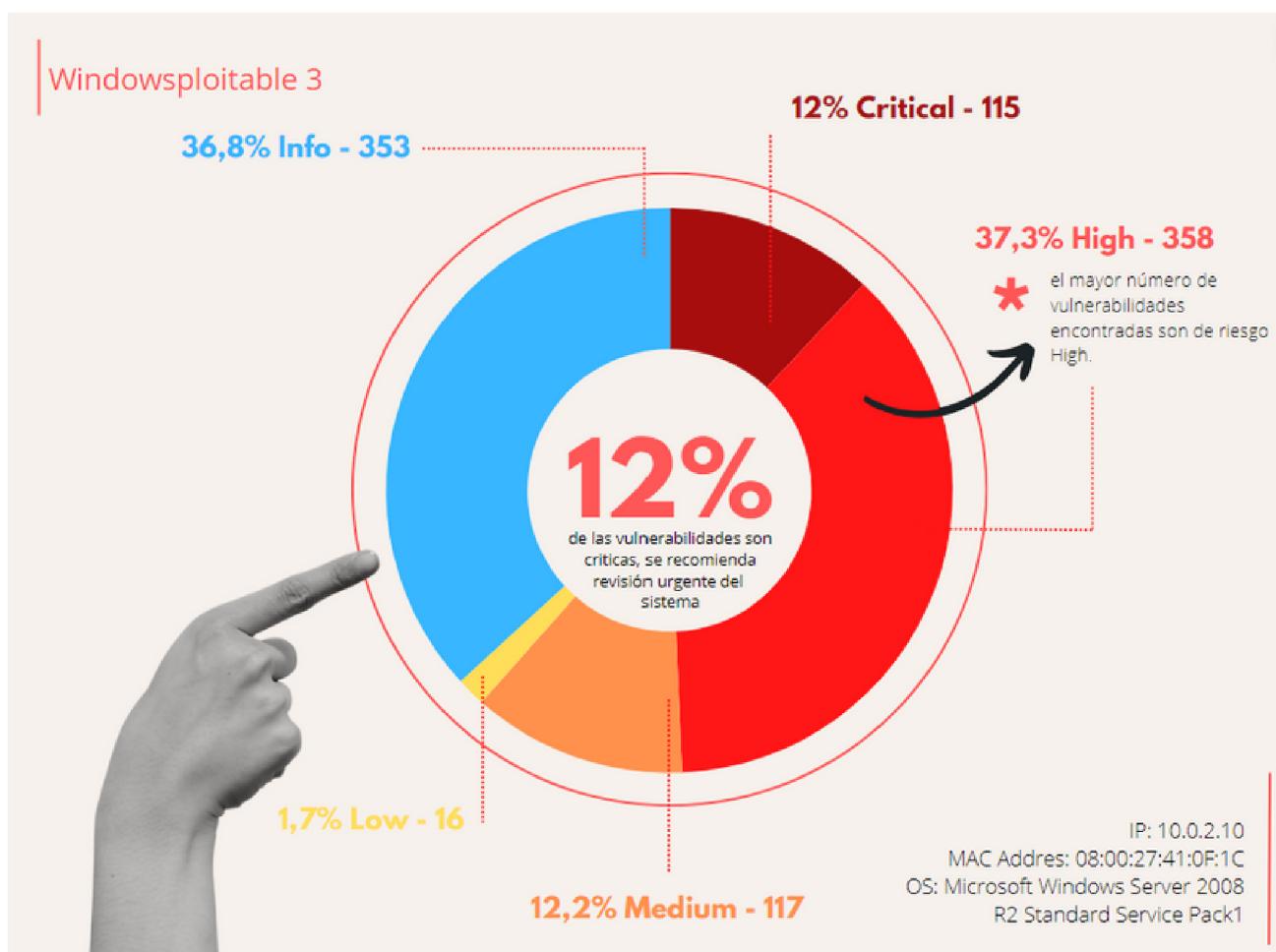


Scan Information

Start time: Wed Jun 26 09:43:06 2024
End time: Wed Jun 26 10:08:11 2024

Host Information

Netbios Name: METASPLOITABLE3
IP: 10.0.2.10
MAC Address: 08:00:27:41:0F:1C B8:BB:20:52:41:53 08:00:27:12:95:5B
OS: Microsoft Windows Server 2008 R2 Standard Service Pack 1



A continuación les mostramos los datos recabados mediante el estudio de vulnerabilidades con Nessus del segundo host de la herramienta experimental (Windowsxploitable 3).

Detallamos la fecha y la hora de la realización de la prueba con Nessus, el nombre del host, su IP, su dirección MAC y su sistema operativo actual.

Puerto	Estado	Servicio	Versión	Puerto	Estado	Servicio	Versión
21/tcp	open	ftp	Microsoft IIS ftpd	8282/tcp	open	http	Apache Tomcat/Coyote JSP engine 1.1
22/tcp	open	ssh	OpenSSH 7.1 (protocol 2.0)	8383/tcp	open	http	Apache httpd
80/tcp	open	http	Microsoft IIS httpd 7.5	8484/tcp	open	http	Jetty winstone-2.8
135/tcp	open	microsoft-ds	Microsoft Windows RPC	8585/tcp	open	http	Apache httpd 2.2.21 (Win64) PHP/5.3.10 DAV/2
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn	8686/tcp	open	java-rmi	Java RMI
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds	9200/tcp	open	wap-wsp?	
1617/tcp	open	java-rmi	Java RMI	9300/tcp	open	vrace?	
3306/tcp	open	mysql	MySQL 5.5.20-log	47001/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
3389/tcp	open	tcpwrapped		49152/tcp	open	microsoft-ds	Microsoft Windows RPC
3700/tcp	open	giop	CORBA naming service	49153/tcp	open	microsoft-ds	Microsoft Windows RPC
4848/tcp	open	ssl/http	Oracle Glassfish Application Server	49154/tcp	open	microsoft-ds	Microsoft Windows RPC
5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)	49155/tcp	open	microsoft-ds	Microsoft Windows RPC
7676/tcp	open	java-message-service	Java Message Service 3.01	49176/tcp	open	java-rmi	Java RMI
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)	49177/tcp	open	tcpwrapped	
8020/tcp	open	http	Apache httpd	49201/tcp	open	microsoft-ds	Microsoft Windows RPC
8027/tcp	open	papachi-p2p-srv?		49204/tcp	open	microsoft-ds	Microsoft Windows RPC
8080	open	http-proxy	GlassFish Server Open Source Edition 4.0	49258/tcp	open	ssh	
8191/tcp	open	ssl/internmapper?		49259/tcp	open	jenkins-listener	Apache Mina sshd 0.8.0 (protocol 2.0)

2 - Alcance

Dadas las vulnerabilidades encontradas en la herramienta experimental a la que hemos realizado un análisis de puertos y vulnerabilidades con los pasos anteriormente explicados hemos llegado a la conclusión de que los activos para los que esta herramienta experimental fue creada tienen una gran peligro de ser extraídos por un cibercriminal y suponen un riesgo alto para la organización la utilización de ella. Y por tanto no recomendamos utilizarla hasta haber resuelto todos los problemas.

3 - Vulnerabilidades encontradas

The infographic is titled "VULNERABILIDADES ENCONTRADAS" and "Metasploitable 3". It features five numbered sections, each with an icon and a brief description:

- 01 MÓDULO MOD_COPY EN PROFTPD**: An illustration of a person in a hoodie holding a laptop. Description: Permite a atacantes remotos leer y escribir en ficheros arbitrarios a través de los comandos site cpfr y site cpto.
- 02 ESCALADA DE PRIVILEGIOS DE SUDO EN LINUX**: An illustration of a user icon, a fingerprint, and a password field. Description: Permite a usuarios locales sin privilegios ejecutar comandos arbitrarios como root.
- 03 API DE ABSTRACCIÓN DE BASE DE DATOS DRUPAL SQLI**: An illustration of a network of devices connected to a central WiFi icon. Description: Permite a atacantes remotos inducir a ataques de inyección SQL a través de un array que contiene claves manipuladas.
- 04 EJECUCIÓN REMOTA DE CÓDIGO BASH (SHELLSHOCK)**: An illustration of a person in a hoodie using a laptop. Description: Versión de Bash que es vulnerable a la inyección de comandos mediante la manipulación de variables de entorno.
- 05 SISTEMA UNIX NO COMPATIBLE**: An illustration of a locked folder. Description: El sistema operativo Unix que se ejecuta en el host es antiguo y no recibe actualizaciones de seguridad.

Windowsploitable 3

06 VERSIÓN DE APACHE TOMCAT SIN SEGURIDAD

En la actualidad la versión de Tomcat 8.0.X no recibe actualizaciones de seguridad lo cual la hace vulnerable a un atacante.



07 INTERNET EXPLORER DESACTUALIZADO



La versión instalada del navegador IE podría permitir la ejecución de código arbitrario de un cibercriminal.

08 CIFRADO DE SEGURIDAD SSL NIVEL MEDIO

El host utiliza un cifrado de nivel medio, el cual es poco seguro y más fácil para un cibercriminal poder descifrarlo.



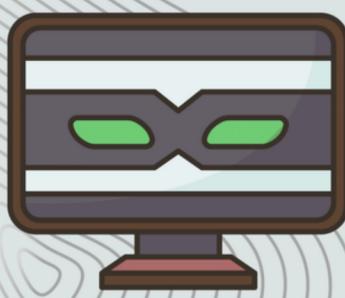
09 EL SISTEMA DE SEGURIDAD DE WINDOWS NO ESTÁ ACTUALIZADO



Esto implica varias vulnerabilidades las cuales pueden ser aprovechadas por un atacante para ejecutar código arbitrario con privilegios elevados en el sistema.

10 VULNERABILIDAD EN HTTP.SYS

Un usuario ajeno al host podría aprovecharla para ejecutar código arbitrario en el sistema con privilegios y tomar el control del host.



4 - Soluciones y recomendaciones

1. Actualizar el Sistema y las aplicaciones usadas a la Última Versión:

- Implementar un ciclo de actualización regular.
- Usar herramientas de gestión de parches automatizadas para garantizar que no se omita ninguna actualización.

2. Configurar el Cifrado SSL a Alta Intensidad:

- Revisar y modificar las configuraciones de SSL/TLS en los servidores y aplicaciones.
- Asegurarse de que las longitudes de claves sean de al menos 64 bits.
- Adoptar el uso del cifrado 3DES o equivalente para mejorar la seguridad de las comunicaciones.

3. Aplicación de Parches de Seguridad:

- Establecer un protocolo para la rápida implementación de parches tan pronto como se liberen.
- Monitorear continuamente las publicaciones de seguridad de los proveedores y aplicar los parches recomendados sin demoras.

Implementar estas soluciones ayudará a asegurar los hosts y protegerlos contra ataques cibernéticos, reduciendo significativamente el riesgo de explotación de vulnerabilidades.

INFORME TÉCNICO

1 - Introducción

Por indicación de la empresa The Bridge | Talent Acelerator se va a proceder al análisis de una nueva herramienta interna experimental que desean incorporar en su organización con el fin de agilizar y mejorar el rendimiento de las instalaciones TI y la protección de activos. Dicha herramienta consta de dos host (Metasploitable 3 y Windowsploitable 3).

Para ello vamos a hacer dos tipos de análisis de vulnerabilidades (Black Box y White Box) para determinar los niveles de seguridad de su nuevo sistema a incorporar.

Para realizar estudio de la herramienta experimental por completo también se va a implementar un escaneo de todos los puertos disponibles para determinar cual están abiertos, que servicios corren en ellos y cuales son peligrosos vistas a un cibercriminal. Para ello contaremos en este caso con la herramienta Nmap la cual nos dará un análisis detallado y unos resultados con una alta fiabilidad.

En el análisis de vulnerabilidades tipo Black Box se va a proceder a un análisis completo de la herramienta experimental desde el exterior del sistema sin conocer ningún tipo de credencial ni acceso a ella. En la cual se podría interpretar como las vulnerabilidades que estarían expuestas a un cibercriminal desde el exterior de la organización.

En este caso en el análisis de vulnerabilidades tipo White Box se procederá a un análisis de la herramienta experimental usando credenciales y accediendo al sistema como si de un usuario interno de la organización se tratase o si un cibercriminal consiguiera entrar al sistema de la herramienta y tuviera acceso al interior de esta.

Para ello vamos a utilizar la herramienta de escaneo de vulnerabilidades Nessus, la cual nos ayudará a determinar en ambos casos las vulnerabilidades del sistema y nos proporcionará los datos suficientes para poder solventarlos de manera correcta.

Dado que al realizar los dos tipos de escaneos (Black Box y White Box) la cantidad de vulnerabilidades de criticidad más elevadas encontradas es por parte de White Box, vamos a proceder al perfilado del documento centrandonos en las vulnerabilidades más críticas para su herramienta experimental así podremos solventar y corregir los riesgos para ella y su organización.

2 - Alcance

Las vulnerabilidades encontradas en ambos sistemas con la herramienta Nessus y Nmap nos detallan un número importante de vulnerabilidades las cuales la mayoría son por una falta de actualizaciones de varios sistemas, herramientas, versiones de servicio de los protocolos. También se ha detectado un cifrado de nivel medio en SSL. También se ha detectado que el sistema operativo principal UNIX sobre el que se ejecuta Metasploitable 3 está desactualizado. Todos estos hallazgos nos confirman que sus sistemas son vulnerables a cualquier cibercriminal que se disponga a intentar acceder a ellos, los cuales provocaría perdidas de sus activos protegidos por ella y provocaría un efecto dominó pudiendo acceder mediante escalada de privilegios y la técnica de pivoting a los demás sistemas de su organización desencadenando perdidas incalculables.

3 - Vulnerabilidades encontradas

Las vulnerabilidades encontradas en ambos sistemas con la herramienta Nessus y Nmap nos detallan un número importante de vulnerabilidades las cuales la mayoría son por una falta de actualizaciones de varios sistemas, herramientas, versiones de servicio de los protocolos. También se ha detectado un cifrado de nivel medio en SSL. También se ha detectado que el sistema operativo principal UNIX sobre el que se ejecuta Metasploitable 3 está desactualizado. Todos estos hallazgos nos confirman que sus sistemas son vulnerables a cualquier cibercriminal que se disponga a intentar acceder a ellos, los cuales provocaría perdidas de sus activos protegidos por ella y provocaría un efecto dominó pudiendo acceder mediante escalada de privilegios y la técnica de pivoting a los demás sistemas de su organización desencadenando perdidas incalculables.

METASPLOITABLE 3

CVSS 9,8 -- ProFTPD mod_copy Information

Disclosure

(CVE-2015-3306)

Información de la vulnerabilidad descrita por Nessus:

El host remoto ejecuta una versión de ProFTPD que se ve afectada por una vulnerabilidad de divulgación de información en el módulo mod_copy debido a que los comandos SITE CPFR y SITE CPTO están disponibles para clientes no autenticados. Un atacante remoto no autenticado puede aprovechar esta falla para leer y escribir en archivos arbitrarios en cualquier ruta web accesible en el host.

Solución:

Actualice a ProFTPD a la última versión disponible.

Explicación detallada:

- En concreto este host utiliza una versión de ProFTPD 1.3.5 la cual contiene una vulnerabilidad en su sistema en el módulo mod_copy, la cual nos permite a través del puerto 21/tcp con el servicio ftp mediante el comando SITE CPFR (site copy from) copiar cualquier archivo desde un directorio accediendo al host y mediante el comando SITE CPTO (site copy to) le permitiría a un cibercriminal copiarse ese archivo a su host sin la necesidad de estar autenticado. Así como copiarse cualquier código arbitrario desde su máquina atacante para conseguir acceso por completo a su herramienta y activos de la organización
- Esta vulnerabilidad está clasificada como muy grave en la escala CVSS con un 9.8
- La solución para esta vulnerabilidad sería actualizar a la última versión de este servicio la cual es: 1.3.8b20

CVSS 7,8 -- Linux Sudo Privilege Escalation (Out-of-bounds Write)

(CVE-2021-3156)

Información de la vulnerabilidad descrita por Nessus:

Sudo versiones anteriores a 1.9.5p2 contiene un error de desbordamiento que puede resultar en un desbordamiento de búfer basado en la pila, lo que permite la escalada de privilegios a root a través de "sudoedit -s" y un argumento de línea de comandos que termina con un solo carácter de barra invertida

Solución:

Actualizar el paquete sudo

Explicación detallada:

- La versión de sudo actualmente es 1.8.9p5 la cual tiene una vulnerabilidad que permite a cualquier usuario sin privilegios obtener permisos de root en su host. Mediante un desbordamiento de buffer provocado al utilizar comando ./sudoedit y a continuación la barra invertida \ seguido del código a ejecutar como root en su host Metasploitable 3.
- Cuando ejecutamos sudo en modo Shell podemos utilizar 2 parámetros:
 - -s: Indica la flag MODE_SHELL
 - -i: Indica las flags MODE_SHELL y MODE_LOGIN_SHELL
- Y posteriormente el comando que queremos que sea ejecutado como sudo. Si comprobásemos el código de sudo, observaríamos que primero reescribe los argumentos concatenándolos en la línea de comando y escaparía los metacaracteres con "\", después almacena los argumentos en un buffer y elimina el escape de los metacaracteres para que coincida con el sudoers y poder loguear correctamente.
- Y aquí es donde viene el problema, la función que almacena los argumentos en un buffer sufre de una vulnerabilidad de desbordamiento de buffer, que permite introducir caracteres externos en dichos argumentos. Teóricamente, no podría ser utilizado ya que existen unas condiciones if que impiden que se añadan las flags MODE_SHELL o MODE_LOGIN_SHELL y nos saltaría con un error. pero, si en vez de utilizar sudo, utilizásemos sudoedit, el código establecería automáticamente las flags necesarias.
- Por lo tanto, ejecutando sudoedit -s definiríamos las flags evitando que se ejecutara la función que impide establecer las flags.
- Esta vulnerabilidad está clasificada como Crítica en la escala CVSS con un 9.8
- La solución es actualizar la versión del paquete sudo a la última disponible.

CVSS 7,5 --Drupal Database Abstraction API SQLi (CVE-2014-3704)

Información de la vulnerabilidad descrita por Nessus:

El host Metasploitable 3 ejecuta una versión de Drupal que se ve afectada por una vulnerabilidad de inyección SQL debido a una falla en la API de abstracción de la base de datos de Drupal, que permite a un atacante remoto utilizar solicitudes especialmente diseñadas que pueden resultar en una ejecución SQL arbitraria. Esto puede provocar una escalada de privilegios, una ejecución arbitraria de PHP o una ejecución remota de código.

Solución:

Actualice a la versión 7.32 o posterior.

Puerto80/tcp - Servicio http

Explicación detallada:

- La versión de la base de datos de Drupal que actualmente utiliza en su host posee una vulnerabilidad en su API especialmente diseñada para evitar este problema que permitiría a un atacante mediante una inyección SQL con código arbitrario acceder a los activos de dicha base de datos, ejecutar código PHP u otros ataques. También es a considerar que existen exploits para automatizar este tipo de ataque lo cual facilita el acceso a un cibercriminal. Este ataque se produciría por el puerto 80/tcp con el servicio http.
- En este caso hablamos de una vulnerabilidad clasificada como Alta en la escala CVSS con un 7.5
- La solución para este problema sería actualizar la versión de Drupal a la 7.32 o posterior.

CVSS 9.8 -- Bash Remote Code Execution (Shellshock) (CVE-2014-6271)

Información de la vulnerabilidad descrita por Nessus:

Metasploitable 3 ejecuta una versión de Bash que es vulnerable a la inyección de comandos mediante la manipulación de variables de entorno. Dependiendo de la configuración del sistema, un atacante podría ejecutar código arbitrario de forma remota.

Solución:

Actualizar bash.

Explicación detallada:

- Este ataque permite a un atacante que acceda a la máquina y modifique una variable de entorno de bash introducir un código arbitrario que le permitiría un acceso remoto al host.
- Esta vulnerabilidad se encuentra en las versiones de bash desde la 1.14 a la 4.3, su host Metasploitable 3 tiene la 4.3 lo cual la hace vulnerable a este tipo de ataque. Al tener acceso remoto al host podría poner en peligro el host en si mismo, los activos que de él dependan así como el resto de la organización, ya que podría producirse mediante la técnica de pivoting acceso a cualquier host de la organización.
- Esta vulnerabilidad es crítica y está clasificada en la escala CVSS con un 9.8
- La solución sería actualizar bash a la última versión 5.2.21 para solucionar el problema.

CVSS 10 -- Detección de versión no compatible del sistema operativo Unix

Información de la vulnerabilidad descrita por Nessus:

Según el número de versión autoinformado, el sistema operativo Unix que se ejecuta en el host remoto ya no es compatible.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad.

Solución:

Actualice a una versión del sistema operativo Unix que sea compatible actualmente.

Explicación detallada:

- A continuación explicamos las vulnerabilidades encontradas que podrían ser explotadas por un cibercriminal con el sistema operativo Unix desactualizado y el peligro que conlleva:

1.Buffer Overflows:

- Los desbordamientos de búfer ocurren cuando un programa escribe más datos en un bloque de memoria de lo que estaba previsto. Esto puede permitir a un atacante sobrescribir la memoria adyacente, potencialmente ejecutando código arbitrario.

2.Exploits en Servicios de Red:

- Unix tradicionalmente incluye muchos servicios de red que, si no están debidamente configurados o actualizados, pueden ser explotados. Ejemplos incluyen vulnerabilidades en servicios como FTP, telnet, y rlogin.

3.Errores de Configuración:

- Configuraciones predeterminadas inseguras o mal configuradas pueden ser explotadas. Esto incluye permisos de archivo incorrectos, servicios innecesarios habilitados y contraseñas débiles.

4.Vulnerabilidades en el Kernel:

- El kernel de Unix ha tenido varias vulnerabilidades a lo largo de los años, que permiten escalada de privilegios, denegación de servicio o ejecución de código arbitrario.

5.Shellshock:

- Una vulnerabilidad crítica descubierta en el intérprete de comandos Bash, utilizado en muchos sistemas Unix y Unix-like. Permite a los atacantes ejecutar comandos arbitrarios en un sistema afectado.

6.Heartbleed:

- Una vulnerabilidad en la biblioteca de cifrado OpenSSL, ampliamente utilizada en sistemas Unix. Permite a los atacantes leer datos de la memoria de los servidores, potencialmente exponiendo información sensible.

7.Fallas en NFS (Network File System):

- NFS permite compartir archivos a través de una red. Malas configuraciones o fallas en NFS pueden permitir a los atacantes acceder a archivos no autorizados o ejecutar ataques de tipo "man-in-the-middle".

8.Inyección de Comandos:

- Aplicaciones que no validan correctamente la entrada del usuario pueden ser vulnerables a la inyección de comandos, permitiendo a un atacante ejecutar comandos arbitrarios en el sistema.

9.Race Conditions:

- Condiciones de carrera en la ejecución de programas pueden ser explotadas para obtener privilegios elevados o causar comportamiento no deseado en el sistema

10.Vulnerabilidades en Software Antiguo:

- Uso de software desactualizado o sin soporte puede tener vulnerabilidades conocidas y sin parches que los atacantes pueden explotar.

Para mitigar estos riesgos, es importante mantener los sistemas actualizados, aplicar parches de seguridad, configurar adecuadamente los servicios y sistemas, utilizar contraseñas fuertes y realizar auditorías de seguridad regularmente. Además, la implementación de políticas de seguridad y el uso de herramientas de monitoreo y detección de intrusiones pueden ayudar a proteger los sistemas Unix contra ataques.

Se recomienda actualizar Unix a la última versión disponible, en la actualidad V7.0

WINDOWSPOITABLE 3

Apache Tomcat SEOL (8.0.x)

Información de la vulnerabilidad descrita por Nessus:

Según su versión, Apache Tomcat es la 8.0.x. Por lo tanto, ya no lo mantiene su vendedor o proveedor.

La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, puede contener vulnerabilidades de seguridad.

Solución:

Actualice a una versión de Apache Tomcat que sea compatible actualmente.

Explicación detallada:

- A continuación se detallan las vulnerabilidades que podría aprovechar un atacante a este sistema por el puerto 8282/tcp con el servicio http:

1. Deserialización insegura:

- Los ataques de deserialización pueden ocurrir cuando un atacante envía datos maliciosos que se deserializan en el servidor, potencialmente permitiendo la ejecución remota de código (RCE). Ejemplo: CVE-2016-8735.

2. Vulnerabilidades de seguridad en el AJP (Apache JServ Protocol):

- AJP es un protocolo binario que puede ser explotado si no está configurado correctamente, permitiendo a atacantes eludir controles de acceso. Ejemplo: CVE-2020-1938 (Ghostcat).

3. Fugas de información:

- Algunas configuraciones y errores pueden permitir a los atacantes acceder a información sensible, como detalles de configuración, versiones de software, etc. Ejemplo: CVE-2015-5351.

4. Cross-Site Scripting (XSS):

- Estas vulnerabilidades permiten a un atacante injectar scripts maliciosos en páginas web vistas por otros usuarios. Ejemplo: CVE-2014-0119.

5.Directory Traversal:

- Permite a un atacante acceder a archivos y directorios que están fuera del directorio raíz previsto. Ejemplo: CVE-2014-0099.

6.Inyección de comandos:

- Si no se validan correctamente las entradas de los usuarios, un atacante puede injectar comandos que el servidor ejecutará. Ejemplo: CVE-2016-1240.

7.Problemas de autenticación y autorización:

- Fallos en la implementación de mecanismos de autenticación y autorización pueden permitir a atacantes acceder a recursos no autorizados. Ejemplo: CVE-2016-0706.

8.Fallo en el manejo de cookies y sesiones:

- Vulnerabilidades en el manejo de cookies y sesiones pueden permitir el secuestro de sesiones de usuarios. Ejemplo: CVE-2014-0075.
- Debido a la cantidad de vulnerabilidades y posibilidades de ataque para un cibercriminal con Apache Tomcat en esta versión esta vulnerabilidad está clasificada en la escala CVSS con una puntuación de 10.
- Lo cual supone un riesgo importante para su organización y los activos que respaldan. No es aconsejable continuar con esta herramienta si no se toman medidas adecuadas, que en este caso sería con una actualización de Apache Tomcat a la última versión disponible que en el momento de hacer el análisis de vulnerabilidades es la 10.1.19

CVSS 9.3 -- MS13-038: Security Update for Internet Explorer (2847204) (CVE-2013-1347)

Información de la vulnerabilidad descrita por Nessus:

A Windowsploitable 3 le falta la actualización de seguridad 2847204 de Internet Explorer (IE).

La versión instalada de IE se ve afectada por una vulnerabilidad de uso después de la liberación que podría permitir a un atacante ejecutar código arbitrario.

Solución:

Microsoft ha lanzado un conjunto de parches para XP, 2003, Vista, 2008, 7, 2008 R2 y 8.

Explicación detallada:

- A través de esta vulnerabilidad un cibercriminal podría usar la ejecución de código remoto. La vulnerabilidad se produce al acceder a un objeto en memoria que ha sido borrado o que no ha sido asignado correctamente. La vulnerabilidad podría corromper la memoria de forma que permitiría al atacante ejecutar código arbitrario dentro del contexto del usuario actual de Internet Explorer. Un atacante podría alojar un sitio web malicioso diseñado específicamente para aprovechar esta vulnerabilidad a través de Internet Explorer y engañar a la víctima a visitar dicho sitio web. En la cual podría mediante phishing robar los datos personales, credenciales, contraseñas y correos haciéndose pasar por un sitio web falso. Existe un exploit en Metasploit para esta vulnerabilidad detectada por el puerto 445/tcp con el servicio http.
- En pocas palabras, un empleado cualquiera de su organización podría usar el navegador e intentar acceder a parte de la web corporativa la cual seria falsa y así mostrarle al atacante toda la información que necesitase.
- Esta vulnerabilidad tiene un 9.3 en la clasificación CVSS.
- Se recomienda instalar parches de seguridad para XP, 2003, Vista, 2008, 7, 2008 R2 y 8. o una recomendación mejor aún sería cambiar de navegador.

CVSS 7.5 --Compatible con conjuntos de cifrado SSL de potencia media (SWEET32) (CVE-2016-2183)

Información de la vulnerabilidad descrita por Nessus:

Windowsploitable 3 admite el uso de cifrados SSL que ofrecen cifrado de intensidad media. Nessus considera de potencia media cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el conjunto de cifrado 3DES.

Tenga en cuenta que es considerablemente más fácil eludir el cifrado de intensidad media si el atacante está en la misma red física.

Solución:

Vuelva a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media.

- Esta vulnerabilidad está clasificada con un 7.5 en la escala CVSS.

CVSS 7.8 -- MS16-149: Actualización de seguridad para Microsoft Windows (3205655)

(CVE-2016-7219, CVE-2016-7292)

Información de la vulnerabilidad descrita por Nessus:

El host Windowsploitable 3 le falta una actualización de seguridad. Se ve, por tanto, afectado por múltiples vulnerabilidades:

- Existe una vulnerabilidad de divulgación de información en un controlador Crypto de Windows que se ejecuta en modo kernel debido a un manejo inadecuado de los objetos en la memoria. Un atacante local puede aprovechar esto, a través de una aplicación especialmente diseñada, para revelar información confidencial.

(CVE-2016-7219)

- Existe una vulnerabilidad de elevación de privilegios en el instalador de Windows debido a una desinfección inadecuada de la entrada, lo que genera un comportamiento de carga de biblioteca inseguro. Un atacante local puede aprovechar esto para ejecutar código arbitrario con privilegios elevados del sistema. **(CVE-2016-7292)**

Solución:

- Microsoft ha lanzado un conjunto de parches para Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2, 10 y 2016.
- Esta vulnerabilidad cuenta con un 7.8 en la escala CVSS lo cual es un riesgo de nivel Alto y se recomienda solucionarlo lo antes posible para no poner en peligro sus activos y a la organización.

CVSS 10 -- MS15-034: Una vulnerabilidad en HTTP.sys podría permitir la ejecución remota de código (3042553)

(CVE-2015-1635)

Información de la vulnerabilidad descrita por Nessus:

La versión de Windows que se ejecuta Windowsploitable se ve afectada por una vulnerabilidad en la pila del protocolo HTTP (HTTP.sys) debido al análisis incorrecto de solicitudes HTTP diseñadas. Un atacante remoto puede aprovechar esto para ejecutar código arbitrario con privilegios del sistema.

Solución:

Microsoft ha lanzado un conjunto de parches para Windows 7, 2008 R2, 8, 8.1, 2012 y 2012 R2

Explicación detallada:

- Esta vulnerabilidad podría ser explotada por un atacante mediante un exploit para su facilidad de uso, lo cual conllevaría a una rápida y efectiva operación sobre Windowsploitable 3 poniendo en riesgo su sistema, activos y organización.
- Se recomienda instalar los parches mencionados anteriormente para cubrir esta vulnerabilidad lo antes posible ya que está clasificada con un 10 en la escala de CVSS.