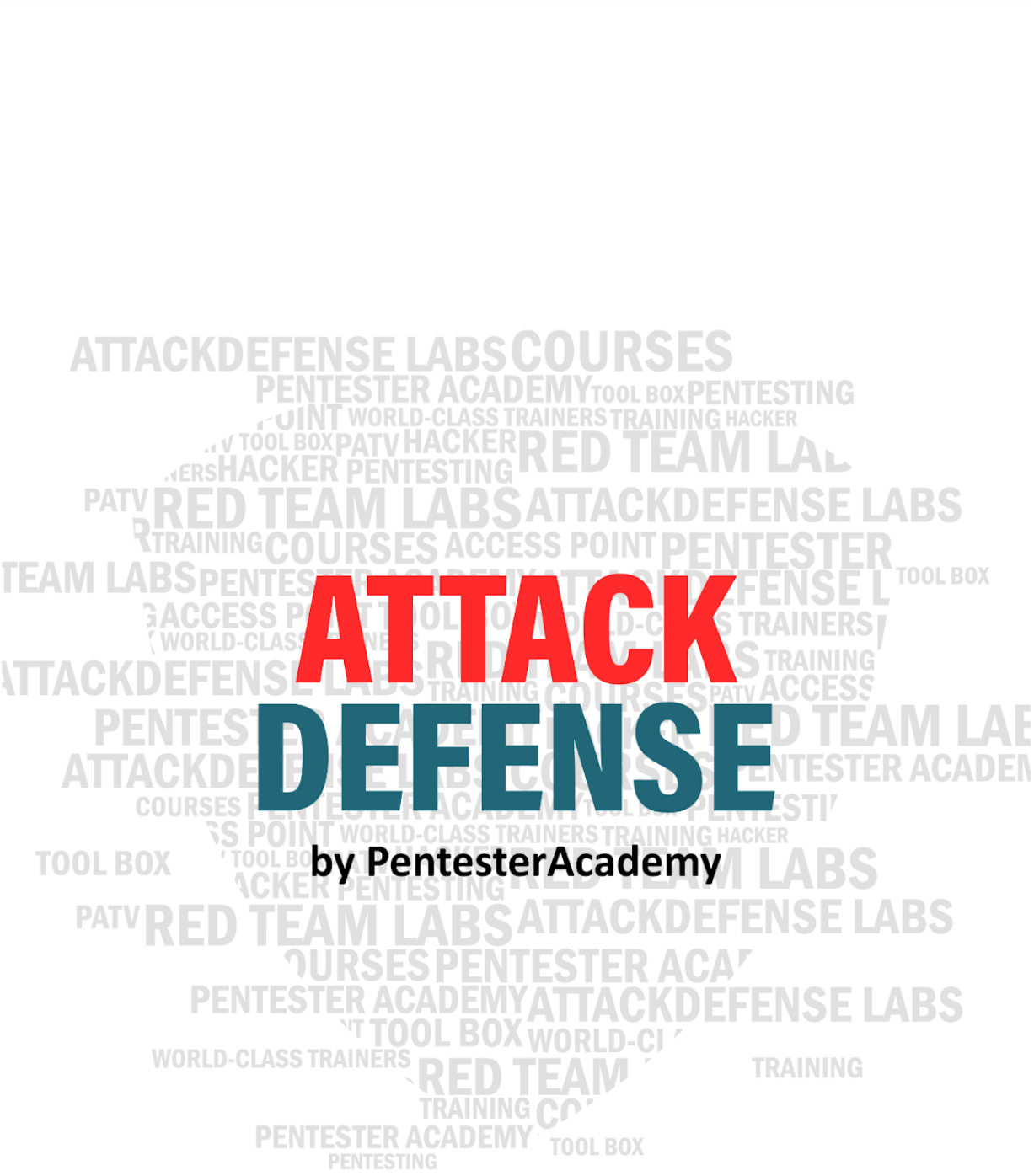
ATTACK
DEFENSE
by PentesterAcademy

Name	Interaction : Socat Listener
URL	https://attackdefense.com/challengedetails?cid=1810
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 Socat listener 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
16421: eth0@if16422: <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
16424: eth1@if16425: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:80:4c:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.128.76.2/24 brd 192.128.76.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The IP of user's machine is 192.128.76.2, so as per the guidelines the IP of remote Linux machine should be 192.128.76.3

Step 2: Connect to listener service

Command: socat - TCP:192.128.76.3:2023

```
root@attackdefense:~# socat - TCP:192.128.76.3:2023
root@victim-1:~#
```

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

Command: ls -l

```
root@victim-1:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 33 Apr  4 10:56 flag
root@victim-1:~#
```

Flag file “flag” is present on the server.

Step 4: Exit the connection.

Command: exit

```
root@victim-1:~# exit
exit
exit
root@attackdefense:~#
```

Step 5: The 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
spawn socat - TCP:192.128.76.3:2023
expect "root@victim-1:~# "
```

```
send "ls -l\r"
expect "root@victim-1:~# "
send "cat flag\r"
expect "root@victim-1:~# "
send "exit\r"
```

```
root@attackdefense:~# vim automate.sh
root@attackdefense:~#
root@attackdefense:~# cat automate.sh
#!/usr/bin/expect -f
spawn socat - TCP:192.128.76.3:2023
expect "root@victim-1:~# "
send "ls -l\r"
expect "root@victim-1:~# "
send "cat flag\r"
expect "root@victim-1:~# "
send "exit\r"
root@attackdefense:~#
```

Step 6: Make this script executable.

Command: chmod +x automate.sh

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

Step 7: Run this script.

Command: ./automate.sh

```
root@attackdefense:~# ./automate.sh
spawn socat - TCP:192.128.76.3:2023
root@victim-1:~# ls -l
ls -l
total 4
-rw-r--r-- 1 root root 33 Apr  4 10:56 flag
root@victim-1:~# cat flag
cat flag
f2e55e1ccdbbbab127f313c4d4787eec
root@victim-1:~# root@attackdefense:~#
```

Flag: f2e55e1ccdbbbab127f313c4d4787eec