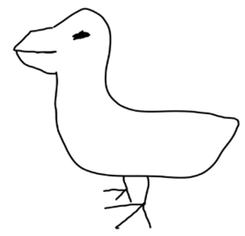
SecHack365

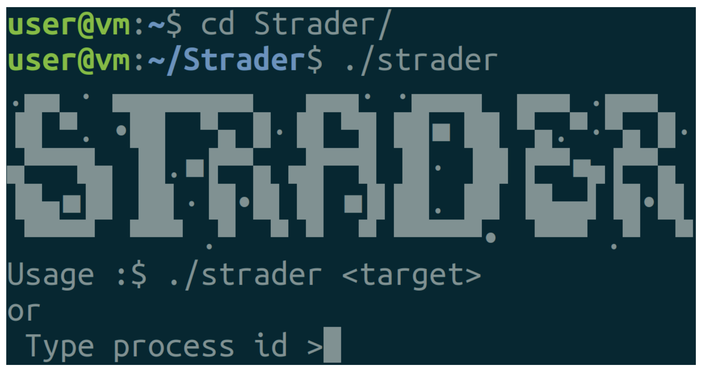
高校生が作る LINUX 用アプリケーションデバッガと IT の勉強会の主催

吉田　直樹



Strader

Linux 用アプリケーションデバッガ



Strader の由来

Simple
Tracer
Debugger
これらの文字を組み合わせて、
Strader という名前になった。

Strader に関する情報

C 言語で現時点で 753 行
CUI 対話型アプリケーション
アプリケーションを操作できる
Linux システムコール（ptrace()）
によってデバッグ対象を操作
制作開始　2019 年 10 月

作成の動機

作り方に関する資料やブログが少なく先駆者が少ないのではと思った
オリジナルのデバッガを作成しアプリケーションが動く仕組みに対する理解を深めたかった
自分で作ったオリジナルのツールとともに CTF に出てみたい。
これらの動機により Strader の作成に着手した。

既存の Linux 用アプリケーションデバッガとの違い

既存のデバッガには gdb, radare2, x64dbg, ollydbg 等があるが、いずれにしても多くの機能を持つ強力なツールであり自分みたいな初心者には使いこなせない、しかし Strader は最低限の機能のみを実装したため誰でも使いやすく、カスタマイズがしやすい。

今後の展望

ハードウェアブレークポイントを置けるようにする。
ptrace() システムコールを使わないデバッガにしたい
対応しているのが x64 アーキテクチャにしか対応していないため他のものにも対応していきたい
他のアプリケーションと連携してディスアセンブルしたものを表示できるようにしたい
最終的にはマルウェア解析に使えるようにしたい

Strader の使い方

./strader ＜デバッグ対象＞　　によって実行

実行中のプロセスもデバッグ可能 ./strader 実行の後
プロセス ID を入力することでデバッグが可能

＞b ブレークポイントの設置
＞ｓ ステップ実行
＞ｃ 動作再開
＞d ブレークポイントの削除
＞ib 設置したブレークポイントの表示
＞m メモリの内容の表示
＞r レジスタの値の表示
＞sr レジスタの書き換え
＞sc 任意の時間おきにステップ実行をするレジスタの値がどのように変化していっているのかがわかる
＞h 使い方の表示

sc ではレジスタの値が変わっていることがわかるが、値が変わったときに色が変わるようにしている

Strader を作ってみて思ったこと

デバッガの作り方を学ぶことを通して Linux 上でアプリケーションがどう動くのかを理解するということはできたが、作り方に関する資料を作ろうとしていたが、対話的にする処理などに関しては作り方の資料を作ったところであまり役立たないので資料を作成するためにはそういった処理を省いたデバッガを作り、その解説をブログなどにまとめる必要があると思った。
また、自分自身がアプリケーションデバッガを使いこなすほどの技量がなく、デバッガにどのような機能を乗せる必要があるのかわからないといった問題があった。しかし、ステップ実行によって変更があったレジスタの色を変えてみることによってレジスタの使われ方がわかるといったオリジナルの機能を載せられたことは良かったと思う。

IWATE の ITConference の主催

勉強会を主催しました

主催した動機としては、岩手には勉強会が少なく実際に会って情報を得るには移動による多くの時間とお金がかかってしまうこと、
自分自身もそういった勉強会で LT をしてみたいと思っても実際に知識が少ない中で自分が LT してもいいのかと思うことがあったこと、
勉強会などのイベントを開催する側の目線で見てみたかったということ
などにより、勉強会を主催することにしました。

勉強会を開いて感じたこと

勉強会を開くこと自体は簡単だが人を集めるなどの作業や工夫などに多くのエネルギーを消費されるまた一人でそれをやるというのもとても難しく感じた、今後は運営の協力者を募る必要があると思った。
人を集める工夫については Twitter などの告知はもちろん、自分は最近になって気づいたが、実際に働いているエンジニアさんに来ていただけるように年末などに合わせる必要があったと思った。
勉強会では、来る人によって雰囲気が変わってしまったり、硬い感じになってしまったりすることがあって、そういった点に関しては自分のオーラというかテンションを高くして引っ張って上げる必要があったと思った。

参加者ゼロ人を記録！

勉強会を主催しても、地方だと誰も来てくれないこともあった。地方で勉強会を開かないと経験する事ができないもので、貴重な経験ができたよ！（笑）

Conference のコンセプト

サイバーセキュリティや IoT をはじめ様々な分野の話を参加者同士が持ち合って話し合うゆるい会というコンセプトでゆるく楽しくやっていくということを目指しているよ。

ポスターの作成

以前は「　岩手の IT 勉強会（笑）　」という名前で勉強会をしていましたが、ポスターを作るにあったって IWATE の ITConference という名前に変更させていただきました。ポスターは A4 サイズで１００枚刷って、他の勉強会などで配らせていただけたりしました。

SecHack365 を通して学んだこと

・自分は広い世界を知ることができた。みんなものづくりに対する熱量がすごくて、自分にはこれはできないと感じて何だ悲しくなることもあったが、でも自分でもできて得意な分野はなんだろうと考えそれをやってみたりそれをやってみることからもいろいろな学びがあり、それがとても面白かった。
・自分自身の知識と経験がまだ足りなくて、与えられた環境を十分に活用できなかったことが残念だった。
・自分自身がこれからどのように生きていけばいいのか悩んでいたけどそれを解決できるヒントを見つけることができた。
・SecHack365 はとても短く感じたけど、それは集合会に向けてやってみたいことだったりやることが多くて、時間を忘れることが多かったからだと思う。

NICT 国立研究開発法人 情報通信研究機構