

最も侵入性の高いタイプの脆弱性スキャナーは、脆弱性の検出を停止することはありません。エクスプロイトフレームワークには、脆弱性を使ってコードを実行したり、システムへのアクセス権を取得しようとしたりするデフォルトのスクリプトが含まれます。このタイプの侵入性の高いテストは、自動化された脆弱性スキャンよりもより一般的なペネトレーションテストです。

認証スキャンと非認証スキャン

非認証スキャンとは、OSまたはアプリケーションにログオンせずに、パケットをホストに直接向けることでテストするものです。取得できる結果は、ホストがネットワーク上の権限のないユーザーに露出している内容です。テストルーチンには、サービスアカウントやデバイス管理インターフェイスにデフォルトパスワードを使用するというようなルーチンを含めることができます。これらは既定の特権アクセスではありません。認証スキャンを使用するとより多くの脆弱性を発見できますが、高レベルな特定のアクセス権や総合的な管理アクセスを持たない脅威アクターに焦点を絞って検討したい場合もあります。非認証スキャンは、ネットワーク境界の外部評価をしたり、ウェブアプリケーションスキャンを実行する際に最適な技術です。

認証スキャンは、ユーザー アカウントに様々なホストへのログオンの権利や、テストルーチンに適したその他のアクセス権を与えます。この類のテストにより、特にいつアプリケーションやセキュリティ設定が誤って設定されたかを検出する際に、より深い分析が可能になります。また、インサイダー攻撃が何を達成できるのか、または脅威アクターがユーザー アカウントを侵害した場合に達成できるものを示すこともできます。認証スキャンは、非認証スキャンよりも侵入性の高いタイプのスキャンです。

New Credential

Name: Classroom Domain
Login: classroom\Administrator
Comment (optional):
 Autogenerate credential
 Password: *****
 Key pair
 Private key:
 Passphrase:

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Kali LinuxにインストールされたGreenbone OpenVASのターゲット（範囲）定義で使用するための認証を設定。（スクリーンショットはGreenbone Networksから許可を得て使用<http://www.openvas.org>。）

脆弱性スキャナーのみが使用する専用のネットワークアカウントを作成。これらのアカウントの認証がスキャンサーバーに安全に保存されるようにする。

誤検知、検知漏れ、ログレビュー

スキャントールは、スキャン中に発見されたすべての脆弱性のサマリーレポートを実行終了直後に生成します。重要度の観点から、脆弱性はカラーコードで報告されます。赤は通常、早急な対応が必要な脆弱性を表します。通常、（全てのホストに関して最も重要度が高い）範囲ごとまたはホストごとに脆弱性を確認できます。報告には各脆弱性や、ホストを修復する方法といった特定の詳細事項を含める、または関連づける必要があります。

Information	Results (135 of 1148)	Hosts (1 of 254)	Ports (17 of 30)	Applications (19 of 44)	Operating Systems (1 of 6)	CVEs (48 of 48)	Closed CVEs (56 of 56)	TLS Certificates (3 of 5)	Error Messages (2 of 2)	User Tags (0)
Microsoft Windows Multiple Vulnerabilities (KB4457131)	10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 9:58 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4467691)	10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:20 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4471321)	10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:40 PM UTC				
Microsoft Windows Multiple Vulnerabilities (KB4512517)	10.0 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:27 PM UTC				
Microsoft Malware Protection Engine on Windows Defender Multiple Remote Code Execution Vulnerabilities	9.3 (High)	97 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:19 PM UTC				
Microsoft Malware Protection Engine on Windows Defender Multiple Vulnerabilities	9.3 (High)	80 %	10.1.0.1	DC1.corp.515support.com	general/tcp	Fri, Jan 3, 2020 10:09 PM UTC				

Windowsのホストに見つかった重大度の高い複数の脆弱性をリストするスキャン報告書。
(スクリーンショット：Greenbone Community Edition greenbone.net/en/community-edition。)

侵入/アクティブスキャナは、ホストシステムのより広い範囲の脆弱性を検出する可能性が高く、誤検知を削減できます。誤検知は、実際は違うのに、スキャナーまたは他の評価ツールが脆弱であると識別することです。例えば、脆弱性スキャナがファイアウォール上のオープンポートを識別できたとします。あるブランドのマルウェアがこのポートを使っていることが分かっていると、ツールはこれをセキュリティリスクであると分類し、あなたにポートを閉じることを推奨します。しかし、あなたのシステムではポートは開かれていません。この問題の調査には時間と労力を要します。過剰な数の誤検知が脆弱性スキャナで提示される場合、スキャナを全く無視してしまうのは簡単ですが、それによってより大きな問題につながる可能性があります。

検知漏れの可能性にも注意を払わなくてはなりません。すなわち、潜在的な脆弱性がスキャナで識別されない可能性です。このリスクは、定期的にスキャナを実行したり、複数のベンダーのスキャナーを使用することで緩和することができます。同様に、自動化されたスキャナのプラグインは、予めコンパイルされたスクリプトに依存しているため、技術的に優れた意欲的なハッカーが成功した侵害を再現することができず、安全に対する誤った意識を生み出す可能性があります。

関連システムやネットワークログを見直すことで、脆弱性の報告の確認プロセスを強化することができます。一例として、あなたの脆弱性スキャナが、Windowsマシンの実行プロセスを識別したとします。スキャナーによると、このプロセスを作成したアプリケーションは不安定で、オペレーティングシステムがロックアップしたり他のプロセスやサービスをクラッシュすることで知られています。コンピューターのイベントログを調査して、過去数週間にいくつものエントリーが、プロセスの失敗を示していることに気づきます。その後さらに、他のいくつかのプロセスが失敗したことをエントリーが表示します。この例では、脆弱性アラートが実際に有効であるのかを確認するために、関連のデータソースを使用しています。

構成レビュー

既知のソフトウェア悪用を、ネットワーク上で見つけた動作中の様々なバージョンのソフトウェアとマッチングするだけでなく、脆弱性スキャンは既定のベンチマークと比較して、セキュリティ管理、アプリケーション設定、許可の構成を評価します。脆弱性スキャンは、必要と考えられる制御に不備がないかや、アップデートされていないウイルス対策ソフトウェアやデフォルト設定のままの管理パスワードなど、制御の有効性を低下または無効化する可能性のあるシステムの構成不備がないかを識別します。概して言えば、この類のテストには認証スキャンが必要です。また、特定のアプリケーションまたはセキュリティ管理を構成する場合は、ベストプラクティスに関する特定の情報も必要です。これらは、制御や適切な構成設定をテンプレートにリストアップすることで提供できます。

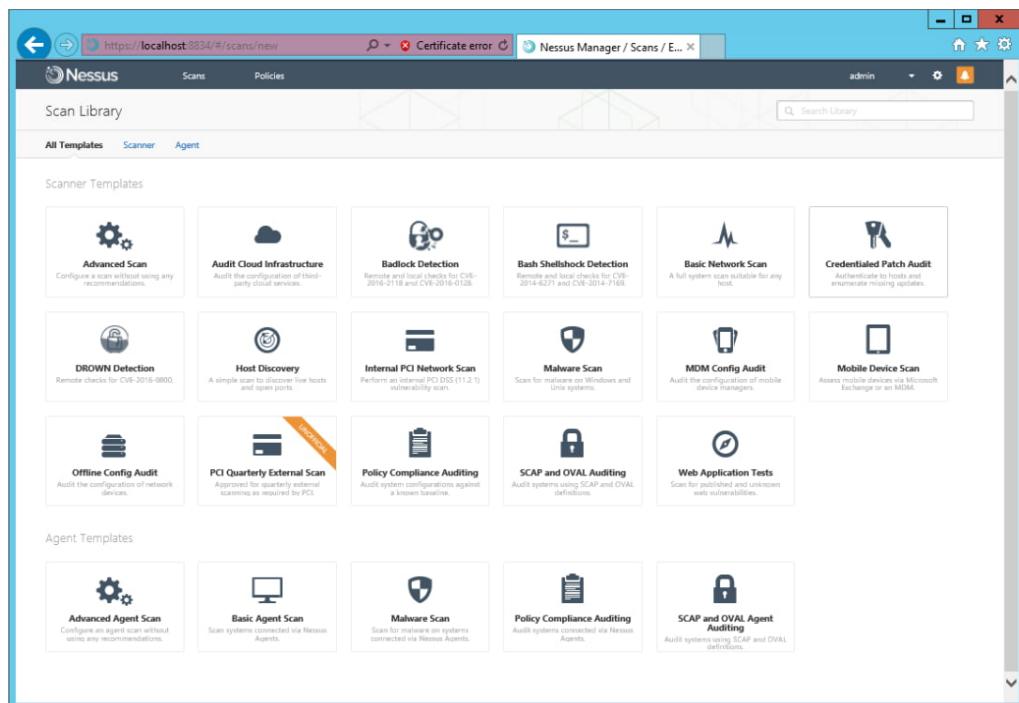
*Security content automation protocol (SCAP)*を使用すると、コンピューターが構成ベースラインを満たしているかを互換性のあるスキャナーで判断できます。SCAPでは、この機能を実現するためにいくつかのコンポーネントを使用しますが、そのうちの最も重要なものをいくつか挙げます。

- Open Vulnerability and Assessment Language (OVAL) — システムのセキュリティ状態を表したり、脆弱性の報告や情報を照会するXMLスキーマ。
- セキュリティ設定チェックリスト記述形式 (Extensible Configuration Checklist Description Format、XCCDF) — ベストプラクティスに沿った構成のチェックリストやルールを開発し監査するXMLスキーマ。以前はベストプラクティスのガイドは文章で書かれていて、システム管理者が手作業で適用していました。XCCDFは、互換性のあるソフトウェアを使って適用・確認できる機械で読み取り可能なフォーマットを提供します。

The screenshot shows the Windows Policy Viewer window titled "Policy Viewer - 513 items". The main pane displays a table of policy settings across five columns: Policy Type, Policy Group or Registry Key, Policy Setting, 515support, and Template. The "Template" column is highlighted in blue. Several rows are selected, showing settings like MaximumPasswordAge (42), MinimumPasswordAge (1), MinimumPasswordLength (7), PasswordComplexity (1), and PasswordHistorySize (24). Below the table, the "Policy Path" is listed as "Security Settings\Account Policies\Password Policy\Minimum password length". Under "515support", details about the GPO (Default Domain Policy) and its file location (C:\Users\administrator\Documents\gpo\{BC850A02-A566-49E6-9269-CF4FFC2610A7}\DomainSysvol\GPO\Machine\microsoft\windows nt\SecEdit\Gpt Tmpl.inf) are shown. The "Template" section shows the value 14 and lists several GPOs from which it is defined, including MSFT Windows 10 1809 and Server 2019 - Domain Security, MSFT Windows 10 and Server 2016 - Domain Security, and various security baselines.

ローカルネットワークセキュリティポリシーとテンプレートを比較。ローカルポリシーで決められている最小パスワード長さは、テンプレートで推奨されているものよりはるかに短い。
(スクリーンショットはMicrosoftからの許可を得て使用。)

一部のスキャナーは、ベストプラクティスに沿ったフレームワークに対してシステムと構成設定を測定します。これをコンプライアンススキャンと呼びます。これは、規制遵守のために必要な場合もあれば、外部で合意されたベストプラクティスの基準に自動的に適合させる場合もあります。



Nessus Managerスキャンコンプライアンスをサポートするスキャンテンプレート。
(スクリーンショットはTenable Network Securityから許可を得て使用。)

脅威ハンティング

脆弱性スキャンがパッチやベースライン構成の標準定義のリストを使用するのに対して、脅威ハンティングは、脅威インテリジェンスから得られる知見を活用して、ネットワークやシステム内にすでに存在するTTPの証拠を積極的に発見する評価手法です。この技術は、インシデント管理システムによってアラート状態が報告された場合のみトリガーされる反応的プロセスとは対照的な技術です。また、脅威ハンティングとペネトレーションテストを対比することもできます。ペネトレーションテストがシステム侵入や具体的な脆弱性の実証を実現しようとしているのに対して、脅威ハンティングはシステム内のデータ分析のみに基づきます。その点で、脅威ハンティングの方がペネトレーションテストよりシステムを混乱させにくいと言えます。

脅威ハンティングプロジェクトは、上級セキュリティアナリストによって指揮される傾向がありますが、一般的な観察ポイントは次の通りです。

- 勧告と報告** — 脅威ハンティングは、労働集約的アクティビティであるため、明確な目的とリソースを決めて実行する必要があります。脅威ハンティングは通常、可能性のある脅威の仮説にしたがって進めます。ベンダーやセキュリティ研究者から入手した、新しいTTPや脆弱性に関するセキュリティ報告と勧告は、脅威ハンティングを実施する際のトリガーとなり得ます。例えば多くの会社のWindowsデスクトップが、脅威インテリジェンスによって現在のマルウェア定義ではブロックできない新しいタイプのマルウェアに感染していることが明らかになった場合、自分のシステムがこのマルウェアに感染しているかどうかを検出するために次の脅威ハンティングプランを開始できます。
- インテリジェンス統合**と脅威データ — 脅威ハンティングは、ネットワークやログデータを手作業で分析することによって実行できますが、これは非常に時間のかかるプロセスです。セキュリティ情報イベント管理(SIEM)と脅威分析プラットフォームを保有する組織は、インテリジェンス統合手法を適用できます。分析プラットフォームは、TTPとIoCの脅威データフィードで最新に保ちます。アナリストはクエリとフィルターを開発し、ネットワークトラフィックとログから抽出したオンプレミスデータと脅威データの相互の関係を比較することができます。このプロセスは、AI支援の分析と相互関係を使用して部分的または全体的に自動化することもできます。

- **Maneuver (マニューバー)** — 疑わしい発生中の脅威を調査している場合は、敵対者のハッキングの性質を忘れないようにしなくてはなりません。能力のある脅威アクターは、脅威ハンティングの可能性を予測し、検出を失敗させるための対策を講じるよう計画している可能性があります。例えば脅威アクターは、DDoS攻撃をトリガーして、セキュリティチームの注意をそらし、目的に対するアクションを実行する計画を進めているかもしれません。マニューバーとは、立場的優位性を獲得することに関する軍事上の教義用語です(ccdcoc.org/uploads/2012/01/3_3_Applegate_ThePrincipleOfManeuverInCyberOperations.pdf)。防御的マニューバーの一例として、脅威ハンティングではパッシブな発見手法を使い、セキュリティチームが封じ込め、根絶、復旧計画を立てる前に、脅威アクターに侵入が発見されたことを悟られないようにすることができます。

レビューアク ティビティ： 脆弱性スキャン技術

次の質問にお答えください。

- 緊急に対応が必要な脅威の助言を受けたため、ネットワーク脆弱性スキャンを設定し、ネットワーク上にCVEに関するものがないかを確認する必要があります。スキャンを実行する前に行うべき脆弱性スキャンソフトに関する構成チェックにはどんなものがありますか？
- あなたは、エンジニアリング関連の企業にネットワーク脆弱性スキャナーを設定しました。スキャンを実行すると、組み込みシステムネットワーク内の複数のセンサーが応答しなくなり、生産が停止しました。代わりに組み込みシステムネットワークに使うべき脆弱性スキャンの方法は何ですか？
- ホスト上にCentOS Linux関連のCVEが存在すると、脆弱性スキャンから報告がありましたが、ホストがCentOSを実行しないようにホストを設定したはずです。これはどのタイプのスキャンエラーイベントですか？
- あなたがセキュリティコンサルティングサポートを提供している小さな会社は、イベント管理や脅威インテリジェンスプラットフォームに投資することに抵抗しています。しかしCEOは、会社の産業分野でのサプライチェーンをターゲットにすることで知られるAPTリスクが存在することに対して懸念を抱いており、すでにターゲットになっているサインがないかシステムをスキャンすることを望んでいます。資金が足りない中、この要求に答えるにはどんな課題がありますか？
- 脅威アクターに気付かれないようにする評価技術に関する用語はどれですか？

トピック3D

ペネトレーションテストの概念を説明する



対象試験範囲

1.8 ペネトレーションテストで使用する手法を説明することができる

自動化された脆弱性スキャンは、能力の高い脅威アクターがどんなことを実現する可能性があるのかをテストすることはできません。ペネトレーションテストは、既知の戦術や技術を採用して侵入を企てるタイプの評価です。ペネトレーションテストの考案、計画、指導は専門的なセキュリティロールですが、ジュニアレベルのあなたがこのタイプの業務に携わる可能性もあるため、基本的な原則を説明できるようにならなくてはなりません。

ペネトレーションテスト

ペネトレーションテスト（縮めてペンテストと呼ぶことがあります）は許可されたハッキング技術を使って、ターゲットのセキュリティシステムの悪用される可能性のある脆弱性を発見します。ペンテストは、倫理的ハッキングと呼ばれることもあります。ペンテストには、次のステップが含まれます。

- 脅威の存在を確認 — 監視ツール、ソーシャルエンジニアリングツール、ネットワークスキャナー、脆弱性評価ツールなどを使用して、脆弱性が悪用される可能性のあるベクトルを特定する。
- セキュリティ管理のバイパス — システムを攻撃する簡単な方法を探す。例えば、ネットワークがファイアウォールによって強力に保護されている場合に、建物内のコンピューターへの物理的なアクセス権を手に入れたり、USBスティックからマルウェアを実行することができるか。
- セキュリティ管理のアクティブなテスト — 弱いパスワードやソフトウェアの脆弱性などの構成上の脆弱性やエラーの制御をプローブする。
- 脆弱性の悪用 — データへのアクセス権を手に入れたり、バックドアをインストールするために脆弱性をエクスプロイトして、脆弱性のリスクが高いことを証明する。

脆弱性のパッシブ評価との主な違いは、セキュリティ制御のテストや発見された脆弱性のエクスプロイトが積極的に試みられる点です。ペンテストは、侵入評価技術です。例えば脆弱性スキャンによって、SQLサーバーに、既知のエクスプロイトから保護するためのパッチ処理がされていないことが明らかになったとします。ペネトレーションテストは、エクスプロイトを利用してコードインジェクションを実行したり、サーバーを侵害したり、「所有」（またはハッカーイディオム「pwn」）したりします。これによって、セキュリティ管理を実際にテストします。エクスプロイトが存在する可能性があるとしても、実際はサーバー上のアクセス権によって、攻撃者による使用が防げる場合があります。これは脆弱性スキャンではほとんど識別されませんが、ペネトレーションテストで証明できる場合とできない場合があります。

交戦規則

セキュリティ評価は、従業員が行う場合と、契約を取り交わしたコンサルタントまたは他のサードパーティが行う場合があります。**交戦規則**でのアクティビティを許可し、どのアクティビティを許可しないかを指定します。これらの規則は、契約上の合意文書に明記するべきです。

例えばペンテストは、「ネットワークへの侵入」目的のようなあいまいなものではなく具体的な目的と範囲を決定しなくてはなりません。ペネトレーションテスト担当者がアクセスや悪用を試みるべきではないシステムやデータがある場合もあります。ペンテストにサードパーティーのサービス（クラウドプロバイダーなど）が含まれる場合、サードパーティーからもテストに対する承認を得る必要があります。



ペンテスト標準ウェブサイトは、ペンテストの実施に関するきわめて貴重な解説を提供しています (pentest-standard.readthedocs.io/en/latest/tree.html)。

攻撃プロファイル

攻撃のソースや動機はさまざまです。外部（ターゲット型および非ターゲット型）とインサイダー脅威の両方に対する耐性をテストすることを望むかもしれません。ネットワークに関する情報をどの程度コンサルタントに提供するかを決定する必要があります。

- **ブラックボックス**（または未知の環境）— ネットワークやそのセキュリティシステムに関する特権情報は一切コンサルタントに提供しません。このタイプのテストでは、テスターが偵察フェーズを実行する必要があります。ブラックボックステストは、外部脅威の行動をシミュレーションする場合に有益です。
- **ホワイトボックス**（または既知の環境）— コンサルタントは、ネットワークに関する情報への完全なアクセス権を与えられます。このタイプのテストは、ブラックボックスのテスト中に発見された欠陥を完全に評価するために、ブラックボックステストのフォローアップとして行われることがあります。このタイプのテストでは、テスターは偵察フェーズをスキップします。ホワイトボックステストは、権限を持つインサイダー脅威の行動をシミュレーションするのに有益です。
- **グレイボックス**（または部分的に既知の環境）— コンサルタントは一般的に、特定タイプのインサイダー脅威をモデル化するため、下級または非IT部門スタッフの知識に類似する情報を与えられます。このタイプのテストでは、テスターが部分的な偵察を実行する必要があります。グレイボックステストは、権限のないインサイダー脅威の行動をシミュレーションするのに有益です。

脅威アクターはシステムについての知識を持っていないが、スタッフはテストが実施されることを知らされている場合のテストをブラインド（またはシングルブラインド）テストと呼びます。スタッフもペネトレーションテストの実施を知らない場合をダブルブラインドテストと呼びます。

バグバウンティ

バグバウンティとは、ソフトウェアのベンダーまたはウェブサイトオペレーターが行うプログラムで、脆弱性を報告すると報酬が支払われます。ペンテストが契約に基づいて実行されると、コンサルタント料が発生しますが、バグバウンティプログラムは、不特定多数の人に対して業務内容と報酬を提示するクラウドソーシング(crowd sourcing)型の脆弱性検出方法です。バグバウンティの中には、従業員だけに報酬を支払う方法で社内プログラムとして運営されているものもあります。しかしほんどの場合が、一般公募されています(tripwire.com/state-of-security/security-data-protection/cyber-security/essential-bug-bounty-programs)。

演習タイプ

ペネトレーションテストで使用する技術の一部は、2つの競合チーム間の演習としても採用されます。

- **レッドチーム** — ターゲットに潜入を試みる攻撃側の役割を実行します。
- **ブルーチーム** — 潜入を検出し防御するために監視と警戒を管理して、防御側の役割を実行します。

ホワイトチームを編成することもあり、交戦規則を設定し、演習を監視し、必要に応じて調停や指導を行います。レッドチームがサードパーティーの場合、ホワイトチームには、コンサルタント会社の代表者を含めます。ホワイトチームの重要なタスクの一つは、あまりにもリスクが高い場合に演習を停止することです。例えば実際の脅威アクターが、レッドチームが設定したバックドアにピギーバックを試みてきた場合などが該当します。

レッドチーム対ブルーチームの演習における典型的なプロセスは、レッドチームが侵入を試み、その試みが成功または失敗し、サマリーレポートを作成するというものです。この対決構造が、建設的に開発や改良を促進するとは限りません。**パープルチーム**の演習では、演習が継続している間、レッドチームとブルーチームは定期的に結果を聞き取るためにミーティングを行います。レッドチームはどの部分で成功したかを明らかにし、ブルーチームと協力して検出メカニズムを捻出します。このプロセスは、進行役のパープルチームのメンバーがサポートします。パープルチーム演習の欠点は、ブラインドまたはダブルブラインド状態でなければ、敵対する相手やこれに対処する緊張状態をシミュレートできないことです。

パッシブ偵察とアクティブ偵察

敵のTPPを分析することで、最新のサイバー攻撃がどのように行われているかに関する様々な「キルチェーン」モデルが確立されます。ペネトレーションテストの実施には一般に、同様の技術を使用します。

ブラックボックステストの最初の偵察フェーズでは、ペンテスターは調査対象のプロファイルを作成し、脆弱性を求めて攻撃対象領域を調査します。偵察アクティビティはパッシブまたはアクティブに分類できます。パッシブ偵察とは一般に入手可能な情報をクエリすることで、調査対象に警戒体制を取らせることはできません。アクティブ偵察は、発見されるリスクが高くなります。アクティブな技術には、建物に物理的にアクセスしたり、ターゲットのウェブサイトや他のネットワークに対してスキャンツールを使用することなどが含まれます。

- **オープンソースインテリジェンス(OSINT)** — ウェブサーチツール、ソーシャルメディア、サイトを使って、インターネット接続されたデバイスやサービスの脆弱性をスキャンし (securitytrails.com/blog/osint-tools)、ターゲットに関する情報を入手します。theHarvester (github.com/laramies/theHarvester)のようなOSINT集約ツールは、複数のソースからこのデータを収集し編成します。OSINTは、意図的にせよ無意識にせよ、企業が一般公開している情報からの発見に依存しているため、特権アクセスをほとんど必要としません。これはパッシブ手法です。
- **ソーシャルエンジニアリング** — これは、情報、建物への物理的アクセス、または勧誘の手口を使ってユーザー アカウントへのアクセスまで取得することを指します。関わり方はさまざまですが、これはアクティブな手法に分類されます。
- **フットプリントティング** — Nmap (nmap.org)のようなソフトウェアツールを使って、ホストまたはネットワークトポロジーに関する情報を入手します。脅威アクターが物理的アクセス権を入手すると、ウェブホストや有線または無線ネットワークセグメントに対してスキャンが行われます。パッシブなフットプリントティングは（**パケットスニッフィング**に限定することによって）可能ですが、多くのスキャン技術では、検出ソフトウェアが収集できる、ターゲットとのアクティブなネットワーク接続を必要とします。
- **ウォードライビング** — ターゲットによって運営されているワイヤレスネットワークの場所やタイプ（周波数チャネルやセキュリティ方法）をマッピングすることです。こういったネットワークは、建物の外からアクセスできる場合もあります。単にワイヤレスネットワークの存在をスニッフィングするのはパッシブアクティビティですが、守衛に見つかったりカメラに写されてしまいうリスクがあります。脅威アクターは、Hak5 Pineapple (shop.hak5.org/products/wifi-pineapple)のような不正アクセスポイントを設置したり、ウォードライビングで収集したインテリジェンスを使ってワイヤレス攻撃を実行します。
- **ドローン/無人航空機(UAV)** — テスターはキャンパスの施設を偵察し、空からウォードライビングを実行することすらできます（ウォーフライング）。Wi-Fi Pineappleのようなツールは、ドローンに簡単に組み込むことができます(hackaday.com/2018/05/27/watch-dogs-inspired-hacking-drone-takes-flight)。ドローンもまた、普遍的にポピュラーなソーシャ

ルエンジニアリング技術を利用してベクトルとします。つまり施設周辺に感染したUSB媒体を落とし、そのうちの少なくとも何個かが拾われて使用されることを期待するわけです (blackhat.com/docs/us-16/materials/us-16-Bursztein-Does-Dropping-USB-Drives-In-Parking-Lots-And-Other-Places-Really-Work.pdf)。

ペントスト攻撃のライフサイクル

キルチェーン攻撃のライフサイクルにおける偵察後の最初の悪用フェーズでは、ソフトウェアツールを使ってターゲットネットワークへの何らかのアクセス権を入手します。フィッシングメールやペイロードを使ったり、ソーシャルエンジニアリングを介して認証情報を取得して足掛かりを作ります。足掛けかりをつかめたら、ペントスターはアクセス手段の確保や拡大に取り掛かります。そのためには、複数の技術が必要となります。

- **持続性** — 侵害されたホストに再接続して、リモートアクセスツール(RAT)またはバックドアとして使用するテスターの能力。この実現のために、テスターはコマンド&コントロール(C2またはC&C) ネットワークを使って侵害されたホストを制御し、追加の攻撃ツールをアップロードし、流出したデータをダウンロードします。侵害されたホストへの接続は、通常、シャットダウン/ログオフのイベントの後に実行されるマルウェア実行ファイルと、ネットワークポートへの接続と脅威アクターのIPアドレスが必要となります。
- **特権エスカレーション** — 持続性の次にさらに偵察が行われ、ペントスターは内部ネットワークをマッピングし、そこで実行中のサービスと、サービスにアクセスするために設定したアカウントの発見を試みます。ネットワーク内を動き回ったり、データ資産にアクセスするには、より高い特権レベルが必要になる可能性があります。例えばオリジナルのマルウェアが、クライアントのワークステーションでローカル管理者の特権を利用したり、Webサーバー上でApacheユーザーとして実行している場合が該当します。マルウェアがシステム/ルートの特権を使ったり、アプリケーションサーバーのような他のホストでネットワーク管理者特権を使ったりして実行する悪用もあります。
- **ラテラルムーブメント** — 他のホストを介して制御します。これは、アクセスを拡大する機会(認証情報の取得、ソフトウェアの脆弱性の検出、その他の「戦利品」の収集)を発見するため、価値のあるデータ資産の場所を特定するため、そして検知を回避するために行われます。ラテラルムーブメントには通常、リモート処理を共有することで攻撃ツールを実行したり、PowerShellのようなスクリプト作成ツールを使用することなどが含まれます。
- **ピボット** — 最も価値のあるデータを保持するホストは通常、外部のネットワークに直接アクセスすることはできません。ペントスターが周辺サーバーに足掛けかりを得ると、ピボットすることでネットワークの境界を回避し、内部ネットワークのサーバーを侵害することができます。ピボットは通常、Secure Shell (SSH)、バーチャルプライベートネットワーク(VPN)、またはリモートデスクトップなどのリモートアクセスやトネリングプロトコルを使用して実行されます。
- **目的に対するアクション** — 脅威アクターにとって、これは1つ以上のシステムからデータを盗むことです(データの流出)。ペントスターの観点から言うと、問題になるのは、これを試みるべき範囲の定義です。多くの場合、目的に対するアクションは達成可能であることを示せば十分です。
- **クリーンアップ** — 脅威アクターにとって、これは攻撃の証拠または少なくとも脅威アクターに結びつく可能性のある証拠を除去することです。ペントスターにとって、このフェーズはバックドアまたはツールを除去し、システムが侵害前より安全性が減少していないことを確認するためのフェーズです。

レビュー アク ティビティ： ペネトレーションテストの概念

次の質問にお答えください。

1. Webサイトの所有者が、サイトのセキュリティは犯罪シンジケートによるリスクを緩和できているかを評価することを希望しています。インサイダー脅威のリスクは無いと仮定します。どのタイプのペネトレーションテストを使用すると、こういった敵の能力やリソースを詳細にシミュレートすることができますか？
2. あなたは、様々なシナリオに基づいてセキュリティ管理をテストする一連のチームベースの演習を行うことに同意しています。あなたはパープルチームによるテストを使用することを提案しますが、請負業者が唯一精通しているのはレッドチームとブルーチームの概念です。パープルチームの演習を実行する利点は何ですか？
3. ホストしているウェブサイトでペントestを行う前にインターネットサービスプロバイダー(ISP)に通知しなくてはならないのはなぜですか？
4. OSINTにはどんなツールを使用しますか？
5. ペネトレーションテストのコンテキストにおける持続性とはなんですか？

レッスン3

概要

脆弱性、脅威ハンティング、ペネトレーションテストなどのセキュリティ評価のタイプを要約できる必要があります。また、これらの評価を行うための一般的な手順を説明できる必要があります。

セキュリティ評価を実行するためのガイドライン

セキュリティ評価の利用を検討する際は、これらのガイドラインに従います。

- 脆弱性の攻撃対象領域をスキャンする場合に必要な手順とツールを特定します。これは、パッシブネットワークスキャナー、アクティブリモートネットワークスキャナー、エージェントベースネットワークスキャナー、アプリケーションスキャナー、またはウェブアプリケーションスキャナーを準備することを意味します。
- 認証スキャンや脆弱性フィードの更新をセキュアに使用できるように、構成や保守の計画を策定します。
- 誤検知と検知漏れを識別するために、定期的にスキャンを実行し、その結果をレビューし、必要に応じてログレビューや追加のCVE情報を使用して結果を確認します。
- 構成レビューと修正プランをスケジュールします。アクションに優先順位をつける場合は、CVSS脆弱性の重要度を使用します。
- 脅威ハンティングプログラムの実施や新しい脅威ソースの助言や情報を監視します。脅威ハンティングは、インテリジェンス統合や脅威データを供給するリソースに投資する必要があります。
- ペネトレーションテスト演習の実施を検討する場合、レッド/ブルーまたはパープルチーム演習タイプや、ブラック/ホワイト/グレイボックスの開示タイプなど交戦規則を明確に設定します。
- ペネトレーションテストは、構造化されたキルチェーンライフサイクルを使って、偵察、エクスプロイト、持続性、特権エスカレーション、ラテラルムーブメント/ピボット、目的に対するアクション、クリーンアップのフェーズで実行します。

レッスン4

ソーシャルエンジニアリングと マルウェアを特定する

レッスン概要

セキュリティ評価では、ソフトウェアの脆弱性と構成のエラーのみに重点を置くだけでは十分ではありません。攻撃対象領域には、ハードウェアシステムやソフトウェアシステムのほかに、企業の従業員も含まれ、不正アクセスや権限を取得するために従業員が悪用のターゲットとなる可能性があります。脅威アクターはソーシャルエンジニアリングの手法を使用し、情報を引き出して、建物へのアクセス許可を得たり、ユーザーをだまして悪意のあるコードを実行させようとします。こうした攻撃について把握し、同僚や顧客がこうした攻撃を検知し、報告できるように指導する必要があります。これらのテクニックを説明できるようになることに加え、さまざまな種類のマルウェアに関するインジケーターを説明して、システムの感染の可能性を分析できる必要があります。

レッスンの目的

このレッスンの内容は、以下のとおりです。

- ソーシャルエンジニアリングの手法を比較・対比する。
- マルウェアベースの攻撃のインジケーターを分析する。

トピック4A

ソーシャルエンジニアリングの手法を比較・対比する



対象試験範囲

1.1 さまざまなタイプのソーシャルエンジニアリング手法を比較対照することができる

従業員、請負業者、サプライヤー、顧客など、人はあらゆる組織の攻撃対象領域の一部です。システムで権限を有する人物はソーシャルエンジニアリングのターゲットになる可能性があります。ソーシャルエンジニアリングの手法を比較・対比できるようになることで、セキュリティ認識トレーニングを先導し、こうしたリスクを緩和するためのポリシーやセキュリティ管理の開発ができるようになります。

ソーシャルエンジニアリング

脅威アクターは、あらゆる手法を用いてセキュリティシステムを侵害しようとする可能性があります。多くの攻撃の前提条件となるのが、ネットワークとセキュリティシステムに関する情報の取得です。ソーシャルエンジニアリングとは、誰から情報を引き出したり、脅威アクターが何らかのアクションを実行させる手段を指します。「人のハッキング」とも呼ばれます。ソーシャルエンジニアリングは、侵入に備えて調査としてインテリジェンスを収集するために使用される場合や、実際の侵入を実行するために使用される場合があります。一般的なソーシャルエンジニアリングの侵入シナリオには次が含まれます。

- 脅威アクターは、ネットワークユーザーにパスワードの入力を求める実行可能ファイルを作成し、ユーザーが入力した内容をすべて記録します。その後脅威アクターはその実行可能ファイルをユーザーに電子メールで送信し、組織でその朝に発生したログオンの問題を解決するために、ファイルをダブルクリックして、ネットワークに再びログオンるように促します。ユーザーがそれに従うと、脅威アクターはネットワークの認証情報にアクセスできるようになります。
- 脅威アクターは、リモートアクセスの設定でサポートが必要なリモートセールス担当者を装つてヘルプデスクに連絡します。脅威アクターは一連の電話連絡を通じて、リモートアクセス用の電話番号と組織の専用電話およびボイスメールシステムにアクセスするための電話番号に加え、リモートアクセスサーバーの名前/アドレスとログイン認証情報を取得します。
- 脅威アクターは、火災報知器を作動させて、混乱状態になっているときに建物内に侵入し、監視デバイスをネットワークポートに取り付けます。

ソーシャルエンジニアリングの原則

ソーシャルエンジニアリングは、最も一般的で成功している悪意のある手法の1つです。ソーシャルエンジニアリングは、基本的な人々の信頼を悪用するため、普段は実行しない行動を実行するように人を操作する上で特に有効な方法であることが証明されています。説得力を持たせるために、ソーシャルエンジニアリング攻撃では次の原則の1つまたは複数に依存します。

親密性/好意

一部の人には生まれ持ったカリスマ性のようなものがあり、要求どおりに人を納得させることができます。ソーシャルエンジニアの基本ツールの1つは、単に話しやすく好かれやすく、要求を、あたかも合理的で反論できないように提示する力に長けていることです。要求が拒否されたとしても、疑われる可能性が低いため、このアプローチのリスクは比較的低いです。ソーシャルエンジニアは、検知されることなく別のターゲットに移動できます。

コンセンサス/社会的証明

コンセンサスまたは社会的証明の原則は、特定の方法で行動するという明確な指示がなければ、多くの人は、他人と同じようにふるまうという事実を指します。ソーシャルエンジニアリング攻撃では、この本能を利用して、リクエストを拒否するのは奇妙だとターゲットを説得するか（「これは他の誰もがノーと言ったことはない」）、誰かがドアを押さえている間に建物に入り込むなど、礼儀正しい行為を悪用する可能性があります。また別の例として、脅威アクターは、サイトを称賛する多数の偽のレビューや紹介文を投稿することで、悪意のあるWebサイトが実際に正当であるとユーザーを騙し、信じこませることができる場合があります。被害者は、他にも多くの人がサイトを容認できると判断していると信じ、それをサイトの正当性の証拠と見なしてサイトに信頼を置きます。

権威と威圧

多くの人は、高い地位にあったり、専門知識が優れていると感じている人からの要求を拒否するのは難しいと感じています。ソーシャルエンジニアは、こうした行動を悪用して上級管理者になりますし、ターゲットを威圧することができます。攻撃は、警察官、裁判官、医師など、多くの場合で意見が聞き入れられる可能性のある人物になりますことから始まることがあります。別の手法は、偽の技術的な話題や専門用語を使用することです。ソーシャルエンジニアリングでは、無知を認めようとする人がほとんどいないという事実を悪用できます。この種の敵対的な戦術は、親密性や好意のアプローチを使用する場合と比較して、疑惑が生じやすく、ターゲットが攻撃の試みを報告する可能性が高いため、脅威アクターにとってリスクが高い可能性があります。

希少性と緊急性

多くの場合は営業担当者によって展開され、希少性や緊急性の誤った感覚を生み出すことは、人々の通常の意思決定プロセスを妨げる可能性があります。ソーシャルエンジニアは、迅速な応答を求めてターゲットにプレッシャーをかけることができます。例えば、ソーシャルエンジニアは、ターゲットに「期間限定」または「招待のみ」のトライアルにサインアップさせ、（ターゲットが他のアカウントにも使用しているパスワードを提供することを期待して）サービスに対するユーザー名とパスワードを要求しようとする可能性があります。偽のウイルス対策製品で、ユーザーをだまして自分のコンピューターがすでにマルウェアに感染していると思わせようとして、切迫感を生み出します。

なりすましと信頼

なりすましとは、単に誰かに見せかけるようにすることです。これは基本的なソーシャルエンジニアリング手法の1つです。なりすましは、コンセンサス/好意または威圧的なアプローチのいずれかを使用できます。なりすましは電話や電子メールのメッセージを通じてなど、ターゲットが脅威アクターの身元が簡単に判明できない場合にできます。

昔ながらのなりすまし攻撃の例として、ある部門にソーシャルエンジニアが電話をかけ、システムをリモートから調整する必要があると偽ってユーザーにパスワードを開示させるというものがあります。この特定の攻撃はプリテキスティングとも呼ばれます。



電話の相手が誰なのか、きちんと把握できていますか？

なりすましに説得力をもたせ、ターゲットとの信頼関係を確立するには、通常、組織に関する秘匿情報を取得することで実現します。例えば、脅威アクターが組織のITサポートチームのメンバーになりますます場合、なりすましている人物とターゲットの身分情報の詳細があれば、攻撃はより効果的になります。

一部のソーシャルエンジニアリング手法では、偵察行動としてこの種のインテリジェンスを取得することに専念します。多くの企業がセキュリティよりもカスタマーサービスを重視しているため、このような情報は大抵簡単に入手可能です。一見無害な情報（部門別の従業員リスト、役職名、電話番号、スケジュール帳、請求書、注文書など）も、なりすまし攻撃に利用される可能性があります。

ダンプスター・ダイビングとテールゲート

ソーシャルエンジニアリングには、情報を盗んだり、アクセス権を取得する物理的な攻撃が含まれます。

ダンプスター・ダイビング

ダンプスター・ダイビングはソーシャルエンジニアリングの一種で、組織や個人が出したごみを詳しく調べて有用な文書を見つけ出そうとすること（あるいは廃棄されたリムーバブルメディアからファイルを入手しようとする）を指します。

攻撃は長期間に渡って段階的に行われる場合もあります。例えば、まず些末な情報や下位のユーザーアカウントへの不正アクセスを試み、それらを利用して、より秘匿性の高い機密データやより厳重に保護された管理者アカウントに対する攻撃へと移行するケースなどがよく知られています。

テールゲートとピギーバック

テールゲートとは、ドアまたはチェックポイントの通過を許可されている人物のすぐ後ろについていくことを意味し、セキュリティ保護された領域に許可なく侵入する手段のひとつです。ピギーバックは同様の状況ですが、脅威アクターが従業員のアクセス許可権限で保護されたエリアに入ることを意味します。例えば、脅威アクターは清掃要員になりますし、清掃用のカートやモップとバケツを運び入れる際に従業員にドアを押させてもらうよう要請する可能性があります。またピギーバックは、建物への入館記録に記録することなく、誰かにアクセス許可を与えることができる内部の脅威アクターの手段である可能性があります。また、ドアを開けた人物に「バッジ/鍵を忘れた」などの口実を語り、一緒に通らせてもらうという手法もあります。

身分詐称と請求書詐欺

身分詐称は、脅威アクターが誰かの身分情報の特定の詳細を使用する特殊ななりすましです。典型的な消費者の身分詐称は、他人の名前と住所を使用してローンを申請したり、盗まれたクレジットカードの詳細を使用して携帯電話を契約したりすることです。請求書詐欺は、また別の一般的な種類の身分詐称です。通常、詐欺師は本物のサプライヤーの請求書の詳細を偽装しますが、銀行口座番号を変更します。これは、ターゲットが口座を再確認しないことに依存している場合や、ソーシャルエンジニアリングの連絡先と組み合わせ、口座変更が本当であるとターゲットを納得させる場合があります。

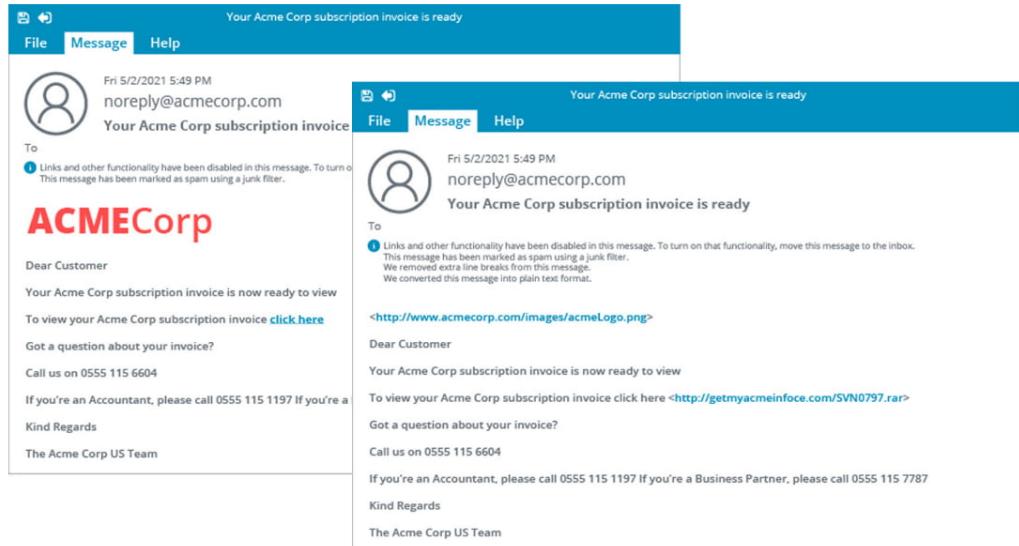
! 身分詐称と個人情報の窃盗という用語は、身元情報を捏造することと他人の個人情報を盗むことを区別するために使用される場合があります。

企業ネットワークの攻撃の場合、身分詐称はコンピューターアカウントの侵害が関わる可能性が高くなります。さまざまなソーシャルエンジニアリングの手法を使用して、マルウェアに依存することなく、アカウントの認証情報を取得できます。ユーザーから直接認証情報を引き出す以外の手法には次が含まれます。

- **認証情報データベース** — 過去の攻撃で得たアカウントの詳細は広く公開されています (haveibeenpwned.com)。脅威アクターは、これらのデータベースの1つでターゲットのマッチングを試み、パスワードが再利用されていることに期待します。またなりすましにサードパーティのサイトを利用する可能性もあります。例えば、職場のアカウントを使用する代わりに、ソーシャルメディアアカウントをコントロールできる可能性があります。
- **ショルダーサーフィン** — 脅威アクターはユーザーの入力操作を見て、パスワードやPIN（またはその他の保護された情報）を学ぶことができます。「被害者の肩越しに情報を入手する」という意味でこう呼ばれていますが、必ずしも脅威アクターが近くにいるとは限らず、高倍率の双眼鏡やCCTVカメラを使用して、離れた場所から直接観察している可能性もあります。
- **ランチタイム攻撃** — ほとんどの認証方法は、ワークステーションの物理的なセキュリティに依存しています。ユーザーがログオンしたままワークステーションを離れる場合、脅威アクターは物理的にシステムへのアクセスを得ることができます。これは多くの場合、ランチタイム攻撃と呼ばれます。ほとんどのオペレーティングシステムは、設定した時間キーボードやマウスの操作がない場合に、パスワードで保護されたスクリーンセーバーが起動するように設定されています。またユーザーは、ワークステーションを離れる場合にロックするか、ログオフするように指導を受けるべきです。

フィッシング、ホエーリング、ビッシング

フィッシングは、ソーシャルエンジニアリングとスプーフィングの組み合わせです。ターゲットを、信頼できるリソースとして見せかけた悪意のあるリソースとやり取りするように説得または誘導します。通常はベクトルとして電子メールが使用されます。フィッシングメッセージでは、偽装されたマルウェアのインストールや脅威アクターによるリモートアクセス接続の許可など、何らかのアクションを実行するようにユーザーを説得しようとする可能性があります。その他のフィッシングキャンペーンでは、銀行やeコマースサイトを模倣した偽装Webサイトやその他ターゲットが信頼するはずのWebリソースを使用します。その後、正規のWebサイトのユーザーに電子メールを送信し、アカウントの更新が必要であると伝えたり、一種の偽アラートや警告として、実際には偽装サイトへと誘導する偽のリンクを提供します。ユーザーが偽装サイトで認証を受けると、ログオンの認証情報がキャプチャされます。



フィッシングメールの例 — 右側では、メールクライアントでリンクの性質を偽装するように設計されたフォーマット（左側に表示）が取り除かれているため、メッセージを実際の形式で表示できます。

以下のフィッシングの変種について認識しておきましょう。

- **スピアフィッシング** — フィッシング詐欺のうち、個々のターゲットが攻撃にだまされやすくなるような情報を脅威アクターが使用するものを指します。各フィッシングメッセージは、特定のターゲットユーザーに対して調整されます。例えば、脅威アクターがターゲットが編集している文書の名前を知っていて悪意のあるコピーを送信したり、フィッシング詐欺メールに受信者のフルネームや役職名、電話番号など（その通信が正規のものであるとターゲットに信じ込ませるような情報）を脅威アクターが知っていることが示されている場合があります。
- **ホエーリング** — 組織の上級管理者（CEOやその他の「大物」）を特に狙ったスピアフィッシング攻撃です。上層部は、基本的なセキュリティ手順を習得することに消極的であるため、通常のフィッシング攻撃に対してより脆弱である可能性があります。
- **ビッシング** — 音声チャネル（電話、VoIPなど）を通じて実施されるフィッシング攻撃。例えば、ターゲットは銀行の担当者を装った者から電話を受け、最近のクレジットカード取引を確認するために、セキュリティ情報を要求される可能性があります。電子メールでの要求に比べ電話口での要求はさらに断りにくい可能性があります。



ディープフェイク技術の急速な向上([forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000](https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/))により、音声や動画メッセージを介したフィッシングの試みは今後さらにまん延する可能性があります。

- **スミッシング** — これは、ベクトルとしてショートメッセージサービス(SMS)テキスト通信を使用します。

スパム、デマ、プリベンディング

未承諾電子メール（**スパム**）は多くの攻撃のベクトルとして使用されます。脅威アクターは、マーケティングリストや過去にプライバシー侵害を受けたデータベースから電子メールアドレスを取得したり、特定の企業の全ての電子メールアドレスを標的にすることを試みる可能性があります。大量メール攻撃は、あらゆる種類のインスタントメッセージングまたはインターネットメッセージングサービスを介して実行される可能性もあります（**スピム**）。

セキュリティアラートやチェーンメールなどの**デマ(hoax)**も一般的なソーシャルエンジニアリングの手法で、多くの場合フィッシング攻撃と組み合わされます。電子メールアラートやWebポップアップでは、ウイルス感染など一種のセキュリティ問題を特定したとして、その問題を修正するツールを提供します。もちろんそのツールはトロイの木馬といった類のアプリケーションです。マルバタイジングは、コンテンツ配信ネットワーク(CDN)から提供される広告用に確保された、あまり監視されていない正当なWebサイト上のスペースの使用を悪用します (blog.talosintelligence.com/2019/07/malvertising-deepdive.html)。また犯罪者は、巧妙な電話詐欺を使用し、ユーザーをだましてログイン認証情報や金融口座の詳細を明らかにしようとします。

フィッシングまたはデマメールは、プリペンド（先頭に追加）することにより説得力のあるものにすることができます。攻撃的な意味で、プリペンドすることは、メールシステムによって生成されたように見えるテキストを追加することを意味します。例えば、脅威アクターは件名に「RE:」を追加して、メッセージが返信であるかのように見せかけたり、「MAILSAFE: PASSED」などを追加して、メッセージはセキュリティソフトウェアによってスキャン済みで、承認済みであるかのように見せかける場合があります。逆に一部のメールシステムでは、外部メッセージやメッセージにスパムとして明確に識別されていませんが疑わしい要素がある場合に外部メッセージや警告メッセージをタグ付けするなど、合法的にプリペンドを実行する場合があります。

ファーミングとクレデンシャルハーベスティング

1つの連絡先へのダイレクトメッセージは、失敗する可能性が非常に高くなります。他のソーシャルエンジニアリングの手法では、偽のサイトやログインページなどの偽装したリソースを使用しますが、被害者を罠にかけるためにリダイレクトや受動的な方法に依存します。

ファーミング

ファーミングとは、正当なWebサイトから悪質なものへとユーザーをリダイレクトする受動的な手段です。ファーミングは、ソーシャルエンジニアリングの手法を使用してユーザーをだます代わりに、被害者のコンピューターによるインターネットの名前解決の実行手段を破損させ、正規のサイトから悪質なものへとリダイレクトさせる形を取ります。例えば、mybank.fooが本来IPアドレス2.2.2.2を示すべきである場合に、ファーミング攻撃が名前解決プロセスを破損させてIPアドレス6.6.6.6を示させるなどです。

タイプスクワッティング

脅威アクターはリダイレクトの代わりに**タイプスクワッティング**を使用する可能性があります。脅威アクターは、connptia.orgなどの実際のドメイン名と非常によく似たドメイン名を登録し、ユーザーが違いに気付かないことを期待していることを意味します。これらは、いとこドメイン、類似ドメイン、またはドッペルゲンガードメインとも呼ばれます。タイプスクワッティングでは、ファーミング攻撃とフィッシング攻撃で使用される可能性があります。もう1つの手法は、onmicrosoft.comなどの信頼できるクラウドプロバイダーのプライマリドメインを使用して、ハイジャックされたサブドメインを登録することです。フィッシングメッセージがcomptia.onmicrosoft.comからのように見える場合、多くのユーザーはそれを信頼する傾向があります。

水飲み場型攻撃

水飲み場型攻撃は、脅威アクターがターゲットと直接通信するリスクのない、また別の受動的な手法です。これは、ターゲットのグループが安全ではないサードパーティのWebサイトを使用する可能性があるという状況に依存しています。例えば、国際的なeコマースサイトを実行するスタッフが、ローカルのピザ配達会社を使用しているとします。脅威アクターは、ピザ配達会社のWebサイトを侵害したり、一種のマルバタイズメントをデプロイできる場合、eコマース企業の従業員のコンピューターを感染させ、eコマース企業のシステムに浸透させることができます。

クレデンシャルハーベスティング

クレデンシャルハーベスティングは、フィッシングとファーミングの一般的な領域内で、アカウントの認証情報を盗むために特別に設計されたキャンペーンです。脅威アクターは、取得されたログインのデータベースを直接悪用するのではなく、販売することに興味がある可能性があります。そのような攻撃では、「お使いのアカウントは、児童ポルノのホスティングに使用されています」や「アカウントストレージに問題があります」などの警告メッセージと、Google、Microsoft、Facebook、Twitterなどの正当なサービスプロバイダーのロゴが大げさに示されたファーミングサイトへのリンクを使用します。マルバタイズメントやショッピングカードのコードに挿入されたスクリプトを使用する攻撃も流行しています(csoonline.com/article/3400381/what-is-magecart-how-this-hacker-group-steals-payment-card-data.html)。ターゲットを絞ったクレデンシャルハーベスティングでは、1つの会社のパスワードリセットやアカウント管理ポータルに対して行われる可能性があります。

インフルエンスキャンペーン

インフルエンスキャンペーンは、国家的アクター、テロリストグループやハクティビストグループなどの高度な能力を持つ脅威アクターによって起動された主なプログラムです。インフルエンスキャンペーンの目標は、あるトピックに関する世論を変えることです。検知されたほとんどのハイプロファイルのインフルエンスキャンペーンは、選挙活動をターゲットとしていますが、アクターはそのようなキャンペーンを使用してさまざまな目標を追求できます。国家的アクターの場合、ソフトパワーの概念は、目的を達成するために外交的および文化的資産を使用することを指します。スパイ活動、偽情報/フェイクニュース、ハッキングとともに展開された場合、敵対的なキャンペーンはハイブリッド戦争として特徴付けることができます(assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/840513/20190401-MCDC_CHW_Information_note_-_Conceptual_Foundations.pdf)。

外交活動と外国のセキュリティサービスによる選挙干渉には非常に長い歴史と確立された戦術があります。最近のキャンペーンでは、ソーシャルメディアを使用して、デマと作り話を広めることができます。脅威アクターはAIアシストボットや大勢の人を利用して、アカウントを開いたり、ハッキングしたり、キャンペーンの目的をサポートするメッセージを繰り返したり、強化します。

対象国を全般的にかく乱させるだけでなく、インフルエンスキャンペーンによって、民間企業は偽の話に巻き込まれるため、影響を受ける可能性があります。企業は、ソーシャルメディアで自社への言及を密接に監視し、間違った投稿や誤解するような投稿を修正または削除する対策を講じることが重要です。インフルエンスキャンペーンが検知される場合、公共事業、選挙管理、運輸など重要な産業で事業を行う企業は、警戒態勢を強化すべきです。