ATTACK DEFENSE

by PentesterAcademy

Name	Interaction : FTP Service
URL	https://attackdefense.com/challengedetails?cid=1809
Type	Beginner Skills : Linux For Pentesters

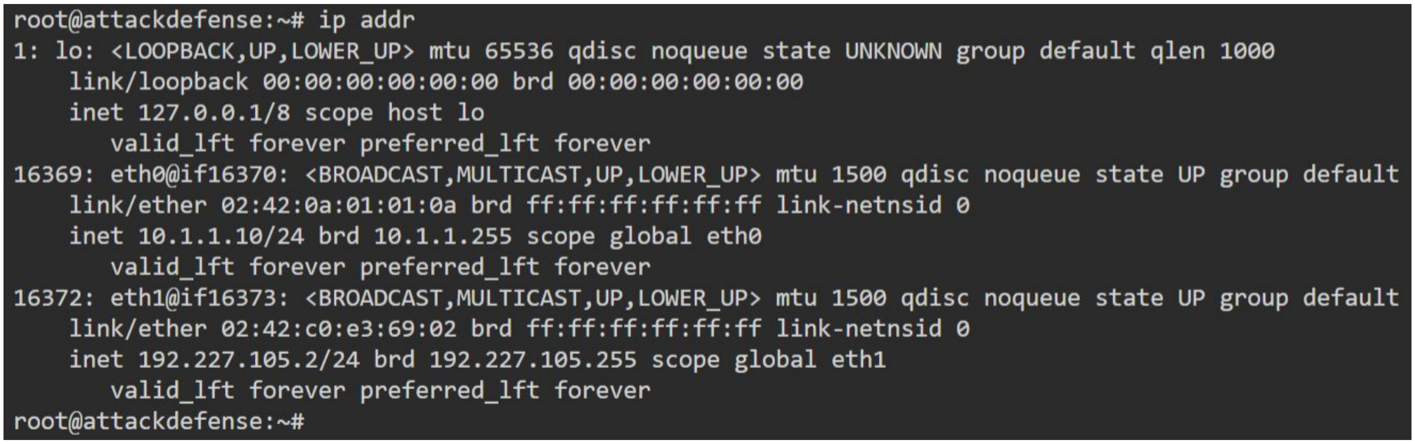
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Objective: Use expect to interact with FTP service and retrieve the flag!

Solution:

Step 1: Check the IP address of the machine.

Command: ip addr

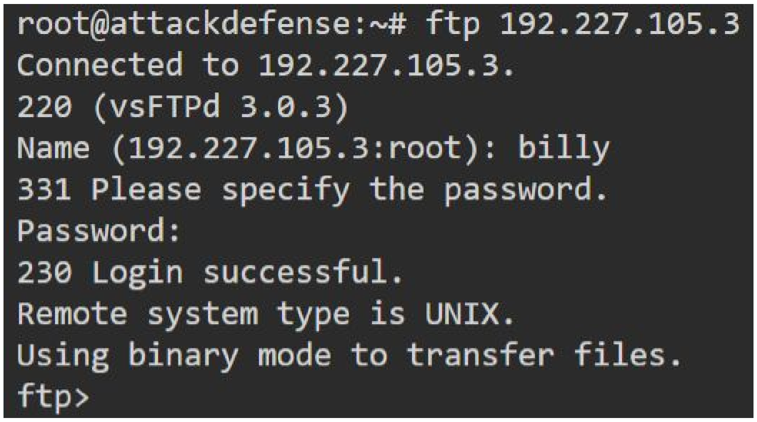


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
16369: eth0@if16370: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:0a brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.10/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
16372: eth1@if16373: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:e3:69:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.227.105.2/24 brd 192.227.105.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP of user's machine is 192.227.105.2, so as per the guidelines the IP of remote FTP machine should be 192.227.105.3

Step 2: Connect to FTP server

Command: ftp 192.227.105.3

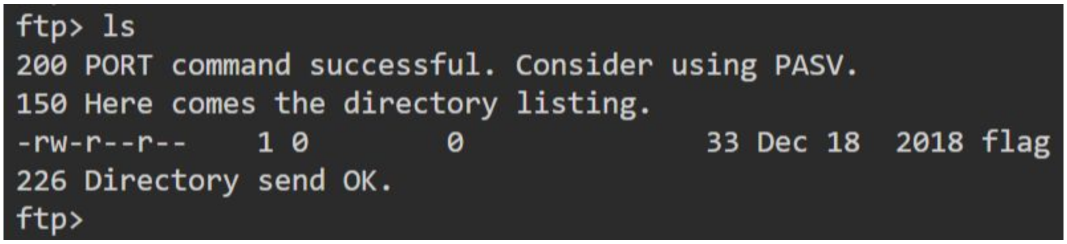


```
root@attackdefense:~# ftp 192.227.105.3
Connected to 192.227.105.3.
220 (vsFTPd 3.0.3)
Name (192.227.105.3:root): billy
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Provide the username “billy” and password “carlos” on prompt.

Step 3: List the files present in the FTP directory.

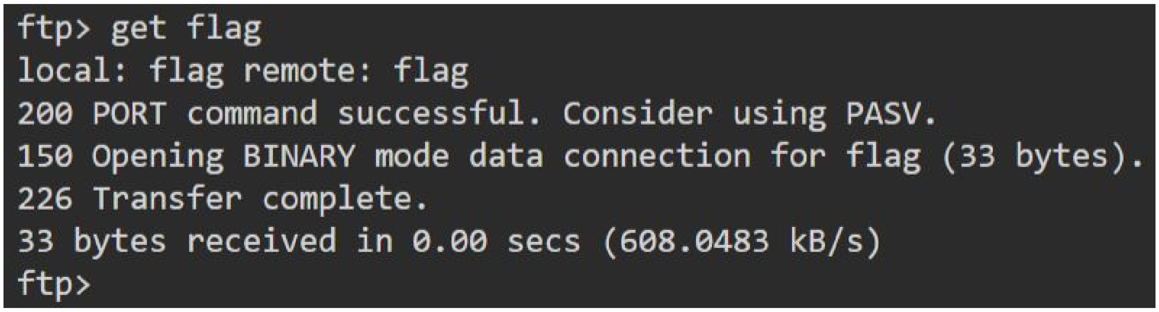
Command: ls



```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              33 Dec 18  2018 flag
226 Directory send OK.
ftp>
```

Flag file “flag” is present on the server. Download this file.

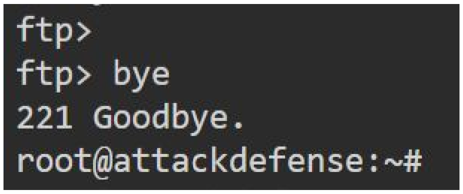
Command: get flag



```
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 (608.0483 kB/s)
ftp>
```

Step 4: Exit from the server.

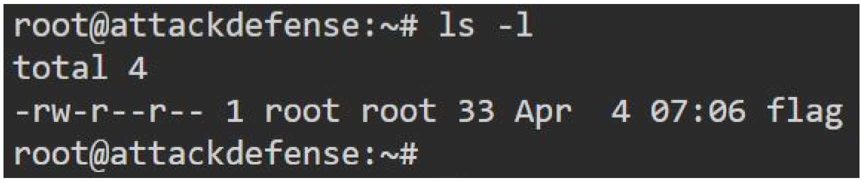
Command: bye



```
ftp>
ftp> bye
221 Goodbye.
root@attackdefense:~#
```

Step 5: Check the local directory.

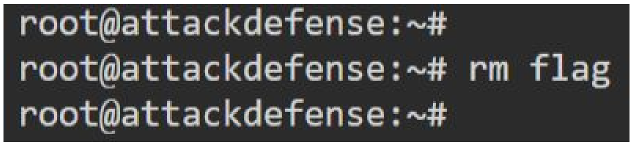
Command: ls -l



```
root@attackdefense:~# ls -l
total 4
-rw-r--r-- 1 root root 33 Apr  4 07:06 flag
root@attackdefense:~#
```

The flag file is here. However, we are supposed to get it with expect. So, delete it.

Command: rm flag

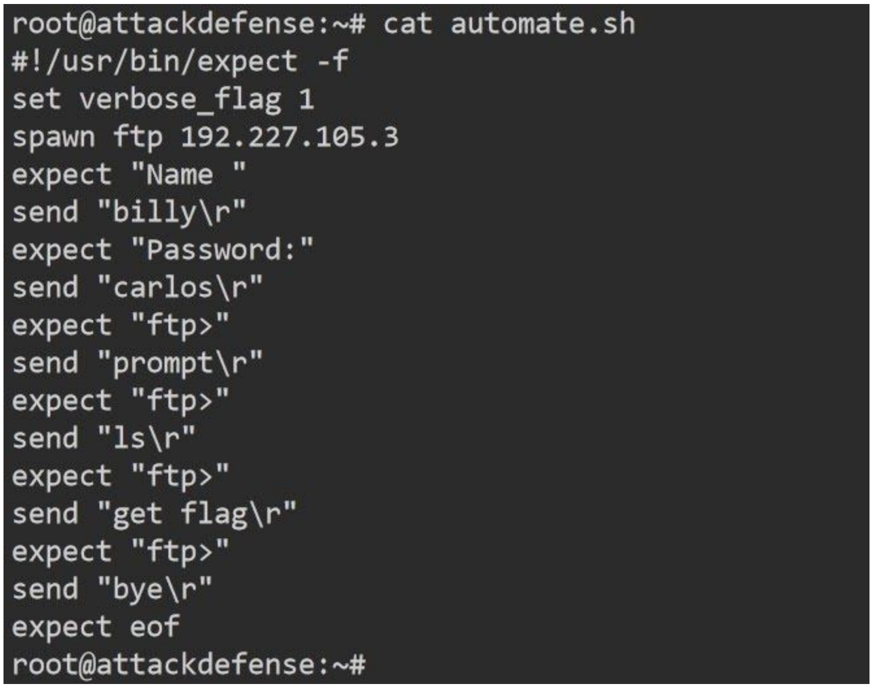


```
root@attackdefense:~#
root@attackdefense:~# rm flag
root@attackdefense:~#
```

Step 6: Whole manual process is clear now, automate this with expect now. Write expect script and save it as automate.sh

Bash script

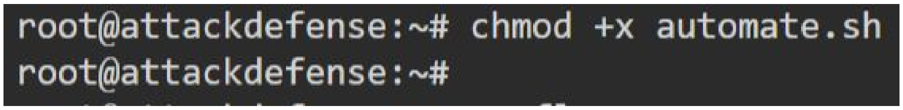
```
#!/usr/bin/expect -f
set verbose_flag 1
spawn ftp 192.227.105.3
expect "Name "
send "billy\r"
expect "Password:"
send "carlos\r"
expect "ftp>"
send "prompt\r"
expect "ftp>"
send "ls\r"
expect "ftp>"
send "get flag\r"
expect "ftp>"
send "bye\r"
expect eof
```



```
root@attackdefense:~# cat automate.sh
#!/usr/bin/expect -f
set verbose_flag 1
spawn ftp 192.227.105.3
expect "Name "
send "billy\r"
expect "Password:"
send "carlos\r"
expect "ftp>"
send "prompt\r"
expect "ftp>"
send "ls\r"
expect "ftp>"
send "get flag\r"
expect "ftp>"
send "bye\r"
expect eof
root@attackdefense:~#
```

Step 7: Make this script executable.

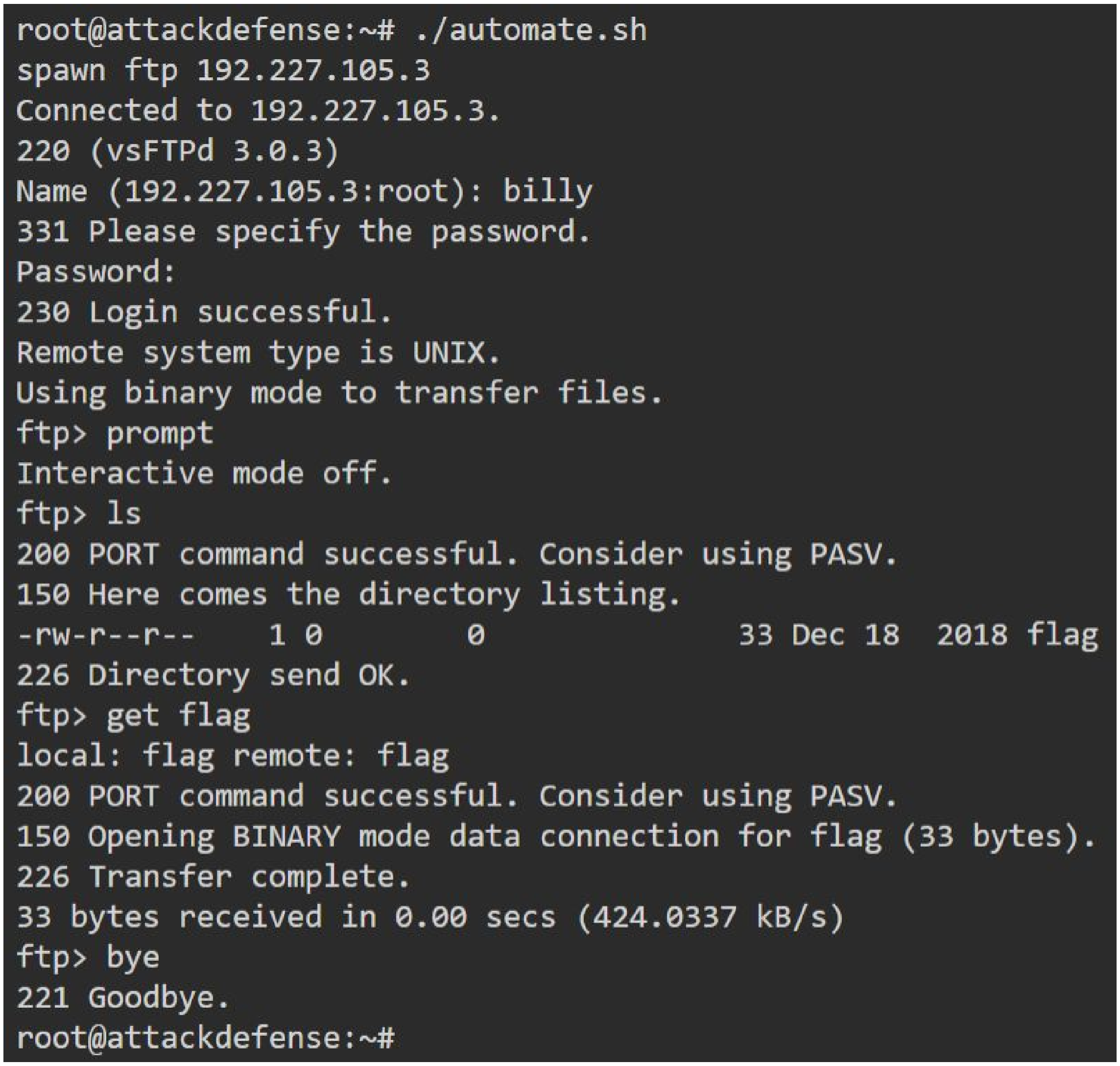
Command: chmod +x automate.sh



```
root@attackdefense:~# chmod +x automate.sh
root@attackdefense:~#
```

Step 8: Run this script.

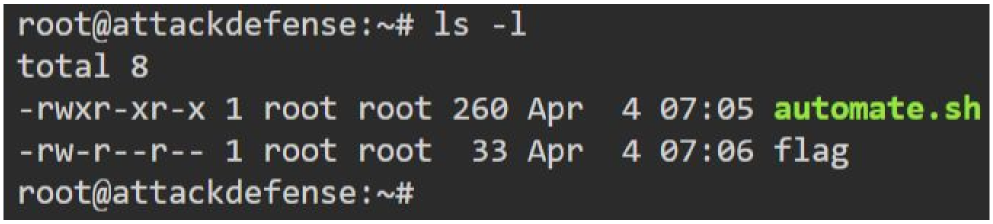
Command: ./automate.sh



```
root@attackdefense:~# ./automate.sh
spawn ftp 192.227.105.3
Connected to 192.227.105.3.
220 (vsFTPd 3.0.3)
Name (192.227.105.3:root): billy
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt
Interactive mode off.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0              33 Dec 18  2018 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 (424.0337 kB/s)
ftp> bye
221 Goodbye.
root@attackdefense:~#
```

Step 9: The flag file is fetched by the script. Check the local directory.

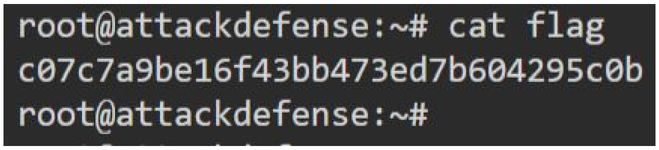
Command: ls -l



```
root@attackdefense:~# ls -l
total 8
-rwxr-xr-x 1 root root 260 Apr  4 07:05 automate.sh
-rw-r--r-- 1 root root  33 Apr  4 07:06 flag
root@attackdefense:~#
```

Retrieve the flag from this file.

Command: cat flag



```
root@attackdefense:~# cat flag
c07c7a9be16f43bb473ed7b604295c0b
root@attackdefense:~#
```

Flag: c07c7a9be16f43bb473ed7b604295c0b