Packet Tracer － ネットワークデバイスのセキュリティ保護

# アドレッシング テーブル

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| デバイス | インターフェイス | アドレス | マスク | ゲートウェイ |
| RTR-A | G0/0/0 | 192.168.1.1 | 255.255.255.0 | 該当なし |
| RTR-A | G0/0/1 | 192.168.2.1 | 255.255.255.0 | 該当なし |
| SW-1 | SVI（vlan1） | 192.168.1.254 | 255.255.255.0 | [　　　　　　　　　　　　　　] |
| PC | NIC | 192.168.1.2 | 255.255.255.0 | [　　　　　　　　　　　　　　] |
| ラップトップ | NIC | 192.168.1.10 | 255.255.255.0 | [　　　　　　　　　　　　　　] |
| リモート PC | NIC | 192.168.2.10 | 255.255.255.0 | [　　　　　　　　　　　　　　] |

# 要件

**注**: このアクティビティを簡潔に管理しやすくするために、一部のセキュリティ設定が行われていません。それ以外の場合、セキュリティのベストプラクティスに従っていません。

このアクティビティでは、要件のリストに基づいてルータとスイッチを設定します。

### ネットワークの文書化

不足している情報を補って、アドレッシングテーブルを完成させます。

### ルータの設定要件 RTR-A

* IOS が、入力ミスされたコマンドをドメイン名に解決することを防止します。  
  Router(config)# [ 　no ip domain-lookup　]
* アドレス指定テーブルの値と一致するIPアドレスの設定。  
  **G0/0/0**Router(config)# [　int G0/0/0　　]  
  Router(config-if)# [ 　ip address 192.168.1.1 255.255.255.0　]  
  Router(config-if)# [ 　shutdown　 ]  
  **G0/0/1**  
  Router(config)# [ 　int G0/0/1　 ]  
  Router(config-if)# [ 　ip address 192.168.2.1 255.255.255.0　 ]  
  Router(config-if)# [　　exit　]
* 新しく作成したパスワードの長さは 最小で10 文字以上にする必要があります。  
  Router(config )#[ 　　security passwords min-length 10　]
* コンソール回線用の強力な 10 文字のパスワード **@Cons1234!** を使います。  
  Router(config )# [　　line console 0　　]  
  Router(config-line)# [ 　password @Cons1234!　 ]
* コンソールおよび VTY セッションは、ちょうど7 分後に終了するようにします。  
  Router(config-line)# [ 　exec-timeout 10　　　 ]
* 特権 EXEC モード用の強力な暗号化された 10 文字のパスワード。このアクティビティでは、コンソール回線と同じパスワードを使用できます。  
  Router(config)# [ 　enable **secret @Cons1234!**]
* デバイスへの不正アクセスについて警告する MOTD バナー。文言は「 authentication access only!! 」  
  Router(config)# [ 　**banner motd #** authentication access only!! **#**　 ]
* すべてのパスワードのパスワード暗号化。  
  Router(config)# [ 　service password-encryption ]
* SSH の有効化
  1. ホスト名をアドレッシングテーブルに基づいて設定します  
     Router(config)# [ 　hostname RTR-A　　　 ]
  2. ドメイン名として **security.com** を使用します。  
     RTR-A (config)# [ 　ip domain name security.com　 ]
  3. **1024**のモジュラスを使用します。  
     RTR-A (config)# [ 　crypto key generate rsa general-keys modulus 1024　 ]
  4. ユーザ **NETAdmin（**暗号化されたパスワード**LogAdmin!9**を持つ）．  
     RTR-A (config)# [ 　username NETAdmin secret LogAdmin!9 ]
  5. VTY 回線では、ログインを認証するように設定されたユーザ名とパスワードを使用する必要があります。  
     RTR-A (config)# line vty 0 4　　※ルータの場合vty回線は0～4の5回線   
     RTR-A (config-line)# [ 　login local　 ]
  6. VTY 回線では、着信接続に SSH を使用する必要があります。  
     RTR-A (config-line)# [ 　transport input ssh　 ]
* ブルートフォースのログイン試行を防ぐために、100秒以内に3回失敗した場合、45秒間ログイン試行をブロックするコマンドを使用します。  
  RTR-A (config)# [ 　　login block-for 45 attempts 3 within 100　]

### スイッチの構成要件 SW-1

* 未使用のスイッチポートはすべて管理上ダウンにします。  
  Switch (config)# int range fa0/1,fa 0/3-9,fa 0/11-24,g0/2 ※複数インターフェイスの選択　  
  Switch (config-if-range)# [　　shutdown　　]
* SW-1 のデフォルト管理インターフェイスは、ネットワーク経由の接続を受け入れる必要があります。アドレス指定表に示されている情報を使用します。スイッチは、リモートネットワークから到達可能である必要があります。  
  Switch (config)# [　　　　　　　　　　　　　　　　　　]  
  Switch (config-if)# [　　　　　　　　　　　　　　　　　]  
  Switch (config-if)# [　　　　　　　　　　　　　　　　　　]  
  Switch (config-if)# exit  
  Switch (config)# [　　　　　　　　　　　　　　　　　　　]
* **@Cons1234!** を特権 EXEC モードのパスワードとして使用します。  
  Switch (config)# [　enable secret @Cons1234!　　]
* ルータと同じように SSH を設定します。
  1. ホスト名をアドレッシングテーブルに基づいて設定します  
     Switch(config)# [ 　　　　　　　　　　　　　　 ]
  2. ドメイン名として **security.com** を使用します。  
     SW-1 (config)# [ 　ip domain name security.com　　　　　 ]
  3. **1024**のモジュラスを使用します。  
     SW-1 (config)# [ 　**crypto key generate rsa general-keys modulus 1024**　 ]
  4. 暗号化されたパスワード**LogAdmin!9**を持つユーザ **NETAdmin**  
     SW-1 (config)# [ 　username NETAdmin secret LogAdmin!9　　　　 ]
  5. VTY 回線では、ログインを認証するように設定されたユーザ名とパスワードを使用する必要があります。  
     SW-1 (config) # line vty 0 15　※スイッチの場合vty回線は0～15の16回線  
     SW-1 (config-line)# [ 　　**login local**　　 ]
  6. VTY 回線では、着信接続に SSH を使用する必要があります。  
     SW-1 (config-line)# [ 　transport input ssh ]

### 設定確認

* PCのDesktopのCommand Promptから、SW-1、RTR-A、リモートPCにpingで接続を確認します  
  SW-1(192.168.1.254)　[　接続できた　]  
  RTR-A(192.168.1.1) 　[　接続できた　]  
  リモートPC(192.168.2.10) 　[　接続できた　]
* リモートPCのDesktopのCommand Promptから、RTR-A、SW-1、ラップトップにpingで接続を確認します  
  RTR-A(192.168.2.1) 　[　接続できた　]  
  SW-1(192.168.1.254)　[　接続できた　]  
  ラップトップ(192.168.1.10) 　[　接続できた　]

アイコン が含まれている画像

自動的に生成された説明

* リモートPCのDesktopのTelnet/SSH ClientでTelnet/およびSSHで、SW-1(192.168.1.254)に接続を試みます　  
  Usernameは、**NETAdmin、**passwordは、**LogAdmin!9**  
  Telnet→　[　接続できた　・　接続できない　]  
  SSH→　[　接続できた　・　接続できない　]
* SW-1に接続後、特権モード（SW-1#）に移行後、RTR-AへSSHで接続を試み、わざと3回連続で接続に失敗します  
  コマンド：SW-1# ssh -l NETAdmin 192.168.1.1   
  ※パスワードを聞かれるの素早く3回Enterを押します  
  再度、コマンド：SW-1# ssh -l NETAdmin 192.168.1.1を実施し、接続を試みます  
  [　接続できた　・　接続できない　]  
    
  45秒程度待ってから、再度SSHで接続を試行します　passwordは、**LogAdmin!9**[　接続できた　・　接続できない　]

「Check Result」で設定が完了していることを教員に確認してもらうこと。

■提出物  
□全員

提出物：Packet Tracerのファイル(pka)

□最後のチェックまで行かなかった人

このWordファイル(docx)

設定に必要なコマンド（ルータとスイッチ）

1. ﾕｰｻﾞﾓｰﾄﾞから特権モードに　 　　　　 Router> **enable** (enに省略可)
2. 特権モードからﾕｰｻﾞﾓｰﾄﾞに戻る　 Router# **disable**
3. 特権モードからグローバル設定モードに　 Router#**conf**igure **t**erminal (conf tに省略可)
4. 一つ上のモードに戻る　　　　　　　 Router(config)#**exit**
5. ホスト名をつけるRouter(config)# **hostname** *ホスト名*
6. 特権モードのパスワードを設定する 　 Router (config)#**enable secret** *パスワード*
7. コンソールのパスワードの設定 Router(config)#**line cons 0**

Router(config-line)#**password** *パスワード*

　　　　　　　　　　　　　　　　　　 Router(config-line)#**login**

1. 設定画面のタイムアウト時間を設定　 Router(config-line)#**exec-timeout***分　秒*
2. 入力中のログ出力を抑制する　　　　 Router(config-line)**logging　synchronous**
3. パスワードを暗号化する 　　　　　 　 Router(config)# **service password-encryption**
4. DNS検索を無効化する　　　　　　　 Router(config)# **no ip domain-lookup**
5. インターフェイスの設定(IPv4)　　　　　 Router(config)#int *インターフェイス名*

Router(config-if)#**ip address** *IPｱﾄﾞﾚｽ ｻﾌﾞﾈｯﾄﾏｽｸ*※今回のサブネットマスクは255.255.255.0のみ

　　　　　　　　　　　　　　　　　　　　 Router(config-if)#**no shutdown**(初回のみ実施)

　　　　　　インターフェイスの説明の記述 Router(config-if)#**description** *説明文*

1. デフォルトルートの設定(ルータ)　　　 Router(config)# **ip route 0.0.0.0 0.0.0.0** *IPｱﾄﾞﾚｽ*
2. デフォルトゲートウェイの設定(スイッチ) Switch(config)#ip default-gateway *IPｱﾄﾞﾚｽ*
3. SSHの設定（6ステップ）
   1. ホスト名を設定 Switch(config)# **hostname *ホスト名***
   2. ドメイン名を設定 Switch (config)# **ip domain-name *ドメイン名***
   3. 1024のモジュラスを使用（秘密鍵を生成）します。  
       Switch (config)# **crypto key generate rsa general-keys modulus 1024**
   4. ローカル データベースのユーザ名、暗号化されたパスワードを設定  
       Switch (config)# **username *ユーザ名* secret *パスワード***
   5. VTY 回線で、ログイン時をローカル データベースのユーザ名、暗号化されたパスワードで認証するように設定  
       Switch (config) # **line vty 0 15　※ルータの場合**vty回線は0～4の5回線  
       Switch (config-line)# **login local**
   6. VTY 回線で、着信接続に SSH のみを限定します  
       Switch (config-line)# **transport input ssh**
4. 全てのパスワードの文字数の最小値を設定する Router(config )# **security passwords min-length 10**
5. ブルートゥースのログイン試行回数の制御  
    **Router(config )#** **login block-for** *ブロック(待機・ブロック)秒数* **attempts** *失敗回数* **within** *制限秒数(〇秒以内)*
6. MOTDバナー(不正アクセスへの警告) **Router(config )#** **banner motd #** *メッセージ* **#**