Wahlpflichtfach
EHK Ethical Hacking

Lehrplan 4.HIF
IV Jahrgang: 7. Semester

Bildungs- und Lehraufgabe:
Die Schülerinnen und Schüler können

- Open Source Intelligence verstehen und anwenden
- Social Engineering erkennen, anwenden und abwehren
- Schwachstellen erkennen und Pentesting Tools anwenden
- Einfache Capture-the-Flag Challenges lösen

Lehrstoff:

- Rechtliche Grundlagen, Hackerethik
- Open Source Intelligence, Social Engineering, Phishing, Awareness
- Passwortsicherheit, Passwort Attacken
- Schwachstellenerkennung, CVE, Enumeration

IV Jahrgang: 8. Semester

Bildungs- und Lehraufgabe:
Die Schülerinnen und Schüler können

- SQL-Injections, Cross-Site-Scripting verstehen und anwenden
- Active Directory Attacken, Privilege Escalation verstehen und ausführen
- Sichere Passwörter erstellen und unsichere cracken
- Verschlüsselung und Hashing verstehen
- Einfache Capture-the-Flag Challenges lösen

Lehrstoff:

- Web Security (SQL Injection, XSS)
- Kryptographie, Verschlüsselung, Hashing
- Betriebssystem-Sicherheit, Windows, Active Directory, Linux

Lehrplan 5. HIF

V Jahrgang: 9. Semester

Bildungs- und Lehraufgabe:
Die Schülerinnen und Schüler können

- Grundlegende Assemblersprache verstehen und programmieren
- Disassembler und Reverse Engineering verstehen und anwenden
- Computerforensik Tools anwenden und digitale Spuren finden
- VPN verstehen und Reverse Shells benutzen
- Capture-the-Flag Challenges lösen

Lehrstoff:

- Netzwerk-Sicherheit: WLAN-Rogue-Access-Points, DHCP-Rogue Server, Reverse Shell, VPN
- Reverse Engineering, Assembly , Digital Forensics

V Jahrgang: 10. Semester

Bildungs- und Lehraufgabe:
Die Schülerinnen und Schüler können

- USB-Attacken vorbereiten und durchführen
- Einen Command-and-Control Server einrichten und betreiben
- WLAN-Rogue-APs und Rogue DHCP-Server einrichten und betreiben
- Capture-the-Flag Challenges lösen

Lehrstoff:

- USB-Attacken mittels geeigneter Pentesting-Geräte (z. B. RubberDucky) und Scripting (z. B. DuckyScript, Powershell, etc.)
- C2 Server, Rogue WLAN-AP, Rogue DHCP-Server

Unterrichtsdurchführung/Beurteilungskriterien

Abhängig von Teilnehmerzahl und Jahrgang werden die Themengebiete im Teamteaching Format oder in 2 getrennten Gruppen (mit Rotation) durchgeführt.
Die Unterrichtsblöcke beginnen üblicherweise mit einen möglichst kurzen (bis max.1h) theoretischen Teil, in dem die praktischen Übungen/Challenges erklärt werden. Der Großteil des Unterrichts steht dann für die praktische Durchführung der Übungen/Challenges zur Verfügung.

Die Bewertung erfolgt schwerpunktmäßig aufgrund der gelösten und (auf den jeweiligen Plattformen oder in Moodle) abgegebenen Übungen/Challenges. Dabei gehen auch selbst gewählte Aufgaben/Challenges in die Bewertung ein. Fragen zu den durchgeführten Übungen/Challenges (üblicherweise im Rahmen von Moodle-Fragen) gehen zu einem kleineren Teil in die Bewertung ein.

Überblick: Lehrerteam und Schwerpunkte

Andreas Stach (stach@spengergasse.at, B2.12a): Cybersecurity, Pentesting

- Pentesting Tools: Schwachstellen, CVE, nmap, KaliLinux, Metasploit, hydra, CyberChef, Reverse-hashing, hashcat, John the Ripper, Password-Attacken, Brute-Force, hydra,, …
- Netzwerk-Sicherheit: WLAN-Rogue-Access-Points, DHCP-Rogue Server, Reverse Shell, VPN, …
- Betriebsystem-Sicherheit: Linux-Security; linpeas, Privilege-Escalation; Windows-Security, Eternal blue; Active Directory, kerberos, mimikatz,…
- Live-Capture-the-Flag Challenges/Events: SpengerH4ckers;Network Security, Web-Security, Cryptography, Software Security, TryHackme, Austria Cyber Security Challenge, …

Angela Stach (stachan@spengergasse.at, B2.12a): OSINT, Social Engineering, Web Security, Computerforensik

- Reconnaissance: OSINT (Open Source Intelligence, IMINT, SOCMINT), Social Engineering, Phishing, Shodan, Google Dorks
- Web Security: BurpSuite, SQL Injection, Cross-Site-Scripting
- Reverse Engineering, Assembly, Ida Pro, ghidra, cutter, Digital Forensics, Autopsy
- USB-Attacken: DuckyScript mit PowerShell für RubberDucky und OMG Cable, C2-Server (Command & Control)
- Kryptografie: Symmetrische & asymmetrische Kryptographie, Hashing, Passwort Security und Passwort Cracking
- CTF Training: ACSC, TryHackme, OliCyber, FuzzyLand, …

Wann bin ich hier richtig?

- Ich möchte an Capture-the-Flag Challenges teilnehmen und dafür trainieren
- Ich bin neugierig, löse gerne Rätsel und gehe gerne den Dingen auf den Grund
- Ich sehe Schwachstellen und möchte diese ausnutzen/ausbessern

Highlights

- Gastvorträge und Workshops aus der Wirtschaft, sowie Exkursionen
  - Security Day St.Pölten, Alite, Deloitte, Cloudflight, NTS, etc.
- Durchführung und Teilnahme an Hacking Challenges und Capture the Flag Events
  - SpengerHacker (gemeinsam mit SpengerH4CKsen) nehmen z.B. an ACSC (Austrian Cyber Security Challenge) und anderen CTFs teil
- Optionale Cybersecurity-Zertifizierungen (Cybersecurity Essentials, CyberOps, etc.)
- Praktische Social Engineering Attacken mit vorhandenen Pentetration Testing Tools
  - Phishingkampagnen
  - WLAN Attacken (Evil Twin mit WIFI-Pineapple)
  - USB-Attacken (RubberDucky, LAN-Turtle, OMG-Cable …)
  - Netzwerkattacken (KaliLinux-Tools)
  - Command-and-Control-Server-Betrieb

Maturatöpfe

Falls ETH als mündliches Maturafach gewählt oder zugewiesen wird, werden Fragen aus folgenden Themengebieten gezogen:

1) Reverse Engineering und Computerforensik
2) Web-Security und Betriebssystemsicherheit
3) Penetration Testing und Netzwerksicherheit
4) Kryptographie und Passwort-Security
5) Social Engineering und Open Source Intelligence