Systemsicherheits-Labor — Einführung

Sebastian Rehms, Stefan Köpsell
sebastian.rehms@tu-dresden.de
stefan.koepsell@tu-dresden.de
APB 3062

⌘ Ziel:

- Vermittlung von theoretischen und praktischen Kenntnissen auf dem Gebiet des *Penetrationstest*

- **Penetrationstest**: Prüfung der Sicherheit möglichst aller Systembestandteile mit Mitteln und Methoden, die ein Angreifer anwenden würde, um unautorisiert in das System einzudringen (Penetration) [Wikipedia: Penetrationstest_(Informatik)]

Vorgehen:

- Vorlesungen zur Vermittlung der theoretischen Grundlagen
- Übungen zur praktischen Anwendung des Erlernten
- in der Regel *wöchentlich* wechselnd
- Unterstützung durch externe Experten
  - BDO Cyber Security GmbH
  - mgm security partners

Organisatorisches

- Web-Seite
  - https://dud.inf.tu-dresden.de/seclab
- Mailing-Liste
  - OPAL als Kommunikationsplattform
    - E-Mail
    - Wiki
    - Blog bzgl. der Veranstaltungen
  - Einschreiben um
    - aktuelle Informationen zur LV zu erhalten
    - mit den Kommilitonen zu diskutieren
    - Fragen zu stellen
- Fragen zu Übungen/Infrastruktur über Matrix: **@sere733a:tu-dresden.de**

Prüfung

- mündliche Prüfung
  - Voraussetzung:
    - erfolgreiches Absolvieren der Übungen

Prüfung

- mündliche Prüfung
  - ~~Voraussetzung:~~
    - ~~erfolgreiches Absolvieren der Übungen~~

Prüfung

- mündliche Prüfung
  - ~~Voraussetzung:~~
    - ~~erfolgreiches Absolvieren der Übungen~~
  - Bonus für Absolvieren der Übungen
    - Jede Aufgabe bringt 5–50 Punkte
      - ➔alle Aufgaben bringen 975 Punkte
  - Notenverbesserung:
    - 0,3: 480 Punkte (ca. 50%)
    - 0,7: 700 Punkte (ca. 75%)
  - Bonus vor mündlicher Prüfung anmelden!
    - 2 Aufgaben werden Teil der Prüfung
  - Die Lösungen werden ab dem **25.07.2025** nicht mehr angerechnet.

Prüfung

- mündliche Prüfung
  - Bonus für Absolvieren der Übungen
  - Umfang:
    - gemäß Modulbeschreibung
    - üblicherweise: ca. 25 Minuten
  - Inhalt:
    - Abprüfen der erlangten Kenntnisse im Gespräch
    - ***keine*** Durchführung eines praktischen Penetrationstests
  - Anmeldung:
    - im Sekretariat (APB 3070)
    - Prüfungszeit individuell vereinbar

Übungen:

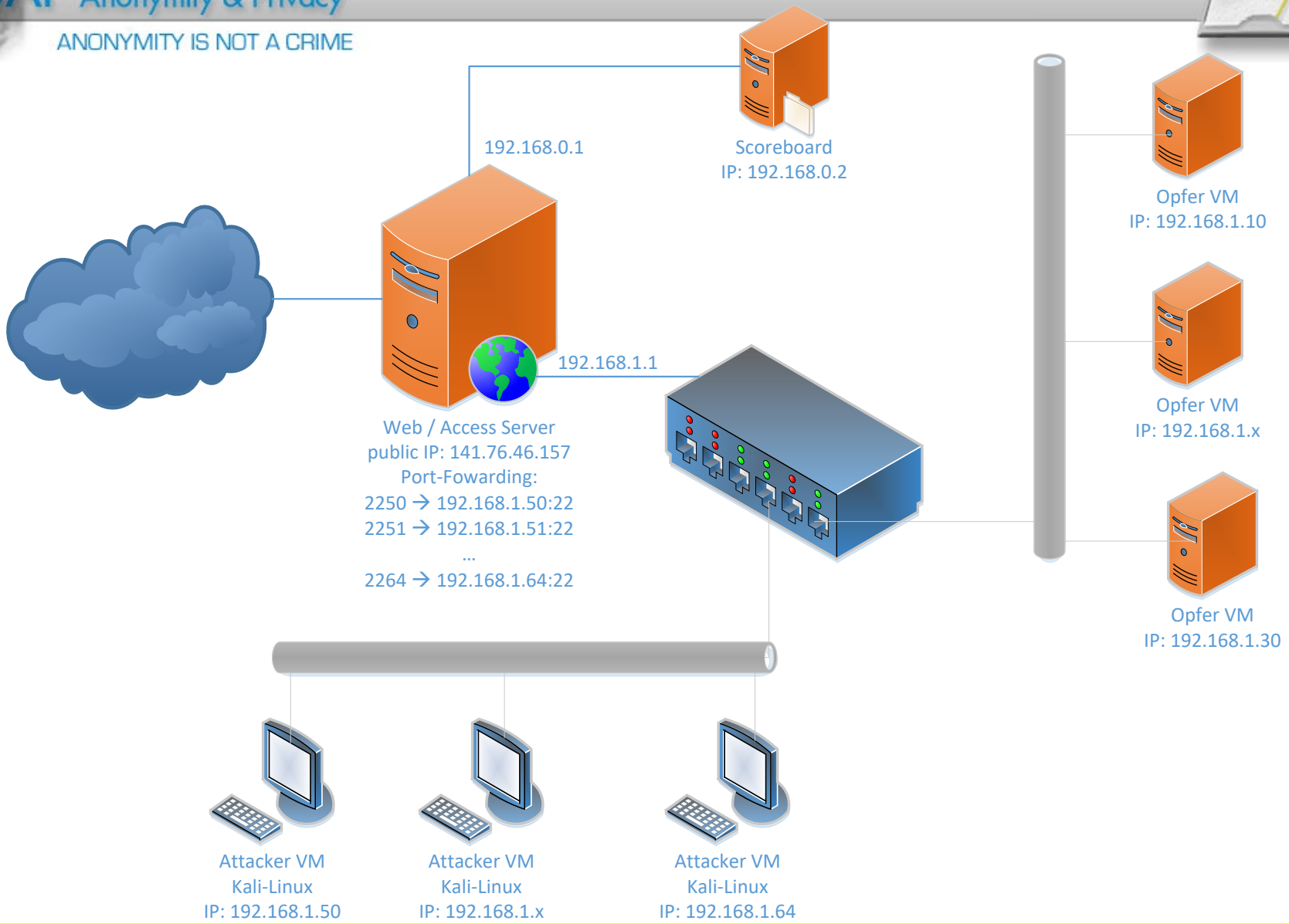
- individuelles Lösen praktischer Aufgaben
  - empfohlen: betreut während der Lehrveranstaltungszeit
  - alternativ: zwischen den Vorlesungen mittels Remote-Zugriff

- angelehnt an „Capture the Flag"-Wettbewerbe
  - vorgegebene Opfer-Rechner müssen erfolgreich angegriffen werden
    ➔ Erlangen eines Lösungswortes
  - Lösungswort muß im Auswertungsserver (Scoreboard) hinterlegt werden
    - https://pentestlab-scoreboard.inf.tu-dresden.de/

- jeweils zu lösende Aufgabe ist im Scoreboard hinterlegt
  - Freischaltung der jeweiligen Aufgabe erfolgt für die Zeit zwischen den Vorlesungen

- jeder Teilnehmer hat Zugriff auf eine individuelle Angreifer-VM
  - Konsole mittels SSH
  - Graphische Benutzungsschnittstelle mittels VNC

Lab Übersicht



SSH-Zugriff

- SSH-Client unter Windows
  - viele Möglichkeiten
  - beispielsweise: https://www.putty.org/
    - kostenfrei
- Verbindung:
  - Host: pentestlab-login.inf.tu-dresden.de
  - Port: x (konkrete Portnummer gemäß persönlichen Login-Informationen)
  - Username: root
  - Password: *** (gemäß persönlichen Login-Informationen)

- Port-Forwarding (für Remote Desktop / VNC)
  - Menü „Connection | SSH | Tunnel“ (Options controlling SSH port forwarding)
  - Source Port: 5900 (frei wählbar)
  - Destination: 127.0.0.1:5900
  - IPv4

SSH-Zugriff

- SSH-Client unter Windows
  - viele Möglichkeiten
  - beispielsweise: https://www.bitvise.com/
    - kostenfrei
- Verbindung:
  - Host: pentestlab-login.inf.tu-dresden.de
  - Port: x (konkrete Portnummer gemäß persönlichen Login-Informationen)
  - Username: root
  - Password: *** (gemäß persönlichen Login-Informationen)

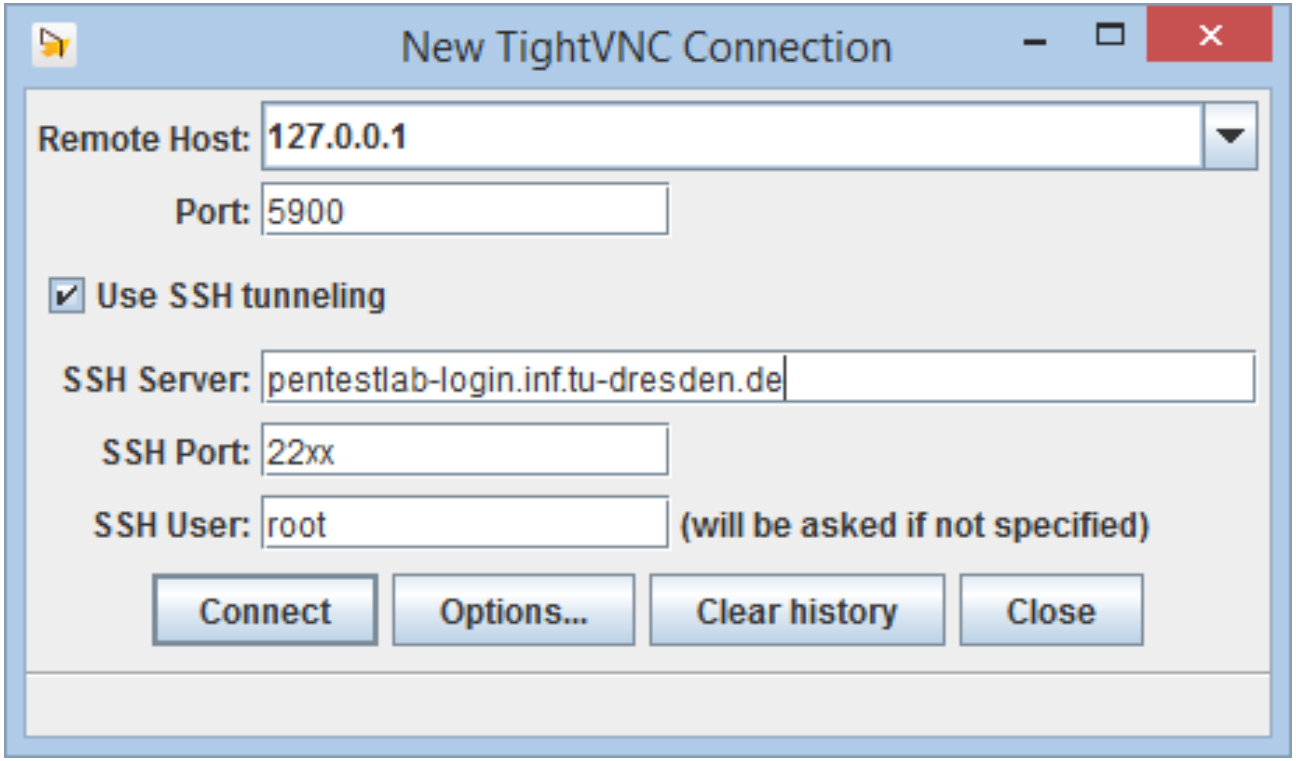
- Port-Forwarding (für Remote Desktop / VNC)
  - „C2S" (Client-to-Server) bei Bitvise SSH-Client
  - Listen Interface: 127.0.0.1 (localhost)
  - Listen Port: 5900 (frei wählbar)
  - Destination Host: localhost
  - Destination Port: 5900

Remote-Desktop

- VNC-basiert
  - Achtung: unsicher (unverschlüsselt)
  - daher: nur über SSH-Tunnel
- Start:
  - von Kommandozeile: **`vncserver`**
  - lauscht standardmäßig an Port: 5900
  - beenden: **`vncserver -kill :1`**
- Remote-Zugriff:
  - mittels VNC-Client
    - viele Möglichkeiten
    - für Windows beispielsweise: UltraVNC (https://www.uvnc.com/downloads/ultravnc.html)
  - Verbindung: 127.0.0.1:5900
    - SSH-Tunnel vorher etablieren
  - Password: pentestlab

Remote Zugriff mit TightVNC

- TightVNC
  - Java Client (Viewer)
  - enthält Unterstützung für SSH-Tunnel
  - https://www.tightvnc.com/download.php



Geplanter zeitlicher Ablauf

Datum	Thema
07.04.2025	Einführung in die LV / Bruteforce-Angriffe: Laufzeiten, Rainbow Tables, Fuzzing, Tools…
14.04.2025	Einführung Werkzeuge
21.04.2025	Ostermontag
28.04.2025	Bruteforce: Teil 2; Angriffe durch fehlerhafte Ein-/Ausgabe-Überprüfung
05.05.2025	Rechtliches & Organisatorisches zum Pen-Testing
12.05.2025	Angriffe durch fehlerhafte Ein-/Ausgabe-Überprüfung (Teil 2) / Übung
19.05.2025	Angriffe auf Web-Anwendungen
26.05.2025	Übung
02.06.2025	Angriffe auf unsichere Programme, Buffer Overflows
09.06.2025	Pfingsten
16.06.2025	Computer Forensik
23.06.2025	Ausnutzen von bekannten Schwachstellen / CERTs | Network Security
30.06.2025	Übung
07.07.2025	Fuzzing des WLAN-Stacks in Linux
14.07.2025	Übung