CTF Tricks

Mu Changrui

February 2021

1 .png

89 50 4E 47 0D 0A 1A 0A

1.1 hidden file

binwalk apple.png # to check if there is any hidden file inside
binwalk -e apple.png # to seperate hidden file from the png(if any)
foremost apple.png # also to seperate hidden file

1.2 broken png

WinHex in Windows to open the png
HexFiend in MacOs
Information may be hidden in intro

1.3 XOR

Perhaps two files can be seperated
.png has some certain headers

1.4 RGB

Hidden info with RGB and some length of colors that human is unable to detect

tool: stegsolve
java -jar stegsolve.jar

1.5 recommended web

https://www.jianshu.com/p/02fdd5edd9fc

2 .zip

2.1 encrypted zip

fcrackzip apple.zip a tool to crack the zip directly

2.2 hidden file

3 Web

3.1 environment

Mac to open Apache and PHP environment: sudo apachectl start
To close: sudo apachectl stop
After enter open command, can enter localhost in Brewer, it will show ”It Works” if you successfully connect
Where the localhost’s php runs: /Library/WebServer/Documents/
Recommendation instro: (environment) https://www.jianshu.com/p/86d297822a24
(environment) https://www.ioa.tw/macOS/Apache.html
(run) https://blog.csdn.net/JonWu0102/article/details/87707088

3.2 PHP

1. https://www.geeksforgeeks.org/how-to-execute-php-code-using-command-line/
2. https://www.php.net/manual/en/function.system.php

3. https://github.com/bwall/HashPump 4. https://xz.aliyun.com/t/2563
5. https://www.cnblogs.com/pcat/p/5478509.html 6.

3.3 reptile

recommended web:
1. https://blog.csdn.net/junli$_c hen/article/details/$53670887

4 Cryptography

Recommended web: 1. https://blog.csdn.net/qq$_4$0837276$/article/details/$83080460.
2.$http : //ctf.ssleye.com/$

4.1 Diffie-Hellman key

$K = A^b modp = B^a modp$
$A = g^a modp$
$B = g^b modp$
$K = g^{ab} modp$
In most case, a and b r small, but p is a very large prime(more than hundreds), A and B should also be big, at least O($p^{0.5}$)
For small p, it's possible to get the dicrete log
For dicrete log intro: https://www.doc.ic.ac.uk/ mrh/330tutor/ch06s02.html: :text=Discrete%20logarithm
An awesome tool: sympy.ntheory (https://docs.sympy.org/latest/modules/ntheory.html)

4.2 ECB

recommended website
1. https://notsosecure.com/hacking-crypto-fun-profit/
2. https://crypto.stackexchange.com/questions/55673/why-is-byte-at-a-time-ecb-decryption-a-vulnerability
3. https://github.com/ashutosh1206/Crypton/tree/master/Block-Cipher/Attack-ECB-Byte-at-a-Time

4. https://robertheaton.com/2013/07/29/padding-oracle-attack/

5. https://dr3dd.gitlab.io/cryptography/2018/10/11/Simple-Attack-On-AES-ECB-Mode/

6. https://eldipa.github.io/book-of-gehn/articles/2018/06/10/Breaking-ECB.html

4.3 CBC

1. https://segmentfault.com/a/1190000019793040

2. https://samsclass.info/141/proj/p14pad.htm

3. https://jiang-zhenghong.github.io/blogs/PaddingOracle.html

4. https://en.wikipedia.org/wiki/Padding$_oracle_attack$

5.$https : //resources.infosecinstitute.com/topic/cbc - byte - flipping - attack - 101 - approach/$

6.$https : //www.freebuf.com/articles/web/15504.html$

7.$https : //paper.seebug.org/1123/$ 8.

4.4 leet

1. https://notsosecure.com/hacking-crypto-fun-profit/

2. https://en.wikipedia.org/wiki/Leet: :text=Leet%20(or%20%221337%22),used%20primarily%20on%20

3. https://wenku.baidu.com/view/fa15fc0590c69ec3d5bb75ad.html

4.5 leet

https://www.forece.net/post/508.htm

5 Conclusion

There is a difference between knowing the path and walking the path.

图 1: The Universe