BRETON Théo

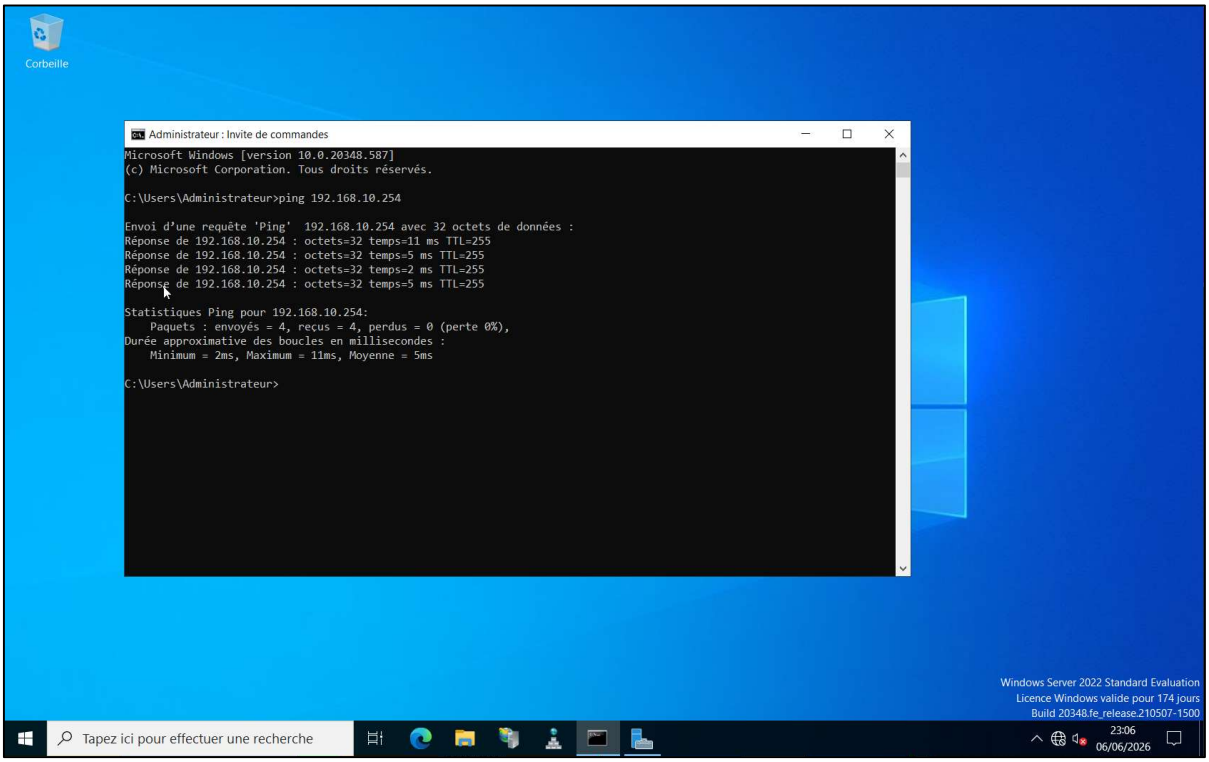
Projet N°5 : PROJET SMARTHOME

Active Directory • DHCP • DNS • RADIUS Cisco • IIS Web Server • FortiGate Security • BGInfo

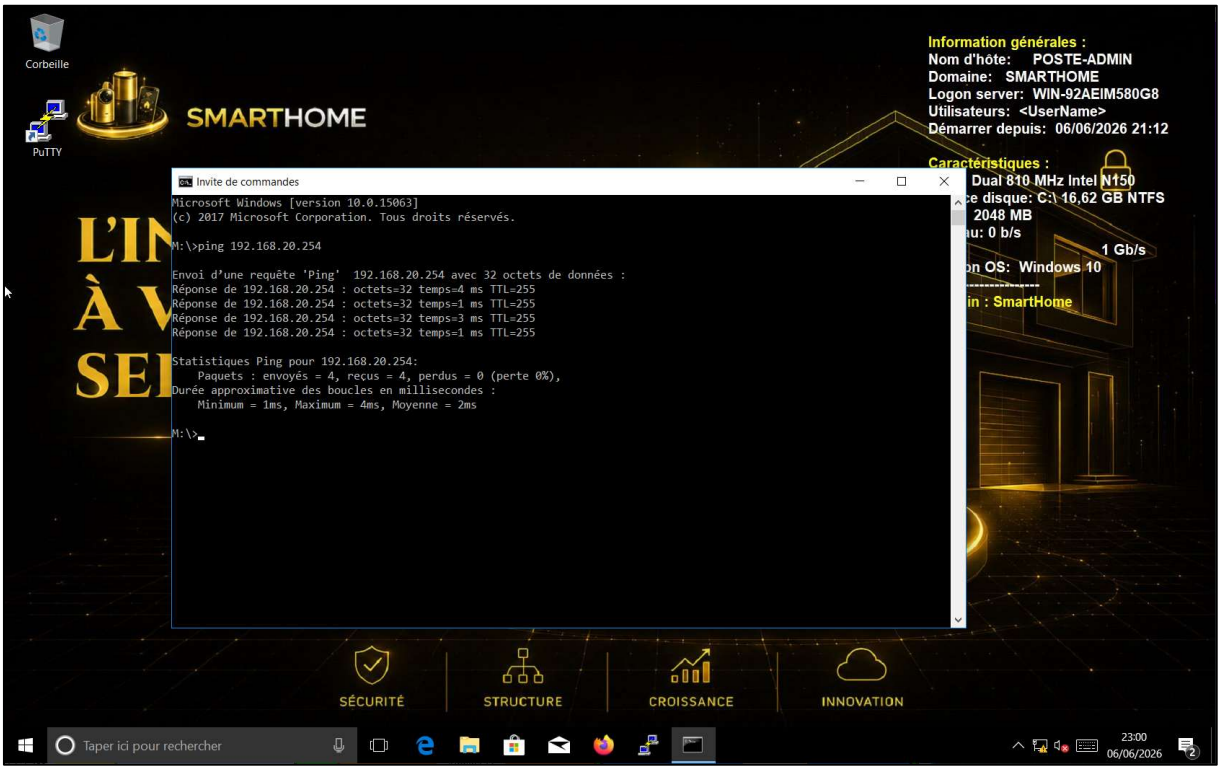
Rapport de Tests

TEST DE COMMUNICATION :

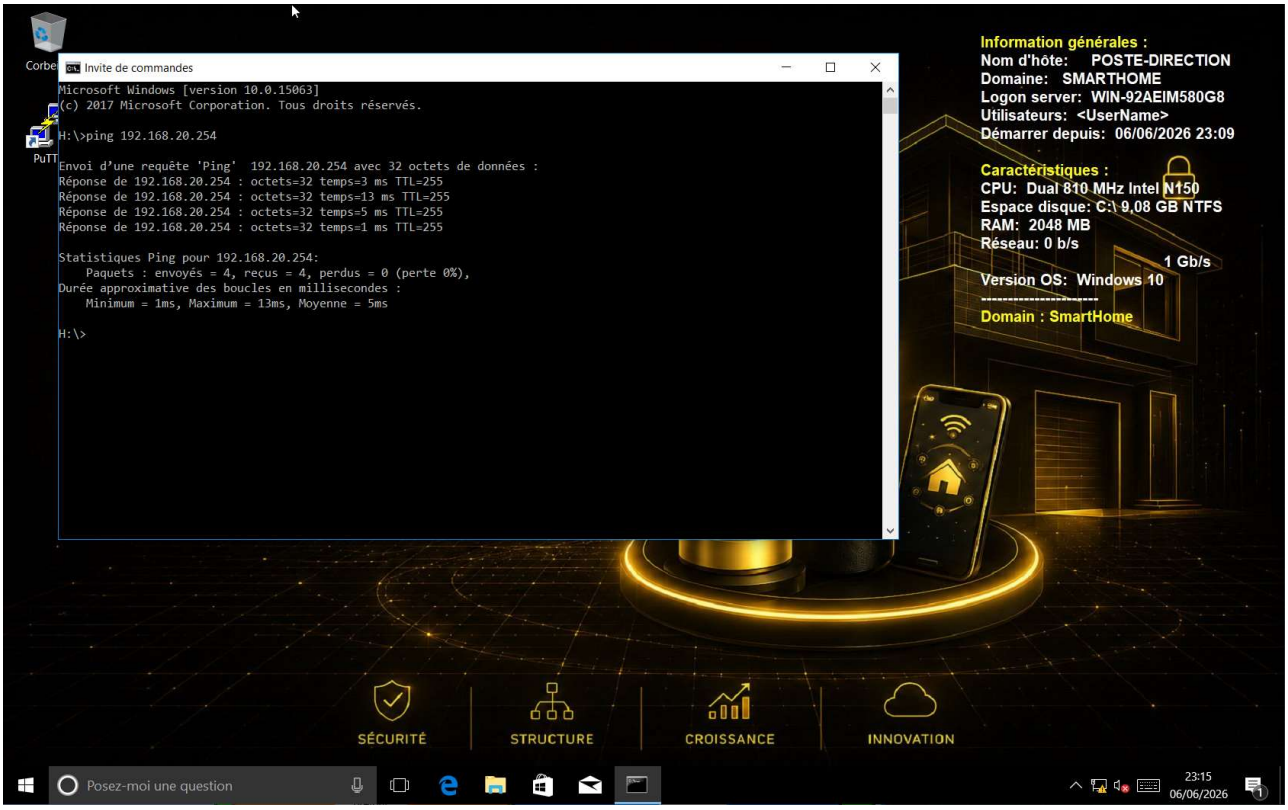
Paquets envoyés depuis	Destinataire	Résultat
TEST COMMUNICATION GATEWAY		
SERV_WEB - 192.168.10.1/24	FORTINET_EVE_NG – 192.168.10.254/24	✅



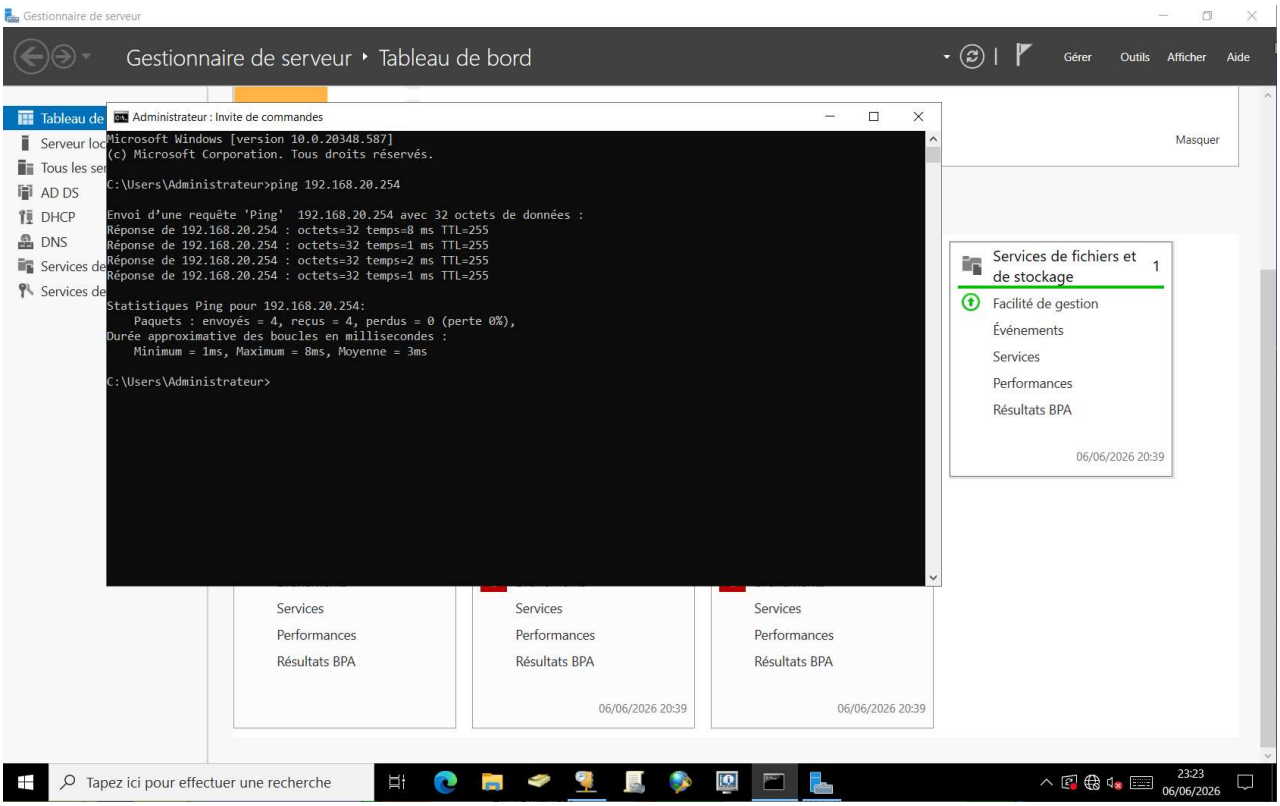
WIN_10_1_ADMIN_RESEAU – 192.168.20.4	FORTINET_EVE_NG – 192.168.10.254/24	✅



WIN_10_2_DIRECTION – 192.168.20.2	FORTINET_EVE_NG – 192.168.10.254/24	



SERV_AD – 192.168.20.1/24	FORTINET_EVE_NG – 192.168.20.254/	



TESTS COMMUNICAITON LABO		
ROUTEUR_CISCO – 172.16.10.253/24	FORTINET_DOMICILE – 172.16.10.254/24	✅

```
Router#ping 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/3/6 ms
```

ROUTEUR_CISCO – 192.168.3.50/24	PCGamer – 192.168.3.4/24	✅

```
Router#ping 192.168.3.4
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.4, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 5/19/38 ms
```

SRV_WEB – 192.168.10.1/24	FORTINET_DOMICILE – 172.16.10.254/24	✅

```
C:\Users\Administrateur>ping 192.168.3.1

Envoi d'une requête 'Ping'  192.168.3.1 avec 32 octets de données :
Réponse de 192.168.3.1 : octets=32 temps=19 ms TTL=253
Réponse de 192.168.3.1 : octets=32 temps=5 ms TTL=253
Réponse de 192.168.3.1 : octets=32 temps=6 ms TTL=253
Réponse de 192.168.3.1 : octets=32 temps=15 ms TTL=253

Statistiques Ping pour 192.168.3.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 19ms, Moyenne = 11ms
```

SRV_WEB – 192.168.10.1/24	ROUTEUR_TP_LINK_DOMICILE – 192.168.3.253/24	✅

```
C:\Users\Administrateur>ping 192.168.3.253

Envoi d'une requête 'Ping'  192.168.3.253 avec 32 octets de données :
Réponse de 192.168.3.253 : octets=32 temps=7 ms TTL=62
Réponse de 192.168.3.253 : octets=32 temps=5 ms TTL=62
Réponse de 192.168.3.253 : octets=32 temps=7 ms TTL=62
Réponse de 192.168.3.253 : octets=32 temps=12 ms TTL=62

Statistiques Ping pour 192.168.3.253:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 5ms, Maximum = 12ms, Moyenne = 7ms
```

PCGamer – 192.168.3.4/24	ROUTEUR_CISCO – 192.168.3.50/24	✅

```
C:\Users\Theo>ping 192.168.3.50

Envoi d'une requête 'Ping'  192.168.3.50 avec 32 octets de données :
Réponse de 192.168.3.50 : octets=32 temps=4 ms TTL=255
Réponse de 192.168.3.50 : octets=32 temps=4 ms TTL=255
Réponse de 192.168.3.50 : octets=32 temps=8 ms TTL=255
Réponse de 192.168.3.50 : octets=32 temps=6 ms TTL=255

Statistiques Ping pour 192.168.3.50:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 4ms, Maximum = 8ms, Moyenne = 5ms

C:\Users\Theo>
```

PCGamer – 192.168.3.4/24	SRV_WEB – 192.168.10.1/24	✅

```
C:\Users\Theo>ping 192.168.10.1

Envoi d'une requête 'Ping'  192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=29 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=12 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=8 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=12 ms TTL=126

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 8ms, Maximum = 29ms, Moyenne = 15ms

C:\Users\Theo>
```

PCGamer – 192.168.3.4/24	Résolution du nom du site web www.smarthome.com	✅

```
C:\Users\Theo>ping www.smarthome.com

Envoi d'une requête 'ping' sur www.smarthome.com [192.168.10.1] avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps=7 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=9 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=8 ms TTL=126
Réponse de 192.168.10.1 : octets=32 temps=12 ms TTL=126

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 7ms, Maximum = 12ms, Moyenne = 9ms

C:\Users\Theo>
```

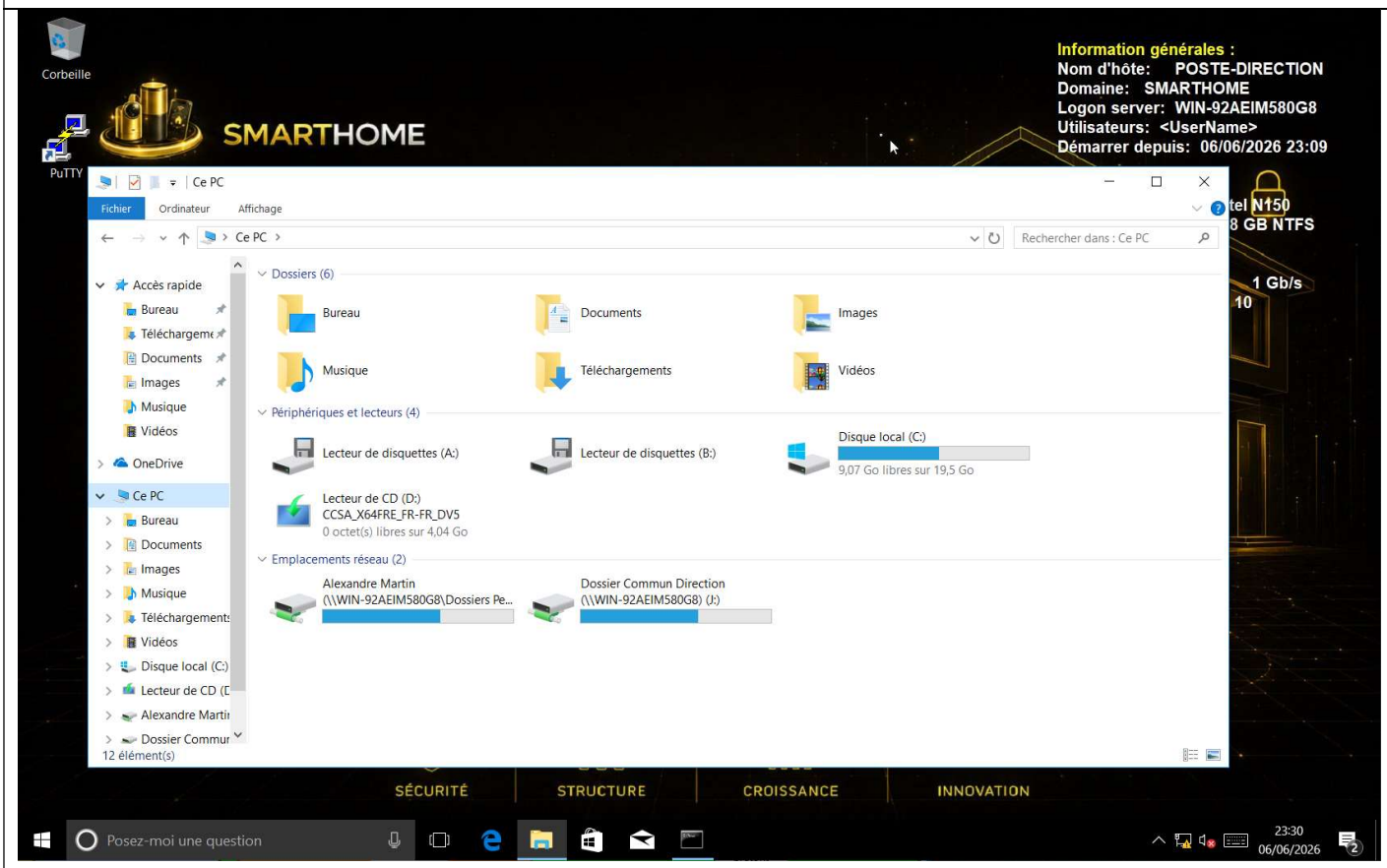
PCGamer – 192.168.3.4/24	Tracert 192.168.10.1 (SRV_WEB)	✅

```
C:\Users\Theo>tracert 192.168.10.1

Détermination de l'itinéraire vers www.smarthome.com [192.168.10.1]
avec un maximum de 30 sauts :

  1     3 ms     2 ms     2 ms  192.168.3.1
  2    24 ms     9 ms    13 ms  192.168.3.50
  3    24 ms     5 ms    12 ms  172.16.10.254
  4     9 ms    12 ms    13 ms  www.smarthome.com [192.168.10.1]

Itinéraire déterminé.

C:\Users\Theo>
```

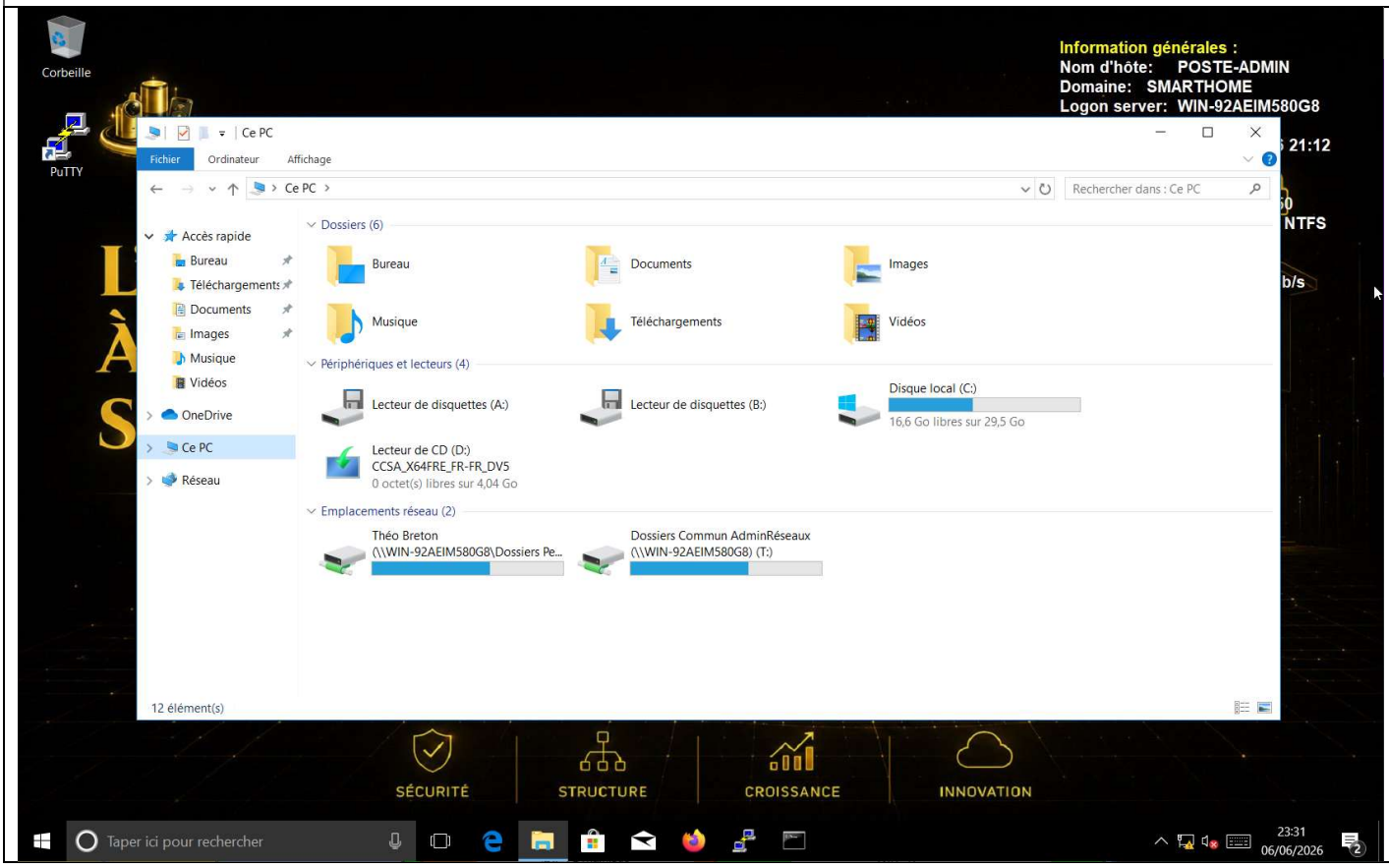
TESTS DE MAPPAGE LECTEUR :

MAPPAGE LECTEUR UTILISATEUR SMARTHOME

WIN_10_1_DIRECTION



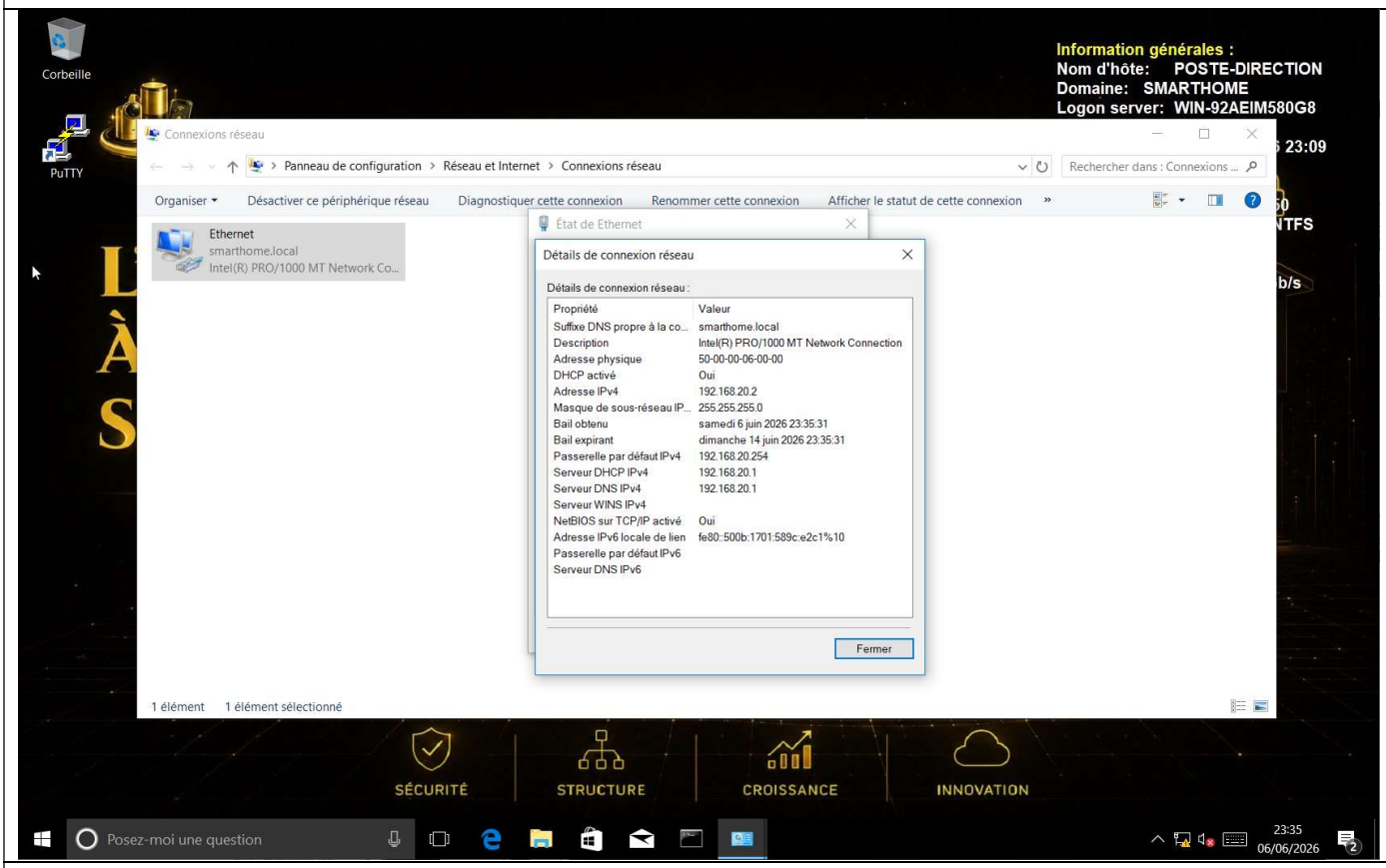
WIN_10_2_ADMINRESEAUX



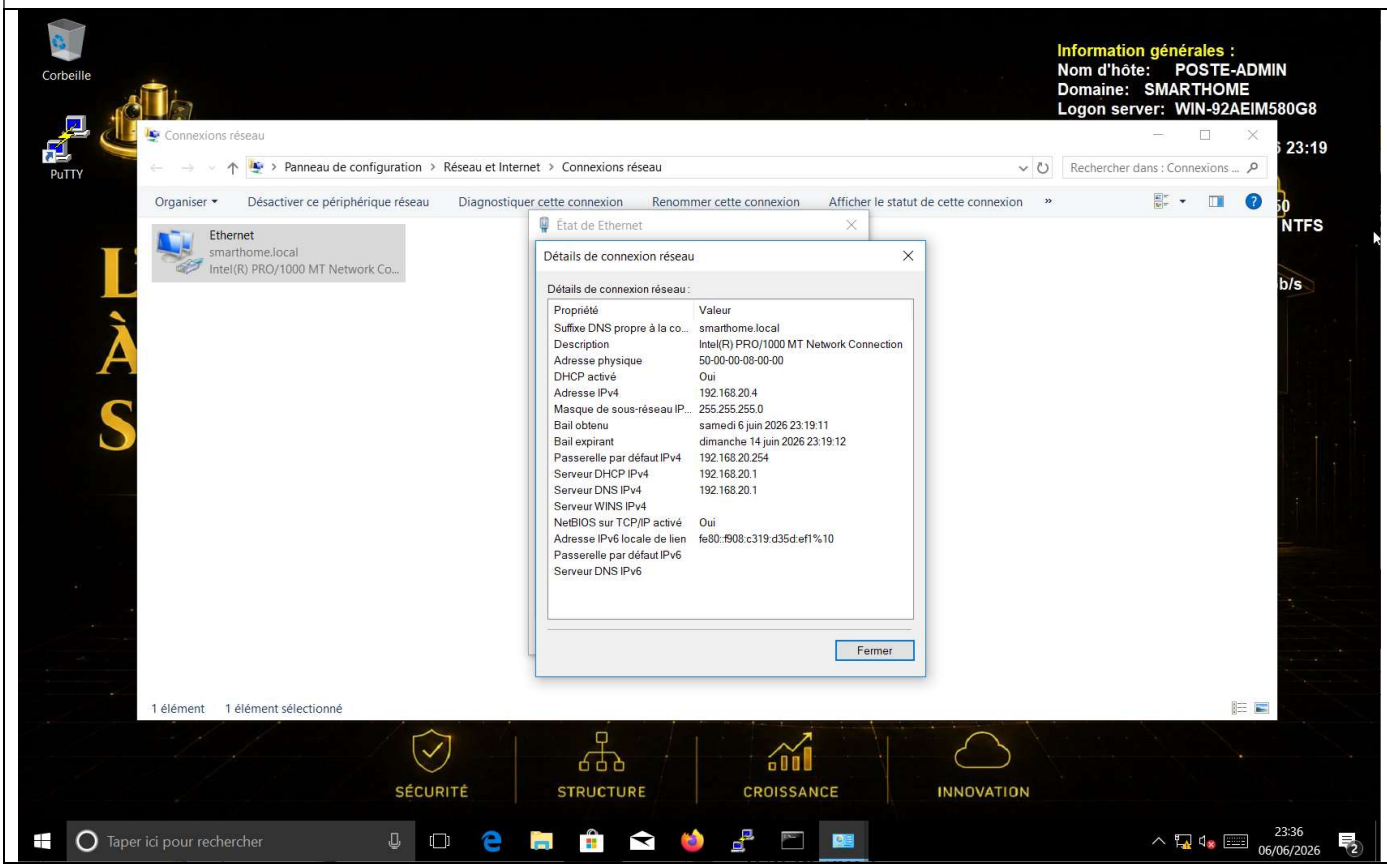
TESTS DNS-DHCP :

TEST RECEPTION DNS-DHCP - UTILISATEUR SMARTHOME

WIN_10_1_DIRECTION



WIN_10_2_ADMINRESEAUX



TESTS RADIUS :

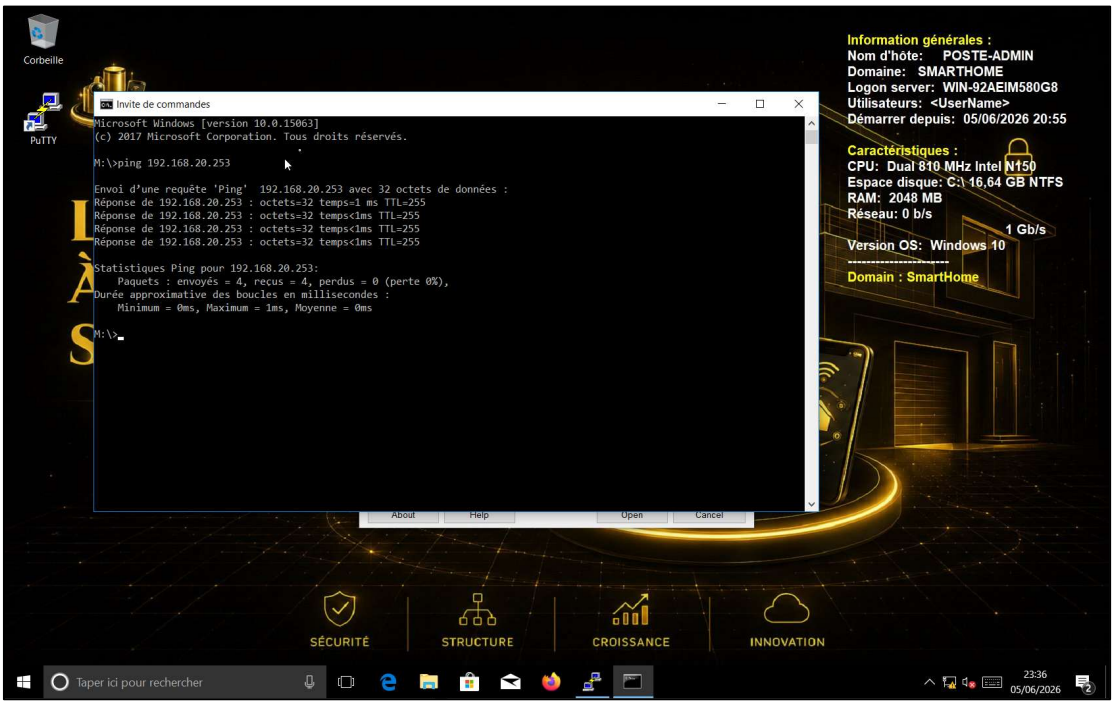
TEST RADIUS CAS REEL
PREMIERE DEMANDE : ***Faire en sorte que seuls les administrateurs du domaine utilisent les connexion SSH pour prendre la main sur les équipements Cisco.*** ✅
CAS N°1 : On se connecte avec un utilisateur autoriser, en l'occurrence l'utilisateur Théo Breton qui est l'AdminRéseaux de SMARTHOME. ✅

Logs SW1 :

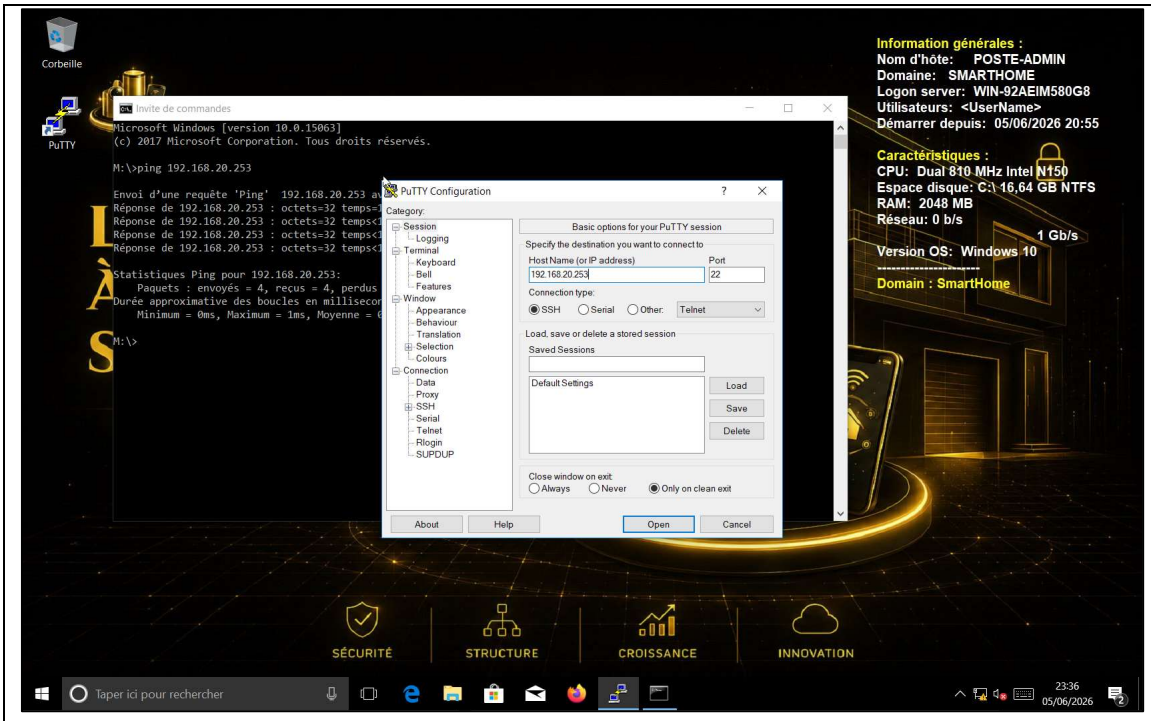
```
*Jun  5 23:36:54.946: RADIUS/ENCODE(00000016):Orig. component type = Exec
*Jun  5 23:36:54.946: RADIUS:  AAA Unsupported Attr: interface         [221]
4   3123053124
*Jun  5 23:36:54.946: RADIUS(00000016): Config NAS IP: 0.0.0.0
*Jun  5 23:36:54.946: RADIUS(00000016): Config NAS IPv6: ::
*Jun  5 23:36:54.946: RADIUS/ENCODE(00000016): acct_session_id: 12
*Jun  5 23:36:54.946: RADIUS(00000016): sending
*Jun  5 23:36:54.946: RADIUS/ENCODE: Best Local IP-Address 192.168.20.253 for
Radius-Server 192.168.20.1
*Jun  5 23:36:54.946: RADIUS(00000016): Sending a IPv4 Radius Packet
*Jun  5 23:36:54.946: RADIUS(00000016): Send Access-Request to
192.168.20.1:1812 id 1645/11,len 75
*Jun  5 23:36:54.946: RADIUS:  authenticator CE 39 4A D7 92 49 BF 53 - 5A 08
CC 9D 5C 23 2C E3
*Jun  5 23:36:54.946: RADIUS:  User-Name           [1]   7   "theob"
*Jun  5 23:36:54.946: RADIUS:  User-Password       [2]   18  *
*Jun  5 23:36:54.946: RADIUS:  NAS-Port            [5]   6   2
*Jun  5 23:36:54.946: RADIUS:  NAS-Port-Id         [87]  6   "tty2"
*Jun  5 23:36:54.946: RADIUS:  NAS-Port-Type       [61]  6   Virtual
[5]
*Jun  5 23:36:54.946: RADIUS:  Service-Type        [6]   6   Login
[1]
*Jun  5 23:36:54.946: RADIUS:  NAS-IP-Address      [4]   6   192.168.20.253
Username:
*Jun  5 23:36:54.946: RADIUS(00000016): Started 5 sec timeout
*Jun  5 23:36:54.985: RADIUS: Received from id 1645/11 192.168.20.1:1812,
Access-Accept, len 72
*Jun  5 23:36:54.985: RADIUS:  authenticator CC 49 40 35 E7 A1 E6 58 - CB 85
3D E9 9D 2E 5B 01
*Jun  5 23:36:54.985: RADIUS:  Service-Type        [6]   6   Login
[1]
*Jun  5 23:36:54.985: RADIUS:  Class               [25]  46
*Jun  5 23:36:54.985: RADIUS:   AE 6D 09 27 00 00 01 37 00 01 02 00 C0 A8 14
01 00 00 00 00 3D 45 7C 4D 75 D8 64 E7 01 DC F5 1C 28 06 A2 B0 00 00 00 00 00
00 00 1D        [ m'7=E|Mud(]
*Jun  5 23:36:54.985: RADIUS(00000016): Received from id 1645/11
Username:
*Jun  5 23:36:57.822: AAA: parse name=tty2 idb type=-1 tty=-1
*Jun  5 23:36:57.822: AAA: name=tty2 flags=0x11 type=5 shelf=0 slot=0
adapter=0 port=2 channel=0
```

```
*Jun  5 23:36:57.822: AAA/MEMORY: create_user (0xBB1191D8) user='theob'
ruser='NULL' ds0=0 port='tty2' rem_addr='192.168.20.4' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
*Jun  5 23:36:57.822: AAA/AUTHEN/START (568529534): port='tty2' list=''
action=LOGIN service=ENABLE
*Jun  5 23:36:57.822: AAA/AUTHEN/START (568529534): console enable - default
to enable password (if any)
*Jun  5 23:36:57.822: AAA/AUTHEN/START (568529534): Method=ENABLE
Username:
*Jun  5 23:36:57.822: AAA/AUTHEN(568529534): can't find any passwords
*Jun  5 23:36:57.822: AAA/AUTHEN (568529534): status = ERROR
*Jun  5 23:36:57.822: AAA/AUTHEN/START (568529534): Method=NONE
*Jun  5 23:36:57.822: AAA/AUTHEN (568529534): status = PASS
*Jun  5 23:36:57.822: AAA/MEMORY: free_user (0xBB1191D8) user='theob'
ruser='NULL' port='tty2' rem_addr='192.168.20.4' authen_type=ASCII
service=ENABLE priv=15 vrf= (id=0)
```

On vérifie que le poste communique avec l'adresse IP du VLAN.



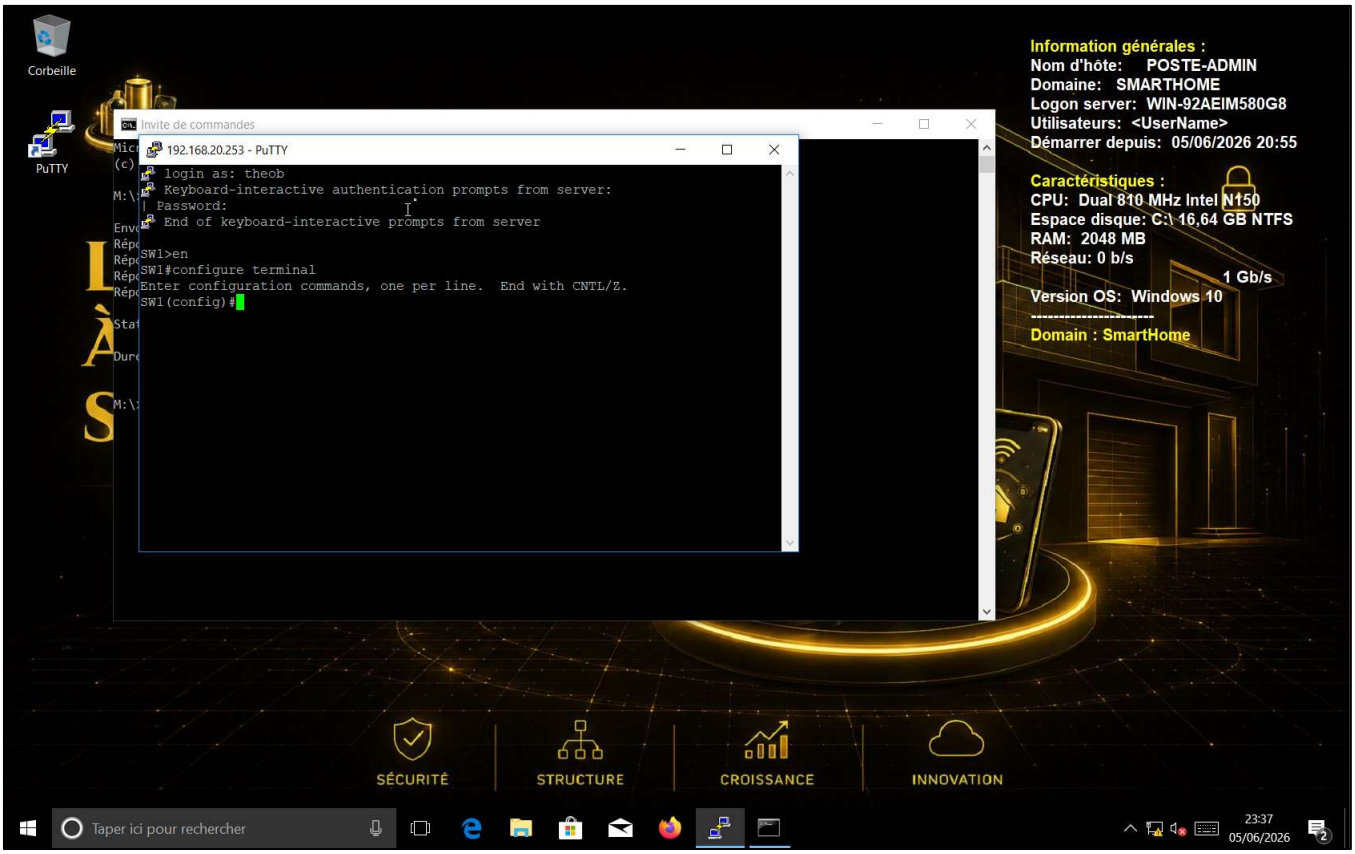
Ensuite une fois que la communication est validée on lance une session SSH.



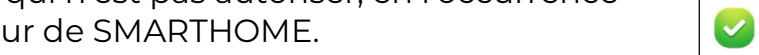
Puis on se connecte via nos identifiant Active Directory

Pour mon cas :

Identifiant : theob
MDP : Admin1234

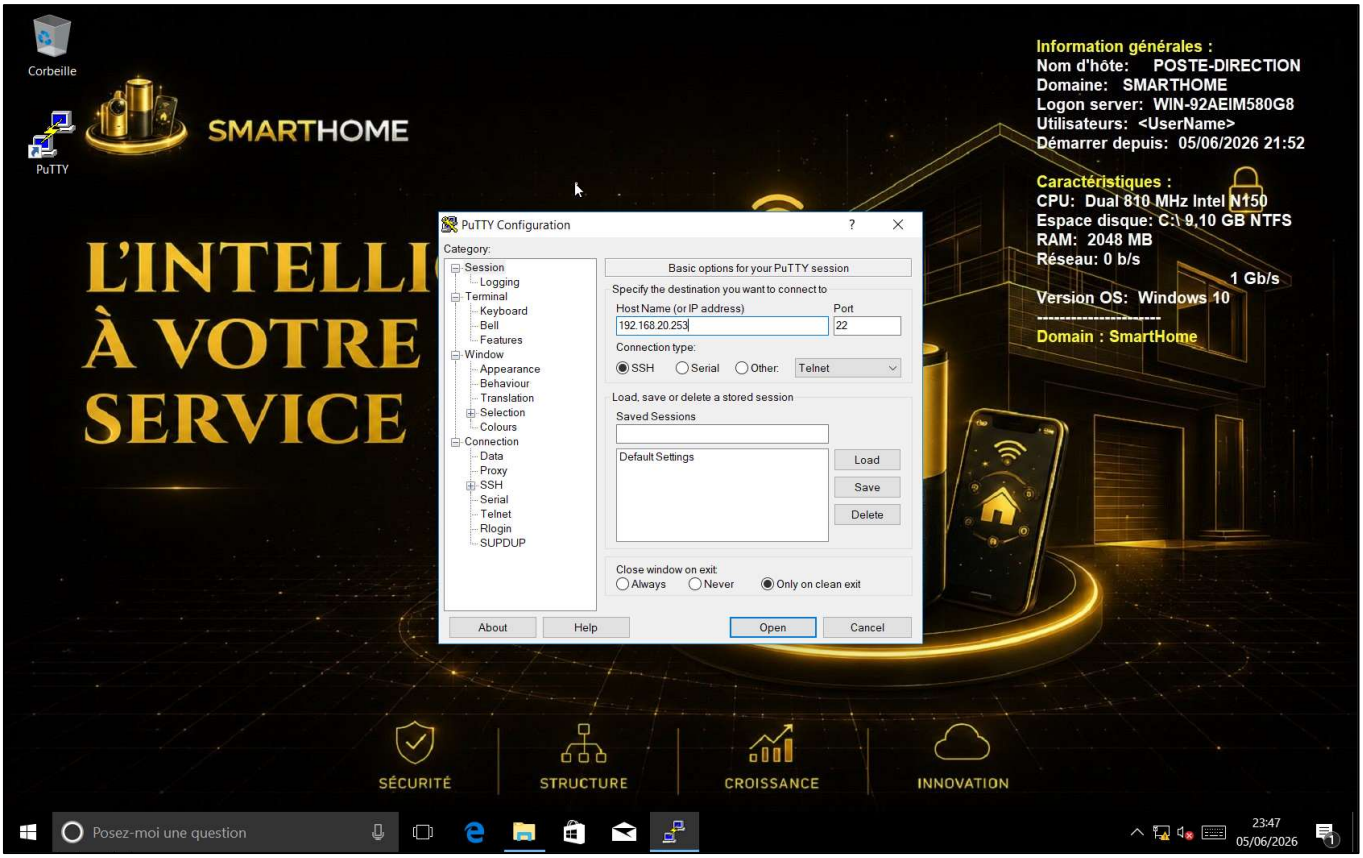


CAS N°2 : On se connecte avec un utilisateur qui n'est pas autoriser, en l'occurrence l'utilisateur Alexandre Marti qui est le directeur de SMARTHOME.

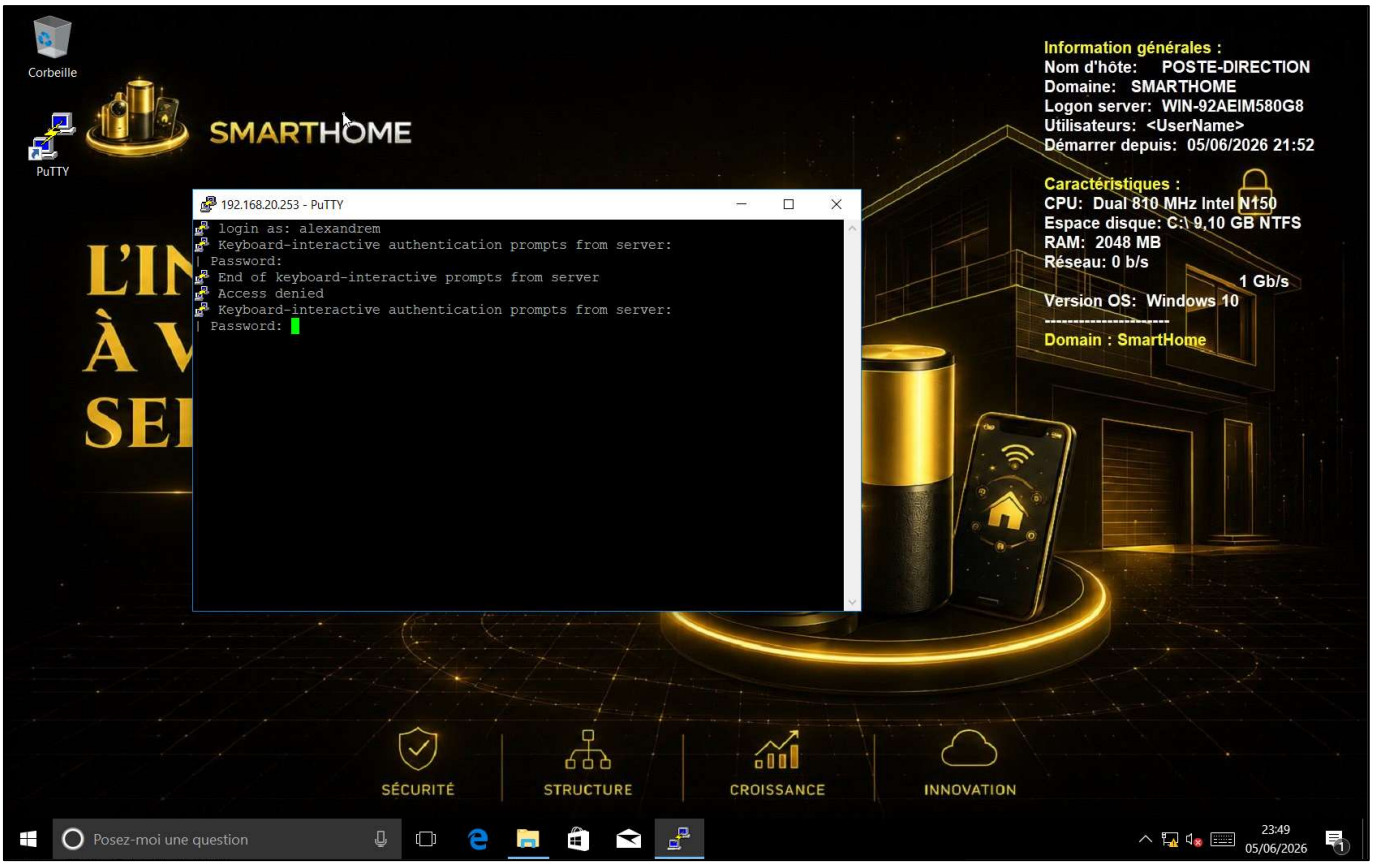


Logs SW1 :

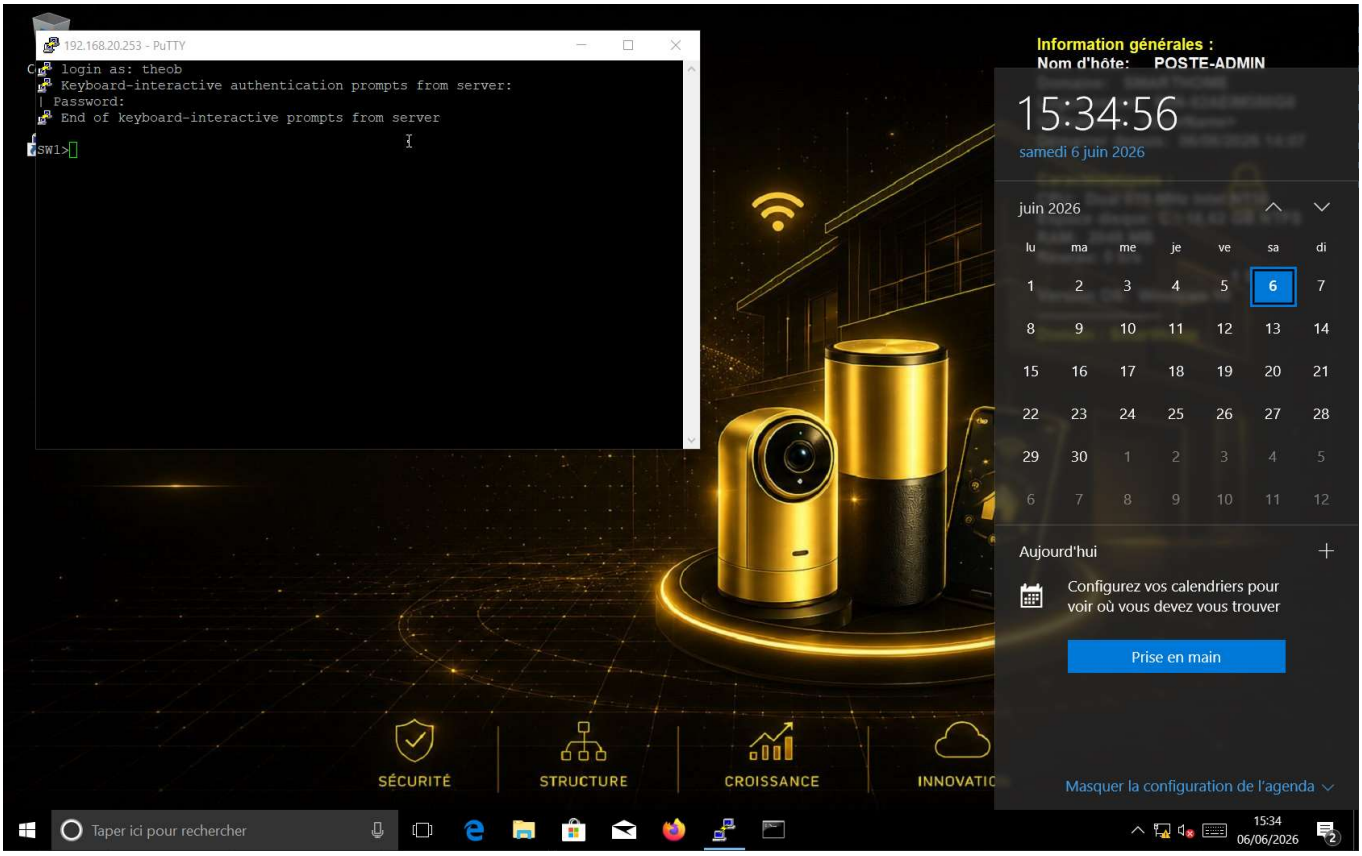
```
*Jun  5 23:47:02.873: %SYS-5-CONFIG_I: Configured from console by theob on
vty0 (192.168.20.4)
*Jun  5 23:47:39.427: AAA/BIND(00000017): Bind i/f
*Jun  5 23:47:39.427: AAA/AUTHEN/LOGIN (00000017): Pick method list 'default'
*Jun  5 23:47:39.427: RADIUS/ENCODE(00000017): ask "Password: "
*Jun  5 23:47:39.427: RADIUS/ENCODE(00000017): send packet; GET_PASSWORD
*Jun  5 23:47:44.229: RADIUS/ENCODE(00000017):Orig. component type = Exec
*Jun  5 23:47:44.229: RADIUS:  AAA Unsupported Attr: interface         [221]
4   3123053124
*Jun  5 23:47:44.229: RADIUS(00000017): Config NAS IP: 0.0.0.0
*Jun  5 23:47:44.229: RADIUS(00000017): Config NAS IPv6: ::
*Jun  5 23:47:44.229: RADIUS/ENCODE(00000017): acct_session_id: 13
*Jun  5 23:47:44.229: RADIUS(00000017): sending
*Jun  5 23:47:44.229: RADIUS/ENCODE: Best Local IP-Address 192.168.20.253 for
Radius-Server 192.168.20.1
*Jun  5 23:47:44.229: RADIUS(00000017): Sending a IPv4 Radius Packet
*Jun  5 23:47:44.229: RADIUS(00000017): Send Access-Request to
192.168.20.1:1812 id 1645/12,len 80
*Jun  5 23:47:44.229: RADIUS:  authenticator F3 16 4B D8 0F 50 D6 DB - EB F5
63 9C 55 A7 14 95
*Jun  5 23:47:44.229: RADIUS:  User-Name           [1]   12  "alexandrem"
*Jun  5 23:47:44.229: RADIUS:  User-Password       [2]   18  *
*Jun  5 23:47:44.229: RADIUS:  NAS-Port            [5]   6   2
*Jun  5 23:47:44.229: RADIUS:  NAS-Port-Id         [87]  6   "tty2"
*Jun  5 23:47:44.229: RADIUS:  NAS-Port-Type       [61]  6   Virtual
[5]
*Jun  5 23:47:44.229: RADIUS:  Service-Type        [6]   6   Login
[1]
*Jun  5 23:47:44.229: RADIUS:  NAS-IP-Address      [4]   6   192.168.20.253
*Jun  5 23:47:44.229: RADIUS(00000017): Started 5 sec timeout
*Jun  5 23:47:44.237: RADIUS: Received from id 1645/12 192.168.20.1:1812,
Access-Reject, len 20
*Jun  5 23:47:44.237: RADIUS:  authenticator E5 01 67 63 21 7B 5D 52 - 44 D0
1A 23 DB 8B D5 8B
*Jun  5 23:47:44.237: RADIUS(00000017): Received from id 1645/12
*Jun  5 23:47:46.249: AAA/AUTHEN/LOGIN (00000017): Pick method list 'default'
*Jun  5 23:47:46.249: RADIUS/ENCODE(00000017): ask "Password: "
*Jun  5 23:47:46.249: RADIUS/ENCODE(00000017): send packet; GET_PASSWORD
```



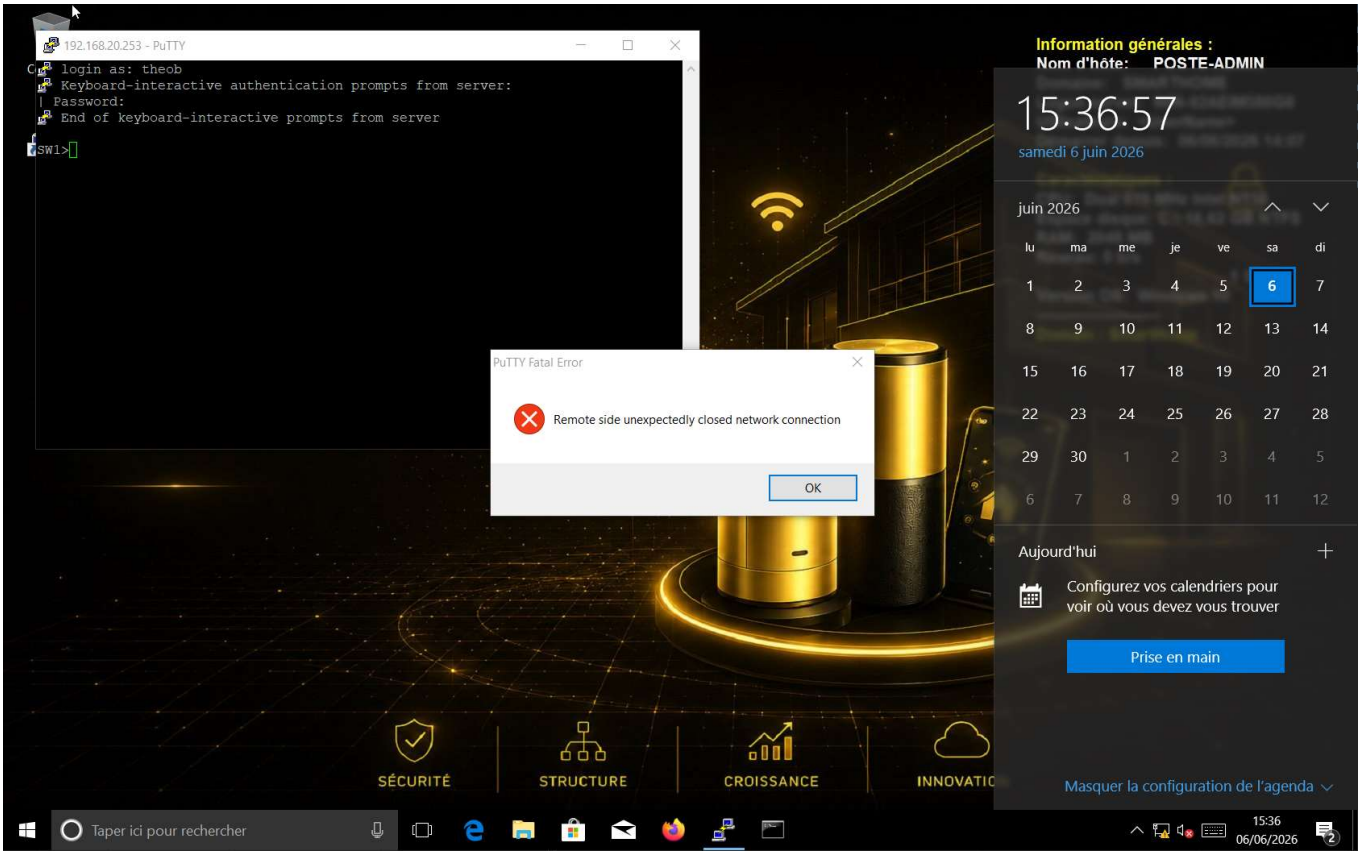
Le directeur étant pas le groupe des admins du domaine, l'accès et refusé !



Ouverture de session à 15:34:56 :



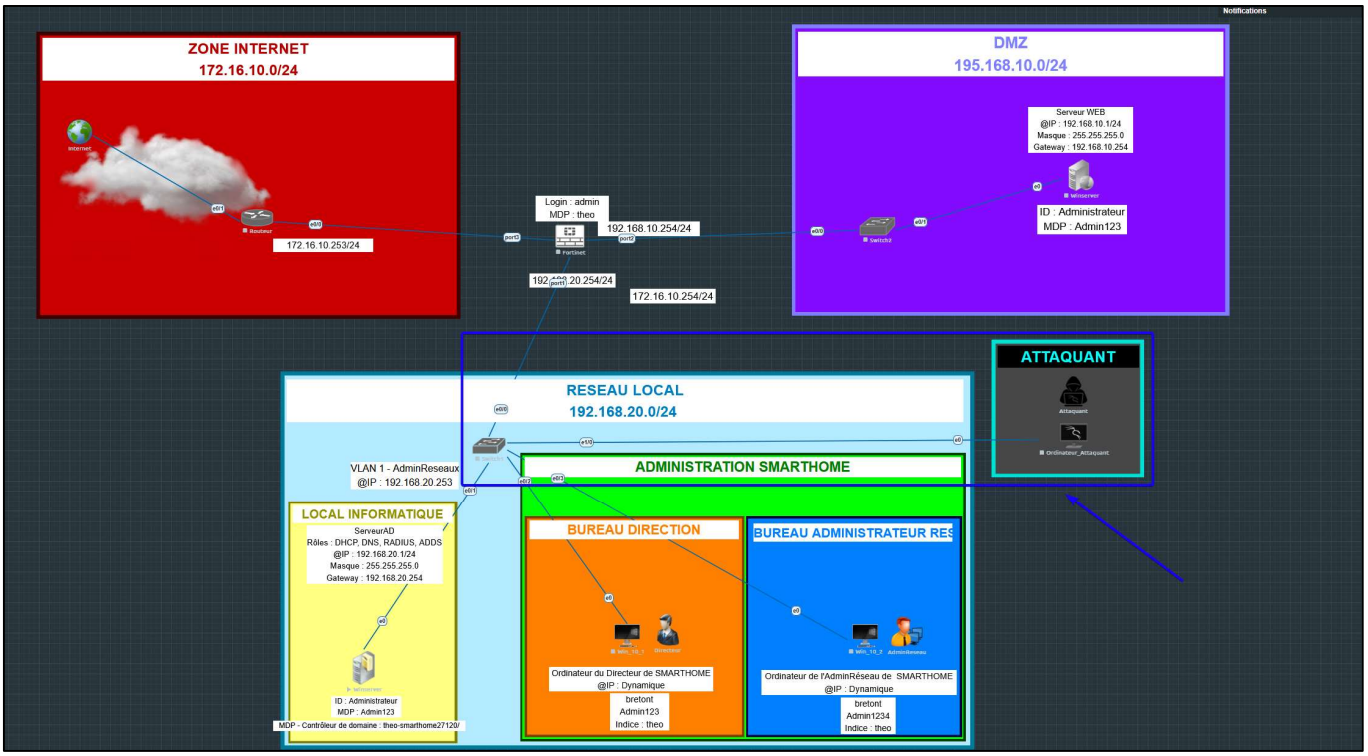
2 minutes plus tard – 15:36:57 :



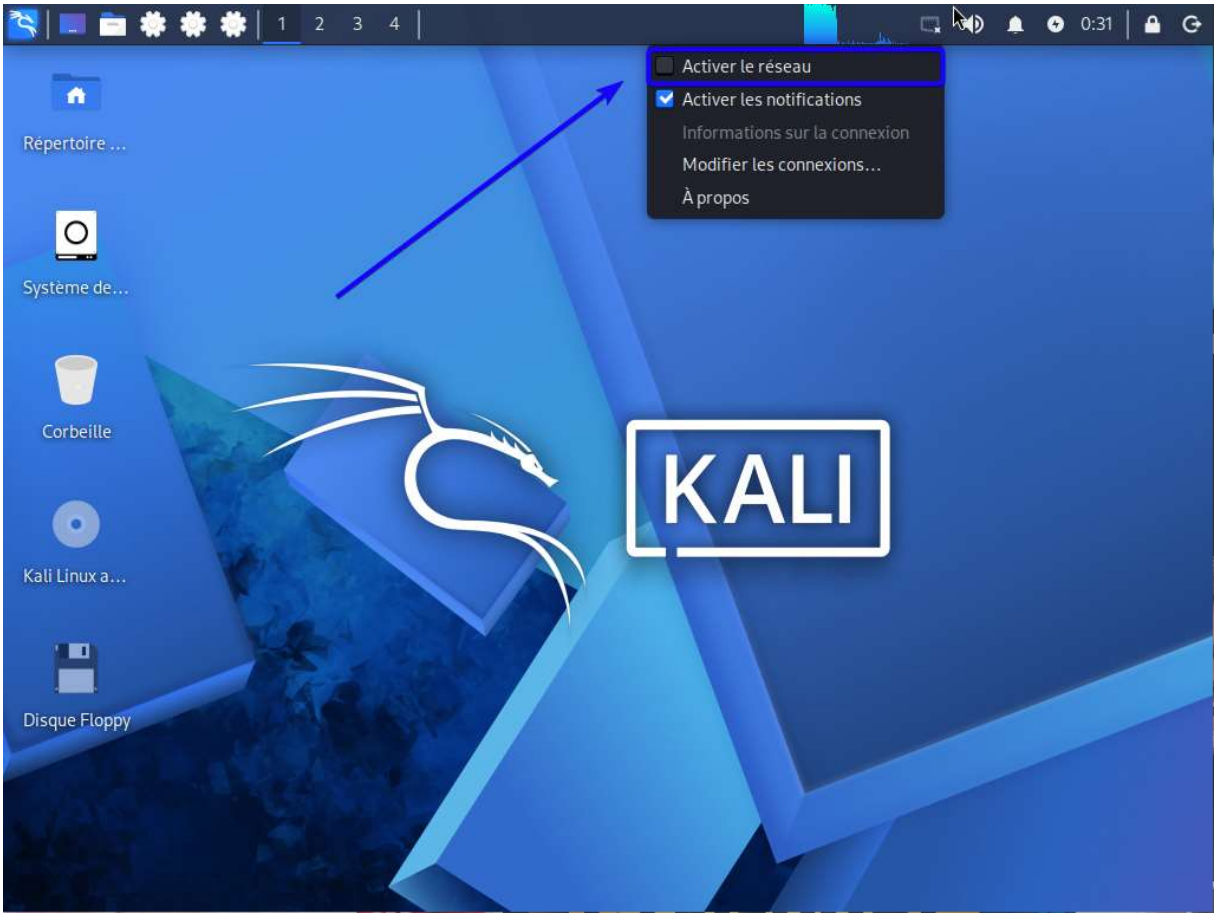
DEUXIEME DEMANDE :

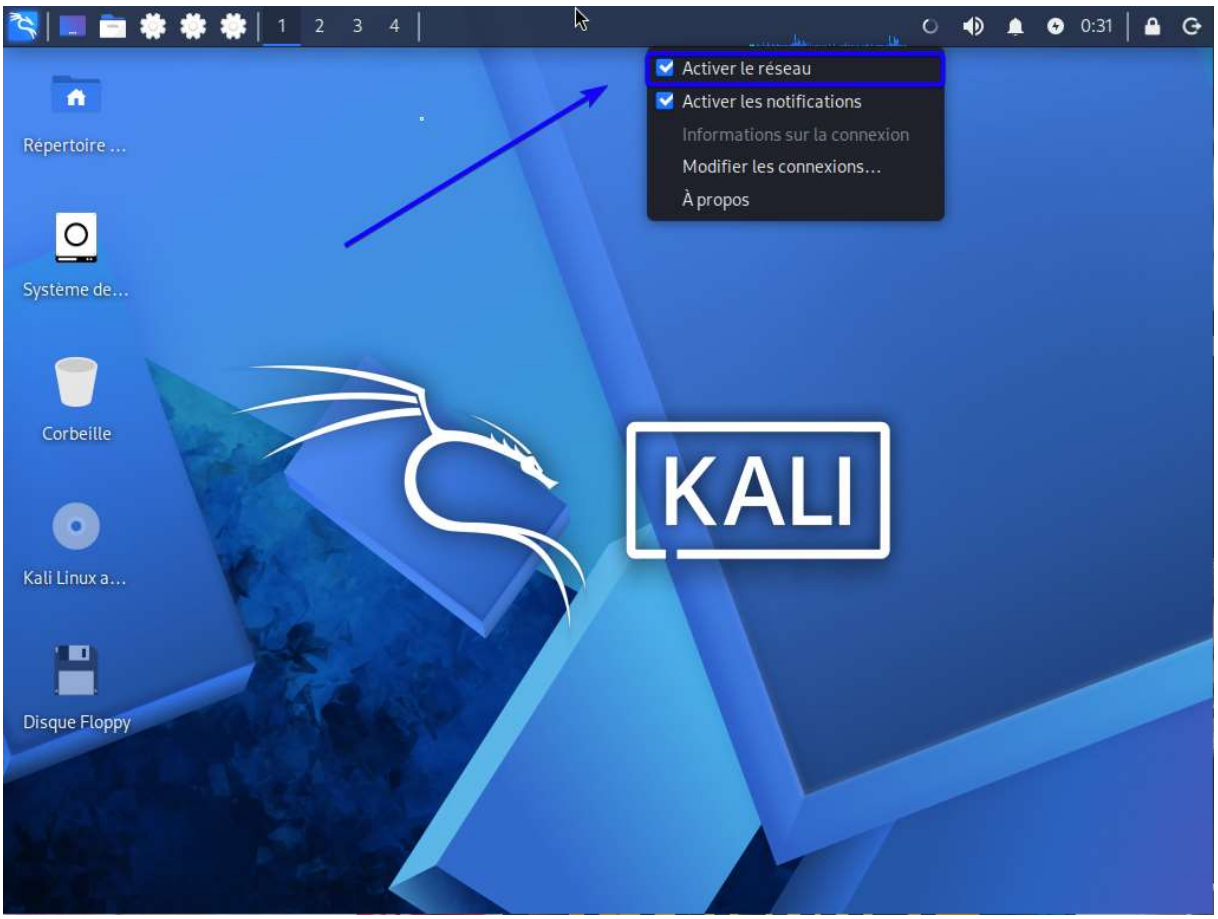
Faire en sorte que aucune autre personne ne se branche sur le switch puisse obtenir une IP du serveur DHCP à part les utilisateurs du domaine.

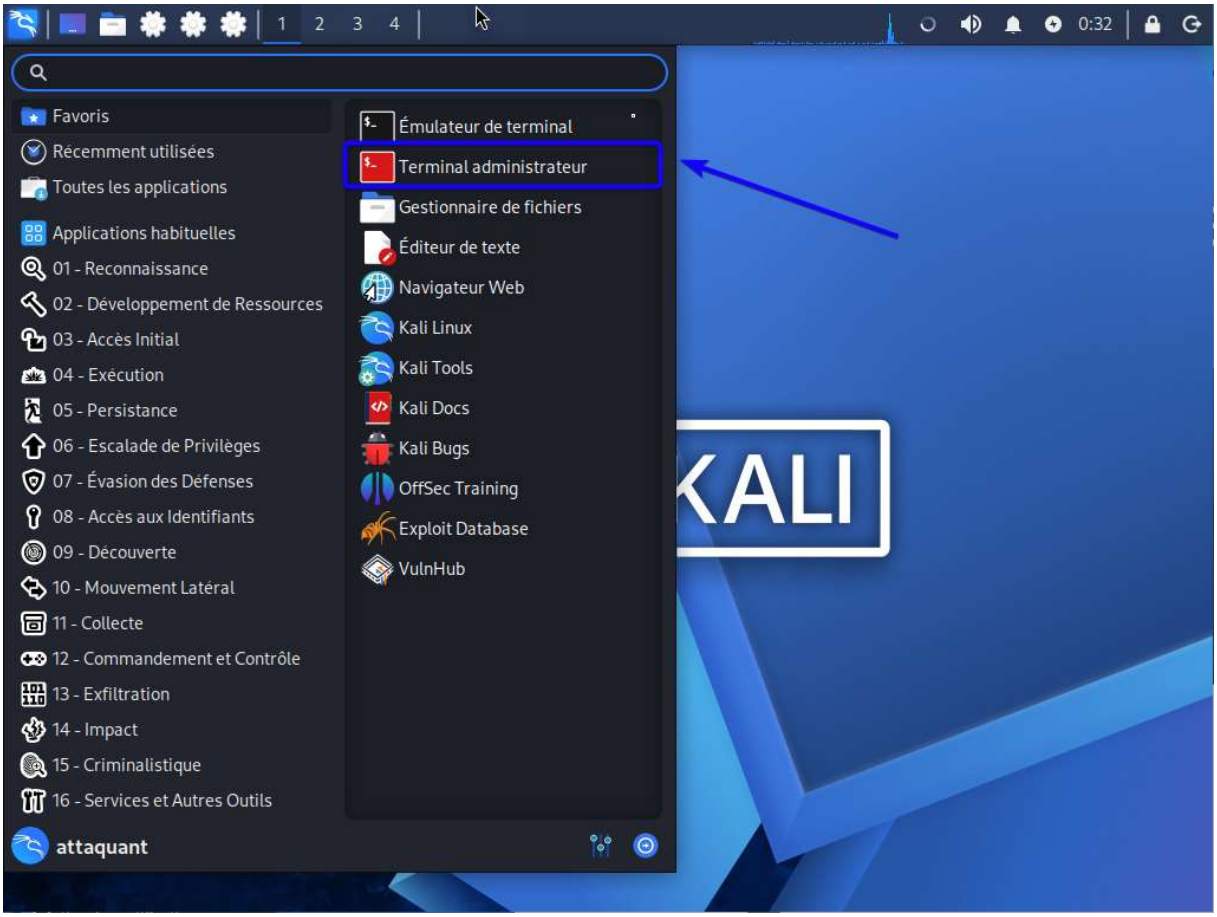
Maintenant que le PC de l'attaquant est sur KaliLinux on va le raccorder sur un port bloqué.



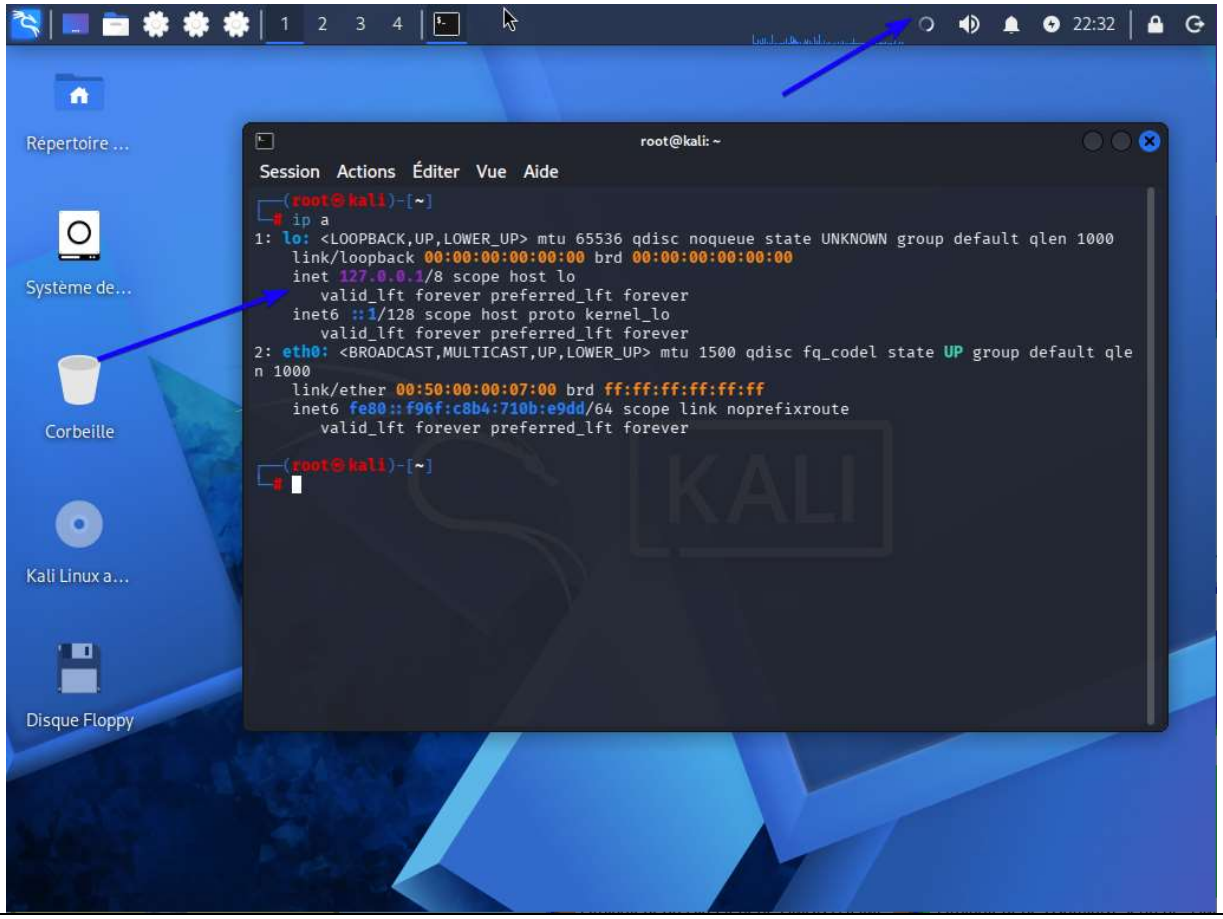
Je désactive la carte réseau manuellement puis je la réactive.


1 2 3 4
0:31
Activer le réseau
Activer les notifications
Informations sur la connexion
Modifier les connexions...
À propos
Répertoire ...
Système de...
Corbeille
Kali Linux a...
Disque Floppy
KALI


1 2 3 4
0:31
Activer le réseau
Activer les notifications
Informations sur la connexion
Modifier les connexions...
À propos
Répertoire ...
Système de...
Corbeille
Kali Linux a...
Disque Floppy
KALI



En tapent la commande « ip a » je vois que je ne reçoit aucune @IP du serveur DHCP de SMARTHOME.



TEST DE SITE :

ACCES AU SITE DEPUIS LE PCGAMER en 192.168.3.4/24		
PCGAMER – 192.168.3.4/24 - HTTP	SRV-WEB (www.smarthome.com)	✅