奈良高専

情報工学実験 II
第5章 サイバーセキュリティ基礎実験2

#1

November 16, 2018

目的

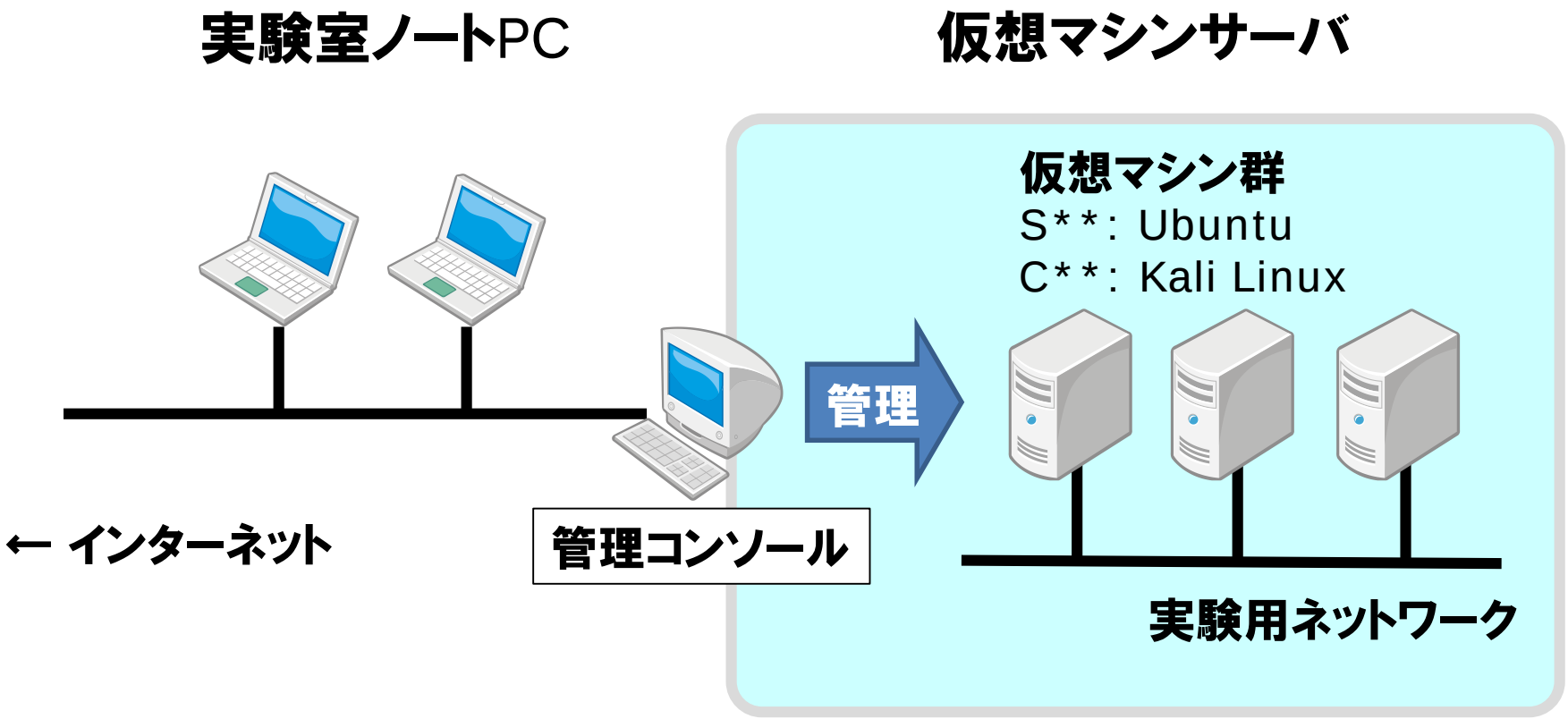
- サイバーセキュリティ基礎実験1で検討した対策が、実際にはどの程度の効力があるのかを調べる。
  - 自班で検討したものだけでなく、他班が検討したものを対象としてもよい
- ネットワーク盗聴に用いられる手法の一つであるARPスプーフィングについて、原理を理解し、対策を検討する。

スケジュール

奈良高専

2018年11月16日(金)	第1回	
2018年11月22日(木)	第2回	金曜振替授業
2018年11月30日(金)	後期中間試験	
2018年12月7日(金)	第3回	
2018年12月14日(金)	第4回	
2018年12月21日(金)	第5回	成果発表会
2019年1月11日(金)	（第6章 第1回）	レポート提出

実験環境(再掲)


実験室ノートPC
仮想マシンサーバ
仮想マシン群
S**: Ubuntu
C**: Kali Linux
管理
← インターネット
管理コンソール
実験用ネットワーク

各班のアドレス（再掲）

奈良高専

	ネットワークアドレス	割り当て可能なアドレス
1班	10.1.0.0/16	10.1.0.1～10.1.255.254
2班	10.2.0.0/16	10.2.0.1～10.2.255.254
3班	10.3.0.0/16	10.3.0.1～10.3.255.254
4班	10.4.0.0/16	10.4.0.1～10.4.255.254
5班	10.5.0.0/16	10.5.0.1～10.5.255.254
6班	10.6.0.0/16	10.6.0.1～10.6.255.254

ネットマスクは255.255.0.0、**ゲートウェイの設定は不要**

注意事項(再掲)

奈良高専

- 実験(パケットの観測など)は実験用ネットワーク内でのみ行うこと。
- 実験用ネットワークの外へ攻撃を加えないこと。
- 仮想マシン上にあるuser以外の既存のアカウントには変更を加えないこと。
- 実験時間外のチェックは行いません。
- 仮想マシンサーバは、実験時間外はメンテナンスのため使用できない場合があります。
- **技術や知識を悪用しないこと。**
  (「できること」と「やっていいこと」は違う)

実験課題1

1. OpenSSLにおける公開鍵証明書の作成手順を調べよ。
2. OpenSSLを用いて公開鍵証明書を作成し、作成した公開鍵証明書の内容を確認せよ。

［証明書の仕様］

公開鍵：RSA2048ビット

サブジェクトのCN(Common Name)：自分の名前

有効期間：365日

これ以外の仕様は自由に決めてよい。なお、通常は認証局によって公開鍵証明書が作成されるが、ここでは、自身の秘密鍵による署名（自己署名証明書）で構わない（認証局も構築できればなお良い）。

※ 内容を確認するのは作成した公開鍵証明書であり、CSR (Certificate Signing Request)ではないことに注意せよ。

実験課題2

奈良高専

1. TLS1.2による通信を行うWebサーバを構築せよ。
2. TLS1.2による通信をWiresharkを用いて観測し、どのようなやりとりがされているかを確認せよ。
3. 2.で観測した通信と、サイバーセキュリティ基礎実験1の課題3で観測した通信(HTTPおよびその前後の通信)を比較し、その違いを説明せよ。
4. TLS1.2による通信を行うWebサーバに対してGETメソッドを用いてデータを送信した場合およびPOSTメソッドを用いてデータを送信した場合の通信をそれぞれ観測し、サイバーセキュリティ基礎実験1の課題4で観測した通信との違いを説明せよ。

実験課題3

奈良高専

1. Webサーバの一部のディレクトリに対して、Basic認証を用いたアクセス制限を行うように設定せよ。
2. 1.でアクセス制限を行ったディレクトリに対してHTTPおよびTLSで通信し、それぞれの通信をWiresharkを用いて観測せよ。
3. Webサーバの一部のディレクトリに対して、Digest認証を用いたアクセス制限を行うように設定せよ。
4. 3.でアクセス制限を行ったディレクトリに対してHTTPおよびTLSで通信し、それぞれの通信をWiresharkを用いて観測せよ。
5. 2.で観測した通信と4.で観測した通信を比較し、その違いを説明せよ。
6. 【任意課題】Webサーバの一部のディレクトリに対してTLSのクライアント認証を用いたアクセス制限を行うように設定せよ。

実験課題4

1. ARPテーブルの内容を表示し、どのような情報が含まれているかを確認せよ。
2. arpspoofによる通信をWiresharkを用いて観測し、arpspoofがどのようにしてARPスプーフィングを実現しようとしているかを説明せよ。また、arpspoofの実行前後のARPテーブルの内容を比較して、ARPスプーフィングが成功したか否かを確認せよ。

検討課題

1. サイバーセキュリティ基礎実験1で検討した対策が、実際にはどの程度の効力があるのかを検討せよ。
   - 対策を実施する上での注意点は？
   - 常時SSL/TLSの必要性と注意点は？

2. ARPスプーフィングが成功した場合に起こり得る問題と、その対策について、実験結果に基づいて論ぜよ。
   - arpspoofを使うことで、他のPCになりすましたり、本来の通信相手とは別のPCへ誘導することは可能か？
   - sshmitmやwebmitmなどを用いた盗聴は可能か？
   - 攻撃が成功/失敗する条件は？

成果発表会、レポート

奈良高専

- 成果発表会
  - 各班発表10分、質疑応答10分
  - 主な内容
    - サイバーセキュリティ基礎実験1で検討した対策が、実際にはどの程度の効力があるのか
    - ARPスプーフィングの脅威と対策
  - 発表内容については班の中で議論し、責任を持って発表を行うこと。
- レポート
  - 実験した内容と結果（これまでのレポートと同様）
  - 自身の班内での役割、貢献、反省点など
  - 成果発表会で受けた質問および回答
  - 成果発表会でした質問および回答