

Laboratoire - Documenter les problèmes de cybersécurité d'une entreprise (fictive)



Auteur : Ismaël Baby

Période : Hiver 2025

Étudiant en Cybersécurité

Rédigé le 25 avril 2025

Introduction: Scénario : L'Auto-Audit de Sécurité du "Home Lab"	3
Contexte	3
La Mission	3
Étape 1 : Préparation de l'environnement.....	3
Étape 2 : Analyse réseau (reconnaissance passive et active)	4
Étape 3 : Analyse de configuration système :	5
• Relevez au moins 3 recommandations de sécurité.....	7
• Vérifiez la présence d'un antivirus actif.	7
• Vérifiez les comptes administrateurs locaux.	8
• Ouvrez les stratégies de sécurité locale (secpol.msc) et identifiez au moins un manquement.....	9
Étape 4 : Analyse des politiques internes (fictives ou existantes) :.....	9
• Identifiez si les pratiques observées ci-dessus et respectent les politiques prévues :.....	7
Conclusions :	7
Références :.....	7

Introduction: Scénario : L'Auto-Audit de Sécurité du "Home Lab"

Contexte

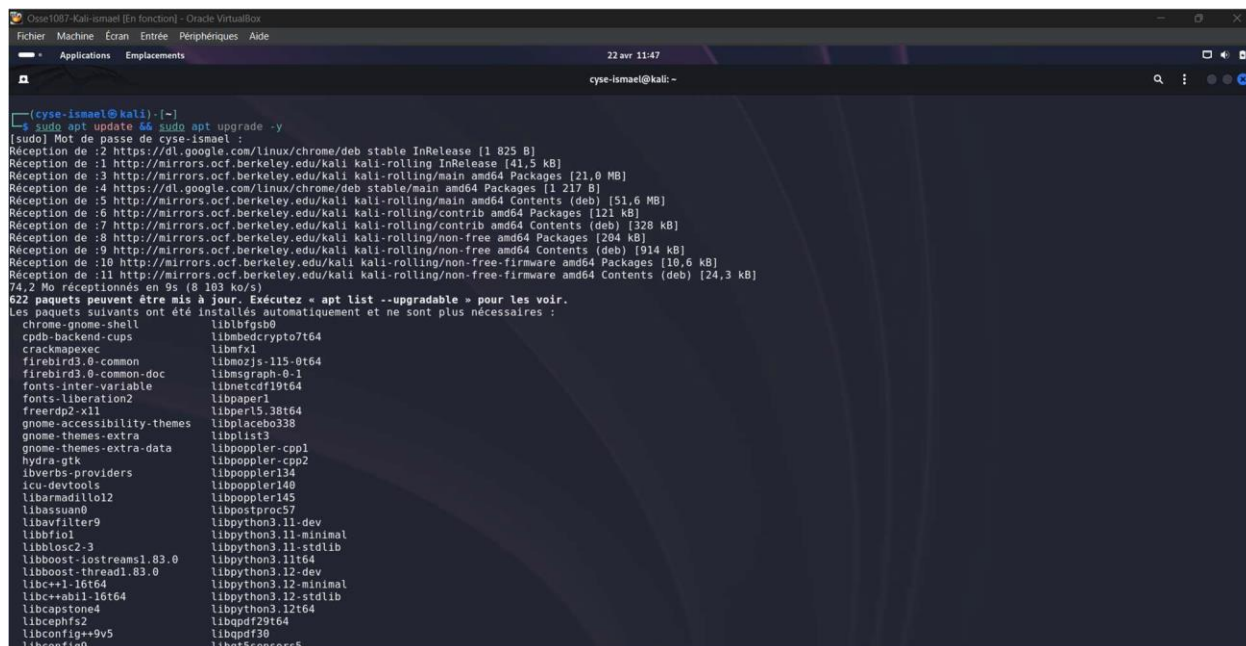
Dans le cadre de mon apprentissage autodidacte, j'ai mis en place un Home Lab composé de plusieurs machines virtuelles (VM) pour m'exercer. Ce laboratoire simule un petit réseau. Avant de passer à des exercices plus avancés comme le hacking éthique, il est essentiel de m'assurer que les bases de la sécurité de cet environnement sont solides.

La Mission

Je me place dans le rôle d'un auditeur interne mandaté pour effectuer un auto-audit de sécurité. L'objectif est de traiter mon Home Lab comme un réseau critique et d'y dénicher les faiblesses avant qu'elles ne soient exploitées (même si je suis le seul utilisateur !)

Étape 1 : Préparation de l'environnement

- Lancement de la machine virtuelle ou connectez-vous à un environnement de simulation (réseau local ou réseau de test).
- Mettez à jour le système :



```
(cyse-ismael@kali) ~  
[sudo] apt update  
[sudo] Mot de passe de cyse-ismael :  
Réception de :2 https://dl.google.com/linux/chrome/deb stable InRelease [1 825 B]  
Réception de :1 http://mirrors.ocf.berkeley.edu/kali kali-rolling InRelease [41.5 kB]  
Réception de :3 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 Packages [21.0 MB]  
Réception de :4 https://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1 217 B]  
Réception de :5 http://mirrors.ocf.berkeley.edu/kali kali-rolling/main amd64 Contents (deb) [51.6 MB]  
Réception de :6 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib amd64 Packages [121 kB]  
Réception de :7 http://mirrors.ocf.berkeley.edu/kali kali-rolling/contrib amd64 Contents (deb) [328 kB]  
Réception de :8 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free amd64 Packages [204 kB]  
Réception de :9 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]  
Réception de :10 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]  
Réception de :11 http://mirrors.ocf.berkeley.edu/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]  
71.2 Mo réceptionnés en 9s (8 183 ko/s)  
622 paquets peuvent être mis à jour. Exécutez « apt list --upgradable » pour les voir.  
Les paquets suivants ont été installés automatiquement et ne sont plus nécessaires :  
chrome-gnome-shell  
cpdb-backend-cups  
crackmapexec  
firebird3.0-common  
firebird3.0-common-doc  
fonts-inter-variable  
fonts-liberation2  
freerdp2-x11  
gnome-accessibility-themes  
gnome-themes-extra  
gnome-themes-extra-data  
hydra-gtk  
libverbs-providers  
icu-devtools  
libbarmadillo12  
libbassoon0  
libbavfilter9  
libbfiol  
libblosc2-3  
libboost-iostreams1.83.0  
libboost-thread1.83.0  
libc++1.16t64  
libc++abi1.16t64  
libcapstone4  
libcephfs2  
libconfig+9v5  
libconfig9  
libbfgsb0  
libbmedcrypto7t64  
libbmx1  
libmozjs-115-0t64  
libmsgpack-0.1  
libnetcdf19t64  
libpaper1  
libperl5.38t64  
libplacebo338  
libplist3  
libpoppler-cpp1  
libpoppler-cpp2  
libpoppler134  
libpoppler140  
libpoppler145  
libpostproc57  
libpython3.11-dev  
libpython3.11-minimal  
libpython3.11-stdlib  
libpython3.11t64  
libpython3.12-dev  
libpython3.12-minimal  
libpython3.12-stdlib  
libpython3.12t64  
libqpdf30  
libqt5sensors5
```

LinkedIn : <https://www.linkedin.com/in/ismael-abdallah-baby-5b7304318/>

Étape 2 : Analyse réseau (reconnaissance passive et active)

- Utilisez des outils comme Nmap pour scanner le réseau :

```
(cyse_ismael@kali)-[~]
$ nmap 10.0.2.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-23 09:11 ADT
Nmap scan report for 10.0.2.1
Host is up (0.00044s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
52/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.00090s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
2021/tcp  open  servexec
3306/tcp  open  mysql
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00012s latency).
All 1000 scanned ports on 10.0.2.3 are in ignored states.
Not shown: 1000 filtered tcp ports (proto-unreach)
MAC Address: 08:00:27:13:FB:DC (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap scan report for 10.0.2.5
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.5 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 256 IP addresses (4 hosts up) scanned in 14.96 seconds
```

- Notez 3 ports ouverts, services actifs, protocoles visibles.

Ports ouverts	Services actifs	Protocoles visibles.
135	MSRCP	TCP
2021	Servexex	TCP
3306	MySQL	TCP

- Identifiez 3 postes vulnérables ou exposés (ex. : port 21 FTP ouvert, absence de chiffrement).
 - Port 135/Tcp ouvert, un pirate peut s'en servir pour exécuter du code malveillant à distance, sans autorisation.
 - Port 2021/Tcp ouvert, pouvant être utilisé pour des exécutions de commandes à distance. Si mal configuré, il peut permettre à un attaquant de prendre le contrôle du système.
 - Port 3306/Tcp ouvert, Ce port permet un accès direct à la base de données. Si l'accès n'est pas restreint ou chiffré, il est vulnérable aux attaques par injection SQL ou brute force.

Étape 3 : Analyse de configuration système :

Sur la VM Linux :

```
sudo lynis audit system
```

```
(cyse_ismael@kali)~$ sudo lynis audit system
```

```
[ Lynis 3.1.4 ]
```

```
=====
Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
welcome to redistribute it under the terms of the GNU General Public License.
See the LICENSE file for details about using this software.
=====
```

```
2007-2024, CISOfy - https://cisofy.com/lynis/
Enterprise support available (compliance, plugins, interface and tools)
=====
```

```
[+] Initializing program
```

```
- Detecting OS ... [ DONE ]
- Checking profiles ... [ DONE ]
```

```
Program version: 3.1.4
Operating system: Linux
Operating system name: Kali Linux
Operating system version: Rolling release
Kernel version: 6.8.11
Hardware platform: x86_64
Hostname: kali

Profiles: /etc/lynis/default.prf
Log file: /var/log/lynis.log
Report file: /var/log/lynis-report.dat
Report version: 1.0
Plugin directory: /etc/lynis/plugins
```

```
Auditor: [Not Specified]
Language: en
Test category: all
Test group: all
```

```
- Program update status ... [ NO UPDATE ]
```

```
[+] System tools
```

```
- Scanning available tools ...
- Checking system binaries ...
```

```

Suggestions (47):
* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]
- Related resources
  * Website: https://cisofy.com/lynis/controls/DEB-0280/
* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]
- Related resources
  * Website: https://cisofy.com/lynis/controls/DEB-0810/
* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]
- Related resources
  * Website: https://cisofy.com/lynis/controls/DEB-0811/
* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]
- Related resources
  * Website: https://cisofy.com/lynis/controls/DEB-0831/
* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]
- Related resources
  * Website: https://cisofy.com/lynis/controls/DEB-0880/
* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]
- Related resources
  * Website: https://cisofy.com/lynis/controls/BOOT-5122/
* Determine runlevel and services at startup [BOOT-5180]
- Related resources
  * Website: https://cisofy.com/lynis/controls/BOOT-5180/
* Consider hardening system services [BOOT-5264]
- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service
- Related resources
  * Article: Systemd features to secure service files: https://linux-audit.com/systemd/systemd-features-to-secure-units-and-services/
  * Website: https://cisofy.com/lynis/controls/BOOT-5264/
* Configure password hashing rounds in /etc/login.defs [AUTH-9230]
- Related resources
  * Article: Linux password security: hashing rounds: https://linux-audit.com/authentication/configure-the-minimum-password-length-on-linux-systems/
  * Website: https://cisofy.com/lynis/controls/AUTH-9230/
* Install a PAM module for password strength testing like pam_cracklib or pam_passwdqc or libpam-passwdqc [AUTH-9262]
- Related resources
  * Article: Configure minimum password length for Linux systems: https://linux-audit.com/configure-the-minimum-password-length-on-linux-systems/
  * Website: https://cisofy.com/lynis/controls/AUTH-9262/
* When possible set expire dates for all password protected accounts [AUTH-9282]
- Related resources
  * Website: https://cisofy.com/lynis/controls/AUTH-9282/

```

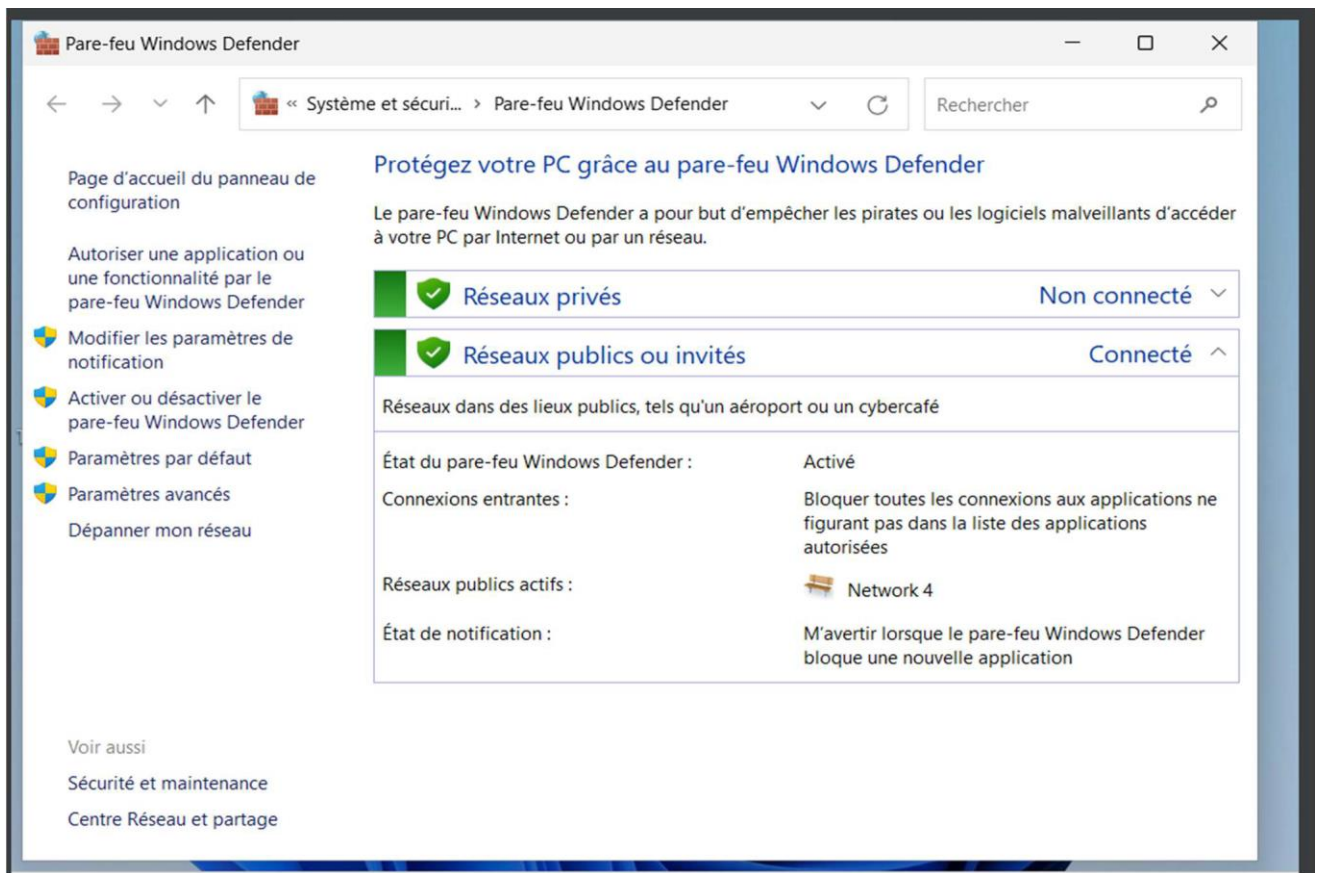
- **Relevez au moins 3 recommandations de sécurité.**

1. Installer fail2ban pour bloquer automatiquement les tentatives de connexion après plusieurs erreurs.
2. Mettre un mot de passe sur le démarrage pour éviter que quelqu'un ne modifie les réglages du système sans autorisation.
3. Renforcer les mots de passe ajouter un module pour obliger l'utilisateur à choisir des mots de passe plus longs et plus solides.

Sur la VM Windows :

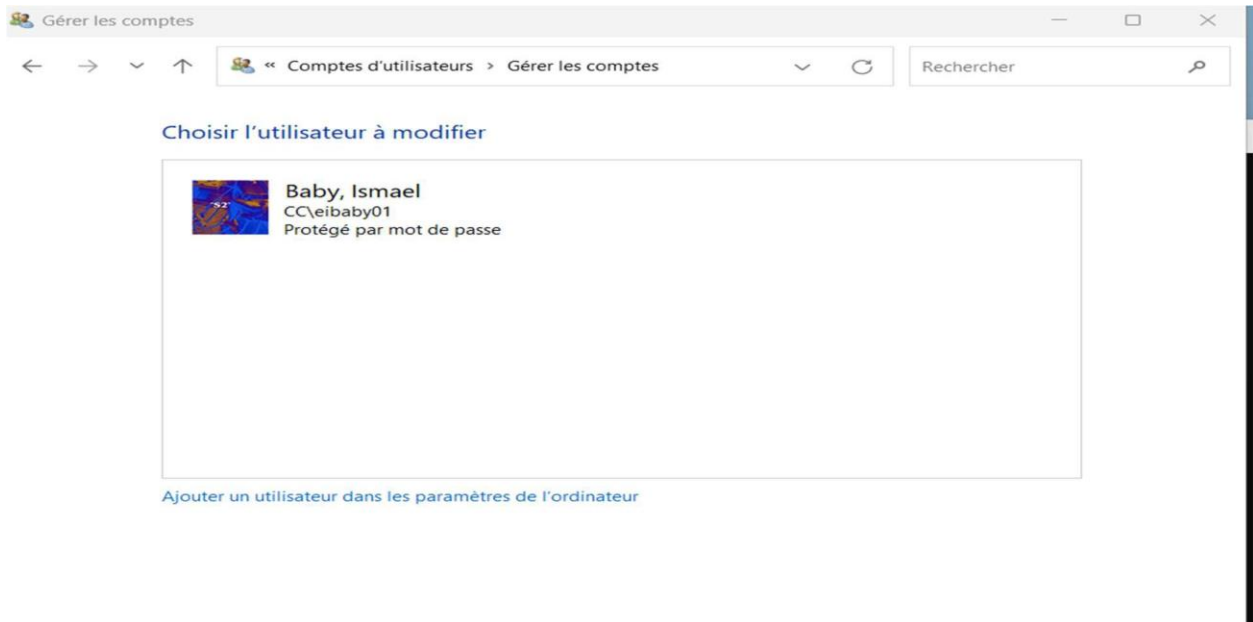
- **Vérifiez la présence d'un antivirus actif.**

- Le pare-feu Windows Defender est activé pour les réseaux publics :

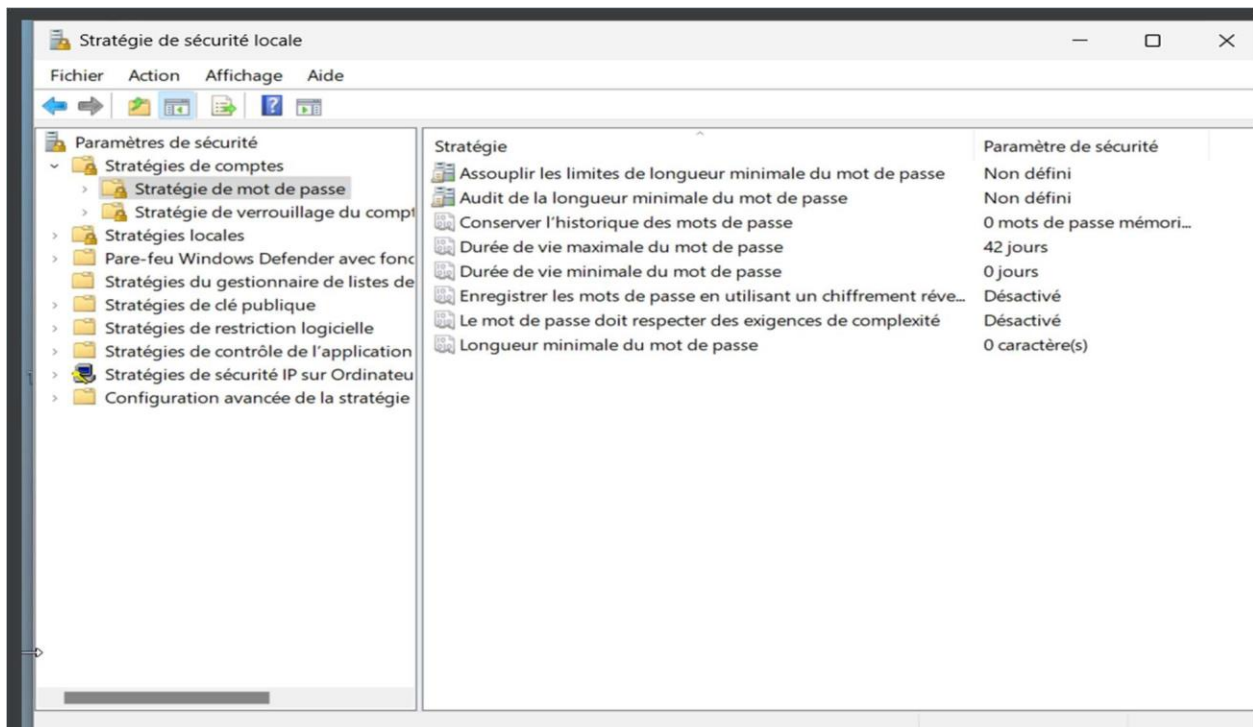


- **Vérifiez les comptes administrateurs locaux.**

- Le seul compte visible est Baby, Ismael, protégé par mot de passe il n'y a pas de compte Administrateur activé visible, donc pas de risque lié au nom par défaut :



- **Ouvrez les stratégies de sécurité locale (secpol.msc) et identifiez au moins un manquement**
 - La complexité des mots de passe est désactivée donc cela est un manquement :



Étape 4 : Analyse des politiques internes (fictives ou existantes) :

- **Créez une courte politique d'accès aux ressources :**

Chaque utilisateur a un identifiant et un mot de passe personnel, qu'il ne doit jamais partager.

LinkedIn : <https://www.linkedin.com/in/ismael-abdallah-baby-5b7304318/>

- ✓ Les mots de passe doivent être complexes.
- ✓ L'utilisateur doit verrouiller son poste lorsqu'il quitte sa machine.
- ✓ Les ports inutiles doivent être fermés, et les services sensibles doivent être protégés.
- ✓ L'utilisation des ressources informatiques est réservée au travail, et tout usage doit rester sécurisé et professionnel.
- ✓ Tout accès aux ressources (réseau, serveurs, fichiers) doit se faire dans le cadre de l'activité professionnelle.

- **Identifiez si les pratiques observées ci-dessus et respectent les politiques prévues :**

Pratique à vérifier	Observation ?	Pourquoi ?
Identifiants personnels	✓ Oui	Un seul compte utilisateur (Baby, Ismael) est utilisé.
Mots de passe complexes	✗ Non	La complexité des mots de passe est désactivée sur Windows.
Verrouillage du poste	?	Non effectuer ici
Ports et services sécurisés	✗ Non	Plusieurs ports ouverts sans filtrage : 135, 2021, 3306.
Usage professionnel sécurisé	?	Non effectuer ici
Antivirus actif	✓ Oui	Windows Defender est activé.

Conclusions :

Ce laboratoire nous permet de mieux comprendre comment identifier et analyser des failles de sécurité dans un réseau informatique réel ou simulé. En utilisant des outils comme Nmap et Lynis, j'ai pu repérer des ports ouverts, des services sensibles, et des mauvaises configurations qui pourraient facilement être exploitées par un pirate. J'ai aussi appris l'importance des politiques de sécurité internes, comme le choix de mots de passe solides, la protection des ports réseau, ou encore la mise en place de contrôles d'accès. Ce que j'ai trouvé sur les VM (Linux et Windows) montre que même un système fonctionnel peut présenter plusieurs risques s'il n'est pas bien configuré. Ce lab nous aide à faire le lien entre les concepts vus en cours (comme la confidentialité, l'intégrité, et la disponibilité) et la réalité d'une infrastructure informatique. Il nous permet aussi de montrer que même de petites négligences peuvent avoir de grosses conséquences.

Références :

<https://www.eramet.com/wp-content/uploads/2020/12/politique-des-technologies-de-Information-et-des-telecommunications.pdf>

