**Lektion 1**

**1.1**

1. Markieren Sie die richtige Antwort.
In welchen zwei Sicherheitsmodi kann Code ausgeführt werden?
	1. Sicherer und unsicherer Modus
	2. Lehrer- und Schülermodus
	3. *Benutzer- und Kernel-Modus*
	4. Amateur- und Profimodus

**1.2**

1. Markieren Sie die richtige Antwort.
Auf welcher Ringebene liegen die höchsten Privilegien für Prozesse?

1. *Ebene 0*
2. Ebene 1
3. Ebene 2
4. Ebene 5

**1.3**

1. Welche digitalen Spuren (Artefakte) werden bei der Analyse von RAM wahrscheinlich gefunden?
	1. Die Schuhgröße der Benutzer:innen
	2. Das Kaufdatum des Computers
	3. *IP-Adressen*
	4. Wann der Computer zuletzt eingeschaltet wurde

**1.4**

1. Welches RAID verfügt über einen Wiederherstellungsmechanismus?
	1. RAID 0
	2. *RAID 5*
	3. RAID 17.5
	4. RAID 100

**1.5**

1. Welche der folgenden Antworten beschreibt das folgende Problem am besten?
Zur Verwaltung der Reaktionszeit auf Ein-/Ausgabeanforderungen muss eine unterbrechungsgesteuerte E/A oder eine programmierte E/A implementiert werden.
	1. Speicherbezogene E/A (Memory-mapped I/O)
	2. Channel I/O
	3. *Systemreaktion*
	4. Geräteunabhängigkeit

**Lektion 2**

**2.1**

1. Der *Kernel-Modus* ist der Modus, in dem die Systemprozesse und ‑abläufe ausgeführt werden und vollen Zugriff auf den Speicherbereich und die Hardware haben.

**2.2**

1. Zum Prozesssteuerungsblock gehört die *Speicherzuweisung*.

**2.3**

1. Die Registry ist \_\_\_\_\_ des Windows-Betriebssystems.
	1. die Seele
	2. der Finger
	3. der Zeh
	4. *das Herz*

**2.4**

* 1. Welches Dateisystem können die Betriebssysteme Microsoft Windows, Mac OS und Linux standardmäßig lesen \_\_\_\_\_\_?
		1. NTFS
		2. EXT 3
		3. APFS
		4. *FAT32*

**2.5**

* 1. Vervollständigen Sie den folgenden Satz:
	Return-to-libc ist ein Angriff des Typs \_\_\_\_\_\_.
		1. Mummy
		2. Byte-Switching
		3. *Pufferüberlauf*
		4. Key-Logger

**Lektion 3**

**3.1**

1. Markieren Sie die richtige Antwort.

Welche der folgenden Adressen ist eine Klasse-A-Adresse?

* *45.152.86.9*
* 137.23.1.251
* 192.168.86.5
* 155.55.22.8

**3.2**

1. Markieren Sie die richtige Antwort.

Welcher der folgenden Datensätze enthält Links von Aliasnamen zu einem anderen Domänennamen?

* AName
* BName
* *CName*
* DName

**3.3**

1. Welcher Protokollaufruf wird zum Schutz der Benutzer:innen bei der Nutzung eines Webbrowsers verwendet?

* HTTP
* *HTTPS*
* DNS
* Sicheres IRC

**3.4**

1. Markieren Sie die richtige Antwort.

Welcher der folgenden Algorithmen ist ein Hashing-Algorithmus?

* AES
* *MD5*
* TLS
* SSL

**3.5**

1. Markieren Sie die richtige Antwort.

Welchen Verschlüsselungscode könnte der Absender einer E-Mail verwenden, um die Vertraulichkeit der Kommunikation zu schützen?

* *Öffentlicher Schlüssel des Empfängers*
* Privater Schlüssel des Empfängers
* Öffentlicher Schlüssel des Absenders
* Privater Schlüssel des Absenders

**Lektion 4**

**4.1**

1. Markieren Sie die richtige Antwort.

Ein forensisches DD-Image ist standardmäßig komprimiert.

* Wahr
* *Falsch*

**4.2**

1. Markieren Sie die richtige Antwort.

Zum Aufzeichnen von RAM kann Volatilität verwendet werden.

* Wahr
* *Falsch*

**4.3**

1. Markieren Sie die richtige Antwort.

Nach welcher der folgenden Informationskategorien werden Angreifer:innen suchen?

* *Persönlich identifizierende Informationen (PII)*
* SQL-Datenbank
* Lizenzschlüssel für das Windows-Betriebssystem
* E-Mail-Laufzeiten

**4.4**

1. Markieren Sie die richtige Antwort.

Welche der folgenden Methoden wird bei der Steganografie verwendet?

* Datenvermittlung
* Datenaufteilung
* *Einfügen von Daten*
* Spiegelung von Daten

**Lektion 5**

**5.1**

1. Markieren Sie die richtige Antwort.

Im F3EAD-Modell wird die Exploit-Phase für Folgendes genutzt:

* *Sammeln von Informationen*
* Ermitteln von Bedrohungen
* Lokalisieren von Angreifer:innen
* Teilen von Informationen

**5.2**

1. Markieren Sie die richtige Antwort.

Der erste Schritt in der Anatomie eines Angriffs ist:

* Root-Zugang
* Datenexfiltration
* *Zielphase*
* Dateninfiltration

**5.3**

1. Markieren Sie die richtige Antwort.

Wie viele Schritte umfasst der „Erkenntniszyklus“?

* 4
* 5
* *6*
* 7

**Lektion 6**

**6.1**

1. Markieren Sie die richtige Antwort.

Wofür ist APT28 ein Beispiel innerhalb des MITRE-ATT@CK-Rahmens?

* + *Bedrohungsgruppe*
	+ Strategie
	+ Anforderungen
	+ Voraussetzungen

**6.2**

1. Markieren Sie die richtige Antwort.

Welcher der folgenden IDPS-Typen ist für die Überwachung des Datenverkehrs und der Ereignisse auf einem bestimmten Host zuständig?

* Verhaltensanalyse
* Netzwerkbasiert
* *Host-basiert*
* Benutzerbasiert

**6.3**

1. Markieren Sie die richtige Antwort.

Mit welchen der folgenden Techniken können Angreifer:innen Malware verstecken?

* Umbenennung
* *Verpacken (Packing)*
* Auffüllen
* Clipping