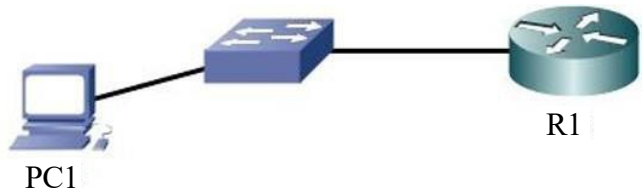
2.8. *Uygulama için alıştırmalar*

ALIŞTIRMA 1.-

Topoloji



Adresleme tablosu

Cihaz	Arayüz	IP adresi / alt ağ maskesi	İşletim sistemi (GNS3)	Ağ Geçidi
R1	G0/0	192.168.0.1/24	c2600-adventerprisek9-mz.124-1	-
PC1	NIC	192.168.0.2/24	Windows 7	192.168.0.1

Hedefler

- Parolaların güvenliğini sağlama.
- Bağlantı kısıtlamalarının uygulamaya konulması.
- Yönetici rollerinin atanması.

Kullanılacak Yazılım

- Paket İzleyici.
- Ya da GNS3.

Bölüm A: Temel cihaz yapılandırmasının oluşturulması

1.1. Ana bilgisayar adını topolojide belirtildiği gibi yapılandırın.

1.2. Adresleme tablosuna göre IP adreslerini cihaz arayüzlerine uygulayın.

Bölüm B: parolaların güvenliğini sağlama

1. Minimum 8 karakterlik bir parola uzunluğu belirleyin.

R1(config)# *security passwords min-length 8*

2. Ayrıcalıklı mod için parolayı yapılandırın.

2.1. Bu mod için bir kelimeyi açık metin olarak tanımlayın.

R1(config)# **enable parola Ci$c0123**

2.2. Bu şifreyi "**show run**" komutundan okuyabilir misiniz?

.....

2.3. Ayrıcalıklı mod için şifreli bir parola belirleyin.

R1(config)# **enable secret Ci$c0ena**

2.4. Bu şifreyi "**show run**" komutundan okuyabilir misiniz?

.....

3. Konsol bağlantı noktalarını, yardımcı bağlantı noktalarını ve sanal erişim hatlarını yapılandırın.

3.1. Bir konsol bağlantı noktası parolası yapılandırın ve hareketsizlik aralığını 5 dakika olarak ayarlayın.

R1(config)# **line console 0**
R1(config-line)# **password Ci$c0con**
R1(config-line)# **exec-timeout 5 0**
R1(config-line)# **login**
R1(config-line)# **günlüğe kaydetme eşzamanlı**

3.2. VTY hatlarında bir parola yapılandırın ve hareketsizlik aralığını 2 dakika olarak ayarlayın.

R1(config)# **hat vty 0 4**
R1(config-line)# **password**
Ci$c0vty R1(config-line)# **exec-**
timeout 2 0 R1(config-line)# **login**

3.3. Yardımcı bağlantı noktasını devre dışı bırakın.

R1(config)# **line aux 0**
R1(config-line)# **no exec**

3.4. Telnet *aracılığıyla* PC1'den R1'e erişin.

PC1> **telnet 192.168.0.1**

4. Tüm şifreleri şifreleyin.

4.1. Konsol ve VTY parolalarını şifrelemek için "Password-Encryption Service" komutunu kullanın.

R1(config)# **service password-encryption**

4.2. Konsol ve VTY şifrelerini "**show run**" komutundan okuyabilir misiniz?

.....

Bölüm C: bağlantı kısıtlamalarının uygulamaya konulması

1. Giriş uyarı banner'ını yapılandırın.

1.1. "**motd**" komutunu kullanarak yetkisiz kullanıcılar için bir uyarı yapılandırın.

R1(config)# **banner motd $** *Yetkisiz kişiler için erişim kesinlikle yasaktır $*
R1(config)# *çıkış*

1.2. "**show run"** komutunda, yapılandırma dosyasındaki "$" karakterinin yerini ne almıştır?

.....

Bölüm D: VTY hatlarına erişimin güvence altına alınması

1. Ssh bağlantılarını yapılandırın.

Ssh bağlantılarını yapılandırmak için aşağıdaki seçenekleri kullanın:

– alan adı: **tri.local**;

– kullanıcı adı: **sshadmin** ve parola: **Ci$c0ssh**;

– RSA şifreleme anahtarı **1024 bittir**;

– kullanılan SSH sürümü sürüm 2'dir;

– bekleme süresi ***90***'lar;

– oturum açma deneme sayısı ***3'tür***;

– ***ssh*** ve ***telnet*** oturumlarını yetkilendirin.

2. Bağlantı parametrelerini yapılandırın.

2.1. ***30s*** içinde iki bağlantı denemesi başarısız olursa bağlantının ***60s boyunca*** durdurulmasını yapılandırmak için "**login block-for**" komutunu kullanın.

R1(config)#login **block-for 60 attempts 2 within 30**

2.2. Ardışık bağlantı denemeleri arasında 5 saniyelik bir gecikme yapılandırmak için "**Oturum** açma **gecikmesi**" komutunu kullanın.

R1(config)#login **delay 5 (GNS3)**

2.3. Her bağlantı denemesi başarılı olduğunda olay günlüğüne bir girdi ekleyin.

R1(config)#login **on-success günlüğü**

ya da:

R1(config)# **login on-success log every 1 (GNS3)**

3. Gizli bir parola ile iki yeni kullanıcı hesabı oluşturun.

R1(config)# **kullanıcıadı user01 gizli user01pass**
R1(config)# **kullanıcıadı user02 gizli user02pass**

4. Bir telnet oturumundan R1'e bağlanın.

4.1. PC1'den R1'e bir **telnet** oturumu oluşturun.

PC1> **telnet 192.168.1.1**

4.2. Sizden bir kullanıcı hesabı girmeniz istendi mi? Neden?

.....

4.3. Yerel olarak tanımlanan oturum açma hesaplarını kullanmak için VTY hatlarını tanımlayın.

R1(config)# **hat vty 0 4**
R1(config-line)# **login local**

4.4. PC1'den R1'e bir **telnet** oturumunu yeniden oluşturun.

PC1> **telnet 192.168.1.1**

4.5. Yanlış bir kullanıcı kimliği veya parola ile iki kez oturum açmayı deneyin. İkinci başarısız denemeden sonra PC1'de hangi mesaj görüntülenir?

.....

4.6. İkinci başarısız bağlantı denemesinden sonra R1 konsolunda hangi mesaj görüntülenir?

.....

4.7. PC1'den, 60 saniye içinde R1'e başka bir **telnet** oturumu kurmayı deneyin. Telnet bağlantı denemesinden sonra PC1'de hangi mesaj görüntülenir?

.....

4.8. Telnet bağlantı denemesinden sonra R1 yönlendiricisinde hangi mesaj görüntülendi?

.....

5. R1 ile bağlantıyı yalnızca ssh protokolü kullanarak kısıtlayın.

5.1. VTY hatlarını yalnızca ssh protokolünü kullanacak şekilde yapılandırın.

```
R1(config)# hat vty 0 4
R1(config-line)# aktarım girişi ssh
R1(config-line)# çıkış
```

5.2. PC1'den R1'e başka bir **ssh** ve **telnet** oturumu kurmayı deneyin.

Bölüm E: idari rollerin atanması

1. Ayrıcalık düzeylerini yapılandırın.

1.1. Aşağıdaki seçeneklerle yeni bir kullanıcı hesabı oluşturun:

– hesap adı: "***SshUser***";

– şifrelenmiş parola '***SshUpa $$***";

– ayrıcalık seviyesi ***10***.

```
R1 (config) # username SshUser privilege 10 secret SshUpa $$
```

1.2. Ayrıcalık düzeyi 10 için "**Priv10P $**" parolasını yapılandırın.

```
R1(config)#enable secret level 10 Priv10P$
```

1.3. ***Yürütme*** modunda bu ayrıcalık düzeyi için "**ping**" komutuna izin verin.

```
R1(config)#privilege exec level 10 ping
```

1.4. ***Yürütme*** modunda bu ayrıcalık düzeyi için "**ssh**" komutuna izin verin.

```
R1(config)#privilege exec level 10 ssh
```

1.5. *Yürütme modunda* bu ayrıcalık düzeyi için tüm "**show IP**" komutlarına izin verin. R1(config)#privilege **exec all level 10 show ip**

1.6. Aşağıdaki seçeneklerle yeni bir kullanıcı hesabı oluşturun:

– kullanıcı adı: "***TelUser***";

– şifreli parola "***TelUpa $$***";

– ayrıcalık seviyesi ***12***.

R1(config)# **kullanıcı adı TelUser ayrıcalık 12 gizli *TelUpa$$***

1.7. Ayrıcalık düzeyi 12 için "***Priv12P $***" parolasını yapılandırın. R1(config)#enable **secret level 12 Priv12P$**

1.8. ***Yürütme*** modunda bu ayrıcalık düzeyi için "**ping**" komutuna izin verin.

R1(config)#privilege **exec level 12 ping**

1.9. ***Yürütme*** kipinde bu ayrıcalık düzeyi için "*telnet*" komutuna izin verin. R1(config)#privilege **exec level 12 telnet**

1.10. Bu ayrıcalık düzeyi için tüm *yapılandırma modu* komutlarına izin ver R1(config)#privilege ***exec all level 12 configure***

1.11. Bir ayrıcalık düzeyi 13'ü aşağıdaki seçeneklerle donatarak yapılandırmak için aynı adımları izleyin:

– **Priv13P$** şifreleri;

– yetkili komutlar: **telnet, traceroute, show** (all), **configure** (all).

1.12. Ayrıcalık düzeyleri 10, 12 ve 13'e erişin ve yapılandırmayı test edin.

```
Yönlendirici> etkinleştir 12
Şifre:
R1#?
Exec komutları:
  <1-99>     Devam edilecek oturum
  numarası connect Bir terminal
  bağlantısı açın disable Ayrıcalıklı
  komutları kapatın
```

disconnect Mevcut bir ağ bağlantısının bağlantısını kes enable Ayrıcalıklı komutları aç
exitExec'ten çıkış
logoutExec'ten çıkış
noHata ayıklama bilgilerini devre dışı bırak
ping Yankı mesajları gönderme
resumeEtkin bir ağ bağlantısını sürdür **telnet** Güvenli bir kabuk istemci bağlantısı açma terminalTerminal satırı parametrelerini ayarlama

NOT.

– 0 (sıfır) ayrıcalık seviyeli komutlar otomatik olarak eklenir.

– Belirli bir ayrıcalık düzeyi için istenmeyen tüm komutlar, diğer ayrıcalık düzeylerine ayrı ayrı atanmalıdır.

– Sonuçlar ve ayrıcalık düzeyleri için testler *TelUser* veya *sshUser* hesapları *kullanılarak ssh üzerinden* de gerçekleştirilebilir

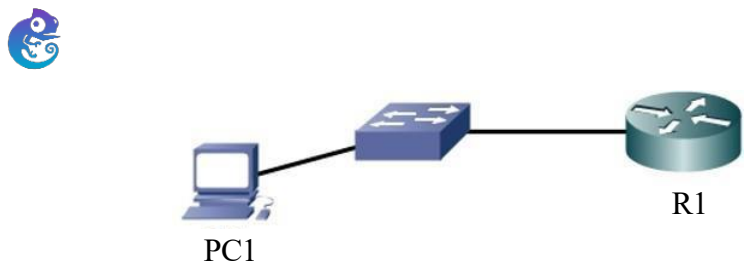
1.13. Geçerli ayrıcalık düzeyini

görüntüleyin. R1# **show**

ayrıcalığı

ALIŞTIRMA 2.-

Topoloji



Adresleme tablosu

Cihaz	Arayüz	IP adresi / alt ağ maskesi	İşletim Sistemi	Ağ Geçidi
R1	G0/0	192.168.0.1/24	c2600-adventerprisek9-mz.124-1	-
PC1	NIC	192.168.0.2/24	Windows 7 veya üstü	192.168.0.1

Hedefler

- Parolaların güvenliğini sağlama.
- Bağlantı kısıtlamalarının uygulamaya konulması.
- "Görünümleri" ve "süper görünümleri" yöneterek erişimi güvence altına alma.
- Yapılandırma dosyalarının ve IOS sisteminin güvenliğinin sağlanması.
- Otomatik güvenlik özelliklerini kullanma.

Kullanılacak Yazılım

- GNS3.

Bölüm A: Temel cihaz yapılandırmasının oluşturulması

1.1. Ana bilgisayar adını topolojide belirtildiği gibi yapılandırın.

1.2. Adresleme tablosuna göre IP adreslerini cihaz arayüzlerine uygulayın.

Bölüm B: parolaların güvenliğini sağlama

1. Minimum 8 karakterlik bir parola uzunluğu belirleyin.

R1(config)# **security passwords min-length 8**

2. Ayrıcalıklı mod için parolayı yapılandırın.

R1(config)# *enable secret Ci$c0ena*

3. Konsol bağlantı noktalarını, yardımcı bağlantı noktalarını ve sanal erişim hatlarını yapılandırın.

3.1. Bir konsol bağlantı noktası parolası yapılandırın ve hareketsizlik aralığını 5 dakika olarak ayarlayın.

R1(config)# **line console 0**
R1(config-line)# **password Ci$c0con R1(config-line)# exec-timeout 5 0 R1(config-line)# login**
R1(config-line)# **logging synchronous**

3.2. VTY hatlarında bir parola yapılandırın ve hareketsizlik aralığını 2 dakika olarak ayarlayın.

R1(config)# **hat vty 0 4**
R1(config-line)# **password Ci$c0vty R1(config-line)# exec-timeout 2 0 R1(**config-line)# **login**

3.3. Yardımcı bağlantı noktasını devre dışı bırakın.

R1(config)# **line aux 0**
R1(config-line)# **no exec**

3.4. Telnet kullanarak PC1'den R1 yönlendiricisine erişin.

PC1> **telnet 192.168.0.1**

4. Tüm şifreleri şifreleyin.

R1(config)# **service password-encryption**

Bölüm C: ssh ile VTY hatlarına erişimi güvence altına alma

1. Ssh bağlantılarını yapılandırın.

Ssh bağlantılarını yapılandırmak için aşağıdaki seçenekleri kullanın:

– alan adı: **tri.local**;
– kullanıcı adı: *sshadmin* ve parola: **Ci$c0ssh**;
– RSA şifreleme anahtarı ***1024 bittir***;
– kullanılan SSH sürümü ***sürüm 2***'dir;
– bekleme süresi ***90 saniyedir***;
– oturum açma deneme sayısı ***3'tür***;
– ***ssh*** ve ***VTY*** oturumlarını yetkilendirin.

2. Bağlantı parametrelerini yapılandırın.

Bir bağlantı bloğu yapılandırmak için "**login block-for**" komutunu kullanın ***30 saniye*** içinde iki başarısız bağlantı denemesi olursa ***60 saniye***.

R1(config)#login **block-for 60 attempts 2 within 30**

Bölüm D: "görünüm" yönetimini kullanarak erişimi güvence altına alma

1. Şifrelenmiş parola "Us01pa$$" ile yeni bir kullanıcı hesabı "User01" oluşturun.

R1(config)# **kullanıcı adı User01 gizli Us01pa$$**

2. R1 üzerinde "AAA "yı etkinleştirin.

R1# *config terminal*
R1(config)# *aaa new-model*
R1(config)# *exit*

3. Bir "ViewRouter" görünümü oluşturun.

R1#görünümü etkinleştir
Parola: (*parola etkin*)
R1#conf t
R1(config)# **parser view ViewRouter**
R1(config-view)#

4. Bu görünüme "*ViewRouPs*" parolasını atayın.

R1(config-view)# **secret ViewRouPs**

5. Bu görünüm için, *yürütme* modunda tüm "*show*" komutlarına izin verin.

R1(config-view)# **komutları exec include all show**

6. *Yapılandırma* modundaki tüm komutlara izin verin.

R1(config-view)# **commands exec include all configure terminal**

7. *Yönlendirici* modunda mod için tüm komutlara izin verin.

R1(config-view)# **configure komutları tüm yönlendiricileri içerir**

8. Bir "ViewTelnet" görünümü oluşturmak ve aşağıdaki seçeneklerle donatmak için aynı adımları izleyin:

- Şifre ***ViewTelPs***;
- Yetkili komutlar: **telnet, traceroute, show** (all).

9. *ViewRouPs* görünümüne erişin ve yapılandırmayı test edin.

R1#enable **view *ViewRouPs***
Şifre:
Yönlendirici#?
Exec komutları:
configure Yapılandırma moduna girin
disable Ayrıcalıklı komutları kapatın
enable Ayrıcalıklı komutları açın exit
EXEC'ten çıkın
logoutExec'ten çıkış
göster Çalışan sistem bilgilerini göster

ViewTelnet görünümü için:

R1#enable **view ViewTelnet**
Şifre:
R1#?
Exec komutları:
disable Ayrıcalıklı komutları kapat
enable Ayrıcalıklı komutları aç exit
EXEC'ten çık
logoutExec'ten çıkış
göster Çalışan sistem bilgilerini göster
telnet Bir telnet bağlantısı açın
traceroute Hedefe giden yolu izleme

10. Görünümlerin listesini görüntüleyin.

R1#show **parser view** Sistemde Mevcut
Tüm Görünümler/SuperViews:
ViewRouter
ViewTelnet
-------(*) üst görünümü temsil eder-------

11. "ViewRouter" öğesini "User01" öğesine atayın.

R1(config)**#kullanıcıadı User01 görünüm ViewRouter**

12. "*$uperView1*" parolasıyla "*SuperView1*" adında bir süper görünüm oluşturun.

R1#görünümü etkinleştir
Parola: (*parola etkin*)
R1(config)# **parser view SuperView1 superview**
R1(config-view)**#secret $uperView1**

13. "ViewRouter" ve "ViewTelnet" görünümlerini bu süper görünümlere atayın.

R1(config-view)# view **ViewRouter**
R1(config-view)# view **ViewTelnet**

14. Görünümlerin listesini görüntüleyin.

R1#show **parser view** Sistemde Mevcut
Tüm Görünümler/SuperViews:
ViewRouter
ViewTelnet
SuperView1 *
-------(*) süper görünümü temsil eder-------

15. "SuperView1" öğesini "User01" öğesine atayın.

R1(config)**#kullanıcıadı User01 görünüm SuperView1**

Bölüm E: yapılandırma dosyalarının ve IOS sisteminin güvenliğini sağlama

1. Flash belleğin içeriğini görüntüleyin.

R1#show **flash**:
Sistem flaş dizini:
Dosya Uzunluğu Ad/durum
3 50938004 **c2800nm-advipservicesk9-mz.124-15.T1.bin**
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[51193823 bayt kullanılmış, 12822561 kullanılabilir, 64016384 toplam] 63488K bayt işlemci kartı Sistem flaşı (Okuma/Yazma

2. IOS görüntü dosyasının Flash bellekte gizlenerek güvenliğinin sağlanması.

R1(config)# **secure boot-image**

3. Geçerli yapılandırma dosyasını Flash bellekte sabitleme.

R1(config)# **secure boot-config**

4. Flash belleğin içeriğini bir kez daha görüntüleyin.

R1#show **flash**:
Sistem flaş dizini:
Dosya Uzunluğu Ad/durum
2 28282 sigdef-category.xml
1 227537 sigdef-default.xml
[51193823 bayt kullanılmış, 12822561 kullanılabilir, 64016384 toplam] 63488K bayt işlemci kartı Sistem flaşı (Okuma/Yazma

5. IOS görüntü dosyasını görebiliyor musunuz? Neden?

.....

6. Cisco IOS görüntüsünün ve yapılandırma dosyasının arşiv durumunu görüntüleyin.

R1# **show secure bootset**
IOS görüntü esnekliği sürüm 12.4, 1 Mart 1993 Pazartesi 00:01:50 UTC'de etkinleştirildi
Güvenli arşiv **flash:/c2800nm-advipservicesk9-mz.124-15.T1.bin** türü görüntüdür (elf) dosya boyutu 50938004 bayt, çalışma boyutu 50938004 bayt Çalıştırılabilir görüntü, giriş noktası 0x8000F000, ram'den çalıştır
IOS yapılandırma esnekliği sürüm 12.4, 1 Mart 1993 saat 00:02:03 UTC'de etkinleştirildi
Güvenli arşiv **flash:/.runcfg-19930301-000203.ar** türü yapılandırma yapılandırma arşiv boyutu 551 bayt

7. ROMMON'dan başlatmayı yapılandırın ve yönlendiriciyi yeniden başlatın.

R1(config)#config-register **0x2100**
R1(config)#exit
R1#reload
Yeniden yükleme ile devam edelim mi? [ONAYLA]

8. ROMMON modunda mevcut güvenli dosyaları görüntüleyin.

rommon 1 > *dir flash:*

Dosya boyutuChecksum Dosya adı
551 bayt (0x227) 0x0227 . **runcfg-19930301-000203.ar**
50938004 bayt (0x3094094) 0x439d **c2800nm-advipservicesk9- mz.124-15.T1.bin**
28282 bayt (0x6e7a) 0x6e7a sigdef-category.xml 227537 bayt
(0x378d1) 0x78d4 sigdef-default.xml

9. İndekslenmiş görüntüyü kullanarak yönlendiriciyi başlatın.

rommon 2 > **boot c2800nm-advipservicesk9-mz.124-15.T1.bin**

10. Güvenli yapılandırmayı Flash'ta bulunan arşive geri yükleyin.

R1(config)**#secure boot-config geri yükleme flash:. runcfg-19930301-000203.ar**

Bölüm F: otomatik güvenlik özelliklerini kullanma

1. "Autosecure" komut dosyasının kullanımını gözden geçirin.

.....

2. "autosecure" komut dosyasını başlatın ve talimatları izleyin.

R1#otomatik **güvenli**