Ismael Rojas Gonzalez
Reporte Pentest ejemplo RootMe

Reporte Pentest

Date: June 18, 2023
Project: 1
Version 1.0

Contents

Disclaimer

Esto es un reporte de un pestesting realizado en un entorno de prueba controlado, en concreto en el laboratorio RootMe de la plataforma TryHackMe.

Este reporte tiene fines didácticos, y es simplificado a las pruebas realizadas con objetivo de comprometer al completo la máquina víctima.

Información de contacto

Name	Title	Contact information
Pentester		
Ismael Rojas Gonzalez	Security Engineer	Github: github.com/IsmaRG

Resumen ejecutivo

Durante los 7 días de duración de este test de penetración, se ha procedido a la enumeración, reconocimiento, análisis y explotación de las vulnerabilidades del objetivo desde un test de caja negra.

Se han detectado numerosos fallos en la seguridad del sistema, pudiendo llegar a vulnerar por completo la máquina que actua como servidor de los servicios expuestos, obteniendo total control sobre ella.

Esto da lugar a un estado de seguridad crítico del objetivo, siendo necesaria su subsanación de inmediato.

A continuación, se sigue el siguiente esquema para exponer los detalles del pentest llevado a cabo.

- Metodología usada – Especificación de guías y metodología usada para el seguimiento de este test de penetración.
- Objetivos del pentest – Identificación de los activos evaluados..
- Vulnerabilidades existentes – Enumeración y análisis de las vulnerabilidades encontradas en el sistema objetivo.
- Valoración de la post-explotación – Identificación de los procesos mediante los cuales la post-explotación ha sido posible, así como el impacto de esta.
- Conclusión – Veredicto final del test de penetración.

Metodología usada

Para la realización de este pentest se ha seguido la guía de pentesting generada por Ismael Rojas Gonzalez. Así mismo, se han utilizado las herramientas propuestas en dicha guía.

Se han aplicado los procesos que cubren ambos tipos de pentest recogidos por la guía, es decir, pentest para redes y para aplicaciones web.

Objetivos del pentest

Dado que este test se trata de un test de caja negra, únicamente se conocía la dirección IP del objetivo, en un principio, siendo esta: 10.10.87.178

Por otro lado, tras un breve escaneo, se descubrió una página web relacionada con dicha IP.

Vulnerabilidades existentes

Rating de criticidad

La siguiente tabla muestra el ranking de criticidad de las vulnerabilidades, indicando el valor CVS correspondiente a cada nivel, así como una breve definición de estos niveles.

Criticidad	CVSS V3 score	Definición
Crítica	9.0 – 10.0	Explotación sencilla que conlleva a un acceso al sistema, comprometiendo este. Se requiere el arreglo de estos fallos.
Alta	7.0 – 8.9	Explotación más complicada pero que repercute enormemente en la seguridad del sistema.
Media	4.0 – 6.9	Vulnerabilidades existentes pero no explotables o de gran complejidad.
Baja	0.1 – 3.9	Vulnerabilidades no explotables, sin mayores consecuencias.
Informativa	N/A	No hay vulnerabilidades. Información adicional que corregir.

Hallazgos

Dado que esto se trata de un reporte de ejemplo, se mostrará a continuación únicamente la vulnerabilidad crítica que ha dado lugar a la obtención del control total del sistema, sirviendo esta como ejemplo para un análisis completo del resto de vulnerabilidades.

Subida y ejecución de archivos PHP (Crítica)

Dentro de la ruta http://10.10.128.49/panel, se permite la subida de archivos y la ejecución de estos, desde la ruta http://10.10.128.49/uploads. Esto conlleva a la ejecución de código remoto, pudiendo obtener acceso a la máquina que actúa como servidor del servicio web.

Aunque no se permite la subida de archivos con extensión .php, esta extensión puede ser modificada por alguna equivalente, como .phtml, y el servidor seguirá interpretando dicho archivo como código PHP y ejecutándolo.

Una vez se ha subido el archivo .phtml que contiene el código de una reverse shell, nos ponemos en escucha en nuestra máquina atacante con el comando "nc -nlvp 1234", siendo 1234 el puerto que se abre para la conexión desde la máquina víctima.

De esta forma, al entrar a la ruta http://10.10.128.49/uploads/<archivo-subido>, se ejecutará el código y obtendremos acceso a la máquina.

Valoración de la post-explotación

Esta sección contiene información acerca de la fase de post-explotación, incluyendo la gravedad de esta en caso de que se haya conseguido.

Permiso SUID en el binario Python (Crítica)

Una vez se obtuvo acceso a la máquina víctima con la explotación mencionada anteriormente, se hizo uso de la herramienta LinPEAS, que ayudó en el proceso de escaneo en la búsqueda de escalada de privilegios.

Esta herramienta marcó como crítico la asignación del permiso SUID en el binario Python, que fue lo que condujo a una escalada de privilegios, obteniendo el usuario root y permitió la obtención del control total del sistema.

Se utilizó la página GTFOBins para identificar cómo se llevaba a cabo la escalada de privilegios con el abuso del permiso SUID del binario Python, resultando esta en el siguiente comando: python -c 'import os; os.execl("/bin/sh", "sh", "-p")'

De esta forma, se ejecutó el comando y se obtuvo una shell como el usuario root.

Se clasifica esta post-explotación como crítica ya que se obtuvo el control total del sistema, pudiendo acceder a todo tipo de información, permitiendo pivotar a otras máquinas, etc.

Conclusión

Dadas las vulnerabilidades encontradas y explotadas, así como su correspondiente fase de post-explotación de estas, la seguridad del objetivo se declara como CRITICA, siendo necesaria su subsanación de INMEDIATO.

Recomendaciones

Subsanación vulnerabilidad subida y ejecución de archivos

Se recomienda no permitir acceso al directorio "/uploads", con el objetivo de impedir la ejecución de los archivos subidos.

Por otro lado, se recomienda actualizar la lista negra de extensiones no permitidas en la ruta "/panel" para la subida de ficheros, incluyendo en esta lista todas las extensiones derivadas de .php.

Subsanación permiso SUID del binario Python

Se debe quitar el permiso SUID del binario Python, impidiendo así la impersonificación del usuario root y, remediando así, la escalada de privilegios por culpa de este binario.