Malware-Labor

Inhalte	Das Experimentieren mit Malware-Samples ist der Fokus dieser Labor-LV. Dieses ist eine strukturierte, aufwändige Tätigkeit, die folgende wesentliche Merkmale aufweist: • Jedes Experiment besteht aus mehreren Phasen • Jede Phase umfasst mehrere Einzelschritte • Im Laufe der Untersuchung werden diverse statische und dynamische Analysen durchgeführt • Für jede Analyse ist i.d.R. der Einsatz von dedizierten Tools notwendig • ggf., jedoch nicht immer, müssen eigene spezifische Skripte ausgearbeitet werden • Die Vor- und Nachbereitung der Experimente ist ein wesentlicher Bestandteil eines Experiments
Textbuch	-
Weitere Quellen	Eine Liste der aktuellen Literatur und weiteren Quellen wird vor der LV bekanntgegeben.
Hinweise zur Vorbereitung auf die Veranstaltung	
Qualifikationsziele	Studierende können - systematische Verbreitung einer Untersuchung der Windows-Executives beim Verdacht einer Malware - eine Auswahl und Einsatz von Tools zwecks Malware-Analyse selbstständig durchführen - Malware-Samples statisch und dynamisch analysieren - die Fähigkeit entwickeln, die Nebeneffekte während einer dynamischen Analyse zu erkennen, zu dokumentieren und zu behandeln
Lehrformen, Sprache	Einleitende Vorlesung (1 SWS) plus Labor (3 SWS)
Voraussetzungen für die Teilnahme	Vorlesung IT Sicherheit bzw. eine ähnliche, sicherheitsrelevante LV
Darauf aufbauende Veranstaltungen, Querbeziehungen	
Voraussetzung für die Vergabe von Leistungspunkten	EA
Leistungspunkte	5
Arbeitsaufwand	60 Stunden Anwesenheitszeit und 90 Stunden für Vor- und Nachbereitung des Lehrstoffes, Prüfungsabnahme
Semester/Dauer	Semesterweise
Lehrende	Gharaei