ネットワークセキュリティ演習

4回 ファイアーウォール

nmap

nmapのインストール

```
sudo apt install nmap
```

nmapで自分自身のポートの開き状態を確認する

```
sudo nmap localhost
```

開いているポートをメモしてください

nmapで同じセグメントのネットワークのポートスキャン

```
sudo nmap -v 192.168.0.0/24
```

ポートスキャンした内容をチェックしてみる

スキャンして見つけたIPアドレスに対してOSやソフトのバージョン情報を調べる

```
sudo nmap -sV <見つけたIPアドレス>
```

OSのバージョン 稼働しているソフトのバージョンをメモしてください

tcpdump をインストールする

```
sudo apt install tcpdump
```

TCPをモニターする（ssh 22番ポート）

```
sudo tcpdump -i lo "port 22"
```

nmapでスキャンしてみる

別ウィンドウを開いてnmapをしてみる

```
sudo nmap -sT localhost
```

tcpdumpの出力を確認してみる

バックドア検出ツール

バックドアを構築するソフトのことをルートキットという

ルートキットを検出するツール

ルートキット検出ツールのインストール

```
sudo apt install chkrootkit
```

チェック

```
sudo chkrootkit
```

Linuxマシンのルータ化

ip_forwardの確認

```
sysctl net.ipv4.ip_forward

net.ipv4.ip_forward = 0
```

ip_forwardの有効化

```
sudo nano /etc/sysctl.conf
```

コメントを取る `net.ipv6.conf.all.forwarding=1`

システムを再起動して確認

ip_forwardの有効化を確認

```
sysctl net.ipv4.ip_forward

net.ipv4.ip_forward = 1
```

iptables

iptables の設定の確認

```
sudo iptables -L

Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
cafe@techcafe:~$
```

gufw

iptablesを簡単に使えるようにするツール gufwのインストール

```
sudo add-apt-repository -y -n ppa:sicklylife/ppa

sudo apt update

sudo apt install gufw
```

gufwの起動

```
sudo gufw
```

GUIのウィンドウが現れる

外部からアクセスしてみる

隣のマシンどうしで、外部からsshでアクセスしてみる

ssh でログインに成功すると touchコマンドでファイルを残してみる

```
touch 自分の名前
```

ファイアーウォールを有効化する

ステータス:の右側のボタンをクリックしてオンにする

有効にしたときのデフォルト設定

- 外部から内部へのアクセスは全て遮断
- 内部から外部へのアクセスは全て許可

確認

外部からsshでアクセスしてみる 外部からhttpでアクセスしてみる

アクセスできないことを確認

ssh を許可するルールの追加

sshは許可するが、httpはアクセスできないことようにしてみる

ルールの追加ボタン + を利用

- 詳細の設定で、「追加」

iptablesで確認してみる

gufwでの設定がうまくいったら、それがiptablesでどのような設定になったか確認する

```
iptables -L
```

httpを許可するルールの追加

httpは許可するが、sshはアクセスできないことようにしてみる

ルールの追加ボタン + を利用

- 詳細の設定で、「追加」

iptablesで確認してみる

gufwでの設定がうまくいったら、それがiptablesでどのような設定になったか確認する

```
iptables -L
```

特定のIPアドレスからのみアクセスできる設定

試行錯誤で隣のIPアドレスからのみsshとhttpが可能で、他のIPアドレスからはアクセスできない設定にしてみてください

レポートURL

```
https://goo.gl/forms/iZOtINdxIyjno2oR2
```