実習 - ネットワーク セキュリティの脅威について

目的

パート 1:SANS Web サイトについて考察する

- SANS Web サイトにアクセスし、リソースを確認します。

パート 2:ネットワークの最新の脅威を識別する

- SANS サイトを使用して最近のネットワーク セキュリティの脅威をいくつか確認します。
- ネットワーク セキュリティの脅威に関する情報を提供する、SANS の域を超えたサイトを確認します。

パート 3:固有のネットワーク セキュリティの脅威を詳説する

- 具体的な最近のネットワーク セキュリティの脅威を選択し、詳しく記述します。
- 情報をクラスに紹介します。

背景/シナリオ

攻撃からネットワークを保護するために、管理者はネットワークを危険にさらす外部の脅威を明らかにする必要があります。セキュリティ Web サイトを使用すると、新たな脅威を識別したり、ネットワークを保護するための脅威の軽減策を提供したりできます。

コンピュータおよびネットワーク セキュリティの脅威に対する防御として特によく使用され、信頼されているサイトの 1 つが SysAdmin, Audit, Network, Security（SANS）です。SANS サイトは、「20 Critical Security Controls for Effective Cyber Defense（サイバー ディフェンスのための 20 の重大なセキュリティ コントロール）」のリストや、週刊ニュースレター「@Risk: The Consensus Security Alert（@リスク：セキュリティ アラートに関する共通認識）」など、複数のリソースを提供しています。このニュースレターは、新しいネットワーク攻撃や脆弱性を詳しく説明しています。

この実習では、SANS サイトにアクセスして調査し、SANS サイトを使用して最新のネットワーク セキュリティの脅威を明らかにするとともに、脅威を識別する他の Web サイトについても調査します。また、特定のネットワーク攻撃の詳細について調査し、発表します。

実習に必要なリソースや機器

- インターネットにアクセスできるデバイス
- PowerPoint または他のプレゼンテーション ソフトウェアがインストールされているプレゼンテーション用コンピュータ

パート 1:　SANS の Web サイトの調査

パート 1 では、SANS の Web サイトにアクセスし、利用可能なリソースを調査します。

手順 1:　SANS のリソースを確認します。

Web ブラウザを使用して、www.SANS.org にアクセスします。ホームページで [**Resources（リソース）**] メニューを強調表示にします。

利用できるリソースを 3 つ挙げてください。

手順 2:　上位 20 件の重大なコントロールを確認します。

SANS Web サイトに掲載されている「**Twenty Critical Security Controls for Effective Cyber Defense（サイバー ディフェンスのための 20 の重大なセキュリティ コントロール）**」は、米国防総省、米国家安全保障局、CIS（Center for Internet Security）、および SANS Institute による官民一体となった協力の集大成です。このリストは、サイバー セキュリティ管理と DOD での支出に対する優先順位付けのために策定されました。これは、米国政府での有効なセキュリティ プログラムの中心的存在となっています。[**Resources（リソース）**] メニューの [**Top 20 Critical Controls（上位 20 件の重大なコントロール）**] を選択します。

20 件の重大なコントロールの 1 つを選択し、そのコントロールの実現案を 3 つ挙げてください。

手順 3:　[Newsletter（ニュースレター）] メニューを探します。

[**Resources（リソース）**] メニューを強調表示の状態にして [**Newsletters（ニュースレター）**] を選択します。参照できる 3 つのニュースレターについて簡単に説明してください。

パート 2:　ネットワークの最新の脅威を識別する

パート 2 では、SANS サイトを使用して最近のネットワーク セキュリティの脅威を調査し、セキュリティの脅威に関する情報がある他のサイトを明らかにします。

手順 1:　「@Risk：Consensus Security Alert（@リスク：セキュリティ アラートに関する共通認識）」ニュースレターのアーカイブを探します。

ニュースレターのページで「@RISK：The Consensus Security Alert（@リスク：セキュリティ アラートに関する共通認識）」の [**Archive（アーカイブ）**] を選択します。画面を下にスクロールして [**Archives Volumes（アーカイブ ボリューム）**] が表示されたら、最近の週刊ニュースレターを選択します。「**Notable Recent Security Issues（注目すべき最近のセキュリティ問題）**」および「**Most Popular Malware Files（特に蔓延しているマルウェア ファイル）**」の各セクションを確認します。

最新の攻撃をいくつか挙げてください。必要に応じて、最近のニュースレターを参照してください。

手順 2:　最近のセキュリティの脅威に関する情報を提供しているサイトを確認します。

SANS サイト以外で、最近のセキュリティの脅威に関する情報が記載された Web サイトをいくつか挙げてください。

これらの Web サイトで詳しく説明されている最近のセキュリティの脅威をいくつか挙げてください。

パート 3:　固有のネットワーク セキュリティの脅威を詳説する

パート 3 では、発生している特定の攻撃について調査し、調査結果に基づいてプレゼンテーション資料を作成します。調査結果に基づいて次のフォームを完成させます。

手順 1:　選択したネットワーク攻撃について次のフォームを完成させます。

攻撃の名前:	
攻撃のタイプ:	
攻撃の日付:	
影響を受けたコンピュータ/組織:	
動作の仕組みとその結果:	
軽減策:	
参考資料および情報へのリンク:	

手順 2:　インストラクタが示すガイドラインに従ってプレゼンテーションを完成させます。

復習

1. 自分のコンピュータを保護するためにどのような措置を取ることができますか。

2. リソースを保護するために組織が実行できる重要な措置は何ですか。