

帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

情報セキュリティ論(7)
セキュリティの層

中野秀男
情報メディア学科/ICTセンター長

1 情報セキュリティ論 セキュリティの層 2016/6/3

今日の話

- ▶ セキュリティ全般を改めて俯瞰してみる
- ▶ セキュリティの層
 - ▶ 中野なりに分類
 - ▶ セキュリティの体系化の必要性
- ▶ 物理セキュリティ
 - ▶ ソーシャルエンジニアリング
 - ▶ 次回のソーシャルアタックは標的型攻撃を中心に
- ▶ TCP/IPセキュリティ
- ▶ 残る層は簡単に

▶ 2 情報セキュリティ論 セキュリティの層 2016/6/3 帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


セキュリティの層(ネットワーク層のOSIをまねて)

- ▶ 1層: 物理的なセキュリティ
- ▶ 2層: 1つのネットワークでのセキュリティ
- ▶ 3層: コンピュータ間のセキュリティ
- ▶ 4層: プログラム間で共通なセキュリティ
- ▶ 5層: セッション毎のセキュリティ
- ▶ 6層: 文字列、画像等のセキュリティ
- ▶ 7層: 特定のプログラム間のセキュリティ

▶ 3 情報セキュリティ論 セキュリティの層 2016/6/3 帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


他の層のセキュリティ

- ▶ ネットワーク層セキュリティ
 - ▶ 各ネットワークでのセキュリティ:電話網、無線
- ▶ セッション層のセキュリティ
 - ▶ ログイン/ログオン
- ▶ プレゼンテーション層のセキュリティ
 - ▶ 文章、画像、音声、動画のセキュリティ等
- ▶ アプリケーション層のセキュリティ
 - ▶ メール、ウェブ
- ▶ それ以外では
 - ▶ クラウドアプリのセキュリティ
 - ▶ ソーシャルメディアのセキュリティ

▶ 4 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


セキュリティの物理層

- ▶ セキュリティの物理層
- ▶ 最近ではソーシャル(エンジニアリング/アタック)
 - ▶ 環境
 - ▶ 破壊欲
 - ▶ 盗聴
- ▶ 人的なセキュリティ
 - ▶ ログアウトせずに離席
 - ▶ サーバ室の入退室管理(鍵、カメラ、記録等)
 - ▶ アクセス可能な情報機器の配置
- ▶ 過失か犯罪か

▶ 5 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


物理的なセキュリティ(環境)

- ▶ 火災・煙・ほこり(ファン)
- ▶ 地震(阪神淡路大震災)
- ▶ 爆発(阪大爆発事件)
- ▶ 温度の上昇と下降(霜)
- ▶ 虫(小さな虫)
- ▶ 電気ノイズ(電源ON/OFF)
- ▶ 雷(廊下にイーサネット)
- ▶ 湿気・水(コーヒー)・飲食物(煎餅等)

▶ 6 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


物理的なセキュリティ(盗聴/破壊)

- ▶ 盗聴
 - ▶ ワイヤによる盗聴(passive,active)
 - ▶ イーサネットでの盗聴
 - ▶ 対策:Secure IP(暗号化)
 - ▶ 無線による盗聴
 - ▶ 端末の補助ポート
 - ▶ 電磁波漏れ
 - ▶ ディスプレー、プリンタケーブル
- ▶ 破壊
 - ▶ ネットワークケーブル/コネクター
 - ▶ 部屋の無断侵入
 - ▶ 機器の持ち出し

▶ 7 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


ソーシャルアタック

- ▶ ショルダーアタック
 - ▶ パスワードや暗証番号やスマホのパスコードの覗き見
- ▶ 偽の電話やメール(標的型メール)
 - ▶ 個人情報を知る
- ▶ ソーシャルエンジニアリング
 - ▶ 情報収集
 - ▶ 誘導質問
 - ▶ 誰かになりすます
 - ▶ 心のトリック
 - ▶ マイクロ表情
 - ▶ 感化—説得の力

▶ 8 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


IP/TCP層におけるセキュリティ

- ▶ Ping of Death(大きなPINGパケット)
- ▶ ネットワーク・スヌーピング(覗き見)
- ▶ メッセージ応答を記録して後から不正使用
- ▶ メッセージ変更
- ▶ メッセージ遅延と拒否
- ▶ アドレス・マスカレーディング
- ▶ ルーティング攻撃

▶ 9 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


セキュリティ用語Web

- ▶ IPA
 - ▶ http://www.ipa.go.jp/security/ciadr/word_idx.html
- ▶ e-Word:IT用語辞典
 - ▶ <http://e-words.jp/p/t-Security.html>
- ▶ Wikipedia

▶ 10 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY


Spoofing

- ▶ 別のマシンになります
- ▶ IP spoofing attack
- ▶ Hardware Address Spoofing
 - ▶ MAC Addressの書き換え
- ▶ ARP Spoofing
- ▶ ICMP Spoofing: ping sweep
 - ▶ ICMP flooding攻撃
- ▶ 経路Spoofing
- ▶ DNS Spoofing
- ▶ TCP Connection Spoofing
 - ▶ Session Hijacking

▶ 11 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

DoS

- ▶ Denial of Service: サービス不能攻撃
- ▶ 種類
 - ▶ ネットワーク帯域の消費
 - ▶ リソースの枯渇
 - ▶ プログラミングの欠陥
 - ▶ 経路制御DoS攻撃
 - ▶ DNS DoS攻撃
 - ▶ DDoS攻撃
- ▶ さまざまなDoS攻撃
 - ▶ SYN flood攻撃
 - ▶ Smurf攻撃: ping broadcast
 - ▶ Buffer Overflow

▶ 12 情報セキュリティ論 セキュリティの層 2016/6/3  帝塚山学院大学
TEZUKAYAMA GAKUIN UNIVERSITY

今週のミニレポート

- ▶ 物理層のセキュリティで実際にみなさんの周りであったこととか、ありそうなことがあれば書いてください。
- ▶ 指定した中野のメールアドレスに6月16日までに送る。
