Vorlesung IT-Security I
Prof. Dr. Vincent Heuveline
IWR, Universität Heidelberg

Übungsblatt 1
Abgabe 3. Dezember 2025 14:00 Uhr

Tutor
Stefan Machmeier
stefan.machmeier@uni-heidelberg.de
Moritz Gutfleisch
moritz.gutfleisch@stud.uni-heidelberg.de

Übungsblatt 1

Allgemeine Hinweise:

- Alle Übungsblätter werden in Moodle bereitgestellt.
- Die Übungen haben einen Capture-The-Flag Charakter. Das Ziel einer Aufgabe ist dabei, eine Flag an einem System zu finden/stehlen und dieses in Moodle abzugeben.
- Für die Abgabe der Flag finden Sie auf Moodle ein entsprechendes Feedbackmodul.
- Bitte verwenden Sie während der Übungen ausschließlich die Mailadresse, die im Moodle System hinterlegt ist. Falsche Mailadressen führen dazu, dass Ihre Abgabe ggfs. als falsch bewertet wird. Am besten kopieren Sie sich die Mailadresse aus dem Moodle System, um Fehler beim Abschreiben zu vermeiden.
- Die Flags werden auf virtuellen Maschinen bereitgestellt. Die Subnetze und IP-Adressen sind userspezifisch.
- Manche Flags sind für jeden Teilnehmer individuell, d.h. die Flag hängt von Ihrer Mailadresse ab.
- Alle Flags sind wie folgt aufgebaut: `ITSEC{.....}`
- Jede in Moodle abgegebene Flag ergibt eine bestimmte Punktzahl, die dadurch erreicht wird, dass Sie die Flag in Moodle in das dafür vorgesehene Modul einpflegen.
- Warnung: Führen Sie die Experimente ausschließlich auf/bei/für/mit den von uns freigegebenen Maschinen/IPs/DNS-Adresse aus. Ein Angriff auf eine hier nicht schriftlich definierte IP-/DNS-Adresse ist ein unbefugter Zugriff und damit eine Straftat.

Allgemeines zu dieser Übung:
Das Netzwerk erreichen Sie über die bereitgestellte OpenVPN Verbindung.

Um sich mit dem Netzwerk verbinden zu können, müssen Sie sich im Netzwerk der Universität befinden. Dafür eignet sich ein VPN. Befolgen Sie zur Einrichtung die Anleitung des Universitätsrechenzentrum der Universität Heidelberg.

1 DIY-Kryptografie (8 Flags)

Aufgabenstellung: Das Institut für Paranoide Kryptografie hat beschlossen, sämtliche kryptografischen Funktionen selbst zu entwickeln - denn was kann schon schiefgehen, wenn man jahrzehntelang erprobte Standards durch eigene Implementierungen ersetzt.

Hilfestellung: Schauen Sie sich die Netzwerkkommunikation von Webservern an. Interessante Informationen können im Source Code (bereitgestellt als ZIP Datei) enthalten sein.

Jeder Übung werden zufällig generierte IP-Adressen aus dem zugehörigen Subnetz zugewiesen. Das bedeutet, dass jede virtuelle Maschine je nach Student eine individuelle IP-Adresse erhält, wodurch eine personalisierte Lernumgebung entsteht.:

Tools: Für die Bearbeitung dieser Aufgabe benötigen sie:

- `dirb`
- `ssh`
- `wireshark`
- `nmap`

Für einige Schritte stehen Ihnen bereits vorbereitete Hilfsskripte zur Verfügung, die Sie in Ihrer Analyse unterstützen:

- `bad_signatures.server.py` – Service zum Signieren einer gewählten Nachricht.
- `payroll.index.php` – Webserver-Datei.
- `readmail.views.py` – Websever-Datei.
- `dont_care_beros.server.py` – Kerberos Server.
- `rsa-server.py` – Service zum Verschlüsseln einer gewählten Nachricht (Für Kerberos) .
- `dh_utils.py` – Diffie-Hellmann-Hilfsfunktionen.
- `skeleton.bad_signatures.py` – bad_signatures.server.py Skeleton-Datei.
- `skeleton.diffie_hellman_small_prime.py` – Diffie-Hellmann Skeleton-Datei.
- `skeleton.diffie_hellman_mitm.py` – Diffie-Hellmann Skeleton-Datei.
- `skeleton.dont_care_bereos.py` – Kerberos Skeleton-Datei.
- `skeleton.readmail.py` – Webserver Skeleton-Datei.
- `skeleton.rsa_weak_modules.py` – Skeleton-Datei für RSA-Verschlüsselung.
- `pw-list.txt` – Generische Passwort-Wortliste.

Status: Diese Übungsaufgabe wurde mit Kali Linux Version 2025.1 getestet. Falls Sie ein anderes Betriebssystem oder eine andere Linux-Distribution verwenden, können wir Ihnen keinen Support anbieten.