別紙.TIPS-3　実習資料

仙台 CTF 2019 セキュリティ技術勉強会 実習資料

TIPS-3 マルウェア解析

2019年9月28日

仙台 CTF 推進プロジェクト

目次

本実習の概要

あなたは、架空の企業「株式会社仙台シーテーエフ」に入社したばかりの新米情報セキュリティ担当者です。

ある日、DMZ の開発用サーバが不正アクセスを受け、第三者への RDP ブルートフォース攻撃の踏み台として悪用されてしまいました。

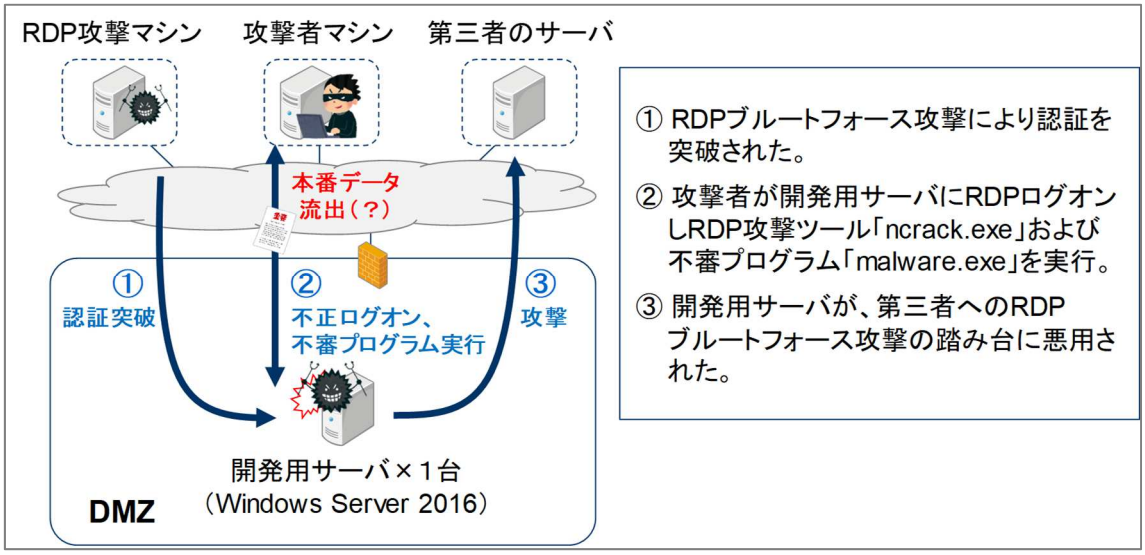
開発用サーバを調査したところ、RDP ブルートフォース攻撃ツール「ncrack.exe」および不審プログラム「malware.exe」が実行されていたことが判明しました。

開発用サーバには、本番データ（顧客情報）が格納されており、情報流出が懸念されます。
不審プログラム「malware.exe」を解析し、情報流出の有無を確認してください。

◆開発用サーバのファイル

不審プログラム （解析対象）	C:¥Users¥Administrator¥AppData¥Local¥Temp¥tools¥malware.exe
本番データ （顧客情報）	C:¥work¥sendaictf.csv
その他	不審プログラムと同じフォルダには「ncrack.exe」および関連ファイルも設置されている。

◆インシデントの状況図



［補足情報］

・　インシデント発生日は 2019 年 8 月 25 日（日）です。

実習1（練習問題） ダウンロードファイルの特定

実習内容

練習用不審プログラム「re01_urldownload.exe」を解析し、以下2点を特定してください。

① 不審プログラムがダウンロードしたファイル名（保存先のフルパス）

② 上記①のダウンロード元 URL

[実習用データ]

実習用仮想マシンに格納してあります。

フォルダ　：/var/samba/public/tips3/
ファイル　：re01_urldownload.exe

（補足） 実害の無いプログラムですが、ウイルス対策ソフトで検知される可能性があります。

回答記入欄

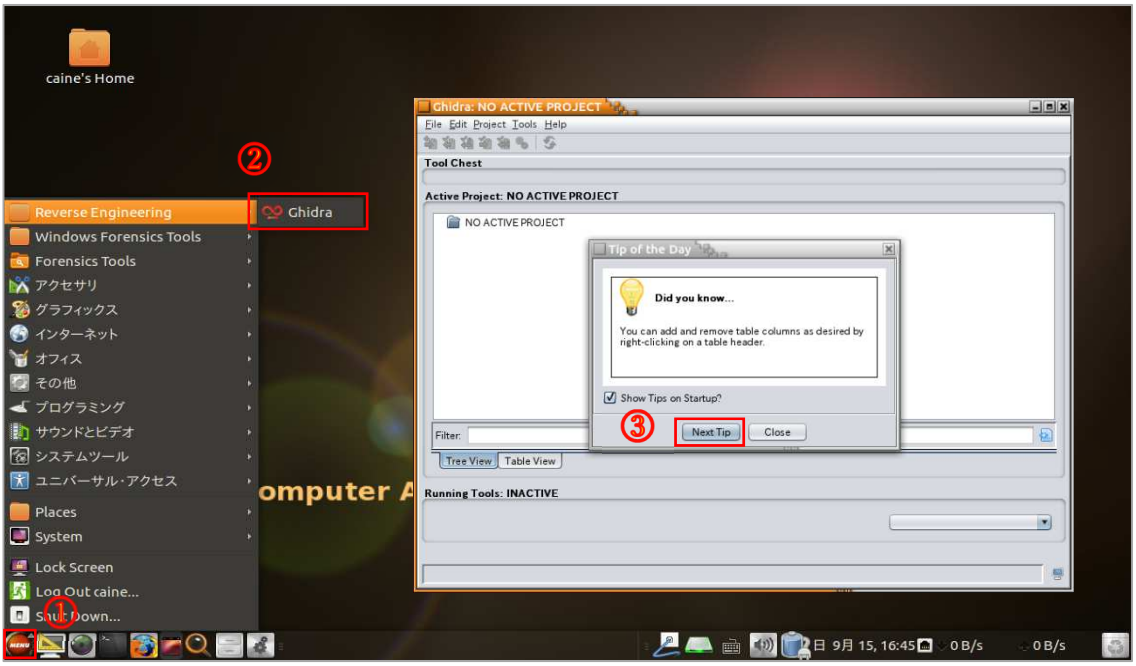
① 不審プログラムがダウンロードしたファイル名（保存先のフルパス）

② 上記①のダウンロード元 URL

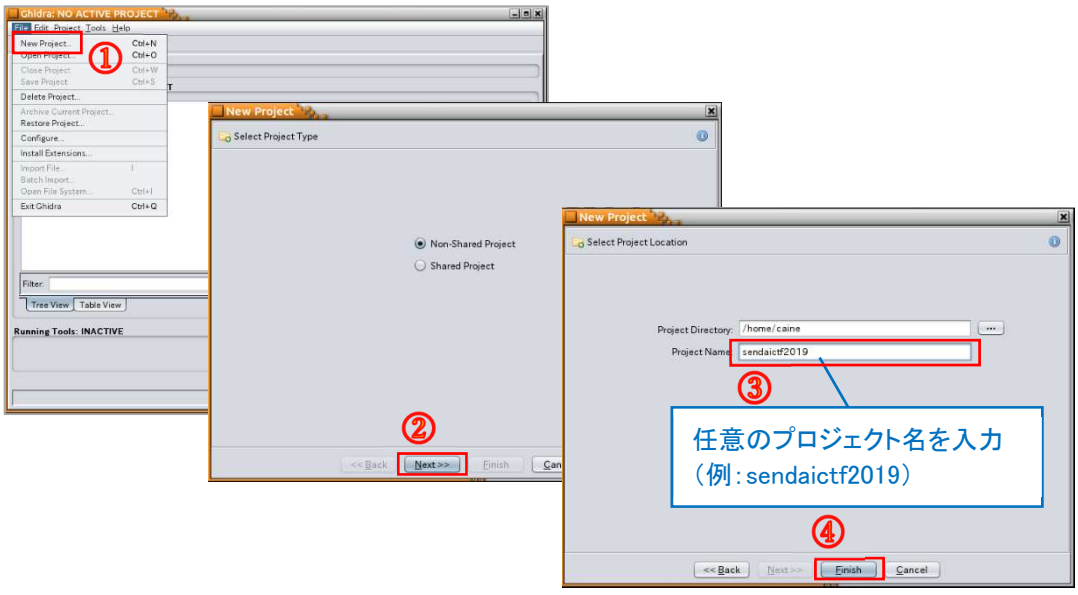
実習1の解説

解析ツール「Ghidra」で不審プログラムを解析します。

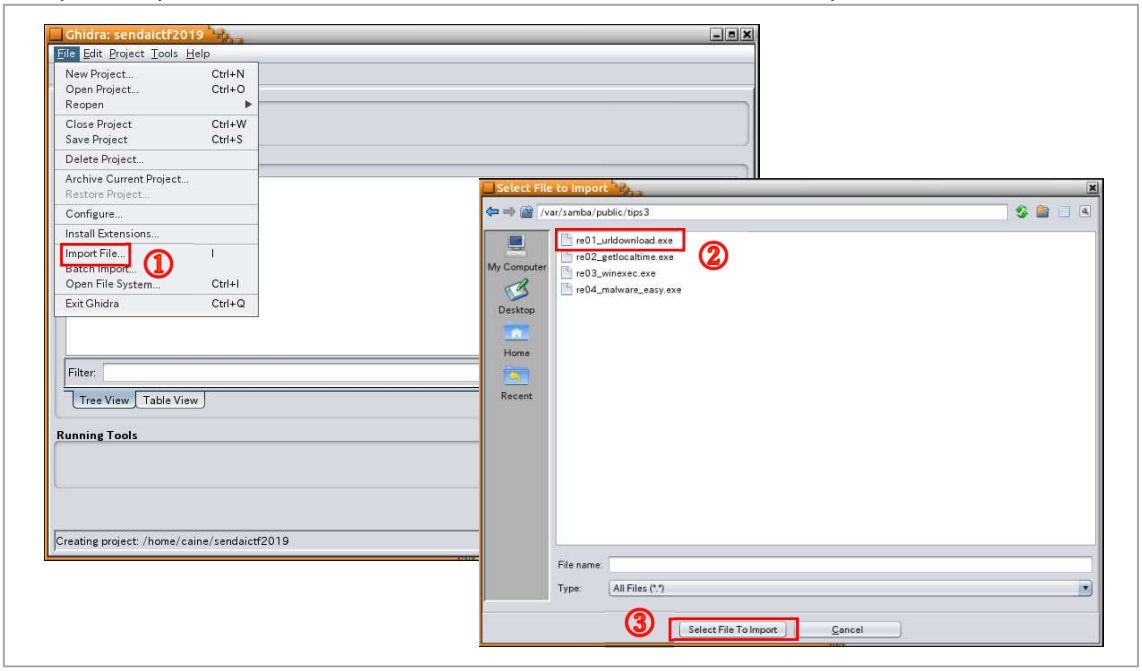
1. 実習用仮想マシン「Caine」を起動します。
2. 「Main Menu」-「Reverse Engineering」から「Ghidra」をクリックし起動します。
   「Tip of the Day」ダイアログは「Close」をクリックして閉じてください。



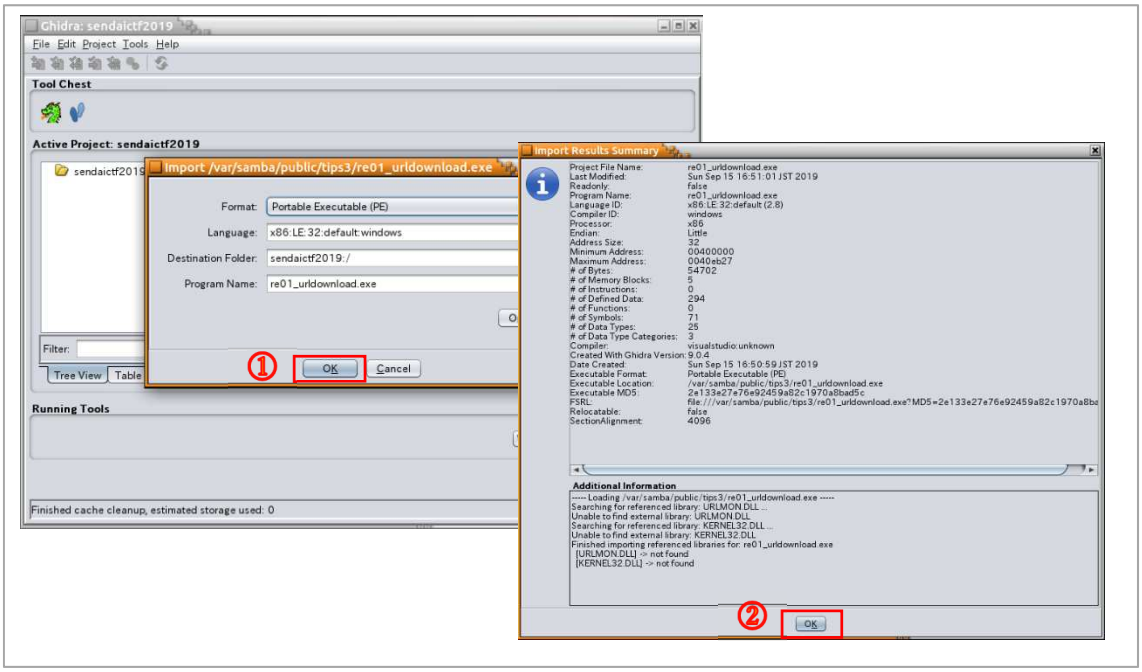
3. Ghidra のメニュー「File」-「New Project」をクリックします。
   「Non-Shared Project」が選択されていることを確認し「Next」をクリックします。
   「Project Name」に任意のプロジェクト名を入力し「Finish」をクリックします。



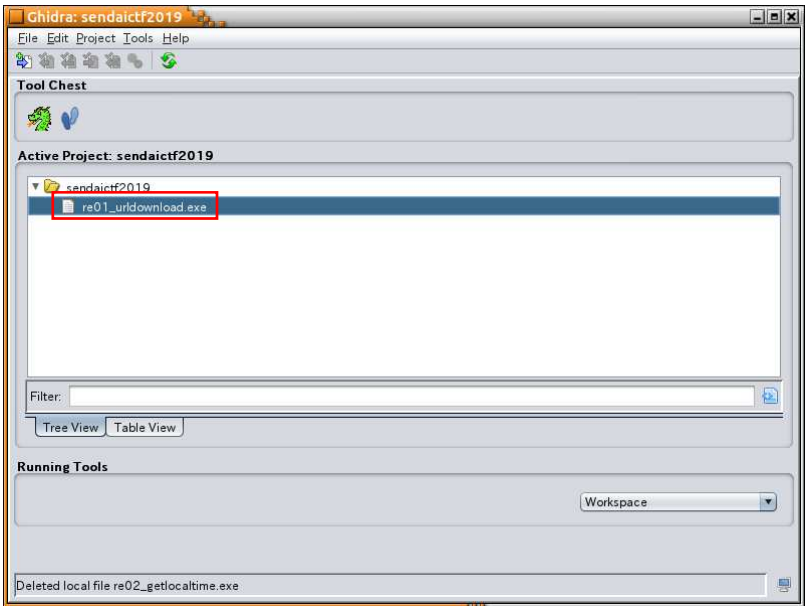
4. Ghidra のメニュー「File」-「Import File」をクリックします。
「Select File to Import」ダイアログで「My Computer」をクリックし、ディレクトリ「/var/samba/public/tips3」-「re01_urldownload.exe」を選択し「Select File To Import」をクリックします。



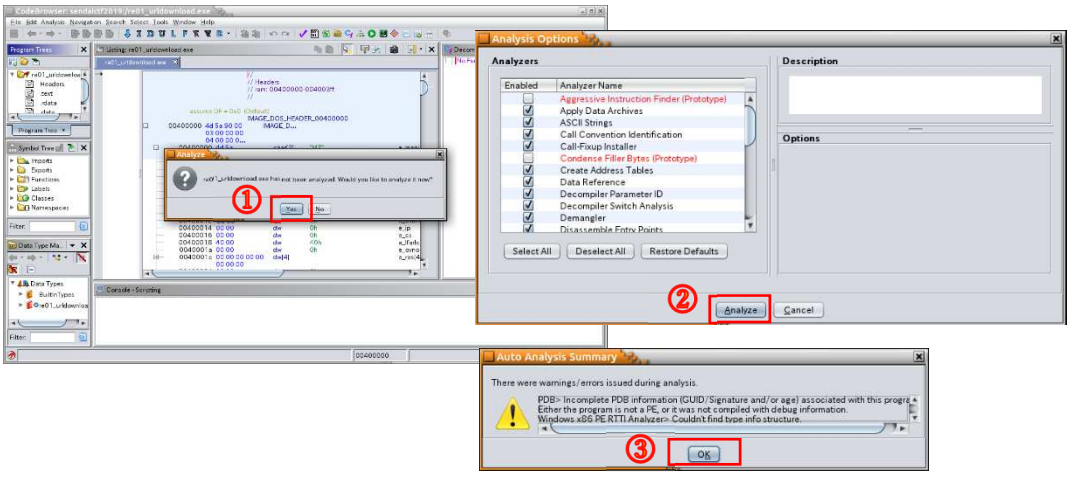
5. 解析対象ファイルの確認ダイアログが 2 回表示されますが、そのまま「OK」をクリックします。



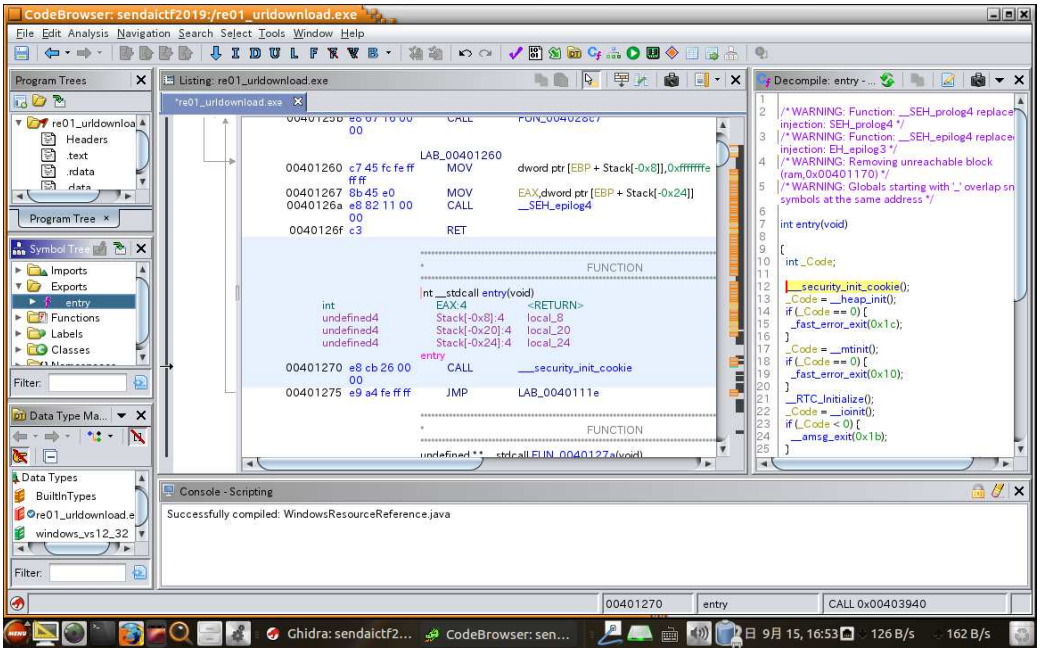
6. プロジェクトウィンドウに解析対象ファイルが追加されました。
解析対象ファイルをダブルクリックし「Code Browser」を開きます。



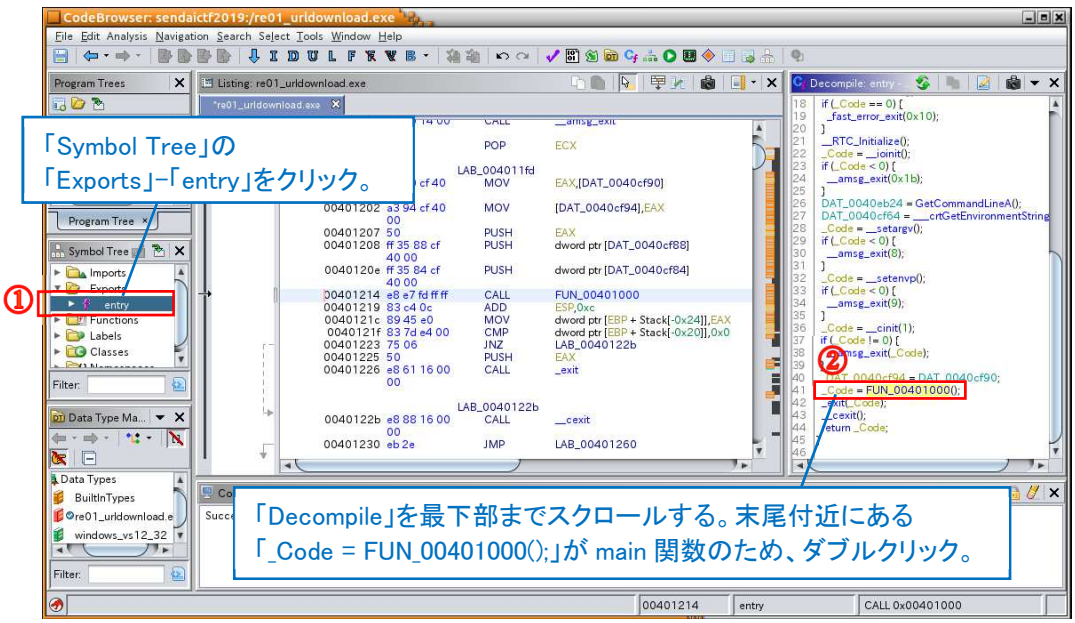
7. 「Analyze」ダイアログが表示されたら「Yes」をクリックします。
「Analysis Options」ダイアログは、そのまま「Yes」をクリックします。
自動解析処理が終了し「Auto Analysis Summary」ダイアログが表示されたら「OK」をクリックします。(PDB に関する警告が表示されますが問題ありません。)



8. Ghidra の画面が表示されます。
（他の実習でも、同様の手順で解析対象ファイルをインポートします。）



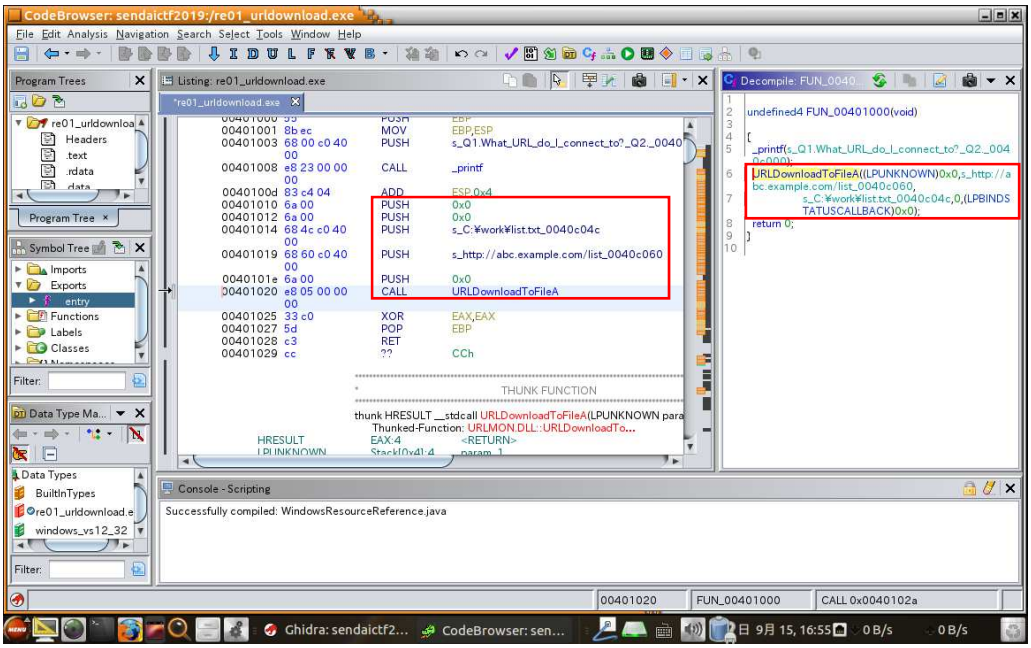
9. 下図手順で main 関数を表示します。
（他の実習でも、同様の手順で main 関数を表示します。）



10. main 関数（FUN_00401000）の「Listing」と「Decompile」から、
Windows API「URLDownloadToFileA」の引数を確認します。

［関数の説明］

URLDownLoadToFileA（0，ダウンロードする URL，ファイル保存先のフルパス，0，0）



11. 上記により、不審プログラムは「http://abc.example.com/list」からダウンロードしたファイルを「C:¥work¥list.txt」に保存することが分かります。

12. なお、「Code Browser」ウィンドウを閉じると、プロジェクトウィンドウに戻ります。
実習2以降は、プロジェクトウィンドウで手順4～手順8の操作を行い、解析対象ファイルをインポートしてください。

回答例

① 不審プログラムがダウンロードしたファイル名（保存先のフルパス）
C:¥work¥list.txt

② 上記①のダウンロード元 URL
http://abc.example.com/list

（空白ページ）

実習2（練習問題） 動作条件の特定

実習内容

練習用不審プログラム「re02_getlocaltime.exe」を解析し、不審プログラムが動作する条件を特定してください。

［実習用データ］

実習用仮想マシンに格納してあります。

フォルダ　：　/var/samba/public/tips3/
ファイル　：　re02_getlocaltime.exe

（補足） 実害の無いプログラムですが、ウイルス対策ソフトで検知される可能性があります。

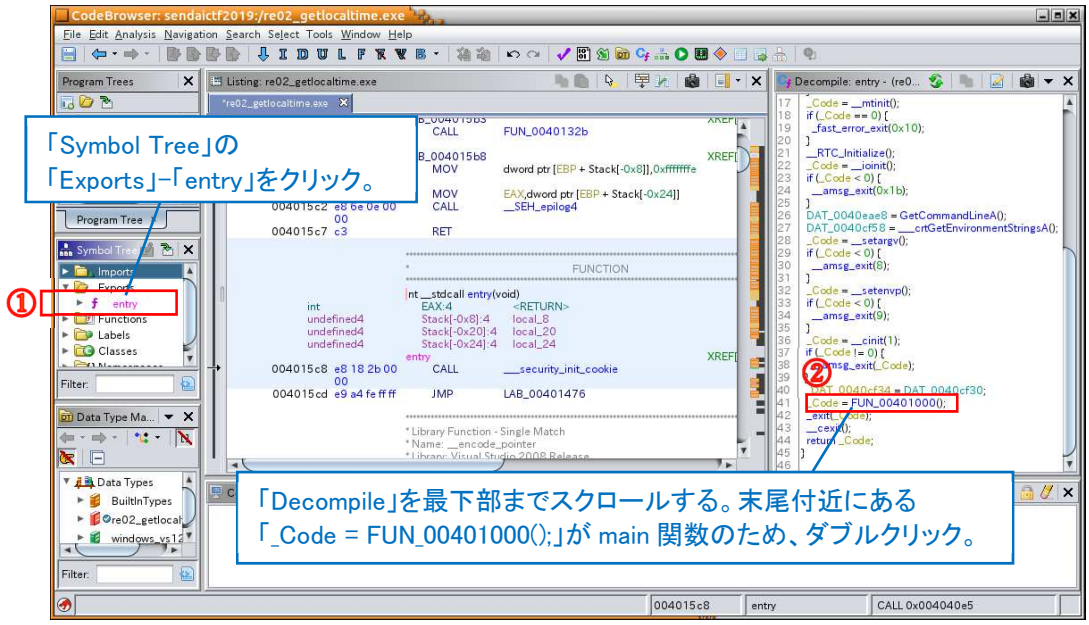
回答記入欄

不審プログラムが動作する条件

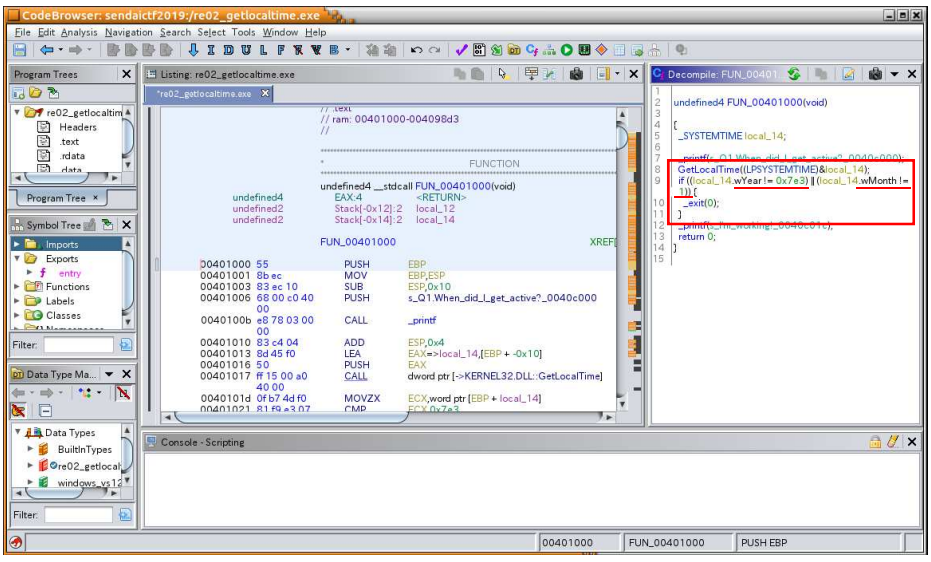
実習2の解説

解析ツール「Ghidra」で不審プログラムを解析します。

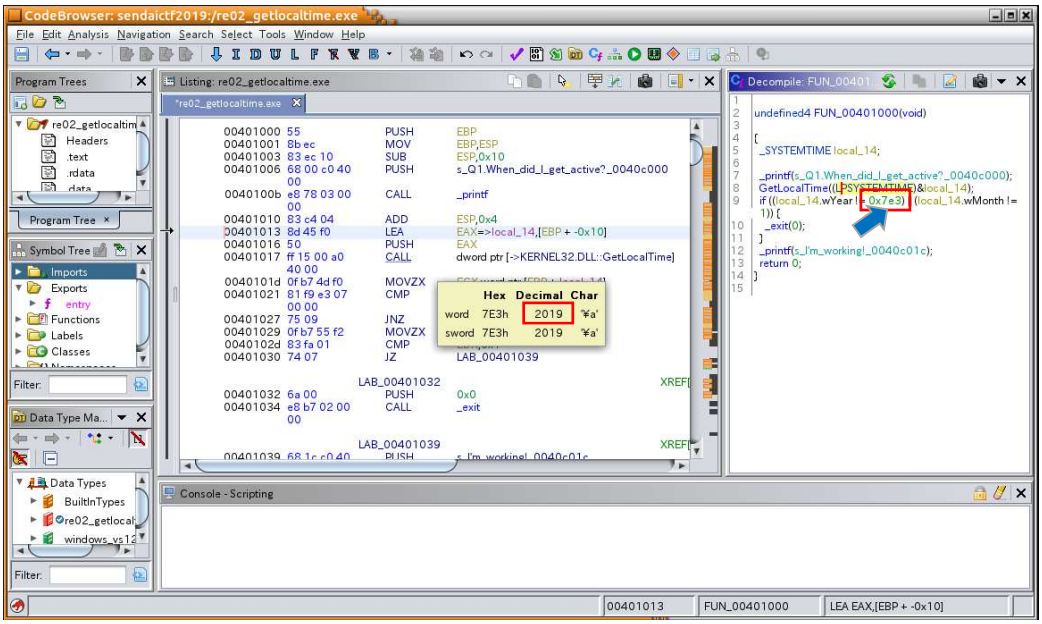
1. 実習用仮想マシン「Caine」を起動します。
2. 「Ghidra」を起動しプロジェクトウィンドウで「/var/samba/public/tips3/re02_getlocaltime.exe」をインポートし「Code Browser」を開きます。（詳細は、実習1の手順4～手順8を参照。）
3. 下図手順で main 関数を表示します。



4. main 関数の中で「GetLocalTime」関数を使用し現在時刻を取得しています。
その後、if 文で現在時刻を確認し、「年（西暦）」が「0x7e3」でない場合、または現在の「月」が「1」でない場合はプログラムを終了する処理となっています。



5. 「0x7e3」にマウスカーソルを合わせるとポップアップウィンドウが表示され、10 進数の「2019」であることが分かります。



回答例

不審プログラムが動作する条件

現在時刻が 2019 年 1 月の場合にのみ動作する。

（空白ページ）

実習3（練習問題） 起動される外部プログラムの特定

実習内容

練習用不審プログラム「re03_winexec.exe」を解析し、不審プログラムから起動される外部プログラムを特定してください。

［実習用データ］

実習用仮想マシンに格納してあります。

フォルダ　：　/var/samba/public/tips3/
ファイル　：　re03_winexec.exe

（補足） 実害の無いプログラムですが、ウイルス対策ソフトで検知される可能性があります。

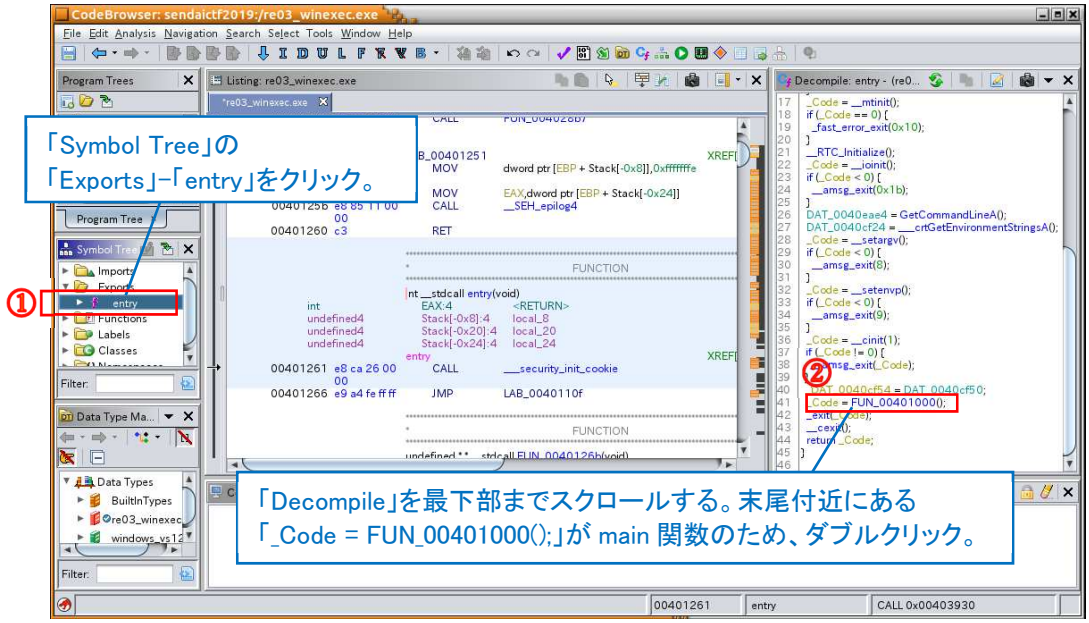
回答記入欄

不審プログラムから起動される外部プログラム名（フルパス）

実習3の解説

解析ツール「Ghidra」で不審プログラムを解析します。

1. 実習用仮想マシン「Caine」を起動します。
2. 「Ghidra」を起動しプロジェクトウィンドウで「/var/samba/public/tips3/re03_winexec.exe」をインポートし「Code Browser」を開きます。（詳細は、実習1の手順4～手順8を参照。）
3. 下図手順で main 関数を表示します。



4. main 関数の中で「WinExec」関数を使用し「C:¥Windows¥system32¥notepad.exe」（メモ帳）を起動しています。
   なお、第 2 引数に「0」が指定されているため、この不審プログラムから起動されたメモ帳は、ウィンドウが非表示となり、画面上では何も起きていないように見えます。

   [関数の説明]

   WinExec（起動したいプログラムのフルパス，ウィンドウの表示状態※1）

   ※1 NULL（0）を指定するとウィンドウが非表示となる。

回答例

不審プログラムから起動される外部プログラム名（フルパス）

C:¥Windows¥system32¥notepad.exe

実習4 情報流出したファイルの特定

実習内容

開発用サーバで実行された不審プログラム「re04_malware_easy.exe」を解析し、以下２点を特定してください。

① 情報流出したファイル名（フルパス）

② 上記①の送信先 FQDN

［実習用データ］

実習用仮想マシンに格納してあります。

フォルダ　：/var/samba/public/tips3/
ファイル　：re04_malware_easy.exe

（補足）実害の無いプログラムですが、ウイルス対策ソフトで検知される可能性があります。
本プログラムは、開発用サーバで実行された不審プログラム「malware.exe」を、実習で解析しやすいよう修正したものです。

回答記入欄

① 情報流出したファイル名（フルパス）

② 上記①の送信先 FQDN

実習４の解説

解析ツール「Ghidra」で不審プログラムを解析します。

1. 実習用仮想マシン「Caine」を起動します。
2. 「Ghidra」を起動しプロジェクトウィンドウで「/var/samba/public/tips3/re04_malware_easy.exe」をインポートし「Code Browser」を開きます。（詳細は、実習１の手順４～手順８を参照。）

3. main 関数（FUN_004011a0）を表示すると、以下の処理を行っていることが分かります。

（1） printf 関数でコンソールに「Q.Do you think I leaked your confidential data?」を印字。

（2） GetLocalTime 関数で現在時刻を取得し「2019 年 8 月」以外の場合は処理を終了。

（3） GetCurrentDirectory 関数でカレントディレクトリを取得。

（4） URLDownloadToFileA 関数で「http://c2.attacker.invalid/targets」からダウンロードしたファイルを、カレントディレクトリにファイル名「targets」で保存。

（5） WinExec 関数でカレントディレクトリの「ncrack.exe」を実行。その際(4)でダウンロードしたファイル「targets」を引数で指定。

（6） 関数「FUN_00401000」を呼び出し、以下の処理を実行。

（7） fopen 関数、fread 関数で本番データ「C:¥work¥sendaictf.csv」を読み込み。

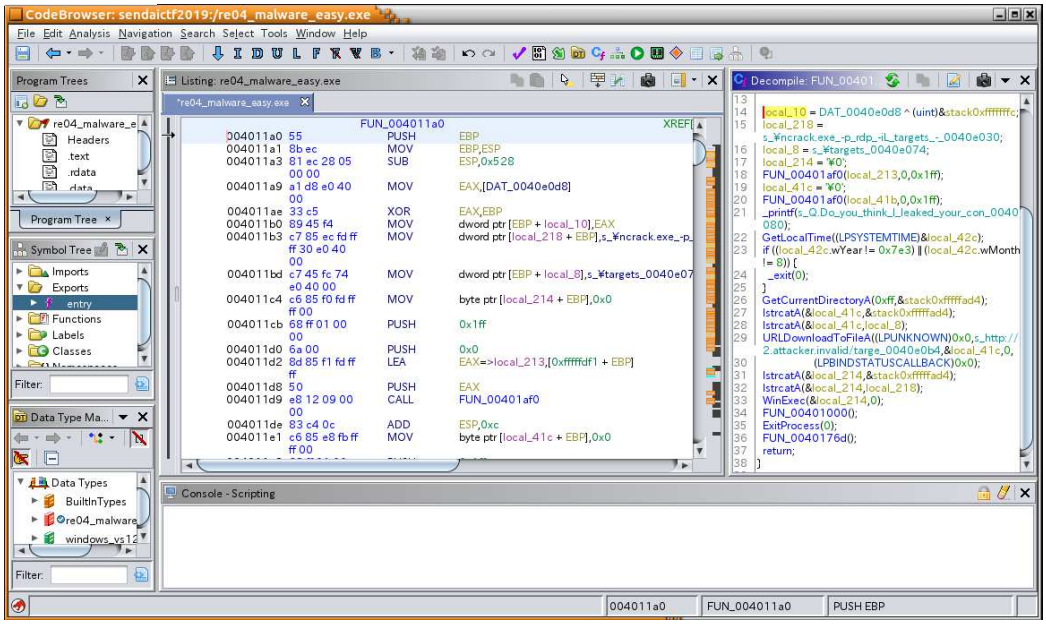
（8） FQDN と思われる文字列「c2.attacker.invalid」を引数として、不明な関数「Ordinal_N」を呼び出し。（N は数字 1～3 桁）
なお、「Symbol Tree」ウィンドウから「Ordinal_N」は WinSock ライブラリ（WSOCK32.DLL）の関数であることが分かる。

（9） 「Ordinal_N」は、本番データに対して何らかの処理を実施。

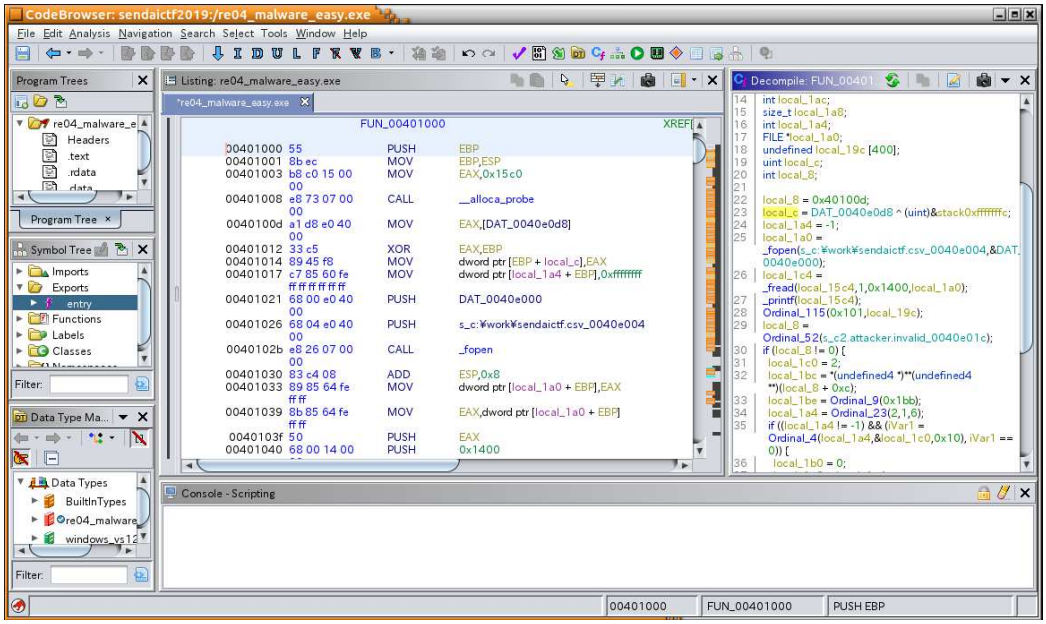
（10）「Ordinal_N」による処理は、WinSock によるネットワーク接続、データ送信の処理と類似しているが断定はできない。
（WinSock のテストコードをコンパイルし、Ghidra で表示すると特徴が一致する。）

4. 関数「Ordinal_N」の詳細が不明なため断定はできませんが、状況から本番データ「C:¥work¥sendaictf.csv」が「c2.attacker.invalid」に送信された可能性が疑われます。

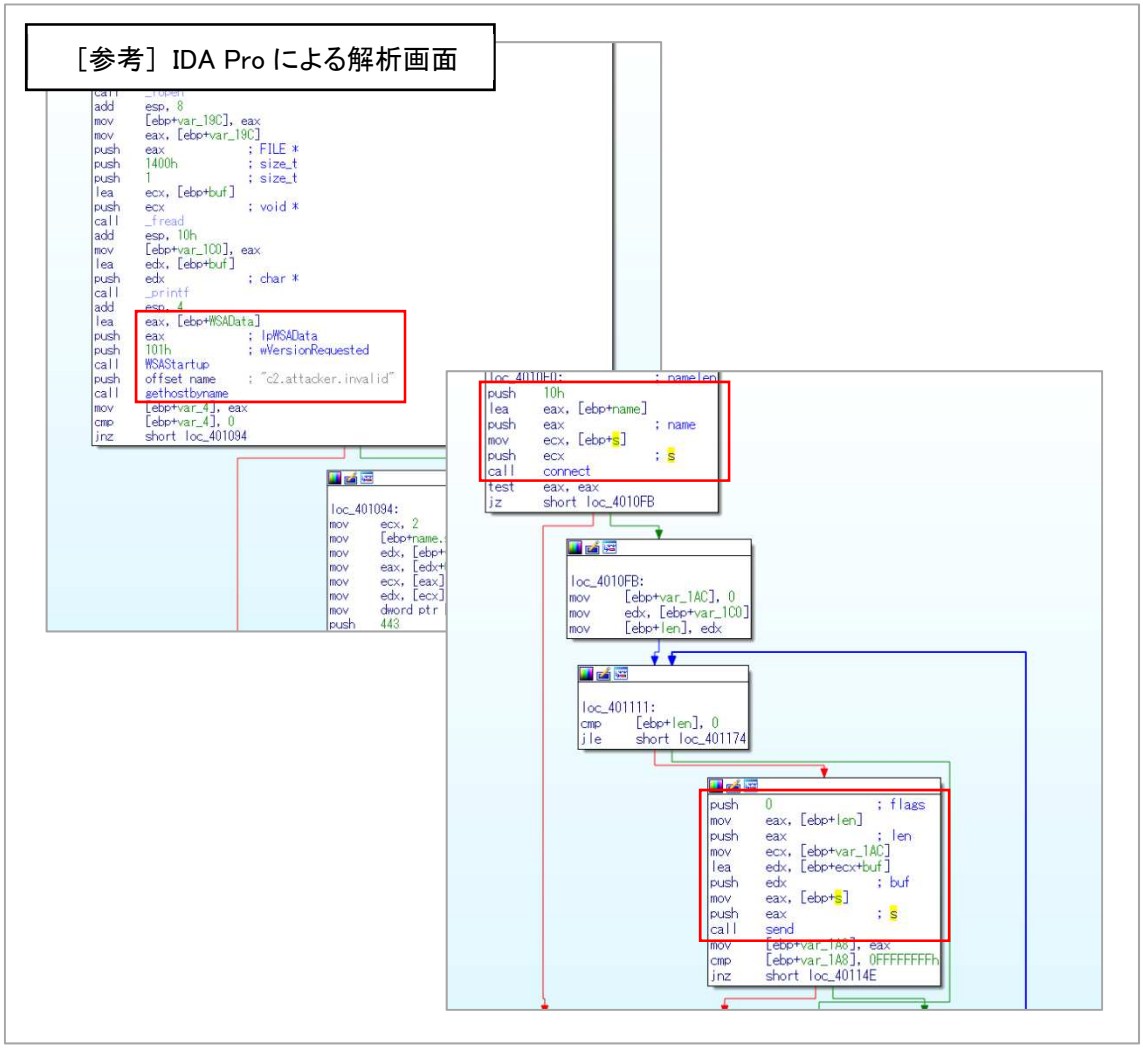
main 関数



不明な関数（FUN_00401000）



5. なお、IDA Pro で解析した場合は、WinSock の send 関数で本番データをネットワーク送信する状況を読み取ることができます。



回答例　※Ghidra による調査では「推測」

① 情報流出したファイル名（フルパス）
C:¥work¥sendaictf.csv

② 上記①の送信先 FQDN
c2.attacker.invalid

以上で演習は終了です。お疲れ様でした。