



Module 4: Présentation de Linux

CyberOps Associate v1.0



Objectifs du module

Titre du module: Présentation de Linux

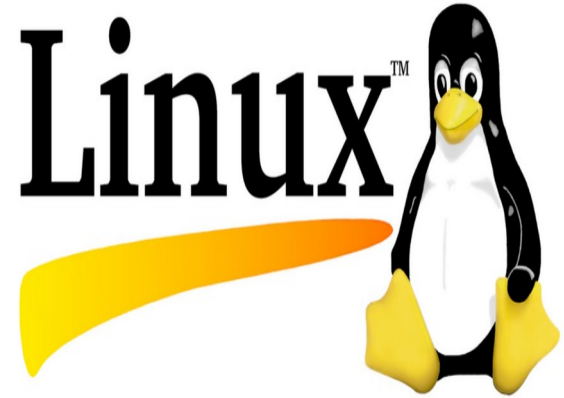
Objectif du module: Mettre en œuvre la sécurité Linux de base.

Titre du Rubrique	Objectif du Rubrique
Notions de base de Linux	Expliquer pourquoi les compétences Linux sont essentielles pour la surveillance de la sécurité du réseau et l'investigation.
Utilisation du Shell Linux	Utiliser le shell Linux pour manipuler des fichiers texte.
Serveurs et clients Linux	Expliquer le fonctionnement des réseaux client-serveur.
Administration de base du serveur	Expliquer comment un administrateur Linux localise et manipule les fichiers journaux de sécurité.
Le système de fichiers Linux	Gérer le système de fichiers Linux et les autorisations.
Utiliser l'interface graphique (GUI) Linux	Expliquer les composants de base de l'interface graphique Linux.
Utiliser un hôte Linux	Utiliser les outils pour détecter les malwares sur un hôte Linux.

4.1 Notions de base sur Linux

Qu'est-ce que Linux?

- Linux est un système d'exploitation créé en 1991
- Linux est Open Source, rapide, fiable et peu encombrant. Hautement personnalisable, son exécution nécessite très peu de ressources matérielles.
- Linux fait partie de plusieurs plates-formes et se rencontre sur toutes sortes d'appareils, des «bracelets-montres aux superordinateurs».
- Linux est conçu pour être connecté au réseau, ce qui rend bien plus simples l'écriture et l'utilisation d'applications basées sur le réseau.
- On parle de distribution Linux pour décrire les paquets créés par différentes organisations et inclure le noyau Linux avec des outils et des paquets logiciels personnalisés



La valeur de Linux

Linux est souvent le système d'exploitation de choix dans le centre de sécurité (SOC). Voici quelques-unes des raisons de choisir Linux :

- **Linux est Open Source** - Toute personne peut acquérir Linux sans frais et le modifier pour l'adapter à des besoins spécifiques.
- **L'interface de ligne de commande (CLI) de Linux est extrêmement puissante**- L'interface de ligne de commande (CLI) de Linux est extrêmement puissante et permet aux analystes d'effectuer leurs tâches non seulement directement sur un terminal, mais aussi à distance.
- **L'utilisateur contrôle mieux le système d'exploitation** : l'utilisateur administrateur sous Linux, appelé utilisateur root (racine) ou super utilisateur, a un pouvoir absolu sur l'ordinateur.
- **Elle permet un meilleur contrôle de la communication réseau** - le contrôle est un élément inhérent de Linux.

Présentation de Linux

Linux dans le SOC (Suite)

- La flexibilité qu'offre Linux est une excellente fonctionnalité pour la SOC. L'ensemble du système d'exploitation peut être adapté pour devenir une plate-forme d'analyse de sécurité parfaite.
- Sguil est la console d'analyste de cybersécurité dans une version spéciale de Linux appelée Security Onion.
- Security Onion est une suite open source d'outils qui fonctionnent ensemble pour l'analyse de la sécurité du réseau.

The screenshot displays the Sguil-0.9.0 interface, which is a security monitoring tool. The top window shows a list of real-time events with columns for ST, CNT, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. The bottom window shows a detailed view of a selected packet, including IP Resolution, Agent Status, Short Statistics, and System Mugs. The packet details section shows a TCP packet from 209.165.201.17 to 209.165.200.235 on port 80, with a message indicating a Trojan download attempt.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	7	seconion...	5.1583	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion...	5.1584	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion...	5.1599	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLoader ...
RT	1	seconion...	5.1600	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	7	seconion...	7.1896	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET INFO Dotted Quad Host HTA ...
RT	7	seconion...	7.1897	2020-05-10 21:29:13	209.165.201.17	52458	209.165.200.235	80	6	ET POLICY Possible HTA Applica...
RT	1	seconion...	7.1912	2020-05-10 21:29:13	209.165.201.17	52460	209.165.200.235	80	6	ET TROJAN Probable OneLoader ...
RT	1	seconion...	7.1913	2020-05-10 21:29:13	209.165.201.17	52468	209.165.200.235	80	6	ET WEB_SERVER Possible Cher...
RT	1	seconion...	5.1679	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash in U...
RT	1	seconion...	7.1992	2020-05-10 21:29:49	209.165.201.17	52836	209.165.200.235	80	6	ET WEB_SERVER /bin/bash in U...
RT	49	seconion...	7.1998	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh in URI...
RT	49	seconion...	5.1701	2020-05-10 21:29:52	209.165.201.17	52896	209.165.200.235	80	6	ET WEB_SERVER /bin/sh in URI...
RT	1	seconion...	5.1770	2020-05-10 21:41:13	209.165.201.17	38782	209.165.200.235	3306	6	ET SCAN Suspicious inbound to ...

Sid	Net	Hostname	Type	Last
1	seconion-os...	seconion-os...	ossec	2020-05-12
2	seconion-en...	seconion-en...	pcap	2020-05-12
3	seconion-en...	seconion-en...	snort	2020-05-10
4	seconion-en...	seconion-en...	pcap	2020-05-12
5	seconion-en...	seconion-en...	snort	2020-05-10
6	seconion-en...	seconion-en...	pcap	2020-05-12
7	seconion-en...	seconion-en...	snort	2020-05-10

Update Interval (secs): 15 NOW

IP Resolution Agent Status Short Statistics System Mugs

Alert: tcp \$HOME_NET any -> \$EXTERNAL_NET \$HTTP_PORTS (msg:"ET TROJAN Probable OneLoader downloader (Zeus P2P)"; flow:to_server,established; content:"GET"; http_method:)

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Flags	Offset	TTL	ChkSum
TCP	209.165.201.17	209.165.200.235	4	5	0	172	50175	2	0	63	16900

U A P R S F
P o r t 1 0 G K H T N N Seq# Ack# Offset Res Window Upd ChkSum

DATA	Source	Dest	RRR	CSS	Y I	Seq#	Ack#	Offset	Res	Window	Upd	ChkSum
47 45 54 20 2F 31 31 20 48 54 54 50 2F 31 2E 31	00 0A 48 6F 73 74 3A 20 32 30 39 2E 31 36 35 2E	32 30 30 2E 32 33 35 00 0A 55 73 65 72 20 41 67	65 6E 74 3A 20 40 6F 7A 69 6C 6C 61 2F 34 2E 30	20 28 63 6F 70 61 74 69 62 6C 65 38 20 40 53	2237277941	1593194311	8	0	501	0	30678	

GET /11 HTTP/1.1
Host: 209.165.200.235
User-Agent: Mozilla/4.0 (compatible; MS

Search Packet Payload Hex Text NoCase

Linux dans le SOC (Suite)

Le tableau répertorie quelques outils que l'on trouve souvent dans un SOC.

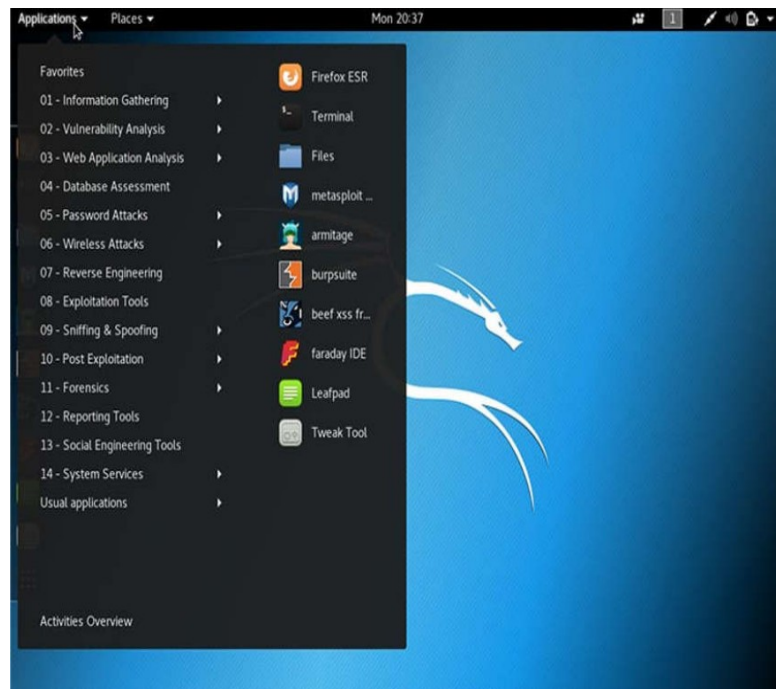
Outil SOC	Description
Logiciel de capture de paquets	<ul style="list-style-type: none">• Un outil essentiel pour un analyste SOC car il permet d'observer et de comprendre tous les détails d'une transaction réseau.• Wireshark est un outil populaire de capture de paquets.
Outil d'analyse des logiciels malveillants (Malware)	<ul style="list-style-type: none">• Ces outils permettent aux analystes d'exécuter en toute sécurité et d'observer l'exécution de logiciels malveillants sans risquer de compromettre le système sous-jacent.
Systèmes de détection des intrusions (IDS)	<ul style="list-style-type: none">• Ces outils sont utilisés pour l'inspection et la surveillance du trafic en temps réel.• Si n'importe quel aspect du trafic circulant actuellement correspond à l'une des règles établies, une action prédéfinie est entreprise.

Linux dans le SOC (Suite)

Outil SOC	Description
Pare-feu	<ul style="list-style-type: none">Ce logiciel est utilisé pour spécifier, à partir de règles prédéfinies, si le trafic est autorisé à entrer dans le réseau ou à le quitter.
Gestionnaires de journaux	<ul style="list-style-type: none">Les fichiers journaux sont utilisés pour enregistrer des événements.Comme un grand réseau peut générer un très grand nombre d'entrées de journal des événements, des gestionnaires de journaux sont employés pour faciliter la surveillance des journaux.
Gestion des informations et des événements liés à la sécurité (SIEM)	<ul style="list-style-type: none">SIEM fournit une analyse en temps réel des alertes et des entrées de journal générées par les appareils de réseau comme les IDS et les pare-feu.
Système de gestion des incidents	<ul style="list-style-type: none">L'affectation de tickets, leur modification et leur enregistrement sont effectués à travers un système de gestion de tickets. Les alertes de sécurité sont souvent attribuées aux analystes par le biais d'un système de billetterie.

Linux Outils Linux

- En plus des outils spécifiques à la SOC, les ordinateurs Linux utilisés dans la SOC contiennent souvent des outils de test de pénétration.
- Également connu sous le nom PenTesting, un test de pénétration est le processus consistant à rechercher des vulnérabilités dans un réseau ou un ordinateur en l'attaquant.
- Des générateurs de paquets, des scanners de ports et des exploits de validation sont des exemples d'outils de PenTesting.
- Kali Linux est une distribution Linux regroupe de nombreux outils de pénétration dans une seule distribution Linux.
- Notez la présence de toutes les grandes catégories d'outils de test de pénétration.



4.2 Utilisation du shell Linux

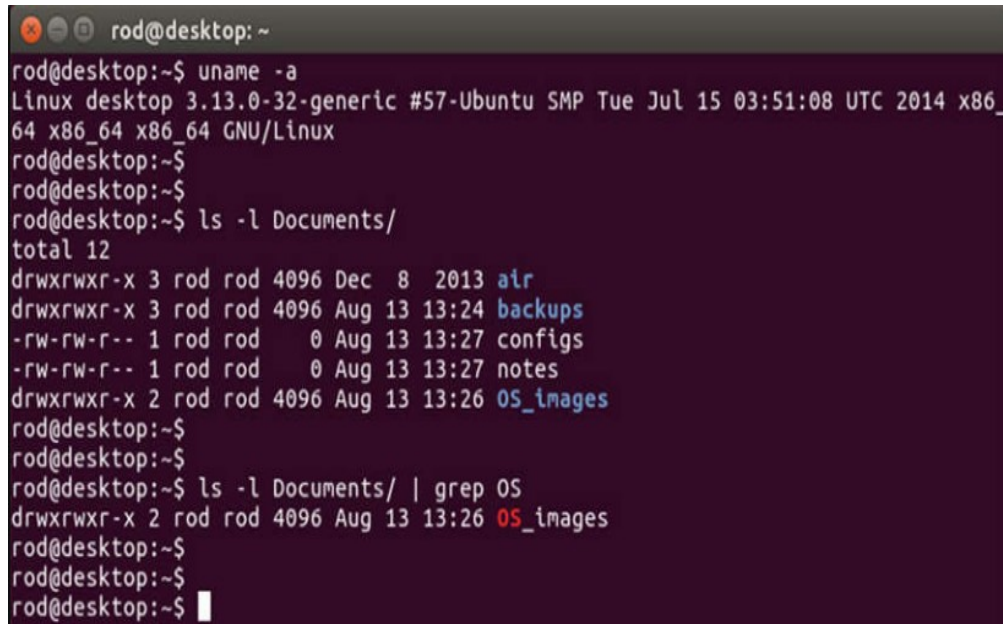
Le shell Linux

- Sous Linux, l'utilisateur communique avec le système d'exploitation à l'aide de l'interface CLI ou de l'interface graphique.
- Linux démarre souvent dans l'interface graphique par défaut. Cela masque l'interface de ligne de commande de l'utilisateur.
- L'accès à la CLI à partir de l'interface graphique peut s'effectuer via une application d'émulation de terminal. Ce type d'application permet à l'utilisateur d'accéder à la CLI. Son nom est souvent une variante du mot «terminal».
- Dans Linux, Terminator, etterm, xterm, konsole, et gnome-terminal sont des émulateurs de terminaux répandus.
- Fabrice Bellard a créé JSLinux qui permet à une version émulée de Linux de fonctionner dans un navigateur.

Remarque : *les termes shell, console, fenêtre de console, terminal CLI et fenêtre de terminal sont souvent utilisés de manière interchangeable.*

Le shell Linux (Suite)

La figure montre gnome-terminal, un émulateur de terminal Linux répandu.



```
rod@desktop: ~  
rod@desktop:~$ uname -a  
Linux desktop 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$ ls -l Documents/  
total 12  
drwxrwxr-x 3 rod rod 4096 Dec  8 2013 air  
drwxrwxr-x 3 rod rod 4096 Aug 13 13:24 backups  
-rw-rw-r-- 1 rod rod   0 Aug 13 13:27 configs  
-rw-rw-r-- 1 rod rod   0 Aug 13 13:27 notes  
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$ ls -l Documents/ | grep OS  
drwxrwxr-x 2 rod rod 4096 Aug 13 13:26 OS_images  
rod@desktop:~$  
rod@desktop:~$  
rod@desktop:~$
```

Commandes de base

- Les commandes Linux sont des programmes créés pour exécuter une tâche spécifique.
- Du fait que les commandes sont des programmes stockés sur le disque, lorsque l'utilisateur saisit une commande, le shell doit la trouver sur le disque avant de pouvoir l'exécuter.
- Le tableau répertorie une liste de commandes Linux de base et leurs fonctions.

Commande	Description
mv	Déplace les fichiers ou les répertoires.
chmod	Modifie les autorisations du fichier
chown	Change le propriétaire d'un fichier
dd	Copie les données de l'entrée vers le résultat.
pwd	Affiche le nom du répertoire actif
ps	Affiche les processus en cours sur le système.
su	Simule une session avec un autre utilisateur ou permet de devenir un super-utilisateur.

Utilisation du Shell Linux

Commandes de base

Commande	Description
sudo	Exécute une commande en tant que super-utilisateur, par défaut, ou un autre utilisateur nommé.
grep	Permet de rechercher les chaînes ou les caractères spécifiés dans un fichier ou dans la sortie d'autres commandes.
ifconfig	Permet d'afficher ou de configurer les informations concernant la carte réseau.
apt-get	Utilisée pour installer, configurer et supprimer des paquets sur Debian et ses dérivés.
iwconfig	Permet d'afficher ou de configurer les informations concernant la carte réseau sans fil.
shutdown	Arrête le système. Vous pouvez demander à shutdown d'effectuer un certain nombre de tâches associées à l'arrêt, notamment le redémarrage, la suspension, la mise en veille ou le rejet de tous les utilisateurs connectés.
passwd	Permet de modifier le mot de passe.
cat	Permet de répertorier le contenu d'un fichier ; attend comme paramètre le nom du fichier en question.
man	Permet d'afficher la documentation d'une commande spécifique.

Commandes de fichiers et de répertoires

De nombreux outils de ligne de commande sont inclus par défaut dans Linux. Le tableau répertorie quelques-unes des commandes les plus courantes liées aux fichiers et aux répertoires.

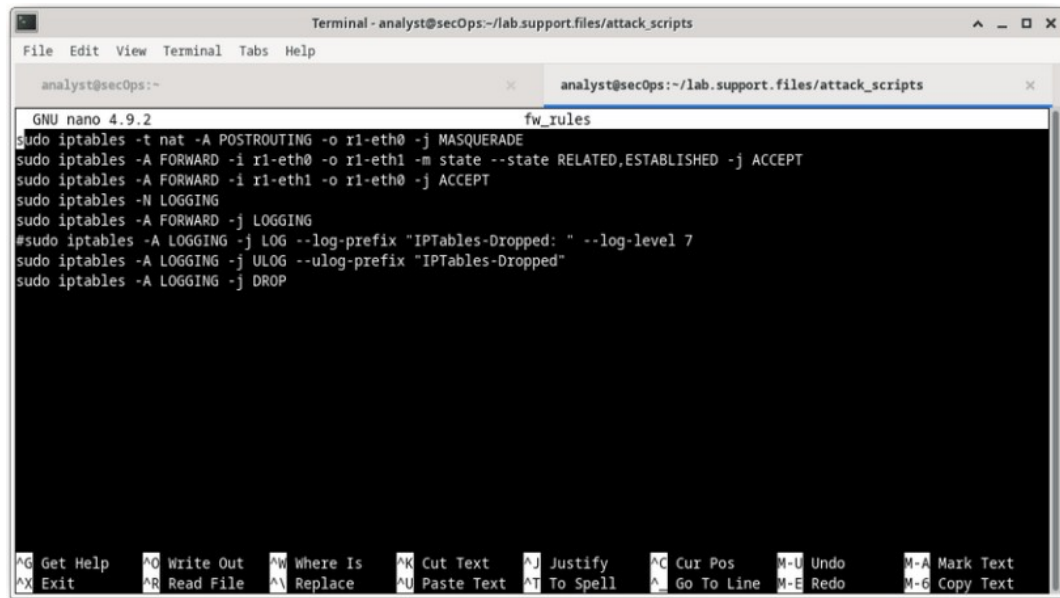
Commande	Description
ls	Affiche les fichiers d'un répertoire.
cd	Change de répertoire actif.
mkdir	Crée un répertoire dans le répertoire actif.
cp	Copie les fichiers de la source vers la destination.
mv	Déplace le fichier dans un autre dossier.
rm	Supprime les fichiers.
grep	Recherche les chaînes ou les caractères spécifiés dans un fichier ou dans le résultat d'autres commandes
cat	Répertorie le contenu d'un fichier et attend le nom de fichier en tant que paramètre.

Travaux pratiques – Utiliser des fichiers texte dans l'interface de ligne de commande (CLI)

- Linux dispose de nombreux éditeurs de texte différents, offrant diverses caractéristiques et fonctions.
- Certains éditeurs de texte incluent une interface graphique, tandis que d'autres sont seulement des outils de ligne de commande. Chaque éditeur possède un ensemble de fonctionnalités conçues pour prendre en charge un type de tâche spécifique.
- Certains éditeurs de texte visent les programmeurs et intègrent des fonctionnalités telles que la mise en évidence de syntaxe, le contrôle des accolades et les parenthèses, les vérifications et d'autres fonctionnalités axées sur la programmation.
- Si les éditeurs de texte graphiques sont pratiques et simples d'emploi, ceux basés sur la ligne de commande sont très importants pour les utilisateurs de Linux. Le principal avantage des éditeurs de texte basés sur la ligne de commande est qu'ils permettent l'édition de texte à partir d'un ordinateur distant.

Travaux pratiques – Utiliser des fichiers texte dans l'interface de ligne de commande (CLI)

- La figure montre **nano**, un éditeur de texte à ligne de commande répandu.
- L'administrateur modifie les règles de pare-feu. Les éditeurs de texte sont souvent utilisés pour la configuration du système et la maintenance sous Linux.
- Du fait de l'absence de prise en charge graphique, nano (ou GNU nano) ne peut être contrôlé qu'avec le clavier.



```
Terminal - analyst@secOps:~/lab.support.files/attack_scripts
File Edit View Terminal Tabs Help
analyst@secOps:~
analyst@secOps:~/lab.support.files/attack_scripts
GNU nano 4.9.2 fw_rules
sudo iptables -t nat -A POSTROUTING -o r1-eth0 -j MASQUERADE
sudo iptables -A FORWARD -i r1-eth0 -o r1-eth1 -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -A FORWARD -i r1-eth1 -o r1-eth0 -j ACCEPT
sudo iptables -N LOGGING
sudo iptables -A FORWARD -j LOGGING
#sudo iptables -A LOGGING -j LOG --log-prefix "IPTables-Dropped: " --log-level 7
sudo iptables -A LOGGING -j ULOG --ulog-prefix "IPTables-Dropped"
sudo iptables -A LOGGING -j DROP
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos ^U Undo ^A Mark Text
^X Exit ^R Read File ^N Replace ^U Paste Text ^T To Spell ^_ Go To Line ^E Redo ^G Copy Text
```

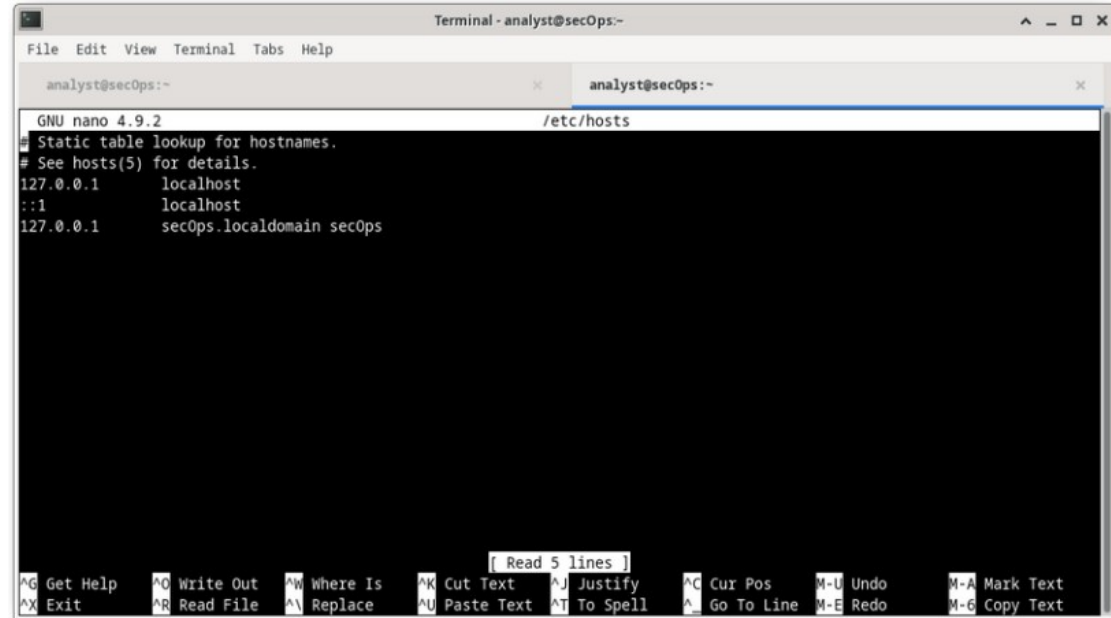
L'importance des fichiers texte dans Linux

- Sous Linux, tous les éléments sont traités comme des fichiers. Cela inclut la mémoire, les disques, le moniteur et les répertoires.
- Appelés fichiers de configuration, ce sont généralement des fichiers texte utilisés pour stocker les réglages et les paramètres pour des applications ou des services spécifiques.
- Les utilisateurs disposant des niveaux d'autorisation appropriés peuvent utiliser des éditeurs de texte pour modifier le contenu des fichiers de configuration.
- Une fois que les modifications ont été apportées, le fichier est enregistré et peut être utilisé par le service ou l'application correspondant. Les utilisateurs sont en mesure de spécifier exactement comment ils veulent qu'une application ou un service donné se comporte. Lors de leur lancement, les services et les applications vérifient le contenu de fichiers de configuration spécifiques pour ajuster leur comportement.

Remarque : *l'administrateur a utilisé la commande **sudo nano /etc/hosts** pour ouvrir le fichier. La commande **sudo** (raccourci pour « superuser do ») appelle le privilège du superutilisateur d'utiliser l'éditeur de texte nano pour ouvrir le fichier hosts.*

L'importance des fichiers texte dans Linux

- Dans la figure, l'administrateur a ouvert le fichier de configuration hosts dans **nano** pour le modifier.
- Le fichier hôte contient des mappages statiques d'adresses IP d'hôte et de noms.
- Les noms servent de raccourcis qui permettent de se connecter à d'autres périphériques en utilisant un nom au lieu d'une adresse IP. Seul le superutilisateur peut changer le fichier hosts.



```
Terminal - analyst@secOps:~
File Edit View Terminal Tabs Help
analyst@secOps:~
analyst@secOps:~
GNU nano 4.9.2 /etc/hosts
# Static table lookup for hostnames.
# See hosts(5) for details.
127.0.0.1    localhost
::1         localhost
127.0.0.1    secOps.localdomain secOps

[ Read 5 lines ]
^G Get Help  ^O Write Out ^W Where Is  ^K Cut Text   ^J Justify   ^C Cur Pos   M-U Undo     M-A Mark Text
^X Exit      ^R Read File ^\ Replace   ^U Paste Text ^T To Spell  ^_ Go To Line M-E Redo     M-6 Copy Text
```

Travaux pratiques – Utiliser des fichiers texte dans l'interface de ligne de commande (CLI)

Au cours de ces travaux pratiques, vous vous familiariserez avec les éditeurs de texte à ligne de commande Linux et les fichiers de configuration.

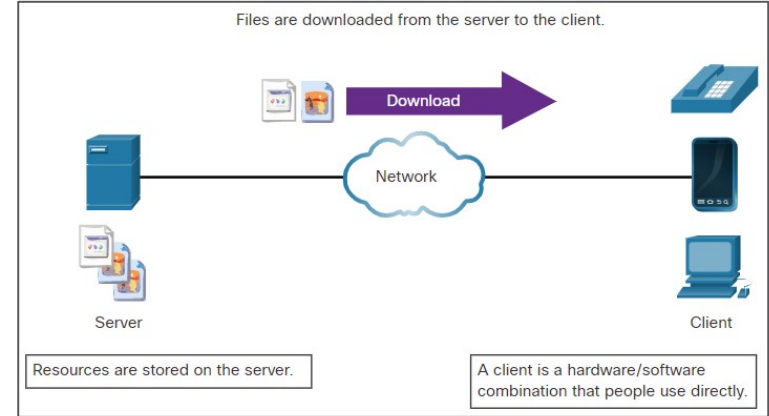
Travaux pratiques – Se familiariser avec le shell Linux

Au cours de ces travaux pratiques, vous utiliserez la ligne de commande Linux pour gérer les fichiers et les répertoires, et pour effectuer quelques tâches d'administration de base.

4.3 Serveurs et clients Linux

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.



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».

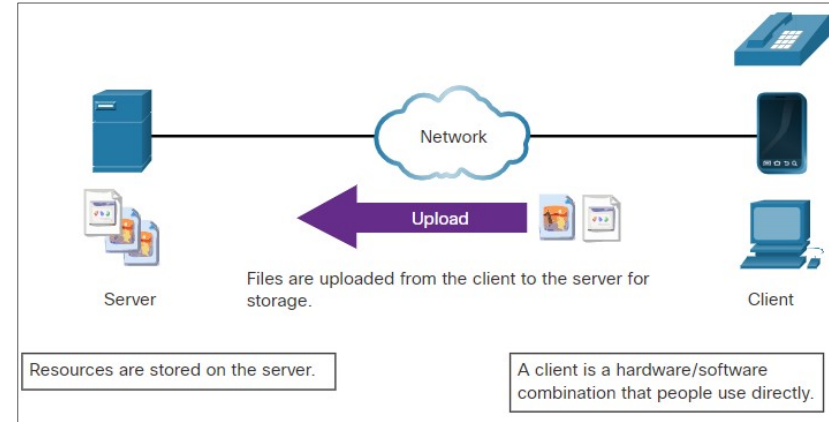
Port	Description
20/21	FTP (File Transfer Protocol)
22	SSH (Secure Shell)
23	Service de connexion à distance Telnet
25	Protocole SMTP
53	Système DNS (Domain Name System)
67/68	Protocole DHCP (Dynamic Host Configuration Protocol)

Serveurs, services et ports

Port	Description
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)

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.



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.

4.4 Administration de base du serveur

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;
```

Fichiers de configuration de service (Suite)

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 ~]$
```

Fichiers de configuration de service (Suite)

- 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
```

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.

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

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.

Surveillance des journaux de service (Suite)

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

Fichier journal Linux	Description
/var/log/messages	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Ce fichier contient les informations relatives à l'amorçage et les messages enregistrés au cours du processus de démarrage de l'ordinateur.

Surveillance des journaux de service (Suite)

Fichier journal Linux	Description
/var/log/dmesg	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• Ce fichier contient les informations consignées par le noyau
/var/log/cron	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none">• 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.

Surveillance des journaux de service (Suite)

- 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 0x00000000000a0000-0x00000000000fffff] reserved
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000003fffff] usable
Mar 20 15:28:45 secOps kernel: BIOS-e820: [mem 0x00000000003fff0000-0x00000000003fffff] 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 0x00000000ffff0000-0x00000000ffffffff] 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 = 0x3ffff0 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.
```

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.

4.5 Le système de fichiers Linux

Les types de systèmes de fichiers sous Linux

- Il y a beaucoup de types de systèmes de fichiers différents, qui varient par leurs propriétés de vitesse, de souplesse, de sécurité, de taille, de structure, de logique et plus encore.
- L'administrateur décide du type de système de fichiers qui convient au système d'exploitation.
- Le tableau répertorie quelques types de systèmes de fichiers couramment disponibles et pris

Le système de fichiers Linux	Description
ext2 (deuxième système de fichiers étendu)	<ul style="list-style-type: none">• ext2 était le système de fichier par défaut de plusieurs grandes distributions de Linux jusqu'à ce qu'il soit supplanté par ext3.• ext2 est toujours le système de fichiers de choix pour les supports de stockage Flash parce que son absence de journal augmente les performances et réduit au minimum le nombre d'écritures.• Du fait que les dispositifs de mémoire Flash disposent d'un nombre limité d'opérations d'écriture, la réduction au minimum des opérations d'écriture augmente leur durée de vie.

Les types de systèmes de fichiers sous Linux (Suite)

Le système de fichiers Linux	Description
ext3 (troisième système de fichiers étendu)	<ul style="list-style-type: none">• ext3 est un système de fichiers journalisé visant à améliorer le système de fichiers ext2 existant.• Le journal, la principale fonctionnalité ajoutée à ext3, est une technique utilisée pour minimiser le risque de corruption des fichiers système en cas de panne d'alimentation soudaine.• Le système de fichiers conserve un journal de toutes les modifications imminentes apportées au système de fichiers.• Si l'ordinateur tombe en panne avant que la modification ne soit terminée, le journal peut servir à restaurer ou à corriger les problèmes éventuels créés par la panne.• La taille maximale des fichiers dans les systèmes de fichiers ext3 est de 32 To.
ext4 (quatrième système de fichiers étendu)	<ul style="list-style-type: none">• Conçu comme un successeur d'ext3, ext4 a été créé à partir d'une série d'extensions d'ext3.• Alors que les extensions amélioraient les performances d'ext3 et augmentaient la taille des fichiers pris en charge, les développeurs du noyau Linux étaient préoccupés par les problèmes de stabilité et s'opposaient au fait d'ajouter les extensions à ext3, qui était stable.• Le projet d'ext3 a été divisé en deux ; une partie a été conservée comme ext3 et a suivi son développement normal et l'autre, nommée ext4, a incorporé les extensions mentionnées.

Les types de systèmes de fichiers sous Linux (Suite)

Le système de fichiers Linux	Description
NFS (Network File System)	<ul style="list-style-type: none">• NFS est un système de fichiers basé sur le réseau, qui permet l'accès aux fichiers via ce dernier.• De point de vue de l'utilisateur, il n'y a pas de différence entre l'accès à un fichier stocké localement ou sur un autre ordinateur du réseau.• La norme NFS est une norme ouverte qui permet à quiconque de la mettre en œuvre.
CDFS (Compact Disc File System)	<ul style="list-style-type: none">• CDFS a été créé spécifiquement pour les supports à disques optiques.
Système de fichiers d'échange	<ul style="list-style-type: none">• Le système de fichiers d'échange est utilisé par Linux quand il est à court de RAM.• Lorsque cela se produit, le noyau déplace le contenu inactif de la RAM sur la partition d'échange sur le disque.• Si les partitions d'échange (également connues sous le nom d'espace d'échange) peuvent être utiles pour les ordinateurs Linux avec une quantité limitée de mémoire, elles ne sauraient être considérées comme solution principale.• La partition d'échange est stockée sur un disque dont la vitesse d'accès est bien plus lente que la RAM.

Les types de systèmes de fichiers sous Linux (Suite)

Le système de fichiers Linux	Description
HFS Plus ou HFS+ (Hierarchical File System Plus)	<ul style="list-style-type: none">• Un système de fichiers utilisé par Apple dans ses ordinateurs Macintosh les plus récents.• Le noyau Linux comprend un module de montage de HFS+ pour les opérations de lecture/écriture.
APFS (Apple File System)	<ul style="list-style-type: none">• Système de fichiers mis à jour utilisé par les appareils Apple.• Il fournit un chiffrement renforcé et optimisé pour les lecteurs flash et les disques SSD.
enregistrement d'amorçage maître (MBR, Master Boot Record)	<ul style="list-style-type: none">• Situé dans le premier secteur d'un ordinateur partitionné, le MBR stocke toutes les informations sur la façon dont est organisé le système de fichiers.• Le MBR donne rapidement la main à une fonction de chargement qui charge le système d'exploitation.

Les types de systèmes de fichiers sous Linux (Suite)

- Le montage désigne le processus d'attribution d'un répertoire à une partition.
- Après une opération de montage réussie, le système de fichiers figurant sur la partition est accessible via le répertoire spécifié.
- La figure illustre la sortie de la commande **mount** émise dans la machine virtuelle CyberOPS de Cisco.

```
[analyst@secops ~]$ mount
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sys on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
dev on /dev type devtmpfs (rw,nosuid,relatime,size=494944k,nr_inodes=123736,mode=755)
run on /run type tmpfs (rw,nosuid,nodev,relatime,mode=755)
/dev/sda1 on / type ext4 (rw,relatime)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /sys/fs/cgroup type tmpfs (ro,nosuid,nodev,noexec,mode=755)
cgroup2 on /sys/fs/cgroup/unified type cgroup2 (rw,nosuid,nodev,noexec,relatime,nsdelegate)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
none on /sys/fs/bpf type bpf (rw,nosuid,nodev,noexec,relatime,mode=700)
cgroup on /sys/fs/cgroup/rdma type cgroup (rw,nosuid,nodev,noexec,relatime,rdma)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpu,cpuacct)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/pids type cgroup (rw,nosuid,nodev,noexec,relatime,pids)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/net_cls,net_prio type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls,net_prio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
systemd-1 on /proc/sys/fs/binfmt_misc type autofs
(rw,relatime,fd=29,pgrp=1,timeout=0,minproto=5,maxproto=5,direct,pipe_ino=11792)
debugfs on /sys/kernel/debug type debugfs (rw,nosuid,nodev,noexec,relatime)
tracefs on /sys/kernel/tracing type tracefs (rw,nosuid,nodev,noexec,relatime)
hugetlbfs on /dev/hugepages type hugetlbfs (rw,relatime,pagesize=2M)
mqueue on /dev/mqueue type mqueue (rw,nosuid,nodev,noexec,relatime)
tmpfs on /tmp type tmpfs (rw,nosuid,nodev)
```

Rôles Linux et autorisations sur les fichiers

- Pour organiser le système et renforcer les frontières dans l'ordinateur, Linux utilise des autorisations de fichiers.
- Chaque fichier dans Linux porte ses autorisations de fichier, qui définissent les actions que le propriétaire, le groupe et les autres utilisateurs peuvent effectuer sur celui-ci.
- Les autorisations possibles sont Lecture, Écriture et Exécution.
- La commande `ls` avec le paramètre `-l` fournit des informations supplémentaires sur le fichier.

Rôles Linux et autorisations sur les fichiers (Suite)

La sortie fournit beaucoup d'informations sur le fichier **space.txt** :

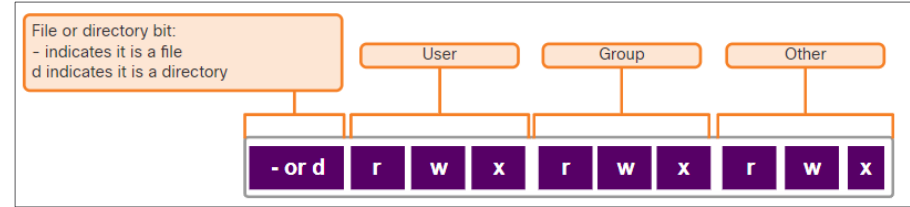
- Le premier champ de la sortie affiche les autorisations associées à **space.txt** (-rwxrw-r--).
- Le deuxième champ définit le nombre de liens matériels vers le fichier (le nombre **1** après les autorisations).
- Les troisième et quatrième champs affichent l'utilisateur (**analyst**) et le groupe (**staff**) qui possèdent respectivement le fichier.
- Le cinquième champ affiche la taille du fichier en octets. **space.txt** comporte 253 octets.
- Le sixième champ affiche la date et l'heure de la dernière modification.
- Le septième champ affiche le nom du fichier.

```
[analyst@secOps ~]$ ls -l space.txt
-rwxrw-r-- 1 analyst staff 253 May 20 12:49 space.txt
(1)(2)(3)(4)(5)(6)(7)
[analyst@secOps ~]$
```

Rôles Linux et autorisations sur les fichiers (Suite)

La figure présente en détail les autorisations de fichiers dans Linux. Le fichier **space.txt** de la Figure 1 présente les autorisations suivantes :

- Le tiret (-) signifie qu'il s'agit d'un fichier.
- Le premier jeu de caractères concerne les autorisations de l'utilisateur (**rw**x). L'utilisateur, **analyst**, qui possède le fichier peut lire (**R**ead), écrire (**W**rite) et exécuter (**eX**ecute) le fichier.
- Le deuxième jeu de caractères concerne les autorisations du groupe (**rw**-). Le groupe, **staff**, qui possède le fichier peut lire (**R**ead) et écrire (**W**rite) dans le fichier.
- - Le **troisième jeu de caractères** concerne les autorisations **de tout** autre utilisateur ou groupe (**r**--).



Rôles Linux et autorisations sur les fichiers (Suite)

- Utiliser des valeurs octales pour définir les autorisations
- Les autorisations de fichier sont un élément fondamental de Linux et ne peuvent pas être enfreintes.
- Le seul utilisateur qui peut contourner les autorisations de fichiers sur un ordinateur Linux est l'utilisateur racine.

Binaire	Octal	Permission	Description
000	0	---	Pas d'accès
001	1	--x	Exécution uniquement
010	2	-w-	Écriture seule
011	3	-wx	Écriture et exécution
100	4	r--	Lecture seule
101	5	r-x	Lecture et exécution
110	6	rw-	Lire et écrire
111	7	rwX	Lecture, écriture et exécution

Liens matériels et liens symboliques

- Un lien matériel est un autre fichier qui pointe vers le même emplacement que le fichier d'origine.
- Utilisez la commande **ln** pour créer un lien matériel.
- Le premier argument est le fichier existant et le second argument le nouveau fichier.
- Le fichier **space.txt** est lié à **space.hard.txt** dans la Figure 1 et le champ de lien affiche maintenant 2.
- Les deux fichiers pointent vers le même emplacement dans le système de fichiers. Si vous modifiez un fichier, l'autre est également modifié.
- La commande **echo** est utilisée pour ajouter du texte à **space.txt**.

```
[analyst@secOps ~]$ ln space.txt space.hard.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l space*
-rw-r--r-- 2 analyst analyst 239 May  7 18:18 space.hard.txt
-rw-r--r-- 2 analyst analyst 239 May  7 18:18 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ echo "Testing hard link" >> space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l space*
-rw-r--r-- 2 analyst analyst 257 May  7 18:19 space.hard.txt
-rw-r--r-- 2 analyst analyst 257 May  7 18:19 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ rm space.hard.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more space.txt
Space... The final frontier...
These are the voyages of the Starship Enterprise. Its continuing mission:
- To explore strange new worlds...
- To seek out new life; new civilizations...
- To boldly go where no one has gone before!
Testing hard link
[analyst@secOps ~]$
```

Liens matériels et liens symboliques (Suite)

- Un lien symbolique, également appelé symlink ou lien logique, est semblable à un lien matériel dans la mesure où modifier le lien symbolique change également le fichier d'origine.
- Comme illustré à la Figure 2, utilisez l'option **-s** de la commande **ln** pour **créer un lien symbolique**.
- Notez que l'ajout d'une ligne de texte à **test.txt** ajoute également cette ligne à **mytest.txt**.

```
[analyst@secOps ~]$ echo "Hello World!" > test.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ln -s test.txt mytest.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ echo "It's a lovely day!" >> mytest.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more test.txt
Hello World!
It's a lovely day!
[analyst@secOps ~]$
[analyst@secOps ~]$ rm test.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ more mytest.txt
more: stat of mytest.txt failed: No such file or directory
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l mytest.txt
lrwxrwxrwx 1 analyst analyst 8 May  7 20:17 mytest.txt -> test.txt
[analyst@secOps ~]$
```

Liens matériels et liens symboliques (Suite)

Le tableau suivant présente plusieurs avantages des liens symboliques par rapport aux liens durs :

lien matériel	Liens souples
Il est plus difficile de localiser les liens matériels.	Pour connaître l'emplacement du fichier d'origine d'un lien symbolique, utilisez la commande ls-l .
Les liens matériels sont limités au système de fichiers dans lequel ils sont créés.	Les liens symboliques peuvent établir un lien vers un fichier situé dans un autre système de fichiers.
Les liens matériels ne peuvent pas être liés à un répertoire parce que le système lui-même utilise des liens matériels pour définir la hiérarchie de la structure de répertoires.	Les liens symboliques peuvent être liés à des répertoires.

Travaux pratiques – Parcourir le système de fichiers Linux et les paramètres d'autorisation

Au cours de ces travaux pratiques, vous allez vous familiariser avec les systèmes de fichiers Linux.

4.6 Utiliser l'interface graphique Linux

Système X Windows

- L'interface graphique présente dans la plupart des ordinateurs Linux repose sur le système X Window.
- Également connu sous le nom de X ou X11, X Window est un système de fenêtrage, conçu pour fournir le cadre de base pour une interface graphique.
- X Window comprend des fonctions permettant de dessiner et de déplacer des fenêtres sur le périphérique d'affichage et d'interagir avec une souris et un clavier.
- X Window fonctionne comme un serveur et, de ce fait, permet à un utilisateur distant d'utiliser le réseau pour se connecter, de lancer une application graphique et de disposer de la fenêtre graphique ouverte sur le terminal distant.
- Notez que X ne précise pas l'interface utilisateur, laissant à d'autres programmes tels que les gestionnaires de fenêtres le soin de définir tous les composants graphiques.

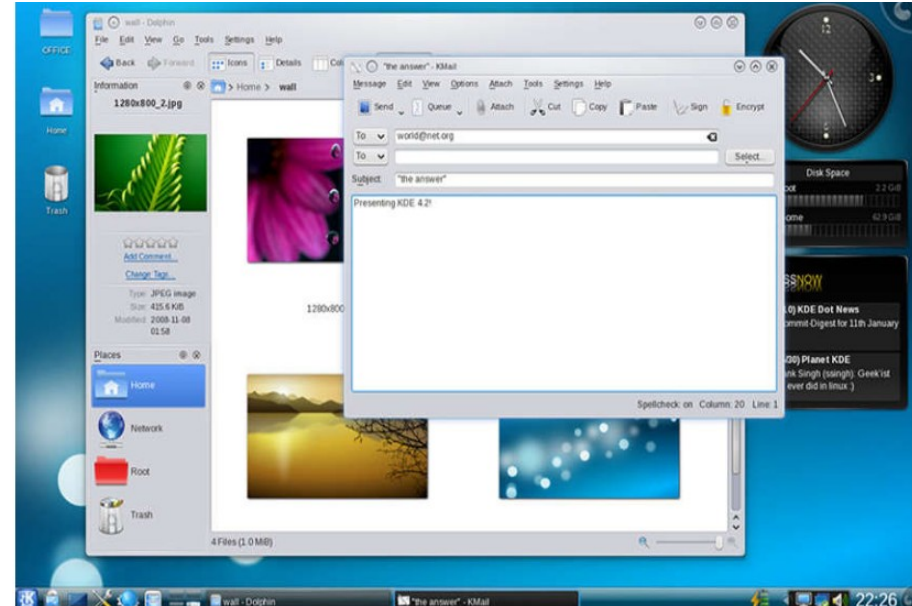
Utiliser l'interface graphique (GUI) Linux

Système X Windows

Des exemples de gestionnaires de fenêtres sont Gnome et KDE.



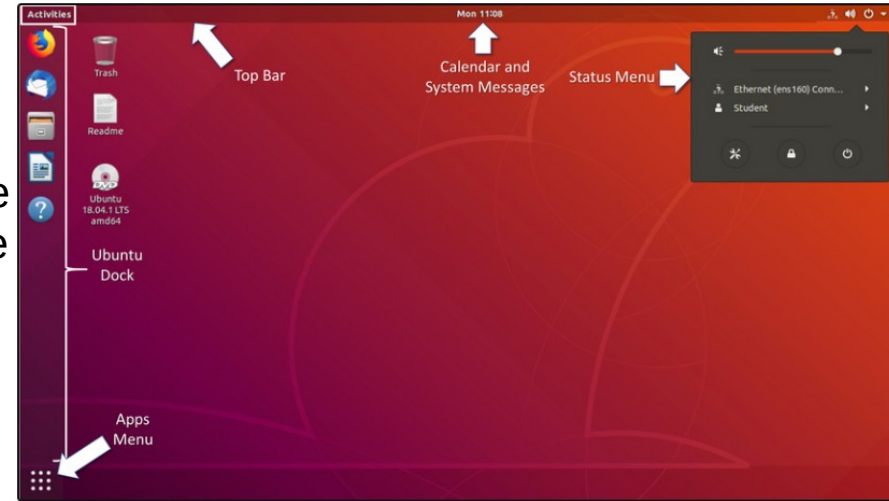
Le gestionnaire de fenêtres Gnome.



Le gestionnaire de fenêtres KDE.

Interface graphique utilisateur Linux

- Bien qu'un système d'exploitation n'ait pas besoin d'une interface graphique pour fonctionner, les interfaces graphiques sont considérées comme plus conviviales que l'interface à ligne de commande (CLI). L'interface graphique de Linux dans son ensemble peut être facilement remplacée par l'utilisateur.
- Ubuntu est une distribution Linux très populaire et conviviale.
- Ubuntu Linux utilise Gnome 3 comme interface par défaut.
- La figure montre l'emplacement de certaines des fonctionnalités du bureau Ubuntu Gnome 3.



Interface graphique utilisateur Linux (Suite)

Le tableau suivant répertorie les principaux composants de l'interface utilisateur de Unity :

Composant UI	Description
Menu d'Applications	<ul style="list-style-type: none">• Le menu Applications affiche les icônes des applications installées sur le système.• Un menu contextuel fournit des raccourcis permettant de démarrer ou de configurer les applications.• La zone de recherche système est disponible à partir de la vue Activités.
Station d'accueil Ubuntu	<ul style="list-style-type: none">• Il s'agit d'un dock sur le côté gauche de l'écran qui sert à lancer des applications et à basculer entre elles.• Cliquez pour lancer une application et lorsque l'application s'exécute, cliquez à nouveau pour basculer entre les applications en cours d'exécution.• Si plusieurs instances d'une application sont en cours d'exécution, le lanceur en affichera toutes les instances.• Cliquez avec le bouton droit sur une application du lanceur pour afficher les détails de cette application.
Barre supérieure	<ul style="list-style-type: none">• Cette barre de menus contient un menu pour l'application qui a actuellement le focus.• Il affiche l'heure actuelle et indique s'il y a de nouveaux messages système.• Il permet également d'accéder à la vue du bureau d'activité et au menu d'état du système.

Interface graphique utilisateur Linux (Suite)

Composant UI	Description
Calendrier et barre de messages système	<ul style="list-style-type: none">• Cliquez sur le jour et l'heure pour afficher le calendrier complet des rendez-vous et tous les messages système actuels.• Accédez au calendrier des rendez-vous à partir d'ici pour créer de nouveaux rendez-vous.
Activités	<ul style="list-style-type: none">• Passez à la vue des applications pour basculer vers ou fermer les applications en cours d'exécution.• Un puissant outil de recherche est disponible ici pour trouver des applications, des fichiers et des valeurs dans les fichiers.• Permet de basculer entre les espaces de travail.
Menu d'état	<ul style="list-style-type: none">• Permet la configuration de la carte réseau et d'autres périphériques en cours d'exécution.• L'utilisateur actuel peut se déconnecter ou modifier ses paramètres.• Vous pouvez apporter des modifications à la configuration du système ici.• Le poste de travail peut être verrouillé ou arrêté à partir d'ici.

4.7 Utiliser un hôte Linux

Installation et exécution d'applications sur un hôte Linux

- De nombreuses applications de l'utilisateur final sont des programmes complexes écrits dans des langages compilés.
- Pour faciliter le processus d'installation, Linux comprend souvent des programmes appelés gestionnaires de paquets.
- Lorsque vous utilisez un gestionnaire de paquets pour installer un paquet, tous les fichiers nécessaires sont placés à l'emplacement correct dans le système de fichiers.
- Un paquet est le terme utilisé pour désigner un programme et tous ses fichiers de prise en charge.
- La sortie de la commande montre la sortie de quelques commandes **apt-get** utilisées dans les distributions Debian.

```
analyst@cuckoo:~$ sudo apt-get update
[sudo] password for analyst:
Hit:1 http://us.archive.ubuntu.com/ubuntu xenial InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu xenial-updates InRelease [102 kB]
Get:3 http://security.ubuntu.com/ubuntu xenial-security InRelease [102 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu xenial-backports InRelease [102 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu xenial-updates/main amd64 Packages [534 kB]
<output omitted>
Fetched 4,613 kB in 4s (1,003 kB/s)
Reading package lists... Done
analyst@cuckoo:~$
analyst@cuckoo:~$ sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
Calculating upgrade... Done
The following packages have been kept back:
linux-generic-hwe-16.04 linux-headers-generic-hwe-16.04
linux-image-generic-hwe-16.04
The following packages will be upgraded:
firefox firefox-locale-en gir1.2-javascriptcoregtk-4.0 gir1.2-webkit2-4.0 libjavascriptcoregtk-4.0-18
libwebkit2gtk-4.0-37 libwebkit2gtk-4.0-37-gtk2 libxext-4.6 libxext-dev logrotate
openssh-client
qemu-block-extra qerau-kvm qemu-system-common qemu-system-x86 qemu-utils
```

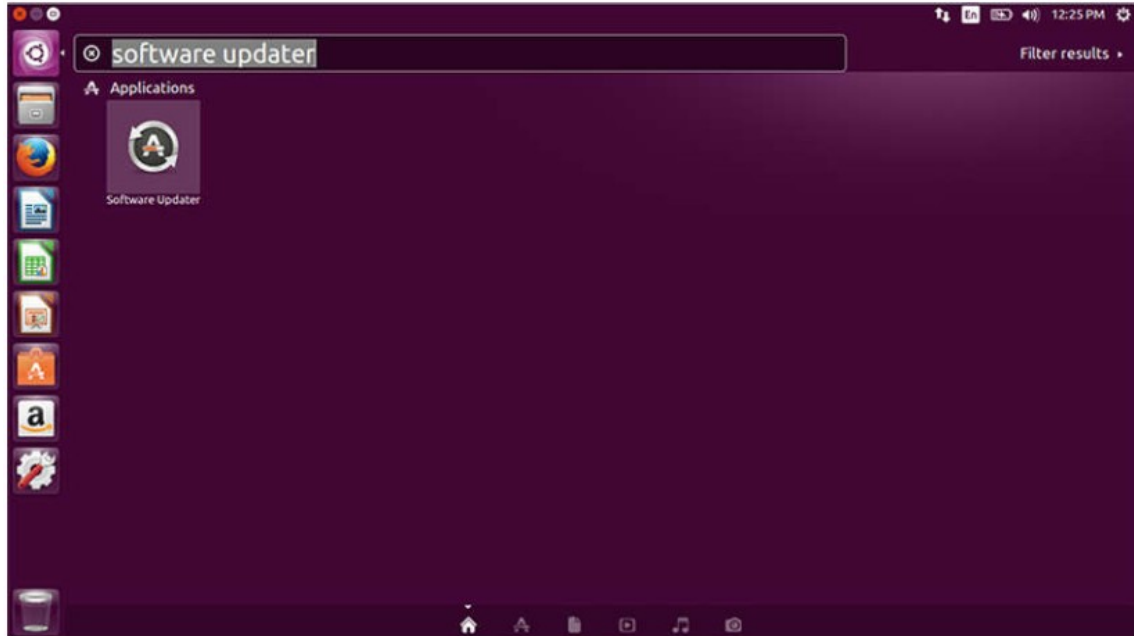
Maintenir le système à jour

- Également appelées correctifs, les mises à jour du système d'exploitation sont publiées périodiquement par les sociétés qui en ont la charge pour traiter les vulnérabilités connues de leur système d'exploitation.
- Les systèmes d'exploitation modernes avertissent l'utilisateur lorsque des mises à jour sont disponibles et prêtes à être téléchargées et installées, mais l'utilisateur peut rechercher des mises à jour à tout moment.
- Le tableau suivant compare les commandes de distribution Arch Linux et Debian/Ubuntu Linux pour effectuer les opérations de base du système de paquetage.

Tâche	Arch	Debian/Ubuntu
Installer un package par son nom	pacman -S	apt install
Supprimer un paquet par son nom	pacman -R	apt remove
Mettre à jour un paquet local	pacman -Syy	apt-get update
Mettre à niveau tous les packages actuellement installés	pacman -Syu	mise à niveau apt-get

Maintenir le système à jour

- Une interface graphique Linux peut également être utilisée pour vérifier et installer manuellement les mises à jour.
- Dans Ubuntu, par exemple, pour installer des mises à jour, cliquez sur **Dash Search Box**, tapez **software updater**, puis cliquez sur l'icône **Software Updater**.



Processus et bifurcations

- Un processus est une instance de programme informatique en cours d'exécution.
- La bifurcation est une méthode utilisée par le noyau pour autoriser un processus à créer sa propre copie.
- Dans les systèmes d'exploitation multitâches, les processus ont besoin d'un moyen de créer de nouveaux processus. L'opération de bifurcation est le seul moyen de le faire sous Linux.
- Lorsqu'un processus appelle la bifurcation, le processus appelant devient le processus parent et le nouveau processus est désigné comme son enfant.
- Après la fourche, les processus sont, dans une certaine mesure, des processus indépendants. Ils ont des ID de processus différents mais exécutent le même code de programme.

Processus et bifurcations (Suite)

Le tableau suivant répertorie trois commandes utilisées pour gérer les processus.

Commande	Description
ps	<ul style="list-style-type: none">• Permet de dresser la liste des processus exécutés dans le système lorsqu'ils sont invoqués.• Peut être programmée pour afficher les processus en cours d'exécution appartenant à l'utilisateur actuel ou à d'autres utilisateurs.
haut	<ul style="list-style-type: none">• Permet également de dresser la liste des processus en cours d'exécution, mais contrairement à ps, la commande top continue d'afficher les processus en cours de façon dynamique.• Appuyez sur q pour quitter la commande top.
kill	<ul style="list-style-type: none">• Permet de modifier le comportement d'un processus spécifique.• Selon les paramètres, la commande kill supprime, redémarre ou interrompt un processus.• Dans de nombreux cas, l'utilisateur exécute ps outop avant d'exécuter kill.• Il fait cela afin d'apprendre le PID d'un processus avant d'exécuter kill.

Processus et bifurcations (Suite)

La sortie de la commande présente la sortie de la commande **top** sur un ordinateur Linux.

```
[analyst@secOps ~]$ top
top - 11:29:16 up 0 min, 1 user, load average: 1.09, 0.31, 0.11
Tasks: 119 total, 1 running, 118 sleeping, 0 stopped, 0 zombie
%Cpu(s): 5.4 us, 2.0 sy, 0.0 ni, 87.4 id, 2.7 wa, 1.4 hi, 1.0 si, 0.0 st
MiB Mem : 982.8 total, 67.9 free, 765.8 used, 149.1 buff/cache
MiB Swap: 0.0 total, 0.0 free, 0.0 used, 39.3 avail Mem

  PID USER      PR  NI  VIRT  RES  SHR S %CPU  %MEM    TIME+  COMMAND
 729 analyst   20   0 2652376 284472 61076 S   2.7   28.3   0:06.75 Web Cont+
 570 analyst   20   0 2691388 215728 62404 S   2.0   21.4   0:06.99 firefox
 357 root       20   0 267972  91960 18468 S   1.3    9.1   0:01.63 Xorg
 461 analyst   20   0 322208  21000  7480 S   1.3    2.1   0:00.67 xfce4-p+
 121 root       20   0         0         0 0 S    0.7    0.0   0:00.43 kswapd0
   1 root       20   0 174376   4196  1688 S   0.3    0.4   0:00.66 systemd
 294 root       20   0 245036  11876   868 S   0.3    1.2   0:00.34 python2+
 539 analyst   20   0 150824    660    0 S   0.3    0.1   0:00.02 VBoxCli+
 800 analyst   20   0 477768  18968  9800 S   0.3    1.9   0:00.30 xfce4-t+
   2 root       20   0         0         0 0 S    0.0    0.0   0:00.00 kthreadd
   3 root       0 -20         0         0 0 I    0.0    0.0   0:00.00 rcu_gp
   4 root       0 -20         0         0 0 I    0.0    0.0   0:00.00 rcu_par+
   5 root       20   0         0         0 0 I    0.0    0.0   0:00.00 kworker+
   6 root       0 -20         0         0 0 I    0.0    0.0   0:00.00 kworker+
   7 root       20   0         0         0 0 I    0.0    0.0   0:00.00 kworker+
   8 root       0 -20         0         0 0 I    0.0    0.0   0:00.00 mm_perc+
   9 root       20   0         0         0 0 S    0.0    0.0   0:00.02 ksoftir+
```

Logiciels malveillants sur un hôte Linux

- Les logiciels malveillants Linux comprennent les virus, les chevaux de Troie, les vers et les autres types de programmes malveillants qui peuvent affecter le système d'exploitation.
- Les processus et les services sont un vecteur d'attaque courant de Linux.
- La sortie de la commande présente un attaquant utilisant la commande Telnet pour sonder la nature et la version d'un serveur web.
- Le hacker a appris que le serveur en question exécute nginx version 1.12.0. La prochaine étape serait de rechercher les vulnérabilités connues dans le code de nginx 1.12.0.

```
analyst@secOps ~]$ telnet 209.165.200.224 80
Trying 209.165.200.224...
Connected to 209.165.200.224.
Escape character is '^]'.
<type anything to force an HTTP error response>
HTTP/1.1 400 Bad Request
Server: nginx/1.12.0
Date: Wed, 17 May 2017 14:27:30 GMT
Content-Type: text/html
Content-Length: 173
Connection: close
<html>
<head><title>400 Bad Request</title></head>
<body bgcolor="white">
<center><h1>400 Bad Request</h1></center>
<hr><center>nginx/1.12.0</center>
</body>
</html >
Connection closed by foreign host.
analyst@secOps ~]$
```

Vérification de Rootkit

- Un rootkit est un ensemble de logiciels malveillants conçus pour augmenter les privilèges d'un utilisateur ou accorder l'accès à certaines parties du logiciel qui doivent normalement rester inaccessibles.
- Un rootkit est destructeur car il modifie le code du noyau et de ses modules, changeant les opérations les plus importantes du système d'exploitation lui-même.
- Les méthodes de détection Rootkit incluent le démarrage de l'ordinateur à partir d'un support approuvé.
- L'enlèvement de rootkit peut être compliqué. La réinstallation du système d'exploitation est la seule vraie solution au problème.
- **chkrootkit** est un programme basé sur Linux répandu conçu pour rechercher les rootkits connus sur l'ordinateur.
- La sortie de commande présente la sortie de **chkrootkit** sur un système Linux Ubuntu.

```
analyst@cuckoo:~$ sudo ./chkrootkit
[sudo] password for analyst:
ROOTDIR is '/'
Checking 'amd'... not found
Checking 'basename'... not infected
Checking 'biff'... not found
Checking 'chfn'... not infected
Checking 'chsh'... not infected
Checking 'cron'... not infected
Checking 'crontab'... not infected
Checking 'date'... not infected
Checking 'du'... not infected
Checking 'dirname'... not infected
Checking 'echo'... not infected
Checking 'egrep'... not infected
Checking 'env'... not infected
Checking 'find'... not infected
Checking 'fingerd'... not found
Checking 'gpm'... not found
Checking 'grep'... not infected
Checking 'hdparm'... not infected
Checking 'su'... not infected
Checking 'ifconfig'... not infected
Checking 'inetd'... not tested
Checking 'inetdconf'... not found
```

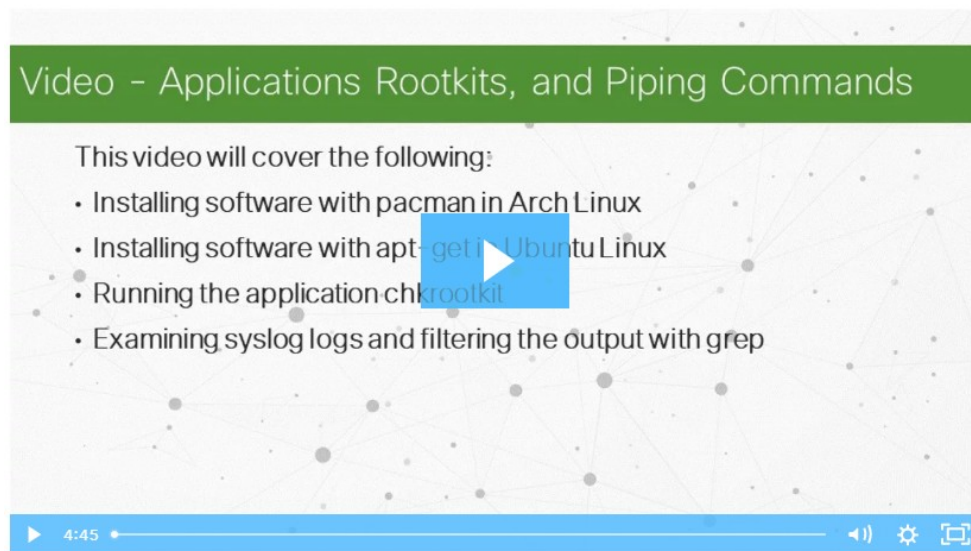
Commandes avec barres verticales

- Bien que les outils de ligne de commande soient généralement conçus pour effectuer une tâche spécifique et bien définie, il est possible de combiner plusieurs commandes pour effectuer des tâches plus complexes par une technique dite de canalisation.
- Les barres verticales permettent d'enchaîner plusieurs commandes et d'alimenter l'entrée d'une commande par la sortie d'une autre.
- Les deux commandes, **ls** et **grep**, peuvent être canalisées ensemble pour filtrer la sortie de **ls**, comme illustré sur la figure avec la commande **ls -l | grep nimda**. Ceci est affiché dans la sortie de la commande **ls -l | grep host** et la commande **ls -l | grep file**.

```
[analyst@secOps ~]$ ls -l
total 40
drwxr-xr-x 2 analyst analyst 4096 Mar 22 2018 Desktop
drwxr-xr-x 3 analyst analyst 4096 April 2 14:44 Downloads
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
-rw-r--r-- 1 analyst analyst 19 May 20 10:53 mytest.com
-rw-r--r-- 1 analyst analyst 228844 May 20 10:54 rkhunter-1.4.6-1-any.pkg.tar.xz
drwxr-xr-x 2 analyst analyst 4096 Mar 21 2018 second_drive
-rw-r--r-- 1 analyst analyst 257 May 20 10:52 space.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep host
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
[analyst@secOps ~]$
[analyst@secOps ~]$ ls -l | grep file
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile1.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:51 hostfile2.txt
-rw-r--r-- 1 analyst analyst 9 May 20 10:52 hostfile3.txt
drwxr-xr-x 9 analyst analyst 4096 Jul 19 2018 lab.support.files
[analyst@secOps ~]$
```

Vidéo de démonstration – Applications, rootkits et commandes avec barres verticales

Cliquez sur Lecture pour voir une démonstration de l'installation et de la mise à jour des applications, de la recherche d'un rootkit et de l'utilisation des commandes de canalisation.



4.8 Récapitulation des principes de base de Linux

Qu'est-ce que j'ai appris dans ce module ?

- Linux est un système d'exploitation open source rapide, fiable et petit.
- Sous Linux, l'utilisateur communique avec le système d'exploitation via une interface graphique ou une interface de ligne de commande (CLI), ou shell.
- Les serveurs sont des ordinateurs sur lesquels est installé un logiciel qui leur permet d'offrir des services aux clients à travers le réseau.
- Sous Linux, les serveurs sont gérés à l'aide de fichiers de configuration. Différents paramètres peuvent être modifiés et enregistrés dans les fichiers de configuration.
- Linux prend en charge un certain nombre de systèmes de fichiers différents qui varient en fonction de la vitesse, de la flexibilité, de la sécurité, de la taille, de la structure, de la logique, etc. Certains des systèmes de fichiers pris en charge par Linux sont ext2, ext3, ext4, NFS et CDFS.
- Le système X Windows, ou X11, est une infrastructure logicielle de base qui inclut des fonctions de création, de contrôle et de configuration d'une interface graphique Windows dans une interface pointer-cliquer.
- Pour installer des applications sur des hôtes Linux, des programmes appelés gestionnaires de paquets sont utilisés. Les packages sont des applications logicielles et tous leurs fichiers de support.

