ATÖLYE 2: SSH

ATÖLYENİN HEDEFİ:

Bu laboratuvar çalışmasının amacı, bir cihaza—bu alıştırmada bir Cisco yönlendiricisine—SSH erişimini nasıl etkinleştireceğinizi öğrenmek ve anlamaktır.

ATÖLYENİN AMACI:

Ağ cihazlarında, özellikle kurumsal ortamlarda, Telnet erişimine izin vermek asla iyi bir fikir değildir. SSH, ağ cihazlarına güvenli bir şekilde bağlanmanın bir yoludur. SSH yapılandırmasını gerçekleştirmek için aşağıdaki adımları izlemeniz gerekir:

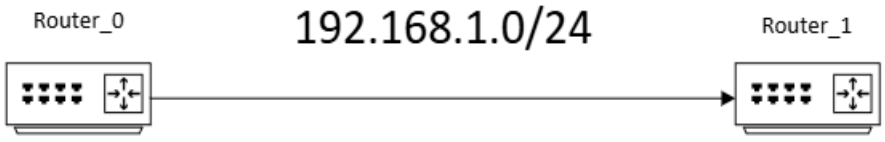
1. Bir hostname (ana bilgisayar adı) oluşturun.
2. Bir domain name (etki alanı adı) oluşturun.
3. Bir kriptografik anahtar oluşturun.

ATÖLYE ARACI:

Cisco Packet Tracer

ATÖLYE TOPOLOJİSİ:

Bu atölyeyi tamamlamak için lütfen aşağıdaki topolojiyi kullanın:



ATÖLYE ANLATIMI:

Adım 1:

İki yönlendiriciyi çalışma alanına sürükleyin ve **crossover(çapraz) kablo** ile birbirlerine bağlayın. Bu labaratuvarda istediğiniz herhangi bir yönlendiriciyi kullanabilirsiniz. Şimdi, **Router0 ve Router1** yönlendiricilerinin **hostname (ana bilgisayar adı)** yapılandırmasını, topolojide gösterildiği gibi ayarlayın. Her zaman başlangıçta "**no**" yanıtını vermelisiniz, çünkü yönlendiriciler soru-cevap moduna girerek kendilerini otomatik yapılandırmaya çalışacaktır.

Bu atölyede hostnameleri R0 ve R1 olarak ayarlayacağız. Aşağıda Router0 (R0) için hostname ayarlama komutlarını bulabilirsiniz. Aynı işlemi Router1 için de tekrarlayın, ancak hostname olarak R1 girin.

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R0
R0(config)#
```

Adım 1:

Her yönlendiricinin Ethernet arayüzüne bir IP adresi atayın ve "no shutdown" komutunu kullanarak arayüzleri aktif hale getirin.

Bu işlemin aynısını Router_1 için de yapın:

```
         --- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: no


Press RETURN to get started!



Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#hostname R0
R0(config)#
```

Daha sonra her ikisine de ip adresi ve subnet mask konfigürasyonlarını yapın:

```
R0>enable
R0#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R0(config)#interface g0/0
R0(config-if)#ip address 192.168.1.1 255.255.255.0
R0(config-if)#no shutdown
R0(config-if)#end
R0#

R1>enable
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface g0/0
R1(config-if)#ip address 192.168.1.2 255.255.255.0
R1(config-if)#end
R1#
```

İki yönlendirici arasında ping atabildiğinizden emin olduktan sonra devam edebilirsiniz:

```
R0#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 seconds:
.!!!!
Success rate is 80 percent (4/5), round-trip min/avg/max = 0/0/0 ms
```

Adım 3:

Router1'i güvenli hale getirerek **SSH** üzerinden gelen bağlantıları kabul etmesini sağlayın. Bunun için bir alan adı (**domain name**) belirlememiz ve kriptografik anahtarlar oluşturmamız gerekmektedir.

Ek olarak, aşağıdaki güvenlik önlemlerini de uygulayacağız:

- Şifre giriş deneme sayısını 2 ile sınırlandırın.
- Herhangi bir etkinlik olmazsa 60 saniye içinde zaman aşımına uğramasını sağlayın.

```
R1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#ip domain-name itusgmyo.net
R1(config)#crypto key generate rsa
The name for the keys will be: R1.itusgmyo.net
Choose the size of the key modulus in the range of 360 to 4096 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#ip ssh time-out 60
*Mar 1 0:21:54.276: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)#ip ssh authentication-retries 2
R1(config)#line vty 0 15
R1(config-line)#transport input ssh
R1(config-line)#password itusgmyo
R1(config-line)#end
R1#
```

Adım 4:

Router0'dan Router1'e SSH ile bağlanın. Bağlantı kurulduğunda, şifre girmeniz istenecektir. Yukarıdaki bilgilerde de görüldüğü gibi, şifre "itusgmyo" olarak ayarlanmıştır. Ayrıca, SSH bağlantısı için bir kullanıcı adı belirleyebilirsiniz. SSH'dan sonra "1" değil "l" harfini kullanın.

```
R0>ssh -l hamza 192.168.1.2

Password:



R1>
```

"exit" yazarak da bağlantıyı sonlandırabilirsiniz.

Adım 5:

Router0'dan Router1'e Telnet ile bağlanmayı deneyerek bağlantının reddedildiğini görebilirsiniz.

```
R0>telnet 192.168.1.2
Trying 192.168.1.2 ...Open

[Connection to 192.168.1.2 closed by foreign host]
R0>
```