Vol.2022-IOT-56 No.45
2022/3/8

オンライン授業で行うセキュリティ教育における ペネトレーションテスト演習の実践と評価

鈴木大助 [1]

概要：本研究の目的は，学部生を対象とする情報セキュリティ教育の一環として，ペネトレーションテスト演習をオンライン授業で実施可能な形で提案・実践し，その教育効果を明らかにすることである．ペネトレーションテスト演習は，受講生各自が保有する PC に実験用仮想環境を構築して行うこととし，全体で 90 分授業 3 コマ分とした．講義動画はオンデマンドで公開し，質問対応には学習管理システムやチャットツールを利用した．趣旨説明・法令遵守・実験環境構築で 2 コマ分とし，講義動画は 8 本（合計 77 分）用意した．3 コマ目は，構築した仮想実験環境でポートスキャン・脆弱性検査・脆弱性攻撃からなるペネトレーションテストを行う内容とし，講義動画は 4 本（合計 57 分）用意した．演習の進捗状況アンケートおよび演習のふりかえりアンケートの結果から，受講生の大半が各自の PC に実験用仮想環境を構築し，各種ソフトウェアやコマンドを利用してペネトレーションテスト演習を完遂することができた．また，この体験を通じて攻撃者の視点や攻撃手法を知り，サイバー攻撃の脅威をより身近に感じた結果，情報セキュリティの重要性を意識するようになったこと，情報セキュリティに対して興味・関心を抱いたことが確認された．ペネトレーションテスト演習は，オンライン授業かつ各自の PC に仮想環境を構築して実施するという条件下でも，十分に実践可能であり，情報セキュリティに対する興味関心を喚起できると言える．

キーワード：情報セキュリティ教育，ペネトレーションテスト，倫理的ハッキング，オンライン授業

Practice and Evaluation of a Penetration Testing Exercise in Security Education Conducted Through Online Learning

DAISUKE SUZUKI[†1]

Keywords: Information security education, penetration testing, ethical hacking, online learning

1. はじめに

個人・組織を対象とするさまざまなサイバー攻撃とその被害が観測・報道される昨今[1][2]，情報資産を脅威から守るため，業種・職種を問わず，すべての社会人は情報セキュリティについて学び，情報セキュリティについて意識する必要がある．大学は社会・組織に人材を送り出す教育機関として，文理問わずすべての学生に情報セキュリティ教育を実施することが求められる．

筆者は，大学学部生を対象とする情報セキュリティ教育に模擬的なサイバー攻撃演習（ペネトレーションテスト演習）の体験を取り入れることで，受講生が攻撃者の視点を知り，情報セキュリティに対する興味・関心が向上することを明らかにした[3]．しかし，これは教室に集合して行う通常授業における結果である．大学の教室に PC やサーバをあらかじめ用意し，受講生に対して直接対面で指導する機会があったからこそ実践可能かつ効果が見られたという可能性もある．

2020 年度以降，新型コロナウイルスの感染が収束しない状況を受けて，各大学ではオンライン授業を取り入れ，教育の継続を可能としながら，効果的な遠隔教育を模索してきた[4]．オンライン授業はいまやごく当たり前に行われており，教室授業よりも学生満足度が高かったといった報告もある[5]．

しかし，遠隔授業において 9 割以上の大学が最も課題を感じていたのは「実験・実習・実技系科目への対応」であり[6], 2021 年度調査でもなお 6 割を超える大学が課題を感じている[7]．実験・実習・実技に関しては引き続き，より教育効果の高い実践を目指して，教育手法の開発と共有が必要である．

ペネトレーションテスト演習を取り入れた情報セキュリティ教育はオンライン授業でも実践可能であろうか．また，実践可能であったとして教室授業と同様に情報セキュリティに対する興味・関心を喚起できるであろうか．本研究の目的は，ペネトレーションテスト演習をオンライン授業として実施可能な形で提案・実践し，その教育効果を明らかにすることである．

2. 科目全体像とペネトレーションテスト演習

2.1 科目の全体像

ペネトレーションテスト演習は 2021 年度北陸大学経済経営学部 3 年後期選択科目「情報通信ネットワークⅡ」の一部として行った．授業日程を表 1 に示す．

1 北陸大学
Hokuriku University

ⓒ2022 Information Processing Society of Japan

表 1　2021 年度「情報通信ネットワークⅡ」授業日程

授業回	テーマ
1	導入／前期の復習
2,3,4	スイッチ
5,6.7	VLAN
8	ACL
9	DHCP
10,11	NAT
12,13,14	ペネトレーションテスト演習
15	小テスト／まとめ

第 2 回から第 11 回までは，Cisco Packet Tracer を用いたネットワーク構築演習である．スイッチに関しては VLAN，ルータに関しては ACL や NAT など，ネットワークのセキュリティを確保するための技術について学んでいる．第 12 回から第 14 回の 3 回でペネトレーションテスト演習を実施する．演習の詳細については後述する．

2021 年度の「情報通信ネットワークⅡ」の実履修者数は 34 名（うち 7 名は未入国留学生）であった．受講生の大多数は，3 年生前期選択科目「情報通信ネットワークⅠ」を受講しており，TCP/IP ネットワークの基礎概念の学習，Wireshark[8]を用いたパケットキャプチャ演習，Cisco Packet Tracer[9]でルータを用いたネットワーク構築演習を経験している．なお，「情報通信ネットワークⅠ・Ⅱ」ともすべてオンライン授業で行った．

2.2 オンライン授業の方法（2021 年度）

2021 年度「情報通信ネットワークⅡ」オンライン授業の授業サイクルを図 1 に示す．

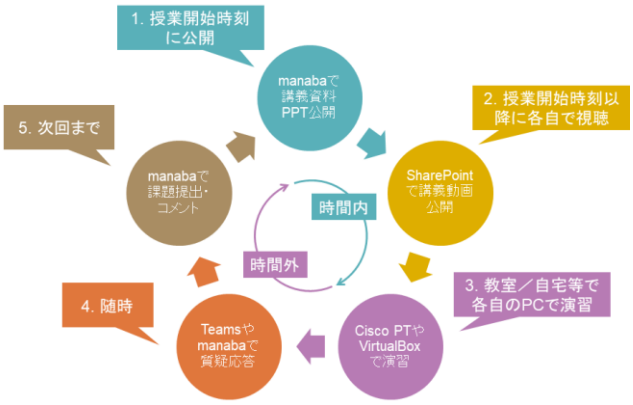


図 1　「情報通信ネットワークⅡ」オンライン授業

PowerPoint で作成した授業資料を授業開始時刻と同時に本学の学習管理システムである manaba[10]で公開する．同時に，録画した講義動画を Microsoft 365 SharePoint[11]で公開し，受講生がいつでも視聴できるようにしている．なお，本学では Google Workspace for Education[12]も利用可能ではあるが，未入国の中国人留学生がアクセスできないため Microsoft 365 SharePoint を利用することにしている．

時間割上の授業時間は各自で講義動画を視聴し，課題に取り組みながら Microsoft Teams[13]や manaba を通じて質問・相談を行う時間と位置付けている．受講生は，第 1 回から第 11 回のネットワーク構築演習の課題については，自分の PC にインストールした Cisco Packet Tracer を利用して取り組む．第 12 回から第 14 回のペネトレーションテスト演習の課題については，Oracle VM VirtualBox[14]を用いて各自の PC に構築した実験用仮想環境を利用して取り組む．

課題を完成した受講生には，その証拠として実行結果のスクリーンショット等を提出するよう求めた．提出期限は次回授業開始時刻としているが，早くに提出があったものや質問が寄せられたものに関してはチェックを行い，個別にフィードバックを行った．授業の出席管理は manaba を利用して提出されたミニッツペーパーで行った．以上が全体的なオンライン授業の進め方である．

次節から，ペネトレーションテスト演習の詳細について説明する．なお，本演習は筆者[3]の演習を基礎にしているため，以降の演習手順の説明において一部重複するところはあるが，本論文のみで内容を了解できるようにするため，重複を厭わず記述している．

2.3 ペネトレーションテスト演習の目的と概要

ペネトレーションテスト演習は，脆弱性を利用したサーバ侵入等の攻撃を行う体験を通じて，攻撃者の行動を知り，情報セキュリティに対する興味・関心を喚起することを目的とする．90 分を 1 回として，3 回からなる授業構成とした．最初の 2 回で実験の趣旨説明，実験用仮想環境の構築，法令順守誓約書の提出を行い，第 3 回で仮想環境におけるペネトレーションテスト演習とそのふりかえりを行った．

2.4 実験用仮想環境の構築

ペネトレーションテスト演習では攻撃役マシンと脆弱性を持った被害役マシンが必要であるが，脆弱性を持ったマシンは外部ネットワークから切り離した環境で扱う必要がある．そこで，実験用仮想環境を受講生各自の PC に構築してもらい，その中で実験を行うこととした．構築する実験用仮想環境の模式図を図 2 に示す．

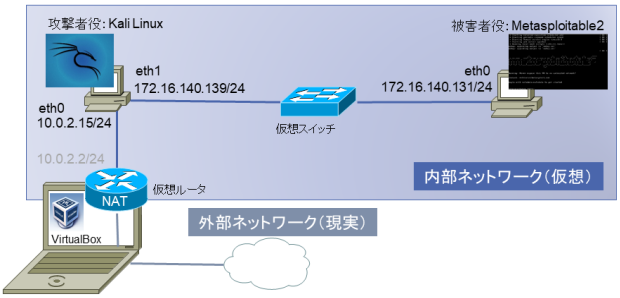


図 2　実験用仮想環境

受講生は各自のノート PC に仮想化ソフト（Oracle VM VirtualBox）をインストールする．仮想環境内に攻撃役ホストとして Kali Linux[15]を，被害役ホストとして Metasploitable2[16]を設置し，それぞれ内部ネットワークで相互に接続する．例では，攻撃役ホストを 172.16.140.139/24，被害役ホストを 172.16.140.131/24 としている．攻撃役ホストである Kali Linux は仮想ルータを通じて外部ネットワーク（ホスト OS の所属するネットワーク）とも通信できるようにするため，NAT の設定を行う．また，脆弱性スキャナ Nessus Essentials[17]（以下 Nessus）のインストール・設定を行う．なお，具体的な操作においては，Linux コマンド操作，vi によるネットワーク設定ファイル編集等が必要となる．

受講生への課題としては，Kali Linux から Metasploitable2 への ping が届くこと，Kali Linux で Google や百度（Baidu）が開けること，および，Nessus の使用準備が完了したこと，以上 3 点を確認できるスクリーンショットを提出することとしている．

2.5 法令遵守誓約書の提出

ペネトレーションテストの意義や概要の説明に続いて，関連法規について紹介した後，受講生には図 3 に示す法令遵守誓約書の提出を求めた．演習では模擬的とは言え攻撃を行うことになり，その過程を通じて知り得た攻撃手法の悪用を防ぐ必要があるためである．誓約書は manaba で電子的に提出することとした．誓約書の文面には，刑法や不正アクセス行為の禁止等に関する法律へのリンクを張っている．

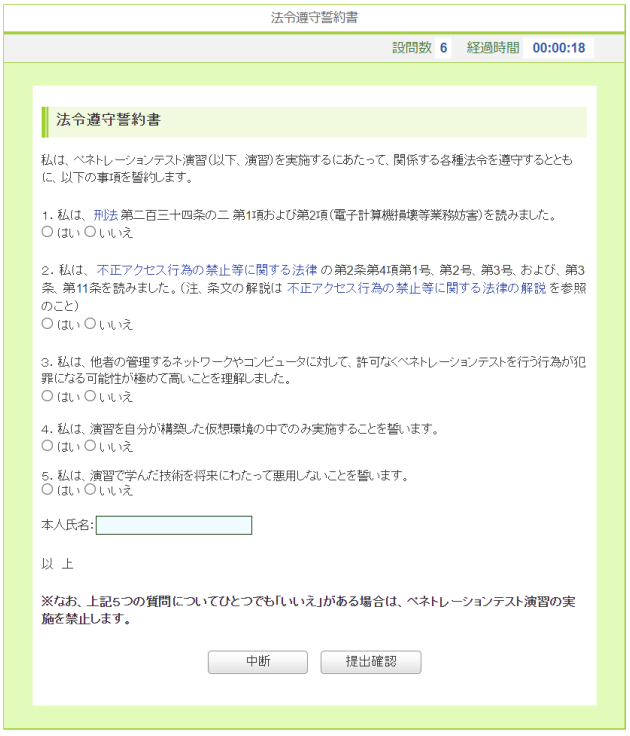


図 3 法令遵守誓約書の提出

以上，趣旨説明・法令遵守・実験環境構築をあわせて，講義動画は 8 本（合計 77 分）となった．ここまでを 2 コマ分の授業内容としている．

2.6 仮想環境におけるペネトレーションテスト演習

3 コマ目は，1 コマ目および 2 コマ目に構築した実験用仮想環境においてペネトレーションテスト演習を実施する．手順は大きく分けて，1．ポートスキャン，2．脆弱性の検索・検査，3．脆弱性攻撃の 3 段階からなる．以下，順に説明する．

2.6.1 ポートスキャン

まず，前回までに構築した実験用仮想環境を起動し，攻撃役ホストと被害役ホストの疎通確認，攻撃役ホストでの Nessus 起動確認等を行う．

次に，攻撃役ホストでポートスキャンを実行し，被害役ホストで開いているポートや稼働しているサービス・バージョンの調査を行う．攻撃役ホストである Kali Linux の端末上で “nmap -v -A 172.16.140.0/24” を実行する過程を図 4 に，その結果判明した，開いているポートと稼働しているサービスの例を図 5 に示す．

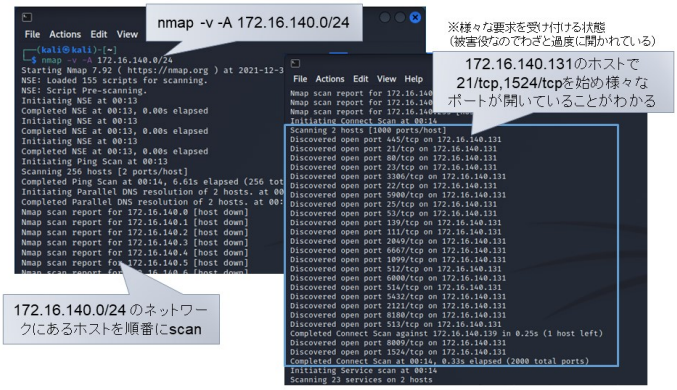


図 4 ポートスキャン実行過程

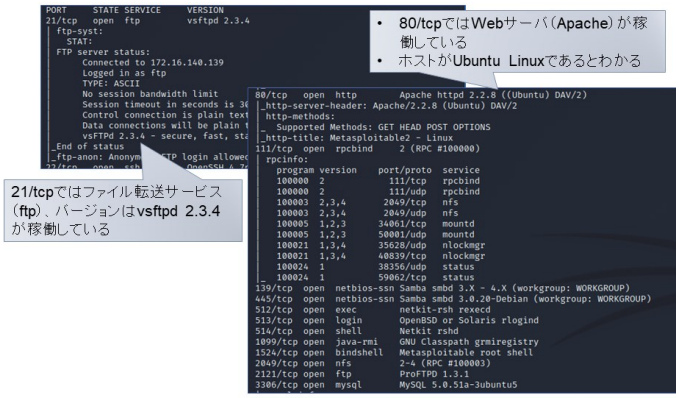


図 5 開いているポートと稼働しているサービス

図 4 では，探索対象であるネットワークにあるホストを順番にスキャンしたところ 172.16.140.131 というホストが

稼働していることが発見され，続いて当該ホストで 21 番や 1524 番ポートなど多くのポートが開いていることが検出されている様子が読み取れる．

さらに，図 5 からは，稼働しているサービス・バージョンの調査結果として 21 番ポートで vsftpd 2.3.4 が稼働していることなどが読み取れる．

2.6.2 脆弱性の検索・検査

次にポートスキャンで判明した vsftpd 2.3.4 が脆弱性を持っていないか，脆弱性情報データベース CVE Details[18]で調査を行う．調査過程を図 6 に示す．

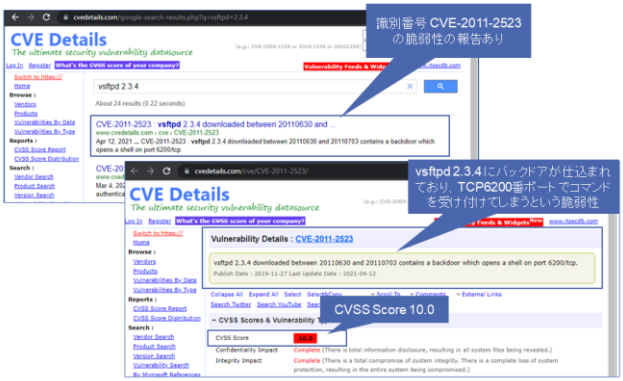


図 6　CVE Details で vsftpd 2.3.4 を検索する過程

vsftd 2.3.4 にはバックドアが仕込まれており，TCP 6200 番ポートでコマンドを受け付けてしまう脆弱性が存在すること，この脆弱性の CVSS スコア（脆弱性の重大度）が 10.0 であることなどが確認できる．



図 7　Exploit DB で攻撃プログラムの検索

続いて，図 7 のように，この脆弱性を攻撃するプログラムを Exploit DB[19]で見つけることができることを確認する．ただし，著名な脆弱性攻撃プログラムは後述の Metasploit framework[20]に取り込まれているので，実際の攻撃に際してはそちらを利用することとした．

以上のように，個別に脆弱性を検索することも可能であるが，脆弱性スキャナ Nessus を利用すると対象の脆弱性を網羅的に検査することができる．Kali Linux にインストールした Nessus を起動し，ブラウザで https://127.0.0.1:8834 を指定，“New Scan”, “Basic Network Scan”を選択する．Targets に攻撃対象ホストの IP アドレスとして，ここでは先のポートスキャンで発見された Metasploitable2 の IP アドレスである 172.16.140.131 を設定し，検査を開始する．Metasploitable2 を対象に Nessus を利用して脆弱性検査を実行した結果の例を図 8 に示す．

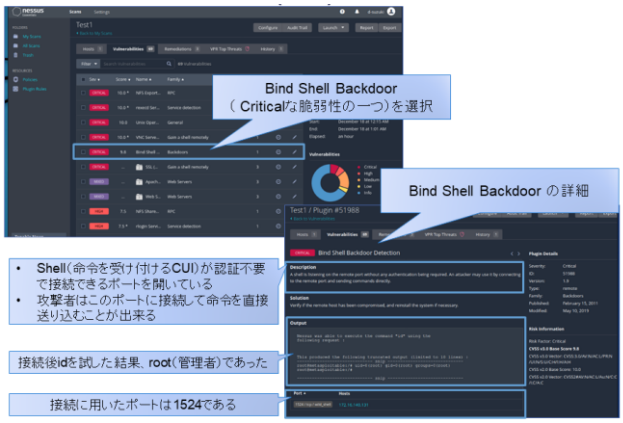


図 8　脆弱性検査結果の例

発見された複数の脆弱性が，重大度に応じて Critical から Info までレベル分けされて表示されている．このうち Bind Shell Backdoor の詳細を確認する．Shell が 1524 番ポートにおいて認証不要でコマンドを受け付けており，攻撃者はこのポートに接続してコマンドを直接送り込むことができることが確認できる．

2.6.3 脆弱性攻撃

Bind Shell Backdoor の脆弱性を利用して侵入を試みる．ネットワークユーティリティの一つである Netcat を利用して “nc 172.16.140.131 1524” を実行すると，以降 metasploitable2 に対して管理者権限でコマンドを実行できる．これはサーバ侵入の一例である．

別の方法として，Metasploit Framework を利用して vsftpd 2.3.4 の脆弱性を利用する攻撃を取り上げる．Kali Linux の端末上で “msfconsole” を実行すると Metasploit framework のコンソールが起動する．コンソールで入力するコマンドの例と実行結果を図 9 に示す．

ⓒ2022 Information Processing Society of Japan



図 9　vsftd 2.3.4 の脆弱性を利用した攻撃実行例

“search vsftpd” で検索したところ，Metasploit framework には vsftpd 2.3.4 の脆弱性を利用する攻撃プログラムが用意されている．“use exploit/unix/ftp/vsftpd_234_backdoor” で指定，“set rhost 172.16.140.131” で Metasploitable2 を攻撃対象に設定，“run” で攻撃を実行する．この結果，確かに Metasploitable2 に対して管理者権限で任意のコマンドが実行可能になっていることが確認できる．

以上が仮想実験環境における脆弱性利用攻撃の一連の流れである．受講生は各自の PC においてこの一連の流れを体験する．なお，この回の講義動画は 4 本（合計 57 分）であった．

受講生に対する課題は二つ用意した．一つ目は，ポートスキャン，脆弱性検査，脆弱性攻撃，それぞれの結果がわかるスクリーンショットの提出である．二つ目は，ペネトレーションテストの目的と手順を自分の言葉で説明した上で，ペネトレーションテスト演習の経験を通じて，情報セキュリティに関して自分が学んだこと・考えたこと，および，今後学びたいこと・学ぶべきことについて記述するという課題である．

3. 結果と考察

3.1 演習ふりかえりアンケート

ペネトレーションテスト演習の学習内容についてふりかえりをするため，事後アンケートを第 14 回授業終了後に実施した．本授業の実履修者数は 34 人であり，そのうち本アンケートに回答した受講生は 33 人（回答率は 97.1%）であった．

まず「ペネトレーションテスト演習」の学習を通じて，「新たな発見や驚きがあった」「学習内容が理解できた」「学習内容を他者に説明できる」「テーマに興味が持てた」の各項目に対して 5 段階評価で回答を求めた結果を図 10 に示す．

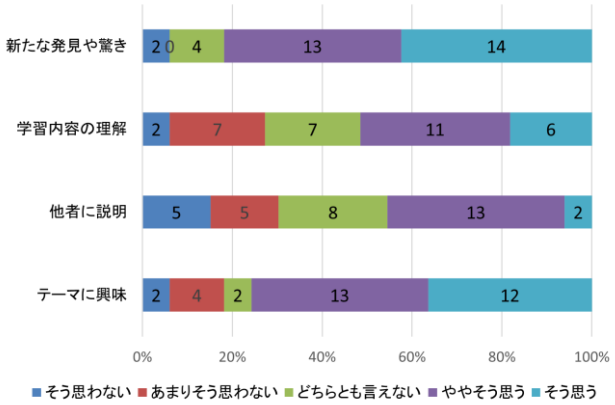


図 10　ふりかえりアンケート結果

「新たな発見や驚きがあった」については，27 人（81.8%）が肯定的な回答（「そう思う」「ややそう思う」）を選択している．また，「テーマに興味が持てた」については，25 人（75.8%）が肯定的な回答をしている．

自分の保有する PC に仮想マシンと仮想ネットワークを構築し，その中でサイバー攻撃を模擬するという本演習は，オンライン授業でも十分に実施可能であり，多くの受講生が興味を持てる学習内容であったと言える．

一方で，「学習内容の理解」「学習内容を他者に説明」については肯定的な回答が，それぞれ，17 人（51.5%），15 人（45.5%）となっている．難易度がやや高く，十分な理解を促すためには，まだ授業方法等に課題がある．

3.2 「自由意見・感想」の確認・検討

演習の事後に行ったふりかえりアンケートでは，演習の学習内容に関して「重要だと思った点，印象に残った点」「疑問に思った点，よく理解できなかった点」「自由意見・感想」についても自由記述回答を求めた．

各項目の詳細な分析は今後の課題とするが，攻撃の体験を通じて情報セキュリティに対する興味関心を喚起できたか，また，そのような演習がオンライン授業で可能であったか，という観点で「自由意見・感想」について回答内容の確認・検討を行った．

「自由意見・感想」には，以下のような回答が見られた．

- 自分で作った仮想環境を攻撃してみて，思ったより簡単にできてしまったことに驚いた．意図的にポートを開放

していたとはいえ，少ない手順で攻撃できてしまったため，自分のパソコンが今どういう状況で，穴がない状態か，あるならパッチを適応するなどの適切な対処が必要だと感じた.

- ペネトレーションテスト演習を通して，知らなかったことを知ることができたため非常によかったと思う. 特に，脆弱性を見つけ出すためのデータベースやソフトがあり，簡単に見つけ出すことができることや，攻撃プログラムが用意されていることなど，知ることができてよかった. 危険であるため，十分にセキュリティ対策をすることが必要であると感じた.
- 今までセキュリティの重要性をあまり感じていなかったが，今回の演習を通して，セキュリティについて興味を持てたし，面白いと感じた.
- 実際にしてみて，簡単にできたことに驚いている. 近年，ますますネット社会になっている為，サイバー攻撃の脅威は高くなっていると思うので，セキュリティ対策をしっかりしていく必要があると思った．また，このようなテストを今まで知らなかったので，知ることができてよかったということと，重要性を理解することができた.
- ペネトレーションテスト演習を通して攻撃者の考えや自分たちがそれらからそのように守るかなどについて身に着けることが出来それを実行することができた

受講生は演習を通じて，攻撃者の視点や攻撃手法を知り，サイバー攻撃の脅威をより身近に感じた結果，情報セキュリティの重要性を意識するようになったこと，情報セキュリティに対して興味・関心を抱いたことがうかがえる.

3.3 演習進捗状況アンケート

演習の進捗状況，困難を感じた過程・内容，興味を感じた過程・内容，演習で利用した PC について，第 15 回授業（2022 年 1 月 14 日）において，アンケート調査を行った. 演習の進捗状況と到達人数を整理して表 2 に示す．なお，演習が完了していない受講生については困難を感じた過程･内容の要点を併記した. 回答者数は 26 人（回答率 76.5%）であった.

回答者 26 人のうち 19 人（73.1%）が最後の脆弱性攻撃の実行まで完了している．仮想コンピュータ・仮想ネットワークを構築し，各種ソフトウェアやコマンドを利用してペネトレーションテストを行うという内容は，教室ですぐに疑問点を聞ける環境で，かつ，全員が同じコンピュータ環境で行ったとしても，それほど容易な演習ではない．オンライン授業，かつ，各自が自由に用意した PC で演習を実施するという今回の条件下では，最悪の場合，演習が滞る受講生が続出する状況も考えられた.

しかし，結果的には多くの受講生が最後のプロセスまでたどり着いている. オンライン授業かつ各自の用意した PC を用いた演習が十分に可能であると言える.

表 2　演習の進捗状況

No.	どこまで進んだか	人数	困難を感じた過程
1	まったくできていない	0	
2	VirtualBox の準備	0	
3	Kali Linux の準備	1	容量不足
4	Metasploitable の準備	2	vi, Metasploitable 操作
5	ネットワーク設定	1	vi による設定
6	nessus の導入	0	
7	ポートスキャン	1	vi による設定
8	脆弱性検査	2	コマンド, nessus
9	脆弱性攻撃	19	

演習が完了しなかった受講生 7 人に関して，「困難を感じた過程・内容」に関する自由記述を確認したところ，PC の記憶容量不足を挙げた受講生が一人いたが，多くは vi や Linux コマンド操作で苦戦していた様子であった．最後まで到達した受講生においても，少なくない受講生が，Linux コマンド操作，vi によるファイル編集を困難に感じていることが確認できた.

本学部では，3 年生前期科目として「情報システムⅠ」を置いており，Linux の学習やコマンド操作を修得することになっているが，必修科目ではない．当該科目の履修を推奨しているものの，未履修者・未修得者も「情報通信ネットワークⅡ」を受講することになり，それが本演習に対して困難を感じさせる一つの原因となっていると考えられる．このため，この点を補うための補習授業動画を用意することが望ましいと言える.

4. おわりに

本研究の目的は，ペネトレーションテスト演習をオンライン授業として実施可能な形で提案・実践し，その教育効果を明らかにすることである.

演習の進捗状況アンケートおよび演習のふりかえりアンケートの結果から，受講生の大半が各自の保有する PC に実験用仮想環境を構築し，各種ソフトウェアやコマンドを利用してペネトレーションテスト演習を完遂することができた．また，この体験を通じて攻撃者の視点や攻撃手法を知り，サイバー攻撃の脅威をより身近に感じた結果，情報セキュリティの重要性を意識するようになったこと，情報セキュリティに対して興味・関心を抱いたことが確認された.

ペネトレーションテスト演習は，オンライン授業かつ各自の PC に仮想環境を構築して実施するという条件下でも，十分に実践可能であり，情報セキュリティに対する興味関心を喚起できると言える.

謝辞

本研究は JSPS 科研費 19K03015 の助成を受けたものです.

ⓒ2022 Information Processing Society of Japan

参考文献

[1] 情報処理推進機構：情報セキュリティ 10 大脅威 2021，入手先<https://www.ipa.go.jp/security/vuln/10threats2021.html> (参照 2022-02-01).
[2] McAfee Enterprise : 2021 年の 10 大セキュリティ事件ランキングを発表，入手先 <https://www.mcafee.com/enterprise/ja-jp/about/newsroom/press-releases/press-release.html?news_id=2021121401> (参照 2022-02-01).
[3] 鈴木大助: 大学学部生を対象とするセキュリティ教育におけるサーバ侵入演習の実践と評価，情報処理学会論文誌教育とコンピュータ Vol.5, No.2, pp.20-29 (2019).
[4] 国立情報学研究所 : edx Archives - 教育機関 DX シンポジウムアーカイブズ，入手先< https://edx.nii.ac.jp/ > (参照 2022-01-30).
[5] 山田剛史：遠隔授業のインパクトとニューノーマルの高等教育, 中央教育審議会大学分科会 質保証システム部会（第 9 回）資料， 入手先 <https://www.mext.go.jp/kaigisiryo/content/000125292.pdf>(参照 2022-02-01).
[6] 河合塾 : 特集 コロナ禍での大学の取り組み ～2020 年度「ひらく日本の大学」緊急調査結果より，Guideline10・11 月号，入手先 <https://www.keinet.ne.jp/magazine/guideline/backnumber/20/0203/tokushu.pdf>(参照 2022-02-01).
[7] 朝日新聞・河合塾 :「ザ・解説 コロナ禍 1 年半、いま大学は（「ひらく日本の大学 2021」共同調査から）」入手先 <https://www.asahi.com/edu/hiraku/>(参照 2022-02-01).
[8] Wireshark, available from <https://www.wireshark.org/> (accessed 2022-02-01).
[9] Cisco Packet Tracer, available from <https://www.netacad.com/ja/courses/packet-tracer> (accessed 2022-02-01).
[10] Manaba，入手先<https://manaba.jp/products/> (accessed 2022-02-01).
[11] Microsoft 365 SharePoint，入手先 <https://www.microsoft.com/ja-jp/microsoft-365/sharepoint/collaboration> (accessed 2022-02-01).
[12] Google Workspace for Education，入手先 <https://edu.google.com/intl/ALL_jp/products/workspace-for-education/> (accessed 2022-02-01).
[13] Microsoft Teams，入手先 <https://www.microsoft.com/ja-jp/microsoft-teams/group-chat-software> (accessed 2022-02-01).
[14] Oracle VM VirtualBox, available from <https://www.virtualbox.org/> (accessed 2022-02-01).
[15] Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution, available from <https://www.kali.org/> (accessed 2022-02-01).
[16] Metaploitable2, available from <https://sourceforge.net/projects/metasploitable/> (accessed 2022-02-01).
[17] Nessus Essentials, available from <https://www.tenable.com/tenable-for-education> (accessed 2022-02-01).
[18] CVE Details, available from <https://www.cvedetails.com/> (accessed 2022-02-01).
[19] Exploit DB, available from <https://www.exploit-db.com/> (accessed 2022-02-01).
[20] Metasploit Framework, available from <https://www.metasploit.com/> (accessed 2022-02-01).

ⓒ2022 Information Processing Society of Japan