

Project 3: Password and Key

C. Project Report

CS 4371

Dr. Gu

04/30/2019

Group 5

Abebe Aryam

Droddy Richard

Geng Rebecca

Rakhsha Hanna

Vielma Oswaldo

Section I (Introduction):

On this project, our team worked on passwords and keys. The project objective was to use passwords and keys, which protect a system, to learn cryptographic algorithms and protocols. We were also able to learn how to crack passwords and keys, as well as develop and use the various security tools. First, we setup the network. Second, we practiced cracking WEP. Third, we were working with a text file to password check. Finally, we did cryptanalysis and brute force password cracking. On Task I, all group members worked on getting the system set up and double checking before each time spent at the lab. On Task II, Aryam and Hanna were able to crack the WEP key. The rest of the group worked on searching for ways to troubleshoot in between. On Task III Rebecca and Aryam worked on all parts. On Task IV Aryam, Rebecca, and Hanna worked on getting all parts. Richard helped with research and troubleshooting throughout.

While writing this paper our team worked on various parts. Aryam worked on the introduction, conclusion, Task III part c, Task IV part e. Rebecca worked on Task III part b and Task IV part d. Hanna worked on Task II and Task IV part d. Oswaldo did some research to find useful commands that may be used for Task II and III as well as made minor revisions/typo corrections on report. Richard worked on grammatical revisions and proofreading.

Section II (Task II):

a) Below are our screenshots of us running the aircrack and obtaining the key.

```
User05@A:~  
Aircrack-ng 1.2 rc4 r2961  
[00:00:00] Tested 820 keys (got 62838 IVs)  
KB depth byte(vote)  
0 0/ 1 01(94464) 4E(73728) 07(71936) 31(71936) 11(71424)  
1 7/ 1 A1(70912) 14(70656) 4F(70400) 93(70400) 22(70144)  
2 0/ 1 69(89600) 8C(73472) EF(73472) 93(72704) 96(70912)  
3 4/ 25 4C(71168) FB(70656) 22(69632) AF(69632) F2(69632)  
4 26/ 4 AD(68096) 3D(67840) 54(67840) A7(67840) E5(67840)  
KEY FOUND! [ 01:23:45:67:89:AB:CD:EF:01:23:45:67:89 ]  
Decrypted correctly: 100%  
[User05@A ~]$  
CH 9 ][ Elapsed: 11 mins ][ 2019-04-22 20:13  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
84:B8:02:80:76:90 -66 99 6733 79476 412 9 54e. WEP WEP OPN APD  
BSSID STATION PWR Rate Lost Frames Probe  
84:B8:02:80:76:90 30:B5:C2:B5:C3:4E 0 48 - 1 24 175745  
CH 9 ][ Elapsed: 12 mins ][ 2019-04-22 20:13  
BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID  
84:B8:02:80:76:90 -65 99 6922 88037 422 9 54e. WEP WEP OPN APD  
BSSID STATION PWR Rate Lost Frames Probe  
84:B8:02:80:76:90 30:B5:C2:B5:C3:4E 0 48 - 1 26 194977  
Read 284399 packets (got 92762 ARP requests and 91920 ACKs), sent 96410 packets.  
Read 284547 packets (got 92811 ARP requests and 91968 ACKs), sent 96459 packets.  
Read 284692 packets (got 92859 ARP requests and 92015 ACKs), sent 96508 packets.  
Read 284837 packets (got 92907 ARP requests and 92062 ACKs), sent 96556 packets.  
Read 284976 packets (got 92950 ARP requests and 92108 ACKs), sent 96604 packets.  
Read 285118 packets (got 92994 ARP requests and 92154 ACKs), sent 96653 packets.  
Read 285260 packets (got 93042 ARP requests and 92199 ACKs), sent 96701 packets.  
Read 285402 packets (got 93086 ARP requests and 92246 ACKs), sent 96750 packets.  
Read 285547 packets (got 93135 ARP requests and 92293 ACKs), sent 96799 packets.  
Read 285696 packets (got 93185 ARP requests and 92341 ACKs), sent 96848 packets.  
Read 285839 packets (got 93232 ARP requests and 92387 ACKs), sent 96896 packets.  
Read 285983 packets (got 93281 ARP requests and 92435 ACKs), sent 96945 packets.  
Read 286126 packets (got 93329 ARP requests and 92481 ACKs), sent 96993 packets.  
Read 286269 packets (got 93377 ARP requests and 92527 ACKs), sent 97042 packets.  
Read 286411 packets (got 93422 ARP requests and 92573 ACKs), sent 97091 packets.  
Read 286559 packets (got 93470 ARP requests and 92621 ACKs), sent 97139 packets.  
Read 286699 packets (got 93514 ARP requests and 92666 ACKs), sent 97187 packets.  
Read 286844 packets (got 93561 ARP requests and 92713 ACKs), sent 97236 packets.  
Read 286991 packets (got 93610 ARP requests and 92760 ACKs), sent 97284 packets.  
Read 287139 packets (got 93659 ARP requests and 92807 ACKs), sent 97333 packets.  
Read 287281 packets (got 93706 ARP requests and 92853 ACKs), sent 97381 packets.  
Read 287421 packets (got 93751 ARP requests and 92898 ACKs), sent 97430 packets.  
Read 287566 packets (got 93798 ARP requests and 92945 ACKs), sent 97478 packets.  
(.500 pps)
```

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

Aircrack took about 11 mins to crack the WEP key. It read a total of 287,566 packets and sent 97,478 packets.

Section III (Task III):

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

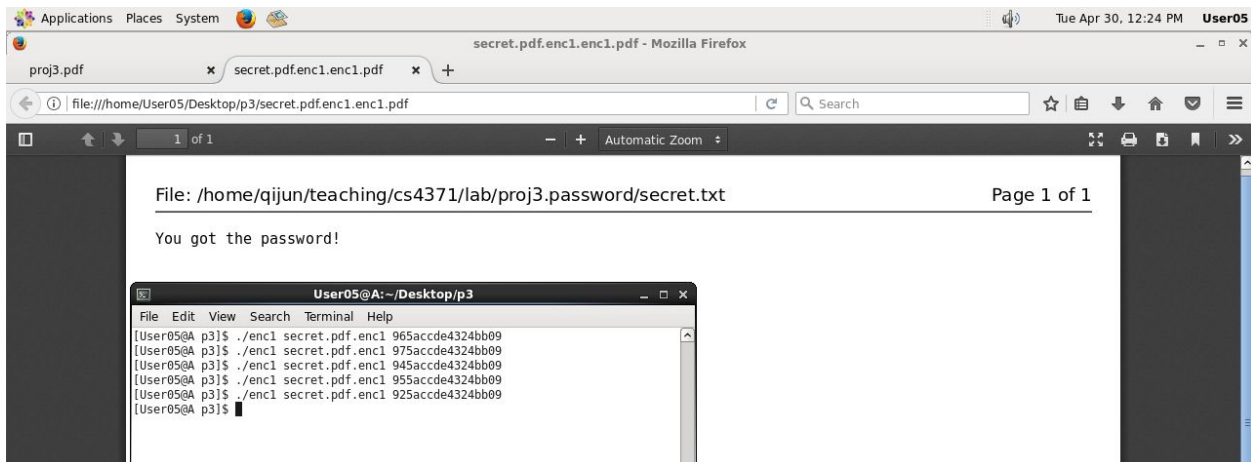
```
User05@A: ~/Desktop
File Edit View Search Terminal Help
[User05@A project3]$ ./sshpas dictionary.txt
Failed to authenticate the user!
Failed to authenticate the user!
Failed to authenticate the user!
Failed to authenticate the user!
Failed to authenticate the user!
Failed to authenticate the user!
Failed to authenticate the user!
Failed to authenticate the user!
Good!
Get the password!
[User05@A project3]$
```

b) Report how long it takes to find the password.
It took our program around 17-18 seconds to find the password.

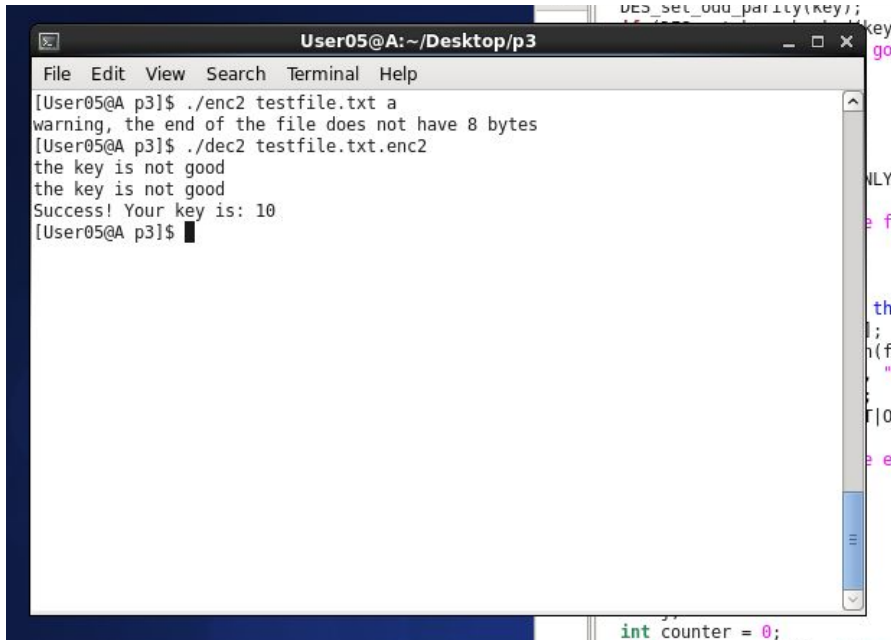
c) If the password is in the file “dictionary.real.txt”, estimate how long it will take to find the password.
The amount of words in dictionary.real.txt is in the hundreds of thousands. The position of the password was the 9th read from the file, which our program took around 18 seconds to find. If we divide the amount of words in the real dictionary by the amount of iterations to find the password of the dictionary file, then multiply that by the time it took to find the password, then we will get this amount to brute force. So, at least 11 days after the math.

Section IV (Task IV):

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

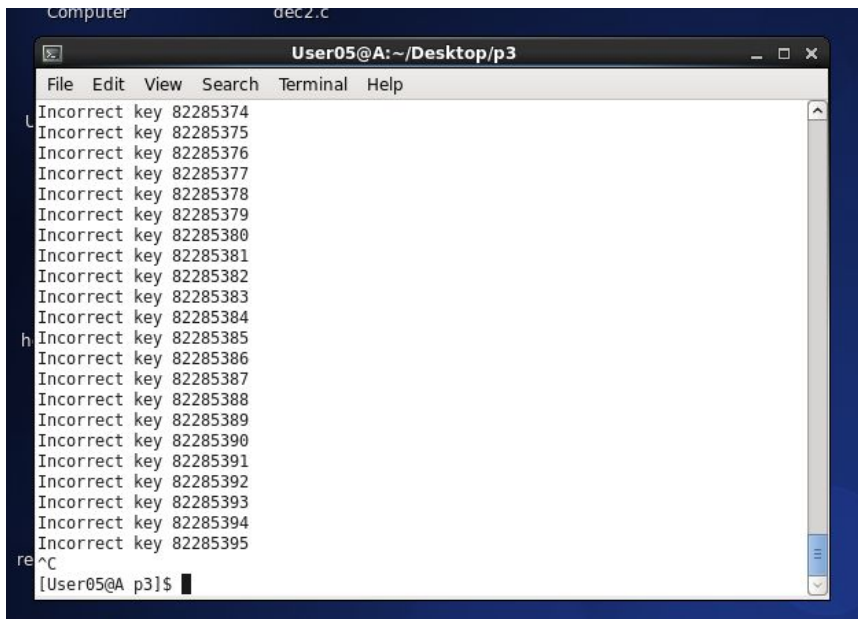


b) Show the screenshot of your cryptoanalysis program when it deciphers a testing file. The test file is created by you and encrypted by enc2.c.



```
User05@A:~/Desktop/p3
File Edit View Search Terminal Help
[User05@A p3]$ ./enc2 testfile.txt a
warning, the end of the file does not have 8 bytes
[User05@A p3]$ ./dec2 testfile.txt.enc2
the key is not good
the key is not good
Success! Your key is: 10
[User05@A p3]$
```

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



```
Computer dec2.c
User05@A:~/Desktop/p3
File Edit View Search Terminal Help
Incorrect key 82285374
Incorrect key 82285375
Incorrect key 82285376
Incorrect key 82285377
Incorrect key 82285378
Incorrect key 82285379
Incorrect key 82285380
Incorrect key 82285381
Incorrect key 82285382
Incorrect key 82285383
Incorrect key 82285384
Incorrect key 82285385
Incorrect key 82285386
Incorrect key 82285387
Incorrect key 82285388
Incorrect key 82285389
Incorrect key 82285390
Incorrect key 82285391
Incorrect key 82285392
Incorrect key 82285393
Incorrect key 82285394
Incorrect key 82285395
^C
[User05@A p3]$
```

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

The number of keys tested in 10 minutes was around 82,285,395. The number of keys in the encryption was in the 2^{50} .

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

It will take at least 24 hours. This comes from multiplying our keys from 10 minutes, converting it to 60 minutes, then by 24 hours. This calculation will continue to go on for days, weeks, months, years and so on.

Conclusion

Completing this project has expanded our knowledge on working with passwords and keys. Our project met the overall objective in using passwords and keys to protect a system. This project also allowed us to learn cryptographic algorithms and protocols. More specifically, we were able to learn how to crack passwords, develop keys, and utilize other security methods. Steps we took such as setting up the configurations, adjusting cisco, cracking WEP, ssh with passwords have all been a challenge but important to comprehend. Finally, we used cryptanalysis and brute force password cracking. In the future, we will be able to look at this project to further grasp cryptography.