Open Competence Center for Cyber Security

B E W E R T U N G S B O G E N
EQF-Bewertung

Zertifikat der Hochschule Albstadt-Sigmaringen (HSAS)

> Z e r t i f i k a t s a n g e b o t "O p e n C 3 S" <

Darmstadt der 09. April 2014

Open C³S

	Module des Zertifikatangebots > "Open C3S" < entsprechend der Modulbeschreibungen Stand September 2013	Erlernter Kompetenz-level nach EQF-Kategorien und EQF-Stufen
1	**Internettechnologien** (2 Monate / 150 Lernstunden / 5 ECTS) * Nach erfolgreichem Abschluss des Moduls hat der Studierende Kenntnisse über die grundlegenden Strukturen und möglichen Transportwege der Informationen im weltweiten Netz. Der Teilnehmer ist mit der für den Betrieb des Internets erforderliche Hard- und Software vertraut und kann deren Bedeutung für die IT-Sicherheit beurteilen. Er kann die aus dem Informationsfluss resultierenden digitalen Spuren bewerten und Ermittlungsansätze ableiten sowie Eigenschaften wichtiger Dienste nachvollziehen und diese einsetzen. Darüber hinaus hat er einen Überblick über die Sicherheitsaspekte der Netze und kann mögliche Tools sowohl bewerten als auch einsetzen. * Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung). **Lerninhalte:** **- Internet** Entstehung und Überblick; Organisationen; Infrastruktur (Netze, Dienstleister, Netzkomponenten, Geräte). **- Netzwerktechnik** Topologien und Kommunikationsarten; Überblick zu TCP-/IP-Schichten (Ethernet, WLAB, IPv4, IPv6, ICMP, TCP, UDP, Anwendungsschicht); Routing (DNS, Ports, VPN, Proxy, Firewall) **- Internet-Dienste** Datenaustauschdienste (FTP, Peer-to-Peer); Zugriffsdienste (Tel-net, SSH); E-Mail (Struktur, Clients, SMTP, POP, Signatur, Verschlüsslung, Sicherheit); Kommunikationsdienste (Chat, Internet-Telefonie, Skype). **- World Wide Web** Technik für die Kommunikation (HTTP, Session, Cookie, Verschlüsselung); Technik für den Betrieb einer Website (HTML5, CSS, JavaScript, Webbrowser, Webserver)	EQF-Kategorien / EQF-Stufe Kenntnisse Fertigkeiten Kompetenz

2

Datenträgerforensik 1

(2 Monate / 150 Lernstunden / 5ECTS)

* Nach erfolgreichem Abschluss des Moduls hat der Studierende grundlegende Kenntnisse über den physikalischen und logischen Aufbau von Datenträgern. Mittels Übungen hat der Studierende theoretische Betrachtungen mit praxisnahen Methoden und Werkzeugen zur Einrichtung und Untersuchung von Dateisystemen überprüft und reflektiert. Er kann verschiedene Werkzeuge zur Analyse und Wiederherstellung von Dateien auf Datenträgern einsetzen und verfügt über grundlegende Kenntnisse, die in dem zweiten Modul „Datenträgerforensik" weiter ausgebaut werden können.
  Dieses Modul fördert die Fachkompetenz auf dem Gebiet der Digitalen Forensik in besonderem Maße: die vertieften Kenntnisse und Fähigkeiten in einem Spezialgebiet führen zu einer starken Ausprägung der fachlichen Kompetenz.

Lerinhalte:

- In diesem Modul gehen wir auf die forensische Untersuchung von sogenannten Massenspeichern (engl. mass storages) ein. Massenspeicher sind Peripheriegeräte, die zur Speicherung großer Datenmengen dienen, wobei als Speichermedium meist magnetische oder optische Träger sowie neuerdings Flash-Speicherbausteine eingesetzt werden. Massenspeicher sind für forensische Untersuchungen von großer Bedeutung, da sie oft einschlägige Informationen enthalten und zudem Rückschlüsse auf Benutzer, Besitzer und Zugriffe ermöglichen. In dem ersten Modul von Datenträgerforensik werden grundlegende Konzepte vermittelt und erste praktische Übungen ohne Fokus auf ein Dateisystem durchgeführt.

1. Einführung, Festplattentechnik, Festplatten kopieren
- Technik klassischer Festplatten (Aufbau, Adressierung)
- Technik von Halbleiterspeichern (USB-Medien, Speicherkarten, geräteinterne Speicher mit USB Zugriff)
- Wear-Leveling
- Systematik zum Sichern von Speichermedien, Datensicherung einer Festplatte, Computerforensik-Programme
- Praktische Übung: Kopieren von Festplatten mit HPA, Datenträger kopieren

2. Datenträgeranalyse
- Master Boot Record
- Partitionstabellen
- Adressierung von Sektoren
- Globally Unique Identifier
- The Sleuth Kit und Autopsy
- Praktische Übung: Arbeiten mit The Sleuth Kit und Autopsy

3. Analyse von Dateisystemen
- Grundlagen
- Ansatz der Kategorisierung der Daten, Kategorien
- Praktische Übung: Arbeiten mit X-Ways und EnCase

EQF-Kategorien	EQF-Stufe
Kenntnisse	
Fertigkeiten	
Kompetenz	

3	**Datenträgerforensik 2** (2 Monate / 150 Lernstunden / 5ECTS) * Nach erfolgreichem Abschluss des Moduls hat der Studierende einen Überblick über die verbreitetsten Datei- und Betriebssysteme sowie deren Funktionsweisen. Er hat grundlegende Kenntnisse über den physikalischen und logischen Aufbau von Datenträgern sowie gängiger Dateisysteme der Windows-Betriebssystemfamilie und bei den Unix-Derivaten. Mittels Übungen hat der Studierende theoretische Betrachtungen mit praxisnahen Methoden und Werkzeugen zur Einrichtung und Untersuchung von Dateisystemen überprüft und reflektiert. Er kann mit verschiedenen Werkzeugen zur Analyse und Wiederherstellung von Dateien auf Datenträgern umgehen und verfügt sowohl über analytische als auch methodische Fähigkeiten im Umgang mit diesen. Dieses Modul fördert die Fachkompetenz auf dem Gebiet der Digitalen Forensik in besonderem Maße: die vertieften Kenntnisse und Fähigkeiten in einem Spezialgebiet führen zu einer starken Ausprägung der fachlichen Kompetenz. **Lerninhalte:** - In diesem Modul werden die Dateisysteme FAT, ExtX und NTFS näher betrachtet. Dieses Modul stellt somit die ideale Ergänzung zu Datenträgerforensik 1 dar und vertieft die Grundlagen, die in dem vorangeführten Modul behandelt wurden. Die einzelnen Studienbriefe sind in sich geschlossen und auch die praktischen Übungen sind auf die einzelnen Dateisysteme speziell abgestimmt. **1. FAT- Dateisysteme:** - Überblick und Vergleich der unterschiedlichen FAT-Dateisysteme (FAT12/16/32) - Bedeutung, Verbreitung und Kompatibilität des FAT-Dateisystems - Allgemeines Partitionsschema des FAT-Dateisystems (MBR, VBR, FAT, Root-Verzeichnis und Datenbereich) - Funktionsweise der File Allocation Table - Aufbau und Organisation von Datei- und Verzeichniseinträgen - VFAT , Dienstprogramme in Zusammenhang mit dem FAT-Dateisystem (z.B. format.exe, attrib.exe und die Windows Datenträ-gerverwaltung) - Praktische Übung: Beispielhafte Einrichtung eines FAT-Dateisystems; Analyse mit Autopsy: Filesystem erkunden, gelöschte Dateien suchen, gelöschte Dateien wiederherstellen **2. NTFS-Dateisystem:** - Allgemeine Informationen über das NTFS-Dateisystem (Einführung eines Berechtigungskonzepts und die Möglichkeit von Mountpoints und Quotas) - Allgemeiner Aufbau von NTFS-Basisdatenträgern (MBR, VBR, MFT) - Aufbau und Funktionsweise der Master File Table sowie deren Record-Einträge (residente und nicht-residente Dateien und Data Runs) - Weitere wichtige Metadaten (Logfile für das Transaction Logging usw.) - Verzeichnisse - Weitere Features des NTFS-Dateisystems (z. B. Kompression, Ver-schlüsselung und Alternative Datenströme) - Dienstprogramme in Zusammenhang mit dem NTFS-Dateisystem (DiskPart.exe, fsutil.exe und die Windows Datenträgerverwaltung) - Praktische Übung: Beispielhafte Einrichtung eines NTFS-Datei-systems; Analyse mit x-Ways, Encase: Filesystem erkunden, gelöschte Dateien suchen, gelöschte Dateien wiederherstellen	

EQF-Kategorien	EQF-Stufe
Kenntnisse	
Fertigkeiten	
Kompetenz	

4	**Einführung in die Informatik** (150 Lernstunden / 5 ECTS) * Die Studierenden haben Kenntnisse über Instrumente und Methoden der Informatik. Sie haben insbesondere grundlegende Kenntnisse in der praktischen, technischen und theoretischen Informatik. * Sie können Darstellungsformen und -formaten von Informationen in Rechnern interpretieren und umwandeln. Die Grundzüge von Rechnern und die Aufgaben unterschiedlicher Software wurden erlernt. Grundlegende Kenntnisse der IT-Sicherheit wurden erworben. * Die praktischen Übungen versetzen den Studierenden in die Lage, an einem Rechner Datenformate und die Konfiguration eines Arbeitsplatzrechners zu analysieren. Der Studierende kann virtuelle Maschinen und darauf basierende Anwendungen und Konfigurationen einrichten. Darüber hinaus kann er fundamentale Maßnahmen zur IT-Sicherheit eines Arbeitsplatzrechners umsetzen und deren Wirkung überprüfen. * Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung). **Lerninhalte:** - In diesem Modul werden die technischen Kenntnisse vermittelt, die ein IT-Sicherheitsexperte braucht, um ein Rechnersystem verstehen und zusammenstellen zu können. Auf der Grundlage des Verständnisses der Hardware-Architektur werden die vom Betriebssystem und den Anwenderprogrammen bewerkstelligten Verarbeitungsschritte klar. In diesem Gesamtzusammenhang werden die grundsätzlichen IT-Angriffsmöglichkeiten und IT-Schutzmechanismen verständlich. **1. Informationsverarbeitung im Computer** Daten-Einheiten, Binäre Vielfache, Zahlensysteme, Zeichensätze/-kodierung, Byte-Reihenfolge, Logische Operatoren Praktische Übung: Codierung einer Textdatei **2. Rechnersysteme** Historische Entwicklung, Aufbau eines Rechners, Rechnerstruktur, Zentraheinheiten, Prozessorarchitektur, Speicherhierarchie, Peripherie-komponenten, Moderne Rechner, Rechnerklassen **3. Software** Zusammenspiel von Hard- und Software, Klassifizierung, Betriebssysteme, Firmware, Virtuelle Maschinen **4. IT-Sicherheit** Hackerparagraph, Schutzziele, Angriffstypen, spezielle Bedrohungen, Angriffsszenario im WWW, Sniffer, Klartext vs. Verschlüsselung, Härten von Betriebssystemen Praktische Übung: Angriffsszenario in einer sicheren Umgebung nachbilden	EQF-Kategorien / EQF-Stufe Kenntnisse Fertigkeiten Kompetenz

5	**Einführung in die Programmierung im IT-Security-Umfeld** (2 Monate / 150 Lernstunden / 5 ECTS) * Die Studierenden können aus einer abstrakten Aufgabenstellung ein ablauffähiges Programm entwickeln. Wenn die Programmierung konkret wird, so findet die Programmiersprache Python Verwendung. Python ist eine leistungsfähige Skriptsprache, die im Forensik-Umfeld häufig verwendet wird. Die Grundkonstrukte von Programmen und deren Umsetzung in Python wurde erlernt. Die Studierenden haben erste Erfahrungen mit programmbasierten Sicherheits-Schwachstellen und verstehen einfachen Angriffsmechanismen. Die Studierenden können mit den selbst erstellten Programmen häufig in der Praxis vorkommende Aufgabenstellungen bewältigen wie z. B. das Durchsuchen eines Rechners nach auffälligen Bildern (Zuwachs an Methodenkompetenz). Dieses Modul fördert die Selbstkompetenz durch das unterstützte Selbstlernen bei den praktischen Aufgabenstellungen in besonderem Maße (Erarbeitung von Lösungen in einem festgelegten Zeitrahmen, Hilfe holen bei Bedarf, Erkenntnisgewinn aus korrigierter Lösung). **Lerninhalte:** - In diesem Modul werden die Kenntnisse in Informatik und Programmieren vermittelt, die in IT-Sicherheitsexperte braucht, um für ein Rechnersystem spezifische Programme zur Analyse des IT-Sicherheitsstands vornehmen zu können sowie um sicherheitsrelevante Vorgängen überprüfen zu können. Damit ist auch die Grundlage für einen guten Einstieg zum Erlernen weiterer Programmiersprachen gelegt. **1. Grundlagen Python** Praktische Übung: Erstellen eines Programms, dass Dateien sucht und diese anhand des Dateityps kategorisch sortiert. In einer gleichnamigen txt-Datei werden Informationen über die Datei festgehalten. **2. Datenbanken mit Python** Praktische Übung: Ergänzung und Optimierung der praktischen Übung aus SB1, txt-Dateien durch Datenbankeinträge ersetzen, Suchanfragen über sqlite3 realisieren **3. Penetration Testing mit Python** Praktische Übung: Optimierung der im Studienbrief vorgestellten Programme **4. Forensik mit Python** Praktische Übung: Optimierung der im Studienbrief vorgestellten Programme **5. Netzwerkanalyse mit Python** Praktische Übung: Optimierung der im Studienbrief vorgestellten Programme	

EQF-Kategorien	EQF-Stufe
Kenntnisse	
Fertigkeiten	
Kompetenz	

Gefördert vom:
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
AUFSTIEG DURCH BILDUNG >> OFFENE HOCHSCHULEN