Another Hidden Page?!

問題概要


Challenge
Another Hidden Page ?!
100
Network
どうやらラズパイではWebサーバが起動しているらしい．ただ，httpのWellknownポート(80)にアクセスしても・・・
http://192.168.1.2
Flag
Submit

ねらい

- ポートの概念の理解
- nmapについて知ってもらう

アプローチ

別問題 ”Welcome to Web !” で http://192.168.1.2 はチェック済

問題でポートについて言及されている

別ポートでのWebページ公開を疑う

アプローチ

- ポートをスキャンし，空いているポートを見つける

  → nmapの使用

```
$ sudo apt install nmap
```

アプローチ

- ポートスキャン実行

```
$ nmap 192.168.1.2
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-22 07:18 UTC
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00046s latency).
Not shown: 997 closed ports
PORT         STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8000/tcp open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds
```

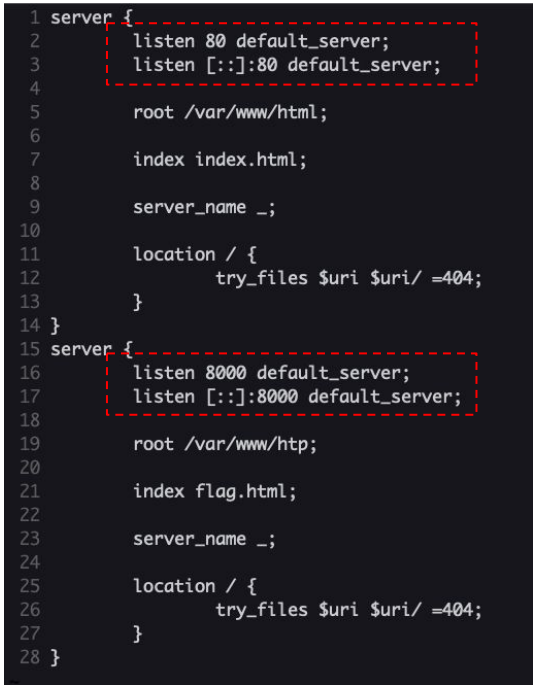
答え

- ブラウザ or “curl” でアクセス

(Webページは80番ポートだけじゃないやで)

その他 (裏側)

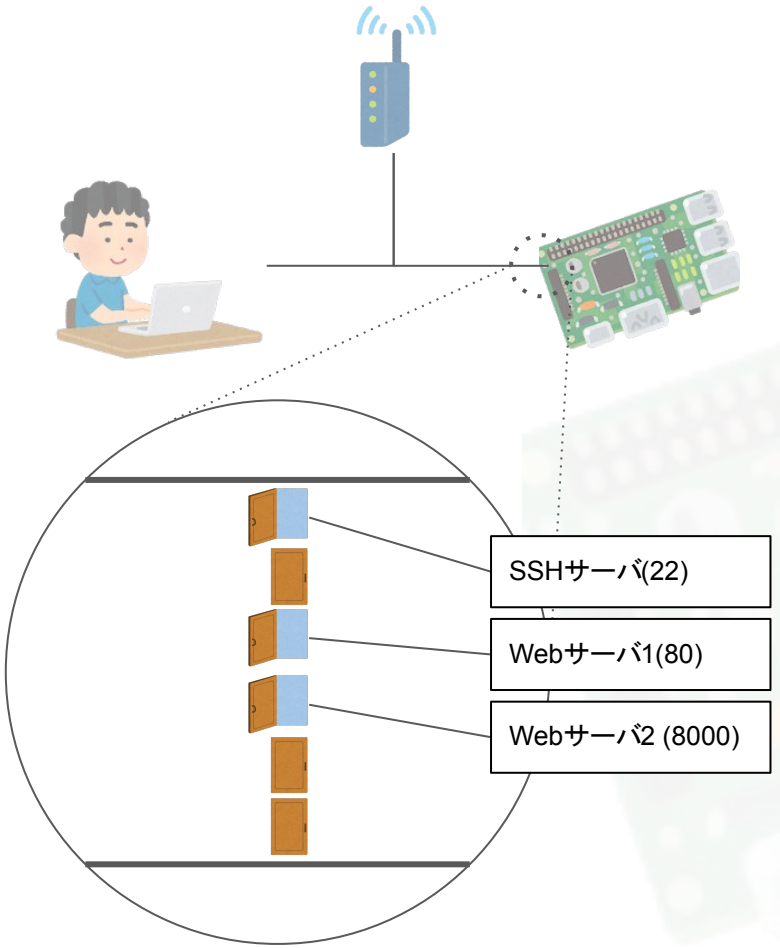
- 使用Webサーバ = nginx
- 複数ポートでの待ち受け
- 公開HTMLを含むディレクトリの権限まわり



```
server {
        listen 80 default_server;
        listen [::]:80 default_server;

        root /var/www/html;

        index index.html;

        server_name _;

        location / {
                try_files $uri $uri/ =404;
        }
}
server {
        listen 8000 default_server;
        listen [::]:8000 default_server;

        root /var/www/htp;

        index flag.html;

        server_name _;

        location / {
                try_files $uri $uri/ =404;
        }
}
```

ポートについて

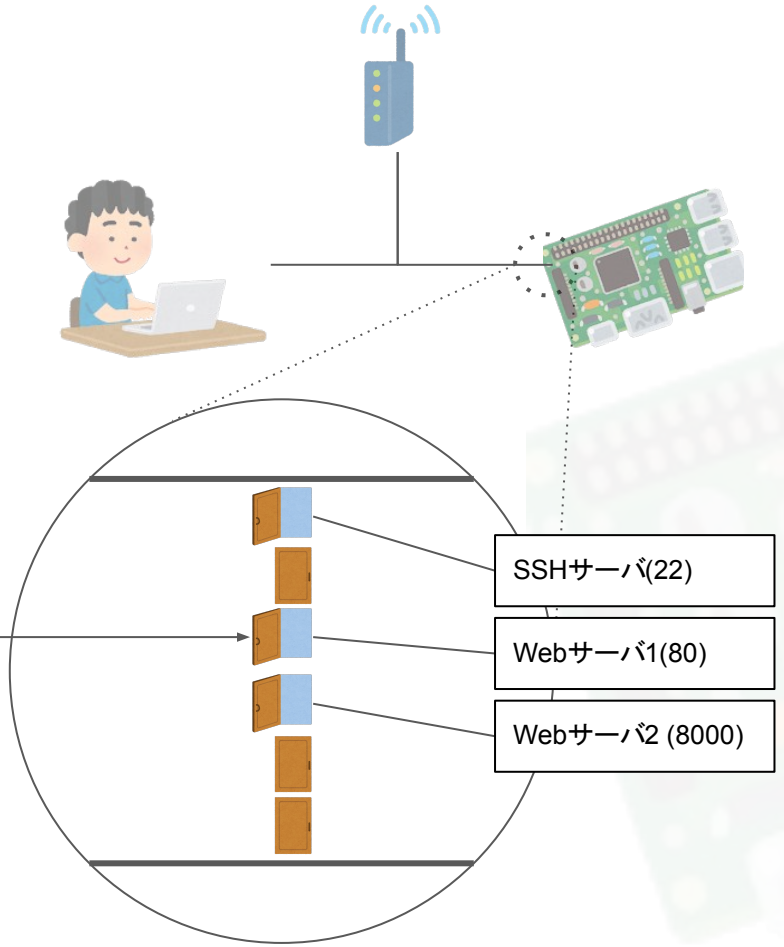
- 0 - 1023番　　：一般(Well Known)
- 1024 - 49151番　：登録済みポート
- 49152 - 65535番　：自由



ポートについて

- 0 - 1023番　　：一般(Well Known)
- 1024 - 49151番　：登録済みポート
- 49152 - 65535番　：自由

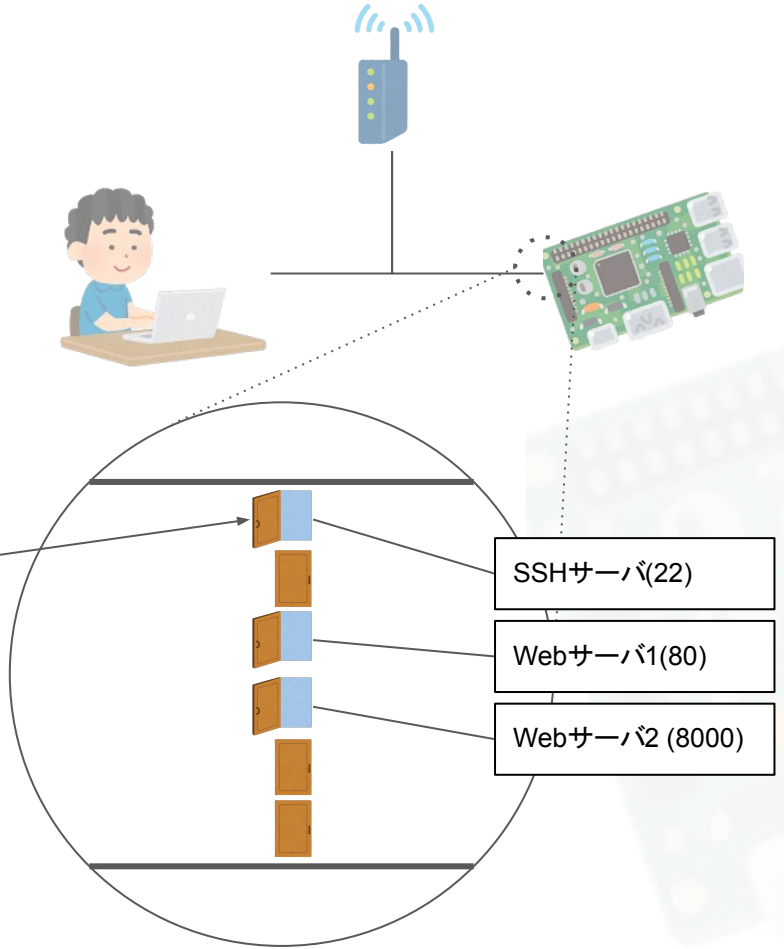
http://hogehoge.com:80



ポートについて

- 0 - 1023番　　：一般
- 1024 - 49151番　：登録済みポート
- 49152 - 65535番　：自由

```
$ ssh hoge@192.168.1.2 -p 22
```



ポートスキャン

```
$ nmap 192.168.1.2
PORT  STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
8000/tcp open  http-alt
```