Clean Access：ネットワーク スキャニング機能を使用して、エージェント チェックのバイパスを試みるユーザを検出する方法

目次

概要

Cisco Clean Access は、ネットワーク管理者が指定するネットワーク アクセスの要件をユーザが満たすことができるセキュリティ ポリシー コンプライアンス ソリューションです。 Cisco Clean Access は、ユーザがアクセス要件を満たすまでネットワークへのアクセスを制限します。 また、Cisco Clean Access は、システムを評価し、コンプライアンス違反を検出し、コンプライアンスを実現するための修復を支援する使いやすいクライアント アプリケーションを通じて、要件への準拠を支援します。 現在、このエージェント（クライアント アプリケーション）は、Windows 98、Windows Me、Windows 2000 Professional、Windows XP（Home と Pro の両方、Pro は 32 ビット バージョンのみサポート）を含む Microsoft Windows オペレーティング システムでのみ使用できます。

コンプライアンス要件のチェックを避けるためにエージェント インストールを迂回しようとする不正なユーザは、システムを変更して Window 以外のシステムに見せかけることがあります。 このドキュメントでは、このようなユーザを検出して、場合によってはネットワークへのアクセスをブロックするために推奨される方法について説明します。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Windows 98、Windows Me、Windows 2000 Professional、および Windows XP（Home およ

び Pro の両方。Pro は 32 ビット バージョンのみサポート）

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

解決策

Cisco Clean Access には、クライアント ベースのスキャンと修復に加え、システムに対してネットワークベースのスキャンを実行して Web ベースの修復を行うメカニズムがあります。 ネットワークベースのスキャンは、主に Windows 以外のシステムに対して使用されます。 ただし、このスキャンは Windows 以外のシステムに限定されるわけではありません。

ネットワーク スキャン機能を使用するには、ネットワーク管理者が Nessus オープン ソース脆弱性スキャナに必要なプラグインを Cisco Clean Access サーバにダウンロードしてインストールする必要があります。 Nessus プラグインのダウンロードおよびインストール方法については、『*Cisco NAC Appliance - Clean Access Manager Installation and Configuration Guide, Release 4.1(2)*』の「Configuring Network Scanning」を参照してください。

このシナリオでは複数の Nessus プラグインを使用できます。 いくつかの例を記載します（すべてを網羅したリストではありません）。

- **オペレーティング システム識別用プラグイン**（プラグイン番号 11936 など）：これらのプラグインをターゲット システムに対して実行すると、検出されたオペレーティング システムの名前がスキャン結果として表示されます。 これらのプラグインを Cisco Clean Access 内で使用するには、プラグインを変更する必要があります。 具体的には、スキャンしたオペレーティング システムが Windows 以外のシステムではない場合には HOLE を返すようにプラグインを変更する必要があります。 たとえば、スキャンした Linux システムが Windows システムであることが分かった場合、プラグインは結果として HOLE を返す必要があります。
- **ポート スキャン用プラグイン**（nmap.nasl など）：これらのプラグインをターゲット システムに対して実行する場合、オープン ポート、リスナーなどのリストを提供するようにプラグインを設定できます。 これらのプラグインも、TCP フィンガープリントなどの手法によって、ホスト上で使用されているオペレーティング システムを検出することができます。 これらのプラグインにも、オペレーティング システム識別用プラグインと同じように変更を加える必要があります。 スキャンしたオペレーティング システムが Windows 以外のシステムではない場合に、プラグインは HOLE を返す必要があります。 具体的には、期待されるオペレーティング システムが Windows 以外のオペレーティング システムでない場合には HOLE を返すようにプラグインを変更する必要があります。 たとえば、スキャンした Linux システムが Windows システムであることが分かった場合、プラグインは結果として HOLE を返す必要があります。
- **Windows システムから情報を取得するためのプラグイン**（サーバ メッセージ ブロック（SMB）関連のプラグインおよびプラグイン番号 10859 など）：この手法の背後にある考え方は、Linux ホスト、Mac ホスト、またはその他の Windows 以外のシステムであると主張するマシンが実際に Windows システムであるかどうかを検出するだけで十分であるというものです。 これを行うための最も簡単な方法は、何らかの SMB 関連の Nessus プラグイン（特

に、SMB のホスト SID を取得する、ID 番号 10859 のプラグイン）を有効にすることです。このプラグインは、Windows システムに関する値だけを返します。 そのため、何らかの情報が返されたとしたら、そのシステムが Windows オペレーティング システムを実装していると結論しても構わないでしょう。 また、NetBIOS を使用する Windows システムから情報を回収するプラグインも使用できます。 その場合、システムが NetBIOS の情報を返したとしたら、Windows システムである可能性が高いことになります。**注意：** Samba を実行する Linux マシンなどを誤検出する可能性があります。

Nessus プラグインを使用してネットワーク スキャンを実行するように Cisco Clean Access Manager を設定するには、次の手順を実行します。

1. ブラウザで Cisco Clean Access Manager Web コンソールを開き、管理者としてログインします。
2. [Clean Access] > [Network Scanner] の順に選択して [Scan Setup] ページにアクセスします。
3. [Role] をスキャン対象のユーザ ロールに設定し、オペレーティング システムを [All] に設定した状態で、このドキュメントで箇条書きした「Windows システムから情報を取得するためのプラグイン」で取り上げられているプラグイン（たとえば、10859 番）を選択します。
4. [Vulnerabilities] セクションの [Vulnerable If…] を [HOLE, WARN, INFO] に設定します。
5. Windows オペレーティング システムのスキャンを無効にします。[Operating System] ドロップダウン リストから [WIN_ALL] を選択します。この選択項目に対するスキャンを無効にします。

要約

このドキュメントでは、Cisco Clean Access のネットワーク スキャン機能を使用して、Windows 以外のシステムを使用しているふりをするユーザを検出するメカニズムを説明しました。 オペレーティング システムを検出するのにより一層効果的なプラグインは他にもあるかもしれません。たとえば、Sys-security 製の xprobe2 という NMAP ネットワーク スキャン ツールなどがニーズにより適合する可能性もあります。 また、クライアント マシンがパーソナル ファイアウォールを実行している場合、ネットワーク スキャンでは確実な結果を出せない場合があることに注意してください。

注意事項

- Nessus は Tenable Network Security の登録商標です。
- Nessus プラグインを入手するには、Tenable Security に登録する必要があります。
- プラグインを変更/オーサリングする際は、Nessus および Tenable Network Security のライセンスと商標に関する要件に従ってください。

関連情報

- Cisco Clean Access（NAC アプライアンス）製品のサポート
- テクニカル サポートとドキュメント – Cisco Systems