情報セキュリティマネジメント試験合格講座 03

- サイバー攻撃手法

1. ブルートフォース攻撃
   総当たり攻撃とも呼ばれる攻撃手法。可能性のある組合せをすべて試すタイプの攻撃手法。

2. パスワードリスト攻撃
   あらかじめ入手したパスワードでリストを作成し、インターネットバンキングへのログインを試行したり、流出した利用者 ID とパスワードのリストを用いて、他の Web サイトに対してログインを試行しようとしたりするアカウントハッキングの手法。

3. 辞書攻撃（Dictionary Attack）
   不正アクセスを行う目的で、辞書に載っている単語を入力してパスワードなどを推測しようとする攻撃手法。

4. レインボーテーブル攻撃（Rainbow Table）
   想定されるパスワードと、そのハッシュ値との対のリストを用いて、入手したハッシュ値からパスワードを効率的に解析しようとする攻撃手法。

5. クロスサイトスクリプティング（Cross Site Scripting）
   複数の Web サイトを利用して攻撃を行う手法で、訪問者の入力データをそのまま画面に表示する Web サイトに対して、悪意のあるスクリプトを埋め込んだ入力データを送り、訪問者のブラウザで実行させる攻撃手法。

6. クロスサイトリクエストフォージェリ（Cross Site Request Forgeries）
   悪意のあるスクリプトが埋め込まれた Web ページを訪問者に閲覧させて、別の Web サイトで、その訪問者が意図しない操作を行わせる攻撃手法。

7. クリックジャッキング（Clickjacking）
   Web ページのコンテンツ上に透明化した標的サイトのコンテンツを配置し、利用者が気づかないうちに標的サイト上で不正操作を実行させる攻撃手法。

8. ドライブバイダウンロード（Drive by Download）
   Web サイトを閲覧したとき、利用者が気付かないうちに、利用者の意図にかかわらず、利用者の PC に不正プログラムが転送される攻撃手法。

9. SQL インジェクション（SQL Injection）
   Web アプリケーションに問題があるとき、データベースに悪意のある問合せや操作を行う命令文を入力して、データベースのデータを改ざんしたり不正に取得したりする攻撃手法。

10. ディレクトリトラバーサル（Directory Traversal）
    管理者が意図していないパスでサーバ内のファイルを指定することによって、本来は許されないファイルを不正に閲覧しようとする攻撃手法。

11. 中間者攻撃（Man in the Middle）
    通信を行う二者の間に割り込んで、両者が交換する情報を自分のものとすり替えることによって、気付かれることなく盗聴しようとする攻撃手法。インターネットバンキングの正規サイトに見せかけた中継サイトに接続させ、Web ブラウザから入力された利用者 ID とパスワードを正規サイトに転送し、利用者になりすましてログインする例などがある。

12. 第三者中継(Third Party Mail Relay)
    メールサーバに関係の無い第三者が自由に、電子メール送信に用いる事が可能なメールサーバの設定や状態。

13. サイドチャネル攻撃
    暗号アルゴリズムを実装した攻撃対象の物理デバイスから得られる処理時間や消費電流などの情報やエラーメッセージなどから、攻撃対象の機密情報を得ようとする攻撃手法。

14. IP スプーフィング
    偽の送信元 IP アドレスをもったパケットを送る攻撃手法。外部から入るパケットの送信元 IP アドレスが自ネットワークのものであれば、そのパケットを破棄する対策が必要。

15. キャッシュポイズニング（DNS Cache Poisoning）
DNS（Domain Name System）キャッシュサーバに対して偽の DNS 情報をキャッシュとして登録させることで、利用者を偽の Web サイトに誘導しようとする攻撃手法。

16. セッションハイジャック
セッション ID によってセッションが管理されるとき、ログイン中の利用者のセッション ID を不正に取得し、その利用者になりすましてサーバにアクセスしようとする攻撃手法。

17. リプレイ攻撃
盗聴者が、正当な利用者のログインシーケンスをそのまま記録してサーバに送信して不正アクセスを行う攻撃手法。

18. DoS 攻撃
大量のアクセスを集中させるなどの手法でサービスを不能にしようとする攻撃。このうち、EDoS 攻撃（Economic Denial of Service attack）は、クラウド利用企業の経済的な損失を目的に、リソースを大量消費させようとする攻撃手法。

19. SYN Flood 攻撃
DoS 攻撃のひとつ。TCP 接続において最初に送られるパケットに立てられるフラグである SYN パケットを大量に送り付ける攻撃手法。Flood は洪水という意味。

20. Smurf 攻撃
DoS 攻撃のひとつ。ネットワークが通じているか否かを確認する ping コマンドを使って送信元を偽装した大量のパケットを送ってサービスを不能にしようとする攻撃手法。

21. DDoS 攻撃（Distributed Denial of Service Attack）
DoS 攻撃のひとつで、分散型サービス妨害攻撃。複数のネットワークの複数の端末からから DoS 攻撃を行う攻撃手法。

22. メールボム（E-Mail Bomb）
サイズの大きい電子メールや大量の電子メールを送り付ける手法。大量送信されたメールにより、メールサーバの処理能力が飽和し、DoS 攻撃のようにサービス提供が不能な状態に陥る場合がある迷惑行為。

23. 標的型攻撃（APT、Advanced Persistent Threats）
攻撃者は特定の目的をもち、特定組織を標的に複数の手法を組み合わせて気付かれないよう執拗に攻撃を繰り返す手法。

24. 水飲み場型攻撃（Watering Hole Attack）
標的組織の従業員が頻繁にアクセスするWebサイトに攻撃コードを埋め込み、標的組織の従業員がアクセスしたときだけ攻撃が行われるようにする攻撃手法。

25. ワンクリック詐欺
アクセスするとすぐにPCや携帯端末の画面に料金請求の画面が表示され、不当に料金を請求しようとする手法。

26. スミッシング（Smishing）
携帯端末で用いられるショートメッセージサービス（SMS）に、企業や銀行などを装って偽のメッセージを送り、特定のサイトへ誘導したり、不正な課金をしようとしたりする攻撃手法。

27. ゼロデイ攻撃
セキュリティの脆弱性に対する対策がとられる日より前に攻撃しようとする攻撃手法。

28. テンペスト攻撃（Tempest Attack）
処理中に機器から放射される微弱な電磁波を観測し、解析することで、元の情報を再現しようとする攻撃手法。

29. ウォードライビング（War Driving）
建物の外部に漏れた無線LANの電波を傍受して、セキュリティの設定が脆弱な無線LANのアクセスポイントを見つけ出そうとする手法。

〔問題集〕

- ✓ 石川敢也（共著）「情報セキュリティマネジメント要点整理＆予想問題集」 翔泳社
- ✓ 情報セキュリティマネジメント試験合格講座 http://rakupass.com/security/