ペネトレーションテスト実務者座談会

2018/11/28

Internet Week 2018

D2-3 知れば組織が強くなる！ペネトレーションテストで分かったセキュリティ対策の抜け穴

出演者紹介

- パネリスト
  - 小河 哲之 (三井物産セキュアディレクション株式会社)
  - 北原 憲 (株式会社ラック)
  - 大塚 淳平 (NRIセキュアテクノロジーズ株式会社)
  - サイフィエフ ルスラン (株式会社イエラエセキュリティ)
- モデレータ兼パネリスト
  - 中津留 勇 (SecureWorks Japan 株式会社)

本日のテーマ

- 参加いただいた皆様のセキュリティ対策の一助となることを目的として、ペネトレーションテストで見かけた穴を以下のテーマごとに語ります。

穴だらけの社内システム

人の脆弱性とどう向き合うか

組織としてのインシデント対応

リアルさの追求

穴だらけの社内システム

- 古い OS, アプリケーション
  - 業務に必要だから残すケースなど完璧にアップデートするのは難しい
- 最新の OS であれば良いわけではなく、脆弱な設定を引き継ぐケースがある
  - Windows Server をアップグレードしても LM ハッシュが残る
  - チェックが難しく（マイクロソフトの資料を隅々まで読む）ペネトレで始めて認知するケースがほとんど
- 運用として脆弱なケース（脆弱性を突く必要がない）
  - バッチファイルなどに管理者パスワード
  - PowerShell で暗号化したパスワードをハードコードしているケースは調べればすぐ復号できる
  - 運用系の自動化スクリプトや実行ファイルから取れる
- 保存しているバックアップに認証情報が含まれるケースがあった
  - ブルースクリーン時に作成された Windows のクラッシュダンプを解析して認証情報を取れる場合も
- 社内 Web サービスだと HTTPS になっておらず盗聴ができるケースも
  - HTTPS であっても MITM できる（証明書エラーを気にせず進むユーザが存在）
- 分離・仮想化
  - Web は仮想マシン上でしかアクセスできず、仮想マシン側しか乗っとれないと思いきや同じドメインにいて色々アクセスできたケース
  - 分離のためのフィルタリング不十分なケースがある
  - DNS トンネリングすれば Web 制限も突破できる
    - ホワイトリストで問題が発生した際の対処が容易なように、自由に外に出れるプロキシが別に存在するケースも

人の脆弱性とどう向き合うか

- パスワードの脆さ
  - Active Directory から取得したパスワードを解析
    - 全アカウントの 8割くらいはクラック可能（LM ハッシュならさらに簡単に解析可能）
    - パスワードがユーザ名と一緒のケースや、パスワードに会社名を使う人が多い
  - 定期的変更を強制しているとパスワードが貧弱になりがち
    - password01, password02, password03…
  - 強ければ安心というわけではなく、キーロガーや前述の運用不備などから取得する
- 管理者権限のアカウントと分離していても容易に推測可能なケース
  - bob がいたら admin_bob がいてパスワードが一緒
- メール開封率は高い
  - パッチ適用、マクロ無効化など技術的に対処する必要がある
  - 不審メールとして報告・転送したら管理者が開いてしまうケースも存在
- 分離や二要素認証があったとしても、残っているセッションを使うことで突破可能
  - ランチタイムに操作し立ち上げっぱなしのコンソールを触る、クッキーを取ってきてセッションハイジャック、など
  - セッションを都度切る人はまずいない
- ドアをあけて待ってくれる、知らない人でも声をかけない、など物理侵入は容易なケースがほとんど

組織としての対応

- 使用しているツールを検知されたケースはある
  - 事前に検証して使用するため、検知したとしてもほんの一部のファイルのみ
  - 製品にのみ頼るとまず気付かない
    - いつもと違う動作を不審だと報告できる社員が必要
- 気付けたとしても対応しきれないケースが非常に多い
  - 不審な動作（ツール検知やロックアウトなど）を標的型攻撃と結びつけられない
    - ウイルス対策ソフトで検知しなければ終了
    - 過去にも出たかのチェックなど調査が甘い
  - ツールを使いこなす難しさ
    - ログが多すぎて見ていない、管理コンソールにそもそもログインしていない/週1でしか見ない
  - 調査が手間のかかる作業の場合「やらない」を選択してしまう

リアルさの追求

- 本番環境 vs テスト環境
  - 端末にあるファイルやメールなど本番環境だからこその状況で成否が変わる可能性があるので本番が良い
    - そもそもテスト環境が本番環境と同じバージョン・設定になっていない場合も
  - 本番でもスコープを狭くするケースは評価が十分にできない
    - 各所を経由すれば AD にたどりつけるのにそれが調査できないケースなど
- 内部情報の収集・精査は時間がかかるため、担当者から情報を出してもらえるとスムーズに進む
  - より本質的なことに時間をかけることができる
    - 実施期間が短いペネトレーションテストでは全てを精査すること自体が不可能なため担当者との協力が不可欠

最後に一言

- 本番環境への影響を怖がりすぎる必要はない
  - ロックアウトやウイルス対策ソフト等の検知などが発生する程度で業務が止まるレベルの影響はまず無い
- 攻撃をシミュレーションするツールは中身を知らずに使っても意味がないため、ペネトレーションテスト実務者が効率化で使うのは良い
  - 自社でそれを使ってペネトレーションテストをやったと考えるのは危険
    - 導入するかどうか検討する上でも、一度ペネトレーションテストを受けるのがおすすめ
- 製品を導入するだけでなく、それを使いこなすこと（設定はもちろんログ監視まで）が重要
- USB デバイスの制限をしていても、SafeMode で起動可能な場合には USB 読み込み・書き込みができてしまう可能性がある
- フルディスク暗号化をしていないと、 USB ブートで他の OS を起動してディスクをマウントして情報を取り出せる
- やるならスコープの縮小、テスト環境の使用ではなく本番環境でのペネトレーションテストを圧倒的におすすめしたい
- やってみましょう、ペネトレーションテスト！