

- サイバー攻撃手法

1. 〔ブル〕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〕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〕
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〕
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. 〔クジグ〕
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。

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ID]
セッションIDによってセッションが管理される時、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. [リクエスト 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 (Denial of Service Attack)
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、[SYN DoS 攻撃]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 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. [ICMP 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 DoS 攻撃]
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. [_____ 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で気付かれないよう執拗に攻撃を繰り返す手法。
24. [_____ 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する攻撃手法。
27. [_____ 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. [_____ 攻撃]
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/>

