

FACULTÉ DES SCIENCES DE RABAT

DÉPARTEMENT D'INFORMATIQUE

MASTER EN CYBERSÉCURITÉ INTELLIGENTE ET
TECHNOLOGIES ÉMERGENTES (CITECH)

Module : Sécurité des applications et des systèmes d'exploitation

Sécurisation d'un Système d'Exploitation avec des Protocoles d'Authentification et des Modèles de Contrôle d'Accès

Réalisé par :
Maach Nada

Encadré par :
Pr. Oussama Sbai

Contents

1	Problème 1 : Centralisation de l'authentification avec RADIUS	3
1.1	Problème 2 : Sécurisation des connexions avec Kerberos et SSO	5
1.2	Problème 3 : Application de politiques de contrôle d'accès (DAC, MAC) .	5
1.2.1	Mandatory Access Control (MAC)	6
1.3	Mise en place d'un fichier immuable	6
1.4	Problème 4 : Surveillance et journalisation des accès	7
1.4.1	Observation des logs d'audit générés	8
1.5	Conclusion	9

Introduction

Ce projet a pour but de renforcer la sécurité d'un système d'exploitation Linux à travers la mise en place de mécanismes d'authentification centralisée et de modèles de contrôle d'accès. Nous avons implémenté et testé plusieurs solutions :

- Centralisation de l'authentification avec FreeRADIUS.
- Mise en place de l'authentification unique avec Kerberos (SSO).
- Application de politiques de contrôle d'accès (DAC, MAC, RBAC).
- Surveillance et journalisation des accès avec auditd et fail2ban.

Chapter 1

Problème 1 : Centralisation de l'authentification avec RADIUS

Configuration du serveur et des clients

J'ai configuré le serveur FreeRADIUS sur une machine dédiée. Dans le fichier `/etc/freeradius/3.0/clients.conf`, j'ai défini le client avec son adresse IP :

```
client linux_client{
    ipaddr = 10.0.2.15
    secret = Client1
    require_message_authenticator = no
}
```

Figure 1.1: Configuration du client dans FreeRADIUS

Ensuite, j'ai ajouté un utilisateur interne dans le fichier `/etc/freeradius/3.0/users` : `testuser Cleartext-Password := "Password"`

```
testuser Cleartext-Password := "Password"
#
# Configuration file for the rlm_files module.
```

Figure 1.2: Ajout d'un utilisateur dans FreeRADIUS

Dans le fichier `/etc/freeradius/3.0/radiusd.conf`, j'ai également modifié un paramètre en remplaçant `no` par `yes`.

```
#
auth = yes

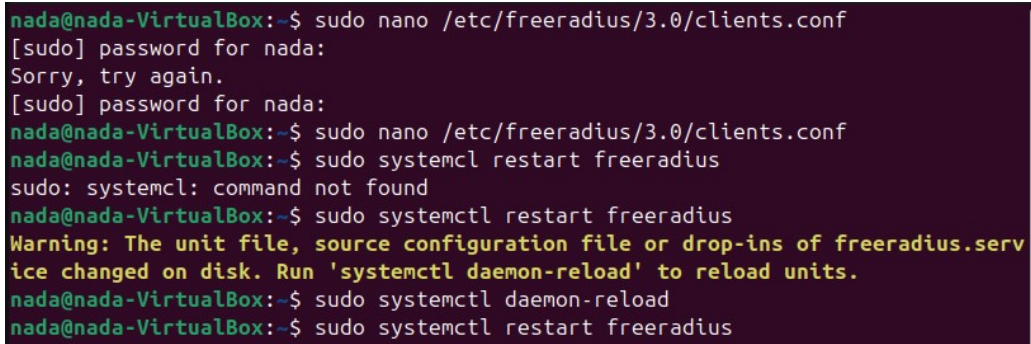
# Log Access-Accept results to the log file.
#
# This is only used if "auth = no"
#
# allowed values: {no, yes}
#
auth_accept = no
```

Figure 1.3: Modification de radiusd.conf

Redémarrage du service et tests

Après modification des fichiers de configuration, j'ai redémarré le service avec :

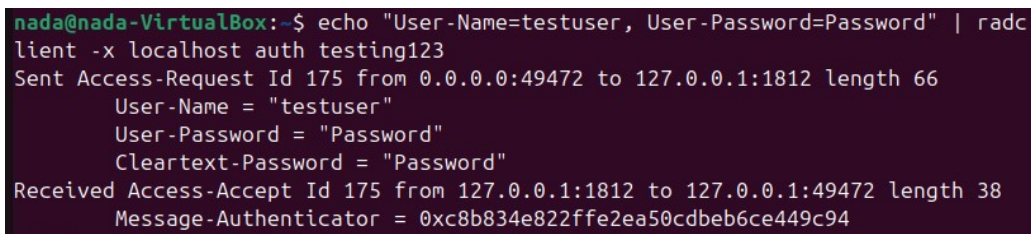
```
sudo systemctl restart freeradius
```



```
nada@nada-VirtualBox:~$ sudo nano /etc/freeradius/3.0/clients.conf
[sudo] password for nada:
Sorry, try again.
[sudo] password for nada:
nada@nada-VirtualBox:~$ sudo nano /etc/freeradius/3.0/clients.conf
nada@nada-VirtualBox:~$ sudo systemctl restart freeradius
sudo: systemctl: command not found
nada@nada-VirtualBox:~$ sudo systemctl restart freeradius
Warning: The unit file, source configuration file or drop-ins of freeradius.service changed on disk. Run 'systemctl daemon-reload' to reload units.
nada@nada-VirtualBox:~$ sudo systemctl daemon-reload
nada@nada-VirtualBox:~$ sudo systemctl restart freeradius
```

Figure 1.4: Redémarrage du service FreeRADIUS

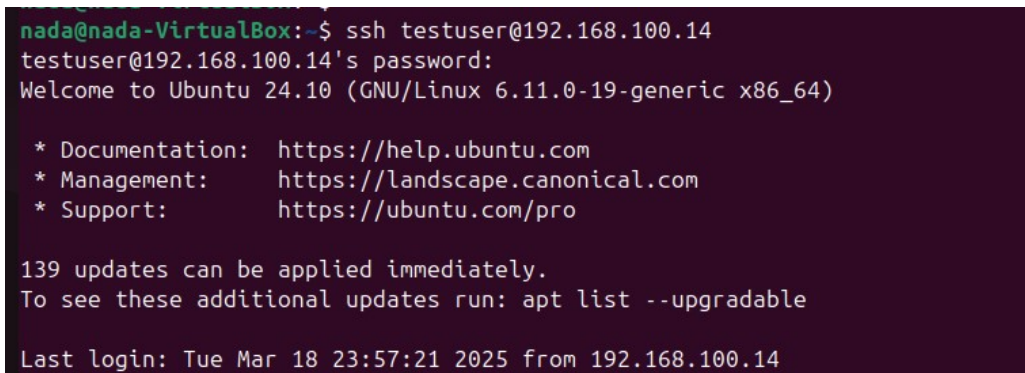
J'ai ensuite exécuté un test de login, et le serveur a bien accepté la demande d'authentification :



```
nada@nada-VirtualBox:~$ echo "User-Name=testuser, User-Password=Password" | radclient -x localhost auth testing123
Sent Access-Request Id 175 from 0.0.0.0:49472 to 127.0.0.1:1812 length 66
  User-Name = "testuser"
  User-Password = "Password"
  Cleartext-Password = "Password"
Received Access-Accept Id 175 from 127.0.0.1:1812 to 127.0.0.1:49472 length 38
  Message-Authenticator = 0xc8b834e822ffe2ea50cdbeb6ce449c94
```

Figure 1.5: Test de login RADIUS (Access-Accepted)

Enfin, j'ai réalisé une connexion SSH depuis la machine cliente en utilisant l'utilisateur défini (`intern@client_ip_address`):



```
nada@nada-VirtualBox:~$ ssh testuser@192.168.100.14
testuser@192.168.100.14's password:
Welcome to Ubuntu 24.10 (GNU/Linux 6.11.0-19-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

139 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Tue Mar 18 23:57:21 2025 from 192.168.100.14
```

Figure 1.6: Connexion SSH réussie

Après avoir saisi le mot de passe, l'authentification a réussi et l'événement est également apparu dans les logs du serveur FreeRADIUS :

```
nada@nada-VirtualBox:~$ sudo tail -f /var/log/freeradius/radius.log
Tue Mar 18 23:40:20 2025 : Info: Exiting normally
Tue Mar 18 23:40:21 2025 : Info: Debug state unknown (cap_sys_ptrace capability not set)
Tue Mar 18 23:40:21 2025 : Info: systemd watchdog interval is 30.00 secs
Tue Mar 18 23:40:21 2025 : Info: Loaded virtual server <default>
Tue Mar 18 23:40:21 2025 : Warning: Ignoring "sql" (see raddb/mods-available/README.rst)
Tue Mar 18 23:40:21 2025 : Warning: Ignoring "ldap" (see raddb/mods-available/README.rst)
Tue Mar 18 23:40:21 2025 : Info: Loaded virtual server default
Tue Mar 18 23:40:21 2025 : Info: # Skipping contents of 'if' as it is always 'false' -- /etc/freeradius/3.0/sites-enabled/inner-tunnel:366
Tue Mar 18 23:40:21 2025 : Info: Loaded virtual server inner-tunnel
Tue Mar 18 23:40:21 2025 : Info: Ready to process requests
Tue Mar 18 23:45:48 2025 : Error: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Tue Mar 18 23:45:48 2025 : Error: BlastRADIUS check: Received packet without Proxy-State.
Tue Mar 18 23:45:48 2025 : Error: Setting "limit_proxy_state = true" for client linux_client
Tue Mar 18 23:45:48 2025 : Error: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Tue Mar 18 23:45:48 2025 : Error: The packet contains Message-Authenticator.
Tue Mar 18 23:45:48 2025 : Error: The client has likely been upgraded to protect from the attack.
Tue Mar 18 23:45:48 2025 : Error: Please set "require_message_authenticator = true" for client linux_client
Tue Mar 18 23:45:48 2025 : Error: !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Tue Mar 18 23:45:48 2025 : Auth: (0) Login OK: [testuser] (from client linux_client port 0)
```

Figure 1.7: Apparition dans les logs

1.1 Problème 2 : Sécurisation des connexions avec Kerberos et SSO

Configuration du serveur Kerberos

J'ai installé et configuré un serveur Kerberos pour gérer les identités. Ensuite, j'ai créé le premier client et testé les commandes suivantes : `kinit client@KRB.COM` et `klist`.

```
nada@nada-VirtualBox:~$ ssh testuser@192.168.100.14
testuser@192.168.100.14's password:
Welcome to Ubuntu 24.10 (GNU/Linux 6.11.0-19-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

139 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Tue Mar 18 23:57:21 2025 from 192.168.100.14
```

Figure 1.8: Obtention d'un ticket Kerberos

Connexion SSH avec Kerberos

Après avoir configuré le serveur SSH, j'ai vérifié que l'utilisateur pouvait se connecter sans ressaisir son mot de passe, grâce à l'authentification par tickets Kerberos.

1.2 Problème 3 : Application de politiques de contrôle d'accès (DAC, MAC)

J'ai commencé par créer un utilisateur nommé `test`, puis un fichier nommé `sensitive`.

```
touch sensitive
ls -l sensitive
-rw-rw-r-- 1 test test ... sensitive
```

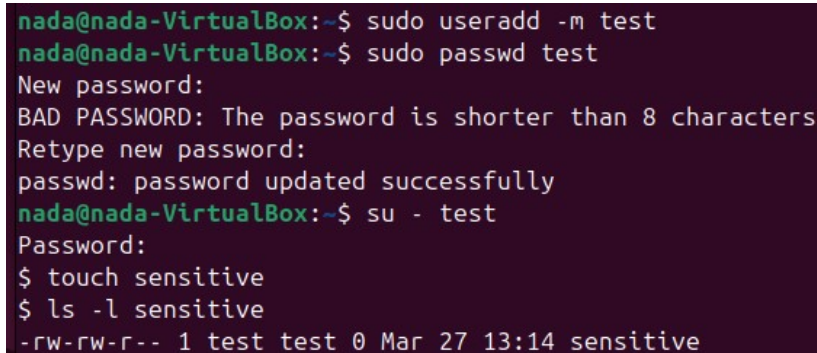
Ensuite, j'ai modifié les permissions avec :

```
chmod 600 sensitive
```

Le fichier est alors devenu :

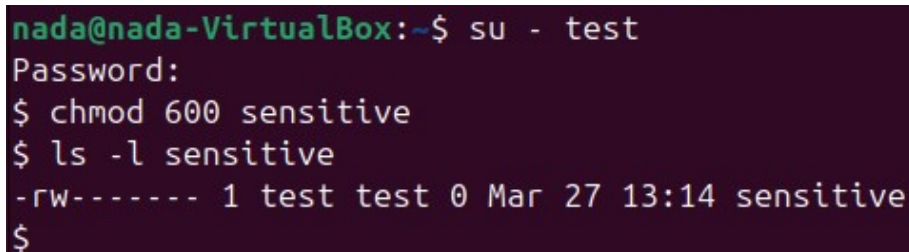
```
-rw----- 1 test test ... sensitive
```

Ainsi, seul moi (l'utilisateur propriétaire) ai pu lire et écrire le fichier, tandis que les autres utilisateurs ont été exclus.



```
nada@nada-VirtualBox:~$ sudo useradd -m test
nada@nada-VirtualBox:~$ sudo passwd test
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
nada@nada-VirtualBox:~$ su - test
Password:
$ touch sensitive
$ ls -l sensitive
-rw-rw-r-- 1 test test 0 Mar 27 13:14 sensitive
```

Figure 1.9: Création du fichier `sensitive` et modification des permissions avec `chmod 600`.



```
nada@nada-VirtualBox:~$ su - test
Password:
$ chmod 600 sensitive
$ ls -l sensitive
-rw----- 1 test test 0 Mar 27 13:14 sensitive
$
```

Figure 1.10: Affichage des permissions confirmant que seul l'utilisateur propriétaire a accès.

1.2.1 Mandatory Access Control (MAC)

1.3 Mise en place d'un fichier immutable

Pour tester le MAC, j'ai utilisé la commande :

```
sudo chattr +i /home/test/sensitive
```

Cette opération a rendu le fichier **immutable**. Lorsque j'ai tenté de modifier les permissions, l'accès m'a été refusé :

```
chmod 777 /home/test/sensitive
chmod: changing permissions ... : Operation not permitted
```

Cela montre que le MAC a été appliqué avec succès : le système refuse toute modification non autorisée, même par le propriétaire.


```
nada@nada-VirtualBox:~$ sudo chattr +i /home/test/sensitive
nada@nada-VirtualBox:~$ su - test
Password:
$ chmod 777 /home/test/sensitive
chmod: changing permissions of '/home/test/sensitive': Operation not permitted
$
```

Figure 1.11: Tentative de modification des permissions d'un fichier protégé par `chattr +i`.

1.4 Problème 4 : Surveillance et journalisation des accès

Logs d'authentification SSH

Les tentatives de connexion acceptées et échouées ont été observées dans `/var/log/auth.log`.

```
nada@nada-VirtualBox:~$ grep "Accepted" /var/log/auth.log
2025-03-18T23:57:19.803867+00:00 nada-VirtualBox sshd[5556]: Accepted password for testuser from 192.168.1.106 ssh2
2025-03-19T00:23:14.476497+00:00 nada-VirtualBox sshd[6477]: Accepted password for testuser from 192.168.1.146 ssh2
nada@nada-VirtualBox:~$
```

Figure 1.12: Connexion acceptée dans les logs SSH

```
nada@nada-VirtualBox:~$ grep "Failed" /var/log/auth.log
2025-03-18T19:21:46.454435+00:00 nada-VirtualBox dbus-daemon[1091]: [system] Failed to activate service 'org.freedesktop.DBus': (service_start_timeout=25000ms)
2025-03-18T21:00:56.757622+00:00 nada-VirtualBox dbus-daemon[942]: [system] Failed to activate service 'org.freedesktop.DBus': (service_start_timeout=25000ms)
2025-03-18T21:53:21.678148+00:00 nada-VirtualBox dbus-daemon[870]: [system] Failed to activate service 'org.freedesktop.DBus': (service_start_timeout=25000ms)
2025-03-18T22:43:42.676741+00:00 nada-VirtualBox sshd[4103]: pam_radius_auth: Failed bind to vrf-blue: No such file or directory
2025-03-18T22:43:44.587657+00:00 nada-VirtualBox sshd[4103]: Failed password for invalid user testuser from 192.168.1.13 port 43158 ssh2
2025-03-18T22:43:50.332314+00:00 nada-VirtualBox sshd[4103]: pam_radius_auth: Failed bind to vrf-blue: No such file or directory
2025-03-18T22:43:52.346372+00:00 nada-VirtualBox sshd[4103]: Failed password for invalid user testuser from 192.168.1.13 port 43158 ssh2
2025-03-18T22:47:15.037267+00:00 nada-VirtualBox sshd[4203]: pam_radius_auth: Failed bind to vrf-blue: No such file or directory
2025-03-18T22:47:16.852570+00:00 nada-VirtualBox sshd[4203]: Failed password for invalid user testuser from 192.168.1.13 port 45206 ssh2
2025-03-18T22:47:36.855616+00:00 nada-VirtualBox sshd[4203]: pam_radius_auth: Failed bind to vrf-blue: No such file or directory
2025-03-18T22:47:38.915695+00:00 nada-VirtualBox sshd[4203]: Failed password for invalid user testuser from 192.168.1.13 port 45206 ssh2
2025-03-18T22:47:43.251840+00:00 nada-VirtualBox sshd[4203]: pam_radius_auth: Failed bind to vrf-blue: No such file or directory
2025-03-18T22:47:45.908336+00:00 nada-VirtualBox sshd[4203]: Failed password for invalid user testuser from 192.168.1.13 port 45206 ssh2
2025-03-18T22:55:47.096756+00:00 nada-VirtualBox sshd[4232]: pam_radius_auth: Failed bind to vrf-blue: No such file or directory
2025-03-18T22:55:48.865760+00:00 nada-VirtualBox sshd[4232]: Failed password for invalid user testuser from 192.168.1.13 port 60940 ssh2
2025-03-18T22:56:07.419591+00:00 nada-VirtualBox sshd[4232]: pam_radius_auth: Failed bind to vrf-blue: No such file or directory
2025-03-18T22:56:09.601108+00:00 nada-VirtualBox sshd[4232]: Failed password for invalid user testuser from 192.168.1.13 port 60940 ssh2
```

Figure 1.13: Tentative échouée de connexion SSH

Audit des accès

Nous avons configuré `auditctl` afin de surveiller les accès aux fichiers sensibles.

Surveillance du fichier `/etc/passwd`

Un message d'avertissement `Old style watch rules are slower` est affiché, ce qui indique que la méthode utilisée est plus ancienne, mais encore supportée. Si la règle existe déjà, l'erreur suivante peut apparaître : `Error sending add rule data request (Rule exists)`.

Surveillance du fichier /etc/shadow

Ce fichier contient les mots de passe chiffrés des utilisateurs. Il est essentiel de surveiller toute tentative de modification.

Surveillance du fichier /var/log/auth.log

Le fichier `/var/log/auth.log` enregistre les événements d'authentification (SSH, sudo, etc.). Sa surveillance permet de détecter des intrusions ou tentatives d'accès suspectes.

```
nada@nada-VirtualBox:~$ sudo auditctl -w /etc/passwd -p wa -k passwd_changes
Old style watch rules are slower
nada@nada-VirtualBox:~$ sudo auditctl -w /etc/passwd -p wa -k passwd_changes
Old style watch rules are slower
Error sending add rule data request (Rule exists)
There was an error while processing parameters
nada@nada-VirtualBox:~$ sudo auditctl -w /etc/shadow -p wa -k shadow_changes
Old style watch rules are slower
nada@nada-VirtualBox:~$ sudo auditctl -w /var/log/auth.log -p wa -k authlog_changes
Old style watch rules are slower
nada@nada-VirtualBox:~$ sudo auditctl -l
-w /etc/passwd -p wa -k passwd_changes
-w /etc/shadow -p wa -k shadow_changes
-w /var/log/auth.log -p wa -k authlog_changes
```

Figure 1.14: configuration `auditctl`

1.4.1 Observation des logs d'audit générés

```

nada@nada-VirtualBox:~$ sudo ausearch -k passwd_changes
-----
time->Thu Mar 27 21:44:01 2025
type=PROCTITLE msg=audit(1743111841.231:309): proctitle=617564697463746C002D77002F727463746E676573746573
007061737377645F6368616E676573
type=SYSCALL msg=audit(1743111841.231:309): arch=c000003e syscall=44 success=yes exit=100
3=0 items=0 ppid=5827 pid=5828 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0
ditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1743111841.231:309): auid=1000 ses=2 subj=unconfined op=add
4 res=0
-----
time->Thu Mar 27 21:44:15 2025
type=PROCTITLE msg=audit(1743111855.704:316): proctitle=617564697463746C002D77002F657463746E676573746573
007061737377645F6368616E676573
type=SYSCALL msg=audit(1743111855.704:316): arch=c000003e syscall=44 success=yes exit=100
3=0 items=0 ppid=5831 pid=5832 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0
ditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1743111855.704:316): auid=1000 ses=2 subj=unconfined op=add
4 res=1
-----
time->Thu Mar 27 21:44:41 2025
type=PROCTITLE msg=audit(1743111881.192:323): proctitle=617564697463746C002D77002F657463746E676573746573
007061737377645F6368616E676573
type=SOCKADDR msg=audit(1743111881.192:323): saddr=10000000000000000000000000000000
type=SYSCALL msg=audit(1743111881.192:323): arch=c000003e syscall=44 success=yes exit=100
3=0 items=0 ppid=5843 pid=5844 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0
ditctl" exe="/usr/sbin/auditctl" subj=unconfined key=(null)
type=CONFIG_CHANGE msg=audit(1743111881.192:323): auid=1000 ses=2 subj=unconfined op=add
4 res=0
nada@nada-VirtualBox:~$

```

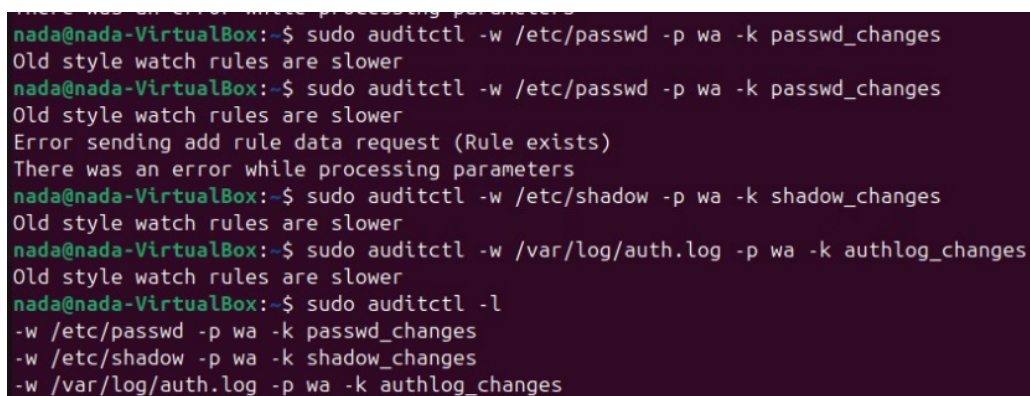
Figure 1.15: Observation des logs

1.5 Conclusion

Grâce à `auditctl`, nous avons configuré la surveillance des fichiers sensibles suivants :

- `/etc/passwd` : gestion des utilisateurs.
- `/etc/shadow` : stockage des mots de passe chiffrés.
- `/var/log/auth.log` : journaux d'authentification.

Ainsi, tout accès ou modification sur ces fichiers générera un événement enregistré dans le journal `/var/log/audit/audit.log`. Les clés associées (`passwd_changes`, `shadow_changes`, `authlog_changes`) facilitent la recherche ultérieure via la commande `ausearch -k <clé>`.



```
nada@nada-VirtualBox:~$ sudo auditctl -w /etc/passwd -p wa -k passwd_changes
Old style watch rules are slower
nada@nada-VirtualBox:~$ sudo auditctl -w /etc/passwd -p wa -k passwd_changes
Old style watch rules are slower
Error sending add rule data request (Rule exists)
There was an error while processing parameters
nada@nada-VirtualBox:~$ sudo auditctl -w /etc/shadow -p wa -k shadow_changes
Old style watch rules are slower
nada@nada-VirtualBox:~$ sudo auditctl -w /var/log/auth.log -p wa -k authlog_changes
Old style watch rules are slower
nada@nada-VirtualBox:~$ sudo auditctl -l
-w /etc/passwd -p wa -k passwd_changes
-w /etc/shadow -p wa -k shadow_changes
-w /var/log/auth.log -p wa -k authlog_changes
```

Figure 1.16: Exemple de logs générés par `auditctl`

Alertes automatiques

Un système d'alerte a été configuré avec `fail2ban`, permettant de bloquer une IP après plusieurs tentatives échouées.

Conclusion

Ce projet nous a permis de mettre en place différentes solutions de sécurité sur un système Linux : centralisation de l'authentification avec RADIUS et Kerberos, mise en place de modèles de contrôle d'accès (DAC, MAC), et surveillance avec journalisation. Ces mesures renforcent significativement la sécurité du système, en limitant les accès non autorisés et en assurant une meilleure traçabilité des actions.