| COMMANDE | DESCRIPTION |
| --- | --- |
| netstat -tulpn | Afficher les ports réseau Linux avec les ID de processus (PID) |
| watch ss -stplu | Regardez les ports TCP et UDP ouverts en temps réel. |
| lsof -i | Montrer les connexions établies. |
| macchanger -m MACADDR INTR | Changer l’adresse MAC (Kali). |
| ifconfig eth0 192.168.2.1/24 | Définir une adresse IP sous Linux. |
| ifconfig eth0:1 192.168.2.3/24 | Ajouter une adresse IP à une interface existante. |
| ifconfig eth0 hw ether MACADDR | Changer l’adresse MAC via ifconfig. |
| ifconfig eth0 mtu 1500 | Changer la taille du MTU (Maximum Transmission Unit – taille maximum des données transitant sur le réseau). |
| dig -x 192.168.1.1 | Faire une recherche inverse d’une adresse IP. |
| host 192.168.1.1 | Recherche inverse avec la commande host. |
| dig @192.168.2.2 domain.com -t AXFR | Transfert de zone DNS via dig. |
| host -l domain.com nameserver | Transfert de zone DNS avec host. |
| nbtstat -A x.x.x.x | Obtenir le nom d’hôte depuis une adresse IP. |
| ip addr add 192.168.2.22/24 dev eth0 | Ajoute une adresse IP cachée dans Kali, non affichée avec ifconfig. |
| tcpkill -9 host google.com | Bloque l’accès à google.com. |
| echo "1" > /proc/sys/net/ipv4/ip\_forward | Activer l’IP forwarding pour transformer Kali en routeur par lequel transite les données. |
| echo "8.8.8.8" > /etc/resolv.conf | Utiliser les serveurs DNS de Google. |

# Commandes systèmes

| COMMANDE | DESCRIPTION |
| --- | --- |
| whoami | Affiche l’utilisateur connecté à la machine Linux. |
| id | Affiche des informations sur l’utilisateur courant. |
| last | Affiche les dernières connexions utilisateurs. |
| mount | Afficher les périphériques montés. |
| df -h | Affiche l’utilisation disque. |
| echo "user:passwd" | chpasswd | Réinitialise le mot de passe en une commande. |
| getent passwd | Liste les utilisateurs Linux. |
| strings /chemin/prog | Affiche les chaînes de caractères d’un programme. |
| uname -ar | Affiche la version du noyau. |
| PATH=$PATH:/mon/chemin | Ajoute un nouveau chemin à la variable PATH. |
| history | Affiche l’historique des commandes tapées. |

# Debian / Ubuntu (Kali)

| COMMANDE | DESCRIPTION |
| --- | --- |
| cat /etc/debian\_version | Affiche la version de Debian. |
| cat /etc/\*-release | Affiche la version d’Ubuntu. |
| dpkg -l | Liste les packages installés. |

# Gestion des utilisateurs

| COMMANDE | DESCRIPTION |
| --- | --- |
| useradd new-user | Créer un nouvel utilisateur |
| passwd username | Réinitialise le mot de passe de l’utilisateur « username » |
| deluser username | Retire un utilisateur du système. |

# Commandes de décompression de fichiers

| COMMANDE | DESCRIPTION |
| --- | --- |
| unzip archive.zip | Extrait un fichier .zip. |
| zipgrep \*.txt archive.zip | Cherche dans un fichier .zip. |
| tar xf archive.tar | Extrait un fichier .tar. |
| tar xvzf archive.tar.gz | Extrait un fichier .tar.gz. |
| tar xjf archive.tar.bz2 | Extrait un fichier .tar.bz2. |
| tar ztvf file.tar.gz | grep blah | Recherche dans un fichier tar.gz. |
| gzip -d archive.gz | Extrait un fichier .gz. |
| zcat archive.gz | Lit un fichier .gz sans le décompresser. |
| zless archive.gz | Même commande que précédemment. |
| zgrep 'blah' /var/log/maillog\*.gz | Cherche dans un fichier compressé (par exemple un fichier log) |
| Nano fichier.txt | Edite un fichier quelconque avec nano. |
| upx -9 -o output.exe input.exe | Compresse un fichier .exe avec UPX. |

# Commandes de compression de fichiers

| COMMAND | DESCRIPTION |
| --- | --- |
| zip -r file.zip /dir/\* | Créer un fichier .zip. |
| tar cf archive.tar files | Créer un fichier .tar. |
| tar czf archive.tar.gz files | Créer un fichier .tar.gz. |
| tar cjf archive.tar.bz2 files | Créer un fichier .tar.bz2. |
| gzip file | Créer un fichier gzip. |

# Commandes de gestion de fichiers

| COMMANDE | DESCRIPTION |
| --- | --- |
| df -h blah | Affiche la taille d’un fichier. |
| diff file1 file2 | Affiche les différences entre deux fichiers. |
| md5sum file | Génère un hash md5. |
| md5sum -c blah.iso.md5 | Vérifie le hash md5 d’un fichier (le hach .md5 doit être dans le même dossier que le fichier à tester) |
| file blah | Affiche le type du fichier. |
| dos2unix | Convertit les lignes Windows en Linux. |
| base64 < input-file > output-file | Encode un fichier en Base64 et génère un fichier encodé résultant. |
| base64 -d < input-file > output-file | Décode un fichier en Base64 et génère un fichier décodé résultant. |
| touch -r ref-file new-file | Créer un nouveau fichier avec la même date que celle d’un fichier de référence. |
| rm -rf | Supprimer un dossier et TOUT son contenu sans confirmation. |

/bin/sh -i

# Autres commandes

| COMMAND | DESCRIPTION |
| --- | --- |
| init 6 | Redémarre Linux (comme “reboot”) |
| gcc -o output.c input.c | Compilation de code C. |
| gcc -m32 -o output.c input.c | Compile du code 32bits. |
| unset HISTORYFILE | Désactive l’historique des commandes tapées. |
| rdesktop X.X.X.X | Connexion à un serveur RDP. |
| kill -9 $$ | Terminer la session courante. |
| chown user:group blah | Changer le propriétaire d’un fichier/dossier. |
| chown -R user:group blah | Changer le propriétaire d’un dossier et tous les sous-dossiers. |
| chmod a+rwx file | Changer les permissions d’un fichier. a pour « tout le monde », + pour ajouter des droits (- pour supprimer), r = lecture, w = écriture, x = exécution. |

Supprimer l’historique bash :

ssh user@X.X.X.X | cat /dev/null > ~/.bash\_history

# Permissions du système de fichier

| VALEUR | SIGNIFICATION |
| --- | --- |
| 777 | rwxrwxrwx Pas de restrictions, les droits pour tous les utilisateurs. |
| 755 | rwxr-xr-x Le propriétaire à tous les droits, les autres peuvent seulement lire et exécuter le fichier. |
| 700 | rwx------ Uniquement le propriétaire a tous les droits. |
| 666 | rw-rw-rw- Tous les utilisateurs peuvent lire et écrire le fichier, mais pas l’exécuter. |
| 644 | rw-r--r—Le propriétaire peut lire et écrire, les autres uniquement lire. |

Exemple d’application avec chmod :

chmod 755 fichier

On peut utiliser la notation suivante :

chmod o-rwx

pour retirer les droits de lecture (« r »), écriture (« w ») et exécution (« x ») aux autres utilisateurs (non propriétaire, et non membre du même groupe)

# Fichiers Linux intéressants

Fichiers notamment utilisés lors des tests d’intrusion.

| DOSSIER/FICHIER | DESCRIPTION |
| --- | --- |
| /etc/passwd | Contient la liste des utilisateurs. |
| /etc/shadow | Contient la liste des mots de passe chiffrés. |
| /etc/group | Contient les groupes. |
| /etc/init.d/ | Contient la liste des programmes lancés au démarrage de la machine. |
| /etc/hostname | Nom d’hôte système. |
| /etc/network/interfaces | Interfaces réseau. |
| /etc/resolv.conf | Serveurs DNS. |
| /etc/profile | Variables d’environnement systèmes. |
| ~/.ssh/ | Clés SSH. |
| ~/.bash\_history | Historique des utilisateurs |
| /var/log/ | Fichiers logs systems et applications. |
| /var/adm/ | Autres fichiers/dossiers logs. |