Laboratorium - Dostęp do urządzeń sieciowych za pomocą SSH

Topologia

Tabela adresacji

Urządzenie	Interfejs	Adres IP	Maska podsieci	Brama domyślna
R1	G0/1	192.168.1.1	255.255.255.0	Nie dotyczy
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	Karta sieciowa	192.168.1.3	255.255.255.0	192.168.1.1

Cele

Część 1: Konfiguracja podstawowych ustawień urządzenia

Część 2: Konfiguracja dostępu do routera poprzez SSH

Część 3: Śledzenie sesji Telnet za pomocą programu Wireshark

Część 4: Śledzenie sesji SSH za pomocą programu Wireshark

Część 5: Konfiguracja dostępu do przełącznika poprzez SSH

Część 6: Użycie sesji SSH na przełączniku za pomocą wiersza poleceń

Scenariusz

Telnet w przeszłości był powszechnym i szeroko stosowanym protokołem używanym do zdalnego konfigurowania urządzeń sieciowych. Protokoły takie jak Telnet nie posiadają mechanizmu szyfrowanego uwierzytelniania i nie szyfrują informacji wysyłanych miedzy klientem a serwerem. Pozwala to snifferom sieciowym na przechwytywanie haseł oraz konfiguracji.

Secure Shell (SSH) jest protokołem sieciowym który pozwala zestawić bezpieczne połączenie terminalowe do routera lub innych urządzeń sieciowych. SSH szyfruje wszystkie informacje które przechodzą przez sieć i wprowadza mechanizm bezpiecznego uwierzytelniania zdalnego komputera. Profesjonaliści sieciowi szybko zastąpili, używany do zdalnego logowania Telnet protokołem SSH. SSH jest używany przede wszystkim do logowania się do zdalnego urządzenia i wykonywania poleceń, ale można taże wykorzystać SSH do transmisji plików przez protokoły Secure FTP (SFTP) lub Secure Copy Protocol (SCP).

Aby protokół SSH mógł funkcjonować, wymagana jest jego konfiguracja na urządzeniach sieciowych. W tym laboratorium skonfigurujesz serwer SSH na routerze a potem połączysz się z nim używając komputera PC posiadającego zainstalowanego klienta SSH. Połączenia tego typu w sieci lokalnej są zazwyczaj zestawiane poprzez Ethernet i adres IP.

W tym laboratorium będziesz konfigurować router, tak aby zaakceptować połączenie SSH a następnie będziesz używać programu Wireshark do przechwytywania i śledzenia sesji Telnet oraz sesji SSH. Ćwiczenie zaprezentuje znaczenie szyfrowania w SSH. Spróbujesz samodzielnie skonfigurować przełącznik dla połączeń SSH.

Uwaga: Routery używane w laboratorium interaktywnym to Cisco Integrated Services Router 1941 (ISR) z oprogramowaniem Cisco IOS 15.2(4)M3 (obraz universalk9). Przełączniki używane w laboratorium to Cisco Catalyst 2960 z oprogramowaniem Cisco IOS 15.0(2) (obraz lanbasek9). Można używać innych routerów lub przełączników oraz wersji Cisco IOS. Zależnie od modelu urządzenia i wersji systemu IOS dostępne polecenia i wyniki ich działania mogą się różnić od prezentowanych w niniejszej instrukcji. Identyfikatory interfejsów znajdują się w tabeli zestawienia interfejsów routerów na końcu tej instrukcji.

Uwaga: Upewnij się, że konfiguracje routerów i przełączników zostały usunięte i nie mają konfiguracji startowej. Jeśli nie jesteś pewien, poproś o pomoc instruktora.

Wymagane wyposażenie

- 1 router (Cisco 1941 z oprogramowaniem Cisco IOS, wersja 15.2 (4) M3 obraz uniwersalny lub porównywalny)
- 1. przełącznik (Cisco 2960 Cisco IOS wersja15.0 (2) obraz lanbasek9 lub porównywalny)
- 1 komputer PC (z systemem Windows 7, Vista lub XP oraz zainstalowanym emulatorem terminala Tera Term i programem Wireshark)
- Kable konsolowe do konfiguracji urządzeń Cisco przez port konsolowy
- Kable Ethernet zgodnie z pokazaną topologią

Część 1: Konfigurowanie podstawowych ustawień urządzenia

W części 1 będziesz tworzyć topologię sieci oraz konfigurować podstawowe ustawienia takie jak adresy IP, dostęp do interfejsu urządzenia i hasła w routerze.

Krok 1: Połącz okablowanie sieciowe zgodnie z topologią.

Krok 2: Uruchom i zrestartuj router i przełącznik.

Krok 3: Skonfiguruj router.

a. Połącz się przy użyciu konsoli z routerem i przejdź do uprzywilejowanego trybu EXEC.

b. Wejdź do trybu konfiguracji.

c. Aby zapobiec próbom tłumaczenia przez router i przełącznik niepoprawnie wprowadzonych poleceń, jako nazw hostów, wyłącz wyszukiwanie DNS.

d. Jako zaszyfrowane hasło trybu uprzywilejowanego ustaw **class** .

e. Jako hasło dostępu do konsoli ustaw **cisco** oraz włącz logowanie.

f. Jako hasło do VTY ustaw **cisco** oraz włącz logowanie.

g. Zaszyfruj hasła występujące otwartym tekstem.

h. Utwórz baner, który będzie ostrzegał osoby łączące się z urządzeniem, że nieautoryzowany dostęp jest zabroniony.

i. Skonfiguruj i włącz interfejs G0/1 w routerze przy użyciu informacji zawartych w tabeli adresowania.

j. Zapisz konfigurację bieżącą (running-configuration) jako plik konfiguracji startowej (startup-configuration).

Krok 4: Skonfiguruj PC-A.

a. Skonfiguruj adres IP i maskę podsieci dla komputera PC-A.

b. Skonfiguruj bramę domyślną dla komputera PC-A.

Krok 5: Zweryfikuj połączenie sieciowe.

Wykonaj ping od PC-A z R1. Jeżeli ping nie powiedzie się, to poszukaj rozwiązania problemu.

Część 2: Konfigurowanie routera dla zdalnego dostępu poprzez SSH

Korzystanie z usługi Telnet do łączenia się z urządzeniami sieciowymi jest niebezpieczne, ponieważ wszystkie informacje są wysyłane otwartym tekstem. Zalecane jest używanie protokołu SSH dla połączeń zdalnych, ponieważ SSH szyfruje dane sesji oraz zapewnia mechanizm uwierzytelniania urządzenia. W części 2 będziesz konfigurować linie VTY routera w celu akceptacji połączenia SSH, .

Krok 1: Skonfiguruj uwierzytelnianie urządzenia.

Do generowania klucza szyfrującego RSA używane są nazwa urządzenia i nazwa domeny. Dlatego nazwy te muszą być wprowadzone przed wydaniem polecenia **crypto key**.

a. Skonfiguruj nazwę urządzenia.

```
Router(config)# hostname R1
```

b. Skonfiguruj domenę dla tego urządzenia.

```
R1(config)# ip domain-name ccna-lab.com
```

Krok 2: Skonfiguruj klucz szyfrowania.

```
R1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

Krok 3: Skonfiguruj nazwę użytkownika w lokalnej bazie danych.

```
R1(config)# username admin privilege 15 secret adminpass
R1(config)#
*Feb  6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
R1(config)#
```

Uwaga: Poziom uprawnień 15 daje użytkownikowi prawa administratora.

Krok 4: Włącz SSH na liniach VTY.

a. Włącz Telnet oraz SSH na liniach wejściowych VTY za pomocą polecenia **transport input** .

```
R1(config)# line vty 0 4
R1(config-line)# transport input telnet ssh
```

b. Zmień metodę logowania do lokalnej bazy danych w celu weryfikacji użytkownika.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

Krok 5: Zapisz konfigurację bieżącą (running-configuration) do pliku konfiguracji startowej (startup-configuration).

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Część 3: Śledzenie sesji Telnet za pomocą programu Wireshark

W części 3 będziesz używał programu Wireshark do przechwytywania i obserwacji danych przesyłanych w czasie sesji Telnet na routerze. Będziesz korzystać z programu Tera Term w celu połączenia się z R1 za pomocą telnetu, zalogowania się a następnie używania polecenia show na routerze.

Uwaga: Jeżeli pakiet oprogramowania typu klient Telnet/SSH nie jest zainstalowany na twoim komputerze PC, to przed kontynuowaniem ćwiczenia należy go zainstalować. Dwa popularne darmowe pakiety Telnet/SSH to Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) oraz PuTTy (www.putty.org).

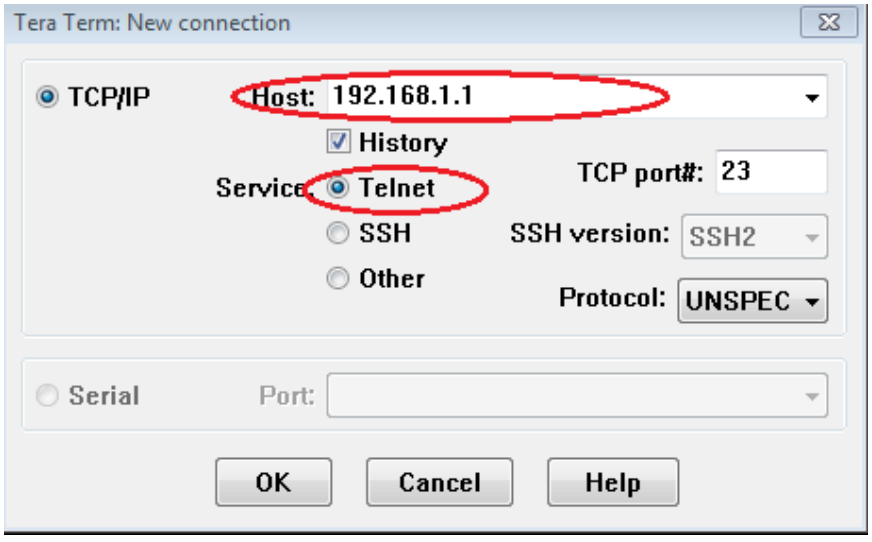
Uwaga: Domyślnie telnet nie jest dostępny w wierszu poleceń w Windows 7. Aby umożliwić korzystanie z Telnet w w wierszu poleceń, kliknij **Start** > **Panel Sterowania** > **Programy** > **Programy i funkcje** > **Włącz lub wyłącz funkcje systemu Windows**. Zaznacz pole wyboru **Klient Telnet** , a potem kliknij przycisk **OK**.

Krok 1: Uruchom program Wireshark i rozpocznij przechwytywanie pakietów danych z interfejsu LAN

Uwaga: Jeżeli nie możesz uruchomić przechwytywania na interfejsie LAN, to może będziesz musiał uruchomić program Wireshark za pomocą opcji **Uruchom jako Administrator**.

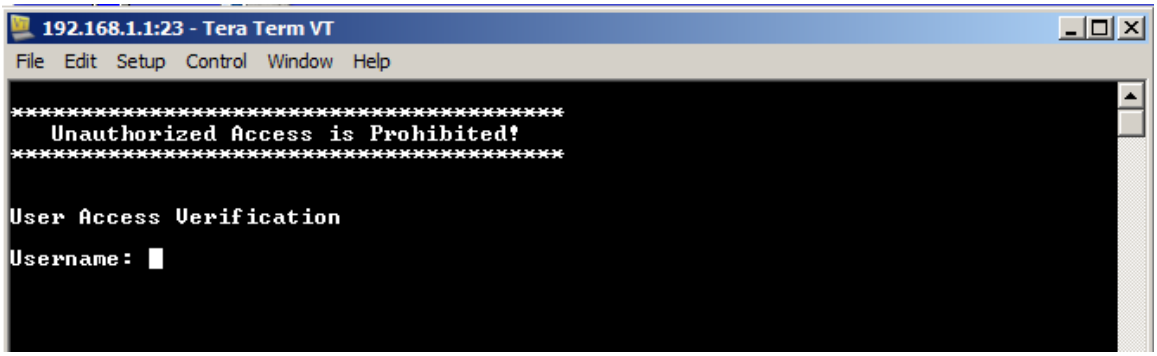
Krok 2: Rozpocznij sesję Telnet do routera.

a. Uruchom program Tera Term zaznacz opcję **Telnet**, a w polu Host wpisz **192.168.1.1**.



Jaki jest domyślny port TCP dla sesji Telnet? _____ Port 23

b. Po zapytaniu o nazwę użytkownika (Username) wpisz **admin** a po zapytaniu o hasło (Password) wpisz **adminpass**. Powyższe zapytania zostały generowane, ponieważ linie VTY skonfigurowałeś tak aby używały lokalnej bazy (polecenie **login local**).



c. Wykonaj polecenie **show run** .

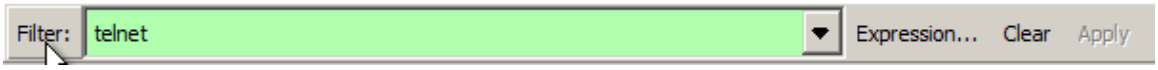
```
R1# show run
```

d. Aby zakończyć sesję Telnet session i wyjść z Tera Term, wpisz **exit** .

```
R1# exit
```

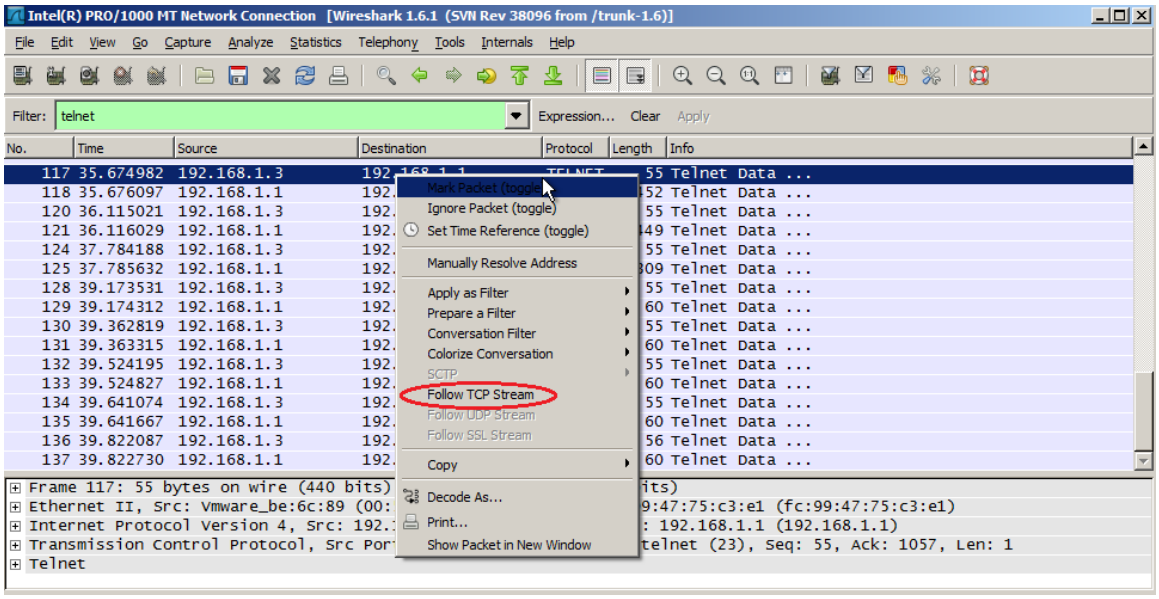
Krok 3: Zatrzymaj przechwytywanie w programie Wireshark.

Krok 4: Zastosuj filtr Telnet dla danych przechwytywanych w Wireshark.

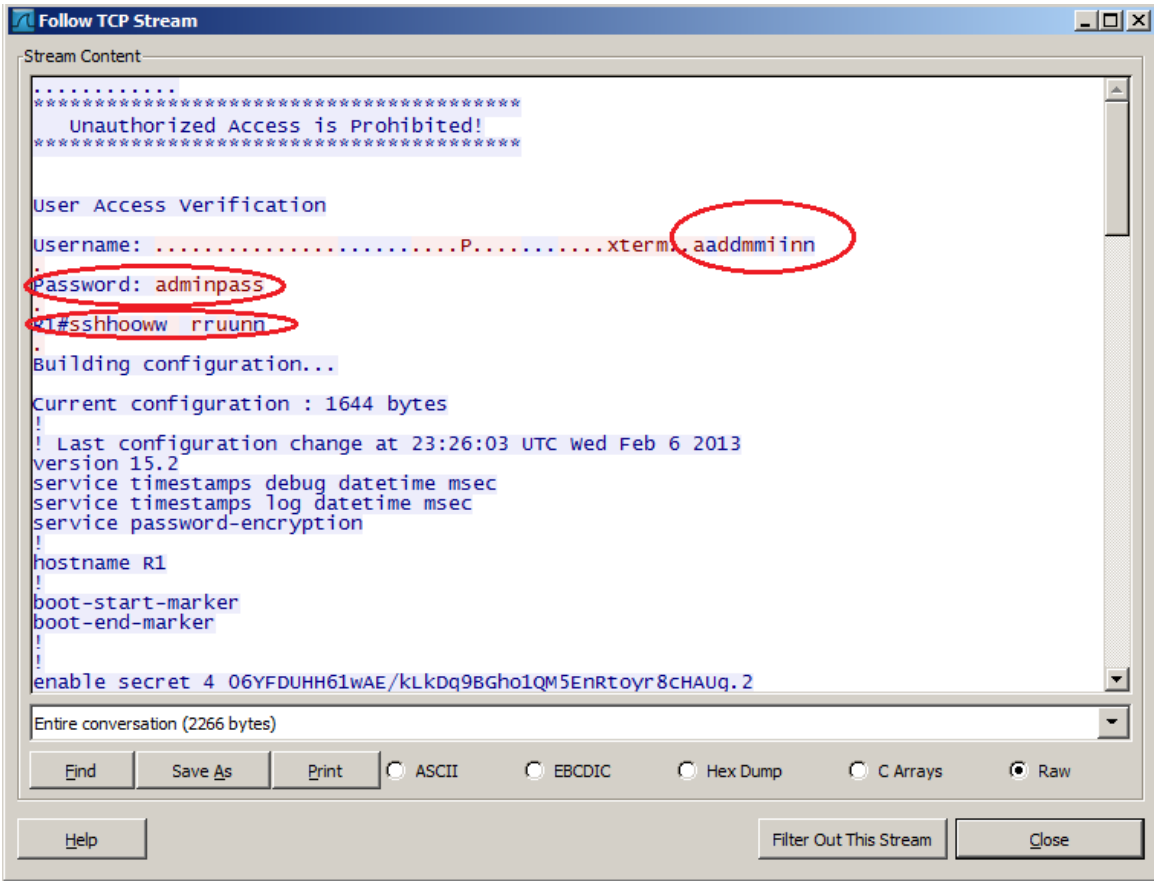


Krok 5: Aby zobaczyć sesję Telnet użyj funkcji "Follow TCP Stream" programu Wireshark.

a. Prawym przyciskiem myszy kliknij jedną z linii **Telnet** w sekcji **Packet list**, rozwiń listę i wybierz **Follow TCP Stream**.



b. Okno Follow TCP Stream wyświetla dane twojej sesji Telnet połączonej z routerem. Cała sesja jest wyświetlana w postaci otwartego tekstu (hasła także). Zauważ, że nazwa użytkownika i polecenia **show run**, które wpisałeś składają się z powtórzonych znaków. Jest to spowodowane przez ustawienie echa w Telnet, które umożliwia wyświetlanie znaków wpisywanych na ekranie.



c. Po zakończeniu oglądania twojej sesji Telnet kliknij **Close** w oknie **Follow TCP Stream**.

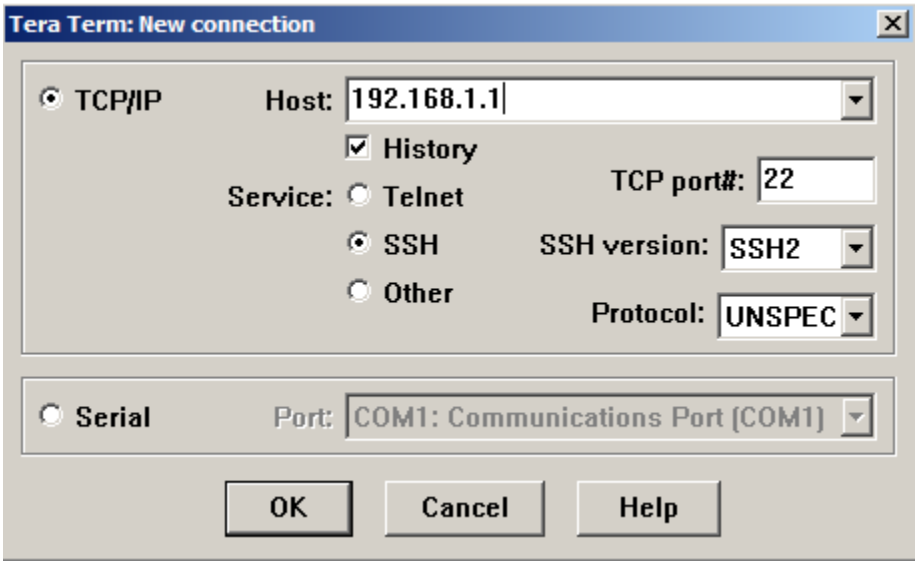
Część 4: Badanie sesji SSH za pomocą programu Wireshark

W części 4 będziesz korzystać z programu Tera Term w celu ustanowienia sesji SSH z routerem. Program Wireshark będzie wykorzystywany do przechwytywania i wyświetlania danych z tej sesji SSH.

Krok 1: Uruchom program Wireshark i rozpocznij przechwytywanie pakietów danych z interfejsu LAN.

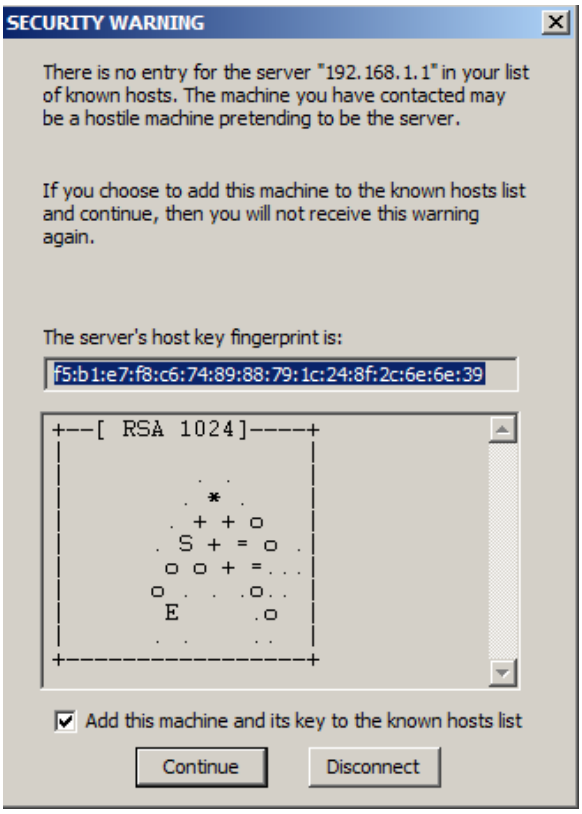
Krok 2: Uruchom sesję SSH na routerze.

a. Otwórz Tera Term a następnie w polu Host: w oknie New Connection wprowadź adres IP dla interfejsu G0/1 routera R1. Upewnij się, czy opcja **SSH** została zaznaczona a potem kliknij **OK** aby połączyć się z routerem.

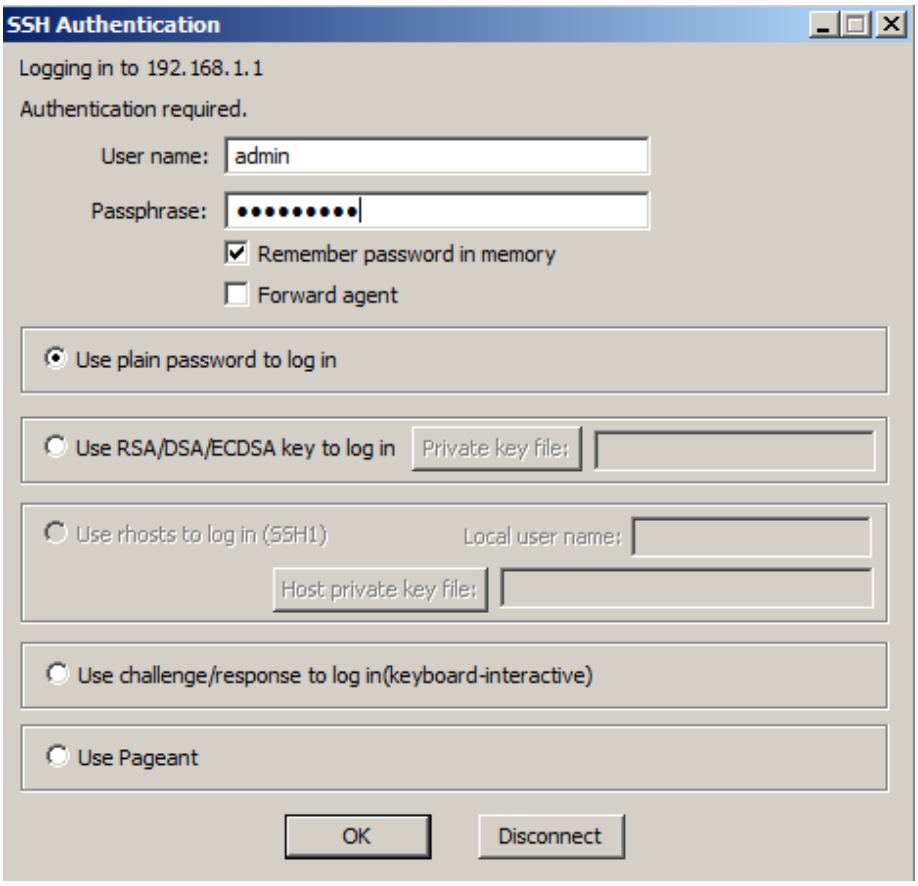


Jaki jest domyślny port TCP dla sesji SSH? _____

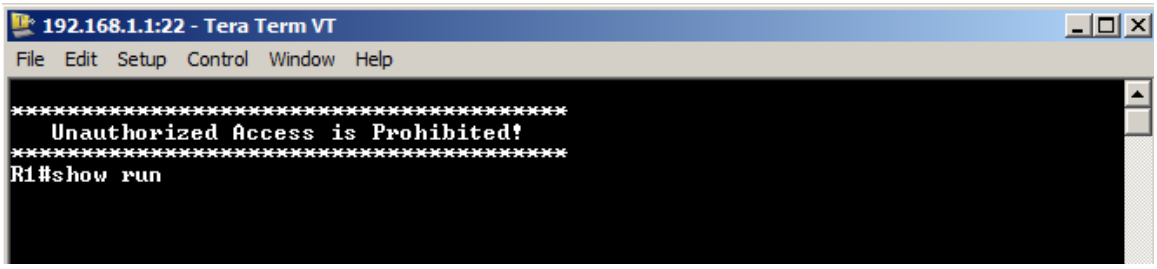
b. Gdy tworzysz sesję SSH do urządzenia po raz pierwszy, to generowane jest **OSTRZEŻENIE O ZABEZPIECZENIACH**, informujące o tym, że wcześniej nie łączyłeś się do tego urządzenia. To ostrzeżenie jest częścią procesu uwierzytelniania. Przeczytaj ostrzeżenie, a następnie kliknij przycisk **Continue**.



c. W oknie SSH Authentication, wpisz **admin** (nazwa użytkownika) oraz hasło **adminpass**. Kliknij przycisk **OK**, aby zalogować się do routera.



d. Ustanowiłeś sesję SSH na routerze. Program Tera Term wygląda bardzo podobne do okna wiersza poleceń. Wykonaj polecenia **show run** w wierszu poleceń.



e. Zakończ sesję SSH oraz wyjdź z programu Tera Term za pomocą polecenia **exit**.

```
R1# exit
```

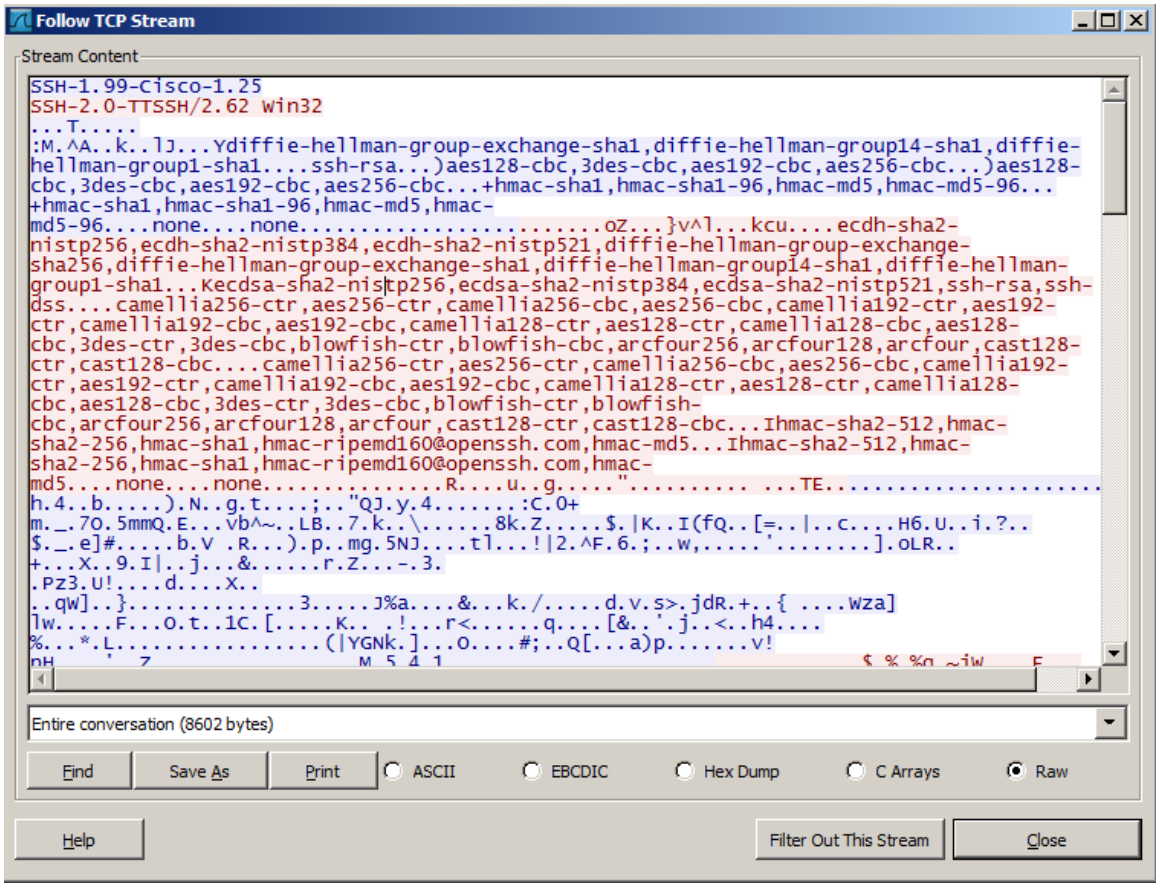
Krok 3: W programie Wireshark zatrzymaj przechwytywanie.

Krok 4: Zastosuj filtr SSH dla danych przechwytywanych w Wireshark.

Krok 5: Aby zobaczyć sesję SSH użyj funkcji "Follow TCP Stream" programu Wireshark.

a. Prawym przyciskiem myszy kliknij jedną z linii **SSHv2** w sekcji **Packet list**, rozwiń listę i wybierz opcję **Follow TCP Stream**.

b. Sprawdź zawartość okna **Follow TCP Stream** w twojej sesji SSH. Dane zostały zaszyfrowane i są nieczytelne. Porównaj dane w sesji SSH z danymi w sesji Telnet.



Dlaczego dla połączeń zdalnych preferowany jest SSH zamiast Telnet?

_____

_____

c. Po zbadaniu sesji SSH kliknij **Close**.

d. Zamknij program Wireshark.

Część 5: Konfiguracja dostępu do przełącznika poprzez SSH

W części 5 będziesz konfigurować przełącznik aby ustanowić połączenie SSH. Jeżeli przełącznik zostanie już skonfigurowany, to ustanów sesję SSH przy użyciu Tera Term.

Krok 1: Skonfiguruj podstawowe ustawienia przełącznika.

Krok 2: Skonfiguruj przełącznik dla połączeń poprzez SSH.

Aby skonfigurować SSH dla przełącznika, zastosuj te same polecenia, których używałeś do konfigurowania SSH na routerze w części 2.

Krok 3: Ustanów połączenie SSH do przełącznika.

Uruchom Tera Term z komputera PC-A, a następnie za pomocą SSH połącz się z interfejsem SVI w S1.

Krok 4: W przypadku wystąpienia problemów spróbuj je rozwiązać.

Czy jesteś w stanie ustanowić sesję SSH do przełącznika?

_____

Część 6: Uruchamianie SSH z linii poleceń CLI w przełączniku

Klient SSH jest wbudowany w systemie Cisco IOS i można go uruchomić z CLI. W części 6 będziesz używać SSH za pomocą wiersza poleceń CLI w przełączniku, do łączenia się z routerem.

Krok 1: Wyświetl parametry dostępne dla klienta Cisco IOS SSH.

Aby wyświetlić opcje parametrów dostępne za pomocą polecenia **ssh** użyj znaku zapytania (**?**).

```
S1# ssh ?
  -c    Select encryption algorithm
  -l    Zaloguj się używając nazwy użytkownika
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

Krok 2: Z S1 uruchom sesję SSH do routera R1.

a. Jeżeli chcesz połączyć się do R1 poprzez SSH, to musisz użyć opcji **–l admin**. To pozwoli ci zalogować się jako **admin**. Jeżeli zostaniesz zapytany o hasło, to wpisz **adminpass**.

```
S1# ssh -l admin 192.168.1.1
Password:
**********************************************
  Warning: Unauthorized Access is Prohibited!
**********************************************


R1#
```

b. Możesz wrócić do S1 bez zamykania sesji SSH ustanowionej do R1 za pomocą kombinacji klawiszy **Ctrl**+**Shift**+**6**. Zwolnij kombinację **Ctrl**+**Shift**+**6** i wpisz **x**. Powinieneś zobaczyć znak zachęty przełącznika w trybie uprzywilejowanym.

```
R1#
S1#
```

c. Aby powrócić do sesji SSH ustanowionej w R1, naciśnij klawisz Enter w pustej linii CLI. Może będziesz musiał nacisnąć klawisz Enter po raz drugi, aby zobaczyć wiersz poleceń routera (CLI).

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1#
```

d. Aby zakończyć sesję SSH w R1, w wierszu poleceń routera wpisz **exit**.

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

Jakie wersje SSH są obsługiwane w wierszu poleceń CLI?

_____

_____

Do przemyślenia

Jak można skonfigurować dostęp dla wielu użytkowników (każdy ma swoją nazwę) do urządzenia sieciowego?

_____

Tabela zbiorcza interfejsów routera

Interfejsy routera - Podsumowanie				
Model routera	**Interfejs Ethernet #1**	**Interfejs Ethernet #2**	**Interfejs Serial #1**	**Interfejs Serial #2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Uwaga: Aby stwierdzić jak router jest skonfigurowany, spójrz na interfejsy aby zidentyfikować typ routera oraz liczbę jego interfejsów. Nie ma sposobu na skuteczne opisanie wszystkich kombinacji konfiguracji dla każdej klasy routera. Ta tabela zawiera identyfikatory możliwych kombinacji interfejsów Ethernet i Serial w urządzeniu. W tabeli nie podano żadnych innych rodzajów interfejsów, mimo iż dany router może być w nie wyposażony. Przykładem może być interfejs ISDN BRI. Informacja w nawiasach jest dozwolonym skrótem, którego można używać w poleceniach IOS w celu odwołania się do interfejsu.