Project 3: Password and Key

Due Date: 04/30

A. Project Objectives

Passwords and keys are the secrets that protect a system. In this project, you will
a) Learn cryptographic algorithms and protocols using passwords and keys;
b) Learn to crack passwords and keys using different methods;
c) Learn to use and develop various security tools.

B. Project Tasks

The networking devices are assigned to three groups.
Group B manages Computer A.B and the devices in Network B.
Group C manages Computer A.C and the devices in Network C.
Group D manages Computer A.D and the devices in Network D.
Group E manages Computer A.E and the devices in Network E.
Group F manages Computer A.F and the devices in Network F.
Group G manages Computer A.G and the devices in Network G.

The following project description applies to Group B. The project description for the other groups is similar to Group B's, except that their configurations are different.
Feel free to install any software, if needed. But, before install any software, check if it is already in the computer.

Do all the following tasks as a normal user!!!
Do not assume you know the root password!!!
Please DO NOT change any settings in Router A, Z, and Switch A, Z.

Task I: Setup the network

1) Wire all devices according to Figure 1 (at the end of this document).
2) Configure the NICs of Computer A.B, B.1, and B.2 according to Figure 1.
3) Make sure the SSH service has been started in Computer B.2.
4) Configure the Firewall B such that outside computers CANNOT access any internal

computers and services.

Note that the wireless access points B, C, D, E, F and G have been configured with SSID "apb", "apc", "apd", "ape", "apf" "apg", IP addresses and WEP keys.

Task II: Crack WEP

1) Assume you have Computer A.B, but cannot access Network B because the access has been disabled by Firewall B. However, you find that a wireless access point is on inside Network B. So, you decide to get into Network B through the access point.

2) Turn off the Ethernet card in Computer A.B, and turn on the wireless card.
Note, you need to setup a static IP address of Network B in the wireless card.

3) Use the command "iwlist" to find the wireless network in Network B, and record the SSID, the channel number, and the MAC address of the access point.

4) Follow the tutorial "crack-wep-tutorial.pdf" to use "aircrack" to find the WEP key of the wireless network.

5) Once you find the WEP key "**xxxx**", set up the wireless card of Computer A.B to access the wireless network of Network B. Ping to the gate way of Network B and Computer B.2 to make sure you have the right access.
Note, if your wireless card does not automatically get an IP address of Network B, you then need to configure the wireless card to have a static IP of Network B.

Task III: Dictionary Password Crack

NOTE: (1) Please use the Makefile provided to compile the code. (2) You may need to install openssl, openssl-devel, libssh2 and libssh2-devel for compilation. Please check the system before proceeding to install.

1) Once you can get into the wireless network using Computer A.B, try to ssh Computer B.2 as "User25". But assume that you do not have the password of "User25".

2) Somehow, you get a dictionary file "dictionary.txt" that has the password of "User25". Make a program to test each password in the file until you can ssh to Computer B.2 as "User25". The provided source code "sshpass.c" is for your reference only. You need to make your own

program based on it.

3) Once you ssh into Computer B.2 as “User25”, retrieve two files “secret.pdf.enc1” and “secret.pdf.enc2” from the “files” directory of “User25”.

Task IV: Cryptanalysis and Brute Force Password Crack

1) “secret.pdf.enc1” is an encrypted pdf file encrypted by a simple but flawed encryption algorithm. The code of the encryption is “enc1.c”. The algorithm takes a key and reads a pdf file eight bytes by eight bytes. Then, each eight bytes are XORed with a stream of eight bytes generated by the key. Read “enc1.c” to understand the encryption.

2) The encryption algorithm is flawed in that if the first eight bytes of both the plain text and the cipher text are known, then the key is disclosed. Because “secret.pdf.enc1” is encrypted from a pdf file, people can obtain the plain text of the first eight bytes of a pdf file from the PDF specification (below). Use this information to find the key and decrypt the pdf file via cryptanalysis.

3) “secret.pdf.enc2” is an encrypted pdf file encrypted by the AES-ECB encryption algorithm. “enc2.c” is the source code of encryption, and “dec2.c” is the source code of decryption. Now, make a program to crack the key of the encryption using the brute force method. You need to test and make sure the program can decrypt a DEC-ECB encrypted file.

7.5.2 File Header

The first line of a PDF file shall be a *header* consisting of the 5 characters %PDF– followed by a version number of the form 1.N, where N is a digit between 0 and 7.

A conforming reader shall accept files with any of the following headers:

%PDF–1.0
%PDF–1.1
%PDF–1.2
%PDF–1.3
%PDF–1.4
%PDF–1.5
%PDF–1.6

C. Project Report

How to Deliver

A group report is needed to show what you did in the project. Please clearly state your results of this project. You are expected to submit a report in the following formats:

a) Hard copies only.
b) A cover page with names of your group members with font size 12.

c) Single space and single column.
d) 5-15 pages (not including the cover page).

What to Deliver

Section I (Introduction):

Summarize what you have done in the project and clearly state the responsibility of each group member, e.g. who did which task, who wrote which part of the report, how your group was coordinated, etc.

Section II (Task II):

a) Show the screen shot when you are running aircrack and obtaining the key.
b) Report how long it takes to crack the WEK key and how many packets are captured in order to crack the 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".
b) Report how long it takes 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.

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.
b) Show the screen shot of your AES 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 AES program when you are brute force cracking the key.
d) Report how many keys are tested in 10 minutes.
e) Estimate how long it will take to find the key.
Note that you may not be able to find the key given the current hardware.

D. Grading Rubrics

If you do not contribute to the project, you get 0.

Group credits (70%)

1) Section I: Introduction (10%)
2) Section II: Task II (20%)
3) Section III: Task III (20%)
4) Section IV: Task IV (20%)

Individual credits (30%)

1) If you did some part of the tasks, you get 15. If you did nothing for the tasks, you get 0.
2) If you wrote some part of the report, you get 15. If you wrote nothing for the report, you get 0.
3) **If you only wrote some part of the report, you get 0.**