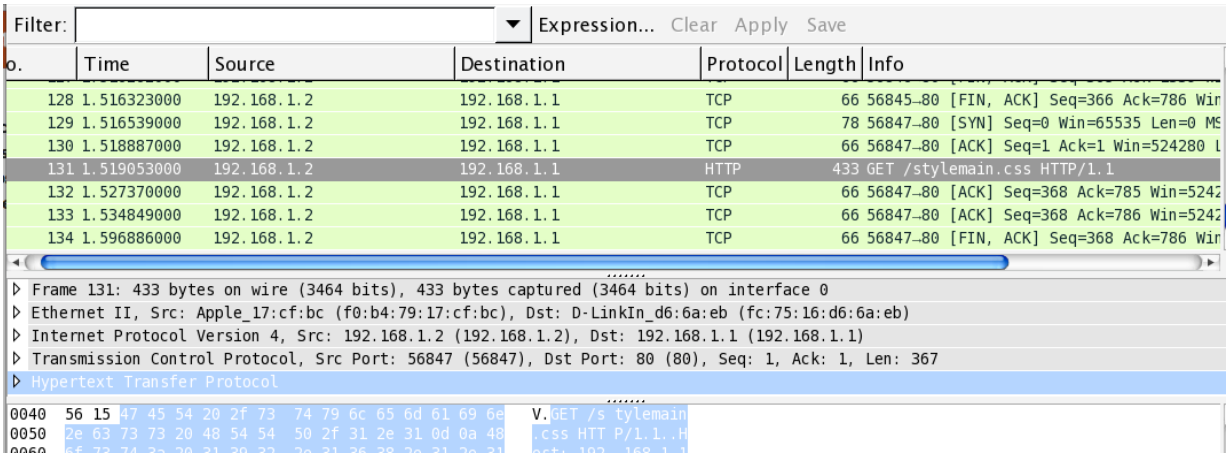
UNIVERSITE ASSANE SECK DE ZIGUINCHOR 2022-2023
♦◊♦♦◊♦♦◊♦◊♦
UFR Sciences et Technologies
♦◊♦♦◊♦
Département d'informatique

Semestre 1 Licence 3 Ingénierie Informatique Cours de Sécurité des réseaux

TP1 : Sécurité Telnet, SSH, Point d'accès (http) etc.

But

L'objectif de ce Lab est de sniffer un mot de passe avec Wireshark. Un mot de passe saisis depuis une interface web peut être intercepté (si https n'est pas utilisé).
Nous allons étudier le cas de l'authentification sur un point d'accès en vue de le configurer à travers une interface web.
Si on suppose que l'interface web du point d'accès est accessible via l'url http://192.168.1.1 par exemple.
Lancer l'analyseur et faites une capture en ne capturant que les paquets en provenance ou à destination de 192.168.1.1.
Ouvrir le navigateur et saisir http://192.168.1.1 dans la barre d'adresse.
Saisir le nom d'utilisateur et le mot de passe pour accéder aux paramètres de configuration du AP
Dans la fenêtre contenant la liste des trames capturées, sélectionner le protocole http avec la méthode GET.
Dans la fenêtre d'affichage de la pile des protocoles décodés, cliquer sur hypertex transfer Protocol.



Dans la fenêtre des protocoles décodés, cliquer sur ***Authorization***, dans ***Credentials*** se trouvent les identifiants de l'utilisateur.

Lab 3: sécurité de TELNET et de SSH

L'objectif de ce Lab est de configurer le routeur pour l'accès Secure Shell (SSH) et d'analyser une session Telnet et une session SSH avec Wireshark.

SSH doit remplacer Telnet pour les connexions relatives à la gestion. Telnet utilise des communications non sécurisées en texte clair. SSH assure la sécurité des connexions distantes en fournissant un chiffrement efficace de toutes les données transmises entre les périphériques. Dans cet exercice, vous allez sécurisé un commutateur distant avec le chiffrement de mot de passe et SSH.

Au cours de ces travaux pratiques, vous allez configurer un routeur pour qu'il accepte les connexions SSH, et vous utiliserez Wireshark pour capturer et afficher des sessions Telnet et SSH.

1. Connecter physiquement et logiquement (adressage IP) le PC au retour puis tester la communication avec la commande **ping**.

2. Configurer le routeur pour qu'il accepte les connexions SSH sur les lignes VTY

- Configurez le nom du périphérique.

  Router(config)# hostname R1

- Configurez le domaine du périphérique.

  R1(config)# ip domain-name univ-zig.sn

3. Configurez la méthode de la clé de chiffrement.

- R1(config)#crypto key generate rsa

  The name for the keys will be: R1.univ-zig.sn

  Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

  How many bits in the modulus [512]:

- Taper **1024** comme taille de la clé

4. Configurez un nom d'utilisateur de base de données locale.

  R1(config)# username admin privilege 15 secret adminpass

  Remarque: un privilège de niveau 15 offre à l'utilisateur des droits d'administrateur

5. Activez SSH sur les lignes VTY.

- Activez Telnet et SSH sur les lignes VTY entrantes à l'aide de la commande **`transport input`**

R1(config)#line vty 0 4

R1(config-line)#transport input telnet

R1(config-line)#transport input ssh

- Modifiez la méthode de connexion de façon à ce que la base de données locale soit utilisée pour la vérification de l'utilisateur.

R1(config-line)# login local

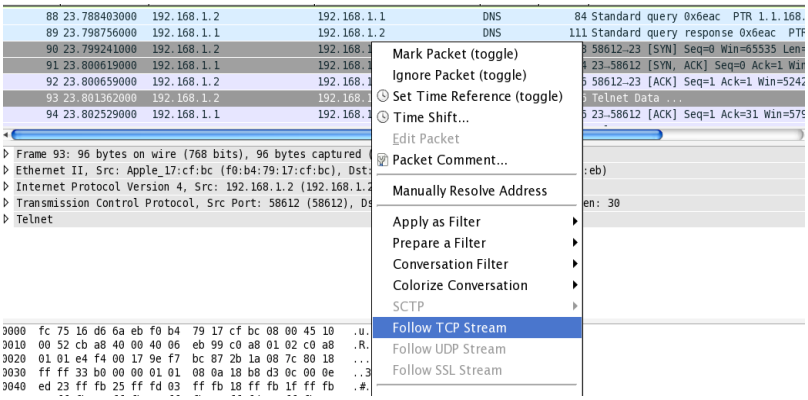
R1(config-line)# end

6. Analyser une session Telnet avec Wireshark

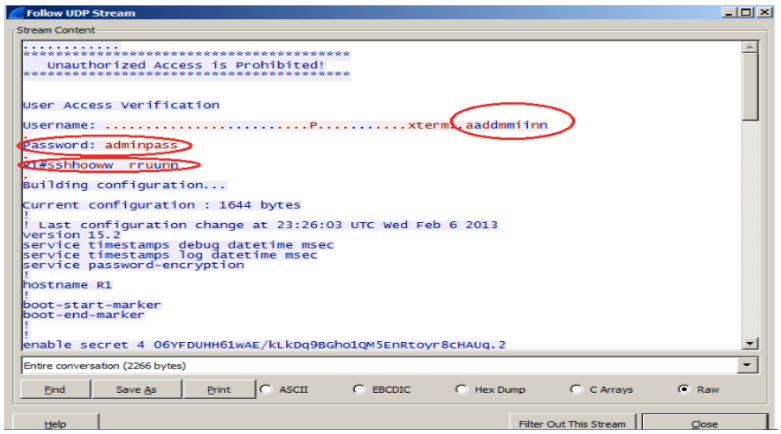
– Démarrez une session Telnet avec votre terminal pour accéder à l'interface du routeur 192.168.1.1 et sélectionnez la case d'option Service Telnet et dans le champ Hôte, entrez 192.168.1.1

- Arrêtez la capture Wireshark, et appliquez un filtre Telnet sur les données de capture Wireshark.

- Utilisez la fonction Follow TCP Stream dans Wireshark pour afficher la session Telnet



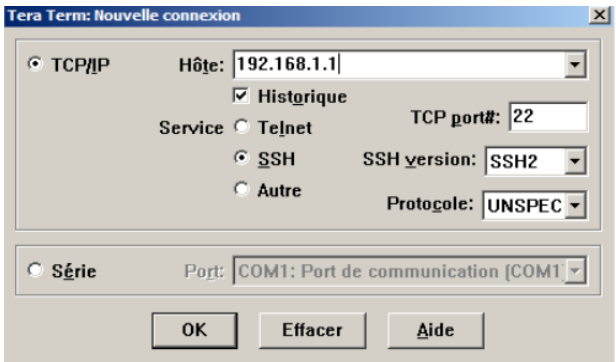
- La fenêtre Follow TCP Stream (Suivre le flux TCP) affiche les données de votre session Telnet avec le
routeur. La session complète s'affiche en texte clair, y compris votre mot de passe. Notez que le nom de
l'utilisateur s'affiche avec des caractères en double. Cela provient du paramètre d'écho dans Telnet qui vous permet d'afficher les caractères que vous tapez à l'écran.



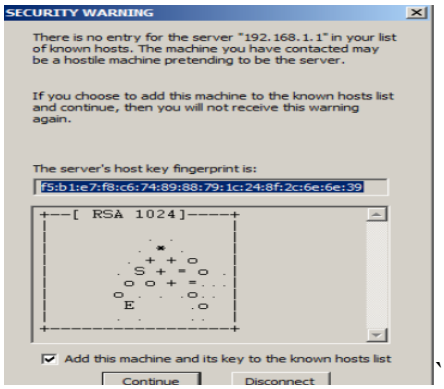
7. Analyser une session SSH avec Wireshark

- Ouvrez Wireshark et commencez à capturer des données sur l'interface LAN.

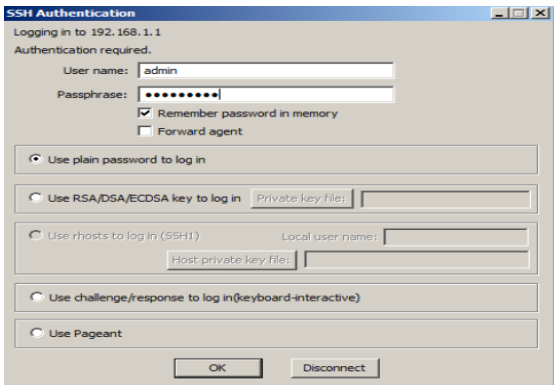
- Démarrez une session SSH sur le routeur via votre terminal et entrez l'adresse IP de l'interface du routeur puis vérifiez que la case d'option SSH est sélectionnée, puis cliquez sur OK pour vous connecter au routeur.



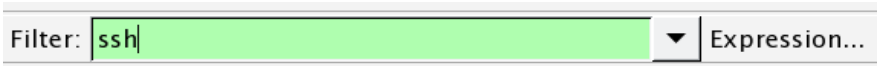
- La première fois que vous avez établi une session SSH à un périphérique, un avertissement de sécurité (SECURITY WARNING) vous informe que vous ne vous êtes pas encore connecté à ce périphérique. Ce message fait partie du processus d'authentification. Lisez l'avertissement de sécurité, puis cliquez sur Continue.



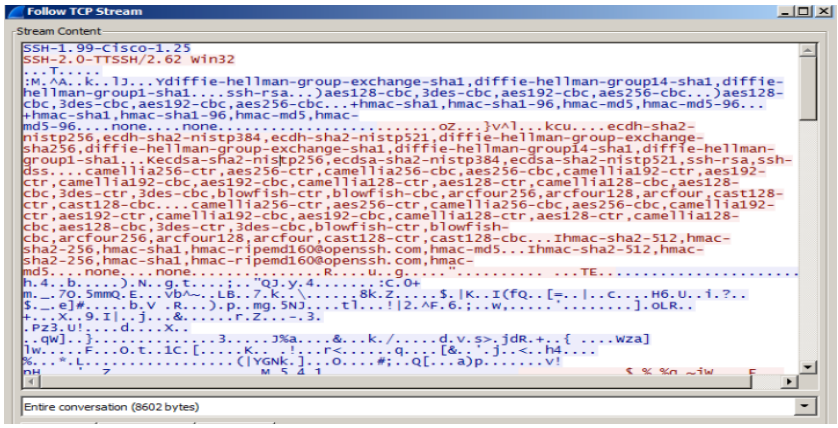
- Dans la fenêtre d'authentification SSH, entrez **admin** comme nom d'utilisateur et **adminpass** pour le mot de passe. Cliquez sur OK pour accéder au routeur



- Arrêtez la capture Wireshark et appliquez un filtre SSH sur les données de capture Wireshark.
-
-



-
- Utilisez la fonction Follow TCP Stream dans Wireshark pour afficher la session SSH.
- Cliquez avec le bouton droit sur l'une des lignes SSHv2 dans la section Packet list (Liste des paquets) de Wireshark et, dans la liste déroulante, sélectionnez l'optionFollow TCP stream (Suivre le flux TCP)
- Examinez la fenêtre Follow TCP Stream (Suivre le flux TCP)de votre session SSH. Les données ont été chiffrées et sont illisibles. Comparez les données de votre session SSH aux données de votre session Telnet


Follow TCP Stream
Stream Content
SSH-1.99-Cisco-1.25
SSH-2.0-TTSSH/2.62 Win32
Entire conversation (8602 bytes)