Accès aux machines

Liens pratiques:

https://ent.univ-rennes1.fr/f/intranet/p/rssEtuEsirIstic.u27l1n88/max/render.uP?pCp

Portal VPN (depuis le navigateur):

https://istic-vpn.univ-rennes1.fr/

Depuis le réseau local de l'ISTIC

- En ligne de commande

  ssh zprojet@[VMS].istic.univ-rennes1.fr
- VMS:
  - ares1,ares2, ..., ares20

Compte utilisateur:

```
User : zprojet
Passwd: Zistic*!1
```

Passer en mode administrateur :

```
$ sudo su
```

Entrer votre mot de passe

En tant que administrateur, vous pouvez changer le mot passe :

```
# passwd
```

TP 3 : Sécurisation des réseaux avec un firewall simple

Objectif :

Appliquer les concepts de pare-feu en utilisant **iptables** ou **UFW** dans un réseau d'entreprise, tout en explorant des questions sur l'architecture réseau et la sécurité. Ce TP permet de configurer des règles de filtrage du trafic entre des machines virtuelles, de tester la connectivité, et d'analyser les journaux.

Durée : 1h30

Prérequis :

- iptables, ufw, nc
- bien définir son architecture réseau, adapter les interfaces réseaux et addresses ip par rapport a votre configuration

Prérequis :

- Partant du précédent TP, nous utiliserons la machine www connecté à virbr2 qui fera office de serveur web.

- le serveur web est émulé avec netcat/socat.
-

Plan du TP

1. Installation des outils de pare-feu (sur VM2, la machine routeur)

1. **Installer iptables** (généralement déjà installé par défaut) : Vérifiez qu'iptables est installé sur votre système avec la commande suivante :

   ```
   sudo apt update
   sudo apt install iptables
   ```

2. **Installer UFW** (si vous préférez une interface plus simple) : Si vous choisissez d'utiliser **UFW** (Uncomplicated Firewall), installez-le :

   ```
   sudo apt install ufw
   ```

3. **Vérifier l'état d'UFW** :

   ```
   sudo ufw status
   ```

---

2. Configuration du seveur web WWW

il vous ait demandé de configurer le serveur web (www); le serveur web sera émulé avec netcat/nc
installation de netcat

```
sudo apt-get install netcat -y
```

émulation d'un serveur web

```
sudo nc -l -p 80
```

3. Création de règles simples de filtrage avec iptables

Dans cette section, vous allez créer des règles pour filtrer le trafic entre plusieurs machines virtuelles (ou sur une seule machine avec plusieurs interfaces).

L'ensemble des règles s'effectuent sous la machine routeur (VM2).

> il vous ait demandé d'installer et configurer la machine www et d'installer netcat pour émuler le serveur web.

1. **Autoriser le trafic HTTP (horts/lwDtsPTdUWcport 80)** :
   - Autoriser les connexions entrantes sur le port HTTP pour les services web :

     ```
     sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
     ```

2. **Bloquer le trafic vers SSH (port 22)** :

- Bloquer toutes les connexions entrantes SSH pour des raisons de sécurité, sauf pour les connexions internes au réseau local (192.168.50.0/24) :

```
sudo iptables -A INPUT -p tcp --dport 22 -s 192.168.50.0/24 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
```

3. **Autoriser les pings** :
   - Autoriser les requêtes ICMP (ping) provenant du réseau local :

```
sudo iptables -A INPUT -p icmp --icmp-type echo-request -s
192.168.50.0/24 -j ACCEPT
```

4. **Bloquer tout le trafic sortant sauf vers des ports spécifiques (HTTP, HTTPS)** :
   - Bloquer tout le trafic sortant sauf le HTTP et le HTTPS :

```
sudo iptables -P OUTPUT DROP
sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
```

Questions :

- **Q3** : Quelle est l'importance de filtrer le trafic à la fois en entrée et en sortie dans un réseau d'entreprise ?
- **Q4** : Dans quel contexte d'architecture réseau est-il nécessaire de bloquer tout le trafic sortant, sauf certains ports (HTTP/HTTPS) ?
- **Q5** : Si vous gérez un réseau où des services critiques sont hébergés (ex : base de données), quelle serait votre approche pour configurer les règles de pare-feu ?
- **Q6** : Quelle influence la segmentation réseau (par VLAN, par exemple) peut-elle avoir sur la configuration du pare-feu dans un réseau d'entreprise ?

---

4. Règles avec UFW (si UFW est utilisé)

1. **Activer UFW** : Avant de créer des règles, activez le pare-feu UFW :

```
sudo ufw enable
```

2. **Autoriser le trafic HTTP** :
   - Autoriser le port HTTP (80) :

```
sudo ufw allow 80/tcp
```

3. **Bloquer le trafic SSH sauf pour le réseau local (192.168.50.0/24)** :
   - Autoriser uniquement les connexions SSH du réseau local et bloquer toutes les autres :

```
sudo ufw allow from 192.168.50.0/24 to any port 22
sudo ufw deny 22
```

4. **Vérifier les règles en cours** :

- Afficher les règles UFW actuelles :

```
sudo ufw status numbered
```

Questions :

- **Q7** : UFW simplifie la gestion des règles de pare-feu. En quoi cela peut-il être un avantage dans une architecture réseau distribuée (multi-sites ou multi-serveurs) ?
- **Q8** : Comment la complexité d'une infrastructure réseau affecte-t-elle le choix des outils de sécurité comme UFW ou iptables ?

---

5. Tests de connectivité et analyse des logs

1. **Tester la connectivité** :
   - Utilisez `ping` pour vérifier la connectivité entre les machines et assurez-vous que le pare-feu bloque/autorise correctement les pings en fonction de vos règles.

```
ping 192.168.50.xx
```

   - Testez les connexions HTTP en accédant à un serveur web sur le port 80.
2. **Analyse des logs avec iptables** :
   - Ajouter une règle iptables pour journaliser les paquets rejetés :

```
sudo iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped: "
```

   - Vérifier les logs générés par iptables dans `/var/log/syslog` :

```
tail -f /var/log/syslog
```

3. **Analyse des logs avec UFW** :
   - Activer les logs UFW :

```
sudo ufw logging on
```

   - Vérifier les logs dans `/var/log/ufw.log` :

```
tail -f /var/log/ufw.log
```

Questions :

- **Q9** : Pourquoi est-il essentiel de surveiller les logs d'un pare-feu dans une architecture réseau d'entreprise ?
- **Q10** : Quelle est la valeur ajoutée de la journalisation des paquets bloqués dans un contexte de gestion de la sécurité réseau ?
- **Q11** : Comment un système de détection d'intrusions (IDS) pourrait-il être complémentaire aux règles de pare-feu dans une architecture réseau d'entreprise ?

Suivi post-TP :

vous devez fournir :

- Les règles de pare-feu créées (sous iptables ou UFW).
- Les résultats des tests de connectivité (ex. : captures de ping ou de requêtes HTTP réussies/échouées).
- Exemples de journaux montrant les paquets bloqués/autorisés.
- Réponses aux questions sur la sécurité réseau et l'architecture réseau.