TP

SOMMAIRE

Partie I : Ports couramment ouverts sur un système Linux et vulnérables

1. Port 22 – SSH (Secure Shell)

- **Fonction** : Permet les connexions distantes sécurisées à la ligne de commande (admin système, transfert de fichiers avec SCP, etc.).
- **Attaques fréquentes** :
    - **Brute force** (essais multiples de mots de passe)
    - **Exploitation de vulnérabilités dans SSH** si la version est obsolète
- **Exemples réels** : Des millions de serveurs sont quotidiennement scannés pour trouver des accès SSH faibles.
- **Mesures de protection** :
    - Utiliser **l'authentification par clés SSH**
    - Modifier le port par défaut (ex. : 2222)
    - Bloquer les adresses IP suspectes avec fail2ban
    - Restreindre l'accès via un **pare-feu (ufw, iptables)**

2. Port 80 – HTTP / Port 443 – HTTPS

- **Fonction** :
    - Port 80 : accès web non chiffré
    - Port 443 : accès web sécurisé via TLS/SSL
- **Attaques fréquentes** :
    - Injection SQL
    - Cross-site scripting (XSS)
    - Exploitation de failles CMS (WordPress, Joomla…)
- **Exemples** : Piratage de sites web via plugins vulnérables ou mauvaise configuration Apache/Nginx.
- **Mesures de protection** :
    - Installer un **certificat SSL/TLS** (Let's Encrypt)

- Utiliser un **pare-feu d'application web (WAF)**
- Tenir les CMS et frameworks à jour

3. Port 3306 – MySQL

- **Fonction** : Connexion à une base de données MySQL ou MariaDB
- **Attaques fréquentes** :
  - Accès non autorisé à la base de données
  - Vol de données sensibles
- **Problèmes courants** :
  - Port exposé publiquement sans authentification forte
- **Mesures de protection** :
  - Limiter l'accès à localhost ou à une IP précise
  - Ne pas autoriser l'accès root à distance
  - Utiliser des comptes limités avec des mots de passe forts

II. Ports couramment ouverts sur un système Windows et vulnérables

1. Port 3389 – RDP (Remote Desktop Protocol)

- **Fonction** : Permet de prendre le contrôle du bureau à distance
- **Attaques fréquentes** :
  - **Brute force** (avec des bots automatisés)
  - **Exploitation de vulnérabilités RDP** (ex. : **BlueKeep** - CVE-2019-0708)
- **Exemples** : Plusieurs ransomwares se sont propagés via des failles RDP.
- **Mesures de protection** :
  - Activer le **chiffrement réseau**
  - Limiter l'accès aux IP de confiance
  - Mettre en place une **authentification à deux facteurs**

- Utiliser des **VPN** pour sécuriser les connexions

2. Port 445 – SMB (Server Message Block)

- **Fonction** : Partage de fichiers et d'imprimantes dans les réseaux Windows
- **Attaques fréquentes** :
  - **WannaCry**, **NotPetya**, **EternalBlue** utilisent SMB pour se propager
- **Risque** : Port très souvent utilisé dans les attaques internes à l'entreprise
- **Mesures de protection** :
  - Désactiver **SMBv1**
  - Restreindre l'accès aux réseaux internes uniquement
  - Appliquer les correctifs de sécurité Microsoft

3. Port 135 – RPC (Remote Procedure Call)

- **Fonction** : Permet la communication entre processus sur des réseaux distribués
- **Attaques fréquentes** :
  - Exécution de code à distance
  - Attaques DCOM
- **Exemples** : Détection de vulnérabilités sur les anciennes versions de Windows
- **Mesures de protection** :
  - Restreindre l'accès avec un **pare-feu Windows**
  - Utiliser des tunnels VPN ou TLS pour sécuriser les communications RPC

III. Recommandations générales pour Linux et Windows

Mesure de sécurité	Description
Scan régulier	Utiliser nmap, netstat, ss, PowerShell pour voir les ports ouverts
Pare-feu actif	iptables, ufw, ou **Pare-feu Windows** doivent limiter les accès réseau
Désactiver les services inutiles	Moins il y a de services actifs, moins il y a de surfaces d'attaque
Authentification forte	Mots de passe complexes, clé SSH, double authentification
Mise à jour régulière	Systèmes et applications doivent être à jour pour corriger les vulnérabilités connues
Segmentation réseau	Ne pas exposer tous les services à Internet (ex : MySQL doit être en accès local)

Conclusion

Les **ports réseau ouverts** sont indispensables au fonctionnement d'un système Linux ou Windows, mais ils sont également une **surface d'attaque majeure**. Les attaquants les ciblent en premier lors d'un scan réseau.

Il est donc indispensable pour tout administrateur système ou ingénieur réseau :

- de **connaître les services actifs**,
- de **restreindre l'accès aux ports critiques**,
- et de **sécuriser chaque point d'entrée** avec des politiques de sécurité adaptées.

Partie II : Shutdown/? Dans le shell de Windows et Linux

1. Shutdown ? Dans le shell de Windows

```
C:\Users\admrsedagbande>shutdown ?
Syntaxe : shutdown [/i | /l | /s | /sg | /r | /g | /a | /p | /h | /e | /o]
[/hybrid] [/soft] [/fw] [/f]
    [/m \\ordinateur][/t xxx][/d [p|u:]xx:yy [/c "commentaire"]]

    Sans argument    Afficher l’aide. Cela revient à entrer /?.
    /?          Afficher l’aide. Cela revient à n’entrer aucune option.
    /i          Afficher l’interface utilisateur graphique (GUI).
                Ce doit être la première option.
    /l          Fermer la session. Ne peut pas être utilisé avec l’option /m
                ou /d.
    /s          Arrêter l’ordinateur.
    /sg         Arrêtez l'ordinateur. Au démarrage suivant, si l'authentification de
redémarrage automatique
                est activée, se connecter automatiquement et verrouiller le dernier
utilisateur interactif.
                Une fois connecté, redémarrez les applications inscrites.
    /r          Arrêtez complètement l’ordinateur et redémarrez-le.
    /g          Arrêter complètement et redémarrer l'ordinateur. Une fois le système
redémarré,
                si l'authentification de redémarrage automatique est activée, se
                automatiquement et verrouiller le dernier utilisateur interactif.
                Une fois connecté, redémarrez les applications inscrites.
    /a          Annuler un arrêt du système.
                Utilisable uniquement pendant le délai imparti.
                Regrouper avec /fw pour effacer tout démarrage en attente vers le
microprogramme.
    /p Éteindre l'ordinateur local sans délai ni avertissement.
                Peut être utilisé avec les options /d et /f.
    /h          Mettre l’ordinateur local en veille prolongée.
                Utilisable avec l’option /f.
    /hybrid     Arrête l’ordinateur et le prépare pour un démarrage rapide.
                Doit être utilisé avec l’option /s.
    /fw         S’associe à l’option d’arrêt pour transférer le prochain démarrage
vers
.                l’interface utilisateur du microprogramme.
    /e          Documenter la raison de l’arrêt inattendu d’un ordinateur.
    /o          Accéder au menu des options de démarrage avancées et redémarrer
l’ordinateur.
                Doit être utilisé avec l’option /r.
    /m \\ordinateur Spécifier l’ordinateur cible.
    /t xxx      Définir la durée avant l’arrêt au bout de xxx secondes
                La plage valide est de 0 à 315360000 (10 ans), avec une valeur par
défaut de 30.
                Si le délai d'attente est supérieur à 0, le paramètre /f est
.                est sous-entendu.
```

/c « commentaire » Commentaire sur la raison du redémarrage ou de l’arrêt.
512 caractères maximum autorisés.
/f Forcer la fermeture des applications en cours d’exécution sans prévenir les utilisateurs.
Le paramètre /f est implicite lorsqu'une valeur supérieure à 0 est utilisée.
est spécifié pour le paramètre /t.
/d [p|u:]xx:yy Fournit la raison du redémarrage ou de l’arrêt.
p indique que le redémarrage ou l’arrêt est planifié.
u indique que la raison est définie par l’utilisateur.
Si ni p ni u ne sont spécifiés, le redémarrage ou l’arrêt n’est pas planifié.
xx représente le code de raison principale (entier positif inférieur à 256).
yy représente le code de raison secondaire (entier positif inférieur à 65536).

2. Shutdown ? Dans le shell de Linux

```
ubuntu@apache2:~$ man shutdown

NAME
       shutdown - Halt, power off or reboot the machine

SYNOPSIS

       shutdown [OPTIONS...] [TIME] [WALL...]

DESCRIPTION
       shutdown may be used to halt, power off, or reboot the machine.

       The first argument may be a time string (which is usually "now"). Optionally, this may be followed by a wall message to be sent to all logged-in users before going down.

       The time string may either be in the format "hh:mm" for hour/minutes specifying the time to execute the shutdown at, specified in 24h clock format. Alternatively it may be in the syntax "+m"
       referring to the specified number of minutes m from now.  "now" is an alias for "+0", i.e. for triggering an immediate shutdown. If no time argument is specified, "+1" is implied.

       Note that to specify a wall message you must specify a time argument, too.

       If the time argument is used, 5 minutes before the system goes down the /run/nologin file is created to ensure that further logins shall not be allowed.

OPTIONS
```

The following options are understood:

--help
Print a short help text and exit.

-H, --halt
Halt the machine.

-P, --poweroff
Power the machine off (the default).

-r, --reboot
Reboot the machine.

-h
The same as --poweroff, but does not override the action to take if it is "halt". E.g. shutdown --reboot -h means "poweroff", but shutdown --halt -h means "halt".

-k
Do not halt, power off, or reboot, but just write the wall message.

--no-wall
Do not send wall message before halt, power off, or reboot.

-c
Cancel a pending shutdown. This may be used to cancel the effect of an invocation of shutdown with a time argument that is not "+0" or "now".

--show
Show a pending shutdown action and time if there is any.

Added in version 250.

EXIT STATUS
On success, 0 is returned, a non-zero failure code otherwise.

COMPATIBILITY

Partie III: Comparaison entre l’adressage statique et dynamique

		Solution	
		Adressage statique	Adressage dynamique
Comparaison	Avantage	- Configuration stable - Contrôle total de l’adresse IP - Idéal pour les serveurs ou équipements réseau fixes	- Configuration automatique - Gain de temps pour l’administrateur - Moins d’erreurs humaines
	Inconvénient	- Configuration manuelle fastidieuse - Risque d’erreurs de duplication IP - Moins flexible en cas de mobilité	- Changement d’adresse à chaque redémarrage - Dépendance au serveur DHCP - Moins de contrôle sur les adresses IP attribuées