FUJITSU
shaping tomorrow with you

第1章
近年のセキュリティ情勢

1.1 インシデント事例
1.2 インシデントの影響
1.3 被害の影響
1.4 サイバー攻撃の背景・傾向の変化

FUJITSU
shaping tomorrow with you

第2章
偵察による情報収集

2.1 前提知識
(1) 各種サーバー役割
(2) TCPとUDP
(3) プロトコルとポート番号

2.2 プロファイリング

2.3 ターゲッティング
(1) 標的な決定
(2) 標的によってプロファイリングで収集する情報

2.4 フットプリンティング
(1) 公開Webサイトでの情報収集
(2) SNS・ブログ・掲示板での情報収集
(3) DNSでの情報収集
(4) 検索サイトハッキング

2.5 スキャニング
(1) pingスイープ
(2) ポートスキャン
(3)フィンガープリンティング

2.6 【参考】探索行為の件数の推移

2.7 〈演習〉スキャニング

2.8 インターネット接続機器検索サービス

2.9 〈演習〉インターネット接続機器検索サービス利用

FUJITSU
shaping tomorrow with you

第3章
サービスを妨害する攻撃

3.1 サービス妨害攻撃の概要
(1) サービス妨害の背景
(2) サービス妨害攻撃の形態
(3) DoS攻撃とは

3.2 代表的な攻撃手口
(1) SYN Flood攻撃
(2) Smurf攻撃
(3) Slow HTTP Heade攻撃
(4) Slow HTTP POS攻撃
(5) Slow Read Dos攻撃
(6) DNSリフレクター攻撃
(7) NYPリフレクター攻撃

3.3 〈演習〉サービス妨害攻撃

FUJITSU
shaping tomorrow with you

第4章
アカウントを窃取する攻撃

4.1 アカウント窃取の概要

4.2 アカウントと認証
(1) アカウントの種類と権限
(2) 認証の仕組み

4.3 代表的なパスワードクラックの手口
(1) 総当たり攻撃(bruteforce attack)
(2) 辞書攻撃(dictionary attack)
(3) パスワードリスト攻撃(list based attack)

4.4 〈演習〉WordPressのアカウント窃取

4.5 〈演習〉SSHサービスのアカウント窃取

4.6 フィッシング

4.7 スミッシング

4.8 フィッシングの被害

4.9 〈演習〉フィッシングサイトからのアカウント窃取

FUJITSU
shaping tomorrow with you

第5章
ソフトウェアの脆弱性に対する攻撃

5.1 ソフトウェアの脆弱性による問題

5.2 代表的なソフトウェアの脆弱性を突いた攻撃
(1) バッファーオーバーフロー
(2) Heartbleed
(3) ShellShock

5.3 〈演習〉ShellShockを悪用した遠隔操作

FUJITSU
shaping tomorrow with you

第6章
Webアプリケーションに対する攻撃

6.1 代表的な攻撃手口
(1) SQLインジェクション
(2) 〈演習〉SQLインジェクション
(3) OSコマンドインジェクション
(4) 〈演習〉OSコマンドインジェクション
(5) クロスサイトクリプティング
(6) 〈演習〉クロスサイトスクリプティング
(7) クロスサイトリクエストフォージェリ

6.2 【参考】OWASP Top10

6.3 〈演習〉OWASP ZAP

FUJITSU
shaping tomorrow with you

第7章
不正アクセス

7.1 不正アクセスとは

7.2 【参考】不正アクセス禁止法違反の検挙状況の推移

7.3 機密情報の窃取

7.4 〈演習〉Apache Struts2の脆弱性を悪用した遠隔操作

7.5 Webサイトの改ざん

7.6 ＜演習＞ WordPressの脆弱性を悪用したWebサイトの改ざん

7.7 踏み台化

FUJITSU
shaping tomorrow with you

第8章
標的型攻撃

8.1　漂的型攻撃の流れ

8.2　初期潜入フェーズ
(1) ソーシャルエンジニアリング
(2) 標的型メール攻撃
(3) 水飲み場攻撃

8.3　攻撃基盤構築フェーズ
(1) コネクトバック通信
(2) 【参考】侵入拡大のために攻撃者がよく利用するコマンド
(3) 【参考】侵入拡大のために攻撃者がよく悪用するツール
(4) Pass the Hash
(5) SMB共有の悪用

8.4　目的遂行フェーズ

8.5　〈演習〉標的型メール攻撃による遠隔操作

8.6　【参考】ランサムウェア

8.7　＜演習＞ランサムウェア感染