Challenges

0ld_is_g0ld

Network Setup

- Connected to HTB OpenVPN Server via OVPN file

Found Vulnerabilities

- Weak Credentials – Dictionary Attack
- Weak Algorithm – PDF MD5

Exploits/Payloads Used

- None

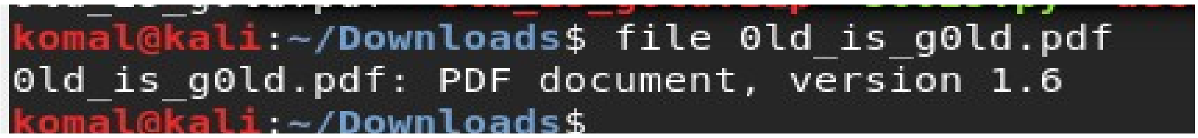
Key Findings

- PDF MD5 Algorithm
- Morse Code

Write-Ups & Screenshots

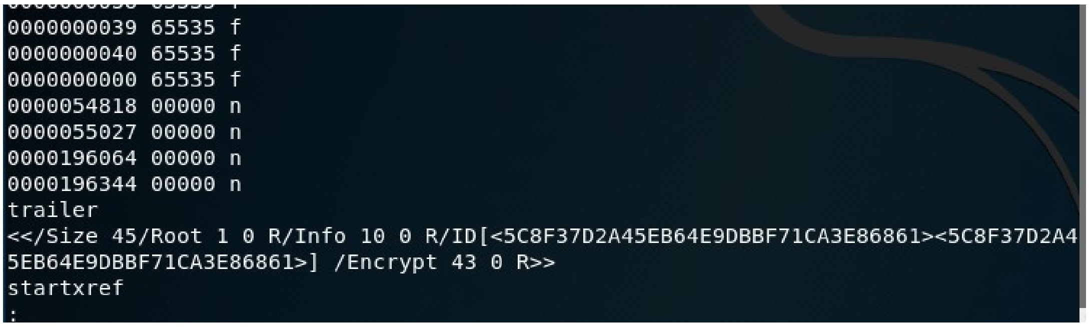
>> The 0ld_is_g0ld.zip file was downloaded from HTB and the given password was 'hackthebox'

>> with the following command: "$ string 0ld_is_g0ld.zip" contained a pdf file. Unzipping this file extracted the contained pdf file.



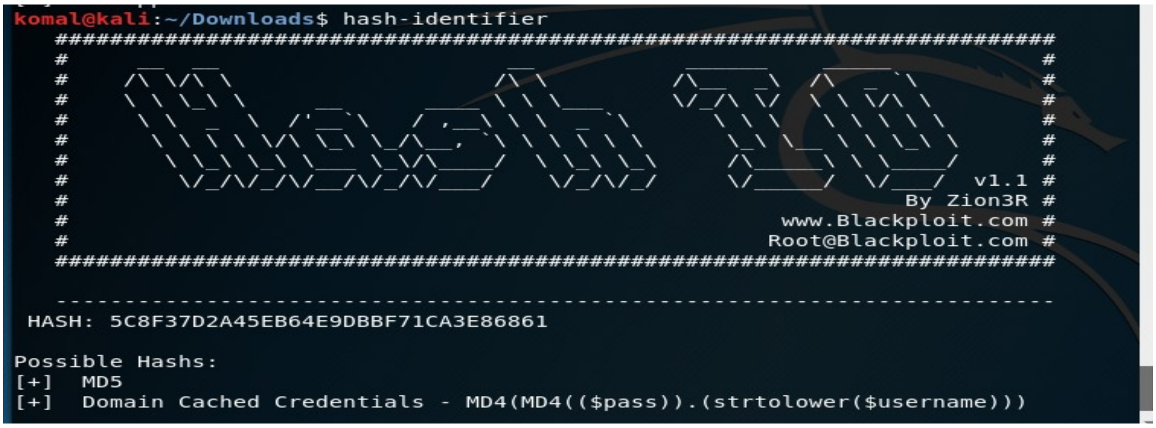
```
komal@kali:~/Downloads$ file 0ld_is_g0ld.pdf
0ld_is_g0ld.pdf: PDF document, version 1.6
komal@kali:~/Downloads$
```

>> Using the command "$ strings 0ld_is_g0ld.pdf" fetched me some interesting results. I found what looks like a hash id as shown below.



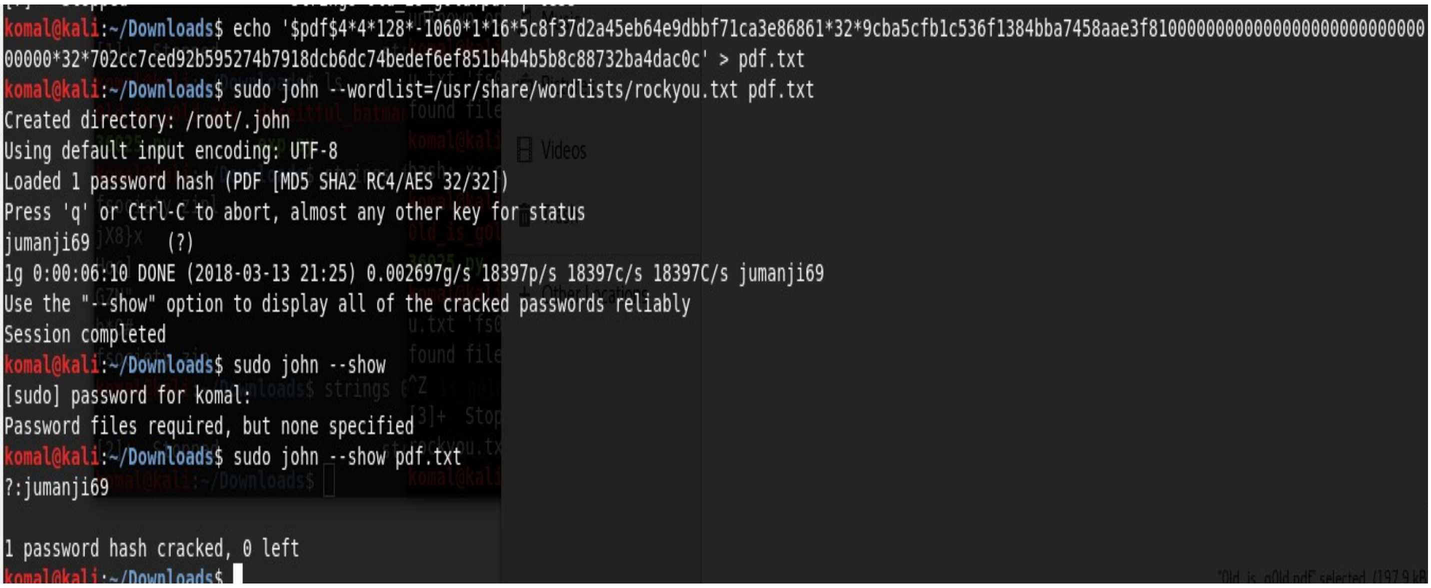
```
0000000039 65535 f
0000000040 65535 f
0000000000 65535 f
0000054818 00000 n
0000055027 00000 n
0000196064 00000 n
0000196344 00000 n
trailer
<</Size 45/Root 1 0 R/Info 10 0 R/ID[<5C8F37D2A45EB64E9DBBF71CA3E86861><5C8F37D2A4
5EB64E9DBBF71CA3E86861>] /Encrypt 43 0 R>>
startxref
:
```

>> The Hash-Identifier identified the hash as an MD5 hash Algorithm.



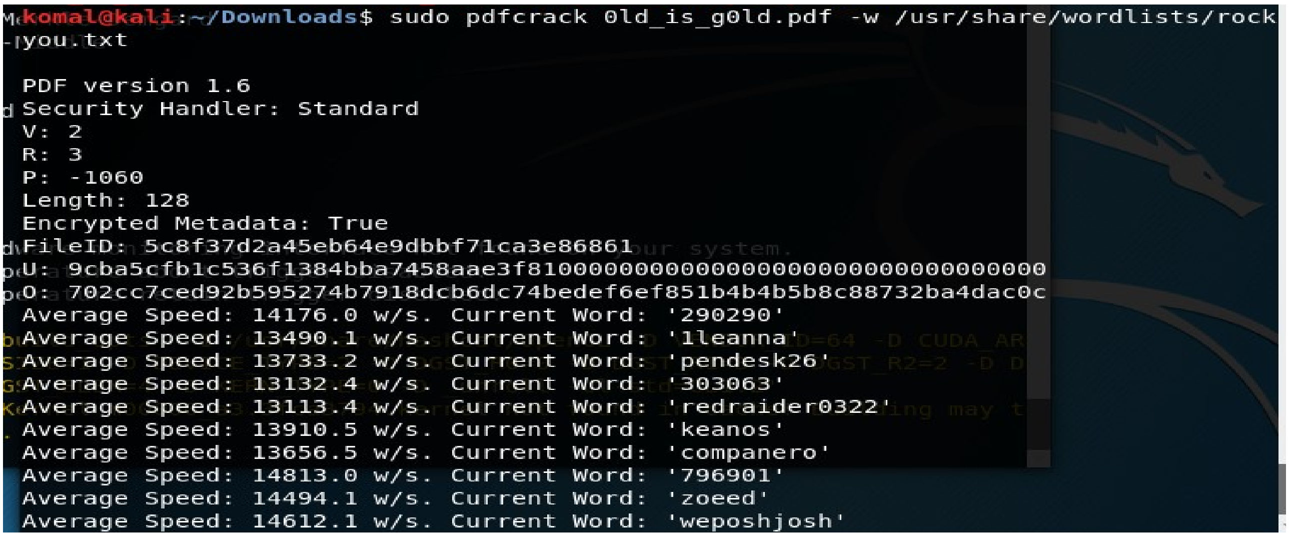
```
komal@kali:~/Downloads$ hash-identifier
   #########################################################################
                                                                     v1.1 #
                                                                By Zion3R #
                                                       www.Blackploit.com #
                                                      Root@Blackploit.com #
   #########################################################################

   --------------------------------------------------------------------------
 HASH: 5C8F37D2A45EB64E9DBBF71CA3E86861

Possible Hashs:
[+]  MD5
[+]  Domain Cached Credentials - MD4(MD4(($pass)).(strtolower($username)))
```

>> The Hash "$pdf$4*4*128*-1060*1*16*5c8f37d2a45eb64e9dbbf71ca3e86861*32*9cba5cfb1c536f1384bba7458aae3f8100000000000000000000000000000000*32*702cc7ced92b595274b7918dcb6dc74bedef6ef851b4b4b5b8c88732ba4dac0c" was found during my google search of the hash id "5c8f37d2a45eb64e9dbbf71ca3e86861". I came across its pdf MD5 hash which I used to extract the password using john the ripper.

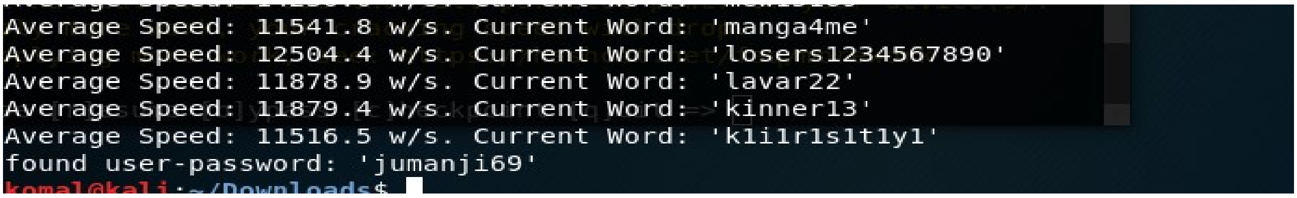


```
komal@kali:~/Downloads$ echo '$pdf$4*4*128*-1060*1*16*5c8f37d2a45eb64e9dbbf71ca3e86861*32*9cba5cfb1c536f1384bba7458aae3f81000000000000000000000000000
00000*32*702cc7ced92b595274b7918dcb6dc74bedef6ef851b4b4b5b8c88732ba4dac0c' > pdf.txt
komal@kali:~/Downloads$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt pdf.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (PDF [MD5 SHA2 RC4/AES 32/32])
Press 'q' or Ctrl-C to abort, almost any other key for status
jumanji69        (?)
1g 0:00:06:10 DONE (2018-03-13 21:25) 0.002697g/s 18397p/s 18397c/s 18397C/s jumanji69
Use the "--show" option to display all of the cracked passwords reliably
Session completed
komal@kali:~/Downloads$ sudo john --show
[sudo] password for komal:
Password files required, but none specified
komal@kali:~/Downloads$ sudo john --show pdf.txt
?:jumanji69

1 password hash cracked, 0 left
komal@kali:~/Downloads$
```

>> Another way is to use the pdfcrack program

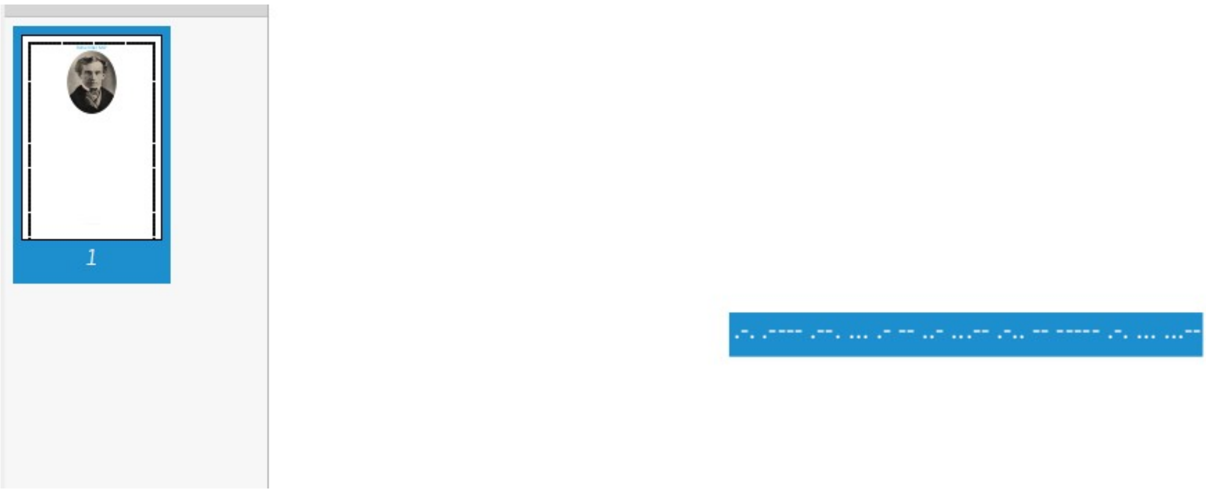


```
komal@kali:~/Downloads$ sudo pdfcrack 0ld_is_g0ld.pdf -w /usr/share/wordlists/rock
you.txt

 PDF version 1.6
 Security Handler: Standard
 V: 2
 R: 3
 P: -1060
 Length: 128
 Encrypted Metadata: True
FileID: 5c8f37d2a45eb64e9dbbf71ca3e86861
U: 9cba5cfb1c536f1384bba7458aae3f8100000000000000000000000000000000
O: 702cc7ced92b595274b7918dcb6dc74bedef6ef851b4b4b5b8c88732ba4dac0c
 Average Speed: 14176.0 w/s. Current Word: '290290'
 Average Speed: 13490.1 w/s. Current Word: '1leanna'
 Average Speed: 13733.2 w/s. Current Word: 'pendesk26'
 Average Speed: 13132.4 w/s. Current Word: '303063'
 Average Speed: 13113.4 w/s. Current Word: 'redraider0322'
 Average Speed: 13910.5 w/s. Current Word: 'keanos'
 Average Speed: 13656.5 w/s. Current Word: 'companero'
 Average Speed: 14813.0 w/s. Current Word: '796901'
 Average Speed: 14494.1 w/s. Current Word: 'zoeed'
 Average Speed: 14612.1 w/s. Current Word: 'weposhjosh'
```

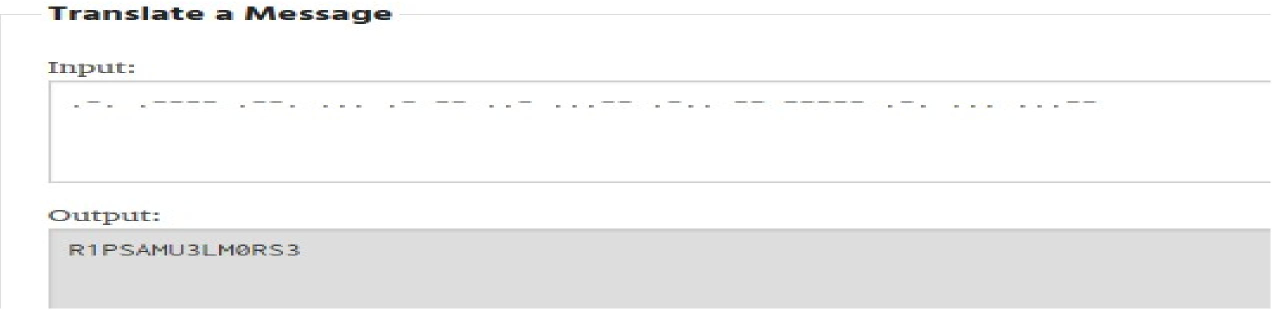


```
Average Speed: 11541.8 w/s. Current Word: 'manga4me'
Average Speed: 12504.4 w/s. Current Word: 'losers1234567890'
Average Speed: 11878.9 w/s. Current Word: 'lavar22'
Average Speed: 11879.4 w/s. Current Word: 'kinner13'
Average Speed: 11516.5 w/s. Current Word: 'k1i1r1s1t1y1'
found user-password: 'jumanji69'
komal@kali:~/Downloads$
```

>> On Opening the pdf file we see a morse code written in tiny characters underneath the image. Converting this data online in a plain text gave me the answer ‘r1psamu3lm0rs3’



```
.-. .---- .--. ... .- -- ..- ...-- .-.. -- ----- .-. ... ...--
```



Translate a Message

Input:

```
.-. .---- .--. ... .- -- ..- ...-- .-.. -- ----- .-. ... ...--
```

Output:

R1PSAMU3LM0RS3