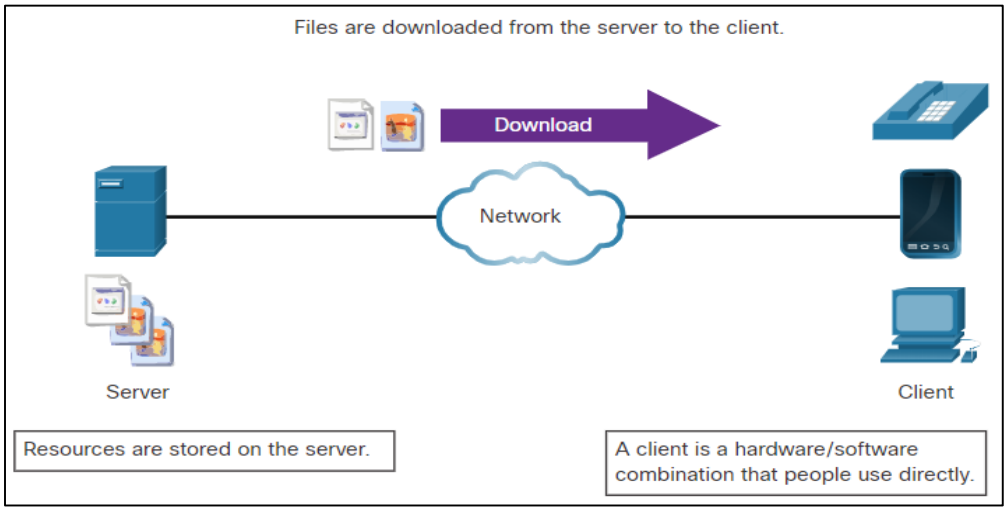
Chapitre 05 : Administration Système

5.1. Serveurs et Clients Linux

5.1.1. Présentation des communications client-serveur

- Les serveurs sont des ordinateurs sur lesquels est installé un logiciel qui leur permet d'offrir des services aux clients à travers le réseau.
- Certains fournissent aux clients, sur demande, des ressources externes telles que des fichiers, des messages e-mail ou des pages web.
- D'autres services exécutent des tâches de maintenance telles que la gestion des événements, la gestion de la mémoire, l'analyse de disque, etc.
- Chaque service nécessite un logiciel serveur distinct.
- Par exemple, le serveur sur la figure utilise un logiciel serveur de fichiers pour permettre aux clients d'extraire et de soumettre des fichiers.



5.1.2. Serveurs, services et ports

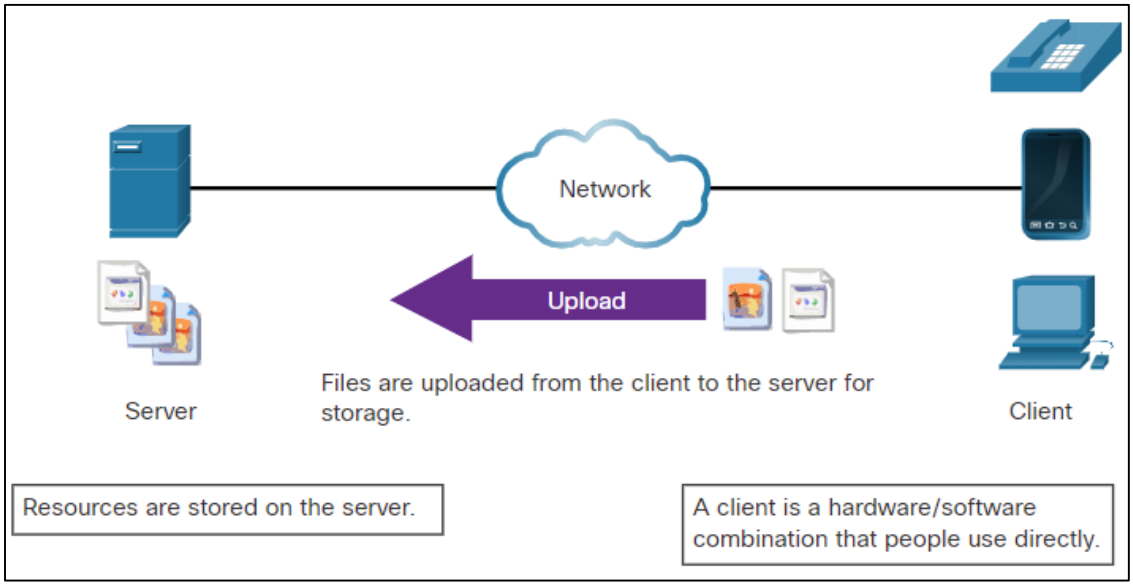
- Un port est une ressource réseau réservée utilisée par un service.
- Si l'administrateur peut décider quel port utiliser pour un service donné, de nombreux clients sont configurés pour utiliser un port spécifique par défaut.
- Le tableau répertorie quelques ports couramment utilisés et leurs services. Ils sont également appelés «ports connus».

Port	Description
20/21	FTP (File Transfer Protocol)
22	SSH (Secure Shell)
23	Service de connexion à distance Telnet
25	Protocole SMTP
53	Système DNS (Domain Name System)
67/68	Protocole DHCP (Dynamic Host Configuration Protocol)
69	Protocole TFTP (Trivial File Transfer Protocol)
80	Protocole HTTP (Hypertext Transfer Protocol)
110	protocole POP3 (Post Office Protocol version 3)
123	Protocole NTP (Network Time Protocol)
143	IMAP (Internet Message Access Protocol)
161/162	Simple Network Management Protocol (SNMP)
443	HTTPS (HTTP Secure)

5.1.3. Clients

- Les clients sont les programmes ou des applications conçus pour communiquer avec un serveur spécifique.
- Les clients, ou applications clientes, utilisent un protocole bien défini pour communiquer avec le serveur.

- Les navigateurs web sont des clients web utilisés pour communiquer avec des serveurs web via le protocole HTTP (Hyper Text Transfer Protocol) sur le port 80.
- Un client FTP (File Transfer Protocol) est un logiciel utilisé pour communiquer avec un serveur FTP.
- La figure montre un client en train de charger des fichiers sur un serveur.



5.1.4. Travaux pratiques – Serveurs Linux

Au cours de ces travaux pratiques, vous utiliserez la ligne de commande Linux pour identifier les serveurs exécutés sur un ordinateur.

5.2. Administration de base du serveur

5.2.1. Fichiers de configuration de service

- Sous Linux, les services sont gérés à l'aide de fichiers de configuration.
- Les options courantes dans le fichier de configuration sont le numéro de port, l'emplacement des ressources hébergées et les détails d'autorisation du client.
- Lorsque le service démarre, il recherche ses fichiers de configuration, les charge en mémoire et s'ajuste en fonction des paramètres des fichiers.
- La sortie de commande présente une partie du fichier de configuration pour Nginx, un serveur web léger pour Linux.

```
[analyst@secOps ~]$ cat /etc/nginx/nginx.conf
#user html;
worker_processes  1;
#error_log  logs/error.log;
#error_log  logs/error.log  notice;
#error_log  logs/error.log  info;
#pid        logs/nginx.pid;
events {
    worker_connections  1024;
}
http {
    include       mime.types;
    default_type  application/octet-stream;
    #log_format  main  '$remote_addr - $remote_user [$time_local] "$request" '
    #                  '$status $body_bytes_sent "$http_referer" '
    #                  '"$http_user_agent" "$http_x_forwarded_for"';
    #access_log  logs/access.log  main;
```

La sortie de commande suivante présente le fichier de configuration pour le protocole NTP (Network Time Protocol)

```
[analyst@secOps ~]$ cat /etc/ntp.conf
# Please consider joining the pool:
#
#       http://www.pool.ntp.org/join.html
#
# For additional information see:
# - https://wiki.archlinux.org/index.php/Network_Time_Protocol_daemon
# - http://support.ntp.org/bin/view/Support/GettingStarted
# - the ntp.conf man page
# Associate to Arch's NTP pool
server 0.arch.pool.ntp.org
server 1.arch.pool.ntp.org
server 2.arch.pool.ntp.org
server 3.arch.pool.ntp.org
# By default, the server allows:
# - all queries from the local host
# - only time queries from remote hosts, protected by rate limiting and kod
restrict default kod limited nomodify nopeer noquery notrap
restrict 127.0.0.1
restrict ::1
# Location of drift file
[analyst@secOps ~]$
```

- La dernière sortie de commande présente le fichier de configuration de Snort, un système de détection d'intrusion (IDS) basé sur Linux.
- Il n'existe aucune règle pour un format de fichier de configuration. C'est le choix du développeur du service. Cependant, le format **option = valeur**est souvent utilisé.

```
[analyst@secOps ~]$ cat /etc/snort/snort.conf
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#       http://www.snort.org                    Snort Website
#       http://vrt-blog.snort.org/      Sourcefire VRT Blog
#
#       Mailing list Contact:   snort-sigs@lists.sourceforge.net
#       False Positive reports: fp@sourcefire.com
#       Snort bugs:             bugs@snort.org
#
#       Compatible with Snort Versions:
#       VERSIONS : 2.9.9.0
#
#       Snort build options:
#       OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --
enable-zlib --enable-active-response --enable-normalizer --enable-reload --enable-react --enable-
flexresp3
<output omitted>
##################################################
# Step #1: Set the network variables.  For more information, see README.variables
##################################################
# Setup the network addresses you are protecting
###ipvar HOME_NET any
###ipvar HOME_NET [192.168.0.0/24,192.168.1.0/24]
ipvar HOME_NET [209.165.200.224/27]
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
```

5.2.2. Renforcement de la sécurité des appareils

- Le renforcement des appareils implique l'implémentation de méthodes éprouvées de sécurisation de l'appareil et la protection de son accès administratif.
- Certaines de ces méthodes impliquent de tenir à jour les mots de passe, de configurer des fonctionnalités de connexion distante améliorée et de mettre en œuvre SSH.
- Selon la distribution Linux, de nombreux services sont activés par défaut. Arrêter ces services et s'assurer qu'ils ne sont pas lancés automatiquement au démarrage est une autre technique de renforcement des appareils.
- Les mises à jour du système d'exploitation sont également extrêmement importantes pour renforcer la sécurité de l'appareil. Les développeurs du système d'exploitation créent et publient régulièrement des correctifs.

5.2.3. Renforcement de la sécurité des appareils

Voici les meilleures pratiques de base pour renforcer la sécurité des appareils

- Assurer la sécurité physique

- Réduire le nombre de packages installés
- Désactiver les services inutilisés
- Utiliser SSH et désactiver l'identifiant du compte racine (root) via SSH
- Mettre le système à jour régulièrement
- Désactiver la détection automatique USB
- Imposer l'utilisation de mots de passe forts
- Modifier régulièrement les mots de passe
- Empêcher les utilisateurs de réutiliser d'anciens mots de passe

5.2.4. Surveillance des journaux de service

- Les fichiers journaux sont des enregistrements qu'un ordinateur stocke pour garder une trace des événements importants. Les événements du noyau, des services et des applications sont tous enregistrés dans des fichiers journaux.
- En surveillant les fichiers journaux Linux, un administrateur acquiert une image claire des performances de l'ordinateur, de l'état de sa sécurité et des problèmes sous-jacents.
- Sous Linux, les fichiers journaux peuvent être classés de la façon suivante :
    - Journaux d'applications
    - Journaux d'événements
    - Journaux de services
    - Journaux système

Certains journaux contiennent des informations sur les processus démons (daemon) qui s'exécutent dans le système Linux. Un démon est un processus d'arrière-plan qui s'exécute automatiquement.

Le tableau répertorie quelques fichiers journaux Linux courants et leurs fonctions :

Fichier journal Linux	Description
/var/log/messages	• Ce répertoire contenant les journaux d'activités génériques de l'ordinateur • Il sert principalement à stocker les messages système d'information non critiques.
/var/log/auth.log	• Ce fichier contient tous les événements liés à l'authentification sur les ordinateurs Debian et Ubuntu. • Vous trouverez tout ce qui concerne le mécanisme d'autorisation de l'utilisateur dans ce fichier.
/var/log/secure	• Ce répertoire est utilisé par les ordinateurs RedHat et CentOS. • Il suit aussi les connexions sudo, les connexions SSH et différentes erreurs enregistrées par SSSD.
/var/log/boot.log	• Ce fichier contient les informations relatives à l'amorçage et les messages enregistrés au cours du processus de démarrage de l'ordinateur.
/var/log/dmesg	• Ce répertoire contient les messages du tampon de l'anneau du noyau. • Les informations liées aux périphériques matériels et à leurs pilotes y sont enregistrées. • Il est très important parce que, du fait que ces événements sont de très bas niveau, les systèmes d'enregistrement tels que syslog ne fonctionnent pas quand ils ont lieu et ils sont donc souvent inaccessibles à l'administrateur en temps réel.
/var/log/kern.log	• Ce fichier contient les informations consignées par le noyau
/var/log/cron	• Cron est un service utilisé pour planifier des tâches automatisées sous Linux et ce répertoire stocke ses événements. • Chaque fois qu'une tâche planifiée (également appelée un job cron) s'exécute, toutes ses informations pertinentes, y compris son état d'exécution et ses messages d'erreur sont stockés ici.
/var/log/mysqld.log ou /var/log/mysql.log	• Il s'agit du fichier journal MySQL. • Tous les messages de débogage, d'échec et de réussite, liées au processus mysqld et au démon (daemon) mysqld_safe sont enregistrés ici.

- La sortie de la commande affiche une partie du fichier journal **/var/log/messages** .
- Chaque ligne représente un événement consigné.
- Les horodatages au début des lignes indiquent le moment où l'événement a eu lieu.

```
[analyst@secOps ~]$ sudo cat /var/log/messages
Mar 20 15:28:45 secOps kernel: Linux version 4.15.10-1-ARCH (builduser@heftig-18961) (gcc version 7.3.1
20180312 (GCC)) #1 SMP PREEMPT Thu Mar 15 12:24:34 UTC 2018
Mar 20 15:28:45 secOps kernel: Command line: BOOT_IMAGE=/boot/vmlinuz-linux root=UUID=07c6b457-3f39-
4ddf-bfd8-c169e8a877b2 rw quiet
Mar 20 15:28:45 secOps kernel: KERNEL supported cpus:
Mar 20 15:28:45 secOps kernel:   Intel GenuineIntel
Mar 20 15:28:45 secOps kernel:   AMD AuthenticAMD
Mar 20 15:28:45 secOps kernel:   Centaur CentaurHauls
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x001: 'x87 floating point registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x002: 'SSE registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: Supporting XSAVE feature 0x004: 'AVX registers'
Mar 20 15:28:45 secOps kernel: x86/fpu: xstate_offset[2]:  576, xstate_sizes[2]:  256
Mar 20 15:28:45 secOps kernel: x86/fpu: Enabled xstate features 0x7, context size is 832 bytes, using
'standard' format.
Mar 20 15:28:45 secOps kernel: e820: BIOS-provided physical RAM map:
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x00000003ffefffff] usable
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000003fff0000-0x00000003fffffff] ACPI data
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fec00000-0x00000000fec00fff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fee00000-0x00000000fee00fff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Mar 20 15:28:45 secOps kernel: NX (Execute Disable) protection: active
Mar 20 15:28:45 secOps kernel: random: fast init done
Mar 20 15:28:45 secOps kernel: SMBIOS 2.5 present.
Mar 20 15:28:45 secOps kernel: DMI: innotek GmbH VirtualBox/VirtualBox, BIOS VirtualBox 12/01/2006
Mar 20 15:28:45 secOps kernel: Hypervisor detected: KVM
Mar 20 15:28:45 secOps kernel: e820: last_pfn = 0x3fff0 max_arch_pfn = 0x400000000
Mar 20 15:28:45 secOps kernel: MTRR: Disabled
Mar 20 15:28:45 secOps kernel: x86/PAT: MTRRs disabled, skipping PAT initialization too.
Mar 20 15:28:45 secOps kernel: CPU MTRRs all blank - virtualized system.
```

5.2.5. Travaux pratiques – Localiser les fichiers journaux

Au cours de ces travaux pratiques, vous allez vous familiariser avec la localisation et la manipulation de fichiers journaux Linux.