

# ATELIER ET TRAVAUX PRATIQUES

## LE PROTOCOLE SSH

ECOLE EUROPEENE DE CYBERSECURITE  
DE VERSAILLE

PROMOTION 2024

## 1. Introduction à SSH et Connexion à Distance

### 1.1 Qu'est-ce que SSH ?

- Présentation de SSH (Secure Shell) et des avantages par rapport aux méthodes non sécurisées comme Telnet.
- **Objectif** : Comprendre pourquoi SSH est utilisé pour les connexions sécurisées à distance.

### 1.2 Connexion à un serveur SSH distant

- **Exercice 1** : Connexion à un serveur SSH public gratuit ([freeshell.org](http://freeshell.org)).
- **Commandes à exécuter** :
  1. **Se connecter à un serveur distant** :

```
ssh username@freeshell.org
```

2. **Vérifier la connexion** en exécutant les commandes suivantes sur le serveur distant :

```
ls
```

```
pwd
```

```
whoami
```

## 2. Authentification par Clés SSH

### 2.1 Génération et utilisation des clés SSH

- **Objectif** : Mettre en place une authentification par clés SSH pour sécuriser les connexions.
- **Exercice 2** : Générer des clés SSH et les installer sur un serveur distant.
- **Commandes à exécuter** :
  1. **Générer une paire de clés SSH** :

```
ssh-keygen -t ed25519
```

- La clé privée est sauvegardée dans `~/.ssh/id_rsa` et la clé publique dans `~/.ssh/id_rsa.pub`.

2. **Copier la clé publique sur le serveur distant** :

```
ssh-copy-id username@freeshell.org
```

### 2.2 Désactivation de l'authentification par mot de passe

- **Exercice 3** : Sécuriser davantage la connexion en désactivant l'authentification par mot de passe.
- **Commandes à exécuter** :
  1. **Modifier le fichier de configuration SSH** pour désactiver les mots de passe :

```
sudo nano /etc/ssh/sshd_config
```

- Changer la ligne :

PasswordAuthentication no

2. Redémarrer le service SSH pour appliquer les changements :

sudo systemctl restart ssh

3. Tester la connexion avec clé SSH, sans mot de passe :

ssh username@freeshell.org

---

### 3. Transfert de Fichiers avec SCP et SFTP

#### 3.1 Utilisation de SCP pour le transfert de fichiers

- **Objectif** : Transférer des fichiers entre la machine locale et un serveur distant via SCP.
- **Exercice 4** : Transférer un fichier avec SCP.
- **Commandes à exécuter** :

1. Créer un fichier local :

echo "Ceci est un fichier test" > fichier.txt

2. Transférer le fichier vers le serveur distant :

scp fichier.txt username@freeshell.org:/home/username/

3. Vérifier le fichier sur le serveur :

ssh username@freeshell.org "ls -l /home/username/"

#### 3.2 Utilisation de SFTP pour le transfert interactif

- **Objectif** : Utiliser SFTP pour un transfert interactif de fichiers.
- **Exercice 5** : Connexion SFTP pour naviguer et transférer des fichiers.
- **Commandes à exécuter** :

1. Connexion au serveur via SFTP :

sftp username@freeshell.org

2. Naviguer dans les répertoires distants :

ls

cd /home/username/

3. Transférer un fichier vers le serveur :

put fichier.txt

## Partie 1 : Questions 1 à 10

### Question 1 : Introduction à SSH

1. Qu'est-ce qui différencie SSH de Telnet en termes de sécurité ?

- A) SSH crypte les communications tandis que Telnet les envoie en clair.
- B) SSH est plus rapide que Telnet.
- C) Telnet nécessite un mot de passe, SSH non.
- D) Telnet crypte les communications, contrairement à SSH.

### Question 2 : Connexion à un serveur SSH

2. Quelle commande permet de se connecter à un serveur distant via SSH ?

- A) ssh -p username@freeshell.org
- B) scp username@freeshell.org
- C) ssh username@freeshell.org
- D) ftp [username@freeshell.org](mailto:username@freeshell.org)

### Question 3 : Authentification par clés SSH

3. Où est stockée la clé publique après la génération d'une paire de clés SSH avec la commande ssh-keygen ?

- A) /etc/ssh/id\_rsa.pub
- B) ~/.ssh/id\_rsa.pub
- C) /usr/local/.ssh/id\_rsa.pub
- D) /home/.ssh/id\_rsa

### Question 4 : Authentification par clés SSH

4. Quelle commande permet de copier la clé publique SSH sur un serveur distant pour l'authentification sans mot de passe ?

- A) ssh-keygen -copy username@freeshell.org
- B) scp ~/.ssh/id\_rsa.pub username@freeshell.org
- C) ssh-copy-id username@freeshell.org
- D) scp ~/.ssh/id\_rsa username@freeshell.org

#### Question 5 : Désactivation de l'authentification par mot de passe

5. Après avoir désactivé l'authentification par mot de passe dans la configuration SSH, quelle commande permet de redémarrer le service SSH pour appliquer les modifications ?
- A) sudo systemctl restart sshd
  - B) sudo systemctl start ssh
  - C) sudo service ssh restart
  - D) sudo reboot ssh

#### Question 6 : Sécurisation de la connexion SSH

6. Quelle directive du fichier de configuration SSH doit être modifiée pour désactiver l'authentification par mot de passe ?
- A) PasswordAuthentication no
  - B) PermitRootLogin no
  - C) PubkeyAuthentication yes
  - D) PasswordLogin no

#### Question 7 : Transfert de fichiers avec SCP

7. Quelle est la commande correcte pour transférer un fichier nommé data.txt vers le répertoire personnel d'un utilisateur distant via SCP ?
- A) scp data.txt username@freeshell.org:~/
  - B) ssh data.txt username@freeshell.org:/home/username/
  - C) scp username@freeshell.org data.txt:/home/username/
  - D) scp data.txt freeshell.org:/username/

#### Question 8 : Utilisation de SFTP

8. Comment se connecter en mode interactif à un serveur distant pour transférer des fichiers via SFTP ?
- A) ftp username@freeshell.org
  - B) ssh -f username@freeshell.org
  - C) sftp username@freeshell.org
  - D) scp -i username@freeshell.org

#### Question 9 : Navigation dans SFTP

9. Quelle commande permet de changer de répertoire dans une session SFTP ?

- A) ls
- B) mv
- C) cd
- D) dir

#### Question 10 : Transfert de fichiers avec SFTP

10. Quelle commande SFTP permet de transférer un fichier de la machine locale vers le serveur distant ?

- A) get
- B) send
- C) put
- D) transfer

---

## 4. Création de Tunnels SSH et Redirection de Ports

### 4.1 Redirection locale avec SSH

- **Objectif** : Sécuriser un service distant via un tunnel SSH.
- **Exercice 6** : Configurer un tunnel SSH.
- **Commandes à exécuter** :

1. **Rediriger le port local 8080 vers le port 80 d'un serveur distant :**

```
ssh -L 8080:localhost:80 username@freeshell.org
```

2. **Accéder à l'application via le port local :**

- Ouvrir un navigateur et accéder à http://localhost:8080.

---

## 5. Sécurisation du Serveur SSH

### 5.1 Changer le port SSH

- **Objectif** : Réduire les attaques brute-force en changeant le port par défaut de SSH.
- **Exercice 7** : Modifier le port SSH.
- **Commandes à exécuter** :

Attention, il existe une autre méthode qui requiert le pare-feu UFW. Exercice facultatif, trouvez la méthode ou les méthodes de gestion de ports via UFW.

1. **Modifier le fichier de configuration SSH :**

```
sudo nano /etc/ssh/sshd_config
```

- Changer le port :

Port 2222

2. **Redémarrer le service SSH pour appliquer les modifications :**

```
sudo systemctl restart ssh
```

3. **Se connecter au nouveau port :**

```
ssh -p 2222 username@freeshell.org
```

## 5.2 Configurer Fail2Ban

- **Objectif :** Protéger le serveur contre les attaques bruteforce en bloquant les IP après plusieurs tentatives échouées.
- **Exercice 8 :** Installer et configurer Fail2Ban.
- **Commandes à exécuter :**

1. **Installer Fail2Ban :**

```
sudo apt install fail2ban
```

2. **Configurer Fail2Ban pour SSH :**

```
sudo nano /etc/fail2ban/jail.local
```

- Ajouter la section suivante :

```
[sshd]
```

```
enabled = true
```

```
port = 2222
```

3. **Redémarrer Fail2Ban :**

```
sudo systemctl restart fail2ban
```

---

## 6. Projet Final : Configuration Complète d'un Serveur SSH

- **Objectif global :** Consolider toutes les compétences apprises en configurant un serveur SSH complet et sécurisé avec redirection de port et transfert de fichiers.
- **Exercice pratique final :**
  1. **Configurer un serveur SSH sécurisé** (changer de port, authentification par clé).
  2. **Configurer un tunnel SSH** et rediriger le trafic.
  3. **Transférer des fichiers via SCP et SFTP.**

---

### 6.1 Exercice Bonus (Optionnel) : Observer le Trafic Réseau avec Wireshark

**Objectif global :** Cet exercice a pour objectif de montrer visuellement les échanges chiffrés entre un client et un serveur lors d'une connexion SSH.

## Étape 1 : Installation et lancement de Wireshark

### 1. Installer Wireshark :

- Sous Linux (Debian/Ubuntu) :

- Ouvrez un terminal et exécutez la commande suivante pour installer Wireshark :

```
sudo apt update
```

```
sudo apt install wireshark
```

- Lors de l'installation, il peut vous être demandé si vous souhaitez permettre à des utilisateurs non-root de capturer des paquets. Répondez Yes pour plus de flexibilité.

### 2. Lancer Wireshark :

```
sudo wireshark
```

## Étape 2 : Configurer Wireshark pour capturer le trafic SSH

### 1. Sélectionner l'interface réseau :

- Une fois Wireshark ouvert, vous verrez une liste des interfaces réseau disponibles (Wi-Fi, Ethernet, etc.).
- Sélectionnez l'interface sur laquelle vous souhaitez capturer le trafic (par exemple, eth0 pour Ethernet ou wlan0 pour Wi-Fi).

### 2. Appliquer un filtre pour le trafic SSH :

- Dans le champ Filter situé en haut de la fenêtre, entrez le filtre suivant pour capturer uniquement les paquets SSH :

```
tcp.port == 2222
```

- Remarque : Remplacez 2222 par le port SSH que vous avez configuré. Si vous utilisez le port SSH par défaut, utilisez tcp.port == 22.

### 3. Démarrer la capture de paquets :

- Cliquez sur le bouton vert Start (en forme de requin) pour lancer la capture des paquets réseau sur l'interface sélectionnée.

## Étape 3 : Initier une connexion SSH sécurisée

### 1. Ouvrir un terminal et établir une connexion SSH :

- Depuis votre machine locale, établissez une connexion SSH vers votre serveur en utilisant le port sécurisé et l'authentification par clé SSH :

```
ssh -p 2222 username@votre_serveur
```

- Remplacez 2222 par le port personnalisé que vous avez configuré, ou 22 si vous utilisez le port par défaut.

## 2. Exécuter des commandes pour générer du trafic :

- Une fois connecté à votre serveur, exécutez quelques commandes simples pour générer des échanges réseau. Par exemple :

ls

pwd

whoami

- Ces commandes généreront du trafic réseau que Wireshark pourra capturer et afficher.

### Étape 4 : Analyser les paquets capturés dans Wireshark

#### 1. Observer les paquets SSH capturés :

- Après avoir exécuté les commandes SSH, revenez à Wireshark et arrêtez la capture en cliquant sur le bouton rouge Stop.
- Dans la colonne Protocol, vous verrez des paquets marqués comme TCP et SSH. Ces paquets représentent les échanges entre votre client SSH et le serveur.

#### 2. Comprendre les échanges TCP :

- Vous verrez des paquets SYN et ACK qui sont utilisés pour établir une connexion TCP, ainsi que des paquets SSH.
- Ces paquets montrent que la connexion SSH a été établie avec succès, mais le contenu des paquets est chiffré, donc illisible.

#### 3. Observer les effets de Fail2Ban (optionnel) :

- Si Fail2Ban est configuré sur le serveur, vous pouvez observer comment il bloque les adresses IP après plusieurs tentatives échouées de connexion.
- Pour cela, essayez de provoquer plusieurs échecs de connexion SSH (par exemple, en entrant un mauvais mot de passe ou une mauvaise clé) depuis un autre terminal.
- Après un certain nombre de tentatives, Fail2Ban bloquera votre IP, ce qui sera visible dans Wireshark sous forme d'arrêt des paquets SSH venant de votre IP.

## Partie 2 : Questions 11 à 20

### Question 11 : Redirection de ports avec SSH

11. Quelle commande permet de rediriger le port 8080 de votre machine locale vers le port 80 d'un serveur distant via un tunnel SSH ?

- A) ssh -L 80:localhost:8080 username@freeshell.org
- B) ssh -L 8080:localhost:80 username@freeshell.org
- C) ssh -R 8080:localhost:80 username@freeshell.org
- D) ssh -R 80:localhost:8080 [username@freeshell.org](mailto:username@freeshell.org)

### Question 12 : Accès à un service redirigé avec un tunnel SSH

12. Une fois un tunnel SSH créé pour rediriger le port 8080 local vers le port 80 distant, comment accéder au service ?

- A) Via l'adresse IP publique du serveur distant
- B) En accédant à http://localhost:8080
- C) En utilisant la commande ssh-access 8080
- D) En accédant à <http://freeshell.org:80>

### Question 13 : Changement du port SSH

13. Après avoir changé le port SSH par défaut dans le fichier de configuration `sshd_config`, quelle commande permet de se connecter à ce nouveau port ?

- A) ssh username@freeshell.org
- B) ssh -P 2222 username@freeshell.org
- C) ssh -p 2222 username@freeshell.org
- D) ssh -port 2222 [username@freeshell.org](mailto:username@freeshell.org)

### Question 14 : Sécurisation du serveur SSH

14. Quelle commande permet de redémarrer le service SSH après avoir modifié son port dans le fichier de configuration ?

- A) sudo systemctl restart ssh
- B) sudo sshd restart
- C) systemctl ssh restart
- D) ssh restart

#### **Question 15 : Installation de Fail2Ban**

15. **Quelle commande permet d'installer Fail2Ban sur un serveur Linux pour protéger le service SSH ?**
- A) apt install ssh-fail2ban
  - B) sudo apt-get install fail2ban
  - C) sudo yum install fail2ban
  - D) apt install fail2ban ssh

#### **Question 16 : Configuration de Fail2Ban**

16. **Quel fichier Fail2Ban doit être modifié pour activer la protection du service SSH sur un port personnalisé ?**
- A) /etc/ssh/sshd\_config
  - B) /etc/fail2ban/fail2ban.conf
  - C) /etc/fail2ban/jail.local
  - D) /usr/local/fail2ban/config

#### **Question 17 : Paramétrage de Fail2Ban**

17. **Quelle directive dans le fichier jail.local permet d'activer Fail2Ban pour le service SSH ?**
- A) ssh = true
  - B) [sshd] enabled = true
  - C) sshd\_enable = true
  - D) fail2ban\_enable = yes

#### **Question 18 : Configuration SSH avancée**

18. **Quel est l'avantage de changer le port SSH par défaut (22) ?**
- A) Augmenter la vitesse de connexion
  - B) Réduire les attaques brute-force automatisées
  - C) Activer le transfert de fichiers
  - D) Utiliser plusieurs comptes SSH simultanément

#### **Question 19 : Transfert de fichiers sécurisé**

**19. Quel protocole est utilisé par SCP pour sécuriser le transfert de fichiers ?**

- A) FTP
- B) SFTP
- C) HTTPS
- D) SSH

#### **Question 20 : Utilisation des clés SSH**

**20. Que contient la clé privée générée par ssh-keygen ?**

- A) Une copie de la clé publique
- B) Les informations de chiffrement nécessaires pour déchiffrer les communications
- C) Le mot de passe de l'utilisateur
- D) Un certificat de sécurité

### Question théorique :

*Dans un contexte où la confidentialité et l'intégrité des données sont cruciales, pourquoi est-il nécessaire de chiffrer les connexions SSH, et en quoi des mesures comme le changement de port ou l'utilisation de Fail2Ban contribuent-elles à renforcer cette protection ? En observant le trafic réseau avec des outils comme Wireshark, que peut-on déduire sur la manière dont la sécurité SSH est mise en œuvre au niveau réseau, même si le contenu des échanges est chiffré ?*

### Pistes de réflexion :

1. Confidentialité des données
2. Observation avec Wireshark
3. Changement de port et Fail2Ban

**Conclusion :** *\*\* Rédiger une conclusion avec votre compréhension et votre vocabulaire sur le protocole SSH. \*\**

Félicitations ! 

Vous avez maintenant toutes les bases (voir plus !) du protocole SSH. Que ce soit pour se connecter à distance, sécuriser un serveur ou transférer des fichiers, vous êtes prêt(e) à gérer tout ça avec confiance.

Bravo pour votre travail et votre engagement, et n'oubliez pas : la pratique est la clé pour continuer à progresser !



# **ECOLE EUROPEENE DE CYBERSECURITE DE VERSAILLE**

## **PROMOTION 2024**