FACULTÉ DES SCIENCES ET TECHNOLOGIES (FST)

TROISIÈME ANNÉE

Rapport du travail de Laboratoire N° 7

Cours : Réseaux I

Étudiante : Christy Gérys LAMBERT

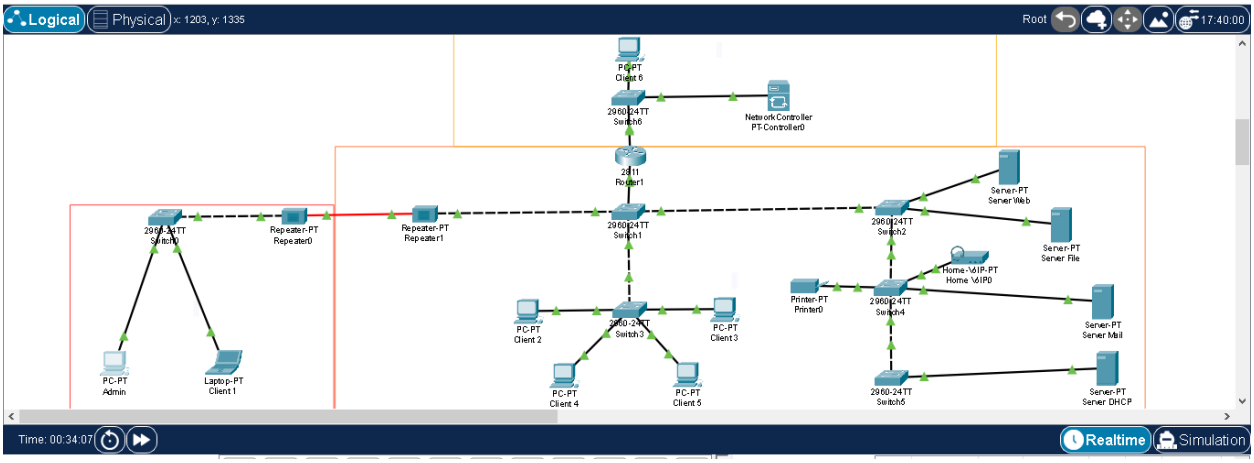
Professeur : Ismaël SAINT AMOUR

Le 14 Décembre 2025

L'objectif de ce TD est de :

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

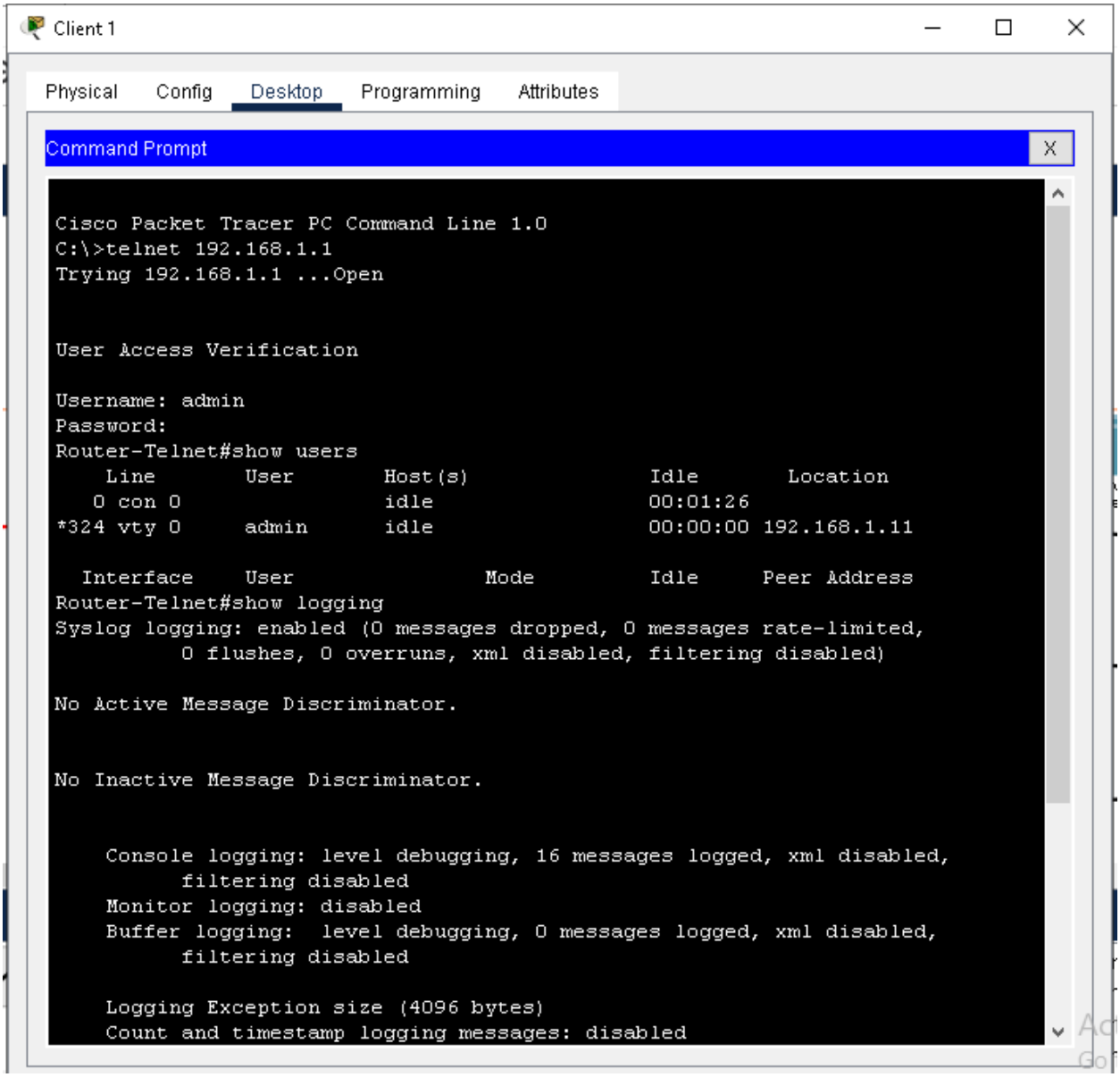
A. Configuration Telnet (partie non sécurisée)

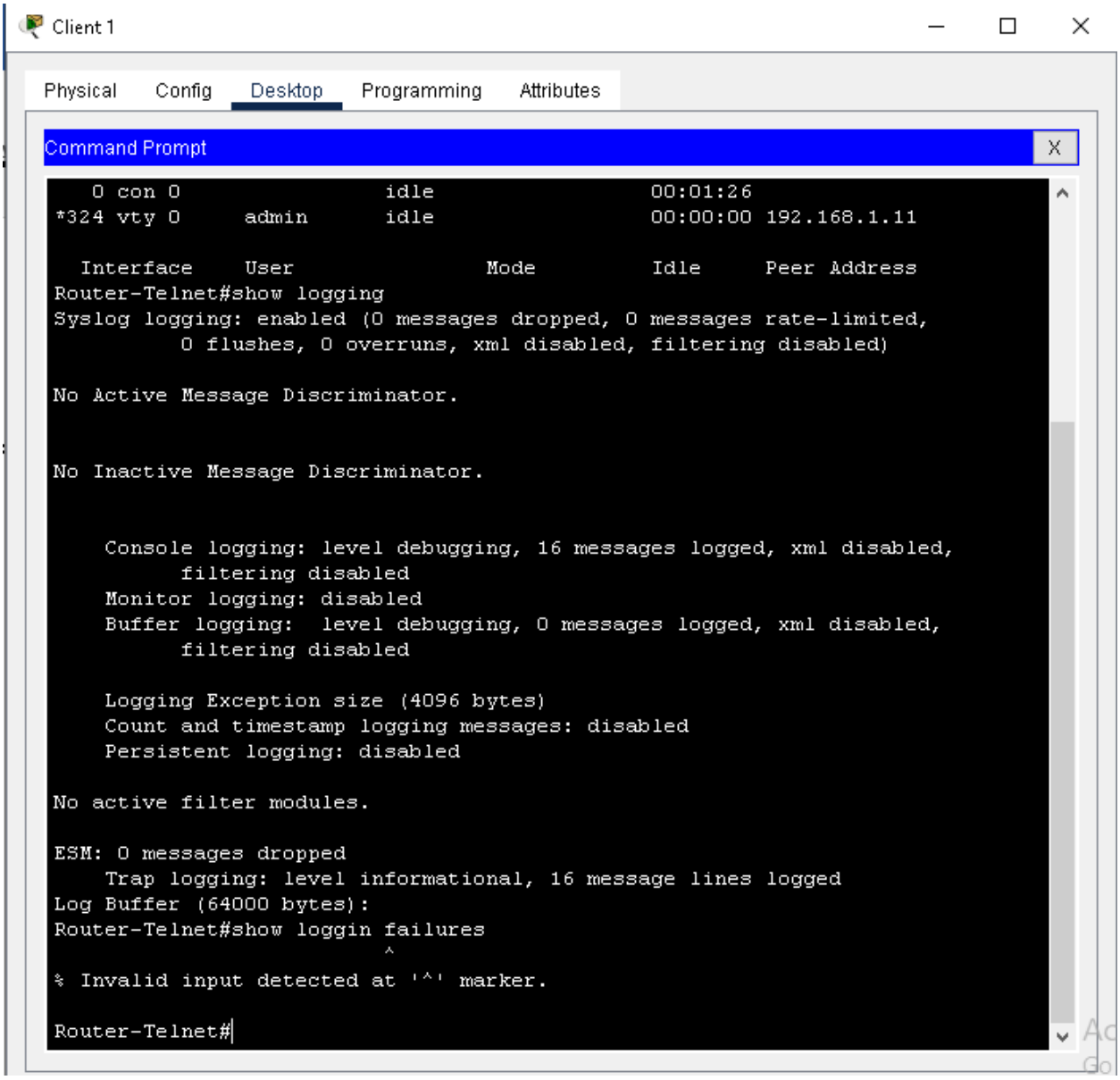


Configuration du mot de passe de ligne

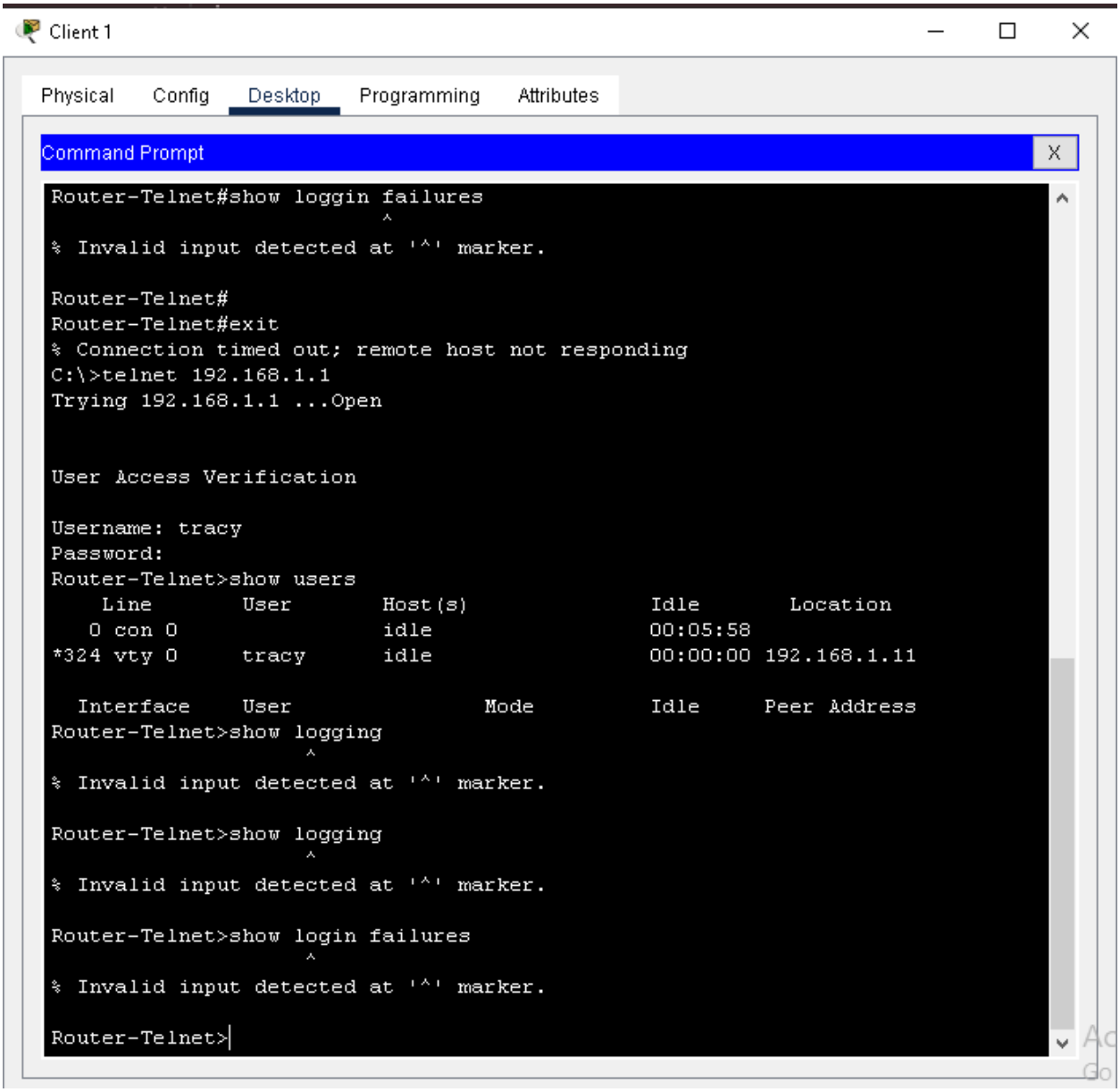
```
Router-Telnet>en
Password:
Router-Telnet#
```

Connexion à Telnet depuis PC1=Client 1 via l'utilisateur ayant un privilège 15

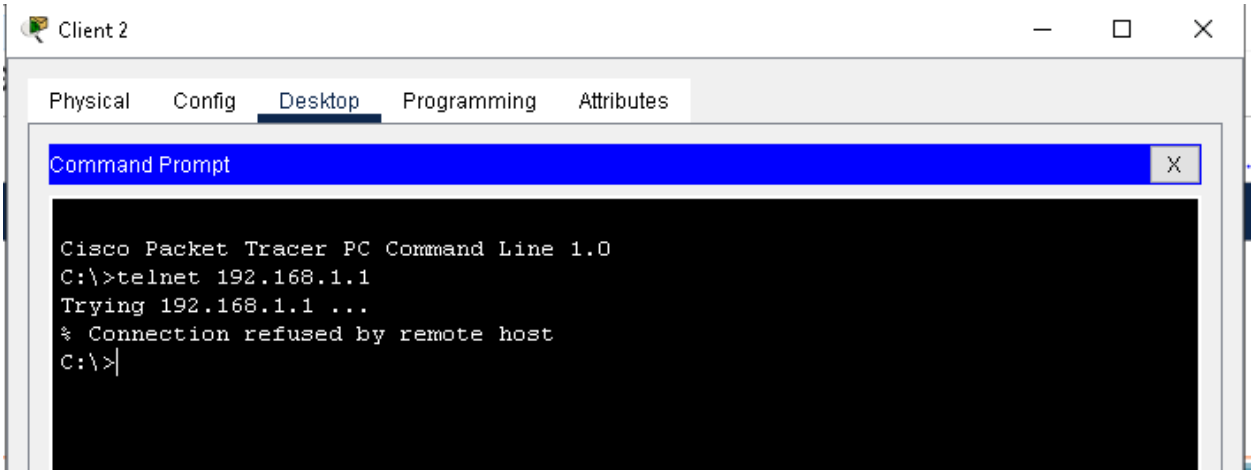



Client 1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
0 con 0 idle 00:01:26
*324 vty 0 admin idle 00:00:00 192.168.1.11
Interface User Mode Idle Peer Address
Router-Telnet#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 16 messages logged, xml disabled,
filtering disabled
Monitor logging: disabled
Buffer logging: level debugging, 0 messages logged, 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, 16 message lines logged
Log Buffer (64000 bytes):
Router-Telnet#show loggin failures
^
% Invalid input detected at '^' marker.
Router-Telnet#

Connexion à Telnet depuis Client 1 via tracy ayant un privilège 1



Impossibilité de se connecter à Telnet depuis Client 2



Questions :

1. Pourquoi Telnet est-il considéré comme non sécurisé ?
   Avant toute chose, Telnet est un protocole réseau qui permet de communiquer à u ordinateur via un autre ordinateur, mais de nos jours, Telnet est considéré comme obsolète et dangereux pour la gestion des serveurs parce que les informations transmises à l'ordinateur ne sont pas chiffrées. Si un pirate informatique fait du **sniffing** (c'est-à-dire écouter le réseau), il pourra lire toutes les données transmises en clair.

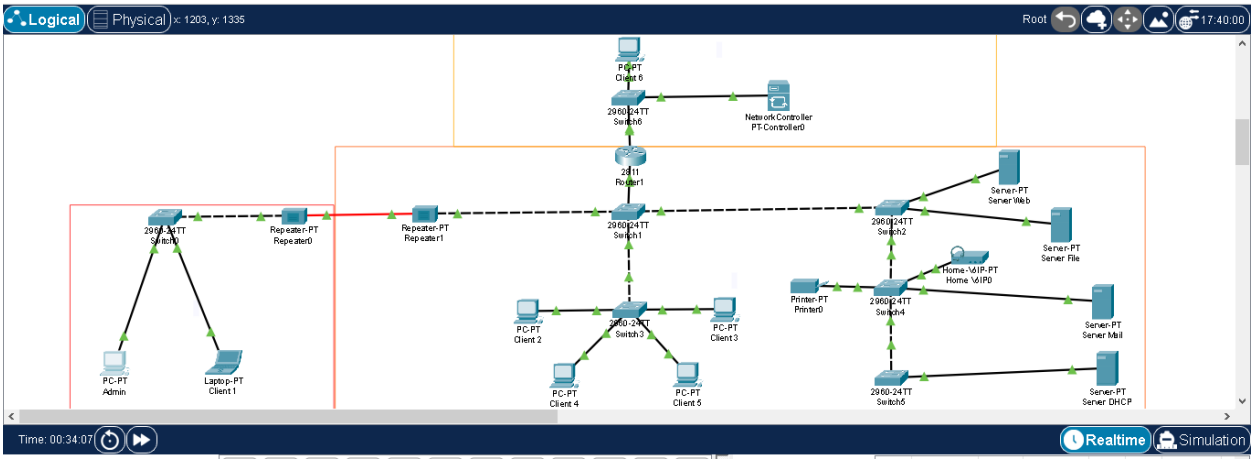
2. Quelles informations transitent en clair ?
   Telnet envoie toutes les informations :
   - Les identifiants

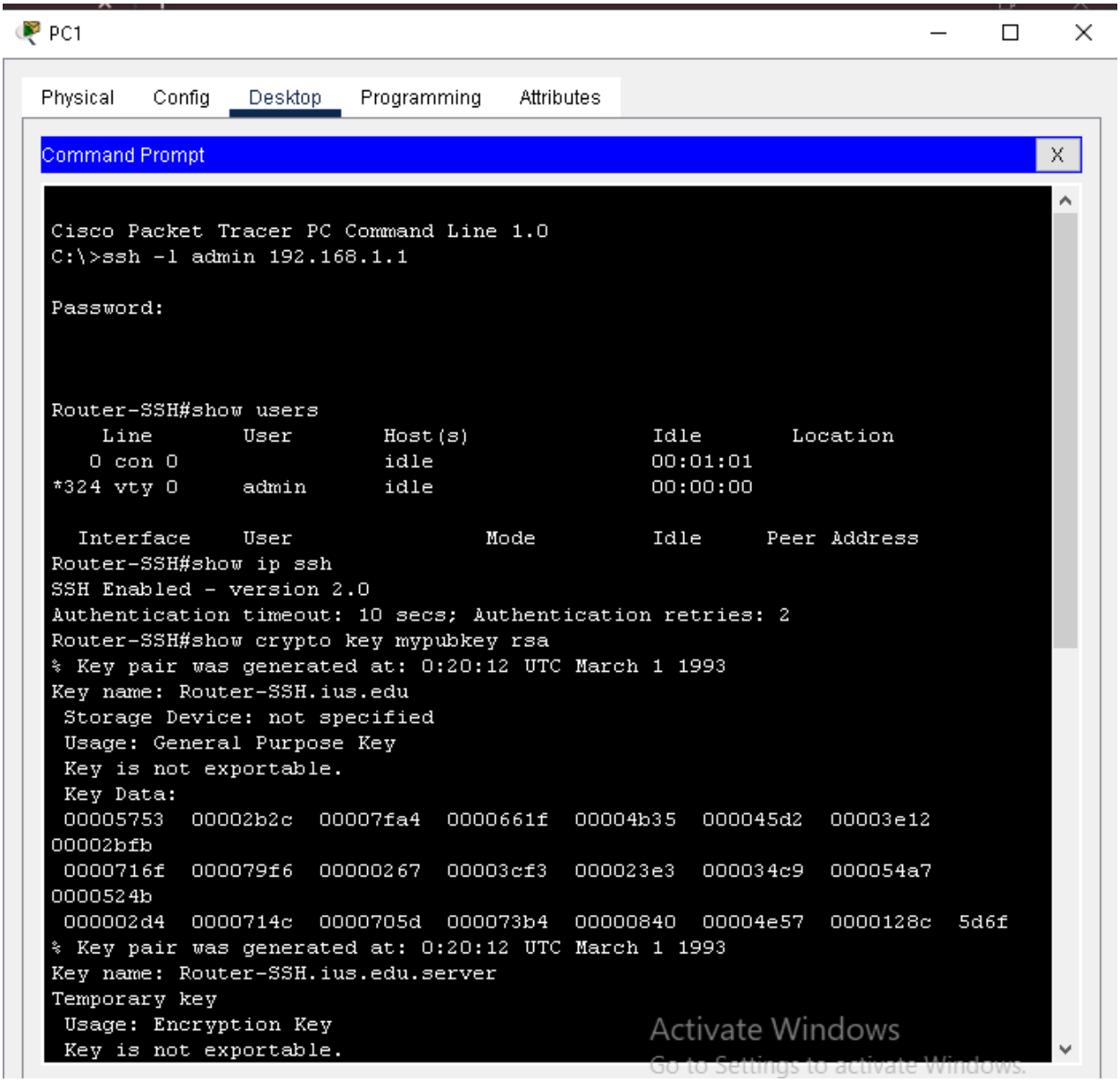
   Le nom d'utilisateur et le mot de passe.
   - Les commandes effectuées et le contenu
   - Les commandes de contrôle
     Par exemple : la taille de la fenêtre du terminal…
     Le type de terminal utilisé.

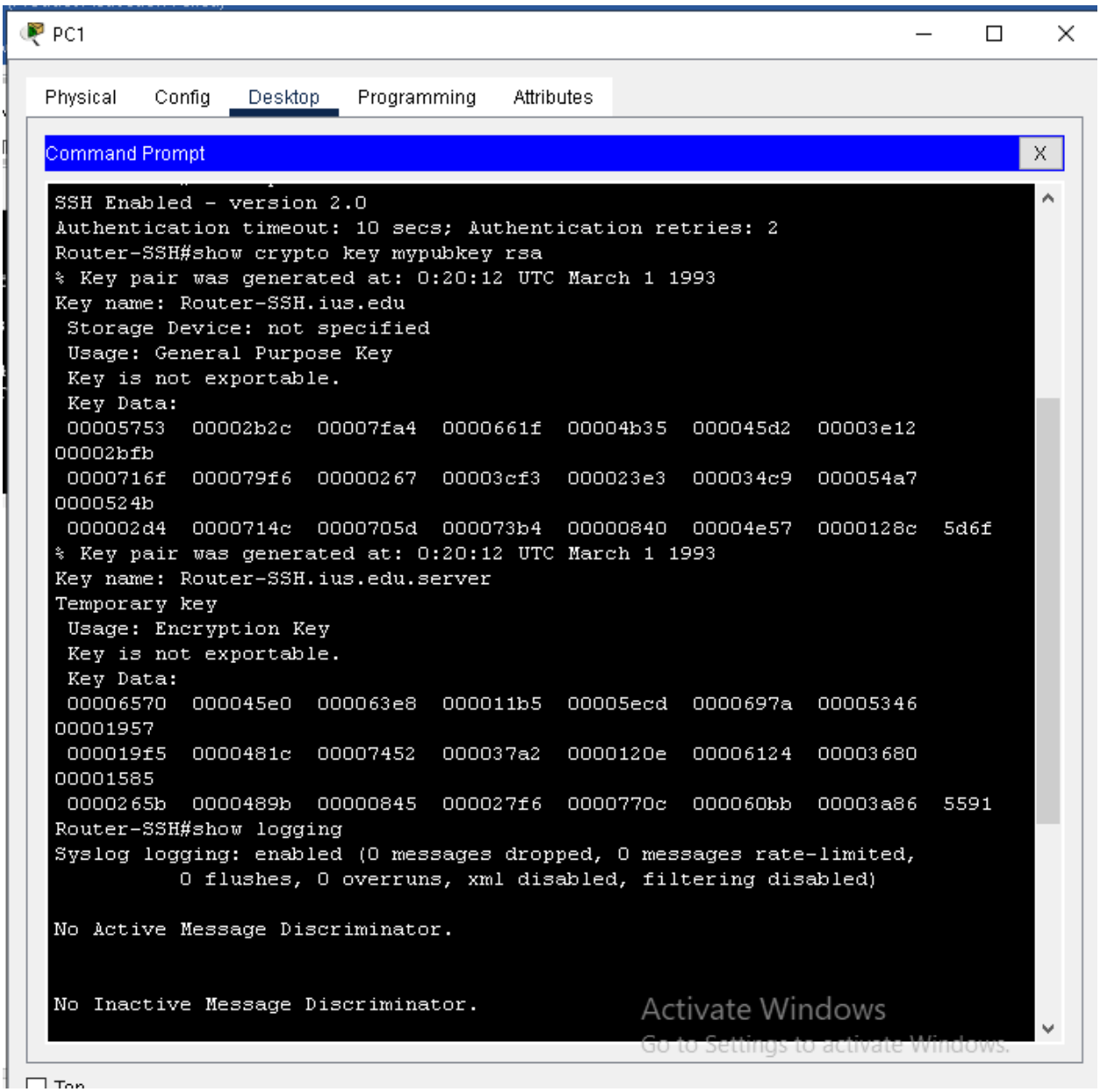
   NB : Toutes ces données sont fournies en texte brut.

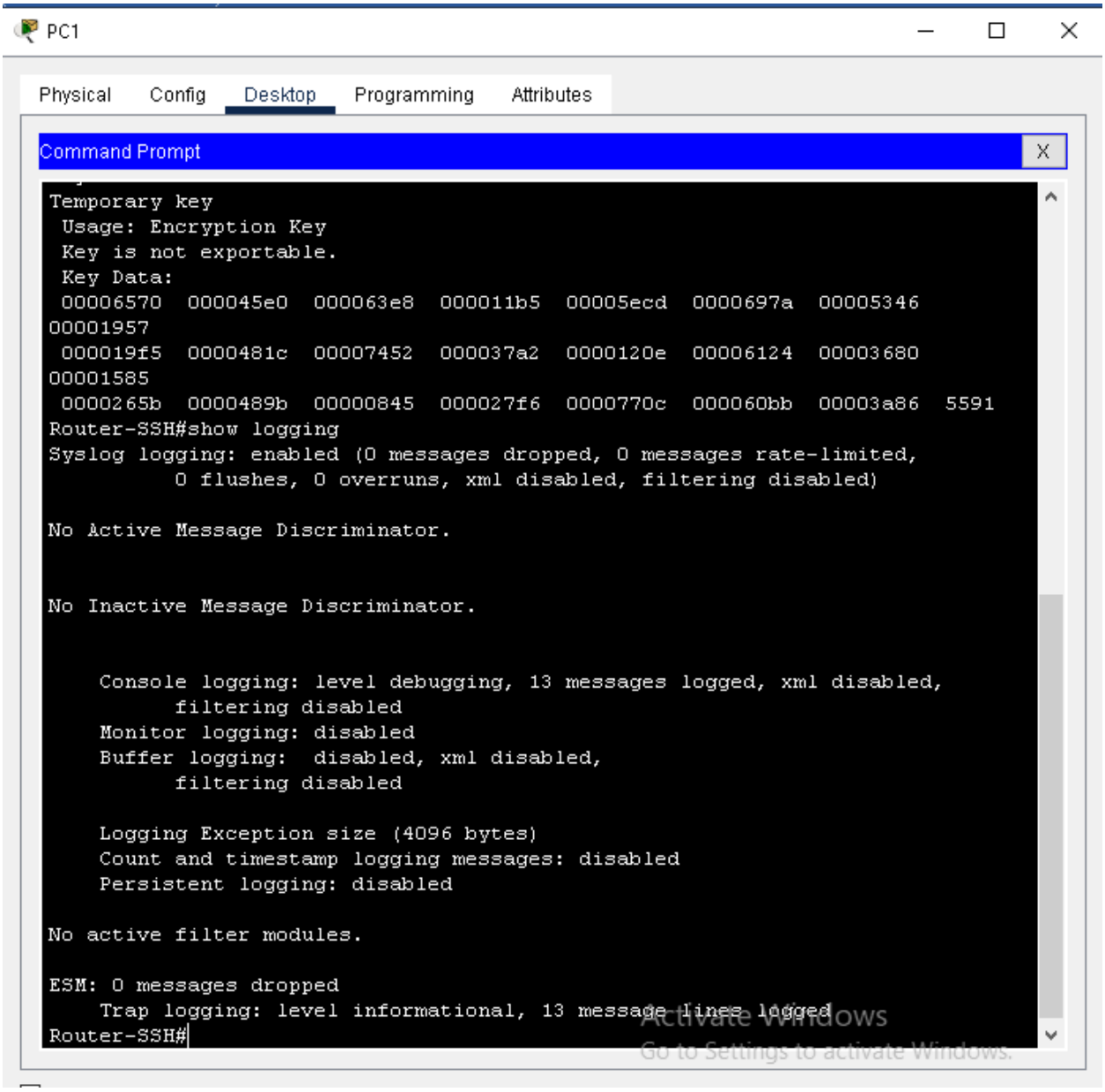
3. Pourquoi est-il déconseillé d'utiliser Telnet en production ?
   Utiliser Telnet en production est considéré comme une faute professionnelle très grave en sécurité informatique, parce que **les données circulent en clair**, à causes **des attaques man-in-the-middle** (l'homme du milieu) , le risque avec Telnet le pirate peut intercepter la communication entre votre ordinateur et le serveur, voler des informations données ou modifier des commandes effectuées, **absence d'authentification forte,** en production il est recommandé d'utiliser les clés cryptographiques ou la double authentification comme garanti de sécurité mais sur Telnet il suffit de se connecter avec ses identifiants pour avoir un accès complet , **problème de conformité légal,** si votre entreprise gère des données clients ou bancaires, utiliser Telnet est considéré comme une action illégale vis-à-vis des normes de sécurité.

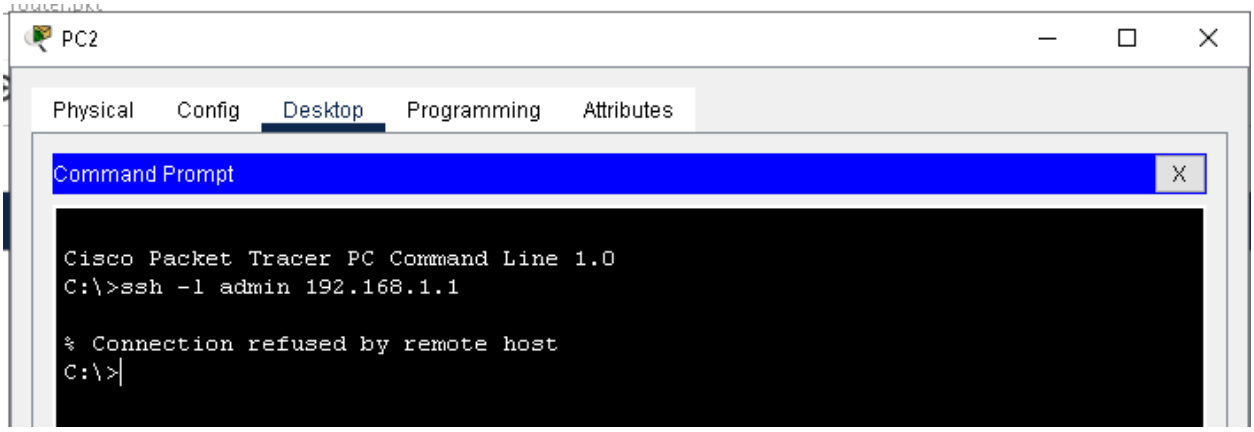
➤ B. Configuration SSH (partie sécurisée)




PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer PC Command Line 1.0
C:\>ssh -l admin 192.168.1.1
Password:
Router-SSH#show users
Line User Host(s) Idle Location
0 con 0 idle 00:01:01
*324 vty 0 admin idle 00:00:00
Interface User Mode Idle Peer Address
Router-SSH#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 10 secs; Authentication retries: 2
Router-SSH#show crypto key mypubkey rsa
% Key pair was generated at: 0:20:12 UTC March 1 1993
Key name: Router-SSH.ius.edu
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00005753 00002b2c 00007fa4 0000661f 00004b35 000045d2 00003e12
00002bfb
0000716f 000079f6 00000267 00003cf3 000023e3 000034c9 000054a7
0000524b
000002d4 0000714c 0000705d 000073b4 00000840 00004e57 0000128c 5d6f
% Key pair was generated at: 0:20:12 UTC March 1 1993
Key name: Router-SSH.ius.edu.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Activate Windows
Go to Settings to activate Windows.


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
SSH Enabled - version 2.0
Authentication timeout: 10 secs; Authentication retries: 2
Router-SSH#show crypto key mypubkey rsa
% Key pair was generated at: 0:20:12 UTC March 1 1993
Key name: Router-SSH.ius.edu
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
00005753 00002b2c 00007fa4 0000661f 00004b35 000045d2 00003e12
00002bfb
0000716f 000079f6 00000267 00003cf3 000023e3 000034c9 000054a7
0000524b
000002d4 0000714c 0000705d 000073b4 00000840 00004e57 0000128c 5d6f
% Key pair was generated at: 0:20:12 UTC March 1 1993
Key name: Router-SSH.ius.edu.server
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00006570 000045e0 000063e8 000011b5 00005ecd 0000697a 00005346
00001957
000019f5 0000481c 00007452 000037a2 0000120e 00006124 00003680
00001585
0000265b 0000489b 00000845 000027f6 0000770c 000060bb 00003a86 5591
Router-SSH#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Activate Windows
Go to Settings to activate Windows.
Top


PC1
Physical
Config
Desktop
Programming
Attributes
Command Prompt
X
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
00006570 000045e0 000063e8 000011b5 00005ecd 0000697a 00005346
00001957
000019f5 0000481c 00007452 000037a2 0000120e 00006124 00003680
00001585
0000265b 0000489b 00000845 000027f6 0000770c 000060bb 00003a86 5591
Router-SSH#show logging
Syslog logging: enabled (0 messages dropped, 0 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)
No Active Message Discriminator.
No Inactive Message Discriminator.
Console logging: level debugging, 13 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, 13 message lines logged
Router-SSH#
Activate Windows
Go to Settings to activate Windows.


PC2
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 ?
   La différence entre ces deux clés réside dans l'architecture te la sécurité. SSH1 est constitué d'un noyau monolithique alors que SSH2 est plutôt constitué de 3 couches (La couche de transport, la couche d'authentification et la couche de connexion). Utiliser SSH1, c'est s'exposer aux risques de se faire attaquer et le pirate ne laisse aucune trace alors qu'avec SSH2, on ne peut pas entrer dans le système sans la bonne combinaison, d'autant plus que toute intrusion est signalé. L'utilisation de SSH1 est devenue obsolète depuis plus de 20 ans.

2. Pourquoi RSA 1024 bits n'est plus recommandé ?
   Parce que de nos jours, la clé RSA est devenue impuissante pour résister à l'attaque des pirates vu qu'elle est faite de combinaison de 4 chiffres (0000 à 9999) et que de nos jours il est facile pour un pirate avec l'aide d'un robot exécutant 1000 codes par secondes de s'introduire dans le système.

3. Que se passe-t-il si on désactive le domaine local ?
   La désactivation du domaine local (va no ip domain-lookup) empêche la résolution DNS automatique, mais ne bloque pas SSH si le nom d'hôte et le domaine sont déjà configure (ip domain-name). Sans cela, la configuration SSH peut échouer.

Conclusion

Ce TD nous a permis de renforcer la sécurité des accès distants aux équipements réseau en configurant Telnet et SSH de manière sécurisé. Nous avons mis en place des niveaux d'utilisateurs, des ACL, des protections contre les attaques (brute-force, timeout), et assure la supervision des connexions.