

インターネットソフトウェア report

155702F 大城由也

2017/8/24

講義の内容

インターネットシステムの基礎知識

主な内容:インターネットの変遷や、そこに関する装置・技術の概要の解説。

- OSI7 階層モデル
- インターネットはの packets 交換は IP ルーティングとスイッチングによって実現している。
- IP ルーティングを実現しているのはルーター。
- スwitchingを実現しているのはスwitchingハブ。
- サーバシステムは OS とサーバアプリケーションで構成。
- OS は基本機能を提供。高次元のサービスは提供しない。
- アプリケーションは OS の基本機能を利用して高次元のサービスを提供。
- セキュリティの実装法はネットワークシステムベースとサーバシステムベースの 2 種類ある。
- ネットワークシステムベースのセキュリティは、「攻撃が来る前に防ぐ」方法であり、アクセスフィルタや UTM の導入などが具体例である。
- サーバシステムベースのセキュリティは、「攻撃が来た時に防ぐ」方法であり、セキュリティ対策ソフトの導入やアクセス制御などが具体例である。

TCP/IP プログラミング演習 (C 言語)

主な内容:ソケットを用いた packets 通信をプログラミングで実装。

取り組んだ課題は「SMTP クライアントの作成」。メールサーバを使用し、自身のアドレスや用意されたアドレスにメールを送信するプログラムの作成を行った。

リンク先の Git リポジトリに作成したプログラムのソースコードを掲載した。

<https://github.com/ooshirooo/internetsoftware/blob/master/821/smtplib.c>

スitchネットワーク構築演習

情報工学実験 II で学習済みのため欠席

セキュリティ演習 (OS&サーバ編)

主な内容:VM を構築し、セキュリティ設定を行った。

行った内容は以下の 5 つ。

- ポート番号を確認して、不要なサービスに対し停止措置・ファイアウォールの設定を行う。
- 一般ユーザーへの root 権限での実行の許可設定。
- root ユーザー、パスワードなしユーザーのアクセス制限。
- 鍵認証の設定、鍵認証のみでアクセスできるような制限の設定。
- アクセス可能ユーザーの制限。

セキュリティ演習 (ツール編)

主な内容:セキュリティチェックツール (Nmap, tcpdump, Wireshark) を使用したポートスキャン、パケットキャプチャを学んだ。

Nmap はポートスキャンを行うツールであり、対象の OS やサーバーアプリケーションの種類、バージョンを調査可能。これを使用すれば、使用しているディストリビューションの状態が明らかになるのと同時に脆弱性も判明する。

tcpdump はパケットキャプチャを行うツールであり、パケットキャプチャを行うことで他人の通信パケットから情報の奪取が行える。奪取された情報はなりすましなどをする際に悪用される。

Wireshark はパケットキャプチャ機能に加え、プロトコル解析機能も有する。この機能により、実際にどのような内容の通信が行われていたのかをより具体的に知ることができる。

講義で得られたこと、今後取り上げて欲しい内容、感想

今回の講義では、VM の構築方法 (OS で行った時は理解できていない部分が多々あった) と、構築した VM に対するセキュリティ設定、セキュリティチェックを行う際使用するツールの使い方を新たに学んだ。もう一度自身で一から VM を構築してみたいと興味が湧いたので、さらに学習していきたい。

時間があれば他のポートで展開されているサービスに関しても学習してみたかった (特に DNS)。

教わる内容が多かったので、得るものも多かった。特に、インターネットの分野に興味が湧いたのは大きい収穫だと思う。将来就きたい職種はインターネットとは切り離せないので、モチベーションがあるうちに色々学ぼうと思う。