Practing with an offline dictionary attack
HW2 - CNS Sapienza

Edoardo Puglisi 1649359

04/11/2019

Contents

1 Overview

The following experiment consists of simulating an offline dictionary attack on a ciphertext given by professor. We (the attackers) know the command used to encrypt the file (openssl enc aes-192-cbc -pbkdf2 -e -in ¡infile.txt¿ -out ciphertext.enc) and that the password is a single word that can be found on dictionary.

2 OFFLINE Dictionary Attack

Dictionary Attack is a particular tecnnique of bruteforce used to break a security mechanism such as a cipher involving words from dictionary as passphrase. The difference between normal bruteforce attack is that if the password (like our case) is a simple word, running time will be much smaller (still huge).

3 Code

Code description.

```
!/bin/bash

echo ++++++ HOMEWORK 2 ++++++
start=$(date +%s)
for dict in en it
do
    while read -r line
    do
        echo -e $line
        openssl aes-192-cbc -d -in "ciphertext-hw2
           -1649359.enc" -out "plaintext.txt" -pass
           pass:$line -pbkdf2 2> /dev/null
        if [[ $(file plaintext.txt | cut -d' ' -f2)
           == "ASCII" ]];
        then
            runtime=$(($(date +%s)-$start))
            printf "La passowrd    $line\n"
            printf "Daje! Hai sprecato ben %dh:%dm:%
               ds. della tua vita\n" $(($runtime
               /3600)) $(($runtime%3600/60)) $((
               $runtime%60))
            exit
        fi
    done < "$dict-prova.txt"
```

```
done
```

The Bash code used for the "attack" is composed by two nested cycles: the first one iterates on different dictionaries (in this case english and italian), the second one iterates on every words of the given dictionary and decrypts the ciphertext with it. At each step the program checks if the decryption gave the right result: if the resulting plaintext is an ASCII file than the decryption was successful.

4 Results

It tooks 1 hour 49 minutes and 53 seconds to find the password used to encrypt the original text. The password is "learning". The experiment was lucky because the passphrase was on the first dictionary it checked and in the middle of it. In the worst case the right word could be in the last position of the last dictionary making the running time much higher.