株式会社ラック

■マルウェア解析ハンズオン専門コース～動的解析・静的解析～受講における習得スキル項目一覧

NO		項目
1	アセンブラの知識	アセンブラとは何かを大まかに理解している
2		アセンブラの基本構文を理解し、必要に応じて調査することができる
3		レジスタとその役割について理解し、必要に応じて調査することができる
4		アセンブラ上の関数の役割について理解し、必要に応じて調査することができる
5		スタックとその役割について理解し、必要に応じて調査することができる
6	デバッガの知識	デバッガの種類について理解し、対象のマルウェアに応じた適切なデバッガを選択することができる
7		デバッガの各種画面や表示項目について理解し、必要に応じて内容を変更するなどの操作ができる
8		デバッガを用いて読み込んだプログラムを実行させ、その地点での状況を確認できる
9		ブレークポイントとは何かを理解しており、それぞれの特徴と使い方を習得している
10		任意の地点にブレークポイントを仕掛けて利用することにより、把握したい特定地点での状況を素早く表示させることができる
11	解析環境検知とその対応	解析環境を検知する手法の存在を知っている
12		解析環境を検知する場所を特定することができる
13		解析環境の検知手法を回避することができる
14	マニュアルアンパック	パッキングされたマルウェアにおいて、初期動作の概要を理解している
15		実行形式ファイルのフォーマットを理解している
16		デバッガを用いてOEPまでマルウェアを実行できる
17		メモリをダンプして核となるマルウェアを取り出すことができる
18		ダンプしたメモリのIATを修正して取得したマルウェアを実行可能状態にすることができる
19	IDAを利用した静的解析	静的解析における基本的なポイントを理解している
20		IDAとは何かを理解している
21		IDAの移動・編集といった操作方法を会得しており、各画面を必要に応じて切り替えることができる
22		IATの修正の意義を理解しており、また修正することができる
23		使用されているAPIからどのような機能を持つか推測することができ、必要に応じて詳細に調査することができる
24		マルウェア全体から要調査ポイントを抑える事ができ、効率的に解析を行うことができる
25	マルウェア解析専門・総合	動的解析・静的解析を状況に応じて使い分け、効率的に解析を進めることができる
26		静的解析において、見るべきポイントを絞り込むことができる
27		マルウェアの全体像を想像しながらか解析することにより、より効率的な解析を行うことができる
28		状況に応じて必要な要素をインターネットから検索し、解析に役立てることができる
29		一般的なマルウェアであれば、詳細報告書を作成することができる