7ZH-05

実体験を重視した導入負担の少ない情報セキュリティ教材の開発

春口拓人† 小島俊輔†
熊本高等専門学校†

1. はじめに

本研究は，情報セキュリティ教育の内容の変化に対して適切な教材を設計・作成することで教員の負担を減らし，実体験を通じた効果的な情報セキュリティ教育の実施に寄与することを目的とする．

情報セキュリティ教育の内容はモラルとリテラシーを教えるものから，攻撃方法や防御方法などを含めた具体的な原理を教えるものへと変化している．内容だけでなく教育対象も拡大しており，情報系の学科に所属する学生から，すべての学科に所属する学生が対象となっている．こうした教育内容の変化は学習者のリテラシーに具体的な根拠を与え，増加しているインターネット上の脅威に対する自己判断による回避能力を養成する上で有効である．また，こうした変化に合わせて，授業で取り扱う題材も以前に比べて高度なものになることが予想される．しかし，こうした高度な内容の授業の実施は，担当教員にかかる負担が大きい，効果的な授業の実施が難しいといった課題がある．そこで本研究では実体験を通じて情報セキュリティの仕組みの理解を促す教材を作成した．

2. 教材の全体像

IPA が発表した資料[1]では，組織部門では「ランサムウェアによる被害」「インターネット上のサービスへの不正ログイン」「脆弱性対策情報の公開に伴う悪用増加」といったマルウェアに関連した被害が多く挙げられている．こうした被害は今後も重大な脅威として認識されると考えられるため，本教材はマルウェアによる攻撃とマルウェアの操作を題材とする以下のような要素を取り入れた．

1) C&C サーバーによる bot プログラムの操作
攻撃者がどのようにしてマルウェアを遠隔操作しているのか体験する
2) SYN flood 型 DDoS 攻撃
DDoS 攻撃によってどのような現象が起こるのか体験する
3) ランサムウェアによるファイル暗号化
ファイルの暗号化によってどのような現象がおこるのか体験する

本教材は 2 つの Operating System(OS)，A と B を利用する．A を攻撃者が扱う bot への司令塔である C&C サーバー，B を bot に感染した被害者として設計し，学習者に A を操作してもらうことで疑似的な攻撃者となり上記の 2)，3)の攻撃を実体験させる．この時の DDoS 攻撃やファイルの暗号化の体験から被害の内容や攻撃に使われている技術・仕組みを理解することでセキュリティ意識の向上を目指す．

3. 教材の構成

本教材は，「bot プログラム」「C&C サーバプログラム」「動作環境」「操作マニュアル」の 4 つから構成されている．「bot プログラム」「C&C サーバプログラム」「操作マニュアル」の 3 つは自作し，「動作環境」については既存のアプリケーションを利用した．教材の対象者は専門を問わない高校生とし，OS の操作やプログラムなどの情報技術に関する能力を要求することのないようユーザーインターフェースを工夫し，教材の理解を補助する操作マニュアルを作成した．

本教材は攻撃者と被害者の環境を構築し，実際の攻撃を再現する．このため 2 つの OS を使用するが，授業導入時に PC を 2 つ用意しそれぞれにシステムを導入するのは教員の立場から負担である．また DoS 攻撃の再現やファイルの暗号化を行うため，万が一システム内の事象がインターネットを通じて外部に漏れた場合，それ自体がインシデントとなってしまう．そこで

1) 授業導入の際の負担をできる限り軽減させること
2) システム内の事象を外部に漏らさないこと

の 2 つを満足させるために，本教材の動作環境は仮想環境構築ソフトウェアと仮想環境上で動作する 2 つの OS のイメージファイルによって構成した．仮想環境の構築には Oracle VirtualBox[2]，攻撃者側の OS は Kali Linux[3]，被害者側の OS は Metasploitable[4]を使用した．

ネットワーク構成は**表.1** のように構成した．特に DDoS 攻撃の再現の際にパケットがシステムの外

Development of User-Friendly Teaching Materials for Experience Oriented Information Security Training
Hiroto Haruguchi†, Shunsuke Oshima†
†National Institute of Technology, Kumamoto College

	LANadapter	Internet	IP address
Kali Linux	NAT&HostOnly	connect	DHCP/Static
Metasploitable	HostOnly	disconnect	Static

表.1　ネットワーク設定

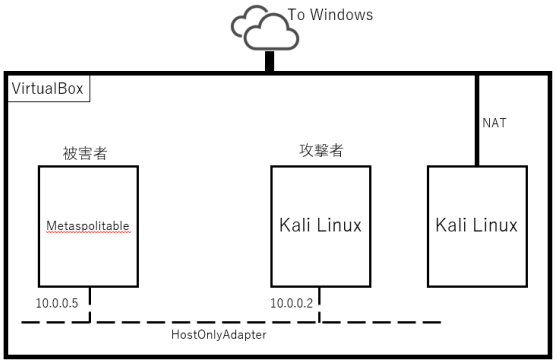

図.1　システムのネットワーク構成

に漏れださないように Metasploitable 側はインターネットへと接続させず Kali Linux との通信のみを行うように設定した．また IP アドレスの割り振りは Kali Linux のインターネット側は DHCP とし Metasploitable 側は Static とした．

以上の設定により構築したシステムの全体概要を図.1 に示す．こうしたシステム構成とプログラムによりシステム外部に影響を出さずに攻撃を実体験することができる教材となっている．

4. 研究結果

本研究では情報セキュリティの攻撃方法を実体験できる教材の開発を行った．体験できる攻撃方法は SYN flood 攻撃とファイルの暗号化の 2 つである．以下に 2 つの攻撃方法の実装内容について説明する．

4. 1　SYN flood 攻撃の実装

本教材が行う SYN flood 攻撃の具体的な仕組みを図.2 に示す．本システムの SYN flood 攻撃は以下のようなシナリオで攻撃をする．

1) C&C プログラムからの攻撃コマンドを待つ
2) 攻撃コマンドを受信したら自身の子プロセスを生成する
3) 親プロセスは C&C プログラムから指示を待つ
4) 子プロセスは送信元 IP アドレスと MAC アドレスを偽装した TCP ヘッダを作成し攻撃相手に SYN パケットを送信し続ける
5) 親プロセスは C&C プログラムから攻撃停止命令を受信すると子プロセスに対して kill シグナルを送信しプロセスを停止させる
6) 以降 C&C からの命令を受信するたびに 2)～5) を繰り返す

4. 2　SYN flood 攻撃の実装

本システムのランサムウェアによるファイル暗号化は以下のように実装している．

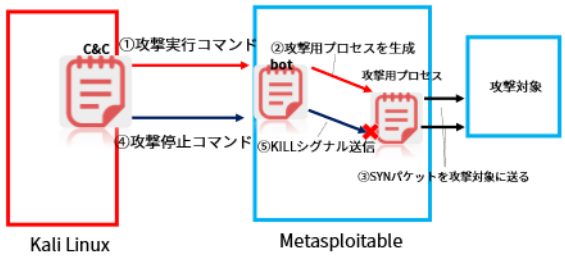

図.2　SYN flood 攻撃実装概要

1) C&C プログラムから暗号化の命令を受信したらカレントディレクトリから C&C 側で指定したファイル名に一致するファイルを探し出す
2) 一致するファイルが見つかったらバイナリモードでファイルを開きファイル内容をメモリ上に展開する
3) メモリ上に展開したデータに対して EXOR 演算で暗号化を施す

5. まとめ

本研究では実際の攻撃方法を体験することを通して原理の理解を促す情報セキュリティ教材を作成した．仮想環境を導入することで授業準備の際の負担をできるだけ軽減しながら，実際の情報セキュリティにおける攻撃方法をシステム外に影響を与えないように再現するシステムを構築した．今後は学習者側の視点でも効果的な教材となるよう内容の増加やユーザーインターフェースの改善を行う．

参考文献

[1] IPA:情報セキュリティ 10 大脅威 2021,Web ページ, https://www.ipa.go.jp/security/vuln/10threats2021.html,2021 年,参照日:2021-12-7.
[2] Oracle:Oracle VirtualBox,Web ページ, https://www.virtualbox.org/,参照日:2021-12-7.
[3] OffSec Services Limited:Kali Linux,Web ページ, https://www.kali.org/get-kali/#kali-virtual-machines,参照日:2021-12-7.
[4] RAPID7:Metasplotaitable,Web ページ, https://docs.rapid7.com/metasploit/metasploitable-2-exploitability-guide/,参照日:2021-12-7.
[5] 土居茂雄,向平卓矢:IoT セキュリティに関する教材の研究開発,平成 30 年電気学会 C 部門大会講演論文集,講演番号 PS4-6,2018.
[6] 増山一光:シナリオによる標的型メール対策教材を用いた情報セキュリティ教育の実践, 教育情報研究 33 巻 1 号 p.25-32,2017.
[7] 佐々木隆宏:切断中心性の教材開発への応用-RSA 暗号システムの教材化を例として-,2018 年数学教育学会誌 Vol.59 No.1・2.