Ciscoネットワーク演習2　第7週　　 クラス　　　　番号　　　　氏名

• 16 - ネットワークセキュリティの基礎

16.0 - 概要

16.0.1 - このモジュールを学ぶ理由

ネットワーク管理者は、脅威のアクターがネットワークにアクセスすることを困難にするのも職務の一環です。 このモジュールでは、ネットワーク攻撃の種類と、脅威アクターが成功する可能性を低減するために何ができるかについて説明します。

16.0.2 - このモジュールで学ぶこと

**セキュリティの脅威と脆弱性：**基本的なセキュリティ対策がネットワークデバイス上で必要な理由を説明します。

**ネットワーク攻撃：**セキュリティの脆弱性の特定

**ネットワーク攻撃の軽減：**一般的な軽減手法を明確にします。

**デバイスのセキュリティ：**デバイス強化機能を使用してネットワークデバイスを構成し、 セキュリティの脅威を軽減します。

16.1 - セキュリティの脅威と脆弱性

16.1.1 - 脅威のタイプ

脅威アクターがネットワークにアクセスすると、 4 種類の脅威が発生する可能性があります。

**情報の盗難**：機密情報を得るためにコンピュータに侵入しています。

**データの消失や改ざん**：コンピュータに侵入し、データ記録を**[** ① **破棄したり、改ざん** **]**したりします。

**ID の窃取**：情報の盗難の1つの形式で、他人の ID を乗っ取る目的で個人情報が盗まれます。

**サービスの中断**：正当なユーザが権利を有するサービスにアクセスすることを妨げています。

16.1.2 - 脆弱性の種類

主な脆弱性または弱点には、技術、構成、およびセキュリティポリシーの 3 つがあります。

**技術的な脆弱性：**TCP/IP プロトコルの弱点、オペレーティングシステムの弱点、ネットワーク機器の弱点

**設定の脆弱性：**保護されていないユーザーアカウント、簡単に推測できるパスワードを持つシステムアカウント、インターネットサービスの設定の誤り、製品の安全でないデフォルト設定、ネットワーク機器の設定誤り

**ポリシーの脆弱性：**書面による**[** ② **セキュリティポリシー ]**の欠如、政治、認証の継続性の欠如、論理アクセスコントロールが適用されていない、ソフトウェアとハードウェアのインストール、および変更がポリシーに従わない、ディザスタリカバリ計画が存在しない

16.1.3 - 物理的なセキュリティ

物理的な脅威の4つのクラスは次のとおりです。

**ハードウェアの脅威：**これには、サーバ、ルータ、スイッチ、配線設備、およびワークステーションへの物理的な損傷が含まれます。

**環境の脅威：**過度な温度（暑すぎるまたは寒すぎる）や過度な湿度（湿度が高すぎるまたは低すぎる）も脅威になることがあります。

**電気的な脅威：**電圧スパイク、不十分な供給電圧（電圧低下）、未調整の電力（ノイズ）、完全な停電などが含まれます。

**メンテナンスの脅威：**これには、主要な電気部品の不適切な取り扱い（静電気放電）、重要なスペアパーツの欠如、ケーブル配線の不良、ラベリングの不良が含まれます。

16.1.4 - 理解の確認-セキュリティの脅威と脆弱性

16..2 - ネットワーク攻撃

16.2.1 - マルウェアの種類

**ウイルス：**コンピュータウイルスは、自身のコピーを別のプログラムに挿入し、そのプログラムの一部となることによって伝播するマルウェアの一種です。ウイルスは、システムに存在していても、ユーザがその悪意のあるホスト ファイルまたはプログラムを実行するか開くかしない限りは、アクティブになったり広まったりしません。

**ワーム：**コンピュータワームは自身の機能的コピーを複製し、同じタイプの障害を発生させるという点でウイルスに似ています。しかし、感染したホスト ファイルによる拡散が必要なウイルスとは対照的に、ワームはスタンドアロン ソフトウェアであり、伝播にホスト プログラムや人間の関与は必要ありません。

**トロイの木馬：**トロイの木馬は別のタイプのマルウェアで，ギリシャ人がトロイに侵入するのに使用した木馬にちなんで命名されています．これは一見、正規のものに見えますが、有害なソフトウェアです。トロイの木馬は、悪意のあるユーザがシステムにアクセスするバック ドアを作成することでも知られています。

16.2.2 - 偵察攻撃

悪意のあるコード攻撃に加えて、ネットワークがさまざまなネットワーク攻撃の餌食になる可能性もあります。ネットワーク攻撃は、次の 3 つの主要なカテゴリに分類できます。

**偵察攻撃：**システム、サービス、または脆弱性の検出とマッピングです。

**アクセス攻撃：**データ、システムアクセス、またはユーザ権限の不正な操作。

**サービス拒否：**ネットワーク、システム、またはサービスの無効化または破損。

16.2.3 - アクセス攻撃

アクセス攻撃により、閲覧権を持たない情報に**[** ③ **不正なアクセス ]**をすることができます。アクセス攻撃は、パスワード攻撃、トラストエクスプロイト、ポートリダイレクト、中間者の 4 種類に分類できます。

**パスワード攻撃：**脅威アクターは、いくつかの異なる方法でパスワード攻撃を実装できます。

**トラスト エクスプロイト：**トラストエクスプロイト攻撃では、脅威アクターが不正な権限を使用してシステムへのアクセスを取得し、ターゲットを危険にさらす可能性があります。

**ポート リダイレクト：**ポートリダイレクト攻撃では，脅威アクターは侵害したシステムを，別のターゲットに対して攻撃する拠点として利用します．

**中間者攻撃：**中間者攻撃では，脅威アクターが 2 つの正当なエンティティの間に割り込み、2 者間で渡されるデータを読み取り、変更します。

16.2.4 - サービス妨害攻撃

サービス妨害（DoS）攻撃は、最も公開されている攻撃形式であり、排除するのが最も困難です。しかし、実装が容易で、重大な損害が発生する可能性があるため、DoS 攻撃はセキュリティ管理者は特別な注意を払う必要があります。

**DoS 攻撃：**DoS 攻撃は通信を妨げ、多大な時間とコスト損失をもたらす、重大なリスクとなります。これらの攻撃は、スキルの低い攻撃者でも比較的容易に実行できます。

**DDoS 攻撃：**DDoS攻撃は、DoS 攻撃に似ていますが、複数の連携した送信元からから発生します。脅威アクターは、コマンド&コントロール (CnC) プログラムを使用して、ゾンビのボットネットに DDoS 攻撃を実行するように指示します。

16.2.5 - 理解の確認-ネットワーク攻撃

16.2.6 - ラボ-ネットワークセキュリティの脅威を調査する

省略

16.3 - ネットワーク攻撃の緩和策

16.3.1 - 多層防御アプローチ

脅威アクターがネットワークに侵入する方法について詳しく理解したので、この不正アクセスを防ぐために何をすべきかを理解する必要があります。このトピックでは、ネットワークのセキュリティを強化するために実行できるいくつかのアクションについて説明します。

ネットワーク攻撃を軽減するには、まずルーター、スイッチ、サーバ、ホストなどのデバイスを保護する必要があります。ほとんどの組織では、セキュリティに対する**[** ④ **多層防御アプローチ ]** (階層型アプローチ) を採用しています。これには、ネットワーキングデバイスとサービスの組み合わせが連携している必要があります。

16.3.2 - バックアップを保持

デバイスの設定やデータのバックアップは、データの損失を防ぐ最も効果的な方法の 1 つです。データ バックアップでは、コンピュータ上の情報のコピーがリムーバブル バックアップ メディアに保存され，安全な場所に保管されます．

コンピュータまたはルータハードウェアに障害が発生した場合は、バックアップコピーを使用してデータまたは設定を復元できます。

16.3.3 - アップグレード、更新、パッチ

最新の開発状況に追従することは、ネットワーク攻撃に対するより効果的な防御につながる可能性があります。新しいマルウェアがリリースされると、企業はウイルス対策ソフトウェアの最新バージョンを最新の状態に保つ必要があります。

ワーム攻撃を軽減する最も効果的な方法は、オペレーティングシステムのベンダーからセキュリティ更新プログラムをダウンロードし、脆弱なすべてのシステムにパッチを適用することです。

16.3.4 - 認証、許可、アカウンティング

すべてのネットワークデバイスは、許可された個人だけがアクセスできるように安全に設定する必要があります。認証，認可，アカウンティング（AAA または トリプルA）ネットワークセキュリティサービスは，ネットワークデバイスのアクセス制御を設定する主要なフレームワークを提供します．

**[** ⑤ **AAA ]**は、ネットワークへのアクセスを許可されるユーザ（認証）、ネットワークへのアクセス中に実行するアクション（認可）を制御する方法で、アクセス中に実行された処理を記録します（アカウンティング）。

16.3.5 - ファイアウォール

ファイアウォールは、外部の脅威からユーザを保護するために利用できる最も効果的なセキュリティツールの 1 つです。ファイアウォールは、望ましくないトラフィックが**[** ⑥ **内部ネットワーク ]**に入るのを防ぐことによって、コンピュータとネットワークを保護します。

16.3.6 - ファイアウォールの種類

**パケットフィルタリング：**IPまたは MAC アドレスに基づいてアクセスを禁止または許可します。

**アプリケーションのフィルタリング：**ポート番号に基づいて特定のアプリケーション・タイプによるアクセスを禁止または許可します。

**URL フィルタリング：**特定の URL またはキーワードに基づいて Web サイトへのアクセスを禁止または許可します。

**ステートフルパケットインスペクション（SPI）：**着信パケットは、内部ホストからの要求に対する正当な応答である必要があります。

16.3.7 - エンドポイントセキュリティ

エンドポイントデバイスのセキュリティ保護は、人間性も関わってくるため，ネットワーク管理者にとって最も困難な作業の 1 つです。企業は、適切な文書化されたポリシーを整える必要があり、従業員はこれらのルールを認識する必要があります。

ポリシーには、**[** ⑦ **ウイルス対策 ]**ソフトウェアとホスト侵入防止の使用が含まれます。

16.3.8 - 理解の確認-ネットワーク攻撃の軽減

16.4 - デバイスのセキュリティ

16.4.1 - Cisco AutoSecure

新しいオペレーティングシステムがデバイスにインストールされると、セキュリティ設定は既定値に設定されます。ほとんどの場合、このレベルのセキュリティは不十分です。Cisco ルータの場合、例に示すように、**Cisco AutoSecure** 機能を使用してシステムのセキュリティを確保できます。

|  |
| --- |
| Router# auto secure  --- AutoSecure Configuration ---  \*\*\* AutoSecure configuration enhances the security of  the router but it will not make router absolutely secure  from all security attacks \*\*\* |

16.4.2 - パスワード

ネットワークデバイスを保護するには、強力なパスワードを使用することが重要です。従うべきガイドラインを示します。

パスワードの長さは 8 文字以上 (できれば 10 文字以上) を使用してください。長いパスワードは、より安全なパスワードです。

パスワードを複雑にします。許可されている場合は、大文字と小文字、数字、記号、スペースを組み合わせて使用してください。

繰り返し、一般的な辞書の単語、連続する文字または数字、ユーザ名、親戚またはペットの名前、来歴情報（生年月日、ID 番号、先祖の名前など）、その他の識別しやすい情報に基づくパスワードは避けてください。

意図的にパスワードのスペルを間違える。例えば、Smith = Smyth = 5myth または Security = 5ecur1ty とする。

頻繁にパスワードを変更する．知らない間にパスワードが侵害された場合でも、脅威アクターがパスワードを使用する機会は制限されます。

パスワードを書き留めて、机やモニターなどのすぐわかる場所に放置しない。

16.4.3 - 追加のパスワードセキュリティ

図の設定例に示されているように、 **service password-encryptionservice**コマンドは、権限のないユーザがコンフィギュレーションファイル内の平文のパスワードを表示することを防止します。たとえばこの図で、 **login block-for 120 attempts 3 within 60** コマンドは，  
**[** ⑧ **60 ]**秒以内に**[** ⑨ **3 ]**回のログイン試行が失敗した場合、 vty ログイン試行を**[** ⑩ **120 ]**秒間ブロックします。

デフォルトでは、Cisco ルータは、非アクティブ状態が 10 分経過すると EXEC セッションをログアウトします。ただし、 **exec-timeout *minutes seconds*** ラインコンフィギュレーションコマンドを使用して、この設定を減らすことができます。

|  |
| --- |
| R1(config)# service password-encryption  R1(config)# security passwords min-length 8  R1(config)# login block-for 120 attempts 3 within 60  R1(config)# line vty 0 4  R1(config-line)# password cisco  R1(config-line)# exec-timeout 5 30  R1(config-line)# transport input ssh  R1(config-line)# end  R1#  R1# show running-config | section line vty  line vty 0 4  password 7 094F471A1A0A  exec-timeout 5 30  login  transport input ssh  R1# |

16.4.4 - SSH の有効化

次の 6 つの手順を使用して、シスコデバイスがSSH をサポートするように設定できます。

**ステップ1. 一意なデバイスホスト名を設定する。 hostname** コマンドを使用

**ステップ2. IPドメイン名を設定する。** **ip domain-name**コマンドを使用します

**ステップ3. SSHトラフィックを暗号化するキーを生成**．**crypto key generate rsa general-keys modulus**コマンドを**使用**

**ステップ4. ローカルデータベースのエントリを確認あるいは作成する。 usernameコマンド**を使用して、ローカルデータベースのユーザ名エントリを作成します。

**ステップ5. ローカルデータベースで認証する.** **ローカルデータベース**に対して vty 回線を認証するには、 **login local**コマンドを使用します。

**ステップ6. SSHセッションの着信を有効にする。** **transport input ssh** コマンドを**使用**して、Telnet や SSH などの複数の入力プロトコルを指定できます。

SSH設定例：

|  |
| --- |
| Router# **configure terminal**  Router(config)# **hostname R1**  R1(config)# **ip domain name span.com**  R1(config)# **crypto key generate rsa general-keys modulus 1024**  The name for the keys will be: Rl.span.com % The key modulus size is 1024 bits  % Generating 1024 bit RSA keys, keys will be non-exportable...[OK]  Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled  R1(config)#  R1(config)# **username Bob secret cisco**  R1(config)# **line vty 0 4**  R1(config-line)# **login local**  R1(config-line)# **transport input ssh**  R1(config-line)# **exit**  R1(config)# |

16.4.5 - 使用していないサービスの無効化

シスコのルータおよびスイッチは、アクティブなサービスとともに始動しますが，ネットワーク内で必要になる場合とそうでない場合があります。**[** ⑪ **未使用のサービス ]**を無効にして、CPU サイクルや RAM などのシステムリソースを節約し、脅威アクターがこれらのサービスを悪用しないようにします。

例に示すように、 **show ip ports all** コマンドを使用して確認できます。

|  |
| --- |
| **Router# show ip ports all**  **Proto Local Address Foreign Address State PID/Program Name**  **TCB Local Address Foreign Address (state)**  **tcp :::443 :::\* LISTEN 309/[IOS]HTTP CORE**  **tcp \*:443 \*:\* LISTEN 309/[IOS]HTTP CORE**  **udp \*:67 0.0.0.0:0 387/[IOS]DHCPD Receive**  **Router#** |

16.4.6 - Packet Tracer - セキュアなパスワードと SSH の設定

省略

16.4.7 - 実習-SSH を使用したネットワークデバイスの設定

16.5 - モジュール練習とクイズ

16.5.1 - Packet Tracer - ネットワークデバイスのセキュリティ保護記載内容: Packet Tracers, Text

16.5.2 - ラボ - ネットワークデバイスのセキュリティ保護記載内容: Labs, Text

16.5.3 - このモジュールで学んだこと記載内容: Text

16.5.4 - モジュールクイズ-ネットワークセキュリティの基礎記載内容: Module Quiz, Text