

DAT_Lab: Environnement de test

Auteur : Yann

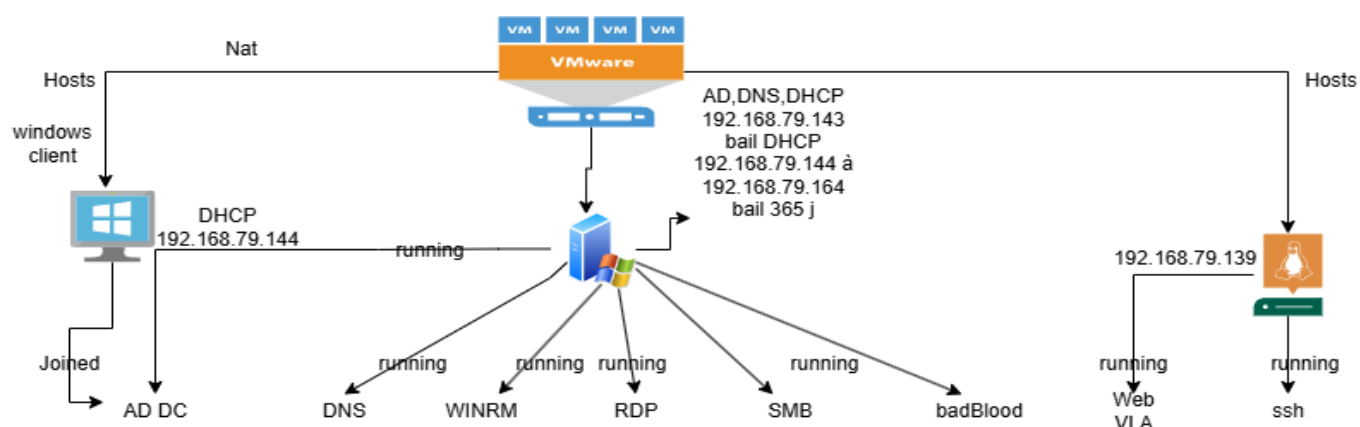
Projet : Lab vulnérable (Windows AD + Linux)

1. Résumé

Ce DAT décrit le déploiement d'un laboratoire reproduisant un service d'entreprise avec un contrôleur de domaine Windows server 2022, un pc client Windows 10 et un serveur Linux hébergeant l'application VulnerableLightApp. L'objectif est de fournir un environnement réaliste et vulnérable pour des exercices d'audit.

2. Contexte et objectifs

- Objectifs pédagogiques du Lab (déploiement et installation des machines comme demandé.
- Contraintes (vérifier intégrités des iso (Hashs ou Signatures).
- Rappels sécurité (isolement réseau, gestion des mots de passe et snapshot).



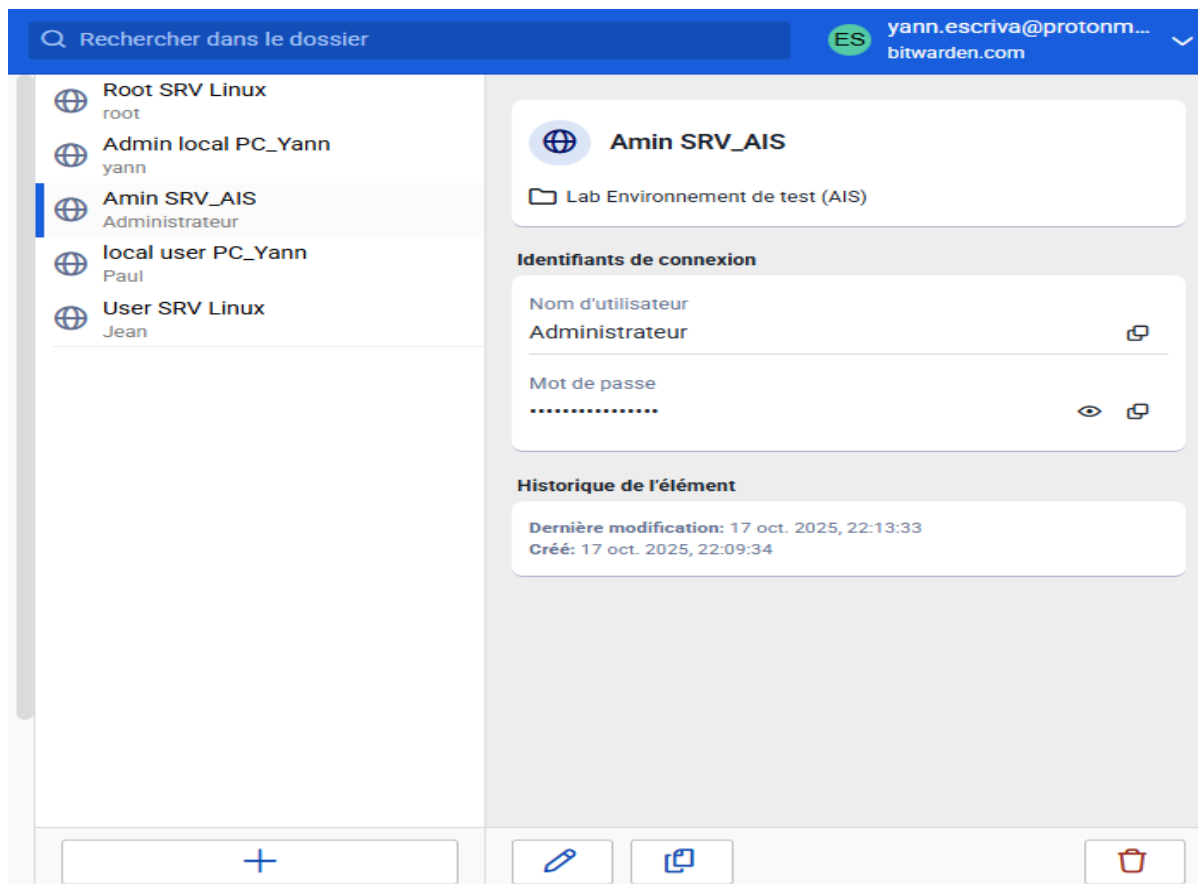
3. Architecture réseau

4. Caractéristiques des machines

Nom VM	Rôle	OS (ISO)	CPU	RAM	Stockage	IP	Notes
SRV-AIS	Contrôleur de domaine	Windows Server 2022 (ISO)	4	4 GB	60 GB	192.168.79.143	AD, DNS, DHCP, WINRM, SMB, RDP, BADBLO OD
PC-yann	Pc-client	Windows 10 (ISO)	4	4 GB	60 GB	192.168.79.144	Joins AD
SRV-Linux	Serveur Web	Debian 12 (ISO)	2	2 GB	20	192.168.79.139	WEB-VLA, SSH

5. Inventaire des comptes à privilèges

Comptes	Rôle	Machine	Emplacement du mdp
Administrateur	Admin du domaine	SRV-AIS	Bitwarden
Local_admin	Admin local	PC_yann	Bitwarden
Local_user	Client	PC_yann	Bitwarden
Root	Admin SRV Linux	SRV_WEB	Bitwarden
SRV_WEB	User SRV Linux	SRV_WEB	Bitwarden



6. Diagramme Projet

DAT_LAB: ENVIRONNEMENT DE TEST

DAT_LAB: ENVIRONNEMENT DE TEST

TÂCHE	DURÉE ESTIMÉE	DÉBUT DU PROJET	FIN DU PROJET	STATUT
Téléchargement Iso et vérification intégrité	1 jour	15 Octobre 2025	15 Octobre 2025	Fait
Création VM	1 jour	15 Octobre 2025	15 Octobre 2025	Fait
Installation contrôleur de domaine (DHCP, DNS, AD DS)	1 jour	15 Octobre 2025	15 Octobre 2025	Fait
Installation Pc client et jointure au domaine	1 demi journée	15 Octobre 2025	15 Octobre 2025	Fait
Installation Serveur Linux avec VLA	1 jour	15 Octobre 2025	15 Octobre 2025	Fait
Configuration services, tests et captures	1 jour	15 Octobre 2025	15 Octobre 2025	Fait
Rédaction DAT et finalisation	2 jours	16 Octobre 2025	17 Octobre 2025	En cours

7. Vérification des images (hashs / signatures)

Hash debian 13

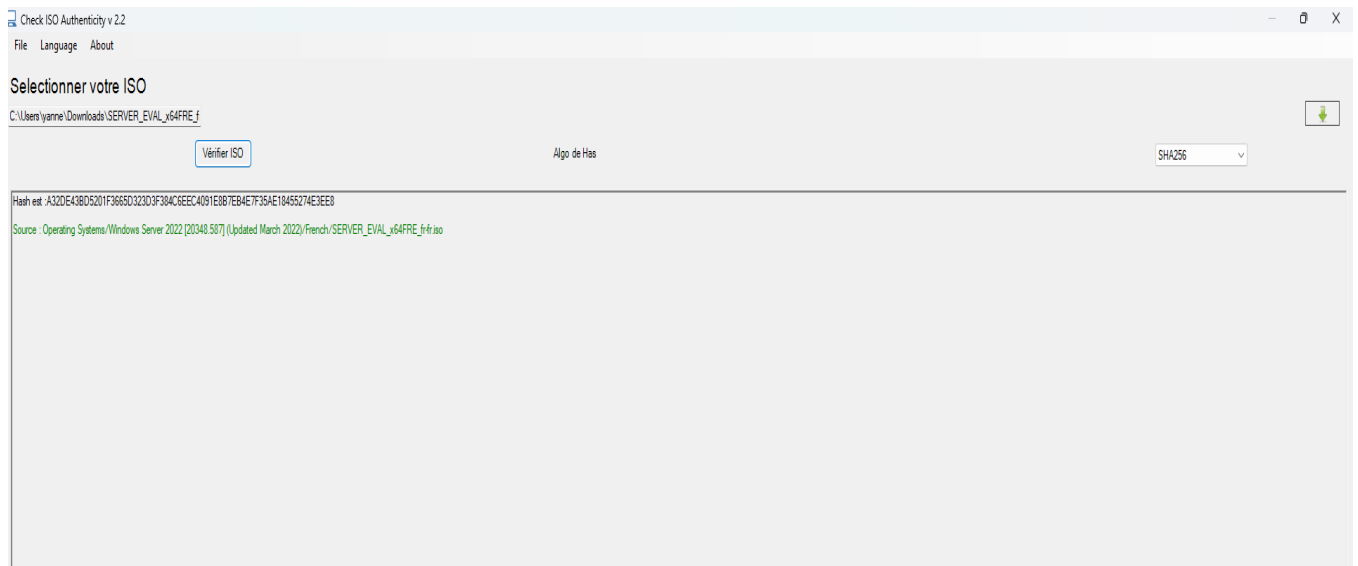
658b28e209b578fe788ec5867deebae57b6aac5fce3692bbb116bab9c65568b3	debian-13.1.0-amd64-netinst.iso
ebfa0ce7fc30917b226c4f2398622933f57a7e6c1dd4ff18e892b4a0944f0136	debian-edu-13.1.0-amd64-netinst.iso
f081cd49a65f8b6e54b60b96ca65f476a3d149205c9f851585f130c36bd1a048	debian-mac-13.1.0-amd64-netinst.iso

```
Windows PowerShell
PS C:\Users\yanne\Downloads> Get-FileHash .\debian-13.1.0-amd64-netinst.iso -Algorithm SHA256 | Format-List

Algorithm : SHA256
Hash      : 658B28E209B578FE788EC5867DEEBAE57B6AAC5FCE3692BBB116BAB9C65568B3
Path      : C:\Users\yanne\Downloads\debian-13.1.0-amd64-netinst.iso

PS C:\Users\yanne\Downloads> "658B28E209B578FE788EC5867DEEBAE57B6AAC5FCE3692BBB116BAB9C65568B3" -eq "658b28e209b578fe788ec5867deebae57b6aac5fce3692bbb116bab9c65568b3"
True
PS C:\Users\yanne\Downloads> |
```

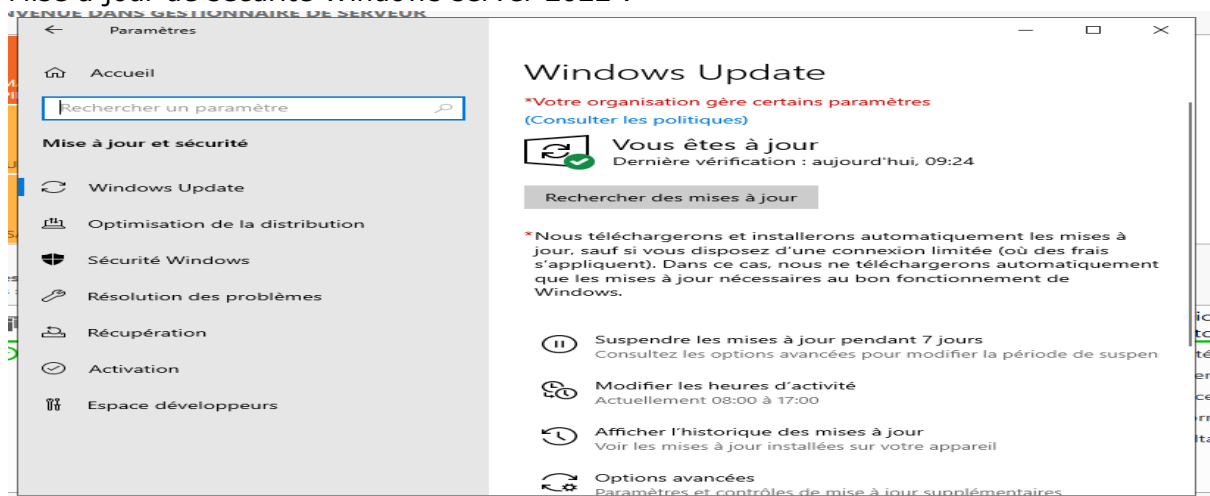
Hash Windows server 2022

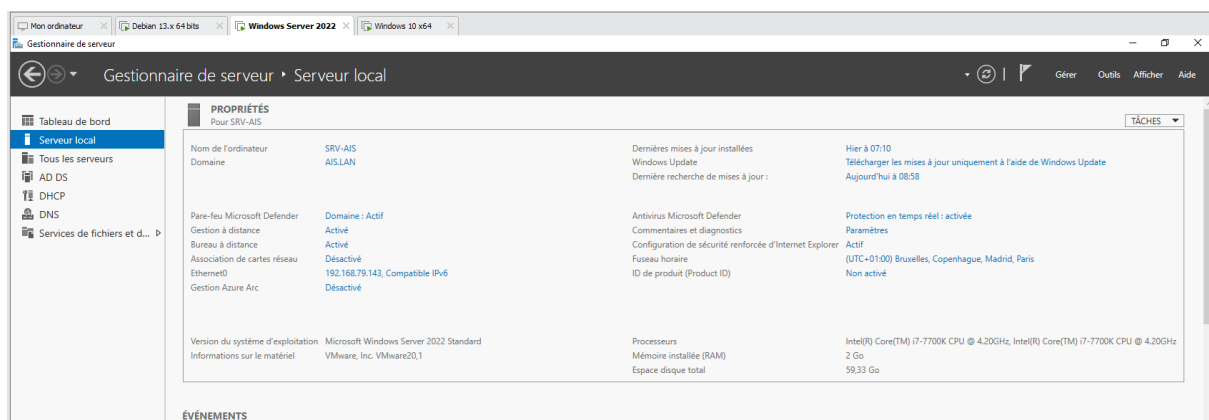
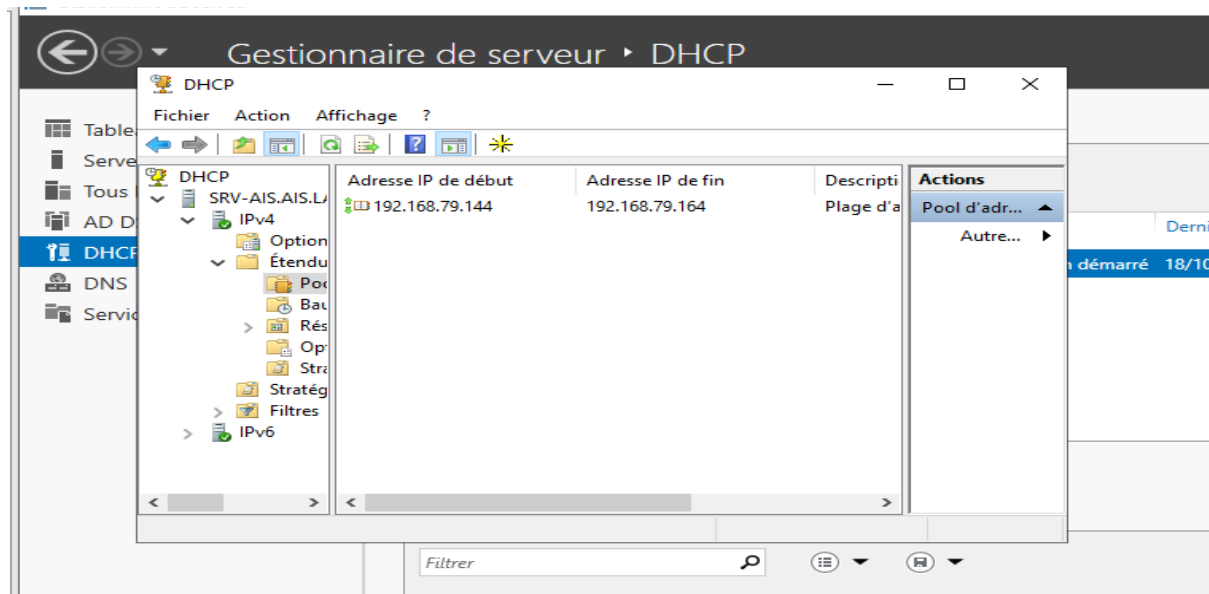
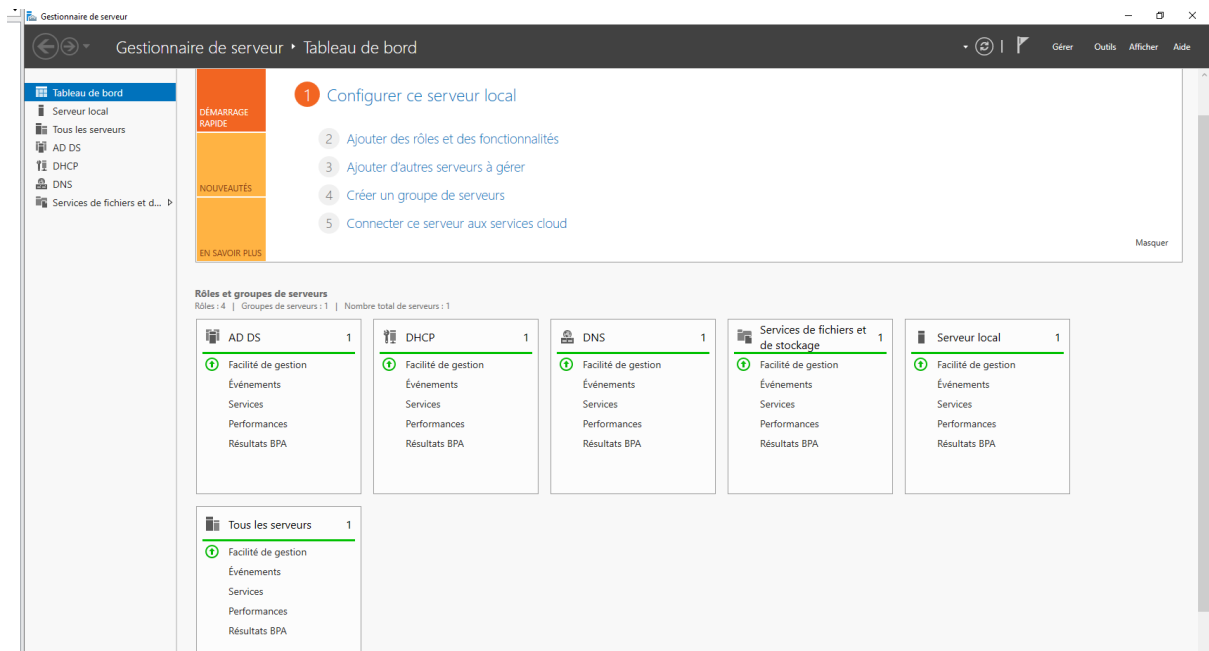


8. Installation et configuration

J'ai installé et configuré mes 3 machines virtuelles sur un hyperviseur de type 2 (VMWare Workstation pro) à savoir Windows server, Windows 10 ainsi que Debian 13. Concernant les 3 machines, j'ai fait les mises à jour de sécurité ainsi qu'installé les VMWare Tools afin d'avoir de meilleurs performances et d'intégrations des VM avec mon hôte. Sur Windows server, j'ai installé mes rôles AD DS, DHCP, DNS et j'ai créé mon domaine (AIS.LAN). J'ai aussi fait mon partage SMB et activé le RDP. J'ai également lancé le script powershell (Badblood) qui permet de rajouter des milliers de comptes dans l'AD. Sur Windows 10, je l'ai joint au domaine et Debian 13, j'ai configuré et activé le SSH. J'ai aussi lancé Vulnerablelightapp qui est une application web volontairement vulnérable, conçue pour l'apprentissage et la pratique de la cybersécurité (tests d'intrusion, analyse de vulnérabilités, sécurisation d'applications, etc.). Elle héberge un serveur web (Kestrel)

Mise à jour de sécurité Windows server 2022 :





Fichier partage SMB :

```
PS C:\Users\Administrateur> Get-ChildItem -Path "C:\Windows\SYSVOL\Share" -Recurse

Répertoire : C:\Windows\SYSVOL\Share

Mode                LastWriteTime         Length Name
----                -
d-----          17/10/2025      12:07      Readonly
d-----          17/10/2025      12:07      Writeaccess

PS C:\Users\Administrateur> _
```

Droits NTFS Readonly :

```
Administrateur: Windows PowerShell
PS C:\Users\Administrateur> Get-Acl -Path "C:\Windows\SYSVOL\Share\Readonly" | Select-Object -ExpandProperty Access

FileSystemRights : ReadAndExecute, Synchronize
AccessControlType : Allow
IdentityReference : Tout le monde
IsInherited       : False
InheritanceFlags  : ContainerInherit
PropagationFlags   : None

FileSystemRights : Read, Synchronize
AccessControlType : Allow
IdentityReference : Tout le monde
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : CREATEUR PROPRIETAIRE
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : InheritOnly

FileSystemRights : ReadAndExecute, Synchronize
AccessControlType : Allow
IdentityReference : AUTORITE NT\Utilisateurs authentifiés
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : AUTORITE NT\Système
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : BUILTIN\Administrateurs
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

FileSystemRights : ReadAndExecute, Synchronize
AccessControlType : Allow
IdentityReference : BUILTIN\Opérateurs de serveur
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None
```

Droits NTFS Writeaccess :

```
PS C:\Users\Administrateur> Get-Acl -Path "C:\Windows\SYSVOL\Share\Writeaccess" | Select-Object -ExpandProperty Access

FileSystemRights : Write, ReadAndExecute, Synchronize
AccessControlType : Allow
IdentityReference : Tout le monde
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : CREATEUR PROPRIETAIRE
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : InheritOnly

FileSystemRights : ReadAndExecute, Synchronize
AccessControlType : Allow
IdentityReference : AUTORITE NT\Utilisateurs authentifiés
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

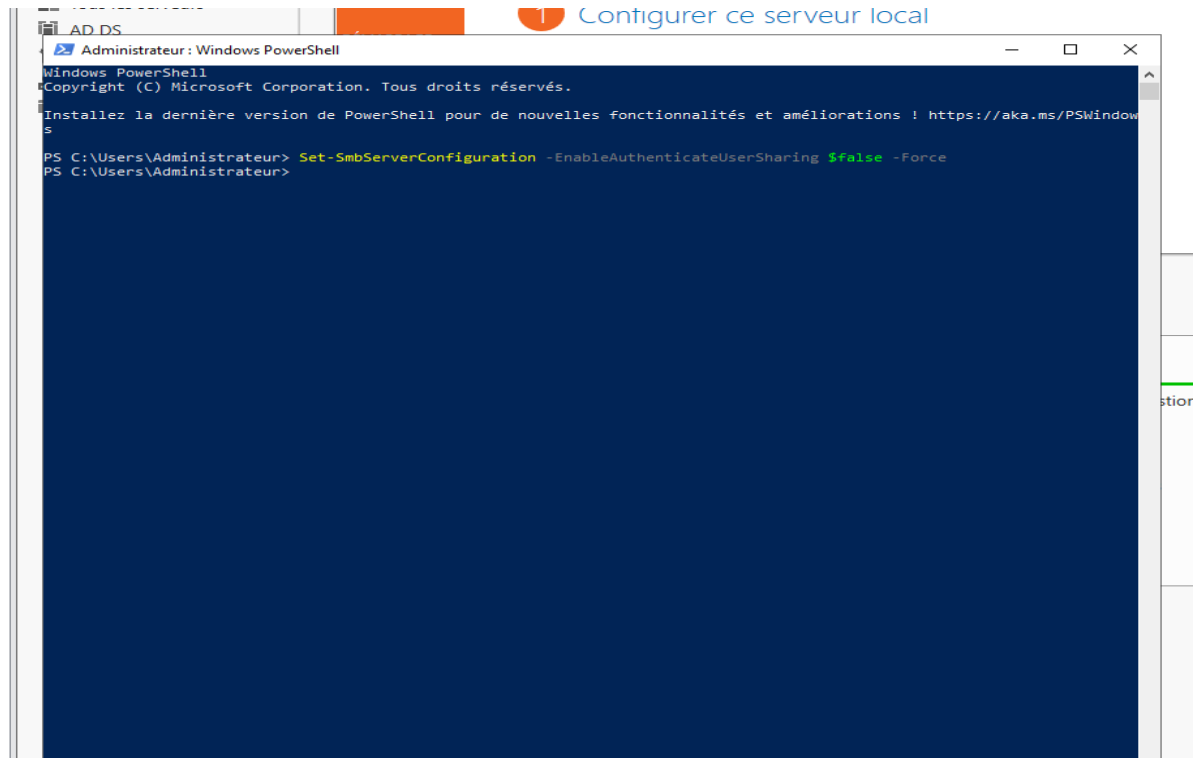
FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : AUTORITE NT\Système
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : BUILTIN\Administrateurs
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

FileSystemRights : ReadAndExecute, Synchronize
AccessControlType : Allow
IdentityReference : BUILTIN\Opérateurs de serveur
IsInherited       : False
InheritanceFlags  : ContainerInherit, ObjectInherit
PropagationFlags   : None

FileSystemRights : FullControl
AccessControlType : Allow
IdentityReference : AIS\Administrateur
IsInherited       : False
```

Partage sans authentification :



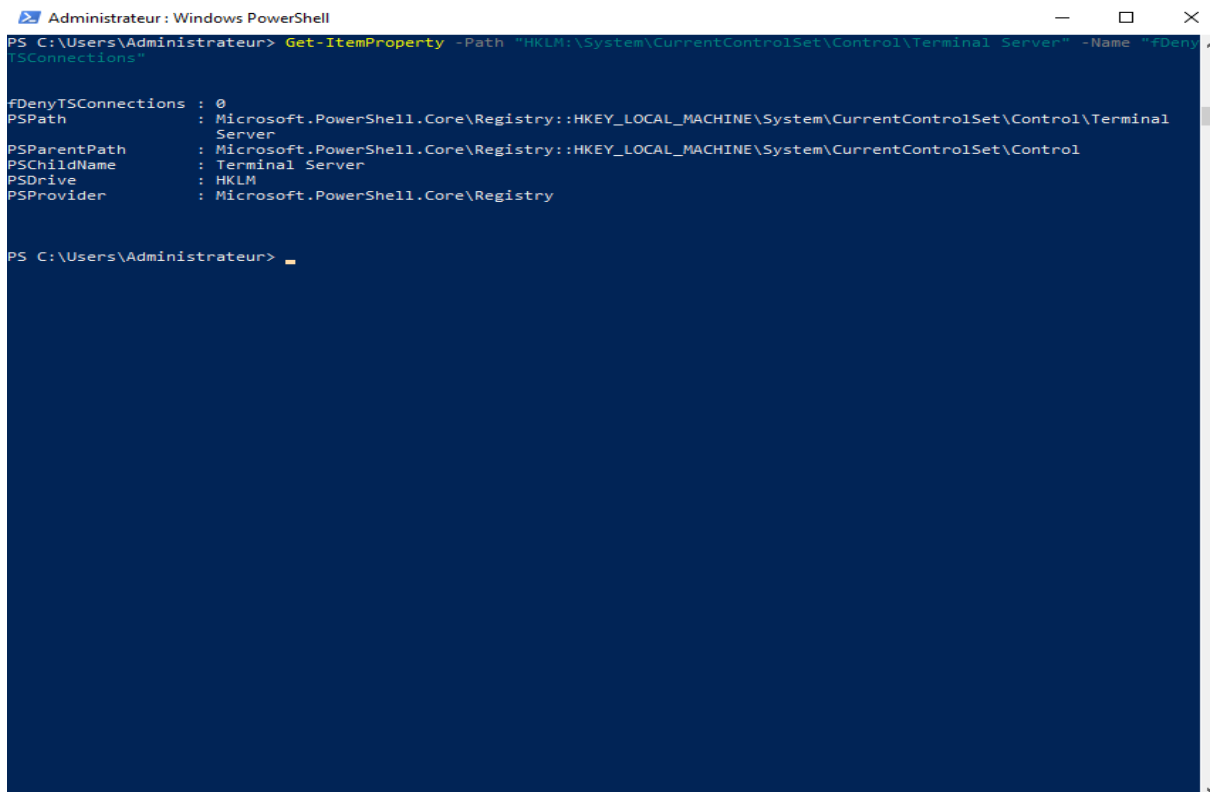
The screenshot shows a Windows PowerShell window titled "Administrateur : Windows PowerShell". The window contains the following text:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Installez la dernière version de PowerShell pour de nouvelles fonctionnalités et améliorations ! https://aka.ms/PSWindows

PS C:\Users\Administrateur> Set-SmbServerConfiguration -EnableAuthenticateUserSharing $false -Force
PS C:\Users\Administrateur>
```

Statut RDP Windows server :



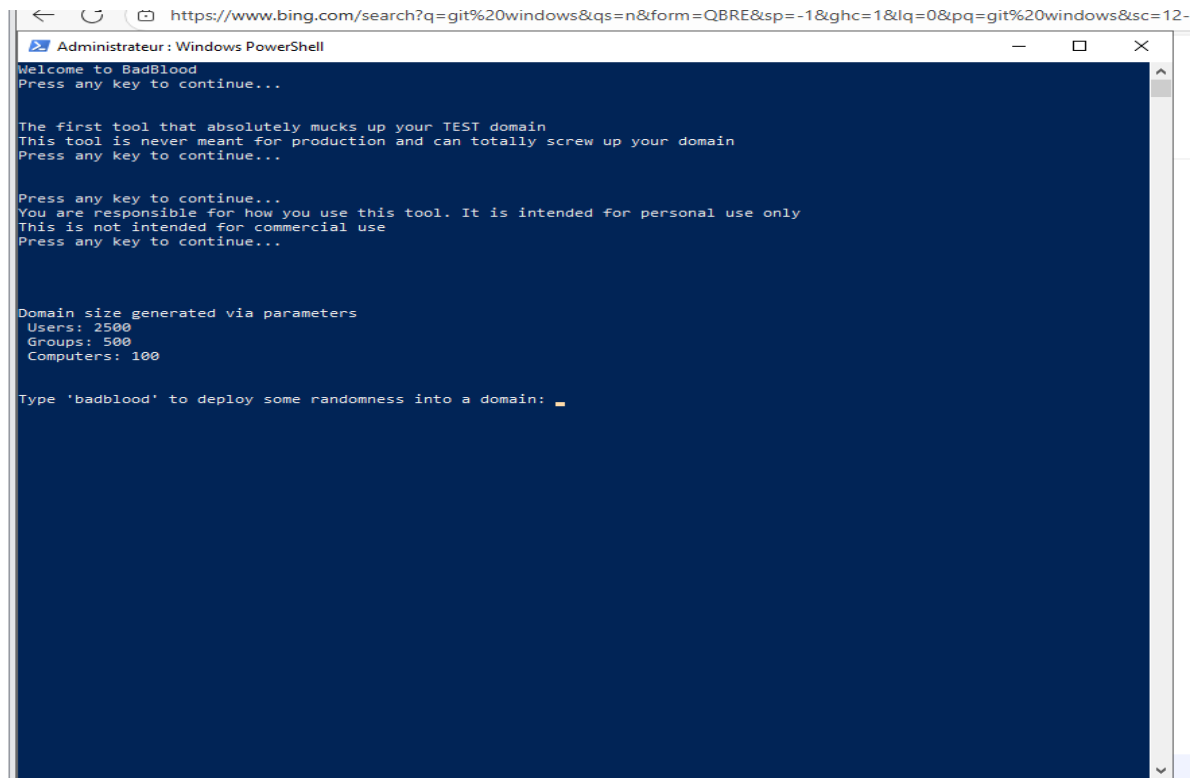
The screenshot shows a Windows PowerShell window titled "Administrateur : Windows PowerShell". The window contains the following text:

```
PS C:\Users\Administrateur> Get-ItemProperty -Path "HKLM:\System\CurrentControlSet\Control\Terminal Server" -Name "fDenyTSConnections"

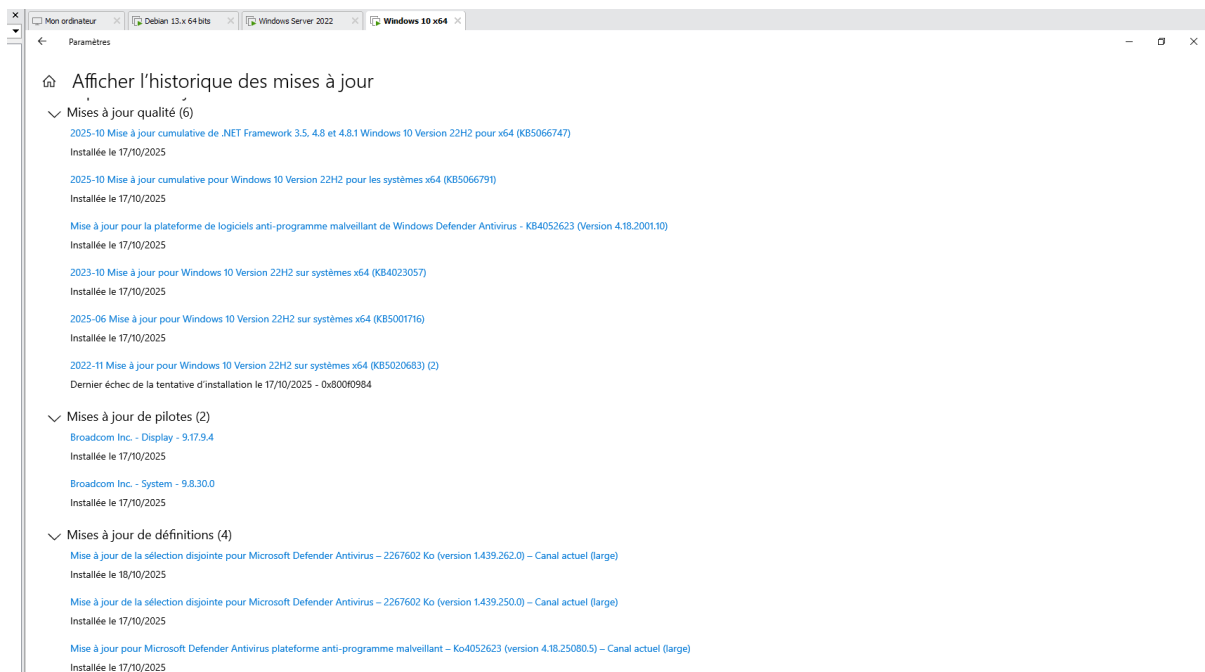
fDenyTSConnections : 0
PSPath              : Microsoft.PowerShell.Core\Registry::HKLM_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal
                    Server
PSParentPath        : Microsoft.PowerShell.Core\Registry::HKLM_LOCAL_MACHINE\System\CurrentControlSet\Control
PSChildName         : Terminal Server
PSDrive             : HKLM
PSProvider          : Microsoft.PowerShell.Core\Registry

PS C:\Users\Administrateur>
```

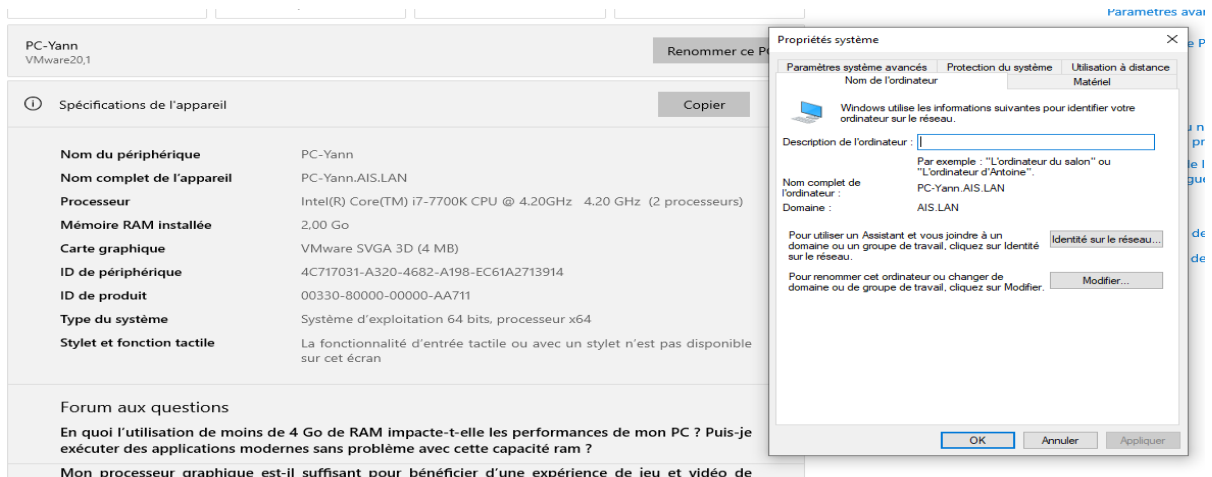

Lancement du script BadBlood :



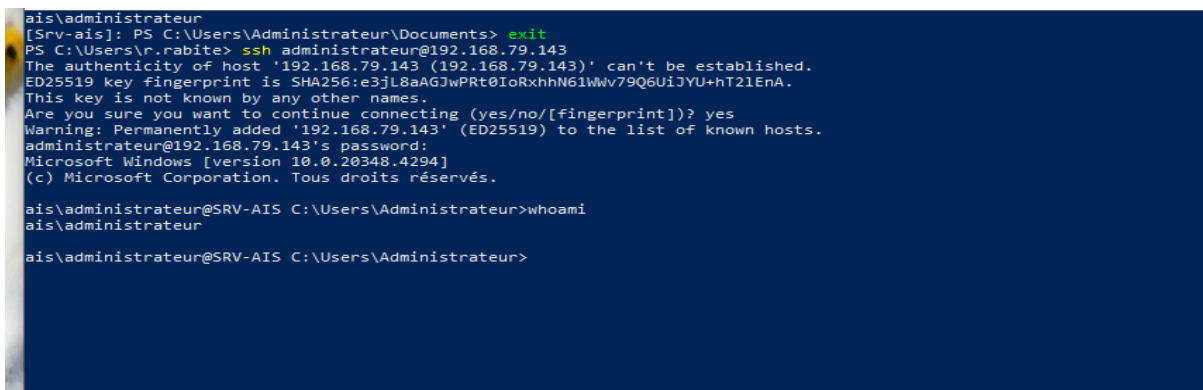
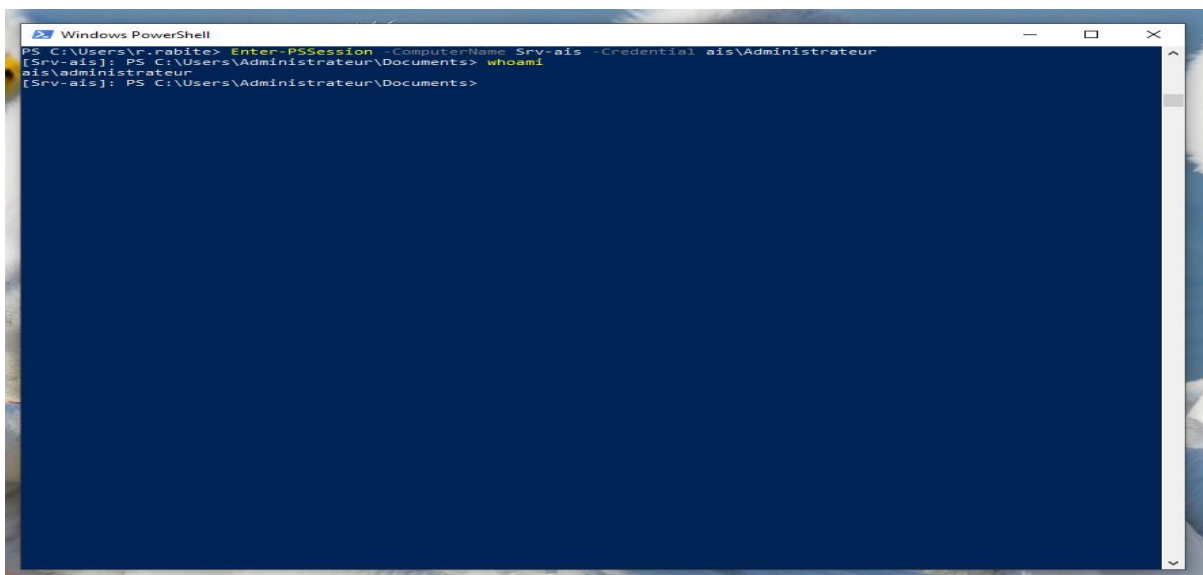
Mise à jour de sécurité Windows 10 :



Windows 10 au domaine :



Connexion winrm et ssh réussi du pc client à l'AD :



Mise à jour de sécurité Debian 13 :

```
yann@debian: ~  
yann@debian:~$ sudo apt update && sudo apt upgrade  
Atteint : 1 http://security.debian.org/debian-security trixie-security InRelease  
Atteint : 2 http://deb.debian.org/debian trixie InRelease  
Atteint : 3 http://deb.debian.org/debian trixie-updates InRelease  
Atteint : 4 https://packages.microsoft.com/debian/12/prod bookworm InRelease  
Tous les paquets sont à jour.  
Attention : https://packages.microsoft.com/debian/12/prod/dists/bookworm/InRelease: Policy will reject signature within a year, see --audit for details  
Sommaire :  
  Mise à niveau de : 0. Installation de : 0Supprimé : 0. Non mis à jour : 0  
yann@debian:~$
```

Statut SSH :

```
yann@debian: ~  
yann@debian:~$ systemctl status ssh  
● ssh.service - OpenBSD Secure Shell server  
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: enab>  
   Active: active (running) since Sat 2025-10-18 09:11:53 CEST; 5min ago  
  Invocation: 07b0f410746c4109a9682c3109e8c0f4  
     Docs: man:sshd(8)  
           man:sshd_config(5)  
  Process: 1179 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)  
 Main PID: 1212 (sshd)  
    Tasks: 1 (limit: 2236)  
  Memory: 2.9M (peak: 3.3M)  
     CPU: 36ms  
   CGroup: /system.slice/ssh.service  
           └─1212 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"  
  
Warning: some journal files were not opened due to insufficient permissions.  
lines 1-15/15 (END)
```

Serveur-Web Linux VulnerableLightApp :

```
yann@debian: ~/VulnerableLightApp
yann@debian:~$ ls
Bureau      Modèles      Public      VulnerableLightApp
Documents   Musique      Téléchargements
Images      packages-microsoft-prod.deb  Vidéos
yann@debian:~$ cd VulnerableLightApp
yann@debian:~/VulnerableLightApp$ ls
appsettings.Development.json  LICENSE      README.md
appsettings.json              LogoVLA.png  SECURITY.md
Controller                   MidlWare     TestCpu
Dockerfile                   Model        Update
english                      nlog.config  VLAusecase.drawio
francais                     Program.cs    VulnerableWebApplication.csproj
Identity                     Properties   VulnerableWebApplication.sln
yann@debian:~/VulnerableLightApp$
```



Nombre d'utilisateurs contenus dans l'AD :

```
PS C:\Users\Administrateur> (Get-ADUser -Filter *).Count
2491
PS C:\Users\Administrateur>
```

Liste des comptes critiques de l'AD :

SamAccountName	Nom Kerberos (UPN)	Date création	Actif	AdminCount	Critiques	Groupes
Administrateur		17/10/2025 08:01	True	1	Oui	CN=MA-hot-distlist1,OU=T0-Permissions,OU=Tier 0,OU=Admin,DC=AIS,DC=LAN
krbtgt		17/10/2025 08:02	False	1	Oui	CN=EA-mam-distlist1,OU=ITS,OU=People,DC=AIS,DC=LAN
MARIA_DOUGLAS	MARIA_DOUGLAS@AIS.LAN	17/10/2025 13:22	True	1	Oui	CN=DO-chacharit-distlist1,OU=ServiceAccounts,OU=AWS,OU=Tier 2,DC=AIS,DC=LAN
GINA_PERKINS	GINA_PERKINS@AIS.LAN	17/10/2025 13:22	True		Oui	CN=EL-DAN-distlist1,OU=Test,OU=HRE,OU=Tier 1,DC=AIS,DC=LAN
MARCELLA_HARRINGTON	MARCELLA_HARRINGTON@AIS.LAN	17/10/2025 13:22	True		Oui	
ELLA_LONG	ELLA_LONG@AIS.LAN	17/10/2025 13:22	True		Oui	CN=MA-m20-admingroup1,OU=ServiceAccounts,OU=ITS,OU=Tier 2,DC=AIS,DC=LAN
LUCILE_KIRK	LUCILE_KIRK@AIS.LAN	17/10/2025 13:22	True		Oui	CN=AN-gal-distlist1,OU=BDE,OU=Tier 1,DC=AIS,DC=LAN
MARION_HENDERSON	MARION_HENDERSON@AIS.LAN	17/10/2025 13:23	True		Oui	CN=MA-seg-distlist1,OU=ITS,OU=Stage,DC=AIS,DC=LAN
DEREK_SILVA	DEREK_SILVA@AIS.LAN	17/10/2025 13:23	True		Oui	
ROSARIO_FIGUEROA	ROSARIO_FIGUEROA@AIS.LAN	17/10/2025 13:23	True		Oui	CN=TO-AUTOMOVIL-distlist1,OU=Groups,OU=BDE,OU=Stage,DC=AIS,DC=LAN
DERRICK_CHARLES	DERRICK_CHARLES@AIS.LAN	17/10/2025 13:23	True		Oui	CN=MA-TrO-distlist1,OU=Tier 0,OU=Admin,DC=AIS,DC=LAN
PEARLIE_GAMBLE	PEARLIE_GAMBLE@AIS.LAN	17/10/2025 13:23	True	1	Oui	CN=CA-123-distlist1,OU=Groups,OU=HRE,OU=Stage,DC=AIS,DC=LAN
JOSEF_CLINE	JOSEF_CLINE@AIS.LAN	17/10/2025 13:23	True		Oui	CN=AB-101236179-distlist1,OU=FIN,OU=Tier 2,DC=AIS,DC=LAN
ELBERT_RAMOS	ELBERT_RAMOS@AIS.LAN	17/10/2025 13:23	True		Oui	CN=SA-mamayapa-distlist1,OU=BDE,OU=Stage,DC=AIS,DC=LAN
SHANA_ADKINS	SHANA_ADKINS@AIS.LAN	17/10/2025 13:23	True	1	Oui	CN=Opérateurs de compte,CN=Builtin,DC=AIS,DC=LAN
WALTER_OWENS	WALTER_OWENS@AIS.LAN	17/10/2025 13:23	True		Oui	CN=ED-TETEVON22-distlist1,OU=FSR,OU=Tier 1,DC=AIS,DC=LAN
JUANITA_FROST	JUANITA_FROST@AIS.LAN	17/10/2025 13:23	True		Oui	CN=BR-a37-distlist1,OU=Devices,OU=OGC,OU=Stage,DC=AIS,DC=LAN
NORBERTO_KNIGHT	NORBERTO_KNIGHT@AIS.LAN	17/10/2025 13:23	True	1	Oui	CN=VE-gab-distlist1,OU=ITS,OU=Tier 2,DC=AIS,DC=LAN
WENDELL_SLOAN	WENDELL_SLOAN@AIS.LAN	17/10/2025 13:23	True		Oui	CN=MA-seg-distlist1,OU=ITS,OU=Stage,DC=AIS,DC=LAN
BRICE_CURRY	BRICE_CURRY@AIS.LAN	17/10/2025 13:23	True		Oui	CN=CH-Zac-distlist1,OU=T2-Roles,OU=Tier 2,OU=Admin,DC=AIS,DC=LAN
MARGARITA_KNOX	MARGARITA_KNOX@AIS.LAN	17/10/2025 13:24	True		Oui	
JOSHUA_COCHRAN	JOSHUA_COCHRAN@AIS.LAN	17/10/2025 13:24	True		Oui	CN=MU-sla-distlist1,OU=Test,OU=TST,OU=Stage,DC=AIS,DC=LAN
SYBIL_POOLE	SYBIL_POOLE@AIS.LAN	17/10/2025 13:24	True		Oui	CN=OR-bat-distlist1,OU=Test,OU=ESM,OU=Tier 1,DC=AIS,DC=LAN
ANNE_NORMAN	ANNE_NORMAN@AIS.LAN	17/10/2025 13:24	True		Oui	CN=GA-hermosa07-distlist1,OU=ServiceAccounts,OU=ITS,OU=Tier 1,DC=AIS,DC=LAN
GARLAND_HINES	GARLAND_HINES@AIS.LAN	17/10/2025 13:24	True	1	Oui	CN=Administrateurs clés,CN=Users,DC=AIS,DC=LAN
KIMBERLEY_FRENCH	KIMBERLEY_FRENCH@AIS.LAN	17/10/2025 13:24	True		Oui	CN=MA-hot-distlist1,OU=T0-Permissions,OU=Tier 0,OU=Admin,DC=AIS,DC=LAN
LEONARDO_FLOWERS	LEONARDO_FLOWERS@AIS.LAN	17/10/2025 13:24	True		Oui	CN=MA-973-admingroup1,OU=Deprovisioned,OU=People,DC=AIS,DC=LAN
KEVIN_VANG	KEVIN_VANG@AIS.LAN	17/10/2025 13:24	True		Oui	CN=AN-kaj-distlist1,OU=Test,OU=SEC,OU=Tier 1,DC=AIS,DC=LAN
CARLENE_HOLMES	CARLENE_HOLMES@AIS.LAN	17/10/2025 13:24	True	1	Oui	CN=RA-cynthia69-distlist1,OU=ServiceAccounts,OU=AWS,OU=Tier 1,DC=AIS,DC=LAN
FAUSTINO_BENSON	FAUSTINO_BENSON@AIS.LAN	17/10/2025 13:24	True		Oui	CN=CH-4ju-distlist1,OU=Devices,OU=FIN,OU=Tier 1,DC=AIS,DC=LAN
ALEXANDER_ADKINS	ALEXANDER_ADKINS@AIS.LAN	17/10/2025 13:24	True		Oui	CN=VI-tresbecer-admingroup1,OU=HRE,OU=People,DC=AIS,DC=LAN
PAULETTE_HANSON	PAULETTE_HANSON@AIS.LAN	17/10/2025 13:24	True	1	Oui	CN=LY-libra1510-distlist1,OU=T1-Servers,OU=Tier 1,OU=Admin,DC=AIS,DC=LAN
ISABEL_ALBERT	ISABEL_ALBERT@AIS.LAN	17/10/2025 13:24	True	1	Oui	CN=EL-kee-distlist1,OU=OGC,OU=Tier 2,DC=AIS,DC=LAN
ANTOINETTE_JENSEN	ANTOINETTE_JENSEN@AIS.LAN	17/10/2025 13:24	True	1	Oui	CN=GL-babigiant-admingroup1,OU=Groups,OU=SEC,OU=Tier 1,DC=AIS,DC=LAN
LAKEISHA_SUAREZ	LAKEISHA_SUAREZ@AIS.LAN	17/10/2025 13:25	True	1	Oui	CN=CR-701-distlist1,OU=Tier 1,DC=AIS,DC=LAN
TROY_LUNA	TROY_LUNA@AIS.LAN	17/10/2025 13:25	True		Oui	CN=LE-cen-distlist1,OU=Groups,OU=FIN,OU=Tier 1,DC=AIS,DC=LAN
CLAIR_EVANS	CLAIR_EVANS@AIS.LAN	17/10/2025 13:25	True	1	Oui	CN=DO-karolmi13-distlist1,OU=Devices,OU=SEC,OU=Stage,DC=AIS,DC=LAN
JACKLYN_LANGLEY	JACKLYN_LANGLEY@AIS.LAN	17/10/2025 13:25	True	1	Oui	CN=KR-rev-distlist1,OU=Devices,OU=ITS,OU=Stage,DC=AIS,DC=LAN
CATHERINE POLLARD	CATHERINE_POLLARD@AIS.LAN	17/10/2025 13:25	True		Oui	CN=93-SKD-distlist1,OU=ServiceAccounts,OU=AWS,OU=Tier 2,DC=AIS,DC=LAN
ALLYSON_GONZALEZ	ALLYSON_GONZALEZ@AIS.LAN	17/10/2025 13:25	True		Oui	CN=MA-seg-distlist1,OU=ITS,OU=Stage,DC=AIS,DC=LAN
JIMMIE_GILLESPIE	JIMMIE_GILLESPIE@AIS.LAN	17/10/2025 13:25	True		Oui	CN=BR-a37-distlist1,OU=Devices,OU=OGC,OU=Stage,DC=AIS,DC=LAN
PRISCILLA_LYNN	PRISCILLA_LYNN@AIS.LAN	17/10/2025 13:25	True		Oui	CN=DO-karolmi13-distlist1,OU=Devices,OU=SEC,OU=Stage,DC=AIS,DC=LAN
TORY_OTH	TORY_OTH@AIS.LAN	17/10/2025 13:25	True		Oui	CN=MI-69_-distlist1,OU=Devices,OU=FSR,OU=Tier 1,DC=AIS,DC=LAN
HAZEL_BURKS	HAZEL_BURKS@AIS.LAN	17/10/2025 13:25	True	1	Oui	CN=SA-khadyiouf-distlist1,OU=AWS,OU=People,DC=AIS,DC=LAN
DIXIE_SINGLETON	DIXIE_SINGLETON@AIS.LAN	17/10/2025 13:25	True		Oui	CN=TO-ANGIE1234-admingroup1,OU=T2-Accounts,OU=Tier 2,OU=Admin,DC=AIS,DC=LAN
DEENA_CHAMBERS	DEENA_CHAMBERS@AIS.LAN	17/10/2025 13:25	True		Oui	CN=ED-tea-distlist1,OU=Groups,OU=ITS,OU=Stage,DC=AIS,DC=LAN
BORIS_ODONNELL	BORIS_ODONNELL@AIS.LAN	17/10/2025 13:25	True		Oui	CN=AM-ArTuRo006-distlist1,OU=Test,OU=SEC,OU=Stage,DC=AIS,DC=LAN
BOBBIE_SOSA	BOBBIE_SOSA@AIS.LAN	17/10/2025 13:25	True	1	Oui	CN=JO-ulanazeri-distlist1,OU=ServiceAccounts,OU=OGC,OU=Tier 2,DC=AIS,DC=LAN
GARY_MCINTYRE	GARY_MCINTYRE@AIS.LAN	17/10/2025 13:25	True	1	Oui	CN=Administrateurs clés,CN=Users,DC=AIS,DC=LAN
LACEY_TALLEY	LACEY_TALLEY@AIS.LAN	17/10/2025 13:25	True		Oui	CN=WI-4al-distlist1,OU=ITS,OU=Stage,DC=AIS,DC=LAN
JERI_SELLERS	JERI_SELLERS@AIS.LAN	17/10/2025 13:26	True		Oui	CN=MO-pea-distlist1,OU=T2-Permissions,OU=Tier 2,OU=Admin,DC=AIS,DC=LAN
ROSARIO CARTER	ROSARIO_CARTER@AIS.LAN	17/10/2025 13:26	True		Oui	CN=CA-amo-distlist1,OU=ServiceAccounts,OU=ESM,OU=Stage,DC=AIS,DC=LAN
DICK_KNIGHT	DICK_KNIGHT@AIS.LAN	17/10/2025 13:26	True		Oui	
NOEMI_MACDONALD	NOEMI_MACDONALD@AIS.LAN	17/10/2025 13:26	True	1	Oui	CN=LA-san-distlist1,OU=OGC,OU=Tier 2,DC=AIS,DC=LAN
KELLY_TALLEY	KELLY_TALLEY@AIS.LAN	17/10/2025 13:26	True	1	Oui	CN=MU-sla-distlist1,OU=Test,OU=TST,OU=Stage,DC=AIS,DC=LAN
CELESTE_CHAN	CELESTE_CHAN@AIS.LAN	17/10/2025 13:26	True	1	Oui	CN=OL-119-admingroup1,OU=ServiceAccounts,OU=AZR,OU=Tier 1,DC=AIS,DC=LAN
LEONA_CASTILLO	LEONA_CASTILLO@AIS.LAN	17/10/2025 13:26	True	1	Oui	CN=NI-golfito20-distlist1,OU=Test,OU=AWS,OU=Tier 2,DC=AIS,DC=LAN
BETHANY_VAUGHN	BETHANY_VAUGHN@AIS.LAN	17/10/2025 13:26	True		Oui	CN=MA-vegarange-admingroup1,OU=ServiceAccounts,OU=OGC,OU=Tier 2,DC=AIS,DC=LAN
LEONEL_HOOPER	LEONEL_HOOPER@AIS.LAN	17/10/2025 13:26	True		Oui	CN=EM-AMOR1234r-distlist1,OU=Devices,OU=OGC,OU=Stage,DC=AIS,DC=LAN
FANNY_AYERS	FANNY_AYERS@AIS.LAN	17/10/2025 13:26	True		Oui	CN=ME-gre-distlist1,OU=T2-Permissions,OU=Tier 2,OU=Admin,DC=AIS,DC=LAN
DELLA_TRUJILLO	DELLA_TRUJILLO@AIS.LAN	17/10/2025 13:26	True		Oui	CN=DA-lacasito1-distlist1,OU=ServiceAccounts,OU=ITS,OU=Stage,DC=AIS,DC=LAN
SANTIAGO_ROACH	SANTIAGO_ROACH@AIS.LAN	17/10/2025 13:26	True		Oui	CN=MU-sla-distlist1,OU=Test,OU=TST,OU=Stage,DC=AIS,DC=LAN
STACY_MORRISON	STACY_MORRISON@AIS.LAN	17/10/2025 13:26	True		Oui	CN=NI-xos-distlist1,OU=Devices,OU=TST,OU=Stage,DC=AIS,DC=LAN
JANELL_SPARKS	JANELL_SPARKS@AIS.LAN	17/10/2025 13:27	True		Oui	CN=JE-atr-admingroup1,OU=ServiceAccounts,OU=FSR,OU=Tier 1,DC=AIS,DC=LAN
IGNACIO_SMITH	IGNACIO_SMITH@AIS.LAN	17/10/2025 13:27	True		Oui	CN=MU-sla-distlist1,OU=Test,OU=TST,OU=Stage,DC=AIS,DC=LAN
LAMONT_BURKE	LAMONT_BURKE@AIS.LAN	17/10/2025 13:27	True	1	Oui	CN=Opérateurs de serveur,CN=Builtin,DC=AIS,DC=LAN
GENEVIEVE_MOSLEY	GENEVIEVE_MOSLEY@AIS.LAN	17/10/2025 13:27	True		Oui	
ANTWAN_WALLS	ANTWAN_WALLS@AIS.LAN	17/10/2025 13:27	True	1	Oui	CN=Admins du domaine,CN=Users,DC=AIS,DC=LAN
LIZA_TRAN	LIZA_TRAN@AIS.LAN	17/10/2025 13:27	True		Oui	CN=CH-REL-admingroup1,OU=ServiceAccounts,OU=OGC,OU=Tier 2,DC=AIS,DC=LAN
CRISTINA_MORSE	CRISTINA_MORSE@AIS.LAN	17/10/2025 13:27	True	1	Oui	CN=Opérateurs de compte,CN=Builtin,DC=AIS,DC=LAN
JOSUE_INGRAM	JOSUE_INGRAM@AIS.LAN	17/10/2025 13:27	True		Oui	CN=ED-TETEVON22-distlist1,OU=FSR,OU=Tier 1,DC=AIS,DC=LAN
IVAN_LARA	IVAN_LARA@AIS.LAN	17/10/2025 13:27	True		Oui	
MIRANDA_BOOKER	MIRANDA_BOOKER@AIS.LAN	17/10/2025 13:27	True		Oui	CN=23-aldo18696-distlist1,OU=Test,OU=SEC,OU=Stage,DC=AIS,DC=LAN

9. Conclusion et retour d'expérience

La mise en place de cet environnement de test m'a permis de reconstituer une architecture réseau complète et réaliste, intégrant les principaux services utilisés en entreprise : Active Directory, DNS, SMB, WinRM, SSH et un service Web.

L'infrastructure, composée d'un contrôleur de domaine Windows Server, d'un poste Client Windows et d'un serveur Linux hébergeant VulnerableLightApp, offre une base fonctionnelle pour la formation et l'analyse de vulnérabilités.

L'exécution du script BadBlood a enrichi le domaine Active Directory avec des comptes et relations typiques d'un réseau d'entreprise, ce qui permet de simuler des scénarios d'attaque et d'audit réalistes.

L'ensemble des services a été vérifié : connexions SSH et WinRM réussies, partages SMB opérationnels avec droits NTFS.

Sur le plan technique, ce projet m'a permis de renforcer mes compétences en administration système Windows et Linux, en gestion des droits NTFS et des comptes AD.

En conclusion, ce laboratoire constitue une base solide pour les futurs audits de sécurité, tests d'exploitation et exercices de pentest.