

Assignment 5

Network Security

Soheil Shirvani 3720505



Brute Force Attack

Here we want to do brute force attack from kali Linux to windows victim to break ftp password that is on from slimftp on windows victim.

The knowledge we know about password is that It countians 2 upper case letter 3 lower case letters and 2 digits. Also, we know the username to ftp.

First we have to setup ftp server on windows victim:

Graphical user interface, text, application, email

Description automatically generated

User Password that is setup is:

Text

Description automatically generated

To attack the ftp server we first set the ip address and username:

A picture containing graphical user interface

Description automatically generated

To do brute force first we have to generate different passwords. To do so I have used the following script: It randomly select 2 uppercase 3 lowercase and 2 digits and shuffle the pattern to generate a new password.

Text

Description automatically generated with medium confidence

To check if the generated password is the actual ftp password:

Graphical user interface, text, application

Description automatically generated

The main function of this script is :

Text

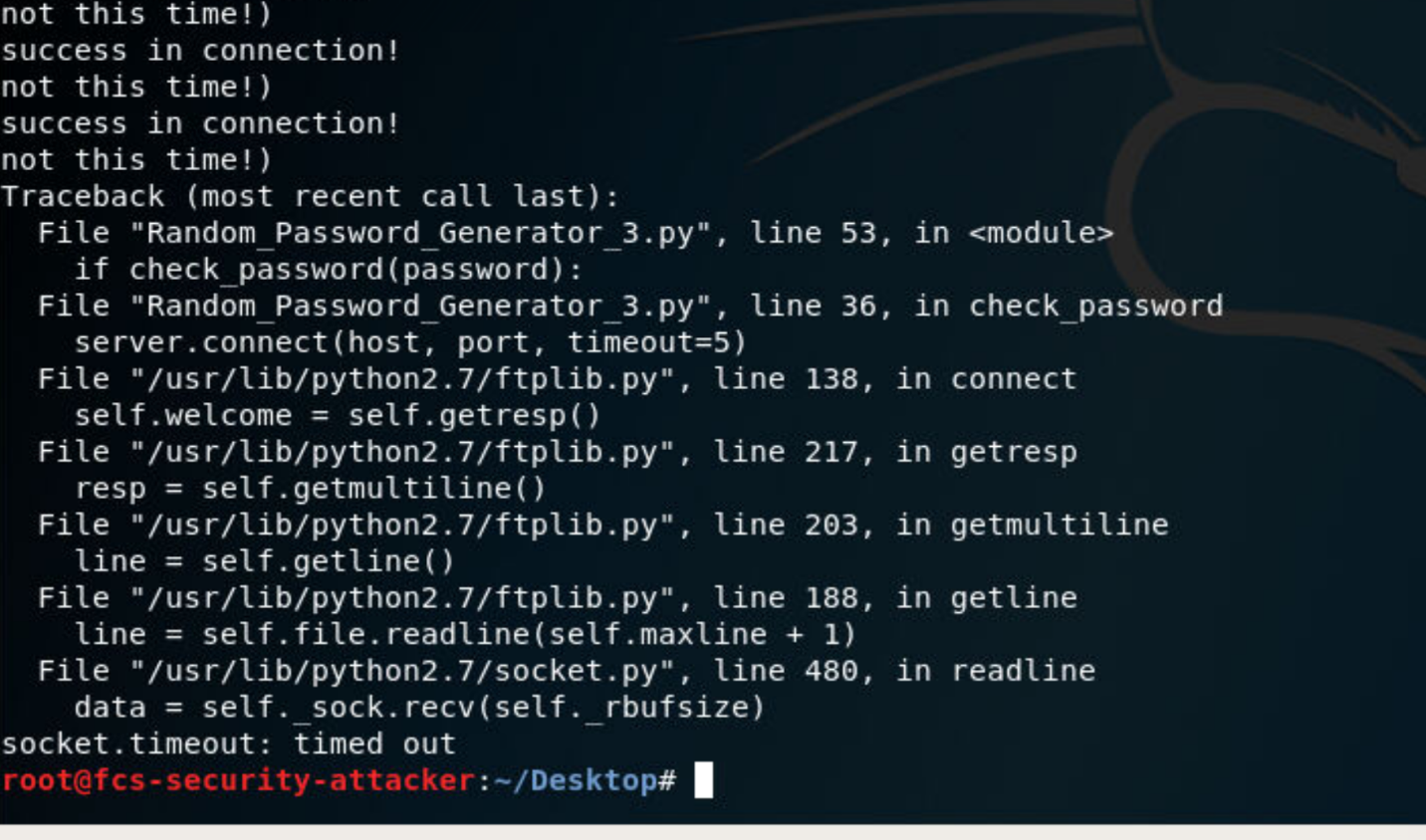
Description automatically generated

After running it we have:

Text

Description automatically generated

Because there is almost 2 billion password that can be generated using the 2 3 2 pattern it take a lot to check all the passwords. The problem was ftp will get timeout after around 100000 password tries. An example of this timeout is:



After I ran my script for several times (around 17 times ☹) I managed to break the password:

Text

Description automatically generated

As you can see the time is 307 seconds but as I said I had to run it many times.