実習 - ネットワーク デバイスの保護

トポロジ

アドレッシング テーブル

デバイス	インターフェイス	IP アドレス	サブネット マスク	デフォルト ゲートウェイ
R1	G0/1	192.168.1.1	255.255.255.0	該当なし
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

目的

パート 1:デバイスの基本設定を構成する

パート 2:ルータに基本的なセキュリティ対策を設定する

パート 3:スイッチに基本的なセキュリティ対策を設定する

背景/シナリオ

すべてのネットワーク デバイスは、少なくとも、ベスト プラクティスのセキュリティ コマンドの最小セットによって設定することが推奨されます。これには、エンドユーザ デバイス、サーバ、ネットワーク デバイス(ルータやスイッチなど)が含まれます。

この実習では、リモート管理用の SSH セッションを受け入れるようにトポロジ内のネットワーク デバイスを設定します。また、IOS CLI を使用して、一般的で基本的なベスト プラクティスのセキュリティ対策の設定も行います。その後、セキュリティ対策をテストして、それらが適切に実装され、正しく動作することを確認します。

注:CCNA の実習で使用するルータは、Cisco IOS リリース 15.2(4) M3(universalk9 イメージ)を搭載した Cisco 1941 ISR です。また、使用するスイッチは、Cisco IOS Release 15.0(2)(lanbasek9 イメージ)を搭載した Cisco Catalyst 2960 です。他のルータ、スイッチ、および Cisco IOS バージョンを使用できます。モデルと Cisco IOS バージョンによっては、使用できるコマンドと生成される出力が、実習とは異なる場合があります。正しいインターフェイス ID については、この実習の最後にあるルータ インターフェイスの要約表を参照してください。

注:ルータとスイッチが消去され、スタートアップ コンフィギュレーションがないことを確認してください。ご不明な点はインストラクタにお問い合わせください。

実習に必要なリソースや機器

- ルータ 1 台(Cisco IOS ソフトウェア リリース 15.2(4) の M3 ユニバーサル イメージを搭載した Cisco 1941 または同等機器)
- スイッチ 1 台(Cisco IOS リリース 15.0(2) の lanbasek9 イメージを搭載した Cisco 2960 または同等機器)

- PC 1 台（Tera Term などのターミナル エミュレーション プログラムをインストールした Windows 7、Vista、または XP）
- コンソール ポート経由で Cisco IOS デバイスを設定するためのコンソール ケーブル
- トポロジで指定されているイーサネット ケーブル

パート 1:　デバイスの基本設定を構成する

パート 1 では、ネットワーク トポロジを設定し、ルータのインターフェイス IP アドレス、デバイス アクセス、パスワードなどの基本設定を構成します。

手順 1:　トポロジに示すようにネットワークを配線する。

トポロジに示されているデバイスを接続し、必要に応じてケーブル配線を行います。

手順 2:　ルータとスイッチを初期化してリロードする。

手順 3:　ルータを設定する。

SSH で必要なコマンドのヘルプについては、前の実習を参照してください。

a. ルータにコンソール接続し、特権 EXEC モードを有効にします。

b. コンフィギュレーション モードに切り替えます。

c. ルータに R1 という名前を割り当てます。

d. DNS lookup を無効にして、誤って入力されたコマンドをルータがホスト名として変換することを回避します。

e. 特権 EXEC の暗号化パスワードとして **class** を割り当てます。

f. コンソール パスワードとして **cisco** を割り当て、ログインを有効にします。

g. vty パスワードとして **cisco** を割り当て、ログインを有効にします。

h. クリア テキストのパスワードを暗号化します。

i. デバイスにアクセスするすべてのユーザに対して、不正アクセスは禁止されていることを警告するバナーを作成します。

j. アドレッシング テーブルに含まれる情報を使用して、ルータの G0/1 インターフェイスを設定し、アクティブ化します。

k. 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存します。

手順 4:　スイッチを設定する。

a. スイッチにコンソール接続し、特権 EXEC モードを有効にします。

b. コンフィギュレーション モードに切り替えます。

c. スイッチに S1 という名前を割り当てます。

d. DNS lookup を無効にして、誤って入力されたコマンドをルータがホスト名として変換することを回避します。

e. 特権 EXEC の暗号化パスワードとして **class** を割り当てます。

f. コンソール パスワードとして **cisco** を割り当て、ログインを有効にします。

g. vty パスワードとして **cisco** を割り当て、ログインを有効にします。

h. クリア テキストのパスワードを暗号化します。

i. デバイスにアクセスするすべてのユーザに対して、不正アクセスは禁止されていることを警告するバナーを作成します。

j. アドレッシング テーブルに含まれる IP アドレス情報を使用して、デフォルトの SVI を設定します。

k. 実行コンフィギュレーションをスタートアップ コンフィギュレーション ファイルに保存します。

パート 2:　ルータに基本的なセキュリティ対策を設定する

手順 1:　パスワードを強化します。

管理者は、各パスワードが強力なパスワードの標準ガイドラインに従うようにする必要があります。これらのガイドラインには、パスワードでの文字、数字、および特殊文字の併用や、最小文字数の設定について記されている場合があります。

注:ベスト プラクティスのガイドラインでは、次に示すような強力なパスワードを実稼働環境で使用することが求められています。ただし、このコースの他の実習では、実習を容易に進められるように cisco や class というパスワードを使用します。

a. ガイドラインを満たすように、特権 EXEC の暗号化パスワードを変更します。

```
R1(config)# enable secret Enablep@55
```

b. すべてのパスワードを 10 文字以上にする必要があります。

```
R1(config)# security passwords min-length 10
```

手順 2:　SSH 接続を有効にします。

a. ドメイン名として **CCNA-lab.com** を割り当てます。

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

b. SSH を介してルータに接続するときに使用するローカル ユーザ データベース エントリを作成します。パスワードが強力なパスワードの基準を満たしていて、ユーザが管理者レベルのアクセス権を持っている必要があります。

```
R1(config)# username admin privilege 15 secret Admin15p@55
```

c. SSH 接続を受け入れるように vty 回線のトランスポート入力を設定します。ただし、Telnet 接続は受け入れないようにします。

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

d. vty 回線では認証のためにローカル ユーザ データベースを使用する必要があります。

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

e. 1024 ビットの法を使用して RSA 暗号キーを生成します。

```
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 2 seconds)

R1(config)#
*Jan 31 17:54:16.127: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

手順 3:　コンソール回線と vty 回線のセキュリティ保護を行います。

a. アイドル状態のまま指定の時間が過ぎると接続のログアウトを行うように、ルータを設定できます。ネットワーク管理者がネットワーク デバイスにログインしてすぐに席を外した場合、このコマンドにより、指定の時間が過ぎるとユーザのログアウトが自動的に行われます。次のコマンドにより、回線は非アクティブの状態のまま 5 分が経過するとログアウトされます。

```
R1(config)# line console 0
R1(config-line)# exec-timeout 5 0
R1(config-line)# line vty 0 4
R1(config-line)# exec-timeout 5 0
R1(config-line)# exit
R1(config)#
```

b. 次のコマンドは、総当たり攻撃によるログイン試行を阻止します。ルータは、ログインの失敗が 120 秒以内に 2 回発生すると、ログイン試行を 30 秒間ブロックします。このタイマーは、この実習のために特に低い値に設定されます。

```
R1(config)# login block-for 30 attempts 2 within 120
```

上記のコマンドの **2 within 120** は何を意味していますか?

上記のコマンドの **block-for 30** は何を意味していますか?

手順 4:　すべての未使用ポートが無効になっていることを確認します。

ルータ ポートはデフォルトで無効になっていますが、念のために必ず、すべての未使用ポートが管理上ダウンの状態であることを確認します。このチェックは **show ip interface brief** コマンドの発行によって迅速に行えます。管理上ダウンの状態にない未使用ポートがあれば、インターフェイス コンフィギュレーション モードで **shutdown コマンド**を使用して無効にする必要があります。

```
R1# show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Embedded-Service-Engine0/0 unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet0/1         192.168.1.1     YES manual up                    up
Serial0/0/0                unassigned      YES NVRAM  administratively down down
Serial0/0/1                unassigned      YES NVRAM  administratively down down
R1#
```

手順 5:　セキュリティ対策が正しく実施されていることを確認します。

a. Tera Term を使用して telnet で R1 に接続します。

R1 はこの Telnet 接続を受け入れますか。

その理由を述べてください。

b. Tera Term を使用して R1 に SSH で接続します。

R1 はこの SSH 接続を受け入れますか。

c. ユーザおよびパスワードの情報を意図的に誤入力することでログインに 2 回失敗した後に、ログイン アクセスがブロックされるかどうかを確認します。

2 回目のログインに失敗した後、何が起こりましたか。

d. ルータのコンソール セッションから **show login** コマンドを発行して、ログイン ステータスを表示します。次の例では、**show login** コマンドが 30 秒間のログイン ブロック期間内に発行されたので、ルータが待機モードであると表示されています。このルータは、あと 14 秒間はログイン試行を一切受け付けません。

```
R1# show login
     A default login delay of 1 second is applied.
     No Quiet-Mode access list has been configured.

     Router enabled to watch for login Attacks.
     If more than 2 login failures occur in 120 seconds or less,
     logins will be disabled for 30 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 14 seconds.
     Denying logins from all sources.
R1#
```

e. 30 秒経過後、再び SSH を R1 に対して実行し、**admin** というユーザ名と **Admin15p@55** というパスワードを使用してログインします。

正常にログインした後、何が表示されましたか。

f. 特権 EXEC モードに入り、パスワードに **Enablep@55** を使用します。

このパスワードの誤入力によって 120 秒以内に 2 回失敗すると、SSH セッションは切断されますか。

その理由を述べてください。

g. 特権 EXEC プロンプトで **show running-config** コマンドを発行して、適用したセキュリティ設定を確認します。

パート 3:　スイッチに基本的なセキュリティ対策を設定する

手順 1:　スイッチのパスワードを強化します。

強力なパスワードのガイドラインを満たすように、特権 EXEC の暗号化パスワードを変更します。

```
S1(config)# enable secret Enablep@55
```

注:security **password min-length** コマンドは、2960 スイッチでは使用できません。

手順 2:　SSH 接続を有効にします。

a. ドメイン名として **CCNA-lab.com** を割り当てます。

```
S1(config)# ip domain-name CCNA-lab.com
```

b. SSH によるルータへの接続時に使用するローカル ユーザ データベース エントリを作成します。パスワードが強力なパスワードの基準を満たしていて、ユーザが管理者レベルのアクセス権を持っている必要があります。

```
S1(config)# username admin privilege 15 secret Admin15p@55
```

c. SSH 接続は受け入れても Telnet 接続は受け入れないように vty 回線のトランスポート入力を設定します。

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

d. vty 回線では認証のためにローカル ユーザ データベースを使用する必要があります。

```
S1(config-line)# login local
S1(config-line)# exit
```

e. 1024 ビットの法を使用して RSA 暗号キーを生成します。

```
S1(config)# crypto key generate rsa modulus 1024
```

手順 3:　コンソール回線と vty 回線のセキュリティ保護を行います。

a. アイドル状態が 10 分間続いた場合はスイッチを回線からログアウトさせます。

```
S1(config)# line console 0
S1(config-line)# exec-timeout 10 0
S1(config-line)# line vty 0 15
S1(config-line)# exec-timeout 10 0
S1(config-line)# exit
S1(config)#
```

b. 総当たり攻撃によるログイン試行を阻止するために、120 秒以内に 2 回ログインに失敗した場合はログイン アクセスを 30 秒間ブロックするようにスイッチを設定します。このタイマーは、この実習のために特に低い値に設定されます。

```
S1(config)# login block-for 30 attempts 2 within 120
S1(config)# end
```

手順 4:　すべての未使用ポートが無効になっていることを確認します。

スイッチ ポートはデフォルトで有効になっています。スイッチで使用されていないすべてのポートをシャットダウンします。

a. スイッチ ポートの状態は **show ip interface brief** コマンドを使用して確認できます。

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  down                  down
FastEthernet0/2        unassigned      YES unset  down                  down
FastEthernet0/3        unassigned      YES unset  down                  down
FastEthernet0/4        unassigned      YES unset  down                  down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  down                  down
FastEthernet0/8        unassigned      YES unset  down                  down
FastEthernet0/9        unassigned      YES unset  down                  down
FastEthernet0/10       unassigned      YES unset  down                  down
FastEthernet0/11       unassigned      YES unset  down                  down
FastEthernet0/12       unassigned      YES unset  down                  down
FastEthernet0/13       unassigned      YES unset  down                  down
FastEthernet0/14       unassigned      YES unset  down                  down
FastEthernet0/15       unassigned      YES unset  down                  down
FastEthernet0/16       unassigned      YES unset  down                  down
FastEthernet0/17       unassigned      YES unset  down                  down
FastEthernet0/18       unassigned      YES unset  down                  down
FastEthernet0/19       unassigned      YES unset  down                  down
FastEthernet0/20       unassigned      YES unset  down                  down
FastEthernet0/21       unassigned      YES unset  down                  down
FastEthernet0/22       unassigned      YES unset  down                  down
FastEthernet0/23       unassigned      YES unset  down                  down
FastEthernet0/24       unassigned      YES unset  down                  down
GigabitEthernet0/1     unassigned      YES unset  down                  down
GigabitEthernet0/2     unassigned      YES unset  down                  down
S1#
```

b. 複数のインターフェイスを一度にシャットダウンするには、**interface range** コマンドを使用します。

```
S1(config)# interface range f0/1-4 , f0/7-24 , g0/1-2
S1(config-if-range)# shutdown
S1(config-if-range)# end
S1#
```

c. 非アクティブ状態のインターフェイスがすべて管理上シャットダウンの状態であることを確認します。

```
S1# show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
Vlan1                  192.168.1.11    YES manual up                    up
FastEthernet0/1        unassigned      YES unset  administratively down down
FastEthernet0/2        unassigned      YES unset  administratively down down
FastEthernet0/3        unassigned      YES unset  administratively down down
FastEthernet0/4        unassigned      YES unset  administratively down down
FastEthernet0/5        unassigned      YES unset  up                    up
FastEthernet0/6        unassigned      YES unset  up                    up
FastEthernet0/7        unassigned      YES unset  administratively down down
```

```
FastEthernet0/8        unassigned      YES unset  administratively down down
FastEthernet0/9        unassigned      YES unset  administratively down down
FastEthernet0/10       unassigned      YES unset  administratively down down
FastEthernet0/11       unassigned      YES unset  administratively down down
FastEthernet0/12       unassigned      YES unset  administratively down down
FastEthernet0/13       unassigned      YES unset  administratively down down
FastEthernet0/14       unassigned      YES unset  administratively down down
FastEthernet0/15       unassigned      YES unset  administratively down down
FastEthernet0/16       unassigned      YES unset  administratively down down
FastEthernet0/17       unassigned      YES unset  administratively down down
FastEthernet0/18       unassigned      YES unset  administratively down down
FastEthernet0/19       unassigned      YES unset  administratively down down
FastEthernet0/20       unassigned      YES unset  administratively down down
FastEthernet0/21       unassigned      YES unset  administratively down down
FastEthernet0/22       unassigned      YES unset  administratively down down
FastEthernet0/23       unassigned      YES unset  administratively down down
FastEthernet0/24       unassigned      YES unset  administratively down down
GigabitEthernet0/1     unassigned      YES unset  administratively down down
GigabitEthernet0/2     unassigned      YES unset  administratively down down
S1#
```

手順 5:　セキュリティ対策が正しく実施されていることを確認します。

a. スイッチで Telnet が無効になっていることを確認します。

b. SSH でスイッチに接続し、ユーザおよびパスワードの情報を意図的に誤入力して、ログイン アクセスがブロックされるかどうかを確認します。

c. 30 秒経過後、再び SSH で S1 に接続し、**admin** というユーザ名と **Admin15p@55** というパスワードを使用してログインを行います。

正常にログインした後、バナーは表示されましたか。

d. パスワードに **Enablep@55** を使用して特権 EXEC モードに入ります。

e. 特権 EXEC プロンプトで **show running-config** コマンドを発行して、適用したセキュリティ設定を確認します。

復習

1. パート 1 の基本設定では、コンソール回線と vty 回線で **password cisco** コマンドが入力されました。ベスト プラクティスのセキュリティ対策が適用された後、このパスワードはいつ使用されますか。

2. 事前に設定された 10 文字未満のパスワードは、**security passwords min-length 10** コマンドの影響を受けますか。

ルータ インターフェイスの要約表

ルータ インターフェイスの要約				
ルータのモデル	**イーサネット インターフェイス #1**	**イーサネット インターフェイス #2**	**シリアル インターフェイス #1**	**シリアル インターフェイス #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 (S0/0/0)	Serial 0/1/1 (S0/0/1)
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)

注: ルータがどのように設定されているかを確認するには、インターフェイスを調べ、ルータの種類とルータが持つインターフェイスの数を識別します。各ルータ クラスの設定のすべての組み合わせを効果的に示す方法はありません。この表には、デバイスにイーサネットおよびシリアル インターフェイスの取り得る組み合わせに対する ID が記されています。その他のタイプのインターフェイスは、たとえ特定のルータに含まれている可能性があるものであっても、表には一切含まれていません。ISDN BRI インターフェイスはその一例です。カッコ内の文字列は、インターフェイスを表すために Cisco IOS コマンドで使用できる正規の省略形です。