



 **Rex0519** Update CR2.md

Latest commit 292c09d now  History

1 contributor

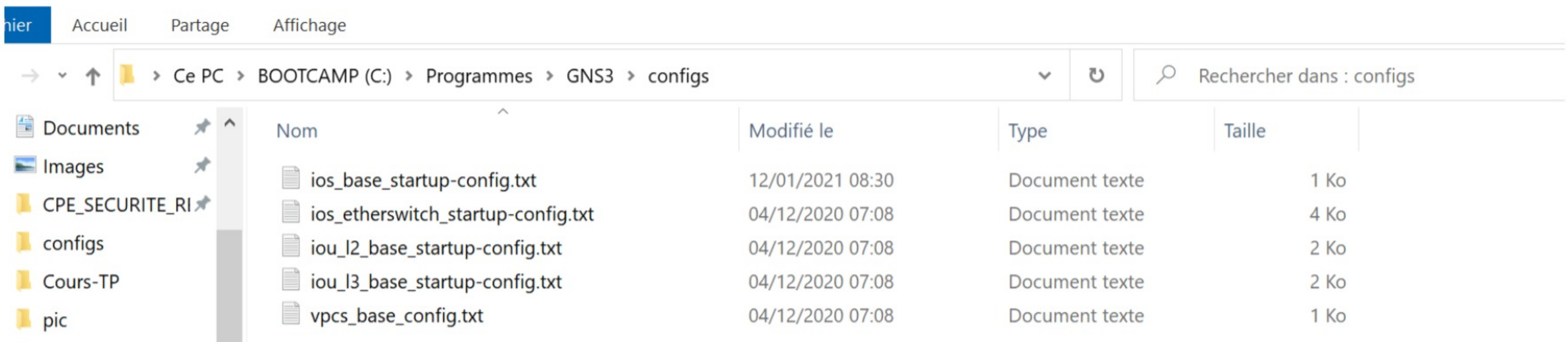
103 lines (61 sloc) | 3.72 KB

[Raw](#) [Blame](#)   

#CR2

AUGMENTER LA SÉCURITÉ D'ACCÈS

sécurité de config par défaut



'no privilege level 15' On ajoute 'no' avant privilege level 15 pour annuler le privilege trop haute pour le vty et aux.

Après bien configuré user, il faut ajouter le permit pour vty. par exemple 'transport input telnet'

'enable password' est pour créer un MDP clair. C'est à dire qu'il peut être vu directement dans le config.txt.

'enable secret' crée un MDP caché par Vigenère cipher qui est bien obscuré.

niv| nom x<5 | Vigenère cipher 5 | md5 8 |sha256 9 |crypted

'enable algorithm-type md5 sha256 crypted' est générer un MDP le plus fort dans le système.

implement username pour login mode enable

Si nous voulons un username et MDP pour agumenter la sécurité, on bascule à la commande suivant:

'#username Fabiola algorithm-type scrypt secret fabiola123' mais on arrive pas en mode login avec username, il faut l'activer dans 'line console 0', saisie la commande 'login local'



'show users' 'show line' montre des infos des sessions on a créé.

banner information

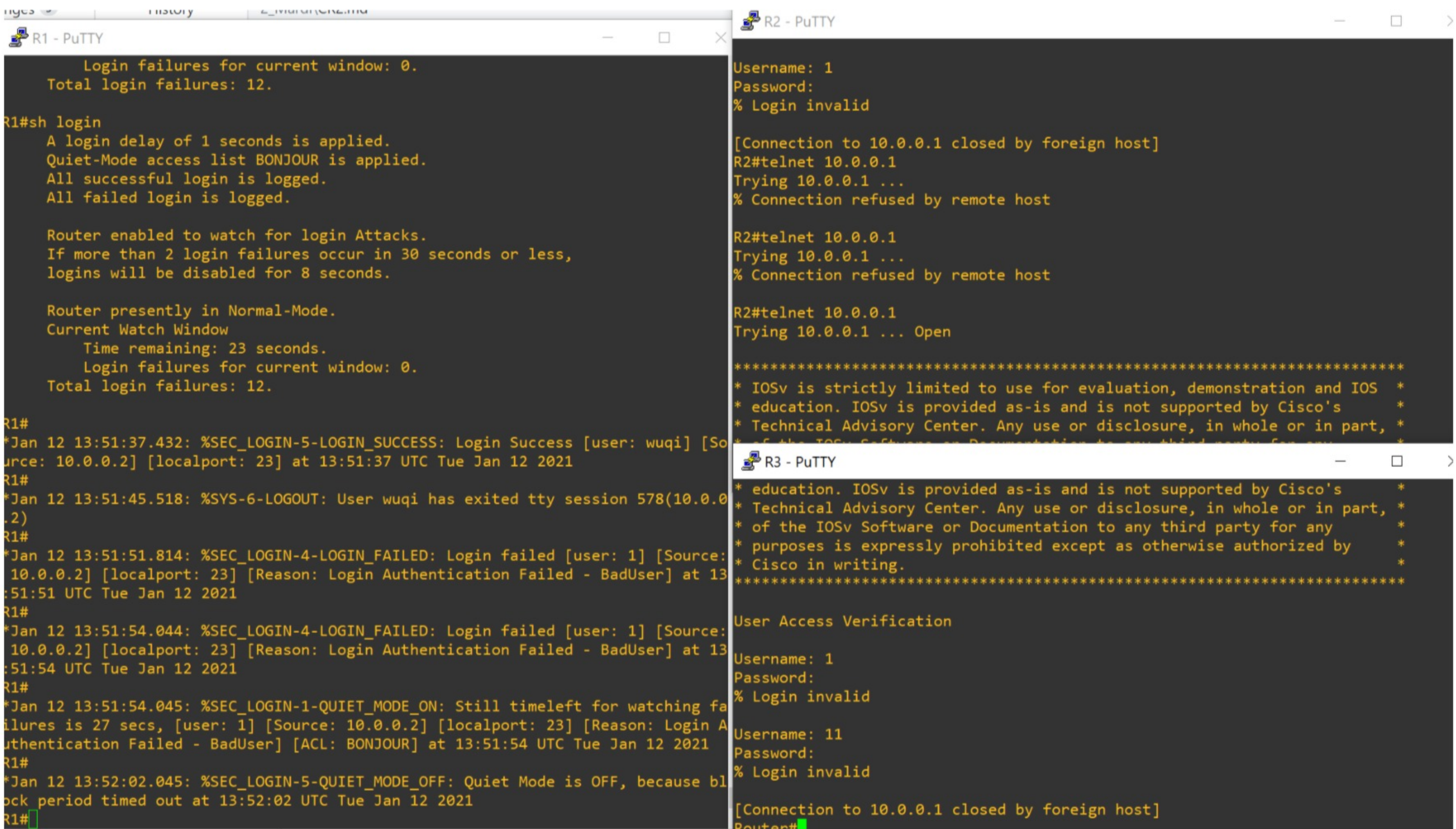
syntax 'banner motd | exec | login'

dans le mode config, on saisie banner motd avec un '#' et ensuite le message qui est terminé par un autre '#'.

► plus d'infos en anglais

Explication syntax

- 'login block-for seconds1 attempts tries within seconds2' S'il y tries fois de login pendant seconds2 secondes, bloquer le dans seconds1 secondes
- 'login quiet-mode access-class acl' si l'adress IP de routeur est dans ce list, ignorer ce block. syntax 'ip access-list standard nom de ACL', 'permit adress-IP'.

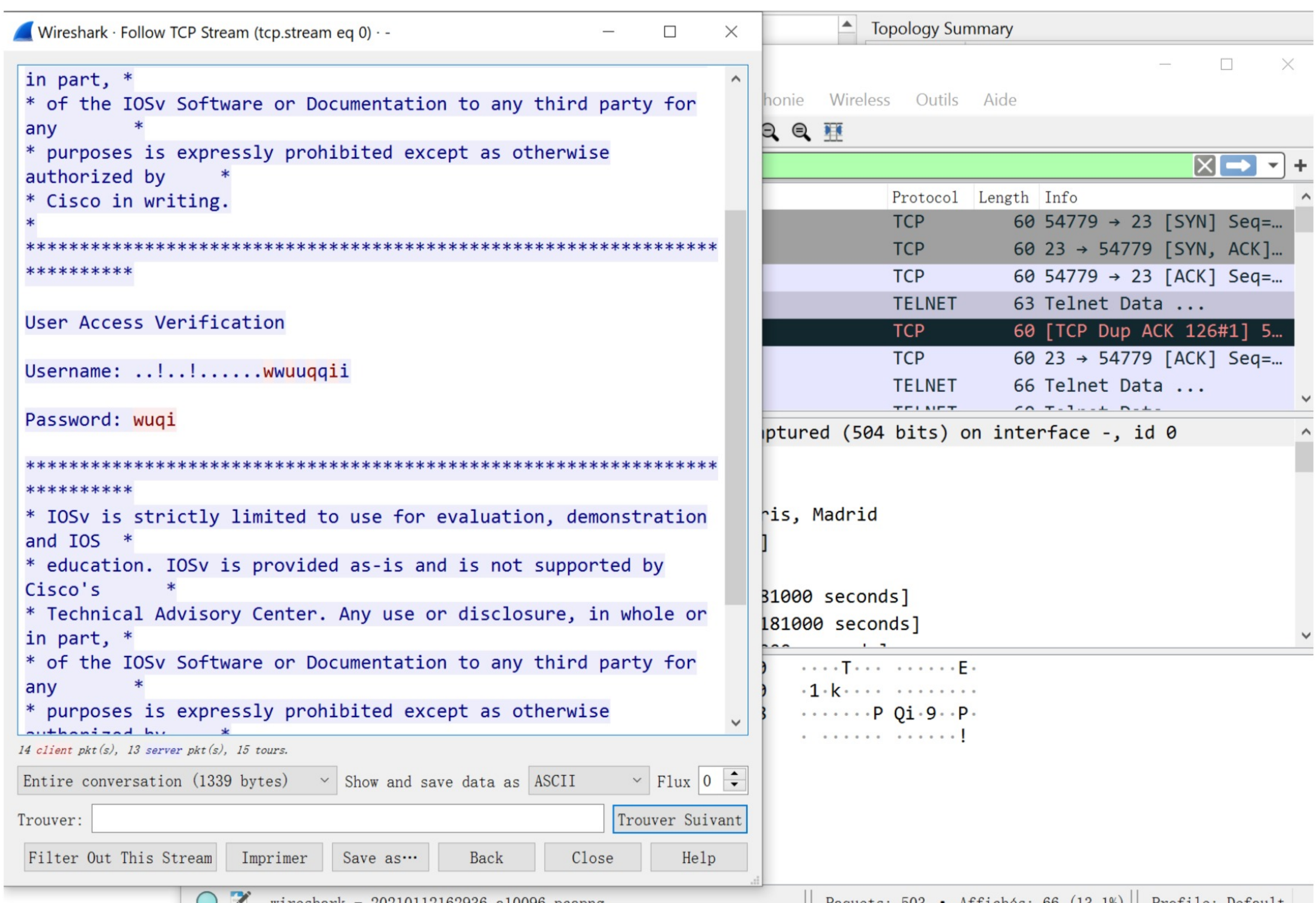


- 'login delay seconds' delais après chaque saisi
- 'login on-success log' et 'login on-failure log' affiche un msg dans CLI du LHOST.

- si l'on est dans 'sh login', on peut observer le mode actuel: Normal-mode ou silence mode. ça depend à l'état block-for.

sécurité SSH

le packet telnet est envoyé en clear-text. Et c'est tres facile de capter par analyseur packet



On utilise ainsi SSH(secu SH).

'ip domain-name crackcpe.com'

'crypto key generate rsa general-keys modulus 2048'

c'est pour créer des clés public et privé qui laissent SSH chiffrement et décrypter des packets.

'ip ssh version 2'

'username chiant algorithm-type scrypt secret chiant12345'

R1(config)#line vty 0 4

R1(config-line)#login local

R1(config-line)#transport input ssh

R1(config-line)#exit ""

