HS2024
Cyber Defense
Ivan Bütler
079'250'06'28

Herzlich Willkommen zum Modul “Cyber Defense”
am 18.9.2024

Erwartungen

(2

- Reale Incidents (CrowdStrike, O365) → Vorgehen → Beheben — Roman
- Wie merkt man, dass man angegriffen wird — Roger
- Blue Teaming
- Hardening
- Abwehrstrategien
- Praktischer Bezug

} Philipp Hunter

Lukas
Stefan
Yannick

Unfreezing - wir reden über Eure Erwartungen.

Ich freue mich über eine aktive Teilnahme und Diskussion mit Euch

Keine Erwartung

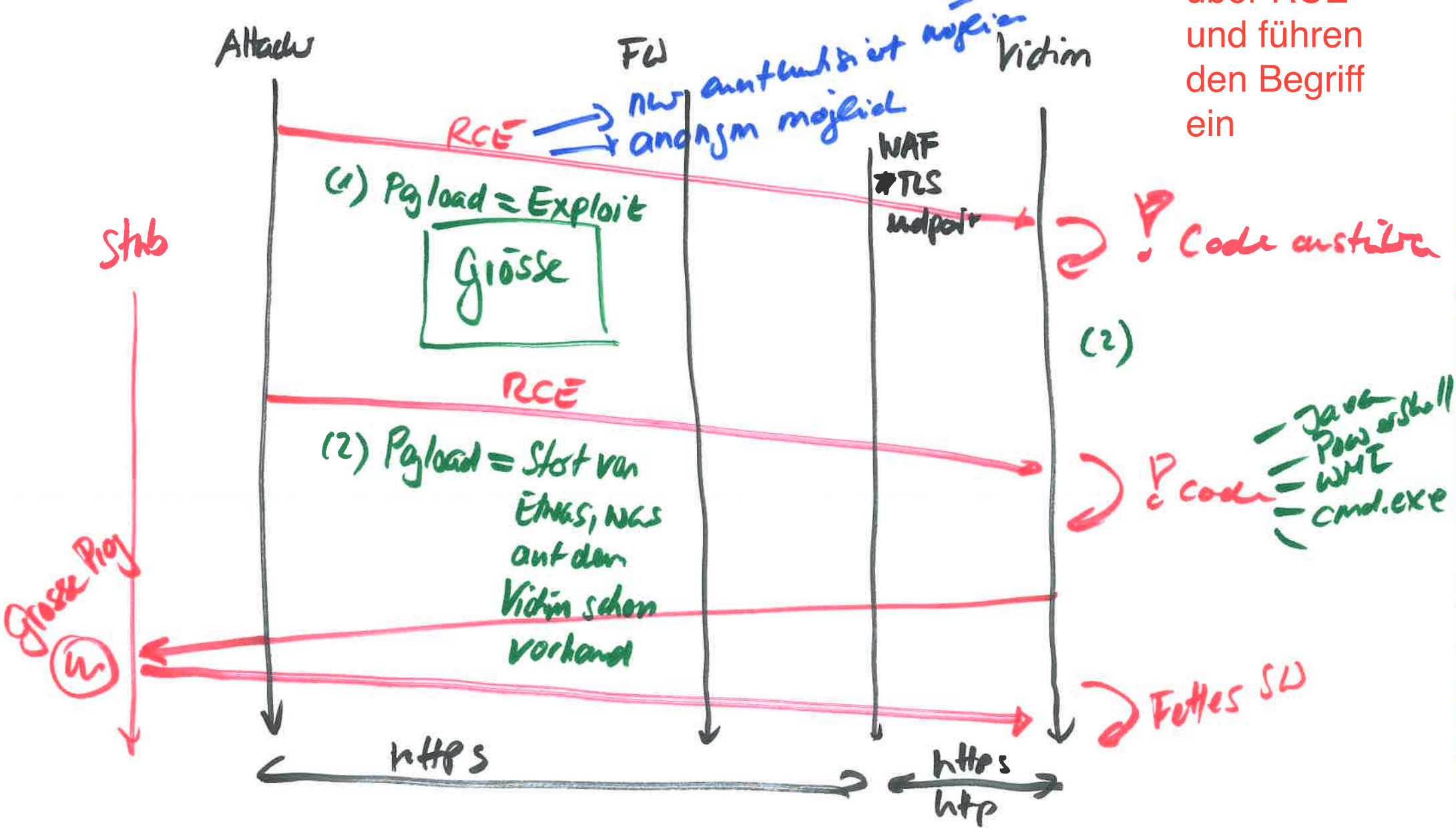
- keine prop/komm Tools → Open Source Tools

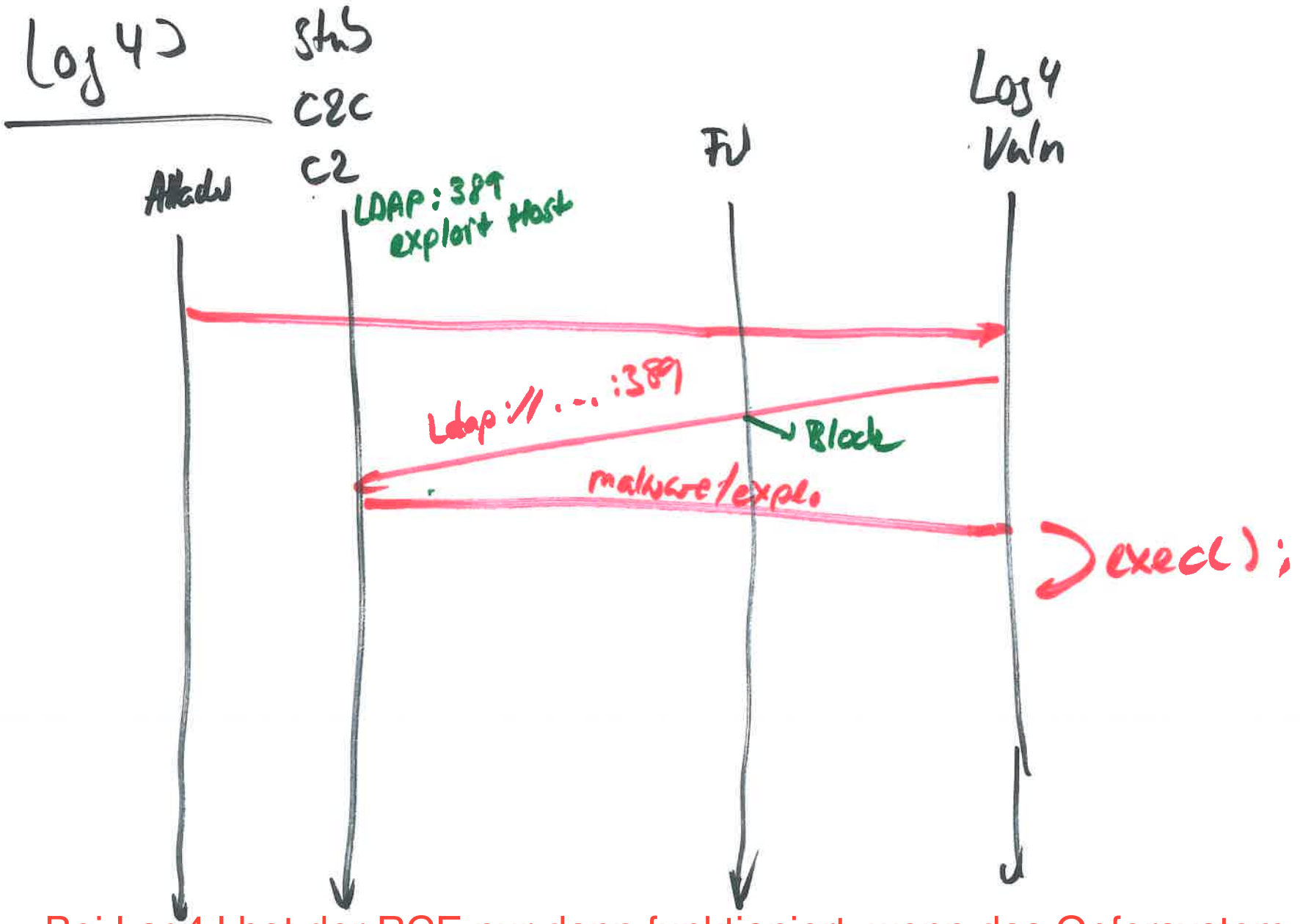
Wunsch möglichst mit Open Source Tools zu arbeiten

RCE

Möglichkeit auf Remote System Code auszuführen!

Wir reden über RCE und führen den Begriff ein





Bei Log4J hat der RCE nur dann funktioniert, wenn das Opfersystem einen LDAP Request ins Internet machen konnte, damit von dort der richtige Exploit nachgeladen werden kann. Daher sind FW Regeln von der DMZ ins Internet so wichtig! Firewall ist wichtig für Cyber Defense

CVE → # bezogen auf Produkt (Schwachstelle)

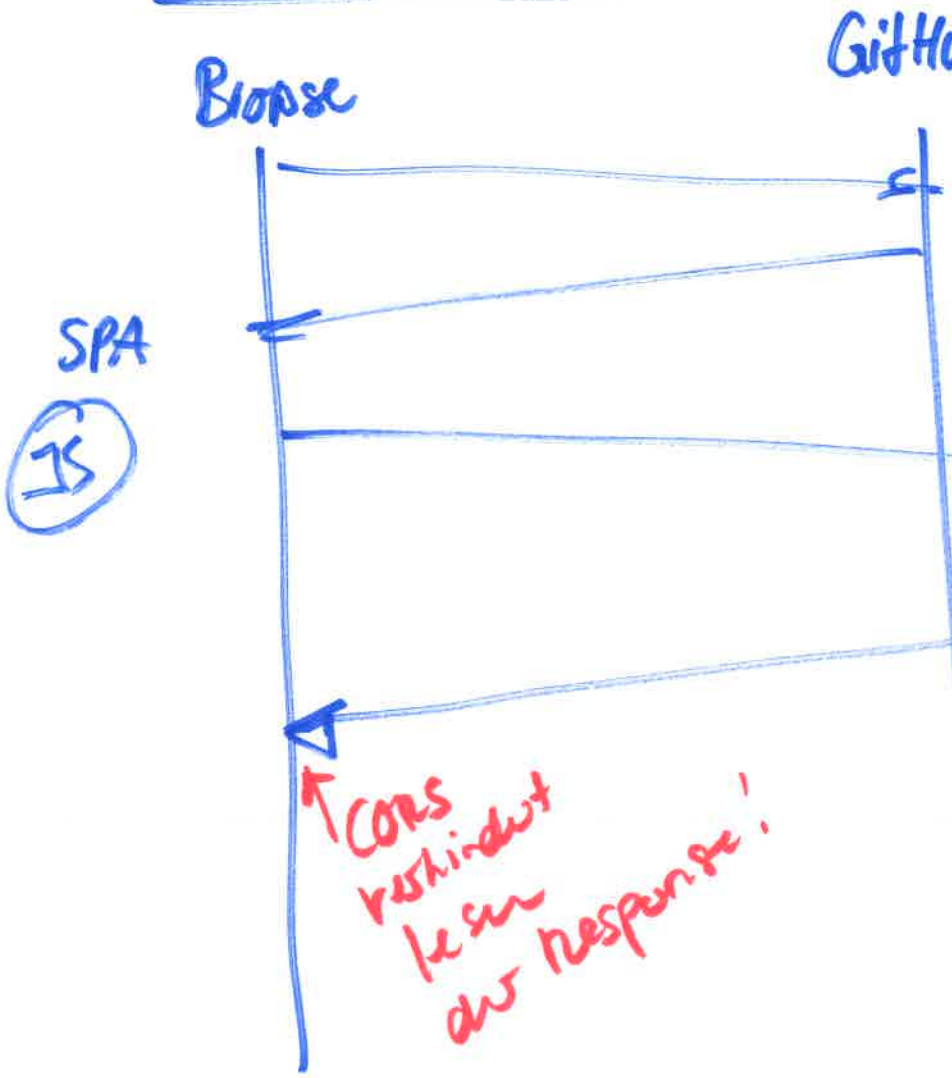
CWE → # bezogen auf ein allg. gültiges Security Problem

Alle von Euch kennen die CVE (Common Vulnerability Exposure). Eine Zahl die eine Schwachstelle auf ein spezifisches Produkt ausweist

Die CWE (Common Weakness Enumeration) war weitestgehend unbekannt in der Klasse. Das ist eine andere Zahl die eine Schwachstelle allgemein und generisch beschreibt

- hard coded credentials
- missing input validation
- weak or no encryption

CORS



CORS (Cross Origin Resource Sharing) verhindert den Request des Browsers nicht, sondern dass der Browser die Daten lesen darf.

Sprich für Angreifer kein Problem wenn es nur darum geht Daten nach Extern (Internet) zu exfiltrieren

CORS zu verstehen ist essentiell

Wir üben anhand von CyberChef und sehen, warum CyberChef nicht ohne Tweaks einen Web Request machen kann

In Dev Tools Console sieht man den Grund