ANALISIS DE PUERTOS YVULNERABILIDADES

Jordi Masó Pla

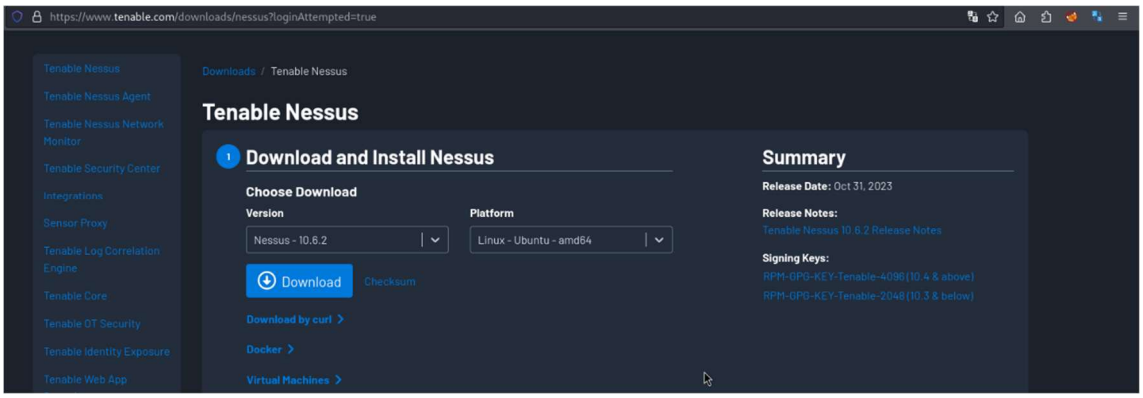
INDICE

1 Preparación escenario

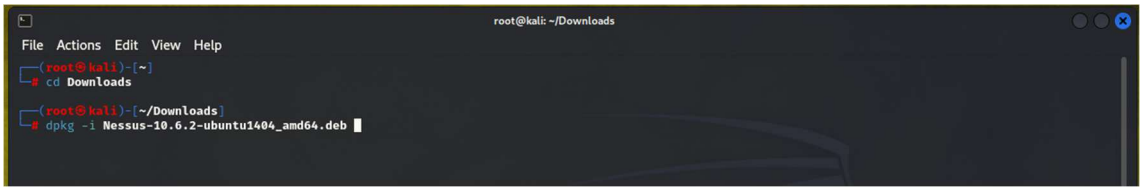
1.1 Registro e Instalación de Nessus

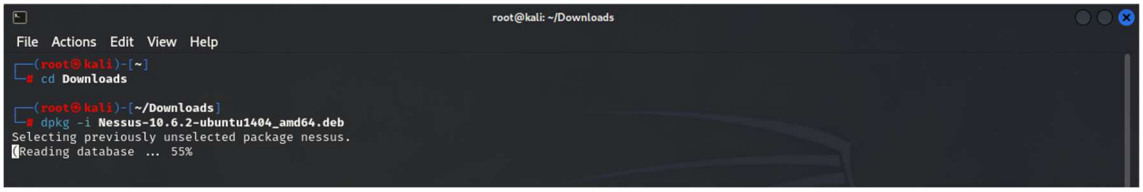
En este ejercicio trabajaremos con la herramienta Nessus Essentials de la empresa Tenable, que es la versión gratuita y limitada en numero de escaneos y en herramientas incluidas.

Accedemos a la página web del producto, en donde nos registramos para poder descargar el software y obtener un numero de registro para poder ejecutar la herramienta más adelante. En nuestro caso la descarga la versión 10.6.2 para Linux-Ubuntu- amd64.deb, ya que nuestro sistema operativo es Kali Linux.



Una vez descargado el archivo desde la consola nos dirigimos al directorio de descargas y ejecutamos el comando “sudo dpkg -i Nessus-10.6.2ubuntu1404_amd64.deb, introducimos la contraseña y la instalación empezara.





Al terminar la instalación en las dos últimas líneas está el procedimiento para poder arrancar Nessus, la primera desde la consola es iniciar “systemctl start nessusd.service”, que es para iniciar el programa y sus servicios y la segunda es abrir el navegador poner el localhost y el puerto 8834. Si es la primera vez ay que avanzar y aceptar el riego por credenciales desconocidas.

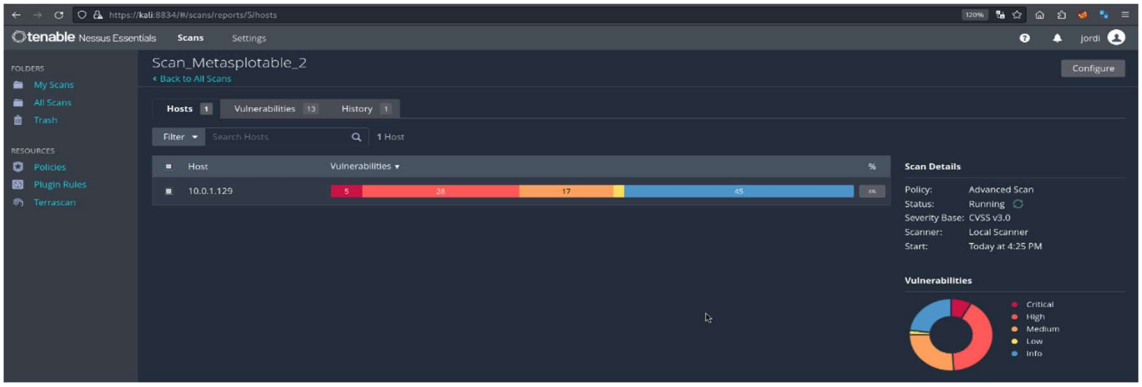
En el navegador tendemos varias opciones de elección de Nessus, en este caso Essentials, acto seguido introducimos el código de activación, procedemos a ingresar el nombre de usuario y la contraseña, y se empezara a descargar e instalar los plugins necesarios, esto pude ser un poco lento. Al terminar ya tenemos Nessus preparado para empezar a trabajar.

1.2 Preparación de escaneo

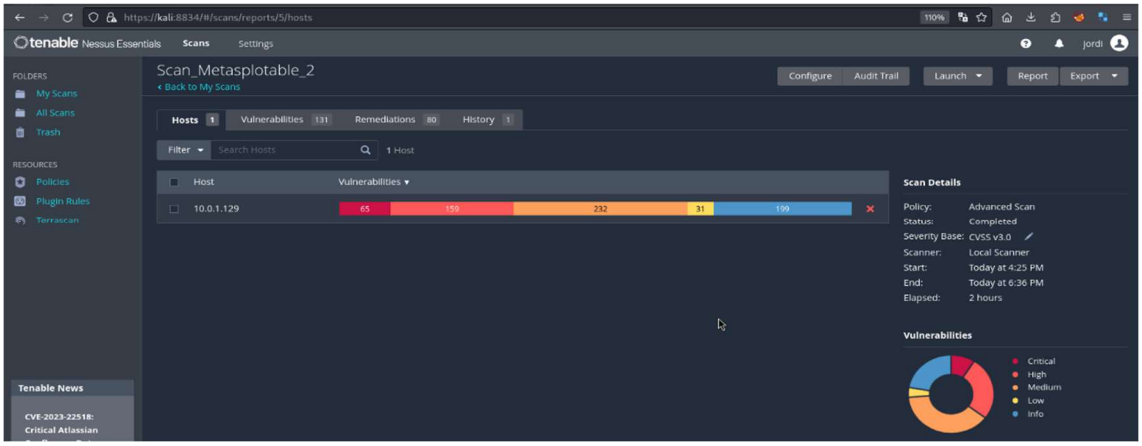
Creamos un nuevo escáner, seleccionamos escáner avanzado. Se abre una nueva ventana donde ponemos el nombre del escáner, una pequeña descripción y la ip o rango de ips a escanear. En la siguiente pestaña de descubrimiento seleccionamos los puertos a escanear, a través de ping o no, utilizar el protocola TCP SYN, enumeración de puertos como SNMP, SSH, entre otros protocolos. En la siguiente pestaña de evaluación, el apartado general seleccionamos que nos muestre los potenciales falsos positivos, en la siguientes definimos el ataque a fuerza bruta si queremos realizar o no, con un diccionario especifico. En la pestaña de aplicación web se selecciona el tipo de escaneo de las aplicaciones web que necesitamos. En la pestaña informe seleccionamos la información que nos muestra y que tipo de depuración de información queremos que nos muestres. Terminada la configuración del escáner lo guardamos y podemos proceder a poner en marcha nuestro escáner.

2 Ejecución del Escáner

Teniendo el escáner preparado podemos lanzar el proceso, es un proceso que puede llevar un tiempo para que termine.

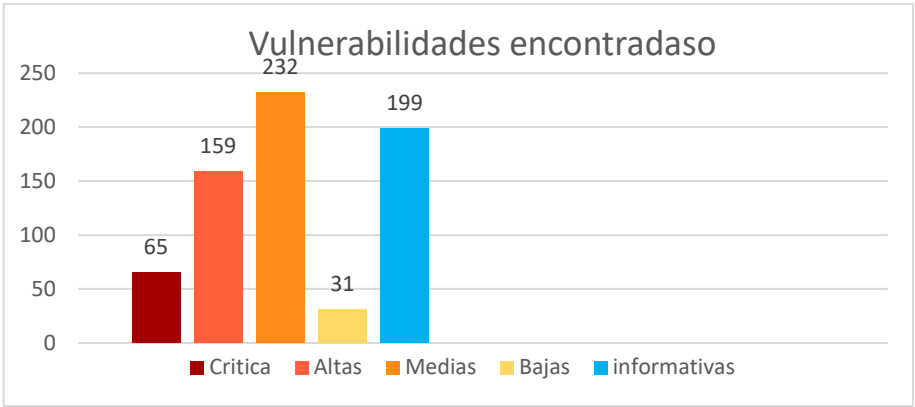


Con un poco de paciencia al cabo de un buen rato el escáner termia contra la maquina Metasplotable-2 con un resultado de posibles vulnerabilidades de 131 y 80 remediaciones posibles.



3 Vulnerabilidades encontradas

Las posibles vulnerabilidades encontradas se clasifican según su gravedad en críticas, altas, medias, bajas e informativas. Se dicen que son posible hasta que no se afirme la explotación de esta misma.



3.1 Vulnerabilidades Criticas

Las vulnerabilidades más grabes son las criticas que en ellas son lasque pueden comprometer el sistema entero y toda la información que hay dentro de este sistema. Empezamos por las principales vulnerabilidades críticas.

- Servicio Apache 2.2.x, 2.4.x, con multitud de vulnerabilidades encontrados en este servicio
- Servicio Apache Tomcat, el atacante podría lere archivos y subir archivos maliciosos
- Problema detectado con la versión de Bash que es vulnerable a la inyección
- El sistema Shell remoto es vulnerable
- ISC BIND esta obsoleto y no tiene soporte
- MySQL versión obsoleta
- El servidor SSH que se ejecuta en el host remoto se ve afectado por una vulnerabilidad de bypass
- El servicio remoto acepta conexiones cifradas usando SSL 2.0 y/o SSL 3.0. Estas versiones de SSL se ven afectadas por varias fallas criptográficas
- La versión de Samba que se ejecuta en el host es obsoleta, por lo tanto, se ve afectado por múltiples vulnerabilidades
- El servidor web remoto alberga una aplicación PHP que se ve afectada por la vulnerabilidad de SQL inyección
- Apache Log4j obsoleta, no tiene soporte
- Apache Tomcat obsoleta, no tiene soporte
- Apache httpd SEoL obsoleta, no tiene soporte
- Versión del leguaje PHP obsoleta
- PostgreSQL versión obsoleta, no tiene soporte
- El sistema operativo que funciona en el host remoto ya no es compatible
- Puede ser posible determinar contraseñas VNC a través de la fuerza bruta
- El sistema operativo Ubuntu le faltan uno o más parches relacionados con la seguridad
- El servidor remoto de IRC contiene una puerta trastornada
- Un servidor VNC que se ejecuta está asegurado con una contraseña débil

3.2 Vulnerabilidades Altas

Las vulnerabilidades altas son importantes, pero hay algunas que vienen dadas por las críticas, al solucionar algunas vulnerabilidades críticas se soluciona también las altas.

- PostgreSQL versión obsoleta, múltiples vulnerabilidades
- El servidor remoto de Samba se ve afectado por una vulnerabilidad remota de la ejecución de código
- Samba se ve potencialmente afectado por una vulnerabilidad de desbordamiento de buffer
- La versión de TWiki que se ejecuta en el host remoto permite a un atacante manipular la entrada al parámetro 'rev' con el fin de ejecutar comandos
- E servicio ISC BIND se ve afectado por ataques DoS
- E servicio Apache 2.2.x se ve afectado por varias vulnerabilidades
- El servidor SSH que se ejecuta en el host remoto se ve afectado por múltiples vulnerabilidades
- La versión de PHP que se ejecuta en el servidor web remoto se ve afectada por múltiples vulnerabilidades

- El servidor FTP remoto se ve afectado por una vulnerabilidad de denegación de servicio
- SSL soporta bloque de cifrado de 64bits débiles
- La versión de MySQL instalada es propenso a un ataque de denegación de servicio
- Ubuntu le faltan uno o más parches relacionados con la seguridad
- El servidor web remoto contiene una aplicación PHP que se ve afectada por una vulnerabilidad de ejecución de código
- El servicio de logines es vulnerable ya que los datos se pasan entre el cliente de rlogin y el servidor en texto claro
- El servicio de rsh es vulnerable ya que los datos se pasan entre el cliente de rsh y el servidor en texto claro
- La versión de MySQL instalada en el host remoto permite al parecer a un usuario remoto ejecutar código arbitrario explotando un desbordamiento de buffer en yaSSL 1.7.5 o anterior

3.3 Vulnerabilidades medias

Las vulnerabilidades medias son importantes, pero hay algunas que vienen dadas por las críticas y las altas, al solucionar algunas vulnerabilidades críticas y altas se soluciona también las medias

- Las principales vulnerabilidades son por servicios obsoletos sin soporte que hay que actualizar, con solucionar las criticas y las altas quedan solucionadas la gran mayoría
- Las cabeceras HTTP enviadas por el servidor web remoto revelan información que puede ayudar a un atacante, como la versión del servidor, el sistema operativo y las versiones de módulos
- Algunos directorios en el servidor web son navegable
- El servidor web remoto alberga scripts CGI que no logran desinfectar adecuadamente las cadenas de solicitud y se ven afectados por las vulnerabilidades de gestión del directorio o archivos locales
- Las funciones de depuración están habilitadas en el servidor web
- La versión de PHP que se ejecuta en el servidor web se ve afectada por una vulnerabilidad de inyección de encabezado de correo electrónico
- El certificado SSL del servidor ya ha expirado
- La aplicación web alberga archivos estáticos que pueden ser de naturaleza sensible
- El servidor web remoto revela información a través de una página de error predeterminada
- El servidor web remoto revela información a través de encabezados HTTP
- El servidor web contiene un script PHP que es propenso a un ataque de divulgación de información
- El servidor web es propenso a ataques de inyección de cookies
- El servidor web alberga scripts CGI que no logran desinfectar adecuadamente las cadenas de solicitud con JavaScript malicioso
- El servidor web es propenso a ataques de XSS
- El servidor web no configura una cabecera de respuesta X-Frame

3.4 Vulnerabilidades bajas

Las vulnerabilidades bajas pueden ser por mala configuración o por falta de actualización del servicio, estas vulnerabilidades no suelen llevar consecuencias tan graves como las demás escritas anteriormente, alguna de estas se describe a continuación.

- Conexiones SSH con cifrado Diffie-Hellman menos o igual a 1024 bits
- El servidor SSH remoto está configurado para permitir algoritmos de intercambio de claves débiles
- La instalación de libcurl se ve afectada por una vulnerabilidad de inyección de cookies
- El servidor web transmitir credenciales en texto claro
- Web Server utiliza la autenticación básica sin HTTPS
- El host remoto está ejecutando un servidor X11. X11 es un protocolo cliente-servidor que se puede utilizar para mostrar aplicaciones gráficas que se ejecutan en un host dado en un cliente remoto

3.5 Vulnerabilidades informativas

Las vulnerabilidades informativas son aquellas que de mala configuración o de dejar los parámetros por defecto, como usuarios y contraseñas por defecto, habilitar mas permisos de los necesarios a un servicio o usuario. En esta maquina se han encontrado una gran cantidad de estos defectos, que no son explotables directamente, pero mediante otros fallos si se pueden llegar a usar.

4 Explicación

Las principales vulnerabilidades detectas en esta máquina Mestasplotable 2 son muchas. Empezamos por la primera el puerto 21 el servicio FTP, hay diferentes formas de poder explotar este servicio una de ellas es con Metasploit otra es utilizando un diccionario con Hydra, con las dos formas obtenemos usuario root. El puerto 22 el SSH con un exploit de Metasploit podemos acceder y de allí ganar privilegios. Una de las vulnerabilidades mas claras el puerto 23 Telnet, que en el momento de acceder al servicio nos muestra las credenciales para logearnos. El servicio SAMBA que corre en el puerto 139 ya que es una versión obsoleta y vulnerable con Metasploit es fácil de tener acceso como administrador. La base de datos MySQL al tener una versión obsoleta es fácilmente explotable con Metasploit o incluso con sqlmap. La web de Apache Tomcat se pueden subir archivos y ejecutarlos obteniendo una Shell para comandos y escalada de privilegios. Hay puertas traseras sin ningún tipo de seguridad que se pueden utilizar para acceder al sistema. Tiene varios servicios que la conexión entre cliente y servidor son en texto claro sin cifrar y fáciles de interceptar. El servicio IRC tiene una puerta trasera fácil de explotar. EL SMTP es susceptible de inyección de código malicioso por lo tanto también es fácil explotar este servicio. ProFTPD, PostgreSQL es obsoleto y tiene varis vulnerabilidades conocidas y que se pueden hace uso de ellas, se tendría de actualizar a una versión mas reciente. El servicio VNC es fácil obtener credenciales con Hydra y un buen diccionario. X-11 es susceptible a un baipás y obtener acceso al sistema.

Las principales medidas de corrección serian actualizar todos los servicios a la versión mas reciente y optar por una configuración mas robustas sin dejar puertas traseras, credenciales por defecto ni información de como acceder al servicio expuesta, evitar los servicios como Telnet y otros servicios que el tráfico no va cifrador. Los servicios web que no se puedan subir archivos o restricciones de formato y no exponer información en el código fuente de la página.