Faculté des Sciences et Technologies

(FST)

Rapport du travail de Laboratoire N° 7_Reseaux I

Etudiant : Donsam Jean Gabard NOEL

Professeur : Ismaël SAINT AMOUR

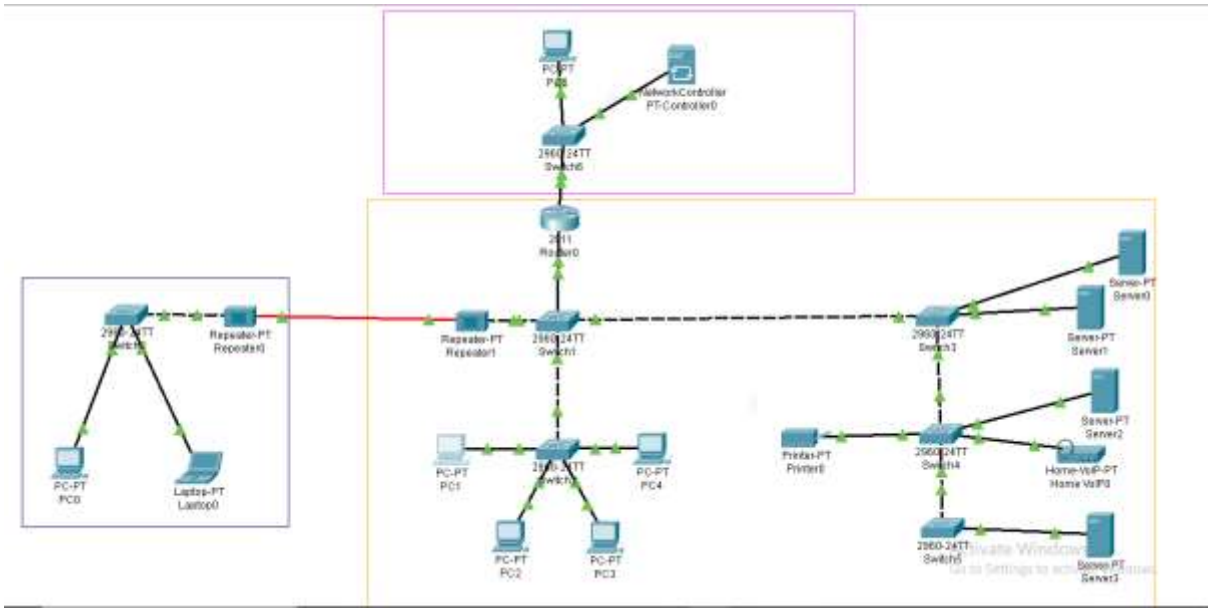
Niveau : L3

Décembre 2025

L’objectif de ce TD est de :

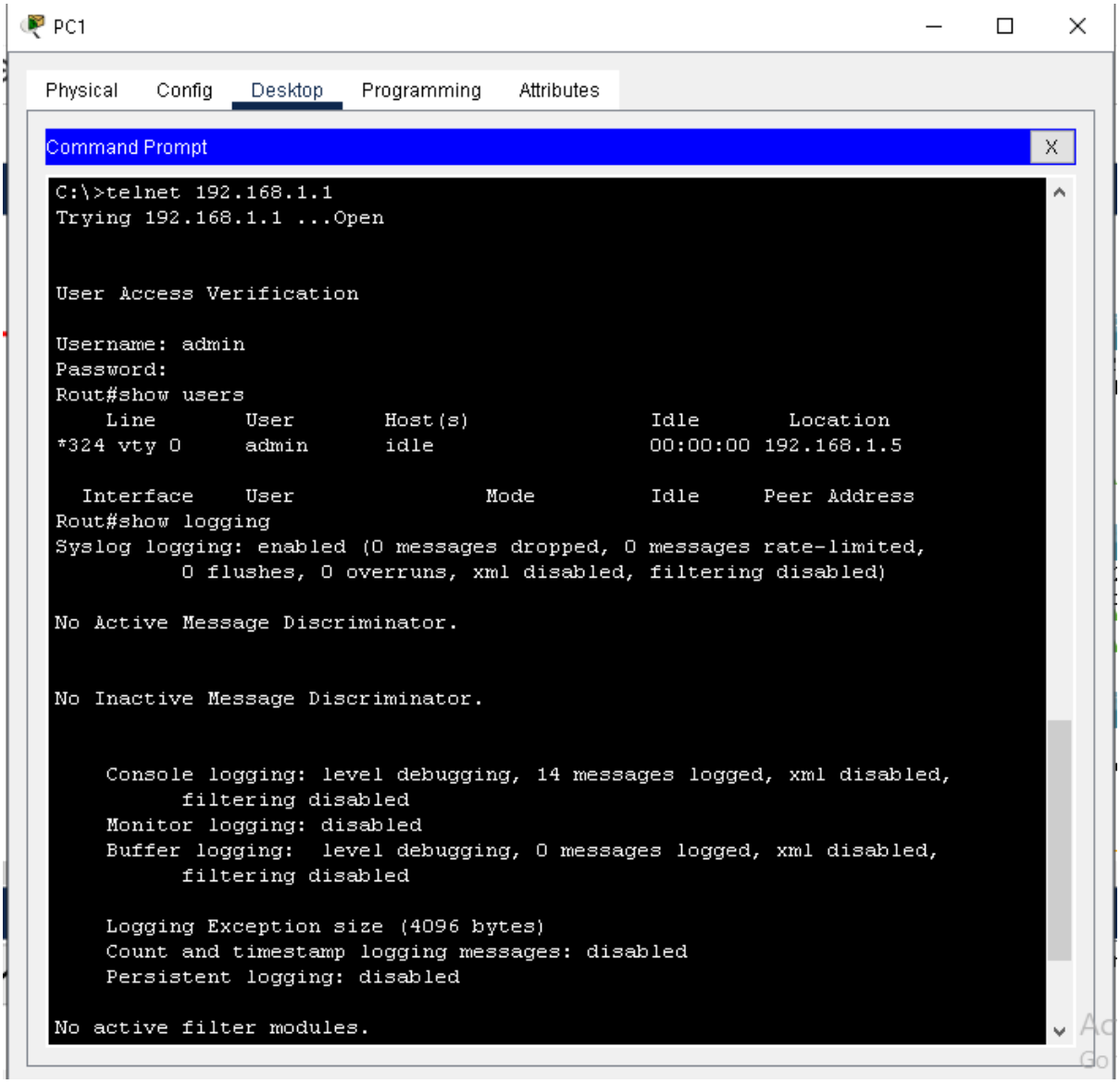
- Activer Telnet en mode sécurisé
- Créer plusieurs niveaux d’utilisateurs
- Restreindre l’accès Telnet via ACL
- Journaliser les connexions
- Mettre en place une bannière légale
- Tester Telnet depuis plusieurs VLAN
- Superviser les sessions actives
- Configurer timeouts et protections
- Configurer SSH avec clés RSA 2048/4096 bits
- Mettre en place différents niveaux d’utilisateurs (privilèges 1, 5, 15)
- Restreindre l’accès SSH via ACL
- Activer SSH version 2 (obligatoire)
- Configurer des timers de sécurité
- Activer protection contre brute-force
- Journaliser tentatives réussies/échouées
- Superviser sessions SSH actives
- Durcir l’équipement

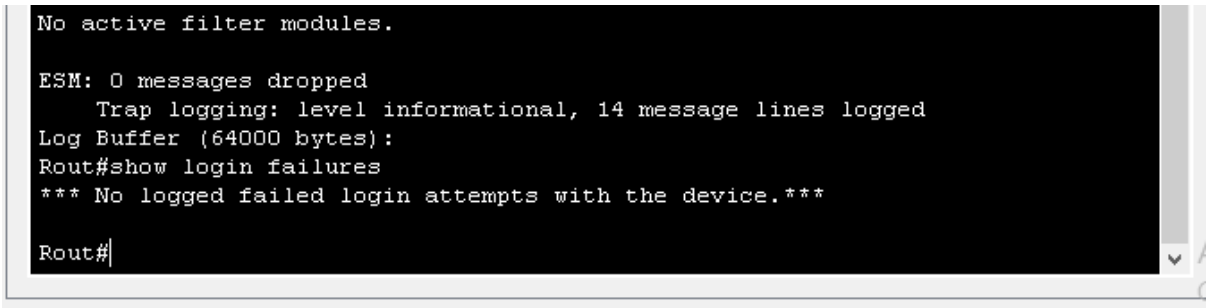
Topologie

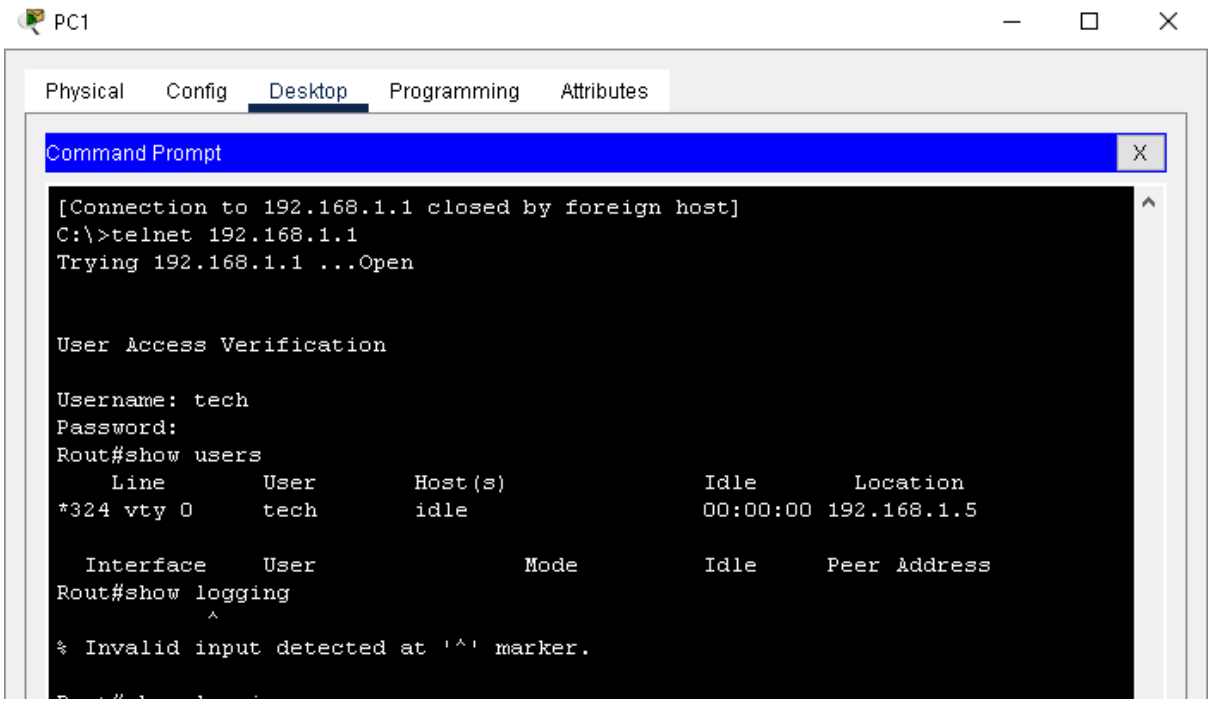

PC-PT
PC0
Laptop-PT
Laptop0
Repeater-PT
Repeater0
Repeater-PT
Repeater1
PC-PT
PC1
PC-PT
PC2
PC-PT
PC3
PC-PT
PC4
Printer-PT
Printer0
Home-VoIP-PT
Server-PT
Server0
Server-PT
Server1
Server-PT
Server2
Server-PT
Server3

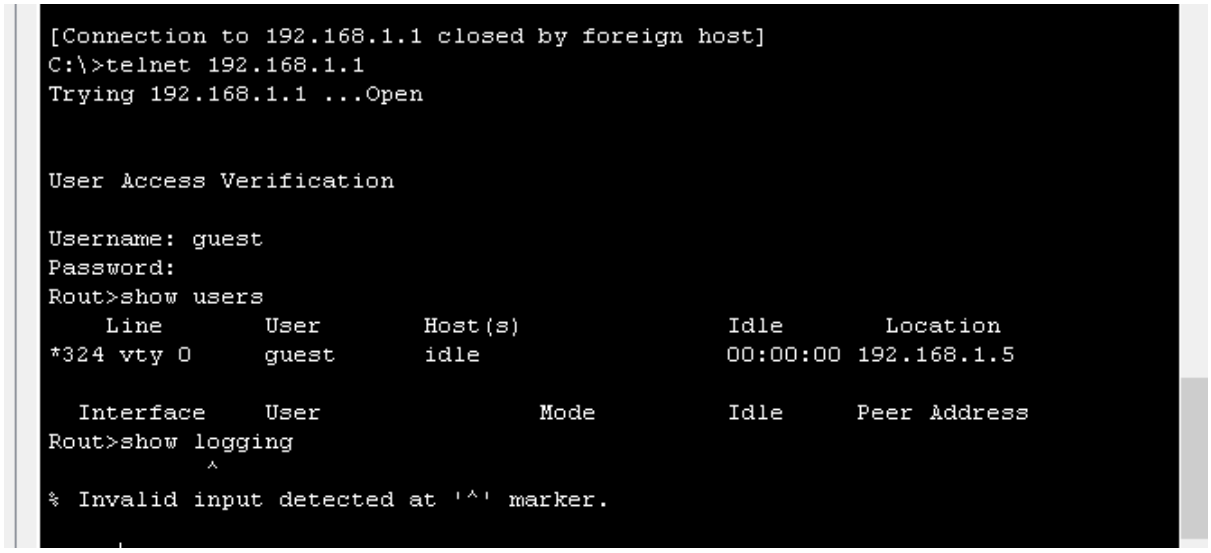
Configuration Telnet (partie non sécurisée)

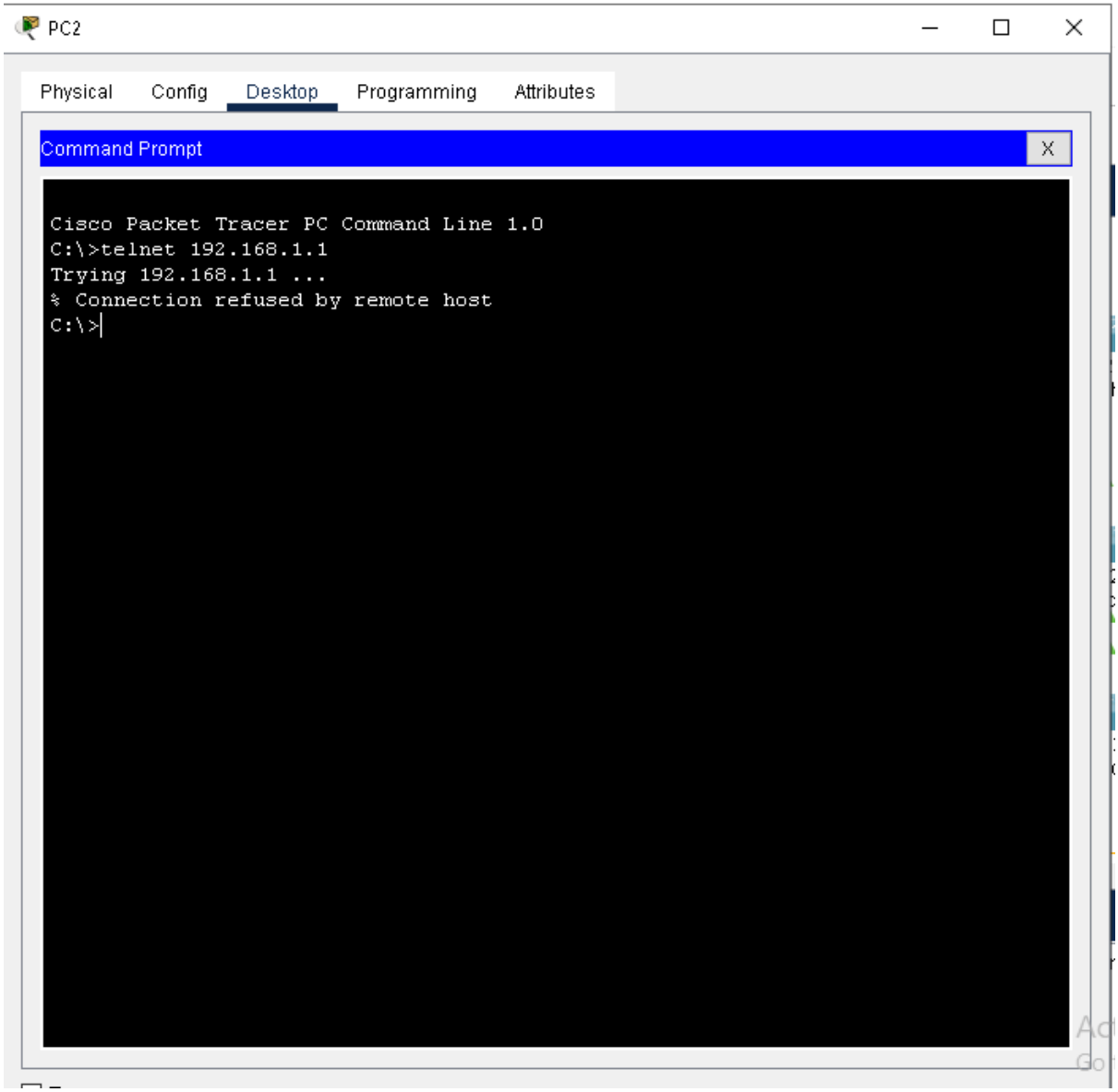
Tester l'accès Telnet :






PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
[Connection to 192.168.1.1 closed by foreign host]
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
User Access Verification
Username: tech
Password:
Rout#show users
Line User Host(s) Idle Location
*324 vty 0 tech idle 00:00:00 192.168.1.5
Interface User Mode Idle Peer Address
Rout#show logging
^
% Invalid input detected at '^' marker.


[Connection to 192.168.1.1 closed by foreign host]
C:\>telnet 192.168.1.1
Trying 192.168.1.1 ...Open
User Access Verification
Username: guest
Password:
Rout>show users
Line User Host(s) Idle Location
*324 vty 0 guest idle 00:00:00 192.168.1.5
Interface User Mode Idle Peer Address
Rout>show logging
^
% Invalid input detected at '^' marker.



Questions :

1. Pourquoi Telnet est-il considéré comme non sécurisé ?

R- Telnet est considéré comme non sécurisé car il transmet toutes les données en clair, y compris les identifiants (noms d'utilisateur et mots de passe). Cela signifie que toute personne interceptant le trafic réseau peut facilement lire ces informations sensibles. De plus, Telnet n'offre aucune protection contre les attaques par écoute (sniffing) ou par usurpation d'identité (spoofing).

2. Quelles informations transitent en clair ?

R- Avec Telnet, toutes les informations échangées entre le client et le serveur transitent en clair, notamment:

- Noms d'utilisateur et mots de passe (authentification).
- Commandes saisies par l'utilisateur.
- Sorties des commandes (résultats affichés à l'écran).
- Toutes les données échangées pendant la session.

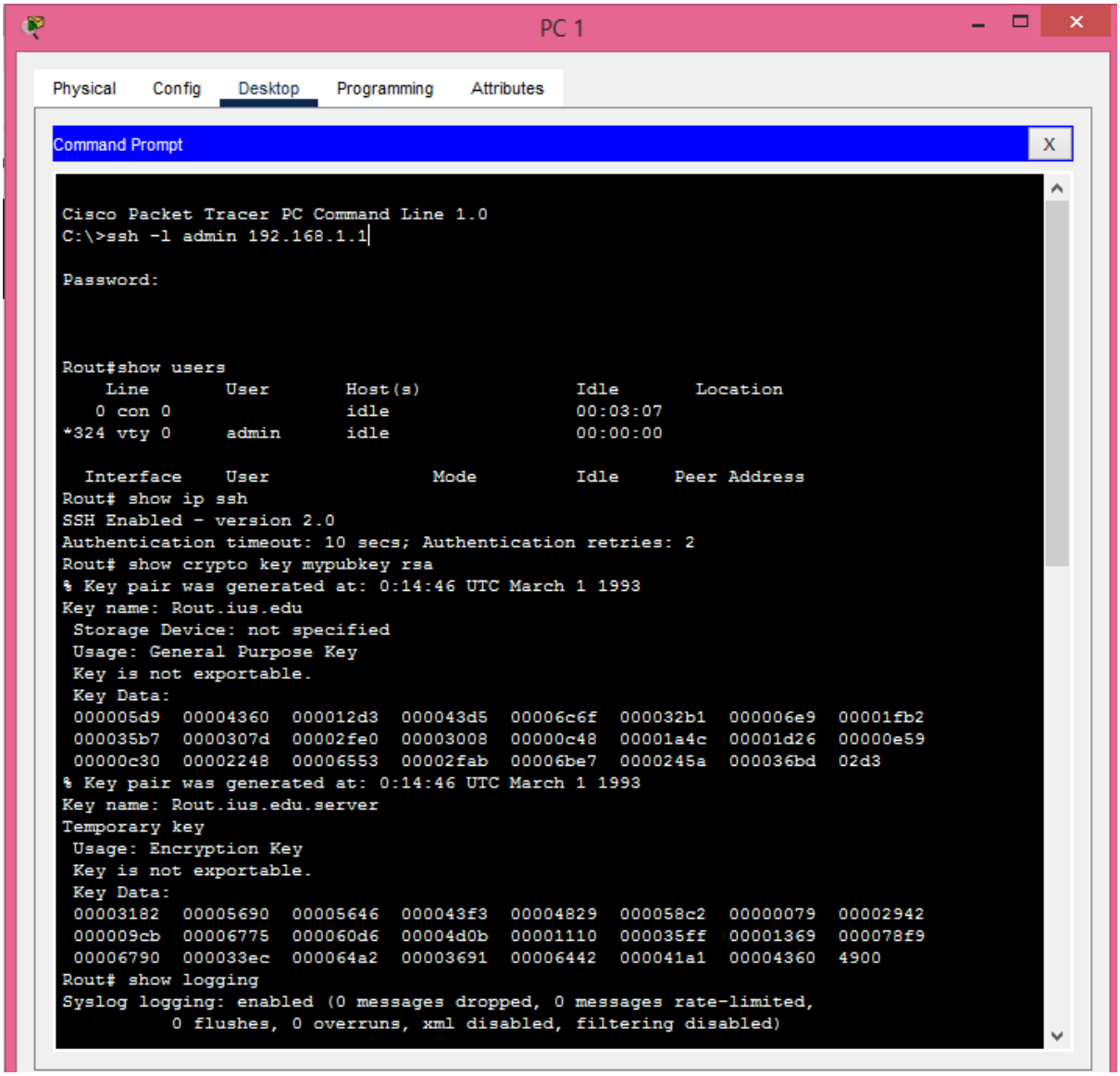
3. Pourquoi est-il déconseillé d'utiliser Telnet en production ?

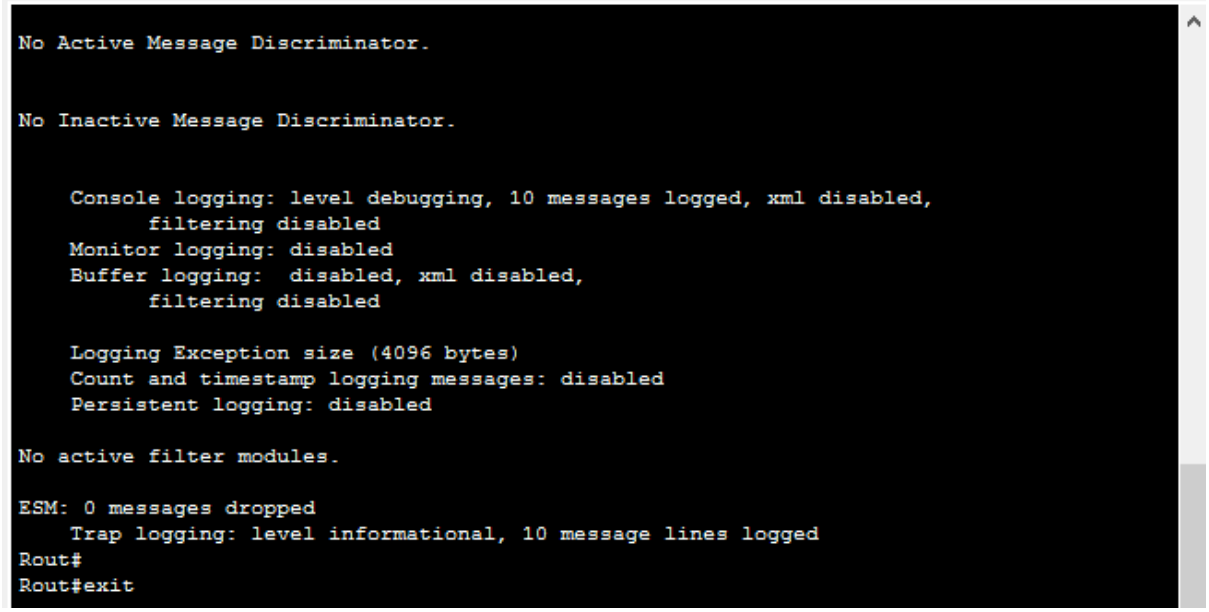
R- Telnet est déconseillé en production pour plusieurs raisons :

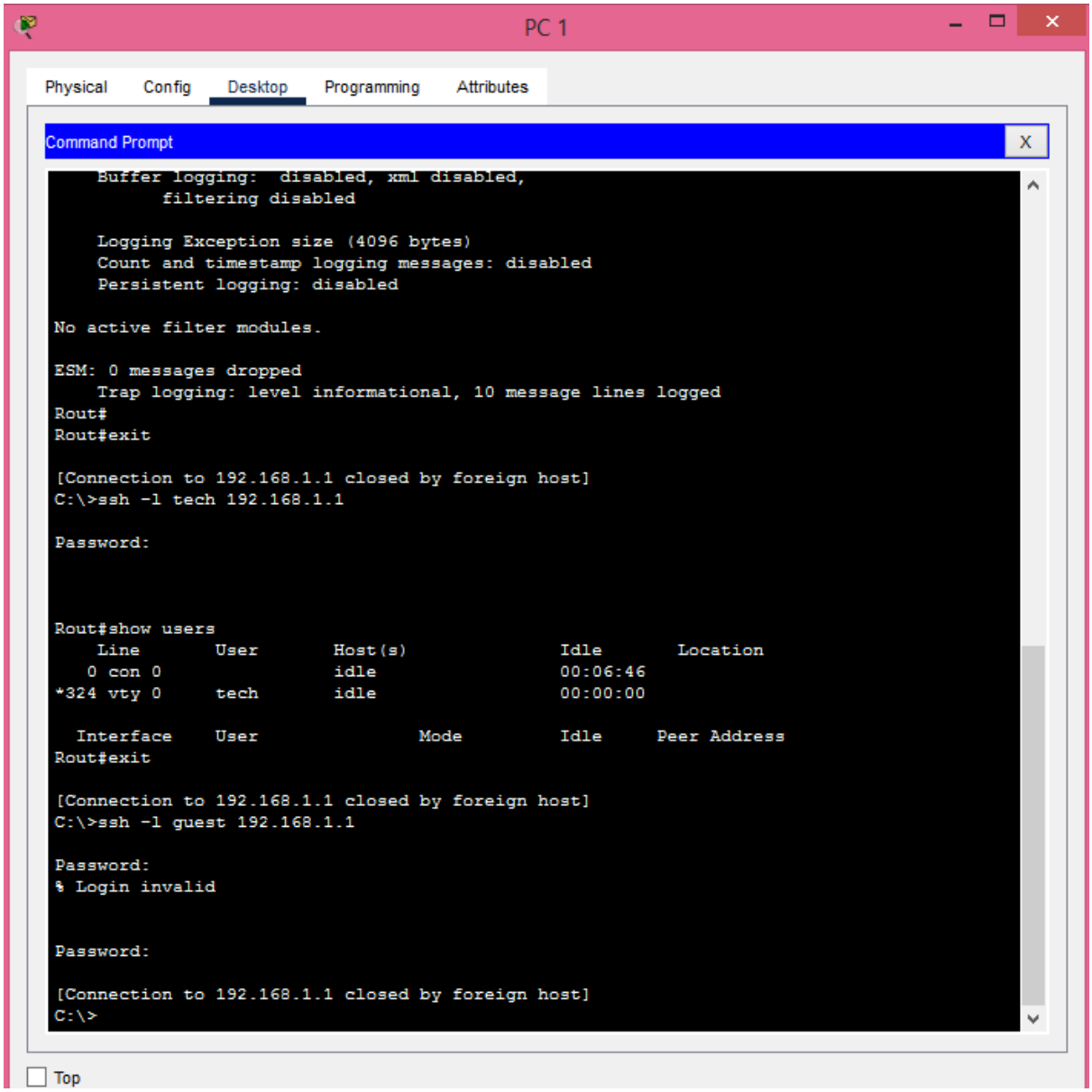
- Absence de chiffrement : Les données sensibles sont exposées aux attaques.
- Vulnérabilité aux attaques : Facilement exploitable par des attaques de type Man-in-the-Middle (MITM) ou replay attacks.
- Non-conformité aux normes de sécurité : Ne respecte pas les exigences modernes de sécurité (RGPD, ISO 27001, etc.).
- Alternatives sécurisées : SSH (Secure Shell) offre un chiffrement robuste et est largement adopté.

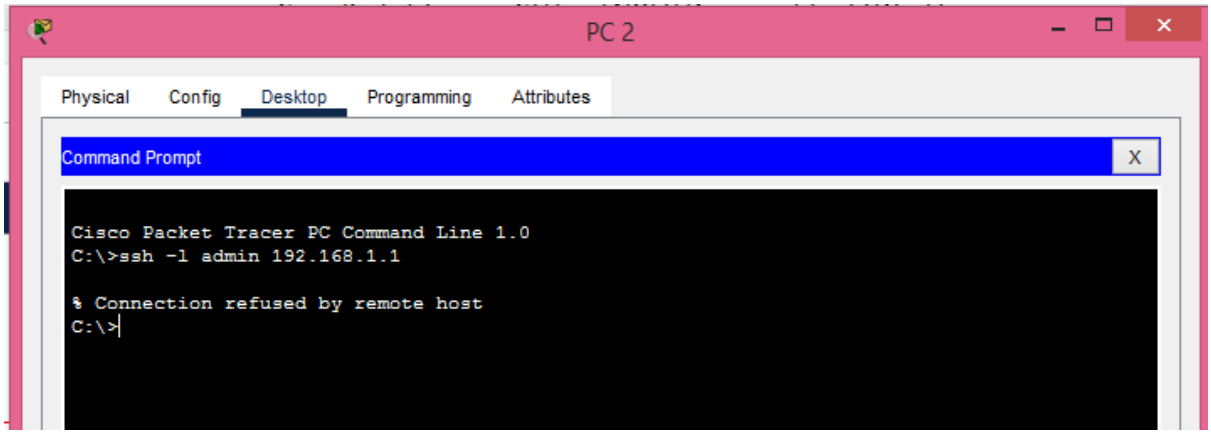
Configuration SSH (partie sécurisée)

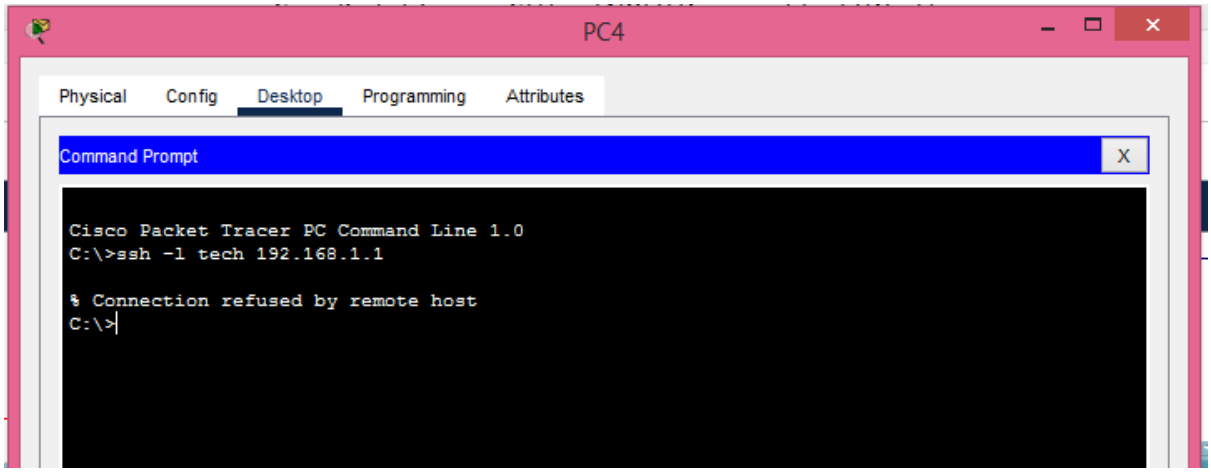
Tester l'accès SSH :




No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 10 messages logged, xml disabled,
filtering disabled
Monitor logging: disabled
Buffer logging: disabled, xml disabled,
filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
ESM: 0 messages dropped
Trap logging: level informational, 10 message lines logged
Rout#
Rout#exit


PC 1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Buffer logging: disabled, xml disabled,
filtering disabled
Logging Exception size (4096 bytes)
Count and timestamp logging messages: disabled
Persistent logging: disabled
No active filter modules.
ESM: 0 messages dropped
Trap logging: level informational, 10 message lines logged
Rout#
Rout#exit
[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l tech 192.168.1.1
Password:
Rout#show users
Line User Host(s) Idle Location
0 con 0 idle 00:06:46
*324 vty 0 tech idle 00:00:00
Interface User Mode Idle Peer Address
Rout#exit
[Connection to 192.168.1.1 closed by foreign host]
C:\>ssh -l guest 192.168.1.1
Password:
% Login invalid
Password:
[Connection to 192.168.1.1 closed by foreign host]
C:\>
Top


PC 2
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.1.1
% Connection refused by remote host
C:\>



Questions :

1. Quelle différence entre SSH v1 et SSH v2 ?

Critères	Sécurité	Algorithmes	Authentification	Compatibilité
SSH v1	Vulnérable à des attaques (ex : insertion de paquet)	Utilise des algorithmes obsolètes (ex : CRC-32)	Moins flexible	Dépréciée et désactivée par défaut
SSH v2	Protocole plus sécurisé, corrigé contre les failles de v1	Prend en charge des algorithmes modernes (AES, SHA-2)	Prend en charge plusieurs méthodes (clés publiques, mots de passe)	Standard actuel, largement utilisé

2. Pourquoi RSA 1024 bits n'est plus recommandé ?

R- Les clés RSA 1024 bits sont désormais considérées comme faibles face à la puissance de calcul actuelle et aux attaques par factorisation. Les normes (NIST, CA/B Forum) recommandent au moins 2048 bits depuis 2013, car 1024 bits peut être cassé par des supercalculateurs ou des attaques quantiques futures.

3. Que se passe-t-il si on désactive le domaine local ?

R- La désactivation du domaine local (via `no ip domain-lookup`) empêche la résolution DNS automatique, mais ne bloque pas SSH si le nom d'hôte et le domaine sont déjà configurés. En revanche, la génération de clés RSA pour SSH nécessite un nom de domaine configuré (`ip domain-name`). Sans cela, la configuration SSH peut échoue.

Conclusion

Ce laboratoire de réseau m’a permis de renforcer concrètement la sécurité des accès distants sur un équipement Cisco. En remplaçant Telnet par SSH (version 2, avec des clés RSA 2048/4096 bits), en restreignant les accès via des ACL, et en configurant des niveaux d’utilisateurs, des bannières légales et une journalisation complète, j’ai pu transformer un équipement vulnérable en un système sécurisé, traçable et conforme aux standards actuels.