impress
An impress Group Company

第1章　ハッキングに向けた準備

1.1　宅内監視システム（ネットワークカメラ）

1　一般的な宅内監視システムの仕組み

2　想定される宅内監視システムへの攻撃

1.2　守るべき資産（攻撃者が狙う資産）

1.3　攻撃者の攻撃ポイント

1　一連のハッキング手順

2　アタックサーフェースにおける攻撃ポイント

3　システムの通信経路における攻撃ポイント

1.4　想定される脅威分析

1.5　宅内監視システムへの攻撃のまとめ

第2章　実践ハッキング　ステップ1：ハードウェアハッキングとファームウェア解析

ハッキング手順の整理

2.1　ハードウェアの情報収集

1　概要

2　基板上のチップやシルクの調査・分析

2.2　デバッグインタフェース（UART、JTAG）の特定とアクセス可否の確認

1　概要

2　デバッグインタフェースの特定と挙動確認

2.3　デバッグインタフェースからのファームウェア抽出

1　概要

2　UARTインタフェース経由でのファームウェアの抽出

2.4　ファームウェア解析

1　概要

2　ファームウェアイメージファイルの解析

【コラム1】JTAG（Joint Test Action Group）

第3章　実践ハッキング　ステップ2：バイナリー解析

3.1　バイナリー解析とバッファオーバーフロー脆弱性の特定

1　概要

2　バイナリー解析によるバッファオーバーフロー脆弱性の特定

〔1〕バイナリーコードのディスアセンブル

〔2〕「dnsmasqバージョン2.78」におけるバッファオーバーフロー脆弱性

3.2　シンボリック実行を利用したバイナリー解析

1　概要

2　シンボリック実行による任意の処理への入力データの特定

3.3　APKファイルのデコンパイル
1　概要
2　APKファイルのデコンパイル
【コラム2】バッファオーバーフロー脆弱性とは？

第4章　実践ハッキング ステップ3：既知脆弱性の診断
4.1　ソフトウェアBOM（SBOM）の作成と脆弱性スキャン
1　概要
2　ソフトウェアBOM（SBOM）の作成および解析
4.2　ネットワーク経由による脆弱性スキャン
1　概要
2　ネットワーク経由の脆弱性スキャンによる検証例
4.3　エクスプロイト：脆弱性への攻撃
1　概要
2　脆弱性スキャンレポートをもとにした脆弱性のエクスプロイト
3　Bluetoothの脆弱性のPoCを利用したエクスプロイト
4.4　ハードコーディングパスワードの調査
1　概要
2　ネットワークカメラのハードコーディングパスワードの調査
4.5　パスワードファイルの解析
1　概要
2　辞書攻撃によるパスワードファイルの解析
4.6　ネットワークサービスのパスワード解析
1　概要
2　辞書攻撃・オンライン攻撃によるパスワードクラック

第5章　実践ハッキング ステップ4：ファジングテスト
5.1　ファイルフォーマットおよびネットワークプロトコルベースのファジング手法
1　概要
2　HTTPサーバへのファジング
3　脆弱なプログラムへのファジング
5.2　コード網羅率を指標とするファジング手法
1　概要
2　コード網羅率を指標とするファジング

第6章　実践ハッキング ステップ5：ネットワーク内調査
6.1　ネットワークポートスキャン

1　概要
2　ネットワークポートスキャンの実行

第7章　実践ハッキング ステップ6：キャプチャデータ分析

7.1　Ethernet：パケットキャプチャ
1　概要
2　ネットワークパケットキャプチャ
7.2　Bluetooth：パケットキャプチャ
1　概要
7.3　アプリケーション通信のパケットキャプチャ
1　概要
2　HTTPアプリケーション通信のキャプチャ

まとめ：ハッキング手法と対策