Files

main

Go to file t

1337UP_2022
UTCTF_2022
VishwaCTF_2022
Cryptography/John_the_Rocker
files
img
README.md
Forensic
Misc
OSINT
README.md

LambdaMamba Added writeup for VishwaCTF John the Ripper 9698b91 · 2 years ago History

Name	Last commit message	Last commit date
..		
files	Added writeup for VishwaCTF John the Rocker	2 years ago
img	Added writeup for VishwaCTF John the Rocker	2 years ago
README.md	Added writeup for VishwaCTF John the Ripper	2 years ago

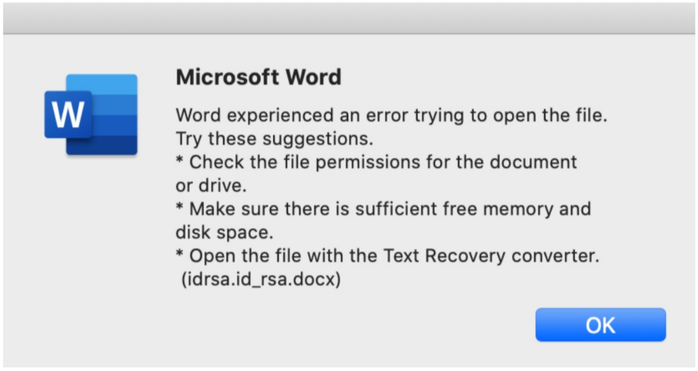
README.md

John the Rocker (Category: Cryptography)

The challenge is the following,

The challenge is the following,

And we are given idrsa.id_rsa.docx. I tried opening this on Word, but gave me the following error,



So I converted this to a .txt file and put it into idrsa.id_rsa.txt. After converting it to a .txt file, the contents were visible,

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,115D424076ADCE7E40ACC1E44E4E791A

flkT1+aCoQZ4YBHg2VRW3x4HzlEKFwqQ+ePMzEi2BIREHXDtHR1+QUrYRSQLzP4E
jDSkmPWPoTvTXRAyXKrQL8FzkvYDcP9hjkzt41tjsRHz2nkI9K+WFm8DNi6qVS9H
J/yWZdvUED6XwwxTFe6D01GwU7yc7xheE4GlIBazk68Q0tNuH34H8T+hnfkTyNA6
BJL861zNhZNIoWm/352vYydnT/HynugCGn+TIu88C+tLBpcLdLSh50OgTiZ8QK2A
Z82PoPfD1ziVmg7E4BIY1/1qJnNxCMTzUG4PbjLpdkRxHu5aOGzbGZK4K0inDNfr
B7ZedUOCSUTN0VGl5/spDO506vSOjzGL9/iDhYNBRvn4hW3V1PE6nRXAQ78r4Z49
ou0r2x7WvzrpFOPXjvlNHUFyWF9x5ZNsqNnr3PfL2wlCVvGq2z/mWvFdmy0tr6nV
FjEpOwrKMt0hvTcCwry8FKAyPDFafpZq4fg90Jd9xCYWJIZMxuEPOY0jfcSC7QOy
woOhMMCFA3mbJJWOAOKynZdx/7fe/0+Q0XMllJDNXNGNqKRqS9OUhKH967FYxw4W
AQHrN2NdT5WoXJhbDu67Z2jb89LAFR+uBlaxauLSYEFatKmAp/IXR4yTX4yn6Ur2
mlrJ6abOjmi+/LcvMN+qCx7pB//MR2HUxcOWdgA5nuXiYBdiSKj8h0Sq3IVVjDFd
Oj1t0D9m6AUsV32qbiXwiiCkOOMHVZH+6sc1ZMKNwR1WGvFBNyR0DVxlXAzyR7zP
nRUXCLihj696lm+Ywe6xsDOPJMl4RHOAvf+cj3fkI3WKhfhTUhoLrEZmIFDNhKrn
JCe4m9p+aNuPSuXL07bxKbYT6D4wlVE4OlkwZyAfc5R/cfE5JYFgwoIW5RJC9nh1
ru/aBj+464986pteEfI0e3nAuDquEvs37Oxv77n/AdW7QmySIb7RrpUfOCcq+rBt
4zg1cS5i2TX1l25h036E45Rn+efM9QBKQEChhgqfLZ9rbQqqm1coOok4sZZ1tWap
7352duKI9fzMq35P9u4T168sYSvZoa2hK7eZZ3KA/MK8u6B1yFiB1E2rEZGnVeOU
KLt1IFxygxZl9yO5yb4pa8t16yKO46+OYmCe9ie7FkOEeq85a0xm0OB3HVxL/40/
116u2fJCRoDBjNZ1J4ujYwYUpWEfVoN26KRRiyRMJbHX9QwuW6k+b1OjLgjU2IaR
4BgG6xBTmM3fRQZhWbJ+06ibWDcIRdZOP02iksp/LdJtqtuYIWf2epUx3oBMrSN/
bFDUmLDzfSUCvz4MdZNp8FE1El M2NK9PWYPe3XA5lzjk19jxWD7M4WKLTjQJu9P0
PB4x+nHPj5j6XONZ74IbM1f7S4oRuhBCs5hPMgxDr7xSa0ROFsTauCeQ6N22JwIk
GzMpmzBzJtL5/SzFCuN148sMUOASnXLSYd79dB15M0nVRo6Iz9mytF/QVuci+8h+
6luGQBgih+L5ghx1qvUXwNyU+Id9fZYRA8pH2hy5pPWVsaws/1cLOc5PBzOaq17G
90iM4IyzSN2AO8/6HnSJ9tZSCG5cdRq+r1ROF30QnvnUowsbq0eeT4TVfb+kCaHx
-----END RSA PRIVATE KEY-----
```

Therefore, this was a RSA private key and I assumed the objective was to crack this RSA private key. Also, the name of the challenge was `John the Rocker`, so I assumed that this was a reference to `John the Ripper` and I had to use John the Ripper to crack the RSA private key.

I first made the hash file of idrsa.id_rsa.txt using,

```
$ ssh2john idrsa.id_rsa.txt > hashidrsa.hash
```

Then specified rockyou.txt as the wordlist using,

```
$ john hashidrsa.hash -wordlist=rockyou.txt
```

After a few minutes, John the Ripper found the password, which was `!!**john**!!`

```
┌──(kali㉿kali)-[~/Desktop/crack]
└─$ ssh2john idrsa.id_rsa.txt > hashidrsa.hash

┌──(kali㉿kali)-[~/Desktop/crack]
└─$ john hashidrsa.hash -wordlist=rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
!!**john**!!      (idrsa.id_rsa.txt)
1g 0:00:00:03 DONE (2022-03-21 05:38) 0.2865g/s 4109Kp/s 4109Kc/s 4109KC/s  !! ..ashli.. !! .. !!!yeah
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

The challenge didn't have any further instructions, so I assumed that the flag would be,

```
vishaCTF{!!**john**!!}
```

and submitting it confirmed that this was the flag.