2019 年度未踏ジュニア提案書

提案するプロジェクトのタイトル

DetExploit – 誰でも簡単に扱えるオープンソース脆弱性スキャナー

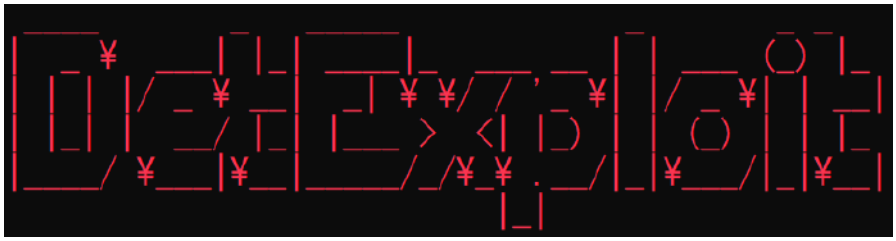
提案者に関する事項

メインクリエータ（代表者）の氏名	もぴ (https://twitter.com/moppoi5168)
グループの場合、メンバーの氏名	

以下の入力欄は必要に応じてサイズを変更できます。図や表の挿入も推奨します。

1. 提案するプロジェクトの簡単な説明（200 字以内）

3. の提案内容に記載される内容を、簡潔にまとめてください。



DetExploit は WMI (Windows Management Instrumentation)やレジストリなどを参照することによって取得したシステム上のアプリケーションの情報と様々なデータベースから取得した情報を照合することによってセキュリティ的に脆弱なソフトウェアを検知し、ユーザーに通知するソフトウェアです。

2. 開発費の使用計画

・使途未定 500,000 円
＊現段階で機種などは特に決めていないが採択後に Windows マシンを開発、デバッグ用に購入する必要あり。
(現在は Parallels という仮想化ソフトウェアを用いて開発しているが、パフォーマンス不足だと考えられるため。)

3. 提案内容

DetExploit

誰でも使えるシンプルで力強い脆弱性スキャナー

概要

DetExploit は Detect (検知)と Exploit (脆弱性)を組み合わせた言葉です。つまり脆弱性を検知する脆弱性スキャナーが今回私が提案するプロジェクトで開発されるプロダクトになります。

ターゲット層

『誰でも使える』というテーマの通り、エンジニアではない一般的なユーザーを対象にしています。後述する類似している脆弱性スキャナーと違い、サーバーではなくパーソナルコンピュータがメインターゲットです。

どうやって誰でも使えるようにするのか

これは本プロジェクト一番の課題だと思っています。何故かというと、例え UI をシンプルでわかりやすいものにしても脆弱性の意味自体を知らない一般ユーザーにとっては結局訳のわからないものという扱いを受けてしまうからです。というわけで製作を通す中で積極的に SNS などを活用して情報発信していきたいと思います。

他の類似サービス、およびそれらと違う点

・Vuls (VULnerability Scanner)
・F-Secure Radare
・その他企業向けセキュリティシステム

まずわかりやすい下の二つとの違いを説明させていただきます。下二つのような企業向けセキュリティシステムは総じてサーバー向けな上に導入コストが非常に高いのです。ライセンス料金、それに加えて導入に必要な技術力などは個人が扱うには大きすぎると言えるでしょう。次に Vuls ですが、こちらは DetExploit ととてもよく機能面で似た脆弱性スキャナーです。機能的にはプロトタイプ段階でほぼ同じだと言えるからです。しかし Vuls と DetExploit は根本的にターゲット層が違います。というもの Vuls は Linux/FreeBSD で動いているサーバー向け脆弱性スキャナーなのです。まず第一に Vuls は Windows プラットフォームを動作環境としていません。デファクトスタンダードである Windows を対象にしていないのでは『誰でも使える』とは言いがたく、DetExploit では Windows を初期段階から動作環境として開発しています。(将来的に別プラットフォームをサポートする可能性はあります。)

ただし Vuls は Go-lang (Go 言語)で実装されており、恐らくソースコードの一部を書き換えれば Windows でも使用可能だと考えられます。しかしその書き換えるということにも技術力が必要であり、一般的な個人が行うにはハードルが高すぎると考えられます。加えて Vuls の方針(ターゲット層)から見ても将来的に Windows が動作環境としてサポートされるということは考えづらく、DetExploit とは対象ユーザーが違うと考えられるのです。

実装予定の機能

~~プロトタイプ段階では ExploitDB のみ、現在 MyJVN からデータを取得する機能を製作中~~ **製作しました。ExploitDB、JVN の両方からのデータ取得及びスキャンに対応しました。**

複数のデータベースから取得した脆弱なアプリケーションのデータとWMI やレジストリから取得したインストールされているアプリケーションのデータを照合して脆弱なアプリケーションがないかスキャンします。プロトタイプ段階では CUI ですが、将来的には Qt などのモジュールを用いて GUI 化して『誰でも使える』脆弱性スキャナーにしていきたいと考えています。

既存のものにはないアイデア

Windows 対応で差別化を図るだけではなく機能面でも他の脆弱性スキャナーを上回っていきたいと考えています。Windows を対象にしているということもあり、Linux や FreeBSD では使えない方法で検知精度を更に上げていきたいと考えています。
(例: 通常のレジストリスキャンに加えて WMI / PowerShell を用いた三段階の脆弱性スキャン機能)

どういったことが開発する上で難しいか

本当は 5 の**このプロジェクトについて現在までに取り組んだこと**に書くべきですが、スペースの関係でこちらに書かせていただきます。
JVN からのデータ取得まで実装してわかったことですが、開発する上での難所は**取得データのサイズ**だと私は感じました。ExploitDB のデータは公開されている CSV ファイルを取得してそれをパースするという流れで使用しています。しかし、それが可能なのは ExploitDB に情報量がそれほどないからです。JVN の場合は API を用いて XML 形式のデータを取得するのですが、こちらは情報量がかなり多いのです。加えて 1998 年からのデータを全て取得するとなると非常に長い時間をダウンロードに使わなければいけません。こればかりは解決が難しいと自分は考えています。サイズの小さいファイルにフォーマットしたものを配布することは JVN の規約的に NG ですし、JVN を利用するかどうか選択することができるようにするのが一番現実的ではないかと考えます。もし面談で話させていただけるのであれば、PM の方の意見も是非お聞きしたいです。

4. あなたが自分の貴重な時間を使ってこのプロジェクトを実現したい理由（任意）
なぜ、世界中の誰かではなく「あなた」がこのプロジェクトに時間を使うべきなのでしょうか？何か、原体験や自分にしかない強み、プロジェクトに対する思いがあれば書いてください。

本プロジェクトの提案に至った理由
2017 年 5 月に猛威を振るったワーム型ランサムウェア『WannaCry』をご存知でしょうか？あの WannaCry は CVE-2017-0144 という Microsoft SMB に存在する脆弱性を利用して感染を拡大しました。ここで重要なのが、この脆弱性は **2017 年 3 月のセキュリティアップデートで修正されていた**ということです。つまり企業や団体などを含んだありとあらゆる Windows マシンが二ヶ月前に公開されていたそのセキュリティアップデートを適用していなかったということです。それ以外の世界中のサイバー攻撃を見ても、まず間違いなく既にパッチの公開された脆弱性を狙った攻撃がほとんどだとわかるでしょう。最近のセキュリティソフトは未知のマルウェア、攻撃に対しサンドボックス方式などで対応していますが私はそもそもこの方針が根本的に間違っていると思います。未知のものを警戒するのは当然です。ですが実際に既知のものを狙った攻撃がこれだけあり、それらがこれだけ成功しているというのに既知の脆弱性を塞ぐための技術が開発されないことに私は疑問を抱いていました。今回のプロジェクトはそんな理由から考え出したものです。

5. このプロジェクトについて現在までに取り組んだこと（任意）
類似品の調査や、実験、プロトタイプの開発など、今までに取り組んだことがあれば書いてください。なにがどこまでできていて、どういったことがこれから難しそうかを詳しく書いてくれたら、面談でのやりとりがスムーズになります

類似品の調査
提案内容の方に記載させていただきました。

プロトタイプの開発
GitHub にてプロトタイプ段階のものを OSS (オープンソースソフトウェア)としてソースコード等を公開させていただいております。
➔ https://github.com/moppoi5168/DetExploit

6. 提案者がこれまで制作したソフトウェアまたはハードウェア

- 自分が、このプロジェクトを進めるにあたり十分な能力があることを、アピールしてください。（特に、5.でまだプロトタイプなどの開発をやっていないと解答した方は、ご自身の能力を強くアピールしてください。）
- これまでの活動実績が載っているホームページや、GitHub のアカウント、YouTube チャネル等がある場合も、こちらでアピールしてください。
- フォーマットは自由です。図表や画像も使用できます。ページ数も制限はありません。複数人で開発した場合は、どの部分を担当したのか、明確に記述してください。

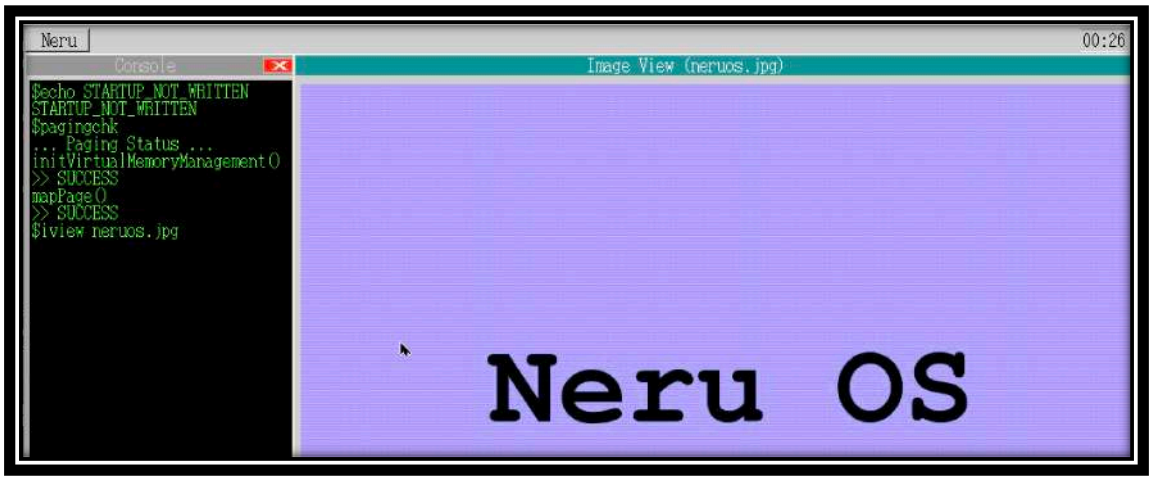
リンク集

ブログ: https://moppoi5168.github.io/
Twitter: https://twitter.com/naogramer/
GitHub: https://github.com/moppoi5168/

制作物

研究 (制作物ではない)

制作物ではありませんが、私がもっとも好きな分野であり自分としては何か形のあるものを作ることよりもずっと意味のあることです。自己アピールにて詳細は書きますが、高校一年生の夏に参加した IPA (セキュリティキャンプ協議会)の主催するセキュリティキャンプ全国大会 2018 を機にセキュリティに関わらず論文を読みそれについて研究するようになりました。具体的には Google File System の構造に関する研究や BadUSB という USB のファームウェアを書き換えることにより作られる攻撃ツールへの GoodUSB という対処法など様々な研究を行ってきました。一部の研究においては実際にコードを書いて実験をするなども行っており私にとってはこれにより得た知識こそが一番の制作物だと言えます。



NeruOS

NeruOS という自作 OS を開発しました。つい最近ページングによるメモリ管理機能を実装したことが自分としては記憶に新しいです。ベースは『はりぼて OS』という『30 日でできる！OS 自作入門』という本で開発される OS ですが、ほぼオリジナルといっても差し支えないレベルでプログラム・デザイン共に変わっています。(PCI バスコンフィギュレーション、シリアル通信機能、独自ウィンドウデザイン、ページングなどの独自機能を多数実装済み。)現在は UEFI で起動することが可能な OS のブートローダを書いています。

mpcc (mcc)

セキュリティキャンプ全国大会 2018 というイベントで知った rui さんという方の 9cc を参考にしながら実装している自作 C コンパイラです。将来的にはセルフホスト(自分で自分をコンパイルできる)可能なコンパイラにしたいと考えています。

SeeQR

QR コードを通して様々なコンテンツを提供するスマートフォンアプリおよび関連する Web アプリ、Python ライブラリを開発するプロジェクトです。現在は Java を勉強しつつ Android 版アプリの開発を行っています。実は数ヶ月前まで今回の未踏ジュニアに応募する気でいたのですが、数日どころか数時間でプロトタイプが完成してしまい、ターゲット層が迷子なので扱いづらいと判断して応募を見送りました。

Baremetal Applications (Toshokan)
セキュリティキャンプ全国大会 2018 (何回も登場してすみません、自己アピールで詳しいことは書かせていただきます)の liva さんという私の講義を担当された方が開発された『手軽に誰でもベアメタルアプリケーションを開発・テストすることが可能なプラットフォーム』である Toshokan 上で動作するアプリケーションです。代表作(?)は RDTSC(CPU クロック)の値を求めるライブラリです。

その他細々としたもの
細々としたものと書いていますが、実際のところ私の書いたほとんどのコードはこの細々としたものに含まれています。テスト用シェルスクリプト、簡易的な Web サーバ、実験に使用する自作のセキュリティツールなどは毎日のように作っています。継続したプロジェクトではなく一日軽く使って書いたコードなどもこちらに含まれますね。CTF の pwn という Binary Exploitation のジャンルでは解くために本当に簡易的な BOF 問題を除けばほとんど問題では絶対に Exploit Code を書く必要があるのでそういうコードも書けたりします。

7. 週あたりの作業時間の目安

作業時間: *学期中 ×時間* *夏休み中 ◇時間*
学期中 14 時間 夏休み中 28 時間 (あくまでも目安。余裕を持ってこの作業時間なので調節可能。)

8. 自己アピール

その他、まだアピールしきれていない、得意なことや、ほかの人にはないような経験があればアピールしてください。必ずしも提案内容と関連している必要はありません。

#whoami

いつも LT をやる時の自己紹介をアレンジしたものを書いていこうと思います。現在高校二年生で、セキュリティに関する色々なことをやっています。プログラミングは小学四年生から始めていて(コンピュータ自体は幼稚園の頃から触っていて Linux のインストール CD をつかったおままごとをやっていた記憶もある)、最初は iOS アプリ開発(Objective-C)、その次に Web 系 (PHP など)の開発を学びました。私自身セキュリティに興味を持ったのはその段階で、興味の赴くままに独学で学習していたらいつの間にか研究するまで好きになっていました。ただセキュリティというと範囲が広すぎて(データベースもプログラミングも最近では機械学習までなんでもセキュリティに関係がある気がします)専門分野がないように思われるので最近は DFIR(Digital Forensics & Incident Response)を主な研究分野としています。2019 年 7 月までカナダのバンクーバーに留学して英語の勉強をしています。

#セキュリティについて語りたい

私は高校生になってから様々なセキュリティ関係のイベントに参加していますが本当に高校生でセキュリティが好きな人がいなくて辛いです。実際後述するセキュリティキャンプ全国大会でもジュニアコースという高校生以下限定のコース以外では私が最年少でしたし、その他セキュリティをテーマとした関西の LT 大会では最早学生が自分だけという悲しくなる事態に遭遇してしまったりしています。というわけで最近の目標はセキュリティに興味を持つ人を増やすことです。

#セキュリティじゃなくてもいい！！

上記の目標の途中にあるサブ目標といいますか、セキュリティじゃなくてもいいのでプログラミングや機械学習でも何でもいいので出来るだけ同年代の方と熱く語りたいです！！！自分でも「どうしてこんな環境で育ってこうなったんだ？」と言いたいくらいですが、家族親戚はもちろん学校に至っても誰もプログラミングが好きな人が身近にいません。初めて LT 大会に行って色々な方々と出会った時は非常に楽しかったのです。U17 という未踏ジュニアだからこそ、私と近い年代の方で面白い話ができるのではないかと考えています。

#未踏ジュニアの公式 Twitter の中の人さんへ

この応募用紙を見られているかは微妙なところですが、本当にこの方には感謝しています。というのも高校に入るまでは未踏ジュニアの存在を知らなかったので未踏 IT 人材発掘育成事業の方しか目に入っていなかったのです。しかし先ほど書いた通り私は本応募用紙を書いている段階で留学しています。未踏の規約で日本にいないので応募できません。それを Twitter で嘆いていると未踏ジュニアの公式 Twitter さんが未踏ジュニアなら応募可能だということをリプライしてくださりました。私が今これを書いているのもその方のおかげなので本当に感謝しています。ありがとうございました。

#活動記録

・総関西サイバーセキュリティ LT 大会第十回
・セキュリティキャンプ地方大会 2018 in 兵庫
・セキュリティキャンプ全国大会 2018
・Global Cybersecurity Camp 2018（GCC2018）一期生

最後の二つは LT も行いました。GCC2018 では私だけが LT 登壇者で緊張しましたが研究していた(正確には現在も研究し

ているが)BadUSB に関する LT を行いました。GCC2018 のスライドは後日一部修正した内容を SlideShare にて公開しています。(内容としては前者も後者も同じものですが、もちろん後に作った GCC の方のスライドの方が出来がいいので前者のスライドのリンクは伏せておきます。)
https://www.slideshare.net/ssuser6c19e1/abyss-of-badusb

#最後に
プロトタイプに関して書いた時に少し言及しましたが DetExploit は OSS として公開しています。理由は私自身が OSS ソフトウェアの制作を経験してみたかったという点もありますが、一番の理由は発展性です。OSS はメンテナンスこそ大変ですが、実際定期的にメンテナンスが必要なレベルまで成長すると毎日のように(は言い過ぎですが)Issue という問題提起が行われます。この Issue を開発者が解決することにより更にソフトウェアが良いものになっていくのです。それ以外にも様々理由はありますが主な理由は以上ですね。未踏ジュニアに採択されたら OSC(オープンソースカンファレンス)にて DetExploit を出展してみるのも面白いと考えています。私はそういう多くの方々にこのソフトウェアの存在を知っていただけるイベントには積極的に参加して自分からも定期的にどんな機能が追加されたかなどをブログ記事にしたり Twitter で報告していこうと思います。