Kiel University
Christian-Albrechts-Universität zu Kiel

Research Group
Distributed Systems

Praktikum IT-Sicherheit

Corona / Online Edition
Einführung & Übersicht

Olaf Landsiedel

Ziel des Praktikums

- Praktische Erfahrungen im Bereich IT-Sicherheit sammeln
- (Und auch Linux)

Image Credit: Richard Patterson (CC BY 2.0)

About Me: Olaf Landsiedel

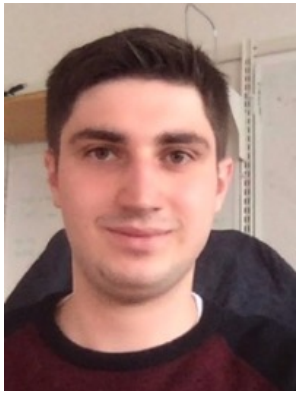
- Leitung der AG Verteilte Systeme / Distributed Systems
  - Seit Oktober 2018
  - Veranstaltungen
    - Betriebs- und Kommunikationssysteme (BSKS)
    - Praktikum IT-Sicherheit
    - Weitere Module als Wahlpflicht:
      - Distributed Systems
      - Wireless Networks and Internet of Things
      - (Pro)Seminare, Bachelor/Master Projekte, …
- “Du / Olaf“ ist völlig ok, aber kein muss

www.ds.informatik.uni-kiel.de

Team IT-Sicherheit

Olaf Landsiedel

Oliver Harms



Valentin Poirot

NN

Was und Wie?

- Praktikum: praktische Versuche
  - Vorversuch
  - 5 Versuche
    - Expertenversuch (Einer der 5 Versuche, s.u.)
  - Capture the Flag Wettbewerb
    - Ihr bekommen Maschinen mit Sicherheitslücken
    - Verteidigen: Lücken finden und beseitigen
    - Angreifen: Lücken finden und ausnutzen

Didaktisches Konzept

- Basierend auf Selbststudium
  - Ihr sollt euch die Informationen selber suchen
  - Bekommt von uns nur Startpunkte
- Ziel: lernen sich eigenständig in neue Gebiete einzuarbeiten
  - Sehr wichtig für die spätere Karriere
    - Wo ihr euch sehr oft eigenständig in neue Themen einarbeiten müssen
- Große Unterschiede zu den Didaktischen Ansätzen der anderen Module
  - Feature, not a bug
  - Auch wenn es euch manchmal anderes vorkommen wird

Weiterer Hinweis

- Ihr werdt sehr viele Programmiersprachen und Tools kennenlernen
  - Ihr sollt nicht Experte in diesen werden
  - Sondern lernen wie man sich zügig und effizient in diese “tief-genug” einarbeitet

- Ziel hier
  - Überall mal hineinschnuppern
  - Sagen zu können: damit habe ich mal was gemacht
  - Ängste vor neuen Sprachen zu nehmen

5 Versuche

Themen (ca.)

- Pufferüberläufe
- SQL injections
- Hintertüren und Rootkits
- Netzwerksicherheit
- Angriffe auf Web-Anwendungen
- System-Sicherheit

- 5 Versuche
  - 4 Versuche
  - 1 Versuch als Expertenversuch,
- Interessante und praktische Mischung
- Beispiele: siehe OLAT aus den letzten Jahren

Versuche

- Bearbeitung
  - In Zweiergruppen
  - In einer Virtuellen Maschine (oder/und Raspberry Pi & Tablet)
  - (oder z.T. eigenem Laptop / VM)
  - **Selbststudium:** Inhalte selbstständig erarbeiten
    - von uns bekommen ihr die Startpunkte,
    - Durch Internetrecherche, Dokumentationen, etc.
    - **Oft eine neue, andere Art des Lernens**
  - Online Testat-Abgabe „wenn fertig“
- Expertengruppen (s.u.)
  - stehen als Ansprechpartner zur Verfügung

Expertenversuch

- Pro Gruppe: Ein Expertenversuch
  - Ausarbeitung einer Dokumentation
  - Gruppe steht während der Durchführung für andere als Experten zur Verfügung

- Auswahl im OLAT
  - Unter „Expertenversuch“

Vorversuch

- Aufgabe
  - Bearbeitung des Vorversuchs
  - Inhalt: Grundlagen Linux, C

Hacking Days: Capture the Flag Contest

- Ihr bekommt von uns: Virtuelle Maschine mit unsicheren Diensten
  - Sicherheitslücken ähnlich denen aus den Versuchen
- Eure Aufgaben
  1. Identifizieren der Sicherheitslücken
  2. Fixen der Sicherheitslücken (ohne die Verfügbarkeit der Dienste einzuschränken)
  3. Ausnutzen der Lücken auf den Maschinen der übrigen Teams (und unserer Server)
- Ziel
  - „Prüfung“
  - Wettbewerb mit Leaderboard etc

Bestehen

- Bestehen
  - Aller Versuche und des Vorversuches
- Mindestpunktzahl im CTF
  - Identifizieren, reparieren und ausnutzen einer bestimmten Anzahl von Sicherheitslücken

Testate

- Online Testat
  - Für Vorversuch, Expertenversuch, Versuche
    - Bei Expertenversuch: zusätzliche Dokumentation
  - Zufällige Quizfragen
  - Plus Abgabe von Texten, Screenshots, Code, …
  - **Achtung: Zeitlimit**
    - Das Quiz erst beginnen, wenn man sich in dem Thema sicher fühlt

- Persönliches Testat
  - Falls nicht bestanden
  - Nachfragen erforderlich

Praktikum Ziele

- Thema: IT-Sicherheit
- Aber auch: Selbständiges Einarbeiten in neue Themen
- Erfahrungen mit neuen Konzepten und Programmiersprachen
  - C, Java, SQL, python, javascript, assembly, …
  - Scripting (Bash, Python, …)
  - Einige davon habt ihr noch nie genutzt
    - (This is a feature, not a bug)
- Manchmal ungewohnt, aber sehr wichtig für die spätere Karriere

Collerteral Damage

- Praktikum IT-Sicherheit…
  - Da geht schon mal was kaputt
- Bitte sudo etc. nur in der Virtuellen Maschine!
- Vor ein paar Jahren
  - Kritische Lücke in OLAT

Virtuelle Maschinen

- Nicht für den Vorversuch & Expertenversuch!

- Für Versuche und CTF
  - Achtung: Neue VM für CTF, alte VM wird gelöscht
  - Auf den VMs keine Daten speichern, keine Backups etc.

- Einloggen via ssh oder x2go,
  - aus den Poolräumen: HRS3 - R.501-503
  - oder eigenen Laptop
  - Details: siehe OLAT

Zusammenfassung

1. Vorversuch
2. Expertenversuch
   - Einen der 5 Versuche auswählen (Auswahl im OLAT)
3. 5 – 1 = 4 Praktische Versuche
   - Nächster Versuch nach dem Expertenversuch: (Expertenversuch + 1) mod 5
4. Hacking Contest

Zeitplan

Details und diese Folien: im OLAT

Datum	Item
ab 15.05.2021	Vorversuch bearbeiten
bis 04.07.2021	Vortestat ablegen (Online), Expertenversuch auswählen
ab 26.07.2021	Expertenversuch bearbeiten
bis 05.09.2021	Expertenversuch durchführen, Online-Testat ablegen, Abgabe Dokumentation zum Expertenversuch
20.–24.09. & 27.9–01.10.2021	Virtueller Block incl. CTF (2 Wochen, Vollzeit)
01.10.2021	Abschlussveranstaltung & Puffertag

Corona Hinweise

- Online Edition: Block 2 Wochen
- Block normalerweise vor Ort
  - VM und login via eignem Laptop oder Pool
- Jetzt online
  - VM und login nur via eigenem Computer

- Mündliche Testate
  - Normalerweise vor Ort
  - Jetzt via Zoom etc.
    - Ihr benötigt Computer, Headset, Mikro, Webcam, Internet

Materialen: im OLAT

- OLAT: Vorversuch, Versuche, Expertenversuch, …
  - Anleitungen
  - Hinweise
  - Testate
  - ~~Forum zur Partnersuche~~ -> Mattermost
  - …

Was ist wo?

- Anmeldung: StudiDB (TODO: anmelden)
- Unterlagen: OLAT (TODO: anmelden)
- Modulbeschreibung: Modul DB
- (Termine & Räume: Univis)

Feedback

- Sehr willkommen
  - Bitte helft uns den Kurs zu verbessern
- Sprecht mit uns
- Feedback Felder in den Online Testaten

Fragen?

In part, inspired from / based on slides from Henning Schnorr and many others