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

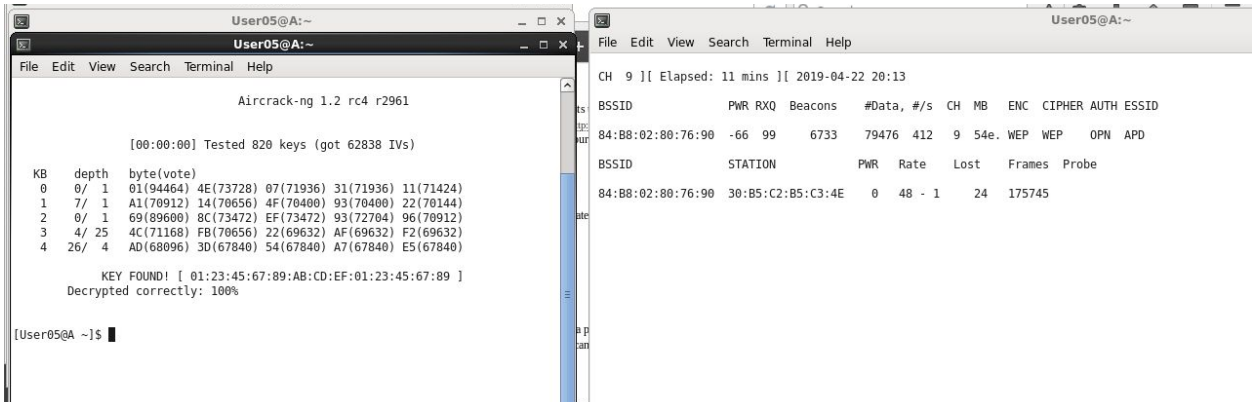
Section I (Introduction):

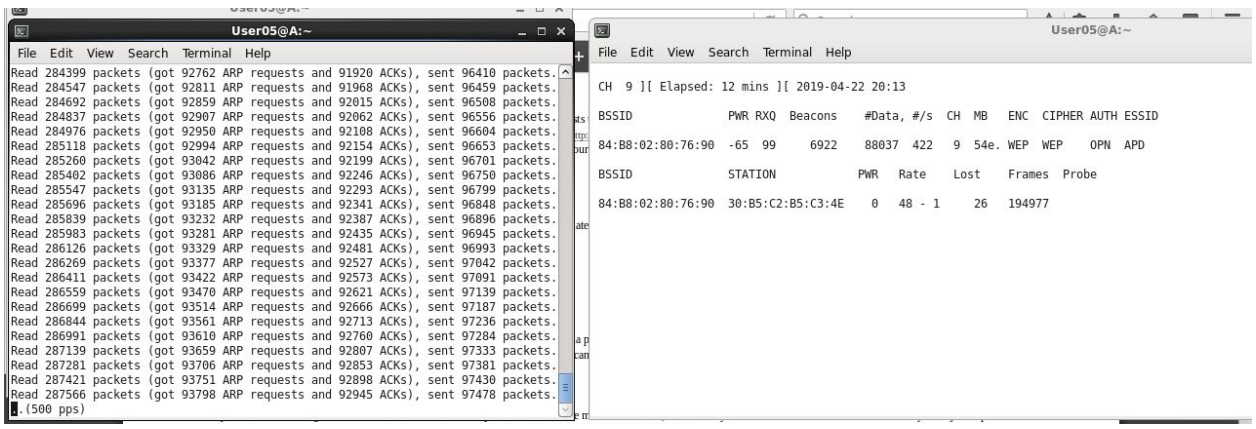
On this project, our team worked on passwords and keys. The project objective was to use passwords and keys, which protect a system, to learn cryptographic algorithms and protocols. We were also able to learn how to crack passwords and keys, as well as develop and use the various security tools. First, 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.



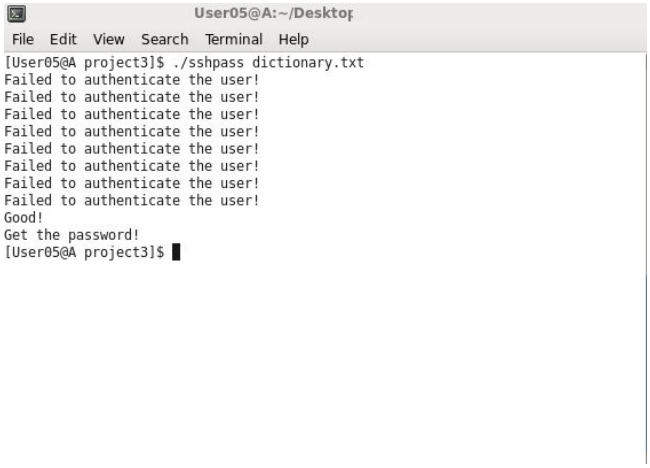


b) Report how long it takes to crack the WEP key and how many packets are captured in order to crack the key.

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”.

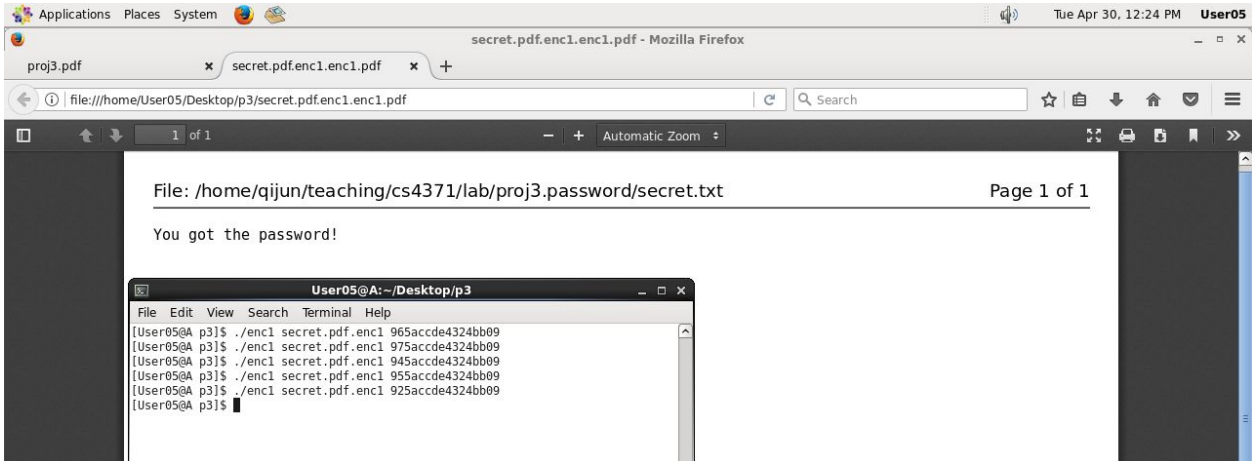


b) Report how long it takes to find the password.
It took our program around 17-18 seconds to find the password.

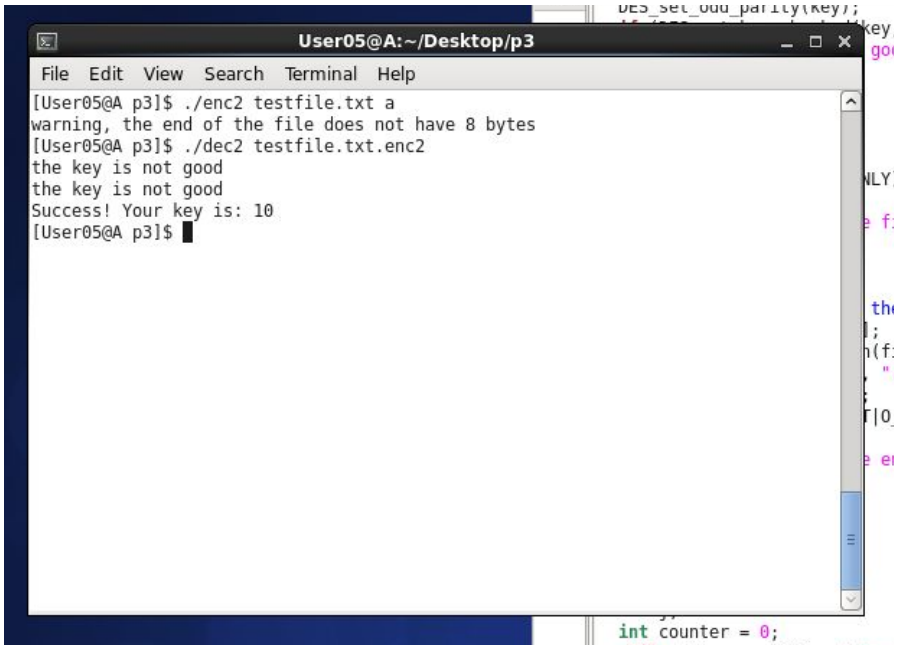
c) If the password is in the file "dictionary.real.txt", estimate how long it will take to find the password.
The amount of words in dictionary.real.txt is in the hundreds of thousands. The position of the password was the 9th read from the file, which our program took around 18 seconds to find. If we 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):

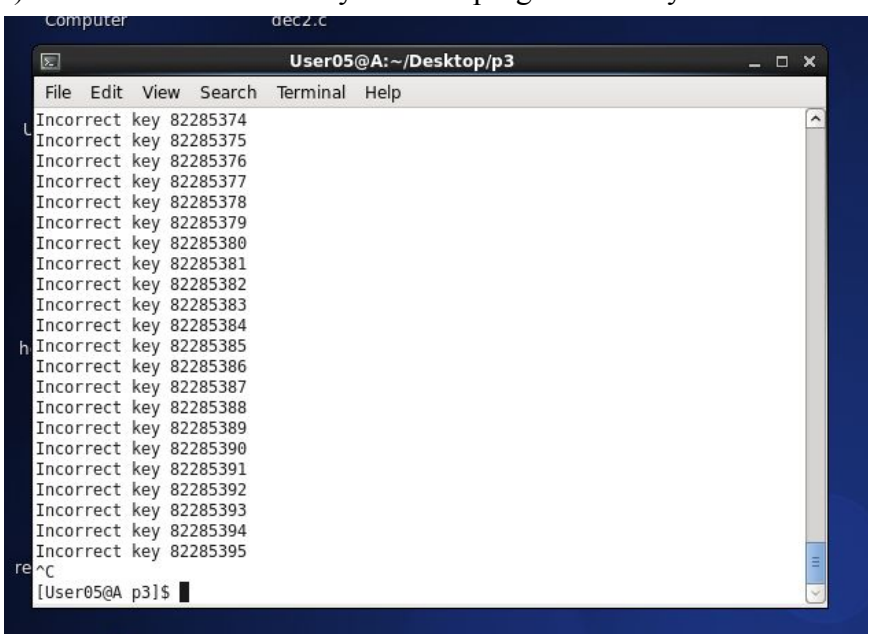
a) Show the screenshot of your cryptoanalysis program when you get the key and the content of the encrypted file secret.pdf.enc1.



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.



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



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.