■マルウェア解析ハンズオン入門コース　～表層解析・簡易動的解析～受講における習得スキル項目一覧

NO		項目
1	マルウェアの知識	マルウェアとは何かを大まかに理解している
2		マルウェアの名称・分類(ドロッパー、ダウンローダ等)について理解している
3		最近のマルウェアの動作傾向についてある程度理解している
4		マルウェアの取り扱いに理解があり、適切に取り扱う事ができる
5	マルウェア解析環境	マルウェアを解析する環境におけるリスクを理解している
6		マルウェアを解析するに相応しい機器を準備する事ができ、安全にマルウェアを移動し解析することができる
7		マルウェアを解析するに相応しいネットワークを構築可能であり、マルウェアの動作に合わせて設定を変更できる
8		マルウェアを解析するに相応しいソフトウェア・サービスを準備する事ができ、マルウェアの動作に合わせて設定を変更できる
9		必要に応じてサンドボックスを選定、必要に応じて構築し、マルウェアの挙動を解析する事ができる
10	マルウェア解析概要	マルウェア解析の目的を理解しており、目標を絞る事ができる
11		マルウェア解析の流れを理解しており、表層解析・動的解析・静的解析の特徴を理解している
12		表層解析とは何かを説明する事ができる
13		動的解析とは何かを説明する事ができる
14		静的解析とは何かを説明する事が出来る
15		必要に応じて自らツールを検索して解析を進める事ができる
16		必要に応じてツールの表記について検索し、総合的に評価ができる
17	表層解析	表層解析について理解しており、流れを説明できる
18		ハッシュ値を算出するツールを使用し、マルウェアのハッシュ値を算出できる。また必要に応じて比較等に活用することができる
19		ファイルタイプを判定するツールを使用し、マルウェアのファイルタイプを判定できる。また、以降の解析をより効率的に行う事ができる
20		文字列を抽出するツールを使用し、マルウェアに含まれている文字列を抽出、大まかな機能にアタリをつけることができる
21		上記で抽出した情報からインターネットを通じて検索し、既知のマルウェアかどうかを判断し情報を収集する事ができる
22		簡易的な圧縮等の耐解析機能がファイルタイプから判明した場合、それを回避する事ができる
23		簡易的な難読化がある場合、それを簡易的に回避する手法を自ら検索して利用し、回避することができる
24	動的解析(簡易)	簡易的な動的解析について理解しており、流れを説明できる
25		マルウェアを監視状態に置きながら実行できる
26		プロセスの一覧を取得し、変更を検出できる
27		レジストリの一覧を取得し、変更を検出できる
28		ファイルの一覧を取得し、変更を検出できる
29		上記情報を駆使してマルウェアのインストール動作を特定し、感染有無診断や一時的な駆除方法について調査・報告できる
30		ネットワーク動作について調査し、マルウェアの通信内容を特定する事ができる
31		マルウェアが通信したいサービスを起ち上げて通信させることにより、より詳細にネットワーク活動を監視する事ができる
32		必要に応じてネットワークの設定を書き換え、より詳細にネットワーク活動を解析できるように調整できる
33	耐解析機能とその対応(簡易)	耐解析機能について理解している
34		一部の簡単な耐解析機能について検出することができ、状況によっては回避することができる

2015/7/15発行

■マルウェア解析ハンズオン入門コース　～表層解析・簡易動的解析～受講における習得スキル項目一覧

NO		項目
35	文書型マルウェア解析	文書型マルウェアの動作の概要について理解しており、おおよそ考えられる分類についても理解している
36		攻撃コードについて理解しており、その役割を説明できる
37		シェルコードについて理解しており、その役割を説明できる
38		シェルコードがどのようにして動くか理解しており、トリガーとなるポイントを抑える事ができる
39		文書型マルウェアにおける表層解析を行う事ができる
40		文書型マルウェアにおける動的解析を行う事ができる
41		必要に応じて、文書型マルウェアにおける静的解析(簡易)を行う事ができる
42	マルウェア解析入門・総合	一般的なマルウェアであれば、速報レベルのマルウェア解析報告書を作成することができる