Day 8 - What's Under the Christmas Tree?

Scenario

Day 8: What's Under the Christmas Tree? - Story:

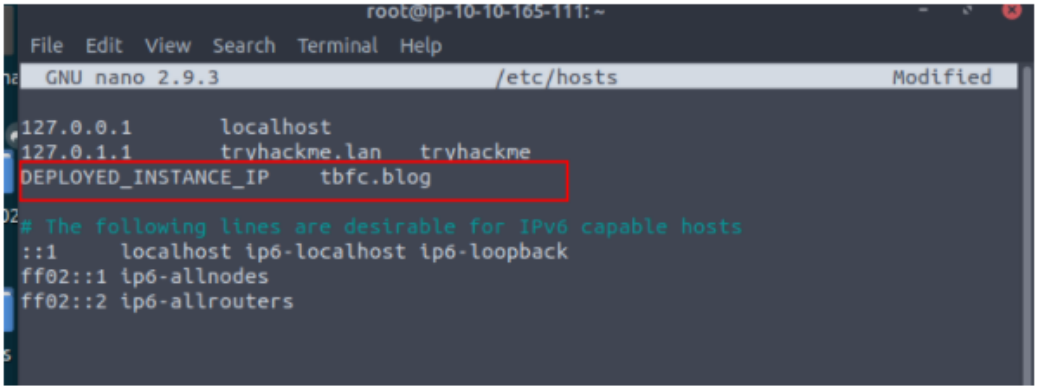
After a few months of probation, intern Elf McEager has passed with glowing feedback from Elf McSkidy. During the meeting, Elf McEager asked for more access to *The Best Festival Company's (TBFC's)* internal network as he wishes to know more about the systems he has sworn to protect.

Elf McSkidy was reluctant to agree. However, after Elf McEager's heroic actions in recovering christmas, Elf McSkidy soon thought this was a good idea. This was uncharted territory for Elf McEager - he had no idea how to begin finding out this information for his new responsibilites. Thankfully, TBFC has a wonderful up-skill program covering the use of Nmap for ElfMcEager to enrol in.

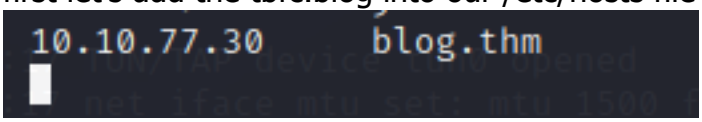
8.9. Challenge

Deploy and use Nmap to scan the instance attached to this task. Take a note of the IP address of the Instance that you have delopyed in this task: `10.10.198.215` and enumerate it for Elf McEager!

Optional bonus: As a result of Elf McEager managing to recover christmas in "*Day 7 - The Grinch Really Did Steal Christmas*", TBFC's website has been restored for all the elves to visit. Can you find it? I hear it's quite the read... You must add `10.10.198.215 tbfc.blog` to your **/etc/hosts** file before the application will load like below:



first let's add the tbfc.blog into our /etc/hosts file



Question: When was Snort created?

When was Snort created?

All | Images | News | Videos | Shopping | More | Settings | Tools

About 2,260,000 results (0.53 seconds)

1998

Snort is a free open source network intrusion detection system (IDS) and intrusion prevention system (IPS) **created** in 1998 by Martin Roesch, founder and former CTO of Sourcefire. **Snort** is now **developed** by Cisco, which purchased Sourcefire in 2013.

en.wikipedia.org › wiki › Snort_(software)

Snort (software) - Wikipedia

now let's scan the host 10.10.198.215 without any flags
//we've found 3 open ports here

```
┌──(nobodyatall㉿0xDEADBEEF)-[~]
└─$ nmap 10.10.198.215
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-08 18:07 EST
Nmap scan report for 10.10.198.215
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server
```

let's set the -Pn flag to let nmap assume that the following host was active without performing any ping scan to make sure the host is live
//sometimes like Windows machine they do block ICMP packets which let you assume that the host is not alive. This flag are useful in this scenario

```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ nmap -Pn 10.10.198.215
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-08 18:09 EST
Nmap scan report for 10.10.198.215
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 13.59 seconds
```

now let's use the -A flag which will perform (OS detection, version detection, script scanning, and traceroute)
// this will includes much more detailed about the host & the services that's running on the open port

```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ nmap -A 10.10.198.215
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-08 18:11 EST
Nmap scan report for 10.10.198.215
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.50 seconds
```

now to get the open ports service details only we can use -sV flag

```
┌──(nobodyatall㉿0×DEADBEEF)-[~]
└─$ nmap -sV 10.10.198.215
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-08 18:14 EST
Nmap scan report for 10.10.198.215
Host is up (0.17s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.32 seconds
```

based on these results we know that the host is running a Ubuntu Linux distro

```
  VERSION
  Apache httpd 2.4.29 ((Ubuntu))
  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

Question: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

```
  VERSION
  Apache httpd 2.4.29 ((Ubuntu))
  OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

now we can use the following NSE script to grab the http title of the webserver
//cmd to find the nse script: locate nse | grep http

```
/usr/share/nmap/scripts/http-title.nse
```

based on the scanned result, it seems that this webserver is most likely hosting a blog

```
└─$ nmap --script http-title tbfc.blog
Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-08 18:23 EST
Nmap scan report for tbfc.blog (10.10.198.215)
Host is up (0.19s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: TBFC&#39;s Internal Blog
```

Question: Based on the value returned, what do we think this website might be used for?

```
80/tcp   open  http
|_http-title: TBFC&#39;s Internal Blog
```