Probeklausur „Cybercrime und IT-Forensik“

Name:

Matrikelnummer:

Bearbeitungszeit: 90 Minuten

Erlaubte Hilfsmittel: Nicht programmierbarer Taschenrechner

Allgemeine Bearbeitungshinweise:

- Die Prüfung besteht (inklusive Deckblatt) aus insgesamt **12 Seiten**. Bitte **überprüfen** Sie, ob Ihnen **alle Seiten vorliegen**.
- Schreiben Sie bitte **leserlich**.
- Wenn Sie **mehr Platz** benötigen, dann verwenden Sie bitte die **Rückseite** oder fragen Sie Ihre Prüfungsaufsicht nach **mehr Papier**.

Aufgabe	Thema	Punkte	Max. Punkte
1	Cybercrime		28
2	IT-Forensik		22
3	Forensic Imaging		12
4	Slack-Space		14
5	Datenvernichtung		15
6	Entropie		13
7	RAM-Forensik		20
8	CSI-Linux		16
∑			140

Erreichte Punktzahl: | Notenbonus:

Prozent (%)	Punkte

Punktzahl: (inkl. Notenbonus)

Note:

Unterschrift: (Dozent)

Aufgabe 1 (ca. 26 P.):

(a) Erklären Sie den Unterschied zwischen Cybercrime im *engeren* und im *weiteren* Sinne:

(b) Was versteht man unter *MaaS*?

(c) Erklären Sie den Unterschied zwischen *Cybercrime* und *Cyberspionage*:

(d) Beschreiben Sie eine nach § 303b StGB (Computersabotage) strafbare Handlung:

(e) Erklären Sie, was man unter *Cybergrooming* versteht:

(f) Erklären Sie, was man unter *Sextortion* versteht:

(g) Eine Person sitzt morgens in einer vollbesetzten U-Bahn und hat ihr Smartphone in der Hand. Plötzlich erscheint auf dem Display eine AirDrop-Anfrage von einem unbekannten Gerät in der Nähe. Ohne Vorwarnung wird ihr ein Bild angezeigt, das den nackten Genitalbereich einer fremden Person zeigt. Die betroffene Person kennt den Absender nicht, hat keinen Kontakt gesucht und keine Zustimmung zum Empfang solcher Inhalte gegeben. Sie befindet sich in einem öffentlichen Raum, kann die Situation nicht sofort verlassen und fühlt sich überrumpelt, beschämt und belästigt. Wie lautet der Fachbegriff für diese Art von Belästigung?

(h) Erklären Sie, wie *Project VIC* technisch funktioniert:

Aufgabe 2 (ca. 22 P.):

(a) Erklären Sie, was man unter der *Chain of Custody* versteht.

(b) Erklären Sie, was man unter der *Locard'schen Regel* versteht.

(c) Erklären Sie, wie man in der IT-Forensik beim *SAP-Modell* vorgeht:

(d) Im Rahmen der Analyse eines Datenträgers wurde ein PDF-Dokument mit dem Namen `vertrag.pdf` sichergestellt. Geben Sie einen Befehl an, mit dem Sie die Metadaten dieses PDF-Dokuments extrahieren können:

(e) Angenommen, ein Täter möchte so wenig Spuren wie möglich auf einem potenziellen Asservat hinterlassen. Welchen Befehl könnte er verwenden, um sein Ziel für das in Aufgabenteil (d) sichergestellte PDF-Dokument `vertrag.pdf` zu erreichen?

(f) Erklären Sie, was man unter *Chain-Hopping* versteht und wie es IT-Forensikern die Arbeit erschwert:

(g) Welche Technik verwenden Kriminelle neben Chain-Hopping noch, um Kryptowährungen zu verschleiern?

(h) Welches Gerät in einem Forensik-Koffer verhindert Schäden durch elektrostatische Entladungen beim Ausbau von Festplatten oder anderen sensiblen Komponenten?

Aufgabe 3 (ca. 12 P.):

(a) Erklären Sie, was man unter *Forensic Imaging* versteht.

(b) Welche Funktion haben *Hashwerte* beim Erstellen von forensischen Images?

(c) Warum werden trotz moderner Hashalgorithmen wie SHA256 für forensische Images häufig noch (veraltete) MD5-Hashwerte berechnet?

(d) IT-Forensiker finden bei einer Hausdurchsuchung ein RAID1-System vor. Wie viele Festplatten müssen in diesem Fall forensisch analysiert werden, um alle potenziell beweiserheblichen Daten abzudecken? Begründen Sie Ihre Antwort.

Aufgabe 4 (ca. 14 P.):

(a) Erklären Sie, was man unter dem *RAM-Slack* versteht.

(b) Die Sektoren auf einem Datenträger sind 512 Bytes groß und acht Sektoren bilden ein Cluster. Wie viele Cluster werden zum Speichern einer 10.234 Bytes großen Datei benötigt?

(c) Wie viel Platz nimmt die Datei aus Aufgabenteil (b) auf dem Datenträger ein?

(d) Berechnen Sie mit den Daten aus Aufgabenteil (b) und (c) die Größe des RAM-Slacks:

Aufgabe 5 (ca. 15 P.):

(a) Erklären Sie, was man im forensischen Kontext unter *Wipen* versteht:

(b) Wie funktioniert die *Gutmann-Methode* zum sicheren Löschen von Festplattendaten?

(c) Löschen Sie mit einem geeigneten `dc3dd`-Befehl das Laufwerk `/dev/sdX` forensisch sicher. Dabei soll ein SHA256-Hash über den gelöschten Datenträger zur Dokumentation der Integrität berechnet werden:

(d) Warum reicht der Befehl aus Aufgabenteil (c) nicht aus, um SSD-Festplatten forensisch sicher zu löschen?

Aufgabe 6 (ca. 13 P.):

(a) Erklären Sie, was man unter dem Begriff *Entropie* versteht.

(b) Berechnen Sie die Shannon-Entropie des Strings `abba`:

(c) Geben Sie eine zehn Byte große Datei mit maximaler Entropie in der Form

`[x0, x1, x2, x3, …, x9]`

an, wobei `x0`, `x1`, `x2` etc. Bytes in Dezimalform sind, die die Werte `0` bis `255` annehmen können.

Aufgabe 7 (ca. 20 P.):

(a) Was versteht man unter einer *Live-Analyse*?

(b) Welche rechtliche Herausforderung ergibt sich bei der Analyse des RAMs bezogen auf die Chain of Custody?

(c) Warum ist die Windows-Registry für forensische Analysen so wertvoll?

(d) Suchen Sie mit einem geeigneten Befehl in dem RAM-Dump `asservat.vmem` nach dem Passwort `abc123`:

(e) Suchen Sie mit einem geeigneten Befehl in dem RAM-Dump `241225.vmem` nach dem Truecrypt-Passwort des Beschuldigten:

Aufgabe 8 (ca. 16 P.):

Kreuzen Sie die richtigen Antworten an. Pro Frage ist jeweils nur genau eine Antwortmöglichkeit richtig. Für eine korrekte Antwort erhalten Sie zwei Punkte. Für eine falsche Antwort erhalten Sie zwei Punkte Abzug. Insgesamt können Sie in der Aufgabe maximal 16 und minimal 0 Punkte erreichen. Wenn Sie eine Frage nicht beantworten, erhalten Sie dafür 0 Punkte.

(a) Ein Ermittler möchte zusätzliche Windows-Tools auf dem CSI-Linux-Triage-Laufwerk installieren. Was sollte er vorher sicherstellen?

☐ Dass GParted ausgeführt wird.

☐ Dass Secure Boot deaktiviert ist.

☐ Dass sich eine NTFS-Partition auf dem Laufwerk befindet.

☐ Dass das Triage-Laufwerk unter Linux eingehängt (gemountet) ist.

(b) Ein Forensiker richtet CSI-Linux in VMware Workstation ein und muss die heruntergeladenen Dateien entpacken. Welches Tool sollte er verwenden?

☐ HDD Raw Copy Tool

☐ GParted

☐ 7-Zip

☐ Clonezilla

(c) Ein Benutzer führt den Befehl `powerup` in CSI-Linux aus und stellt fest, dass der Prozess unvollständig bleibt, weil eine Benutzereingabe angefordert wird. Was ist die beste Vorgehensweise?

☐ `apt update` anstelle von `powerup` verwenden

☐ `powerup` erneut ausführen und auf Eingabeaufforderungen achten

☐ CSI-Linux neu installieren

☐ Das System neu starten und das Update erneut versuchen

(d) Welcher Befehl wird empfohlen, um das Basisbetriebssystem von CSI-Linux zu aktualisieren?

☐ `powerup install`

☐ `apt-get upgrade && apt-get install`

☐ `sudo apt update && sudo apt upgrade`

☐ `sudo dpkg -upgrade`

(e) Welchen Standard verwendet OpenCTI zur Formatierung von Threat-Intelligence-Daten?

☐ YAML

☐ STIX

☐ JSON

☐ XML

(f) Sie möchten Updates in CSI-Linux automatisieren. Welcher Befehl richtet automatische Sicherheitsupdates ein?

☐ `powerup --auto`

☐ `sudo apt install unattended-upgrades`

☐ `sudo dpkg-reconfigure unattended-upgrades`

☐ `sudo apt update`

(g) Wie aktiviert man automatische Updates in CSI-Linux?

☐ `powerup`

☐ `/etc/apt/sources.list` bearbeiten

☐ `sudo apt update`

☐ `sudo dpkg-reconfigure unattended-upgrades`

(h) Auf welcher Linux-Distribution basiert CSI-Linux?

☐ Arch Linux

☐ Ubuntu

☐ Debian

☐ Fedora

Viel Erfolg!