Project 3: Password and Key

CS 4371 COMPUTER SYSTEMS SECURITY

Mack Scott | Blake Burns | Christian Coulter | Muhammed Rasheed | Cody Neal
GROUP 1

Section I

Introduction

i. Summary

In this project, we learned cryptographic algorithms and protocols using passwords and keys, how to crack passwords and keys using different methods as well as how to use and develop various security tools. We also learned how to use brute force attacks using dictionary files and tools such as aircrack.

ii. Task Assignments

For task one, our group had to setup the network properly. We first made sure that all of the devices were wired correctly according to Figure 1 as well as configuring the NICs of Computer A.B, B.a, and B.2 according to the same figure. After making sure that the network was configured properly, we started the SSH service in Computer B.2. We also configured the Firewall B so that no outside computers could access any internal computers and services.

For task two, we had to crack the WEP security protocol. We first had to turn off the ethernet card in Computer A.B and turn of the wireless card instead. For the wireless card, we setup a static IP address of Network B. We found the wireless network in Network B and recorded the SSID, the channel number, and the MAC address of the access point using the command “iwlist”. After this, we used aircrack to find the WEP key of the wireless network. Once the key was found, we set up the wireless card of Computer A.B to access the wireless network of Network B. Then we had to ping to the gateway of Network B and Computer B.2 to make sure that we had the correct access.

For task three, we had to use a dictionary password crack. Once we had gotten into the network, we retrieved a dictionary file called “dictionary.txt” that has the correct password for User25 that we are trying to access. We made a program that would test each password in the dictionary.txt file until we could ssh to Computer B.2 as User25. Once we had ssh into Computer B.2 as User25, we retrieved two files from the “files” directory of User25.

For task four, we used cryptanalysis and brute force to crack passwords. Using the encrypted pdf file from the previous task, we had to decrypt the flawed encryption algorithm. For the second encrypted file from the previous task, we had to creat a program to crack the key of the encryption using the brute force method since this file was encrypted by the DES-ECB encryption algorithm.

iii. Team Evaluation

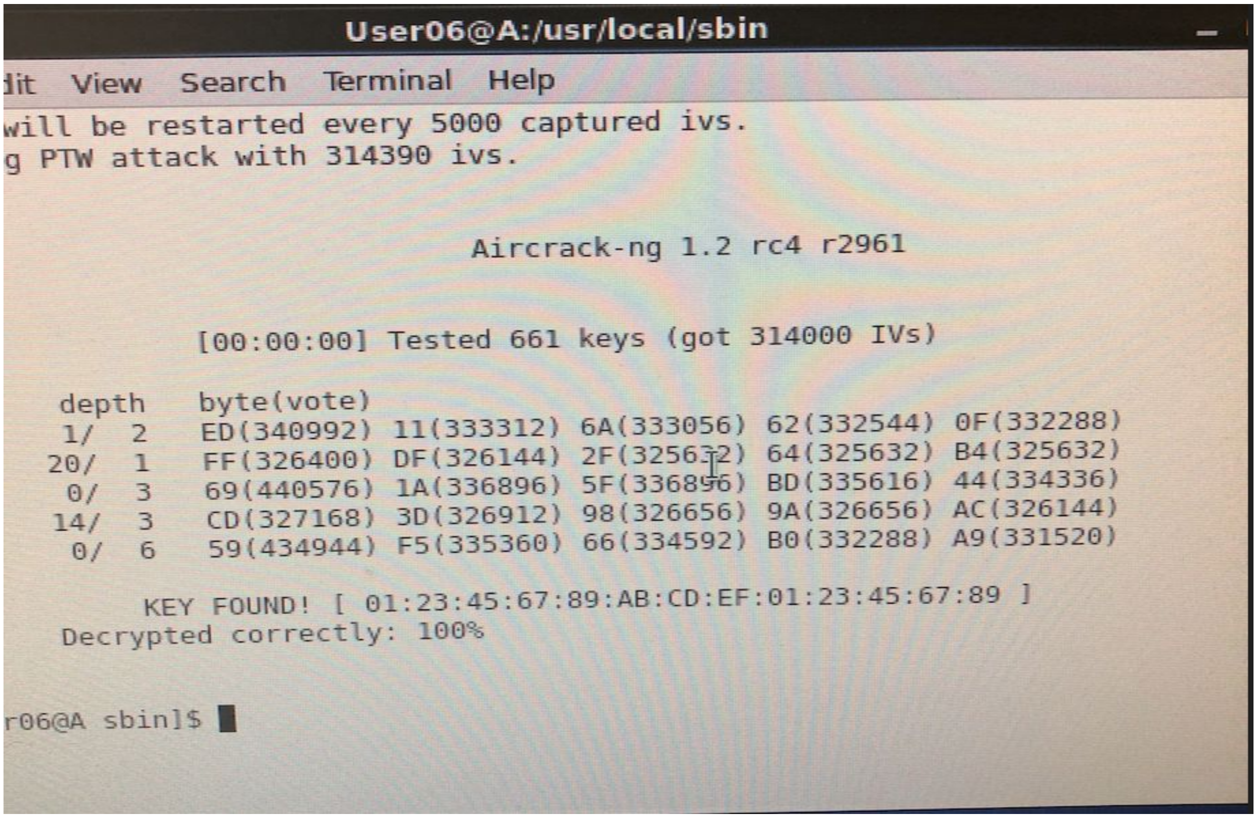
Each week our team was able to meet during our scheduled lab time to make sure that the project was completed on time. For each of the tasks, the team was able to work together to not only finish the task, but learn new cracking tools and security techniques. Task one, which was setting up the network, was assigned to Blake Burns. Blake was able to set up the network correctly while the rest of the team was there to help out. Task two, which was cracking the WEP security protocol, was assigned to Mack Scott. Mack was able to successfully crack the security protocol with the help of the rest of the team. Task three, which was using the Dictionary password crack, was assigned to Christian Coulter and Cody Neal. They were able to complete the task and find the password of User25 using the dictionary password crack with the help of the team. Task four, which was using cryptanalysis and brute force password crack, was assigned to Muhammed Rasheed and Blake Burns. Both Blake and Muhammed were able to complete the task with the help of the rest of the team.

Who Wrote What: Blake Burns (Introduction), Mack Scott(Task Two), Christian Coulter and Cody Neal(Task Three), Muhammed Rasheed and Blake Burns (Task Four).

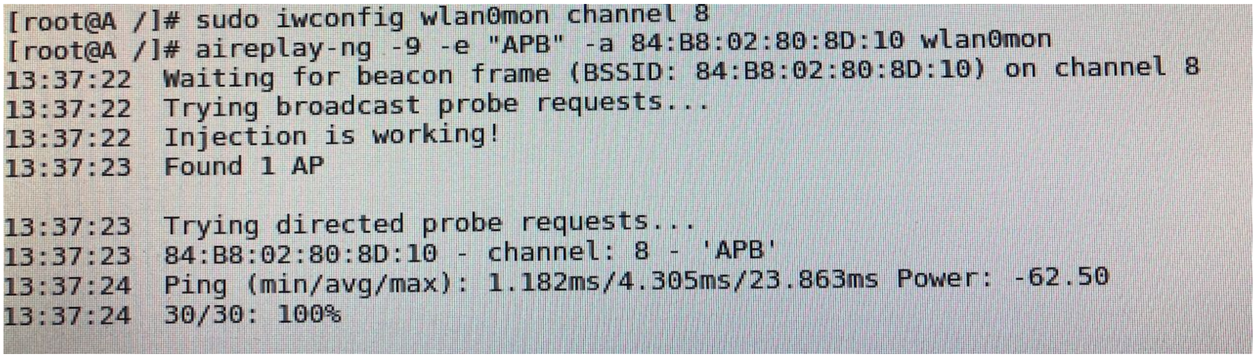
Section II

Task II

a) Show the screen shot when you are running aircrack and obtaining the key.

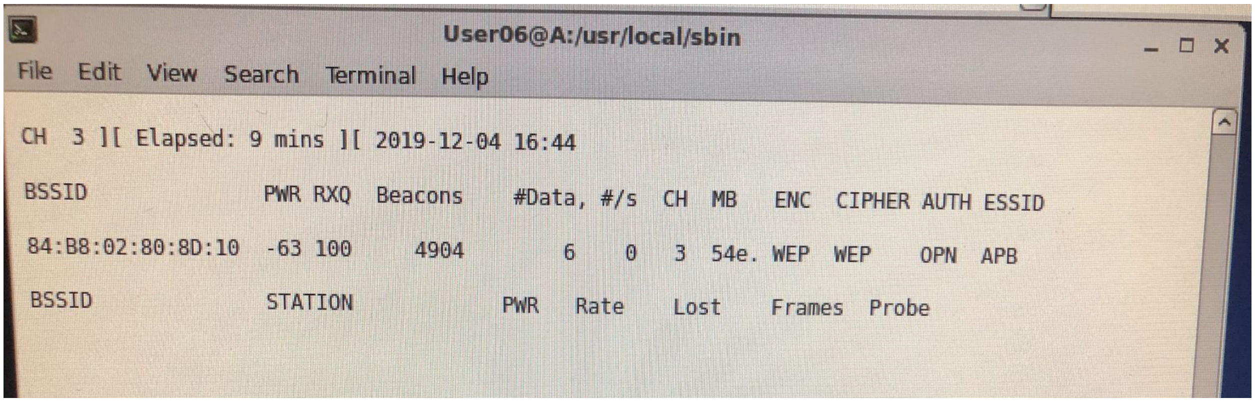


```
will be restarted every 5000 captured ivs.
g PTW attack with 314390 ivs.


                    Aircrack-ng 1.2 rc4 r2961


        [00:00:00] Tested 661 keys (got 314000 IVs)

   depth   byte(vote)
    1/  2   ED(340992) 11(333312) 6A(333056) 62(332544) 0F(332288)
   20/  1   FF(326400) DF(326144) 2F(325632) 64(325632) B4(325632)
    0/  3   69(440576) 1A(336896) 5F(336896) BD(335616) 44(334336)
   14/  3   CD(327168) 3D(326912) 98(326656) 9A(326656) AC(326144)
    0/  6   59(434944) F5(335360) 66(334592) B0(332288) A9(331520)

       KEY FOUND! [ 01:23:45:67:89:AB:CD:EF:01:23:45:67:89 ]
   Decrypted correctly: 100%


r06@A sbin]$
```



```
[root@A /]# sudo iwconfig wlan0mon channel 8
[root@A /]# aireplay-ng -9 -e "APB" -a 84:B8:02:80:8D:10 wlan0mon
13:37:22  Waiting for beacon frame (BSSID: 84:B8:02:80:8D:10) on channel 8
13:37:22  Trying broadcast probe requests...
13:37:22  Injection is working!
13:37:23  Found 1 AP

13:37:23  Trying directed probe requests...
13:37:23  84:B8:02:80:8D:10 - channel: 8 - 'APB'
13:37:24  Ping (min/avg/max): 1.182ms/4.305ms/23.863ms Power: -62.50
13:37:24  30/30: 100%
```

b) Report how long it takes to crack the WEP key and how many packets are captured in order to crack the key.



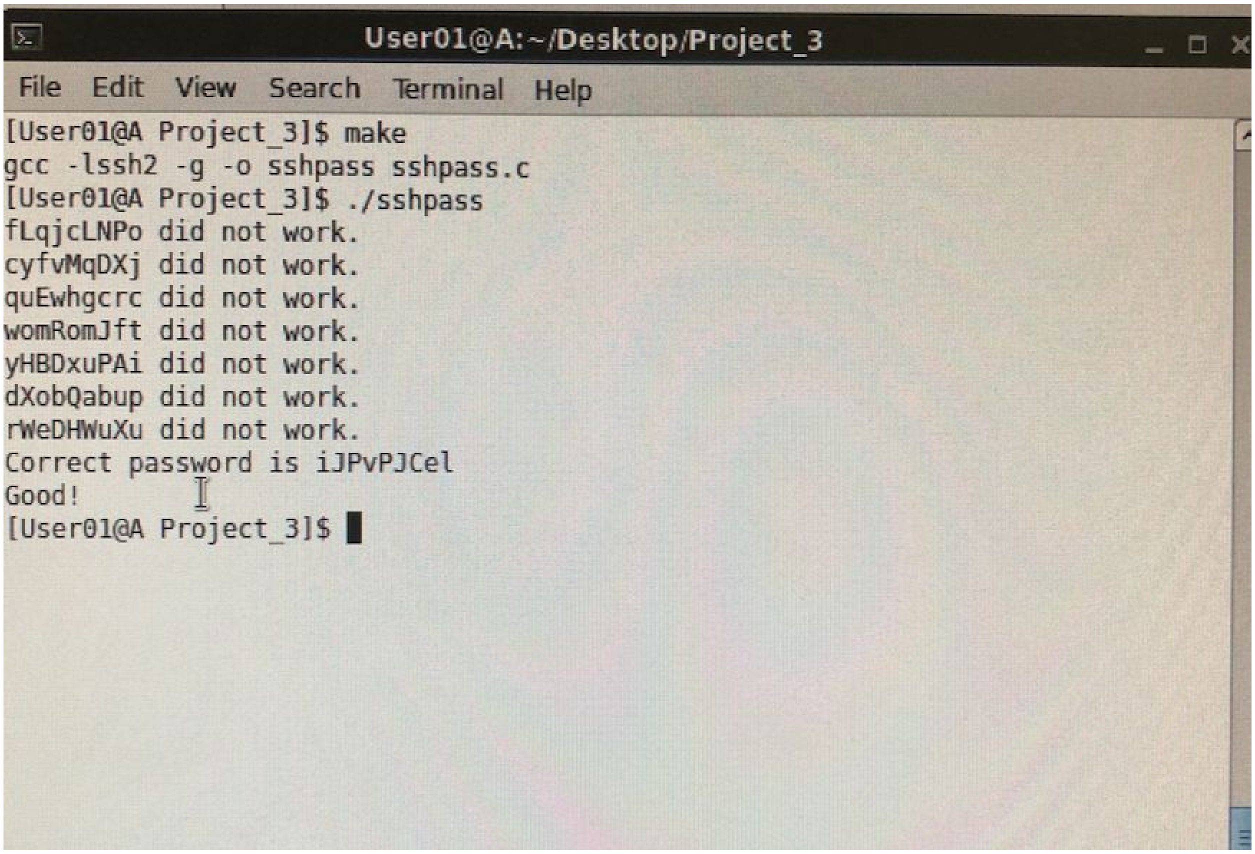
```
CH  3 ][ Elapsed: 9 mins ][ 2019-12-04 16:44

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

84:B8:02:80:8D:10  -63 100     4904        6    0   3  54e. WEP  WEP    OPN  APB

BSSID              STATION            PWR   Rate    Lost     Frames  Probe
```

It took 9 minutes and roughly 60,000 packets in order to crack the WEP key.

Section III

Task III

a) Show the screen-shot of your program when you are testing each password and obtaining the password to ssh Computer B.2 as “User”.



User01@A:~/Desktop/Project_3
File Edit View Search Terminal Help

```
[User01@A Project_3]$ make
gcc -lssh2 -g -o sshpass sshpass.c
[User01@A Project_3]$ ./sshpass
fLqjcLNPo did not work.
cyfvMqDXj did not work.
quEwhgcrc did not work.
womRomJft did not work.
yHBDxuPAi did not work.
dXobQabup did not work.
rWeDHWuXu did not work.
Correct password is iJPvPJCel
Good!
[User01@A Project_3]$
```

b) Report how long it takes to find the password.

It took us about 5 minutes to correctly find the password since the dictionary.txt file only had 10 entries in it.

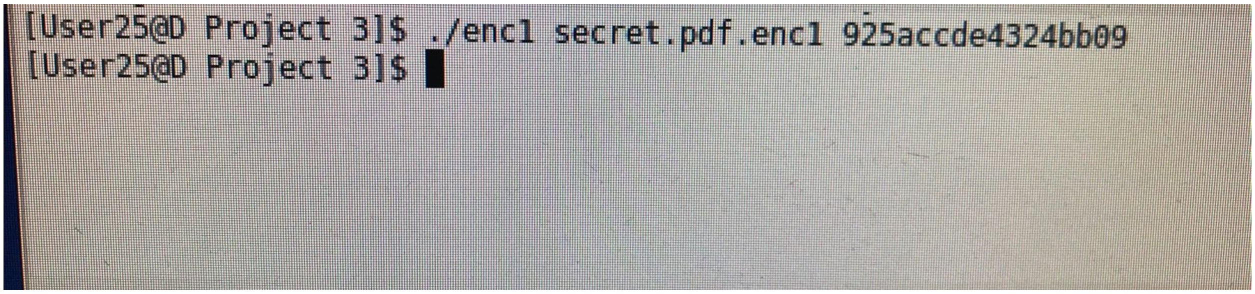
c) If the password is in the file “dictionary.real.txt”, estimate how long it will take to find the password.

479,827 total entries = 3998.56 hours = 166.61 Days
It would take roughly 167 days to find the password in the dictionary.real.txt file.

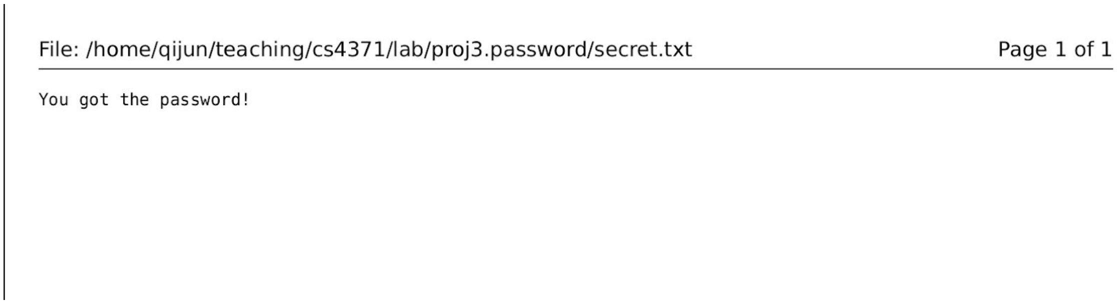
Section IV

Task IV

a) Show the screen-shot of your cryptoanalysis program when you get the key and the content of the encrypted file secret.pdf.enc1.



```
[User25@D Project 3]$ ./enc1 secret.pdf.enc1 925accde4324bb09
[User25@D Project 3]$ █
```



File: /home/qijun/teaching/cs4371/lab/proj3.password/secret.txt   Page 1 of 1

```
You got the password!
```

b) Show the screen-shot of your DES program when it deciphers a testing file. The test file is created by you and encrypted by enc2.c.

c) Show the screen-shot of your DES program when you are brute force cracking the key.

d) Report how many keys are tested in 10 minutes.

We had 7,835,228 keys tested in 10 minutes.

e) Estimate how long it will take to find the key.

There are a total of 1.8446744e^19 (2^64) keys in standard DES.

We had 7,835,228 keys tested in 10 minutes.

That would be 47,011,368 keys in an hour.

It would take over a million years to try all of the passwords.