Nessus コンプライアンス チェック

監査システムの構成とコンテンツ

2014 年 4 月 23 日

(第 78 版)

目次

はじめに

本書では、Nessus 5.x を使用して、Unix、Windows、データベース、SCADA、IBM iSeries、Cisco の各システムの構成をコンプライアンス ポリシーに照らして監視したり、さまざまなシステムのコンテンツに機密コンテンツが含まれていないか確認したりする方法について説明します。

本書では、"ポリシー コンプライアンス" と "コンプライアンス スキャン" は、同じ意味で使われています。

Nessus は SCADA システム監査をサポートしていますが、この機能は本書の範囲外になりますので、この機能の詳細については、Tenable SCADA 情報ページ (こちら) を参照してください。

コンプライアンス監査は、脆弱性スキャンの実行と一部重なる部分もありますが、同じものではありません。コンプライアンス監査では、確立されたポリシーに沿ってシステムが構成されているかどうかを調べます。脆弱性スキャンは、システムが既知の脆弱性の脅威にさらされているかどうかを調べます。本書では、構成パラメータの種類、監査できる機密データの種類、監査を実行するために Nessus を構成する方法、また Tenable の SecurityCenter を使用してそのプロセスを管理および自動化する方法について説明します。

前提条件

本書は、Nessus の脆弱性スキャナに関してある程度の知識をお持ちの方を対象としています。Unix および Windows のローカル パッチ監査を実行するための Nessus の構成方法については、「Unix と Windows での Nessus 認証チェック」(http://www.tenable.com/products/nessus/documentation) を参照してください。

Nessus および SecurityCenter の利用

本書で説明するコンプライアンス チェックを実行するには、有料の Nessus をサブスクライブするか、SecurityCenter をご利用になる必要があります。どちらも、Tenable Network Security (http://www.tenable.com/) から提供されています。監査を実行するための詳細な技術要件については、以下のいくつかのセクションで説明しています。

表記の規則

本書では、ファイル名、デーモン、および実行可能ファイルは、**courier bold** で記載されています。

また、コマンド ライン オプションおよびキーワードも **courier bold** フォントで記載されています。コマンド ラインの例には、コマンド ライン プロンプトおよびコマンド実行の結果得られた出力テキストが含まれる場合と含まれない場合があります。コマンド ラインの例では、実行中のコマンド (ユーザー入力文字) は **courier bold** で、システムによって生成されたサンプル出力は courier (not bold) で記載されています。以下に Unix の **pwd** コマンドの実行例を示します。

```
# pwd
/home/test/
#
```

重要な注意点は、この記号と、グレーのテキスト ボックスで示します。

ヒント、例、およびベスト プラクティスは、この記号と、青字に白文字で示します。

コンプライアンス規定

政府規制や財政規制に従い、さまざまなコンプライアンス要件があります。これらのコンプライアンス要件は最低条件として提示されているものであり、組織の事業目標に応じて異なる解釈が必要となります。リスクを適切に特定し軽減するためには、コンプライアンス要件を事業目標に対応付けなければなりません。このプロセスの開発の詳細については、Tenable の "Maximizing ROI on Vulnerability Management" (http://www.tenable.com/whitepapers) を参照してください。

たとえば、企業によっては、顧客の個人特定情報 (PII) が保存されているすべてのサーバーでは、ログを有効化し、10 文字以上のパスワードを設定しなければならない、というようなポリシーを設定している場合があります。これは、企業が各種の規制に対するコンプライアンスを維持する上で有用なポリシーです。

以下に、一般的なコンプライアンスの規制やガイドの一例を挙げます。

- BASEL II
- Center for Internet Security Benchmarks (CIS)
- Control Objectives for Information and related Technology (COBIT)
- Defense Information Systems Agency (DISA) STIG
- Federal Information Security Management Act (FISMA)
- Federal Desktop Core Configuration (FDCC)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- ISO 27002/17799 Security Standards
- Information Technology Information Library (ITIL)
- National Institute of Standards (NIST) 構成ガイドライン
- National Security Agency (NSA) 構成ガイドライン
- Payment Card Industry Data Security Standards (PCI DSS)
- Sarbanes-Oxley (SOX)
- Site Data Protection (SDP)
- United States Government Configuration Baseline (USGCB)
- 各種州法 (California の Security Breach Notification Act - SB 1386 など)

コンプライアンス チェックは、侵入検知やアクセス制御の実行といった、リアルタイム監視にも対応します。これらのコンプライアンス規制に対応するために、Tenable の構成監査、脆弱性管理、データ漏えい、ログ分析、およびネットワーク監視ソリューションがどのように役立つかを説明した文書 "Real-Time Compliance Monitoring" を提供しています。sales@tenable.com までメールでお問い合わせください。

構成監査、データ漏えい、コンプライアンス

監査とは

Nessus を使用して、Unix および Windows サーバー、Cisco デバイス、SCADA システム、IBM iSeries サーバー、およびデータベースにログインし、それらがローカル サイトのセキュリティ ポリシーに沿って構成されているかどうかを判断することができます。また Nessus では、Windows および Unix システムのハード ドライブ全体を検索して、不正なコンテンツの有無を調べることができます。

アセットを適切に保護するには、監査を実行する前に、サイトのセキュリティ ポリシーを確立することが重要です。脆弱性評価では、既知のエクスプロイトに対するシステムの脆弱性は調べますが、人事データがパブリック サーバーに保存されているかどうかなどは調べません。

セキュリティには、絶対的な基準は存在しません。組織ごとのリスク管理ニーズによって大きく異なります。

たとえば、パスワードの有効期間や変更禁止期間といったパスワード要件や、アカウントのロックアウト ポリシーについて考えてみます。パスワードを頻繁に変更する、または変更しない理由はさまざまです。また、ログインに 5 回失敗したらアカウントをロックするなども正当なポリシーです。しかし、ミッション クリティカルなシステムについてはより厳格なポリシーのほうが適しているでしょうし、逆に何度ログインに失敗してもアカウントをロックしないポリシーのほうが適していることもあります。

これらの構成設定は、システムの脆弱性や欠けているパッチではなく、システム管理やセキュリティ ポリシーに依存します。Nessus は、Unix および Windows サーバーに対してコンプライアンス チェックを実行できます。ポリシーは、個々のコンプライアンス スキャンの要件に応じて、非常に簡単なものから非常に複雑なものまで設定できます。

監査と脆弱性スキャン

Nessus は、ネットワーク サービスの脆弱性スキャンを実行することに加え、サーバーにログインして、欠けているパッチを検出することもできます。しかし脆弱性が検出されないからといって、サーバーが正しく構成されているとは限らず、特定の規制に "準拠している" とも限りません。

Nessus を使用して脆弱性スキャンとコンプライアンス監査を実行する利点は、このようなデータがすべて一度に入手できることです。サーバーの構成状態、パッチの状況、および存在する脆弱性のタイプを知ることで、リスク軽減の手段を決定しやすくなります。

より高いレベルでは、ネットワークやアセット クラス全体に関するこれらの情報を集約することで、セキュリティとリスクをグローバルに分析することが可能になります。Tenable の SecurityCenter はまさにこれを実行します。これにより監査担当者やネットワーク管理者は、非準拠システムの傾向を発見し、より大きな規模で問題を解決するために設定を調整することができます。

項目監査の例

以下のいくつかのセクションで、Windows、Unix、データベース、IBM iSeries、および Cisco システムでの構成監査について説明します。

Nessus 5 の正規表現エンジンは、Perl の特定の方言を基盤としており、その柔軟性とスピードの利点から、"Extended POSIX" と称されています。

監査ファイルはすべて、ANSI フォーマットでエンコードする必要があります。Unicode、Unicode big endian、および UTF-8 フォーマットのファイルは使用できません。

Windows

Nessus では、Microsoft Windows フレームワークで "ポリシー" として構成できるあらゆる設定をテストできます。レジストリ設定の中にも監査できる項目は数百あり、ファイル、ディレクトリ、およびオブジェクトへのパーミッションも分析できます。監査例では、以下の設定のテストなどを紹介しています。

- アカウント ロックアウトの期間
- セキュリティ ログの保持
- ローカルでのログオンを許可
- パスワード履歴を強制

以下は、Windows での "監査" 項目例です。

```
<item>
name: "Minimum password length"
value: 7
</item>
```

この監査は、Windows サーバー上で "最小パスワード長" の設定を検索し、値が 7 文字より小さい場合に警告を生成します。

Nessus は、Windows コンピュータ上で機密データを検索することもできます。以下に、各種ファイル フォーマットでの Visa クレジット カード番号を検索する例を示します。

```
<item>
type: FILE_CONTENT_CHECK
 description: "Determine if a file contains a valid VISA Credit Card Number"
file_extension: "xls" | "pdf" | "txt"
 regex: "([^0-9-]|^)(4[0-9]{3}( |-|)([0-9]{4})( |-|)([0-9]{4})( |-|)([0-9]{4}))([^0-9-
       ]|$)"
expect: "VISA" | "credit" | "Visa" | "CCN"
max_size: "50K"
only_show: "4"
</item>
```

このチェックは、Excel、Adobe、およびテキスト ファイルを検索して、Visa クレジット カード番号として有効な文字列のパターンの有無を調べます。

Unix

Nessus は、各種の Unix ベース システムで、ファイルのパーミッション、ファイル コンテンツ、実行プロセス、およびユーザー アクセス制御のテストに幅広く使用できます。現在、Solaris、Red Hat、AIX、HP-UX、SuSE、Gentoo、および FreeBSD の Unix の監査を実行するためのチェックが提供されています。

```
<item>
 name: "min_password_length"
 description: "Minimum password length"
 value: "14..MAX"
</item>
```

この監査は、Unix システム上で、最小パスワード長が 14 文字に設定されているかどうかをチェックします。

Cisco

Nessus は、Cisco IOS オペレーティング システムを実行しているシステムで実行中の構成をテストし、セキュリティ ポリシー基準に沿っているかどうか確認することができます。チェックは、特権なしでログインしても、または権限のある "enable" パスワードを使用しても実行できます。

```
<item>
type: CONFIG_CHECK
 description: "Require AAA service"
info: "Verify centralized authentication, authorization and accounting"
info: "(AAA)service (new-model) is enabled."
item: "aaa new-model"
</item>
```

Palo Alto Firewall

Nessus は、XSL Transforms (XSLT) とネイティブの API を使用して、PAN-OS ベースの Palo Alto デバイスの情報を要求します。要求はファイアウォールの HTTP または HTTPS インタフェースを通じて実行され、PAN-OS >= 4.1.0 では `Superuser` または `Superuser (readonly)` 管理者認証情報を、PAN-OS < 4.1.0 では `Superuser` 管理者認証情報を必要とします。これにより、デバイスの `operational config` に対して監査を実行できます。

```
<custom_item>
 type: AUDIT_XML
 description: "Palo Alto Security Settings - 'fips-mode = on'"
info: "Fips-mode should be enabled."
api_request_type: "op"
 request: "<show><fips-mode></fips-mode></show>"
xsl_stmt: "<xsl:template match=\"/\">"
xsl_stmt: "  <xsl:apply-templates select=\"//result\"/>"
xsl_stmt: "</xsl:template>"
xsl_stmt: "<xsl:template match=\"//result\">"
xsl_stmt: "fips-mode: <xsl:value-of select=\"text()\"/>"
 regex: "fips-mode:[\\s\\t]+"
 expect: "fips-mode:[\\s\\t]+on"
</custom_item>
```

IBM iSeries

Nessus は、提供された認証情報を使用して、IBM iSeries を実行しているシステムの構成をテストし、セキュリティ ポリシー基準に沿っているかどうか確認することができます。

```
<custom_item>
 type: AUDIT_SYSTEMVAL
systemvalue: "QALWUSRDMN"
 description: "Allow User Domain Objects (QALWUSRDMN) – '*all'"
value_type: POLICY_TEXT
value_data: "*all"
info: "\nref :
       http://publib.boulder.ibm.com/infocenter/iseries/v5r4/topic/books/sc415302.pdf
       pg. 21"
</custom_item>
```

NetApp Data ONTAP

Nessus は、提供された認証情報を使用して、NetApp Data ONTAP システムを実行しているシステムの構成をテストし、セキュリティ ポリシー基準に沿っているかどうか確認することができます。

```
<custom item>
 type: CONFIG_CHECK
 description: "1.2 Secure Storage Design, Enable Kerberos with NFS –
       'nfs.kerberos.enable = on'"
 info: "NetApp recommends the use of security features in IP storage protocols to
       secure client access"
 solution: "Enable Kerberos with NFS"
 reference: "PCI|2.2.3"
see_also: "http://media.netapp.com/documents/tr-3649.pdf"
 regex: "nfs.kerberos.enable[\\s\\t]+"
 expect: "nfs.kerberos.enable[\\s\\t]+on"
</custom_item>
```

データベース

Nessus は、以下のタイプのデータベースにログインして、ローカル セキュリティ ポリシーのコンプライアンスをチェックすることができます。

- SQL Server
- Oracle
- MySQL
- PostgreSQL
- DB2
- Informix/DRDA

Tenable では通常、データベース コンプライアンス スキャンで完全なレポートを生成するためには、Oracle では SYSDBA 権限を持つユーザーとして、MS-SQL では "**sa**" または sysadmin サーバー ロールのアカウントを持つユーザーとして、そして DB2 では DB2 インスタンス ユーザー アカウントで実行するよう推奨しています。これは、システムや隠しテーブルまたは隠しパラメータの中には、これらの権限を持つアカウントからしかアクセスできないものがあるためです。Oracle については、DBA ロールを割り当てられたユーザーは Tenable 監査のほとんどのチェックを実行できますが、いくつかのチェックではより高度なアクセス権限が必要となるため、エラーが報告されることがあります。これは他のデータベースでも同じで、権限が制限されているアカウントを使ってデータベース監査を実行することはできますが、完全なレポートが生成されない場合があるので注意が必要です。

データベース監査は通常、セキュリティが保護されていないストアド プロシージャの有無やステータスといった、セキュリティ関連の詳細情報をデータベースから取得するための select 文で構成されます。以下は、潜在的な危険性を持つ "**xp_cmdshell**" ストアド プロシージャが有効化されているかどうかを判断するチェック例です。

```
<custom_item>
 type: SQL_POLICY
 description: "xp_cmdshell option"
info: "The xp_cmdshell extended stored procedures allows execution of host executables
       outside the controls of database access permissions and may be exploited by
       malicious users."
 info: "Checking that the xp_cmdshell stored procedure is set to '0'"
sql_request: "select value_in_use from sys.configurations where name = 'xp_cmdshell'"
sql_types: POLICY_INTEGER
sql_expect: "0"
</custom_item>
```

組織固有のニーズに応じて、監査ファイルを記述して機密データを検索することができると非常に便利です。本書では、各種のデータを検索するためのカスタム ポリシーを作成する方法を説明します。

監査レポート

Nessus は、監査を実行した後、ホストがポリシーに準拠しているか、していないか、または確定的でないかを決定します。

Nessus のコンプライアンスの結果は、"Pass"、"Fail"、"Warning" のいずれかでログされます。Nessus ユーザー インタフェースおよび Tenable の SecurityCenter は、合格の場合は "Info"、不合格の場合は "High"、確定的でない場合は "Medium" とログします (システム上に見つからないファイルのパーミッション チェックなど)。

脆弱性が実際に存在するかどうかだけをレポートする脆弱性チェックと異なり、コンプライアンス チェックでは、必ず何らかのデータをレポートします。このデータは、ホストが特定のテストに合格した、不合格だった、または適切にテストできなかったことを示す、監査レポートの基盤として使用できます。

必要なテクノロジ

Unix および Windows 構成コンプライアンスの Nessus プラグイン

Tenable は、Unix および Windows システムに対して監査を実行するための API を実装した Nessus プラグインを 2 つ (ID 21156 および 21157) 開発しました。これらのプラグインは、Nessus "**.nbin**" フォーマットでコンパイル済です。

これらのプラグインおよび対応する監査ポリシーは、有償ユーザーおよび SecurityCenter ユーザーに提供されています。本書では、カスタム Windows **.audit** ファイルの作成を支援するための Windows 用ツール 2 つと、Unix **.audit** ファイルを作成するための Unix 用ツール 1 つについても説明します。

Unix コンプライアンス監査では、SSH 認証のみをサポートしています。セキュリティ上の理由から、telnet などのレガシー プロトコルは許可されていません。

Windows コンテンツ コンプライアンスの Nessus プラグイン

Tenable は、Windows システムの監査を行って PII (個人特定情報) や PHI (保護医療情報).などの非準拠のコンテンツの有無を調べるために使用する API を実装した、"Windows File Contents Check" という名前の Nessus プラグイン (ID 24760) を開発しました。これらのプラグインは、Nessus "**.nbin**" フォーマットでコンパイル済です。これらのプラグインおよび対応する監査ポリシーは、有償ユーザーおよび SecurityCenter ユーザーに提供されています。

Unix システムはプラグイン 24760 ではスキャンされません。

データベース コンプライアンスの Nessus プラグイン

Tenable は、各種データベース システムの監査に使用する API を実装した、"Database Compliance Checks" という名前の Nessus プラグイン (ID 33814) を開発しました。このプラグインは、Nessus "**.nbin**" フォーマットでコンパイル済です。このプラグインおよび対応する監査ポリシーは、有償ユーザーおよび SecurityCenter ユーザーに提供されています。

データベース コンプライアンス チェックは、Security Center バージョン 3.4.3 以前では使用できません。

IBM iSeries コンプライアンスの Nessus プラグイン

Tenable は、IBM iSeries を実行するシステムの監査に使用する API を実装した、"IBM iSeries Compliance Checks" という名前の Nessus プラグイン (ID 57860) を開発しました。このプラグインは、Nessus "**.nbin**" フォーマットでコンパイル済です。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。

iSeries システムに対してコンプライアンス スキャンを正しく実行するには、認証ユーザーが以下の特権を持っていなければなりません。

1. (*ALLOBJ) または監査 (*AUDIT) 権限を持つユーザーは、すべてのシステム値を監査することができます。このようなユーザーは通常、(*SECOFR) クラスに属します。

2. (*USER) または (*SYSOPR) クラスのユーザーはほとんどの値を監査できますが、QAUDCTL、QAUDENDACN、QAUDFRCLVL、QAUDLVL、QAUDLVL2、および QCRTOBJAUD は監査できません。

ユーザーが値にアクセスする権限を持たない場合、*NOTAVL という値が返されます。

Cisco コンプライアンスの Nessus プラグイン

Tenable は、CISCO IOS オペレーティング システムを実行するシステムの監査に使用する API を実装した、"Cisco IOS Compliance Checks" という名前の Nessus プラグイン (ID 46689) を開発しました。このプラグインは、Nessus "**.nbin**" フォー

マットでコンパイル済です。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。このコンプライアンス チェックは、Saved、Running、および Startup の構成に対して実行できます。

Palo Alto コンプライアンスの Nessus プラグイン

Tenable は、Palo Alto デバイスを実行するシステムの監査に使用する API を実装した、"Palo Alto Networks PAN-OS Compliance Checks" という名前の Nessus プラグイン (ID 64095) を開発しました。また、監査を実行するために必要な認証情報を構成するには、"Palo Alto Networks Settings" という名前の Nessus プラグイン (ID 64286) を使用します。これらのプラグインは、Nessus "**.nbin**" フォーマットでコンパイル済です。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。このコンプライアンス チェックは、Operational 構成に対して実行できます。

VMware コンプライアンスの Nessus プラグイン

Tenable は、ESX、ESXi、および vCenter ソフトウェアを監査するための VMware SOAP API を実装した、"VMware vCenter/vSphere Compliance Checks" という名前の Nessus プラグイン (ID 64455) を開発しました。認証情報および関連監査ファイルは、ポリシーの "Credentials" セクションと、ポリシーの "Advanced" セクションにある "VMware vCenter SOAP API Settings" に追加できます。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。VMware に対する監査の実行の詳細については、関連するブログ記事を参照してください。

Citrix XenServer コンプライアンスの Nessus プラグイン

Tenable は、Citrix XenServer およびベンダーがオープン ソース コードに基づいて独自に開発した XenServer を実行するシステムの監査に使用する API を実装した、"Citrix XenServerCompliance Checks" という名前の Nessus プラグイン (ID 69512) を開発しました。認証情報および関連監査ファイルは、ポリシーの "Credentials" セクションと、ポリシーの "Advanced" セクションにある "Citrix XenServer Compliance Checks" プリファレンスに追加できます。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。XenServer に対する監査の実行の詳細については、関連するブログ記事を参照してください。

HP ProCurve コンプライアンスの Nessus プラグイン

Tenable は、HP の ProCurve を実行するシステムの監査に使用する API を実装した、"HP ProCurveCompliance Checks" という名前の Nessus プラグイン (ID 70271) を開発しました。認証情報および関連監査ファイルは、ポリシーの "Credentials" セクションと、ポリシーの "Advanced" セクションにある "HP ProCurve Compliance Checks" プリファレンスに追加できます。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。

FireEye コンプライアンスの Nessus プラグイン

Tenable は、FireEye システムを実行するシステムの監査に使用する API を実装した、"FireEyeCompliance Checks" という名前の Nessus プラグイン (ID 70469) を開発しました。認証情報および関連監査ファイルは、ポリシーの "Credentials" セクションと、ポリシーの "Advanced" セクションにある "FireEye Compliance Checks" プリファレンスに追加できます。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。

Fortigate FortiOS コンプライアンス Nessus プラグイン

Tenable は、FortiOS システムを実行するシステムの監査に使用する API を実装した、"FortigateFortiOS Compliance Checks" という名前の Nessus プラグイン (ID 70272) を開発しました。認証情報および関連監査ファイルは、ポリシーの "Credentials" セクションと、ポリシーの "Advanced" セクションにある "FortigateFortiOS Compliance Checks" プリファレンスに追加できます。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。

Amazon AWS コンプライアンスの機能

Tenable は、Amazon AWS インスタンスの監査を支援するため、Nessus 内に Amazon AWS API を実装しました。監査を実行するには、インスタンスのリージョン、AWS アクセス キー、および AWS シークレットキーを指定します。監査では、特定時点での AWS インフラストラクチャのスナップショットが報告され、これには、実行中のインスタンス、ネットワーク ACL、ファイアウォール構成、アカウント属性、ユーザー リストの作成その他が含まれます。

Dell Force10 コンプライアンスの Nessus プラグイン

Tenable は、Dell Force10 FTOS システムを実行するシステムの監査に使用する API を実装した、"Dell Force10 FTOS Compliance Checks" という名前の Nessus プラグイン (ID 72461) を開発しました。このプラグインは、Nessus "**.nbin**" フォー

マットでコンパイル済です。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。監査では、ポリシーや構成オプションを含む、デバイスに関する各種の情報が報告されます。

Adtran AOS コンプライアンスの Nessus プラグイン

Tenable は、Adtran オペレーティング システム (AOS) を実行するシステムの監査に使用する API を実装した、"Adtran AOS Compliance Checks" という名前の Nessus プラグイン (ID 71991) を開発しました。このプラグインは、Nessus "**.nbin**" フォーマットでコンパイル済です。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。監査では、ポリシーや構成オプションを含む、デバイスに関する各種の情報が報告されます。

SonicWALL SonicOS コンプライアンスの Nessus プラグイン

Tenable は、SonicWALL SonicOS を実行するシステムの監査に使用する API を実装した、"SonicWALL SonicOS Compliance Checks" という名前の Nessus プラグイン (ID 71955) を開発しました。このプラグインは、Nessus "**.nbin**" フォーマットでコンパイル済です。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。監査では、ポリシーや構成オプションを含む、デバイスに関する各種の情報が報告されます。

Extreme ExtremeXOS コンプライアンスの Nessus プラグイン

Tenable は、ExtremeExtremeXOS を実行するシステムの監査に使用する API を実装した、"Extreme ExtremeXOS Compliance Checks" という名前の Nessus プラグイン (ID 73156) を開発しました。このプラグインは、Nessus "**.nbin**" フォーマットでコンパイル済です。このプラグインおよび対応する監査ポリシーは、有償ユーザーに提供されています。監査では、ポリシーや構成オプションを含む、デバイスに関する各種の情報が報告されます。

監査ポリシー

Tenable は、Unix、Windows、Palo Alto、IBM iSeries、VMware、および Cisco プラットフォーム用に、多種の監査ポリシーを開発してきました。これらは、**.audit** テキスト ファイルとして有償サブスクリプション ユーザーに提供されており、Tenable サポート ポータル (https://support.tenable.com/) からダウンロードできます。Tenable の監査機能に関する最新情報と、すべての最新 **.audit** ファイル リリースについては、ディスカッション フォーラム (https://discussions.nessus.org/) を参照してください。

これらの監査ポリシーは、開発に際して、SOX、FISMA、PCI DSS の要件といった一般的なコンプライアンス監査を考慮しましたが、これらの要件を満たす公式な監査ファイルではありません。ご利用の際は、これらの **.audit** ポリシーを確認し、ローカルの環境に合わせてチェックをカスタマイズしてください。必要に応じて **.audit** ファイルの名前を変更しても構いません。その他の **.audit** ポリシーは、CERT、CIS、NSA、および NIST による推奨構成設定に直接基づいています。

Tenable では、ユーザー フィードバックおよび進化を続ける "ベスト プラクティス" に基づいて、いくつかの **.audit** ファイルを開発する予定です。また、コンサルティング企業や Tenable のユーザーも独自の **.audit** ポリシーを実装しており、他の Nessus の有償ユーザーと共有することについて積極的な考えをお持ちです。**.audit** ポリシーを共有したり Nessus コミュニティと交流したりするのに最も簡単な方法は、Tenable Network Security ディスカッション フォーラム (https://discussions.nessus.org/) をご利用いただくことです。

有用なユーティリティ

Tenable は、Windows の監査を実行するため、**.inf** ファイルを Nessus の **.audit** ファイルに変換するツールを開発しました。このツールは **i2a** と呼ばれ、本書の後のセクションで詳しく説明します。

Unix **.audit** ファイルの作成に使用できるルーツは 2 つあります。ひとつは **c2a** ("configuration to audit") と呼ばれるもので、既存の構成ファイルから直接 Unix **.audit** ファイルを作成するために使用します。たとえば、Sendmail 構成ファイルがサイトのポリシーに従って正しく構成されている場合、**c2a** ツールを使用すれば、ファイルの MD5 チェックサムに基づいて、または **sendmail.cf** ファイルの特定の値と引数の組み合わせに基づいて、監査ポリシーを作成することができます。もうひとつは **p2a** ("package to audit") と呼ばれるもので、Unix (RPM-based Linux or Solaris 10) システム上に設定されたベース パッケージから、またはパッケージ名のリストが記載されたフラット テキスト ファイルから、Unix **.audit** ファイルを作成することができます。

Unix または Windows の Nessus スキャナ

コンプライアンス チェックはさまざまなプラットフォームから実行でき、通常は Nessus が常駐しているオペレーティング システムの違いは影響しません。OS X ラップトップから Windows 2003 サーバーのコンプライアンス監査を実行したり、Windows ラップトップから Solaris サーバーを監査したりすることができます。

監査するデバイスの認証情報

Nessus がターゲット サーバーにログインするには、どのような場合でも、Unix SSH、Windows Domain、IBM iSeries、Cisco IOS、またはデータベース認証が必要です。ほとんどの場合、ユーザーは "スーパー ユーザー" であるか、そうでない場合は権限昇格能力 (`sudo`、`su` または `su+sudo`) を持っている必要があります。監査を実行するユーザーが "スーパー ユーザー" 特権を持っていない場合、リモート システム コマンドの多くは、実行できないか、または正しくない結果を返します。

サインオン認証情報に使用する Windows アカウントは、ローカル マシンのポリシーを読み取るパーミッションを持っている必要があります。ターゲット ホストが Windows ドメインに参加しない場合は、アカウントがホストの管理者グループのメンバーである必要があります。ホストがドメインに参加する場合、ドメインの管理者グループはホストの管理者グループのメンバーとなり、ドメインの管理者グループのメンバーであるアカウントは、ローカル マシン ポリシーにアクセス権を持っています。

Windows コンテンツ コンプライアンス チェックを実行するには、ドメイン特権を使用してシステムにログインすることに加え、WMI (Windows Management Instrumentation) へのアクセス権も持っている必要があります。このアクセス権がないと、Nessus は、スキャン時に WMI アクセスがなかったことを報告します。

データベース コンプライアンス チェックでは、完全なデータベース コンプライアンス監査を実行するにあたり、データベース認証のみが必要となります。これは、コンプライアンスのスキャン対象が、ホストのオペレーティング システムでなくデータベースのみであるためです。

Cisco IOS コンプライアンス チェックでは通常、システム構成の完全なコンプライアンス監査を実行するには "enable" パスワードが必要です。これは、Nessus が、特権を持つユーザーのみに提供される "`show config`" コマンドの出力を監査するためです。監査に使用する Nessus ユーザーがすでに "enable" 特権を持っている場合は、"enable" パスワードは必要ありません。

ローカル認証の脆弱性チェックを実行するための Nessus または SecurityCenter の構成方法については、「Unix と Windows での Nessus 認証チェック」 (http://www.tenable.com/products/nessus/documentation) を参照してください。

監査での "su"、"sudo"、および "su+sudo" の使用

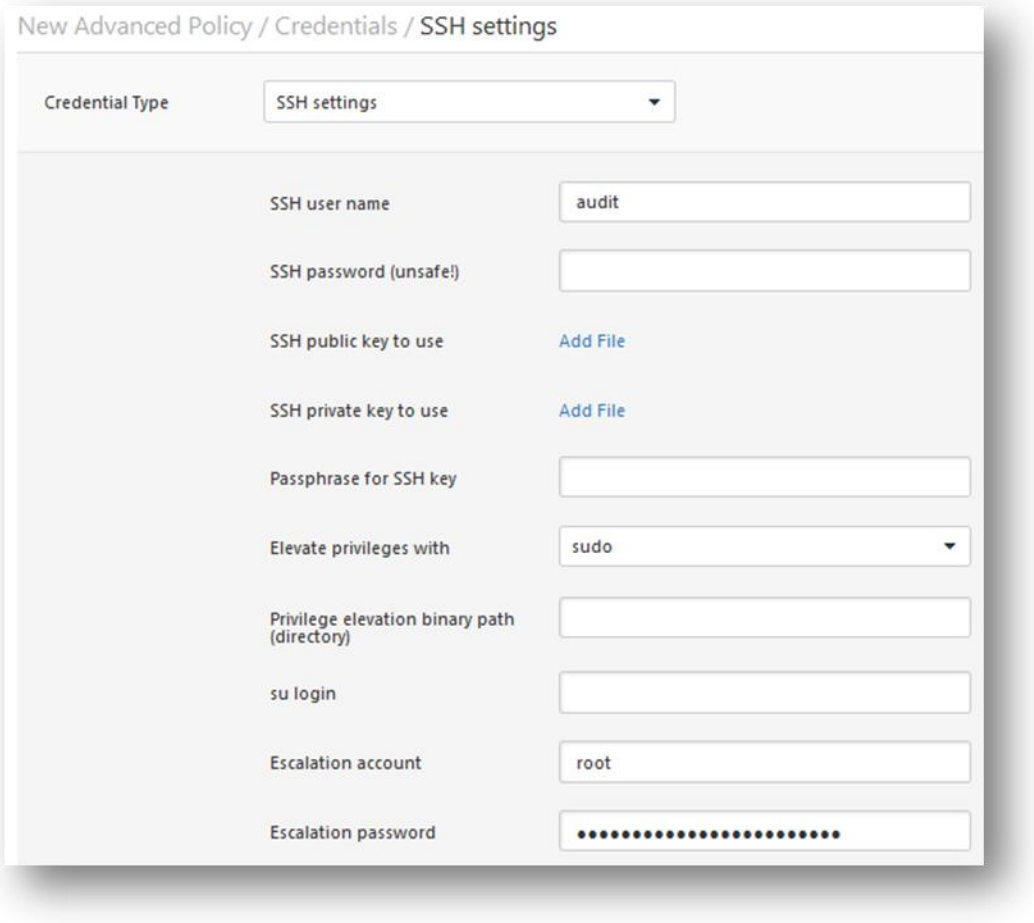
企業のポリシーによって、Nessus がルート ユーザーまたは "`sudo`" 特権を持つユーザーとしてリモート ホストにログインすることが禁じられている場合は、"`su+sudo`" を使用します。リモート ログインでは、特権のない Nessus ユーザーは "`su`" (switch user) を使用して `sudo` 特権に変更することができます。

最も効果的な Unix 認証スキャンは、供給された認証情報が "root" 特権を持つ場合の認証スキャンです。多くのサイトでは root でのリモート ログインが許可されていないため、Nessus ユーザーは、別のパスワードを使用して "`su`"、"`sudo`"、または "`su+sudo`" を呼び出し、適切な特権を持つように設定されているアカウントに変更できるようになりました。

また、SSH `known_hosts` ファイルが利用可能で、スキャン ポリシーの一部として提供されている場合、Nessus は、このファイル内のホストにのみログインを試みます。これにより、既知の SSH サーバーを監査するために使用しているユーザー名とパスワードが、管理下にないシステムへのログインに使用されることを確実に防止できます。

sudo 例

SSH キーと共に "**sudo**" を使用する場合のスクリーン キャプチャを以下に示します。この例では、ユーザー アカウントは "audit" で、スキャンするシステム内の **/etc/sudoers** ファイルに追加されています。入力されているパスワードは "audit" アカウントのパスワードであり、root パスワードではありません。SSH キーは "audit" アカウント用に生成されたキーと一致します。

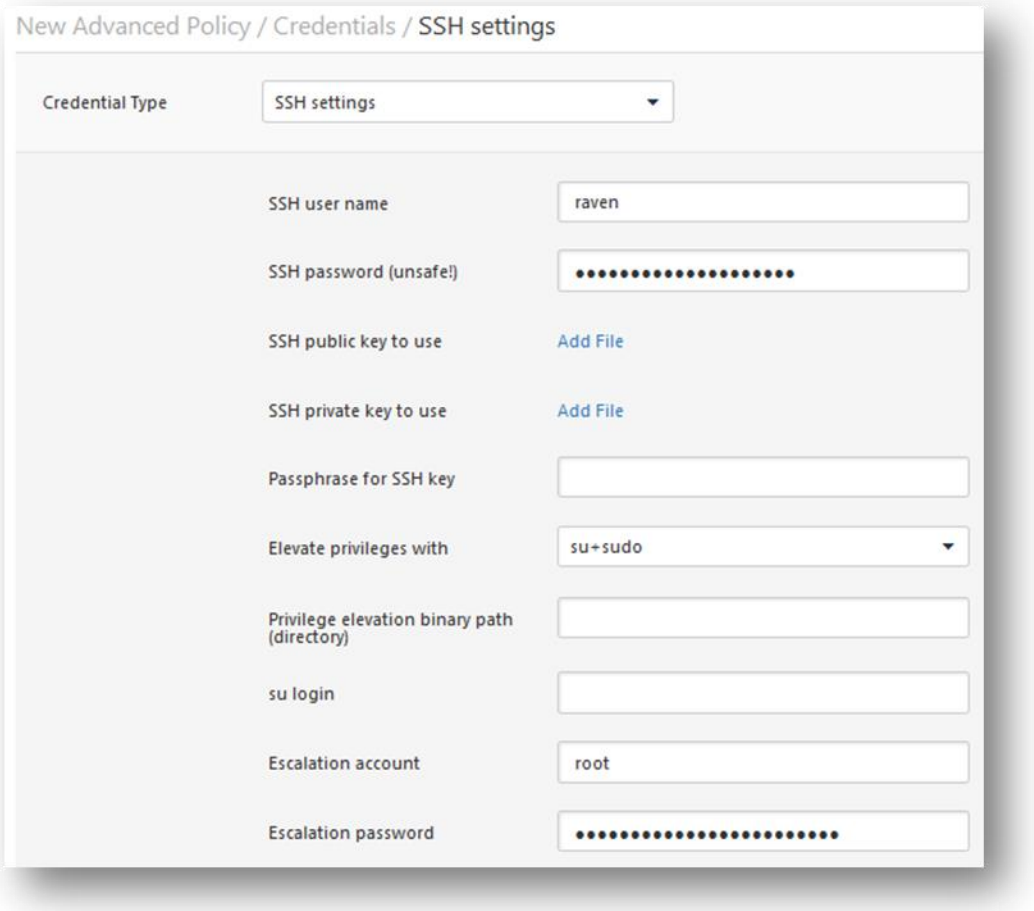


su+sudo 例

Nessus 4.2.2 リリースには、**sudo** がインストールされている Unix ベースのホスト用の新しい認証昇格方法である "**su+sudo**" が含まれています。この方法を使用すると、**sudo** パーミッションを持たないアカウントに認証情報を提供し、パーミッションを持つユーザー アカウントに **su** を使用して変更し、**sudo** コマンドを実行することができます。

この構成を使用することで、スキャン中の認証情報のセキュリティをより確実に維持でき、多くの組織のコンプライアンス要件を満たすことができます。

この機能を有効化するには、以下のスクリーン キャプチャに示すように、credentials/SSH settings にある "Elevate privileges with" (特権昇格) セクションで "su+sudo" を選択します。



"SSH user name" および "SSH password" フィールドに、**sudo** 特権を持たない認証情報を入力します。上の例では、ユーザーアカウントは "raven" です。"Elevate privileges with" (特権昇格) プルダウン メニューで、"su+sudo" を選択します。"su login"(su ログイン) および "Escalation password" (昇格パスワード) フィールドに、特権認証情報を持つユーザー名とパスワードを入力します (この例では "sumi")。必要なスキャン ポリシーの変更はこれだけです。

sudo に関する注意

su、**sudo**、または **su+sudo** を使用して Unix システムを監査する際は、以下の事柄に注意してください。

- Unix システムが、**sudo** またはリモート ユーザーによってアクセスされるファイルを通じて実行できるコマンドを制限するよう強化されている場合、監査に影響が及ぼされることがあります。セキュリティ設定によって監査が制限されていると考えられる場合は、非ルート監査とルート監査を比較してください。

- **sudo** コマンドは Solaris のネイティブ コマンドではないため、ターゲット システムが Solaris を実行している場合は、このコマンドをダウンロードしてインストールする必要があります。**sudo** バイナリが "**/usr/bin/sudo**" としてアクセス可能であることを確認してください。

- **known_hosts** を使用してスキャンする場合でも、Nessus のスキャンでは、スキャン対象のホストを指定する必要があります。たとえばクラス C をスキャンした場合で、そのクラス C 内の 20 の個別ホストのみを含む **known_hosts** ファイルをアップロードした場合、Nessus はファイル内にあるホストのみをスキャンします。

- Unix ベースの構成の中には、sudo で開始したコマンドは **tty** セッションから実行するという要件が設定されている場合があります。"**su+sudo**" オプションで実行した Nessus の脆弱性スキャンは、この要件を満たしません。"**su+sudo**" オプションを使用する場合は、ターゲット システム上で例外を作成する必要があります。お使いの Unix ディストリビューションがこれに当てはまるかどうか判断するには、スキャンするシステムで root として以下のコマンドを入力してください。

  ```
  # greprequiretty `locate sudoers` | grep -v "#" | grep /etc
  ```

  sudoers 構成ファイル内に "**requiretty**" 行がある場合は、以下のようにして、**/etc/sudoers** ファイルにこのルールの例外を作成する必要があります。

  ```
  Defaults    requiretty
  Defaults:{userid} !requiretty
  ```

  {userid} は、"**sudo**" コマンドの実行に使用するユーザー名です (ポリシーの credentials/SSH セクションの "su login" ページ)。また、**sudoers** ファイルに以下の行があることを確認してください。

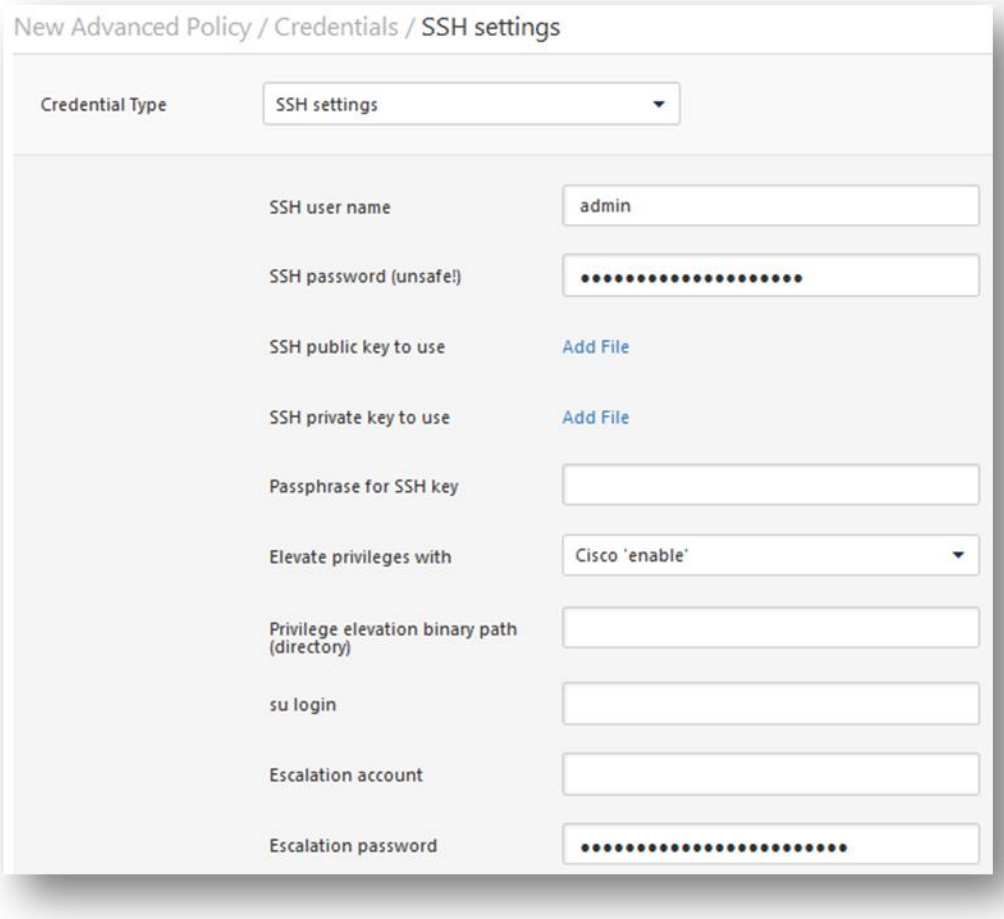
  ```
  {userid}      ALL=(ALL)       ALL
  ```

  ここでも、{userid} は、"**sudo**" コマンドの実行に使用するユーザー名です (ポリシーの credentials/SSH セクションの "su login" ページ)。

Cisco IOS 例:

SSH 認証のみがサポートされます。認証に telnet を必要とするレガシー IOS デバイスは、Nessus Cisco コンプライアンス チェックではスキャンできません。

Cisco IOS 認証情報は、Nessus ユーザー インタフェースの "**SSH settings**" 認証画面で構成します。Cisco ルータへのログインに必要な SSH ユーザー名とパスワードを入力してください。"enable" を使用して特権を昇格する必要があることを指定するには、"**Elevate privileges with**" (特権昇格) 設定の横にある "**Cisco 'enable'**" を選択し、"**Escalation password**" (昇格パスワード) の横に enable パスワードを入力します。



i2a を使用した Windows .inf ファイルから .audit ファイルへの変換

企業または企業の IT 組織が Windows ポリシー ファイル (通常は "`.inf`" 拡張子付き) を所有している場合は、`.audit` ファイルに変換して、Nessus による Windows サーバーの監査に使用することができます。

ツールの取得とインストール

`i2a` ツールは zip ファイルとして提供されており、Tenable サポート ポータル (https://support.tenable.com/) から入手できます。このツールには GUI インタフェースがありません。コマンド ツールから実行してください。

ファイルを任意のディレクトリに解凍し、Windows `.inf` ファイルを同じディレクトリに移動します。

.inf から .audit への変換

変換ツールを実行するには、コマンド プロンプトで以下のように入力します。

```
# i2a-x.x.x.exe yourfile.inf file.audit
```

この例で、`yourfile.inf` は変換元の `.inf` ファイルで、`file.audit` は変換先の `.audit` ファイルです。

変換の分析

Tenable では、**.inf** ファイルの内容をすべて **.audit** ファイルに変換して監査に使用できるよう努めましたが、現在の Nessus 5 テクノロジではテストできないポリシー項目がいくつかあります。

i2a ツールを実行するたびに、変換プロセスのログが作成され、行ごとの変換プロセスの監査内容がすべて記載されます。**.inf** 内の行が変換できなかった場合、このログファイルに記載されます。

正しい .inf 設定フォーマット

処理できなかったとしてログ ファイルに表示されるチェックについては、以下にリストする正しいフォーマットに準拠していることを確認してください。

System Access、**System Log**、**Security Log**、**Application Log**、および **Event Audit** 設定は同じフォーマットです。各エントリは "**Key**" の後に "**value**" という順序で記述されます。

シンタックス:

```
Key = value
```

この場合、**Key** は監査対象の項目で、**value** はリモート システム上でそのキーに対して期待する値です。

例:

```
MinimumPasswordLength = 8
```

Privilege Rights 設定のフォーマットは上述のものと似ていますが、この設定では値は空でも構いません。

シンタックス:

```
PriviledgeRight = User1,User2…UserN
```

例:

```
SeNetworkLogonRight = *S-1-5-32-545,*S-1-5-32-544
```

または:

```
SeTcbPrivilege =
```

Registry Key 設定は以下の 4 つの部分で構成されます。

- Registry Key – 監査対象のレジストリ キー。
- Inheritance Value – このレジストリキーのパーミッションが継承されるかどうかを識別します。値は [0-4] です。
- DACL – DACL は ACL の一種であり、オブジェクトの所有者によって制御され、特定のユーザーまたはグループがそのオブジェクトに対して持つことができるアクセス権を指定します。
- SACL – SACL は ACL の一種で、セキュリティ保護できるオブジェクトへのアクセス試行に関する監査メッセージの生成を制御します。

シンタックス:

```
"Registry Key",Inheritance value,
"D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)... (string_acen)"
```

DACL および SACL フィールドは空でも構いません。その場合はチェックが無視されます。

例:

```
"MACHINE\SYSTEM\CurrentControlSet\Control\Class",0,"D:PAR(A;CI;KA;;;BA)(A;CIIO;KA;;;CO)
      S:PAR(AU;OICIFA;CC;;;WD)"
```

File Security 設定のフォーマットは、前述のレジストリ キーのフォーマットに似ています。

シンタックス:

```
"File Object",Inheritance value,
      "D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)...
      (string_acen)"
```

例:

```
"%SystemRoot%\system32\ciadv.msc",2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;FA;;;SY)S:PAR(AU;OICI
      FA;CC;;;WD)"
```

Service General 設定は以下の 4 つの部分で構成されます。

- Service Name – 監査対象のサービス。
- Service start type – Manual、Automatic、または Disabled。値は [2-4] です。
- DACL – DACL は ACL の一種であり、オブジェクトの所有者によって制御され、特定のユーザーまたはグループがそのオブジェクトに対して持つことができるアクセス権を指定します。
- SACL – SACL は ACL の一種で、セキュリティ保護できるオブジェクトへのアクセス試行に関する監査メッセージの生成を制御します。

シンタックス:

```
Service Name,Start type,
      "D:dacl_flags(string_ace1)...(string_acen)S:sacl_flags(string_ace1)...(string_a
      cen)"
```

例:

```
kdc,3,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;AU)(A;;CCLCSWRPWPDTLO
      CRRC;;;SY)"
```

サービス設定のパーミッションをチェックする必要がなく、startup type のみを監査する必要がある場合は、以下のようにします。

シンタックス:

```
Service Name,Start type
```

例:

```
kdc,3,""
```

Registry Value 設定は以下の 3 つの部分で構成されます。

- Registry Key – 監査対象のレジストリ キー。
- RegistryType – レジストリのタイプ (REG_DWORD、REG_SZ など)。
- RegistryValue – レジストリキーの値。

RegistryValue は、引用符付き、二重引用符付き、または引用符なしで定義できます。

シンタックス:

```
RegistryKey,RegistryType,RegistryValue
```

例:

```
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0
```

.inf ファイル内で特定の行をコメントアウトするには、行の先頭にセミコロン ";" を付けると、スクリプトがその行を無視します。

c2a を使用した Unix .inf ファイルから .audit ファイルへの変換

c2a.pl ツールは、特定のネットワーク上でアプリケーション構成を監査するための **.audit** ファイルの作成を支援することを目的として設計されました。たとえば、特定のネットワーク上のすべての Web サーバーをマスター ホスト X と完全に同じように構成しなければならない場合、このツールをホスト X 上で実行してそのシステムの **httpd** 上に **.audit** ファイルを作成し、そのファイルを Nessus デーモンに入力して他のすべての Web サーバーに対してスキャンを実行し、コンプライアンスをチェックします。

オプションで、このツールを使用して、ホスト全体用に MD5 監査ファイルを作成することもできます。この場合、入力ファイルに、監査対象のすべてのファイルとディレクトリを含むリストが記載されている必要があります。その後、ディレクトリの場合は反復して処理が行われ、システム全体の **.audit** ファイルが作成されます。このファイルはその後、中心的なファイルとディレクトリの変更に対するスキャンに使用されます。

ツールの取得とインストール

c2a ツールは圧縮 **tar** アーカイブとして提供されており、Tenable サポート ポータル (https://support.tenable.com/) から入手できます。

以下のコマンドを実行して、**c2a-x.x.x.tar.gz** の内容をローカル マシンに解凍します。

```
# tar xzf c2a-x.x.x.tar.gz
```

これにより、現在のディレクトリの下に "c2a" ディレクトリが作成され、その中にファイルが抽出されます。別のディレクトリに抽出したい場合は、以下のコマンドを実行します。

```
# tar xzf c2a.x.x.x.tar.gz -C /path/to/directory
```

アーカイブを解凍すると、~/c2a ディレクトリに以下のファイルが置かれます。

- c2a.pl
- c2a.map
- c2a_regex.map
- cmv.pl
- ReadMe.txt

MD5 監査ファイルの作成

以下のように入力して、変換ツールを "-md5" オプション付きで実行します。

```
# ./c2a.pl -md5 -f /path/to/inputfile.txt -o outputfile.audit
```

このツールで使用する入力ファイルには、MD5 値の監査対象とするファイルおよびディレクトリのリストと、監査ファイル用の出力ファイル名が記載されている必要があります。

入力ファイルにファイルを追加する際は、以下のフォーマットを使用してください。

`/path/to/file`

ディレクトリを追加する際は以下のフォーマットを使用してください。

`/path/to/file/`

このフォーマットを使用した場合で、ファイルがディレクトリでなく実際のファイルであった場合、`c2a` ツールは、ファイルが存在していないというエラーを返します。スラッシュ "/" は、ディレクトリを追加する場合には問題ありません。

入力ファイル内のエントリが通常の MD5 ファイルであった場合、そのファイルのみが考慮され、.audit フォーマットに書き込まれます。ディレクトリの場合、スクリプトは、そのディレクトリ内の各ファイルに対して反復調査を行います。出力ファイルが指定されていない場合、結果は ~/c2a/op.audit に書き込まれます。

"inputfile" で指定したファイルのリストを処理する際、シンボリック リンクが出現するとすべて無視されます。その場合、ファイルが存在しないか、またはシンボリック リンクであることを示す警告メッセージが表示されます。現在のバージョンでは、c2a はシンボリック リンクをサポートしていません。

構成ファイルに基づく監査ファイルの作成

c2a ツールは、行ごとに個別のコンテンツが記載された構成ファイルの処理に適しています。XML 構成ファイルのように、複数行で表す機能が記載された構成ファイルの処理には c2a は適していません。

以下のように入力して、変換ツールを "-audit" オプション付きで実行します。

```
# ./c2a.pl -audit -f /path/to/input.txt -o outputfile.audit
```

このツールで使用する入力ファイル (input.txt) には、監査対象とする構成ファイルのリストと監査ファイル用の出力ファイル名を記載する必要があります。

c2a.pl Perl スクリプトは、**c2a.map** および **c2a_regex.map** の 2 つのキー ファイルを使用します。スクリプトは監査対象の構成ファイルの各行をスキャンし、各行の最初の語が **c2a.map** ファイルの "type" (HTTP、SENDMAIL など) とそれに関連付けられた値に一致するかどうかを調べます。たとえば HTTP 設定を監査する場合は、その語が **c2a.map** ファイル内の HTTP キーワードに一致するかどうかを調べます。一致する場合は、**c2a_regex.map** の HTTP の正規表現をその行に適用し、設定と値を抽出します。**c2a.map** に対応するエントリが存在する設定のみが監査されます。

監査対象としない構成ファイルは、"#" 文字を使ってコメントアウトすることができます。

構成ファイルでコメントアウトした設定を **.audit** フォーマットに変換する場合は、**c2a.pl** を編集して "$ENFORCE_COMMENT = 1;" を設定してください。

先の例と同様、出力ファイルが指定されていない場合、結果は **~/c2a/op.audit** に書き込まれます。

Tenable は現時点で、HTTP、SENDMAIL、SYSCTL、および NESSUS の MAP 設定を提供しています。追加のアプリケーション設定は、**cmv.pl** Perl スクリプトを利用して簡単に追加できます。詳細については、次のセクションを参照してください。

MAP ファイルの作成

アプリケーションの MAP ファイルは簡単に作成できます。以下のように **cmv.pl** スクリプトを実行するだけです。

```
# ./cmv.pl -r 'regex' -r tag -f config_file
```

各項目の内容は以下のとおりです。

- "**regex**" は、構成設定と値のペアを抽出する正規表現です。通常は "<name> = <value>" の形式ですが、"=" の代わりにスペースやタブが使われるなど、多少異なる場合があります。
- "**tag**" は、監査対象のアプリケーションをタグするキーワードです。**tag** キーワードは、**config_file** を **c2a.map** 内のキーワードと **c2a_regex.map** 内の正規表現に関連付ける働きを持つため、これらの各ファイル内のタグが同一である必要があります。
- "**config_file**" は、MAP ファイルの作成対象とするファイルです。

たとえば、VSFTPD の構成設定を監査する場合は、以下の手順を実行します。

1. まず、以下のように **cmv.pl** を実行します。

   ```
   # ./cmv.pl -r '([A-Za-z0-9_]+)=([A-Za-z0-9]+)' -t VSFTPD -f /root/vsftpd-0.9.2/vsftpd.conf
   ```

   これにより、**tag.map** ファイル (**VSFTPD.map** など) が作成されます。デフォルトでは、コメントアウトされた行はすべて無視されます。すべての変数を対象とするには、**$ENFORCE_COMMENT** の値を "0" から "1" に変更してスクリプトを再度実行します。

2. MAP ファイルを検査して **c2a.map** に追加します。

   VSFTPD.map ファイルをチェックして、意図せず正規表現に合致してしまっている不要な値がないかどうか調べます。すべてのキーワードが正しいことを確認した後、**c2a.map** に追加します。

3. 以下のようにして、**c2a_regex.map** を、**cmv.pl** で使用されているのと同じ式を使用して更新します。

   ```
   VSFTPD=([A-Za-z0-9_]+)=([A-Za-z0-9]+)
   ```

   注:これは、**cmv.pl** Perl スクリプトで使用されているのと同じ正規表現です。

4. **input.txt** を、VSFTPD 構成ファイルの場所を使用して更新します。

   ```
   VSFTPD=/root/vsftpd-0.9.2/vsftpd.conf
   ```

5. **c2a.pl** スクリプトを実行します。

   ```
   # ./c2a.pl -audit -f input.txt
   ```

6. 最後に、出力ファイルを確認します。

   ```
   # viop.audit
   ```

c2a ツールのその他の使用

Tenable は、Sendmail、Very Secure FTP Daemon (VSFTPD)、Apache、Red Hat **/etc/sysctl.conf** ファイルおよび Nessus の監査を有効化するため、**c2a.map** および **c2a_regex.map** ファイルにいくつかのエントリを含めました。また、近いうちにソフトウェアを追加する予定です。他の Nessus ユーザーと共有するために新しいマッピングを Tenable に送信される場合は、nessus-support@tenable.com 宛てにお送りください。

この点を考慮した上で、**c2a.pl** スクリプトを利用して、ライブ Unix アプリケーション用に Nessus **.audit** ファイルを作成することができます。以下の状況を考えます。

- 多数の Unix ベースのファイアウォールを使用している場合、各ファイアウォールに設定されているべき一般的かつ必須の設定を監査するために、**.audit** ファイルを生成することができます。たとえば、すべてのファイアウォールで RFC 1918 アドレスのフィルタリングが必要とされる場合、実際のファイアウォール ルールをテストすることができます。
- 多種のカスタム アプリケーションが CRON から実行されている場合、各種 CRONTAB を監査して、適切なアプリケーションが適切なときに実行されていることを確認することができます。
- ログの集中管理を行っている場合、リモートの Unix システムでは、SYSLOG、SYSLOG-NG、および LOGROTATE 構成をチェックすることができます。

.audit ファイルの手動調整

最後に、**c2a.pl** スクリプトの出力も手動で編集することができます。たとえば、MD5 チェックサム ルールと FILE_CONTENT_CHECK ルールをひとつのルールに統合するとします。**c2a.pl** スクリプトによって生成される出力も、構成ファイルが常にひとつの場所にあるとみなします。この場合、"**file**" キーワードを編集して、構成ファイルが置かれる別の場所を指定することを検討してください。

リモート ファイル構成に含めたくないコンテンツがある場合は、FILE_CONTENT_CHECK_NOT キーワードを使用して、それらのためのチェックを手動で追加することを検討してください。これにより、存在すべき設定と存在すべきでない設定の両方に対して監査を実行できます。

p2a を使用した、Unix パッケージ リストから .audit への変換

p2a.pl ツールは、RPM ベースの Linux および Solaris 10 システムのインストール パッケージ構成用の **.audit** ファイル設計を支援することを目的として設計されています。たとえば、特定のネットワーク上のすべての Linux Web サーバーがマスター ホスト X として同じ RPM ベースを使用することが望ましい場合、ホスト X 上でこのツールを使用すると、そのシステム上のすべての RPM パッケージを含む **.audit** ファイルが作成されます。その後 Nessus でこの **.audit** ファイルを使用して他の Web サーバーに対してスキャンを実行し、コンプライアンスをチェックすることができます。

オプションで、このツールを使用して、RPM または Solaris 10 パッケージをリストしたテキストから監査ファイルを作成することもできます。この場合は、入力ファイルの内容として、パッケージを 1 行に 1 つずつ記載したリストが必要となり、またターゲット システム用に **.audit** を適切なフォーマットにする必要があります。生成された **.audit** ファイルはその後、中心的なインストール パッケージの変更に対するスキャンに使用されます。

ツールの取得とインストール

p2a ツールは圧縮 **tar** アーカイブとして提供されており、単一の Perl スクリプトと **ReadMe.txt** ヘルプ ファイルで構成されています。Tenable サポート ポータル (https://support.tenable.com/) から入手できます。

以下のコマンドを実行して、**p2a-x.x.x.tar.gz** の内容をローカル マシンに解凍します。

```
# tar xzf p2a-x.x.x.tar.gz
```

これにより、現在のディレクトリの下に "**p2a**" ディレクトリが作成され、その中にファイルが抽出されます。

別のディレクトリに抽出したい場合は、以下のコマンドを実行します。

```
# tar xzf p2a.x.x.x.tar.gz -C /path/to/directory
```

アーカイブを解凍すると、**~/p2a** ディレクトリに以下のファイルが置かれます。

- **p2a.pl**
- **ReadMe.txt**

以下を実行して、スクリプトを実行可能にします。

```
# chmod 750 p2a.pl
```

使用法

以下のように Perl スクリプトを実行します。

```
# ./p2a.pl [-h] -i inputfile.txt -o outputfile.audit
```

スタンドアロンの引数 "**-h**" はオプションです。ヘルプ ツールを表示します。

すべてのインストール パッケージに基づいた出力ファイルの作成

スクリプトに "**-o**" オプションだけを付けて実行した場合は、ローカルにインストールされたすべてのシステム パッケージ名を抽出するシステム コマンドが実行され、その結果得られた **.audit** ファイルは **/path/to/outputfile.audit** に書き込まれます。

```
# ./p2a.pl -o /path/to/outputfile.audit
```

スクリプトを実行するには、出力ファイルに **.audit** 拡張子が付いている必要があります。そうでないと、ファイル拡張子が正しくないというエラーが表示されます。

パッケージ リストに基づく出力ファイルの作成と、画面への送信

すべての出力をターミナル ウィンドウに送信するには、**p2a** を以下のシンタックスで実行します。

```
# ./p2a.pl -i /path/to/inputfile.txt
```

このオプションでは入力ファイルが必要となります。また、ターミナル ウィンドウに出力された内容 (**stdout**) は、コピーして、**.audit** ファイルに貼り付けることができます。入力ファイルのフォーマットは、1 行に 1 パッケージで、区切り文字は付けません。

例:

```
mktemp-1.5-23.2.2
libattr-2.4.32-1.1
libIDL-0.8.7-1.fc6
pcsc-lite-libs-1.3.1-7
zip-2.31-1.2.2
```

多くの Unix ベースのシステムではインストール パッケージを 1,000 個以上維持できるため、出力結果がスクロール バッファを超える大きさになり、出力全体を見ることが難しい場合があります。

指定した入力ファイルに基づく監査ファイルの作成

p2a に入力と出力の両方の引数を付けて実行すると、フォーマットされたパッケージ リストを使用して、指定した場所に **.audit** ファイルが生成されます。

```
# ./p2a.pl -i /path/to/input_file.txt -o /path/to/outputfile.audit
```

入力ファイルのフォーマットは、1 行に 1 パッケージで、区切り文字は付けません。

例:

```
mktemp-1.5-23.2.2
libattr-2.4.32-1.1
libIDL-0.8.7-1.fc6
pcsc-lite-libs-1.3.1-7
zip-2.31-1.2.2
```

スクリプトを実行するには、出力ファイルに **.audit** 拡張子が付いている必要があります。そうでないと、ファイル拡張子が正しくないというエラーが表示されます。

Nessus ユーザー インタフェース使用例

コンプライアンス チェックの取得

有償ユーザーはすでに Nessus スキャナ用のコンプライアンス チェックをお持ちですし、また複数の **.audit** ファイルが Tenable サポート ポータル (https://support.tenable.com/) で提供されています。これを確認するには、Nessus ユーザー インタフェースを実行し、認証して、既存のポリシーを管理または編集します。"Plugins" タブで "Policy Compliance" ファミリーを見つけ、プラグイン ファミリー名をクリックして、以下のプラグインが表示されることを確認してください。

- Cisco IOS Compliance Checks
- Database Compliance Checks
- IBM iSeries Compliance Checks
- PCI DSS Compliance
- PCI DSS Compliance: Database Reachable from the Internet
- PCI DSS Compliance: Handling False Positives
- PCI DSS Compliance: Insecure Communication Has Been Detected
- PCI DSS Compliance: Remote Access Software Has Been Detected
- PCI DSS Compliance: Passed
- PCI DSS Compliance: Tests Requirements
- Unix Compliance Checks
- Windows Compliance Checks
- Windows File Contents Compliance Checks

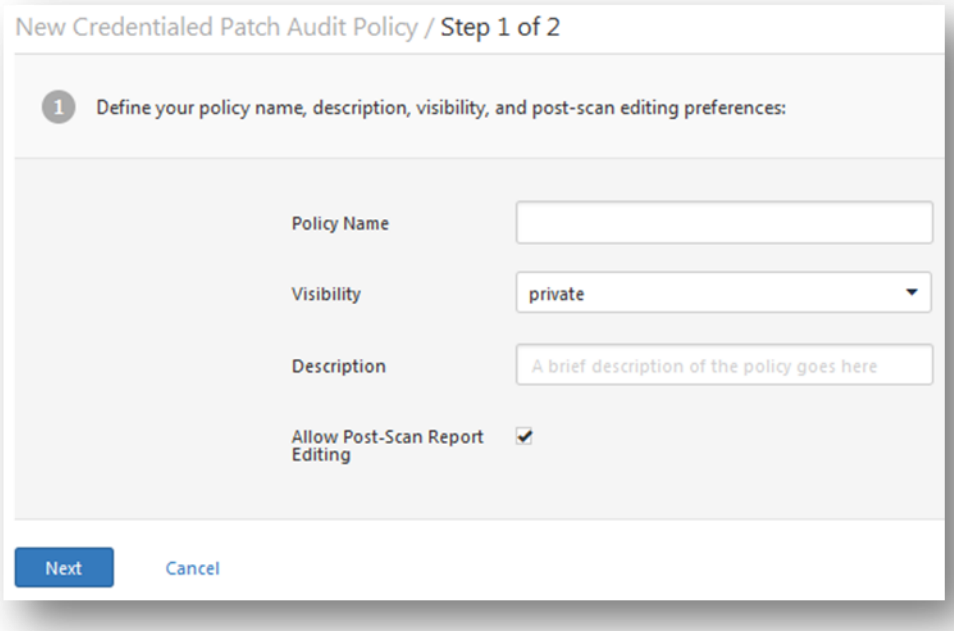
スキャン ポリシーの構成

Nessus でコンプライアンス チェックを有効化するには、以下の属性を使用してスキャン ポリシーを作成する必要があります。

- "Policy Compliance" プラグイン ファミリーにあるコンプライアンス チェック プラグインを有効化します。
- プリファレンスとして、1 つ以上の `.audit` コンプライアンス ポリシーを指定します。
- ターゲット サーバーにアクセスするための認証情報を指定します。該当する場合は、"Preferences" タブのデータベース認証も含みます。
- プラグインの依存関係を有効にします。

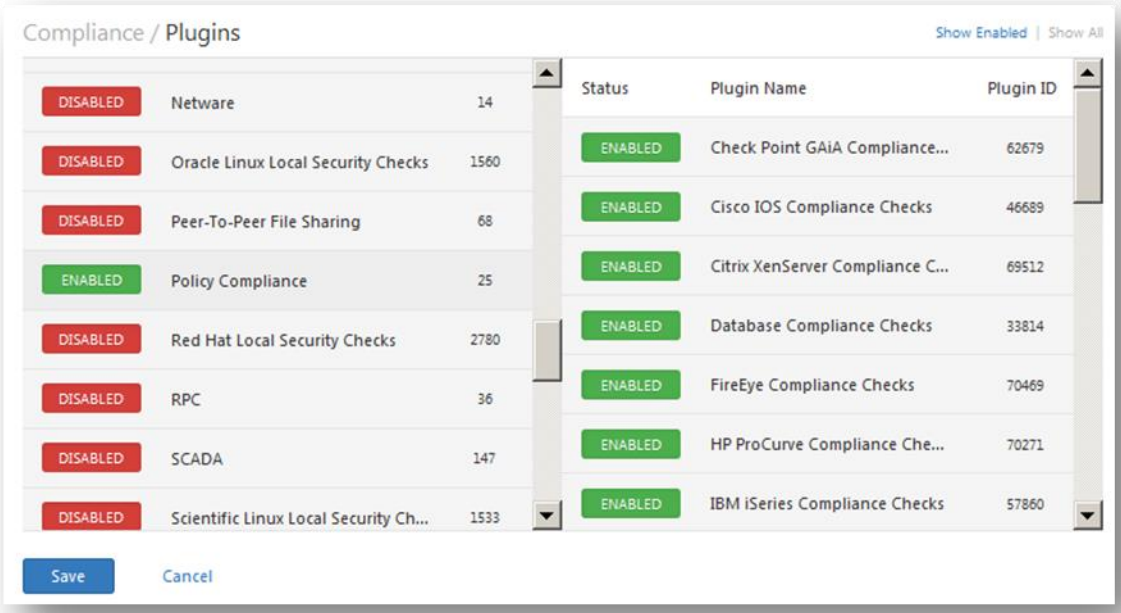
これを実行するには、Policy Wizard で "**Credentialed Patch Audit**" ウィザードを選択するか、または手動で "**Advanced Policy**" を通じて行います。

選択した `.audit` ファイル内のチェックについて理解することが重要です。カスタム ファイルを作成した場合は特にそうです。1 つのスキャンで 2 つの `.audit` ファイルを使用すると、両方のファイルが統合され、各ファイルの結果が 1 つのスキャン内で生成されます。ファイル間で競合する結果が得られた場合は、1 つは合格、もう 1 つは不合格という結果が得られることがあります。レポート内の結果は常に確認してください。



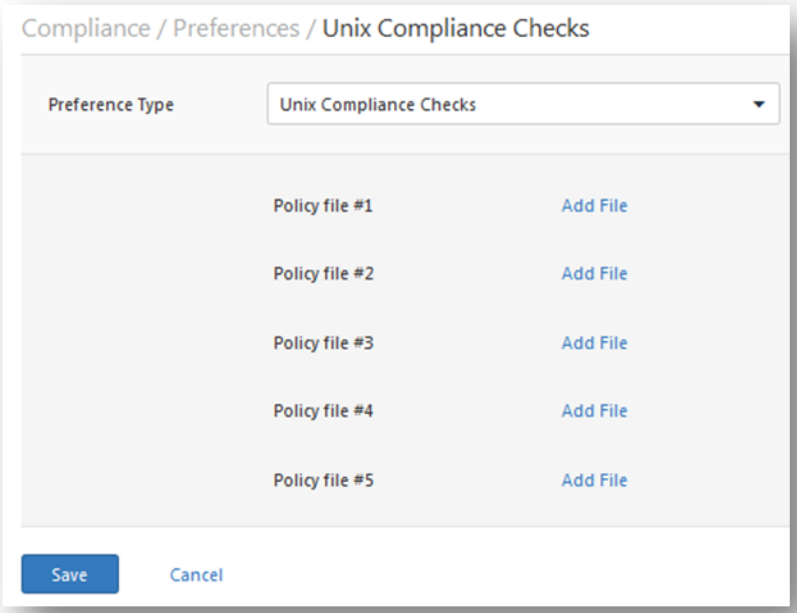
スキャン ポリシーを作成するには、Nessus ユーザー インタフェースにアクセスし、認証して、"Policies" を選択します。既存のポリシーを編集するか、または新しく作成します。ターゲット サーバーにアクセスするための認証情報を指定するには、左側にある "**Credentials**" タブを使用します。

"**Plugins**" タブで "Policy Compliance" プラグイン ファミリーを有効化し、Advanced 設定で "`auto_enable_dependencies`" が "**yes**" (デフォルト) に設定されていることを確認します。



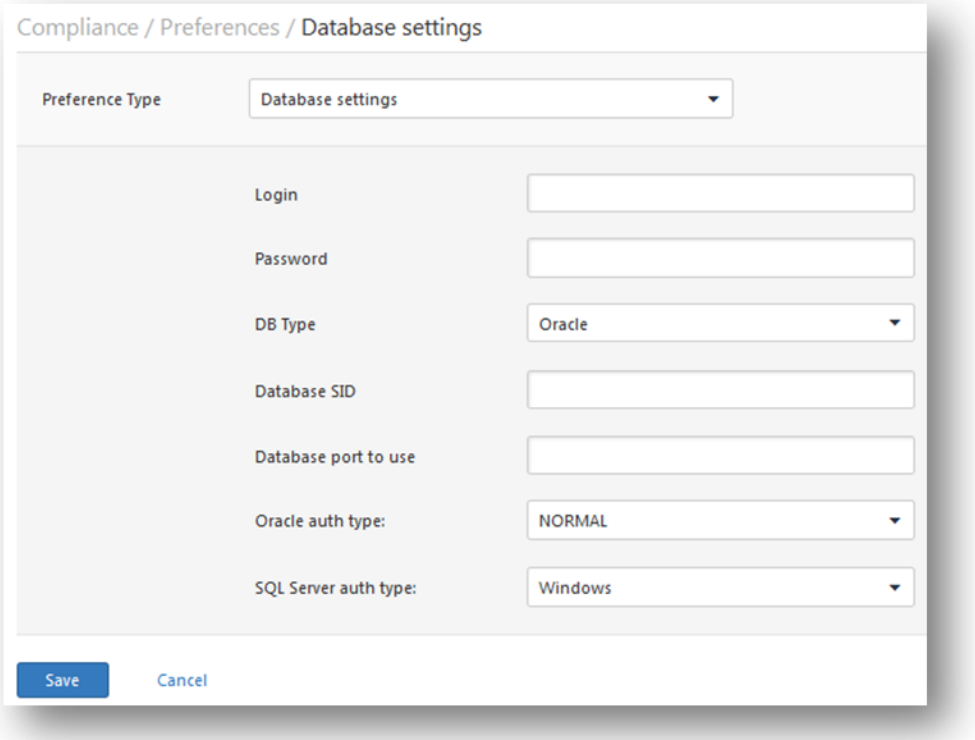
スキャン ポリシーを編集して、ポリシー コンプライアンスが利用可能であることを確認

.audit ファイルの使用を有効化するには、"**Preferences**" タブのドロップダウン メニューから、"Cisco IOS Compliance Checks"、"Unix Compliance Checks"、"Windows Compliance Checks"、"Windows File Content Compliance Checks"、"IBM iSeries Compliance Checks"、または "Database Compliance Checks" を選択します。各セクションには 5 つのフィールドがあり、個別の **.audit** ファイルを指定することができます。指定したファイルは、事前に Tenable サポート ポータルからローカル クライアント システムにダウンロードしておきます。



Unix の .audit ファイルを指定するための Nessus ユーザー インタフェース ダイアログ ボックス例

先のドロップダウン メニューで "Database Compliance Checks" を選択した場合は、"**Preferences**" -> "**Database Settings**" にデータベースのログイン パラメータを入力する必要があります。



以下を含め、"Database Settings" の数々のオプションが利用できます。

オプション	説明
Login	データベースのユーザー名。
Password	指定したユーザー名に対応するパスワード。
DB Type	Oracle、SQL Server、MySQL、DB2、Informix/DRDA、および PostgreSQL がサポートされています。
Database SID	監査対象のデータベース システム ID。Oracle、DB2、および Informix のみで使用できます。
Oracle auth type	NORMAL、SYSOPER、および SYSDBA がサポートされています。
SQL Server auth type	Windows または SQL Server がサポートされています。

これらのフィールドに指定すべき値については、ローカルのデータベース管理者にお問い合わせください。

ここで、ウィンドウの下部にある "Save" をクリックすると、構成が完了します。新しいスキャン ポリシーが、管理対象のスキャン ポリシーのリストに追加されます。

スキャンの実行

コンプライアンス チェックが有効化されたスキャンの実行は、他のローカル パッチ監査スキャンや、通常のネットワーク スキャンの実行と変わりません。必要に応じてこれらを組み合わせて同時に実行することもできます。

結果の例

Nessus では、コンプライアンスの結果はすべて、テストを実行したプラグインの ID 付きで返されます。以下の例では、スキャンされた Windows サーバーに対して返されるデータはすべて、Windows コンプライアンス `.nbin` プラグインからのもので、プラグイン 21156 として識別されています。

Status	Plugin Name	Plugin Family	Count
FAILED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
FAILED	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
WARNING	3 Security Settings (Minor Settings): 111.22.11.222 ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Major Auditing): ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Major Auditing): ...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2
PASSED	2 Auditing and Account Policies (Minor Auditing)(...	Windows Compliance Checks	2

Windows サーバー スキャンのコンプライアンス結果の例

Nessus ユーザー インタフェースの "Reports" タブからダウンロードできる HTML レポートでは、コンプライアンス テストのうち合格したものは青色で "PASSED" と表示され、不合格のものは赤色で "FAILED" と表示され、監査できなかったものは黄色で "WARNING" と表示されます。

上記の例では、4 つの項目のみが表示されています。これらの項目はすべて、不要かつセキュリティ保護されていないサービスやプロトコルの有無を調べるアクセス制御ポリシー チェックの結果です。サービスのいくつかは実行されておらず `.audit` ポリシーの条件を満たしており、いくつか ("remote registry" サービスなど) は実行中で、"FAILED" としてリストされています。"FAILED" としてリストされた項目については、セキュリティ基準に沿って、ポリシーの条件を満たすように構成しなおしてください。

Unix コマンド ラインで使用する Nessus 例

コンプライアンス チェックの取得

有料 Nessus インストールを構成した場合は、プラグイン ディレクトリ内に 5 つのコンプライアンス `.nbin` ファイルがあります。

必要な **.audit** ファイルを Tenable サポート ポータル (https://support.tenable.com/) から入手し、スキャナのプラグイン ディレクトリに置きます。ほとんどのディストリビューションでは、以下のディレクトリがデフォルトの場所です。

/opt/nessus/lib/nessus/plugins

これらのプラグインは、Nessus の脆弱性スキャンで使用する 40,000 以上の **.nasl** プラグイン ファイルの中にあります。これらのファイルを見つけるには、以下のように **.nbin** 拡張子を探します。

```
# ls compliance*nbin database*nbinunix*nbincisco_compliance*nbin

cisco_compliance_check.nbindatabase_compliance_check.nbin
compliance_check.nbinunix_compliance_check.nbin
compliance_check_windows_file_content.nbin
```

Skype プラグイン など、Tenable が提供する他の **.nbin** ファイルは、コンプライアンス チェックには関係ありません。

実際の Nessus デーモンへのローカル アクセス権はないが、サーバーにログインするためのユーザー名とパスワードがある場合は、以下のように **nessus** コマンド ライン クライアントの "**-p**" オプションを使用して 、プラグインのリストをリクエストすることができます。

```
#/opt/nessus/bin/nessus -xp 192.168.20.1 1241 username password | grep 21156
*** The plugins that have the ability to crash remote services or hosts
have been disabled. You should activate them if you want your security
audit to be complete
21156|Policy Compliance|Checks if the remote system is compliant with the
       policy|infos|This script is Copyright (C) 2006 Tenable Network Security|Check
       compliance policy|$Revision: 1.3 $|NOCVE|NOBID|NOXREF|\nSynopsis
       :\n\nCompliance checks\n\nDescription :\n\nUsing the supplied credentials this
       script perform a compliance\ncheck against the given policy.\n\nRisk factor
       :\n\nNone
```

クエリの実行には数分かかることがあります。クエリが正しく実行されたにも関わらずデータが返されない場合は、リモート Nessus スキャナにコンプライアンス チェックがインストールされていません。

.nessus ファイルの使い方

Nessus では、構成したスキャン ポリシー、ネットワーク ターゲット、およびレポートを **.nessus** ファイルとして保存することができます。「Nessus ユーザー インタフェース利用例」セクションでは、コンプライアンス チェック用のスキャン ポリシーを含む **.nessus** ファイルの作成方法を説明しています。**.nessus** ファイルを使用してコマンド ライン スキャンを実行する方法については、"Nessus 5.2 HTML5 User Guide" (http://www.tenable.com/products/nessus/documentation) を参照してください。

.nessusrc ファイルの使い方

Nessus コマンド ライン クライアントでは、構成したスキャン ポリシーを **.nessusrc** ファイルとしてエクスポートすることもできます。これは、コマンド ライン スキャンを有効化する際に便利です。「Nessus ユーザー インタフェース利用例」セクションで、Nessus でのコンプライアンス チェック用にスキャン ポリシーを作成する手順を説明しています。

Nessus でコマンド ライン スキャンを呼び出すには、以下を指定する必要があります。

- Unix、Windows、またはデータベース コンプライアンス チェック プラグイン
- スキャン対象のターゲット ホストの認証情報
- コンプライアンス チェック プラグインを実行するための 1 つ以上の **.audit** ファイル
- 依存関係が有効化されていること

.nessusrc ファイル内の関連エントリが以下のフォーマットになっていること (省略コンテンツあり)。

```
begin(SERVER_PREFS)
…
auto_enable_dependencies = yes
…
end(SERVER_PREFS)
begin(PLUGINS_PREFS)
…
Compliance policy file(s) : = federal_nsa_microsoft_xp_file_permissions.audit
…
end(PLUGINS_PREFS)
begin(PLUGIN_SET)
 21156 = yes
 21157 = yes
…
End(PLUGIN_SET)
```

この例では、スキャンが実行できる項目を指定した他の多くのデータが除外されています。省略されているコンテンツは、使用中の特定の **.audit** ポリシー ファイルの有効化、依存関係の有効化、実際のコンプライアンス プラグイン自体などです。

スキャンの実行

コンプライアンス チェックが有効化されたスキャンの実行は、他のローカル パッチ監査スキャンや、通常のネットワーク スキャンの実行と変わりません。必要に応じてこれらを組み合わせて同時に実行することもできます。

結果の例

GUI クライアントと同様、検出された準拠結果または非準拠結果は、以下のフォーマットでレポートされます。

```
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Reset lockout account counter
       after" : [FAILED]\n\nRemote value: 30\nPolicy value: 20\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Minimum password length" :
       [FAILED]\n\nRemote value: 0\nPolicy value: 8\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Minimum password age" :
       [FAILED]\n\nRemote value: 0\nPolicy value: 1\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Maximum password age" :
       [FAILED]\n\nRemote value: 42\nPolicy value: 182\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Enforce password history" :
       [FAILED]\n\nRemote value: 0\nPolicy value: 5\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Account lockout threshold" :
       [FAILED]\n\nRemote value: 0\nPolicy value: 3\n\n\n
192.168.20.16|unknown (0/tcp)|21156|Security Hole|"Account lockout duration" :
       [FAILED]\n\nRemote value: 30\nPolicy value: 60\n\n\n
```

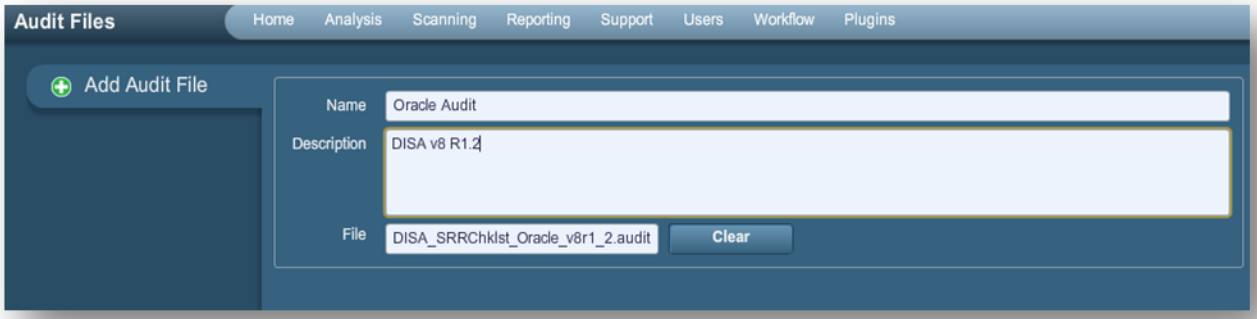
Nessus のデータは、**.nsr** レポート フォーマットで提供されます。これらは非準拠のイベントです。

SecurityCenter の使用

以下の情報は、SecurityCenter 4 以上でのコンプライアンス スキャンの実行に基づいています。Security Center 3.x ユーザーの方は、Tenable サポート ポータル (https://support.tenable.com/) から提供されている "Security Center 3.4 Documentation" を参照してください。

コンプライアンス チェックの取得

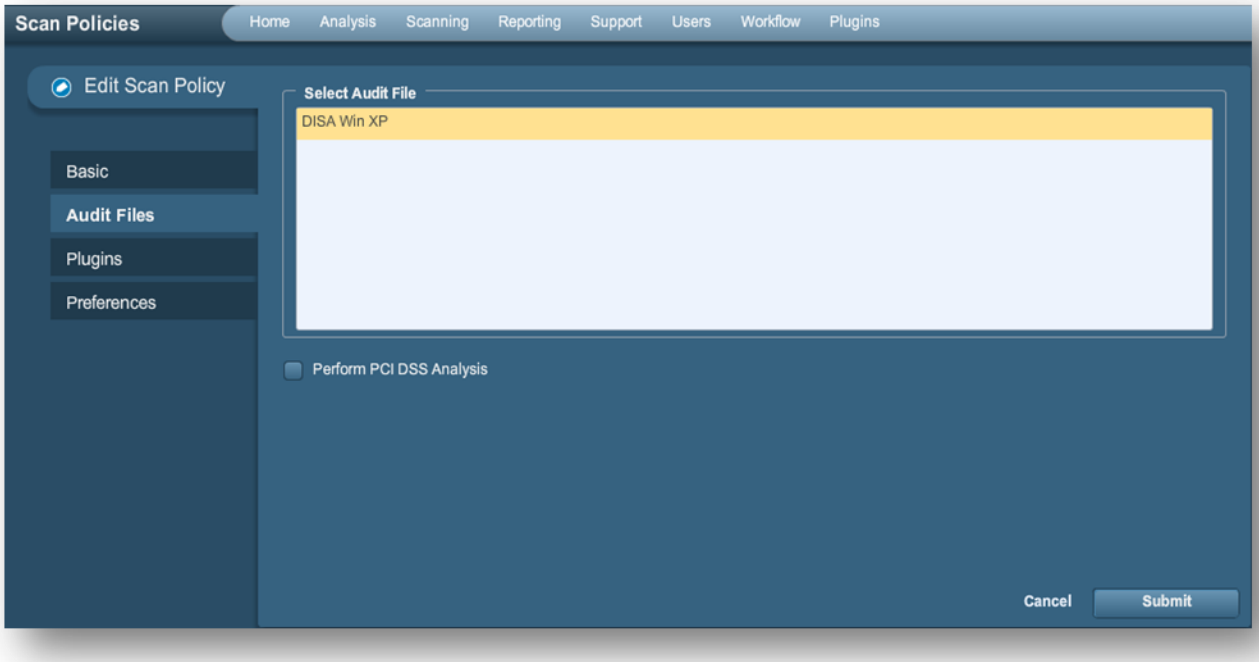
SecurityCenter ユーザーは Nessus 有料プラグインにアクセスできます。これには、Cisco、IBM iSeries、Unix、Windows、Windows File Contents、およびデータベース コンプライアンス チェック プラグインが含まれます。これらのプラグインを使用することで、Tenable が提供する、構築済みでカスタマイズ可能な `.audit` ファイルを使用した、コンプライアンス スキャンのアップロードと実行が可能になります。必要な `.audit` ファイルは Tenable サポート ポータル (https://support.tenable.com/) から入手できます。これらの `.audit` ファイルは、"Create Audit Files" パーミッションを持つユーザーなら誰でも、"Support" タブで "Add Audit File" ツールを使用して、SecurityCenter にアップロードすることができます。



SecurityCenter にアップロードされた `.audit` ファイルはすべて、"Create Policies" パーミッションを持つ SecurityCenter ユーザーなら誰でも利用できます。新しいまたは更新された `.audit` ファイルを Nessus スキャナに配布する処理は、SecurityCenter が行います。

コンプライアンス監査を実行するためのスキャン ポリシーの構成

SecurityCenter でコンプライアンス スキャンを実行するには、コンプライアンス関連の適切な設定を使用してスキャン ポリシーを構成する必要があります。このポリシーでは、スキャン オプション、監査ファイル、有効化されるプラグイン、および詳細設定を指定します。"Scan Policy" の 2 ページ目では、コンプライアンス監査に使用する `.audit` ファイルを指定します。



ここで、**.audit** ファイルをハイライト表示して "Submit" をクリックすることで、1 つまたは複数の **.audit** ファイルを選択することができます。複数の **.audit** ファイルを選択するには、"Ctrl" キーを押しながら選択します。基本 PCI DSS 分析が必要な場合は、送信する前に "Perform PCI DSS Analysis" チェックボックスがオンになっていることを確認してください。

PCI データ セキュリティ スタンダード (PCI DSS) は、Visa、American Express、Discover Financial Services、MasterCard を含む PCI Security Standards Council の創設メンバーが確立した、包括的なセキュリティ基準です。PCI DSS は、あらゆるクレジット カードについて所有者の機密データを守るための共通条件を提供することを目的としており、クレジット カード データを受け取って保管する多くの電子商取引業者によって使用されています。

Tenable では、PCI DSS 監査の実行プロセスを自動化するための 12 のプラグインを SecurityCenter の全ユーザーに提供しています。以下の表にこれらのプラグインをリストします。

これらのプラグインは、スキャンの結果とスキャンの実際の構成を評価して、公開されている PCI コンプライアンス要件をターゲット サーバーが満たしているかどうか判断します。これらのプラグインは実際のスキャンは実行しません。他のプラグインの結果を参照します。PCI DSS プラグインを有効化するには、"Compliance" 画面の "Perform PCI DSS Analysis" ボックスをオンにします。

目的の **.audit** ファイルと PCI DSS 設定を選択した後、"Plugins" タブをクリックしてプラグインの設定を確認します。コンプライアンス スキャンを実行するには、"Policy Compliance" プラグイン ファミリーの項目をポリシー内で有効化する必要があります。

スキャン ポリシーの "Audit Files" タブで 1 つまたは複数の監査ファイルを選択すると、正しいプラグインが "Plugins" タブで自動的に有効化されます。SecurityCenter は選択された **.audit** ファイルを分析し、ファイル内で指定されたタイプに基づいて、正しいプラグインが有効化されます。

"Policy Compliance" ファミリーには、以下のような、コンプライアンス監査に使用できるプラグインが 13 あります。

プラグイン ID	プラグイン名	プラグインの説明
21156	Windows Compliance Checks	一般的な Windows 構成設定を監査するために使用します。
21157	Unix Compliance Checks	一般的な Unix 構成設定を監査するために使用します。
24760	Windows File Contents Compliance Checks	Windows サーバー上の機密ファイル コンテンツを監査するために使用します。
33814	Database Compliance Checks	一般的なデータベース構成設定を監査するために使用します。
33929	PCI DSS compliance	リモート Web サーバーが、クロスサイト スクリプティング (XSS) 攻撃に対して脆弱ではないか、古い SSL2.0 暗号を使用していないか、旧版のソフトウェアを実行していないか、または危険な脆弱性の影響を受けていないか (CVSS 基本値 >= 4) を調べます。
57581	PCI DSS Compliance: Database Reachable from the Internet	インターネットからアクセス可能なデータベースの存在を検出します。存在すると、コンプライアンス監査に合格しません。
60020	PCI DSS Compliance: Handling False Positives	PCI DSS スキャンの誤検知を適切に処理するかどうか調べます。
56208	PCI DSS Compliance: Insecure Communication Has Been Detected	セキュリティ保護されていないポート、プロトコル、またはサービスが検出されていないかを調べます。検出されている場合はコンプライアンスに準拠していません。

56209	PCI DSS Compliance: Remote Access Software Has Been Detected	リモート アクセス ソフトウェアの存在を検出します。存在している場合はコンプライアンスに準拠していません。
33930	PCI DSS Compliance: Passed	利用可能なスキャン情報を使用した結果、Nessus はこのホスト上で欠陥を検知しませんでした。
33931	PCI DSS Compliance: Tests Requirements	Nessus スキャンが PCI テスト要件を満たすかどうかを分析します。技術的なテストに合格しても、このレポートでは、このサーバーを合格と見なすには不十分な場合があります。
46689	Cisco IOS Compliance Checks	一般的な Cisco デバイス構成設定を監査するために使用します。
57860	IBM iSeries Compliance Checks	一般的な IBM iSeries 構成設定を監査するために使用します。

認証情報の管理

SecurityCenter で認証ベースのスキャンを実行する利点のひとつは、使用中の認証情報の管理に役立つことです。SecurityCenter で認証情報を作成するには、"Support" タブを選択し、"Credentials"、"Add" の順にクリックします。

Unix、Windows、および Cisco の認証情報は、スキャン ポリシーとは別に保管および管理されます。認証情報を作成する際の可視性は、現在のユーザー用には "User" を、他の SecurityCenter ユーザーも使用する場合は "Organizational" を使用します。これによりユーザーは、スキャンの結果について作業をしながら、スキャンに必要な認証情報を認識する必要なく、新しいスキャンを実行することができます。

データベース システムをスキャンするには、別の認証情報が必要になります。これらの認証情報はスキャン ポリシー内に保管され、スキャン ポリシー プリファレンス内で、"Database settings" (プラグイン 33815) を通じて構成します。これらの認証情報は、前の段落で指定した認証情報とは別に構成されます。

結果の分析

SecurityCenter を使用して、Nessus スキャンによって返されたコンプライアンス データをさまざまな方法で分析しレポートすることができます。一般的なレポートには以下のようなものがあります。

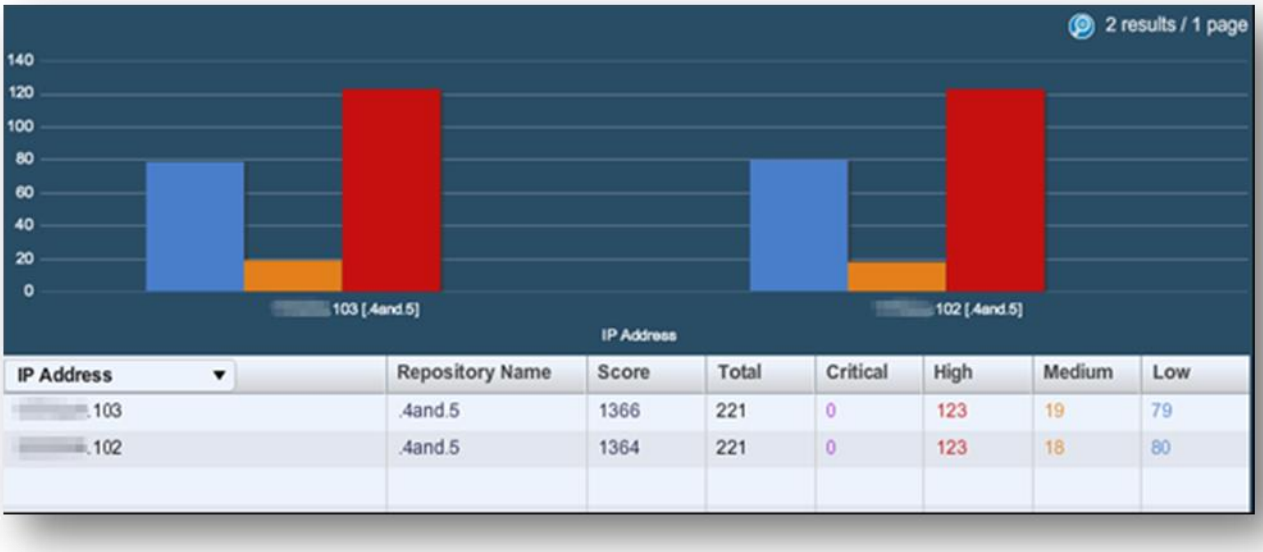
- アセット グループごとに、すべての準拠または非準拠の脆弱性をリストする
- ホストまたはネットワークごとに、すべての準拠または非準拠の脆弱性をリストする
- すべての非準拠問題の概要
- 一般的な構成ミスに関するデータベース設定の監査
- IT のニーズに基づくユーザーまたはソフトウェアのステータス

SecurityCenter によってコンプライアンス データが検出されると、チケット発行、レポート作成、および分析ツールを使用して、監査されたデバイスを再構成する最適な方法を決定することができます。このデータは、他の脆弱性、セキュリティ パッチ、または受動的に検出された情報と並行して分析することができます。

以下は、スキャンしたホストに関するコンプライアンス情報を SecurityCenter を使用して分析している様子を示したスクリーン キャプチャです。

Plugin ID	Total ▼	Severity	Name
1000282	4	Low	HKLM\\software\\microsoft\\windows nt\\currentversion\\winlogon\\allocatedasd
1000295	4	Medium	HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlog\\AutoAdminLogon
1000294	4	Low	HKLM\\System\\CurrentControlSet\\Control\\SecurePipeServers\\Winreg\\AllowedPaths\\Machine
1000293	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Parameters\\NullSessionPipes
1000292	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LanManServer\\Parameters\\NullSessionShares
1000291	4	Medium	HKLM\\Software\\Policies\\Microsoft\\Cryptography\\ForceKeyProtection
1000290	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\ForceGuest
1000289	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\LimitBlankPasswordUse
1000288	4	High	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\NTLMMinClientSec
1000287	4	High	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\MSV1_0\\NTLMMinServerSec
1000286	4	Low	HKLM\\System\\CurrentControlSet\\Control\\Lsa\\NoDefaultAdminOwner
1000285	4	Low	HKLM\\System\\CurrentControlSet\\Services\\LDAP\\LDAPClientIntegrity
1000284	4	Low	HKLM\\Software\\Microsoft\\Driver Signing\\Policy
1000283	4	High	HKLM\\software\\microsoft\\non-driver signing\\policy
1000296	4	Low	HKLM\\System\\CurrentControlSet\\Control\\FileSystem\\NtfsDisable8dot3NameCreation
1000281	4	High	HKLM\\software\\microsoft\\windows nt\\currentversion\\winlogon\\scremoveoption
1000280	4	High	HKLM\\system\\currentcontrolset\\control\\lsa\\lmcompatibilitylevel
1000279	4	High	HKLM\\system\\currentcontrolset\\control\\print\\providers\\lanman print services\\servers\\addprinterdrive
1000278	4	Medium	HKLM\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Winlogon\\AutoAdminLogon
1000277	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NetworkNoDialIn
1000276	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\NetworkHideSharePwds
1000275	4	Medium	HKLM\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer\\NoDriveTypeAutoRun
1000274	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\PerformRouterDiscovery
1000273	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\SynAttackProtect
1000272	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\DisableIPSourceRouting
1000271	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\KeepAliveTime
1000270	4	Medium	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\EnableDeadGWDetect
1000269	4	High	HKLM\\system\\CurrentControlSet\\Services\\Tcpip\\Parameters\\EnableICMPRedirect

SecurityCenter でのコンプライアンス監査データのリスト表示



IP Address	Repository Name	Score	Total	Critical	High	Medium	Low
.103	.4and.5	1366	221	0	123	19	79
.102	.4and.5	1364	221	0	123	18	80

SecurityCenter での、サーバーごとのコンプライアンス監査データのリスト表示

SecurityCenter の使用方法の詳細については、SecurityCenter のドキュメント (https://support.tenable.com/) を参照してください。

詳細情報

Tenable では、Nessus のインストール、展開、構成、ユーザー操作、総合的なテストについて詳述したドキュメントを多数用意しています。

- **Nessus 5.2 インストールおよび構成ガイド** – インストールおよび構成の詳しい手順を説明しています。
- **Nessus 5.2 ユーザー ガイド** – Nessus ユーザー インタフェースの構成および操作方法を説明しています。
- **Unix と Windows での Nessus 認証チェック** – Nessus 脆弱性スキャナを使用して認証ネットワーク スキャンを実行する方法を説明しています。
- **Nessus コンプライアンス チェック リファレンス** – Nessus コンプライアンス チェック シンタックスの総合ガイドです。
- **Nessus v2 File Format** – Nessus 3.2 と NessusClient 3.2 で導入された `.nessus` ファイル フォーマットの構造について説明しています。
- **Nessus 5.0 REST Protocol Specification** – Nessus の REST プロトコルとインタフェースについて説明しています。
- **Nessus 5 and Antivirus** – いくつかの有名なセキュリティ ソフトウェア パッケージが Nessus とどう連動するかについて概要を説明し、セキュリティの侵害や脆弱性スキャンの妨害を招くことなく、より良い共存を可能にするためのヒントや解決方法を示します。
- **Nessus 5 and Mobile Device Scanning** – Nessus が Microsoft Active Directory およびモバイル デバイス管理サーバーと統合されて、ネットワーク上で使用されているモバイル デバイスを特定する方法について説明しています。
- **Nessus 5.0 and Scanning Virtual Machines** – Tenable Network Security の Nessus 脆弱性スキャナを使用して仮想プラットフォームの構成およびそこで実行されているソフトウェアを監査する方法について説明しています。

- **Strategic Anti-malware Monitoring with Nessus, PVS, and LCE** – Tenable の USM プラットフォームが悪意のあるさまざまなソフトウェアを検知し、マルウェアを特定し、その感染範囲を判定する方法について説明しています。
- **Patch Management Integration** – Nessus と SecurityCenter が、IBM TEM、Microsoft WSUS と SCCM、VMware Go、および Red Hat Network Satellite パッチ管理システム上の認証情報を活用して、Nessus スキャナで認証情報が利用できない可能性があるシステム上でパッチ監査を実行する方法について説明しています。
- **Real-Time Compliance Monitoring** – さまざまなタイプの政府規制や財政規制に適合するために、Tenable のソリューションがどのように使用できるかを説明しています。
- **Tenable Products Plugin Families** – Nessus、Log Correlation Engine、Passive Vulnerability Scanner 用のプラグイン ファミリーの説明とサマリーが記されています。
- **SecurityCenter Administration Guide**

その他のオンライン リソースは以下のとおりです。

- Nessus ディスカッション フォーラム：https://discussions.nessus.org/
- Tenable ブログ：http://www.tenable.com/blog
- Tenable ポッドキャスト：http://www.tenable.com/podcast
- 使用例のビデオ：http://www.youtube.com/user/tenablesecurity
- Tenable Twitter ページ：http://twitter.com/tenablesecurity

support@tenable.com または sales@tenable.com までお気軽にお問い合わせください。または Tenable の Web サイト http://www.tenable.com/ をご参照ください。

Tenable Network Security について

Tenable Network Security は、新たに生じる脆弱性、脅威、コンプライアンス関係のリスクに事前に対応するために、米国防総省全体、および多数の世界最大級の企業と政府をはじめとする 24,000 以上の組織に信頼され、利用されています。同社の Nessus および SecurityCenter ソリューションは、脆弱性の特定、攻撃の防止、および多数の規制要件へのコンプライアンスに対する標準を設定し続けます。詳細については、www.tenable.com をご参照ください。

本社グローバル

Tenable Network Security
7021 Columbia Gateway Drive
Suite 500
Columbia, MD 21046
410.872.0555
www.tenable.com