

Day 8 - Networking What's Under the Christmas Tree?

List of tools used: Firefox, Nmap

Question 1


When was Snort created?

Methodology: We use Firefox and search the question online. We can see that Snort was created in 1998.

Snort

Software

snort.org



Snort is a free open source network intrusion detection system and intrusion prevention system created in 1998 by Martin Roesch, founder and former CTO of Sourcefire. Snort is now developed by Cisco, which purchased Sourcefire in 2013. In 2009, Snort entered InfoWorld's Open Source Hall of Fame as one of the "greatest [pieces of] open source software of all time". [Wikipedia](#)

Developer(s): Cisco Systems

Written in: C++ (since version 3.0)

Operating system: Cross-platform

Type: Intrusion detection system, Intrusion prevention system

License: GPLv2+

Answer: 1998

Question 2

Using Nmap on MACHINE_IP, what are the port numbers of the three services running?

Methodology: We run command “nmap 10.10.128.107(MACHINE_IP)” in terminal and see there are 3 open ports which are 80,2222,3389.

```
(kali㉿kali)-[~]  
$ nmap 10.10.128.107  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 04:54 EDT  
Nmap scan report for 10.10.128.107  
Host is up (0.19s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
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 27.65 seconds
```

Answer: 80,2222,3389

Question 3

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

Methodology: We run command “nmap -A 10.10.128.107(MACHINE_IP)” in terminal with -A to aggressive scan which enables more features such as OS detection and version scanning. Then, we can see it is running on Apache in Ubuntu.

```
(kali㉿kali)-[~]  
$ nmap -A 10.10.128.107  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 04:55 EDT  
Nmap scan report for 10.10.128.107  
Host is up (0.19s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE        VERSION  
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))  
|_http-generator: Hugo 0.78.2  
|_http-title: TBFC6#39;s Internal Blog  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
2222/tcp  open  ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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 45.31 seconds
```

Answer: Ubuntu

Question 4

What is the version of Apache?

Methodology: We run command “nmap -A 10.10.128.107(MACHINE_IP)” in terminal with -A to aggressive scan which enables more features such as OS detection and version scanning. Then, we can see the Apache is on 2.4.29 version.

```
(kali㉿kali)-[~]  
$ nmap -A 10.10.128.107  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 04:55 EDT  
Nmap scan report for 10.10.128.107  
Host is up (0.19s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))  
|_http-generator: Hugo 0.78.2  
|_http-title: TBFC6#39;s Internal Blog  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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 45.31 seconds
```

Answer: 2.4.29

Question 5

What is running on port 2222?

Methodology: We run command “nmap -A 10.10.128.107(MACHINE_IP)” in terminal with -A to aggressive scan which enables more features such as OS detection and version scanning. Then, we can see the port 2222 is running SSH.

```
(kali㉿kali)-[~]  
$ nmap -A 10.10.128.107  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 04:55 EDT  
Nmap scan report for 10.10.128.107  
Host is up (0.19s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))  
|_http-generator: Hugo 0.78.2  
|_http-title: TBFC6#39;s Internal Blog  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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 45.31 seconds
```

Answer: SSH

Question 6

Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

Methodology: We run command "nmap -A 10.10.128.107(MACHINE_IP)" in terminal with -A to aggressive scan which enables more features such as OS detection and version scanning. Then, we can see the http-title return value is "TBFC's Internal Blog". Therefore, we think the website might be used for blog.

```
(kali㉿kali)-[~]
$ nmap -A 10.10.128.107
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-30 04:55 EDT
Nmap scan report for 10.10.128.107
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))
|_ http-generator: Hugo 0.78.2
|_ http-title: TBFC&#39;s Internal Blog
|_ http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh            OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 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 45.31 seconds
```

Answer: blog