

# Willkommen zum Penetration Testing Workshop

---

Korbinian Bauer

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



## Name

Korbinian Bauer

## Studium

Bachelor  
Wirtschaftsinformatik  
Schwerpunkt: IT-Security

## Berufserfahrung

SHK am Lehrstuhl für  
Wirtschaftsinformatik I  
NTT Data  
intouchCONSULT

## Workshop

Im Rahmen meiner  
Bachelorarbeit

## Kurze Vorstellungsrunde

- Name
- Erwartungen

## 1 Planung & Vorbereitung

- Zieldefinition
- Scope & Regeln
- Auftragsklärung

## 2 Informationsbeschaffung

- Passive Informationsgewinnung
- Aktive Informationsgewinnung

## 3 Schwachstellenanalyse

- Identifikation potenzieller Schwachstellen
- Vergleich mit bekannten Exploits

## 4 Ausnutzung

- Versuch gezielter Angriffe auf erkannte Schwachstellen
- Ziel: Zugriff auf Systeme oder Daten

## 5 Post-Exploitation

- Privilegienerweiterung, Persistenz
- Überblick über interne Systeme gewinnen

## 6 Reporting

- Dokumentation der Befunde
- Empfehlungen zur Behebung & Absicherung

## **§ 202 Verletzung des Briefgeheimnisses**

Das heimliche Öffnen, Lesen oder Sich-Verschaffen des Inhalts von verschlossenen Briefen oder anderen privaten Sendungen ist strafbar.

## **§ 202a Ausspähen von Daten**

Das unbefugte Beschaffen von nicht für den Täter bestimmten, besonders gesicherten Daten durch Überwindung von Zugangsschutz ist strafbar.

## **§ 202b Abfangen von Daten**

Das heimliche Abfangen von Daten, die nicht für den Täter bestimmt sind, z. B. durch Mitlesen von Kommunikation, ist strafbar.

## **§ 202c Vorbereiten des Ausspähens und Abfangens von Daten**

Die Herstellung, Verbreitung oder Verschaffung von Hacking-Tools zum Zweck des Ausspähens oder Abfangens von Daten ist bereits strafbar.

## **§ 202d Datenhehlerei**

Wer wissentlich mit illegal ausgespähten oder abgefangenen Daten handelt oder sie verwertet, macht sich strafbar.

## **§ 203 Verletzung von Privatgeheimnissen**

Bestimmte Berufsgeheimnisträger (z. B. Ärzte, Anwälte) machen sich strafbar, wenn sie unbefugt Geheimnisse offenbaren, die ihnen anvertraut wurden.

- 1 Passive Reconnaissance
- 2 Aktive Reconnaissance
- 3 SMB
- 4 Web Application
- 5 Vulnerability Scanning
- 6 Exploitation
- 7 Gruppenarbeit

# Passive Reconnaissance

---

Korbinian Bauer

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



Passive Reconnaissance bedeutet, Informationen über ein Ziel zu sammeln, ohne direkt mit dem Zielsystem zu interagieren



## Google Dorking

Nutzt gezielte Suchanfragen in Google, um öffentlich zugängliche, aber möglicherweise sensible Informationen zu finden.

## Crt.sh

Eine Plattform zur Abfrage von öffentlich registrierten SSL/TLS-Zertifikaten, nützlich zur Aufdeckung von Subdomains.

## theHarvester

Ein OSINT-Tool zur automatisierten Sammlung von E-Mails, Domains, Benutzernamen und IPs aus öffentlich zugänglichen Quellen.

## Shodan.io

Eine Suchmaschine für mit dem Internet verbundene Geräte, die nach offenen Ports, Services und IoT-Geräten scannt.

# Active Reconnaissance

---

Korbinian Bauer

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



Aktives Ermitteln von Informationen über Zielsysteme durch direkte Interaktion (z. B. Portscans, Ping, etc).

**Ziel:**  
Netzwerkstruktur verstehen  
Schwachstellen, offene Ports und Dienste zu identifizieren

- Nmap**
- Standardwerkzeug für Netzwerk, Portscans
  - Sendet gezielt Pakete und wertet Antworten aus

Ebene	Ziel	Befehl	Kommentar
Layer 2	Wer ist im lokalen Netz erreichbar?	<code>nmap -PR -sn &lt;ip&gt;</code>	ARP-Scan, nur lokal sinnvoll
Layer 3	Welche Hosts antworten auf Pings?	<code>nmap -sn &lt;ip&gt;</code>	ICMP oder ARP
Layer 4	Welche Ports sind offen?	<code>nmap -sS/-sT/-sU &lt;IP&gt;</code>	TCP SYN (stealth), Connect, UDP
Layer 7	Was läuft auf offenen Ports? OS?	<code>nmap -sV -O &lt;IP&gt;</code>	Dienst- & Betriebssystemerkennung

## Host Discovery

→ Wer ist erreichbar?

→ `nmap -sn 192.168.1.0/24`

## Port Scan

→ Welche Ports sind offen?

→ `nmap -sS 192.168.1.10`

## Service Detection

→ Was läuft auf den Ports?

→ `nmap -sV -O 192.168.1.10`

Bei größeren Netzwerken lohnt es sich nmap über Metasploit laufen zu lassen

Workflow	
msfconsole	Metasploit öffnen
workspace -a <name>	Neuen Workspace anlegen
workspace <name>	In Workspace wechseln
db_nmap	Nmap Befehl
hosts	Übersicht über alle Hosts
services	Übersicht offene Ports & Dienste

1. Erstelle einen neuen Workspace in Metasploit
2. Wechsel in den neuen Workspace
3. Führe einen ARP/ICMP-Scan auf dem Subnetz durch
4. Führe einen Port-Scan durch
5. Finde Betriebssystem und Version raus
6. Lass dir die Ergebnisse nochmal anzeigen (hosts, services)

# SMB

---

**Korbinian Bauer**

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg





## SMB (Server Message Block)

- **Netzwerkprotokoll hauptsächlich für Datei- und Druckerfreigabe (Port 445)**
- **Relevant für Pentests wegen:**
- **Fehlkonfigurationen (z. B. anonymer Zugriff auf Freigaben)**
- **Schwachen Passwörtern (für SMB-Login → Brute-Force möglich)**

## Netexec (früher CrackMapExec)

- **Automatisiertes Tool für SMB-Scans (Benutzer, Shares, Passwörter)**
- **Unglaublich praktisch, um einen Überblick über bestimmte verwendete Protokolle zu bekommen**

# Vulnerability Scanning

---

Korbinian Bauer

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



## Was ist OpenVAS?

- Open Source Scanner zur Suche nach **bekannten Schwachstellen**
- Entwickelt von **Greenbone**, basiert ursprünglich auf Nessus
- Scan läuft gegen eine **aktuelle Datenbank von Tests (NVTs)**

## Was wird geprüft?

- Veraltete Softwareversionen (z. B. Apache, SSH, ...)
- Unsichere Konfigurationen (z. B. SSLv2 erlaubt)
- Standardpasswörter
- Fehlende Patches, CVEs etc.

## Ausgabe & Bewertung

- Ergebnisbericht mit Risikoeinstufung(Low–Critical)
- **Priorisierung** → Wichtige Lücken zuerst beheben
- Ideal als Vorbereitung für Exploits

1. Web-GUI öffnen: <https://localhost:9392>  
<https://127.0.0.1:9392>
2. Target anlegen (IP eintragen)
3. Task erstellen (Target auswählen)
4. Scan starten

# Pause?

---

**Korbinian Bauer**

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



# Burp Suite

---

**Korbinian Bauer**

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



**Burp Suite** ist ein führendes Toolkit für Web Pentesting (Community Edition ist kostenlos verfügbar, Pro Version mit Scanner etc. kostenpflichtig).

**Burp Proxy:** Man-in-the-Middle zwischen Browser und Webserver,  
**Repeater** (zum Wiederholen/Modifizieren von einzelnen Requests)

## Was ist Burp?

Ein **interaktives Test-Toolkit für Webanwendungen** – zum Abfangen, Analysieren und Manipulieren von HTTP(S)-Verkehr.

## Wichtige Komponenten:

- **Burp Proxy** – Man-in-the-Middle zwischen Browser & Webserver
- **Repeater** – Einzelne HTTP-Requests anpassen & erneut senden



1. Juice Shop starten: `sudo juice-shop`

2. Burp Suite starten

3. Juice Shop im integrierten Browser öffnen

`http://localhost:42000`

4. Im Shop etwas tun:

Einloggen, suchen, Artikel in den Warenkorb legen

5. Proxy:

Intercept nur bei Bedarf aktivieren

Sonst → Intercept is Off, Verlauf nutzen

6. Request auswählen und modifizieren:

An den Repeater senden und erneut abschicken

# Nikto

---

**Korbinian Bauer**

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



Nikto ist ein Open-Source-Scanner, der Webserver auf bekannte Sicherheitslücken, Fehlkonfigurationen und veraltete Software überprüft.

## Scan-Ziele:

- Veraltete Server-Softwareversionen
- Fehlkonfigurationen
- Unsichere Skripte & Standardverzeichnisse (z. B. /admin, /phpinfo.php)
- Bekannt gewordene Schwachstellen (CVE)
- Gefährliche CGI-Dateien

1. Starte einen Webseite-Scan mit Nikto auf ein Ziel deiner Wahl
2. Werte die ersten drei Ergebnisse des Scans aus.

# OpenVAS

---

**Korbinian Bauer**

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



1. Öffne deinen Scan-Report in OpenVAS
2. Wähle 1–2 Schwachstellen aus, z. B. mit High oder Critical Severity
3. Lies die Details zur Schwachstelle:

Beschreibung, CVE-Nummer, Empfehlung zur Behebung

4. Recherchiere zum Exploit:

Was genau wird hier ausgenutzt?

Gibt es öffentlich bekannte Exploits dazu? (z. B. Exploit-DB, Metasploit)

Wie funktioniert der Angriff grundsätzlich?

# Metasploit

---

**Korbinian Bauer**

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



## Metasploit – Exploitation-Framework

Tool zur Ausnutzung bekannter Schwachstellen

Enthält hunderte Exploit-Module + Payloads (z. B. Reverse Shells)

Beliebte Payload: meterpreter (interaktive Shell)



# Exploits sind kein Glücksspiel



## **Disclaimer: Exploits vorher verstehen**

Was wird ausgenutzt? Wie funktioniert der Angriff? Ist das Zielsystem betroffen?

1. Öffne deinen Scan-Report in OpenVAS
2. Wähle 1–2 Schwachstellen aus, z. B. mit High oder Critical Severity
3. Lies die Details zur Schwachstelle:

Beschreibung, CVE-Nummer, Empfehlung zur Behebung

4. Recherchiere zum Exploit:

Was genau wird hier ausgenutzt?

Gibt es öffentlich bekannte Exploits dazu? (z. B. Exploit-DB, Metasploit)

Wie funktioniert der Angriff grundsätzlich?

## Auswahl: Angriffsziele mit Metasploit

vsftpd\_234\_backdoor

distcc\_exec

php\_cgi\_arg\_injection

twiki\_cmd\_inject

# Pause

---

**Korbinian Bauer**

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



# Gruppenarbeit

---

**Korbinian Bauer**

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



Ziel:  
Erstellt einen Rogue Access Point mit Custom Captive Portal

## Vorgehen (Beispiel)

- Informiert euch, was ein Evil Twin / Rogue-AP ist und was der Unterschied ist
- Wie kann man einen Rogue-AP erstellen?
- Erstellt die nötigen Dateien oder benutzt ein Tool
- Erstellt ein eigenes angepasstes Captive Portal
- Startet den Rogue Access Point
  
- Wichtig: Es dürfen keine Daten von „Opfern“ gespeichert werden!
- Keine Deauthentication verwenden

# Workshop - Vorstellung

---

Korbinian Bauer

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg



# What now?

Tipps:

David Bombal - YouTube

TryHackMe/HackTheBox

CTFs – VulnHub

Einfach ausprobieren







# Vielen Dank fürs Mitmachen!

Korbinian Bauer

Lehrstuhl für Wirtschaftsinformatik I

Universität Regensburg

