Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Fachhochschule Dortmund
University of Applied Sciences and Arts

Übungsblatt 1 **Informationssicherheit SoSe 2023** Datum: 28.03.2023

Aufgabe 1.1

Machen Sie sich mit folgenden Informationsquellen anhand von Heartbleed vertraut:

- Common Vulnerabilities and Exposures (CVE)
  https://cve.mitre.org/, aufgerufen am 27. März 2023
- National Vulnerability Database (NVD)
  https://nvd.nist.gov/, aufgerufen am 27. März 2023
- Common Weakness Enumeration (CWE)
  https://cwe.mitre.org/, aufgerufen am 27. März 2023

a) Was ist das Hauptziel von CVE? Wie werden Verwundbarkeiten standardmäßig beschrieben? Wer ist Betreiber von CVE und welche Organisationen finanzieren das Projekt?

b) Was umfasst NVD im Vergleich zu CVE und wie werden Verwundbarkeiten standardmäßig beschrieben? Wer ist Betreiber von NVD und welche Organisationen finanzieren das Projekt?

c) Wie werden die Auswirkungen von Heartbleed in der NVD beurteilt? Machen Sie sich mit dem „Common Vulnerability Scoring System Calculator Version 3.1“ (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator, aufgerufen am 27. März 2023) vertraut und rechnen sie den CVSS 3.1 Score von Heartbleed nach.

d) Was ist das Ziel von CWE? Wie werden Verwundbarkeitstypen standardmäßig beschrieben? Wer ist Betreiber von CWE?

e) Was für ein Verwundbarkeitstyp ist Heartbleed laut CWE?

f) Lernen Sie weitere Details zu Heartbleed, bspw. hinsichtlich Gegenmaßnahmen, Exploits, betroffener Software und ähnlichen Verwundbarkeiten.

Aufgabe 1.2

Recherchieren Sie zu CVE-2017-5754 mithilfe von CVE, NVD und CWE zu den nachfolgenden Fragestellungen. Dokumentieren Sie Ihre Rechercheergebnisse.

a) Um welche Verwundbarkeit handelt es sich genau? Um welchen Verwundbarkeitstyp handelt es sich?

b) Was ist die Ursache der Verwundbarkeit und wie kann sie ausgenutzt werden?

c) Welche Produkte sind von der Verwundbarkeit betroffen?

d) Welche Gegenmaßnahmen wurden ergriffen?

e) Berechnen Sie den CVSS Score mit dem „Common Vulnerability Scoring System Calculator Version 3.1“ (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator, aufgerufen am 27. März 2023). Welche qualitativen Unterschiede zum CVSS 3.1 Score von Heartbleed können Sie dabei feststellen?

Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Aufgabe 1.3

Auf den nächsten Übungsblättern sollen Sie Pentesting Übungsaufgaben mit Hilfe des *OWASP WebGoat Projekt* (https://owasp.org/www-project-webgoat/, aufgerufen am 27. März 2023) bearbeiten. Auf weiteren Übungsblättern sollen Sie vereinzelt Übungsaufgaben mit Hilfe verschiedener Hacking Tools bearbeiten, welche unter *Kali Linux* (https://www.kali.org/, aufgerufen am 27. März 2023) zur Verfügung stehen.

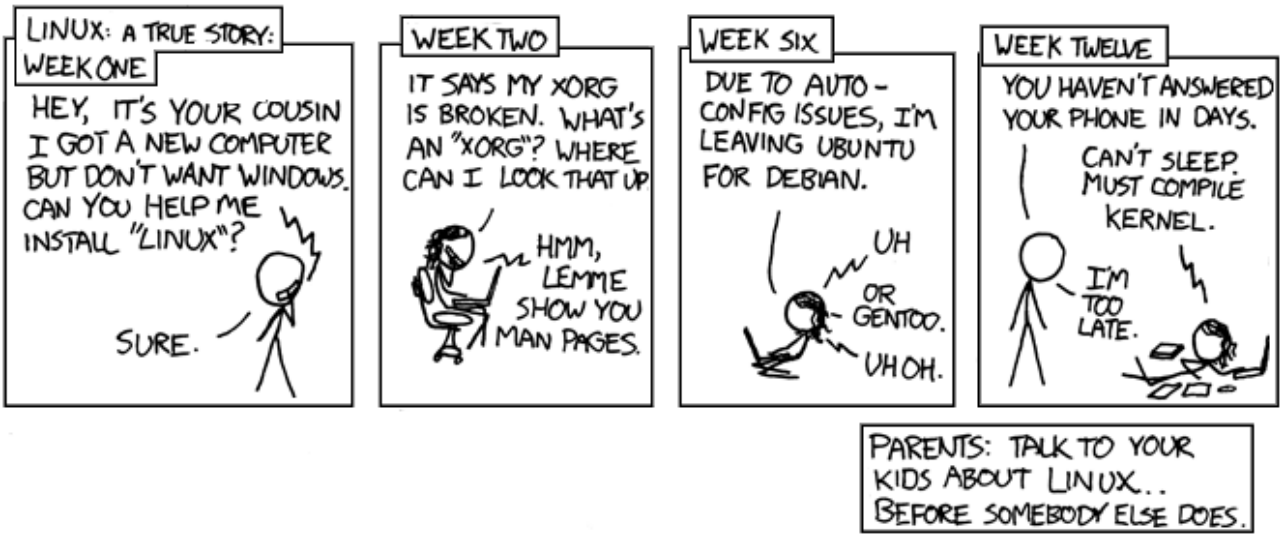

Abbildung 1: „Cautionary“, http://xkcd.com/456/, aufgerufen am 27. März 2023, lizensiert unter CC BY-NC 2.5.0, https://creativecommons.org/licenses/by-nc/2.5/, aufgerufen am 27. März 2023

Damit Sie diese Übungsaufgaben bearbeiten können, ist entsprechend *Kali Linux* auf einer virtuellen Maschine auf Ihrem Computer einzurichten, z. B. wie nachfolgend beschrieben:

a) Nutzen Sie für die Virtualisierung *Oracle VirtualBox* (https://www.virtualbox.org/, aufgerufen am 27. März 2023).

b) Laden Sie sich eine fertig eingerichtete virtuelle Maschine (VM) mit Kali Linux runter (https://www.osboxes.org/kali-linux/, aufgerufen am 27. März 2023).

c) Starten Sie die VM mit VirtualBox[1].

- Sie können sich als Benutzer `osboxes` mit dem Passwort `osboxes.org` anmelden.
- Über die Anwendung `Keyboard` können Sie unter `Layout` die Tastatursprache auf Deutsch einstellen.

[1]Bei Problemen mit VirtualBox konsultieren Sie die Dokumentation (https://www.virtualbox.org/wiki/End-user_documentation, aufgerufen am 27. März 2023). Wenn Sie bisher keine Virtualisierung auf Ihrem PC genutzt haben, dann ist ein häufiges Problem, dass eine VM nicht gestartet werden kann, da die entsprechenden Fähigkeiten (Intel VT-x bzw. AMD-V Technologie) zunächst im BIOS aktiviert werden müssen.

- Aktualisieren Sie Java RE mit folgenden Befehlen:
  `sudo apt-get update && sudo apt-get install default-jre`.

d) Installieren Sie in der VM WebGoat, z. B. basierend auf dem JAR Release (https://github.com/WebGoat/WebGoat/releases, aufgerufen am 27. März 2023).

e) Deaktivieren Sie den Netzwerkadapter der virtuellen Maschine bevor Sie WebGoat starten.

f) Sie können nun die Webanwendung WebGoat z. B. im Firefox ESR Browser in der virtuellen Maschine unter http://localhost:8080/WebGoat aufrufen.

In ILIAS / sciebo befindet sich eine Datei `Kali-Linux-2022.3-WebGoat.ova` im Verzeichnis `Zusatzmaterial`, die eine gemäß obiger Anleitung erstellte VM enthält. Die Datei kann (alternativ zur selbst durchgeführten Einrichtung der Kali Linux VM) in VirtualBox importiert werden.

Lesen Sie sich abschließend *Introduction* → *WebGoat* durch und arbeiten Sie die Lektionen *HTTP Basics, HTTP Proxies, Developer Tools* und *CIA Triad* unter *General* durch.