Challenges

fs0ciety

Network Setup

- Connected to HTB OpenVPN Server via OVPN file

Found Vulnerabilities

- Weak Credentials – Dictionary Attack
- base64 encoding to encrypt ssh credentials

Exploits/Payloads Used

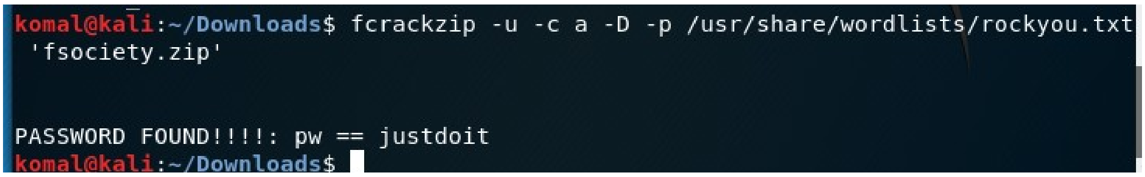
- None

Key Findings

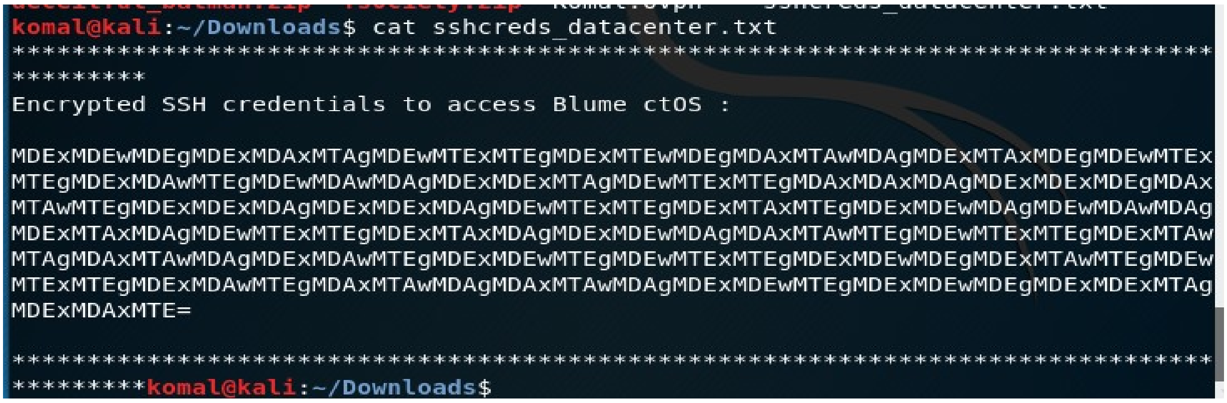
- Base64 Encoded text
- Binary text

Write-Ups & Screenshots

>> Used fcrackzip to extract the password for the fsociety.zip file which extracted the ssh credentials text file.

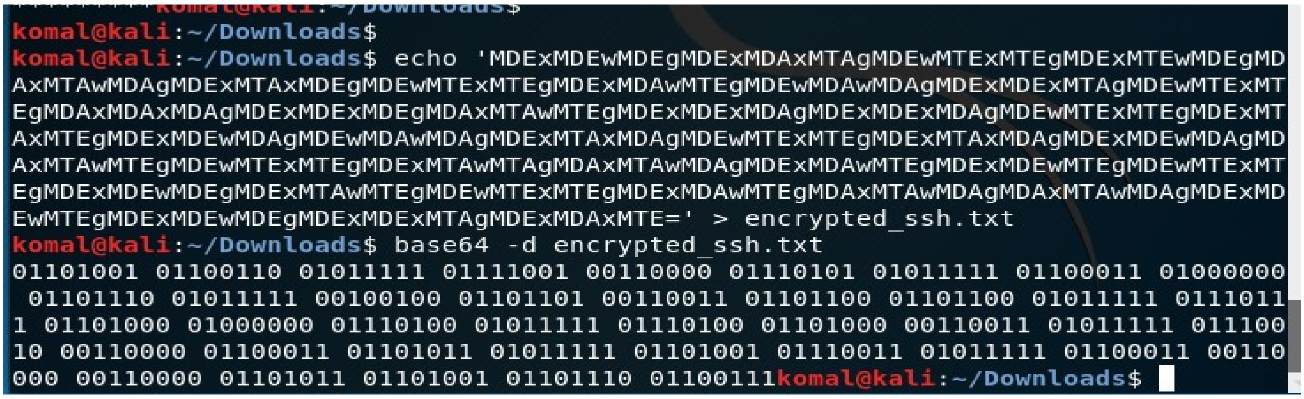


```
komal@kali:~/Downloads$ fcrackzip -u -c a -D -p /usr/share/wordlists/rockyou.txt
 'fsociety.zip'


PASSWORD FOUND!!!!: pw == justdoit
komal@kali:~/Downloads$
```

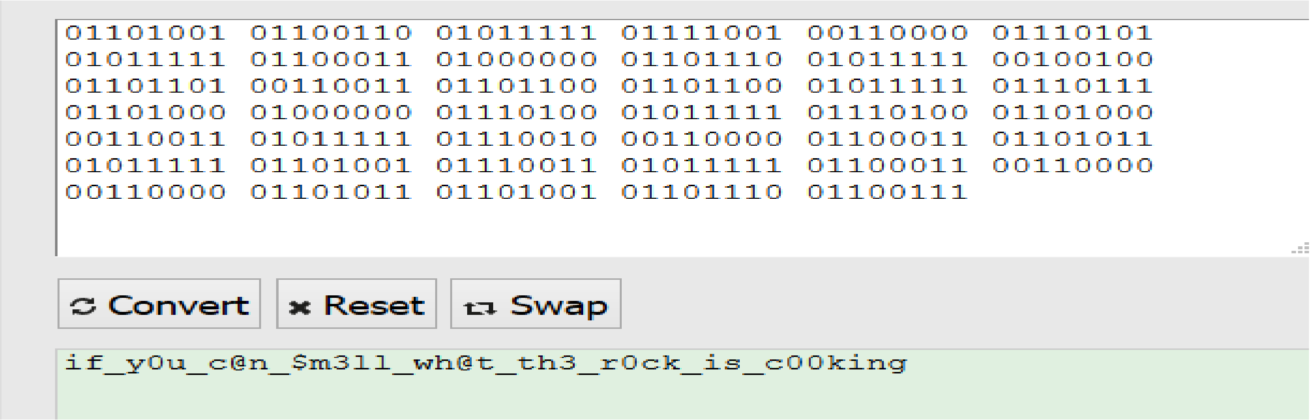


```
komal@kali:~/Downloads$ cat sshcreds_datacenter.txt
********************************************************************************
*********
Encrypted SSH credentials to access Blume ctOS :

MDExMDEwMDEgMDExMDAxMTAgMDEwMTExMTEgMDExMTEwMDEgMDAxMTAwMDAgMDExMTAxMDEgMDEwMTEx
MTEgMDExMDAwMTEgMDEwMDAwMDAgMDExMDExMTAgMDEwMTExMTEgMDAxMDAxMDAgMDExMDExMDEgMDAx
MTAwMTEgMDExMDExMDAgMDExMDExMDAgMDEwMTExMTEgMDExMTAxMTEgMDExMDEwMDAgMDEwMDAwMDAg
MDExMTAxMDAgMDEwMTExMTEgMDExMTAxMDAgMDExMDEwMDAgMDAxMTAwMTEgMDEwMTExMTEgMDExMTAw
MTAgMDAxMTAwMDAgMDExMDAwMTEgMDExMDEwMTEgMDEwMTExMTEgMDExMDEwMDEgMDExMTAwMTEgMDEw
MTExMTEgMDExMDAwMTEgMDAxMTAwMDAgMDAxMTAwMDAgMDExMDEwMTEgMDExMDEwMDEgMDExMDExMTAg
MDExMDAxMTE=

********************************************************************************
*********komal@kali:~/Downloads$
```

>> The SSH credentials were encrypted using base64 encoding. Decrypting it gave me the binary figures.



```
komal@kali:~/Downloads$
komal@kali:~/Downloads$ echo 'MDExMDEwMDEgMDExMDAxMTAgMDEwMTExMTEgMDExMTEwMDEgMD
AxMTAwMDAgMDExMTAxMDEgMDEwMTExMTEgMDExMDAwMTEgMDEwMDAwMDAgMDExMDExMTAgMDEwMTExMT
EgMDAxMDAxMDAgMDExMDExMDEgMDAxMTAwMTEgMDExMDExMDAgMDExMDExMDAgMDEwMTExMTEgMDExMT
AxMTEgMDExMDEwMDAgMDEwMDAwMDAgMDExMTAxMDAgMDEwMTExMTEgMDExMTAxMDAgMDExMDEwMDAgMD
AxMTAwMTEgMDEwMTExMTEgMDExMTAwMTAgMDAxMTAwMDAgMDExMDAwMTEgMDExMDEwMTEgMDEwMTExMT
EgMDExMDEwMDEgMDExMTAwMTEgMDEwMTExMTEgMDExMDAwMTEgMDAxMTAwMDAgMDAxMTAwMDAgMDExMD
EwMTEgMDExMDEwMDEgMDExMDExMTAgMDExMDAxMTE=' > encrypted_ssh.txt
komal@kali:~/Downloads$ base64 -d encrypted_ssh.txt
01101001 01100110 01011111 01111001 00110000 01110101 01011111 01100011 01000000
 01101110 01011111 00100100 01101101 00110011 01101100 01101100 01011111 0111011
1 01101000 01000000 01110100 01011111 01110100 01101000 00110011 01011111 011100
10 00110000 01100011 01101011 01011111 01101001 01110011 01011111 01100011 00110
000 00110000 01101011 01101001 01101110 01100111komal@kali:~/Downloads$
```



```
01101001 01100110 01011111 01111001 00110000 01110101
01011111 01100011 01000000 01101110 01011111 00100100
01101101 00110011 01101100 01101100 01011111 01110111
01101000 01000000 01110100 01011111 01110100 01101000
00110011 01011111 01110010 00110000 01100011 01101011
01011111 01101001 01110011 01011111 01100011 00110000
00110000 01101011 01101001 01101110 01100111
```

```
if_y0u_c@n_$m3ll_wh@t_th3_r0ck_is_c00king
```