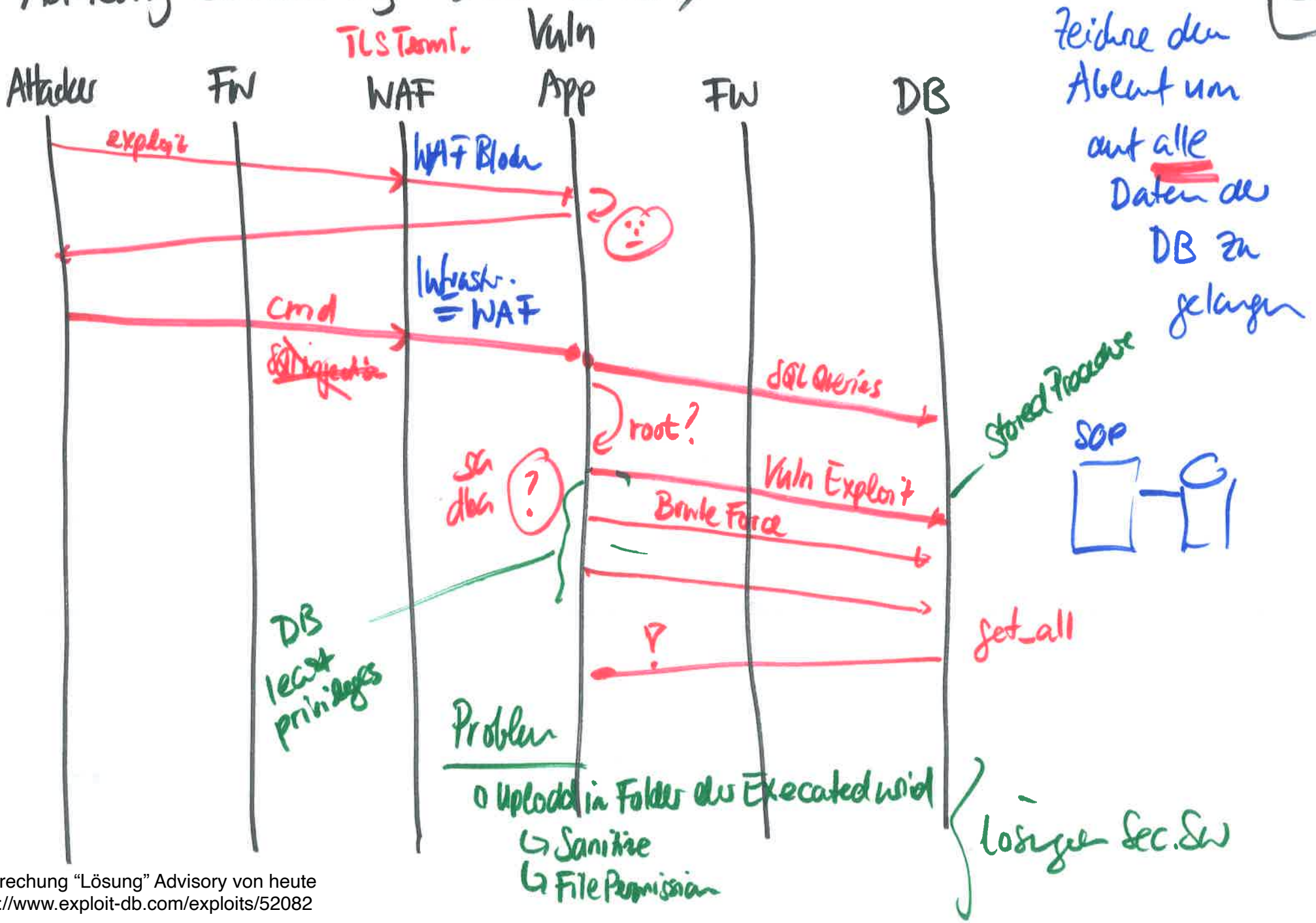
Cyber Defense

4.12.2024

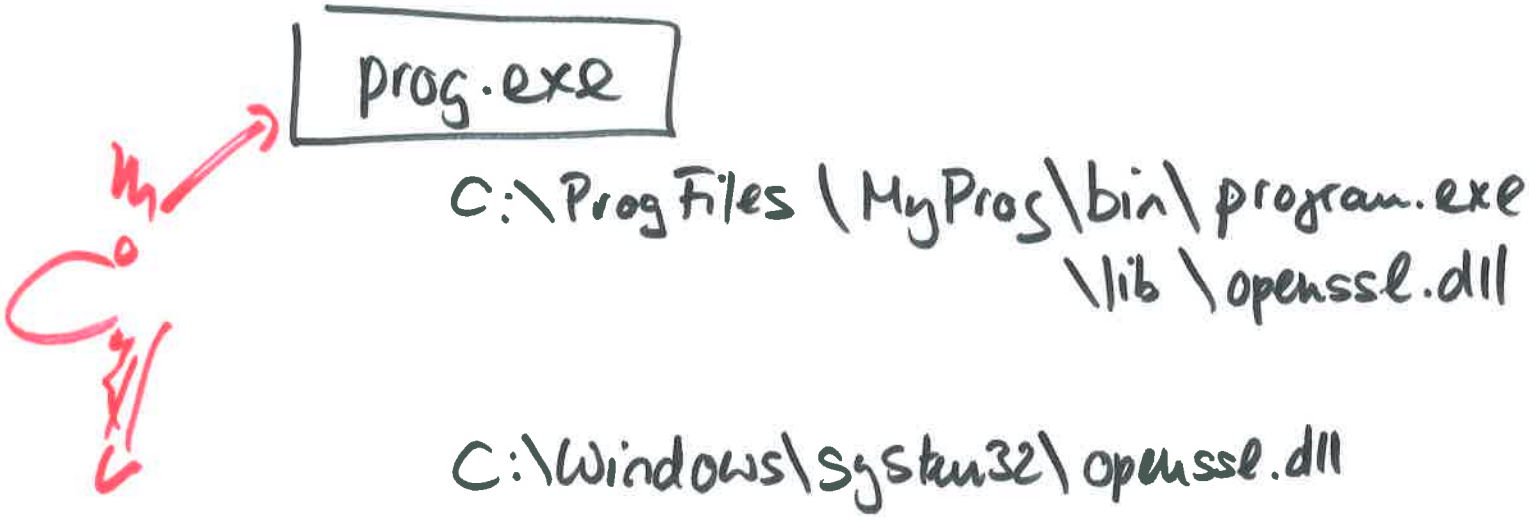
- [ ] Advisory Beispiel
- [ ] DDoS Diskussion
- [ ] Alte Prüfungen
- [ ] Sigma
- [ ] Forensic Readiness
- [ ] EMail
- [ ] Sysmon

Advisory SOPlanning (Diskussion)



Besprechung “Lösung” Advisory von heute
https://www.exploit-db.com/exploits/52082

DLL Hijack | SO-Preload [kurze Vorstellung]



SEARCH PATH based DLL Hijacking

Google: dll hijacking!

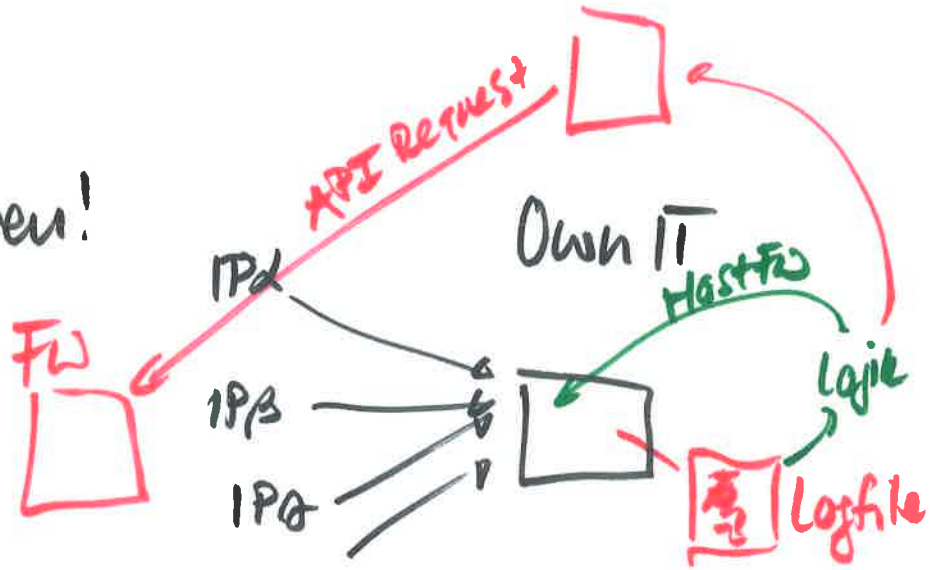
DLL Hijacking Attacks

DLL (Dynamic Link Library) hijacking is a type of cyberattack where an attacker exploits the way applications load DLL files in Windows operating systems. When an application starts, it often searches for required DLL files in a specific order, typically beginning with its own directory and system directories. However, if an attacker places a malicious DLL with the same name as a legitimate one in a location that the application searches first, the application may load the malicious file instead of the intended one.

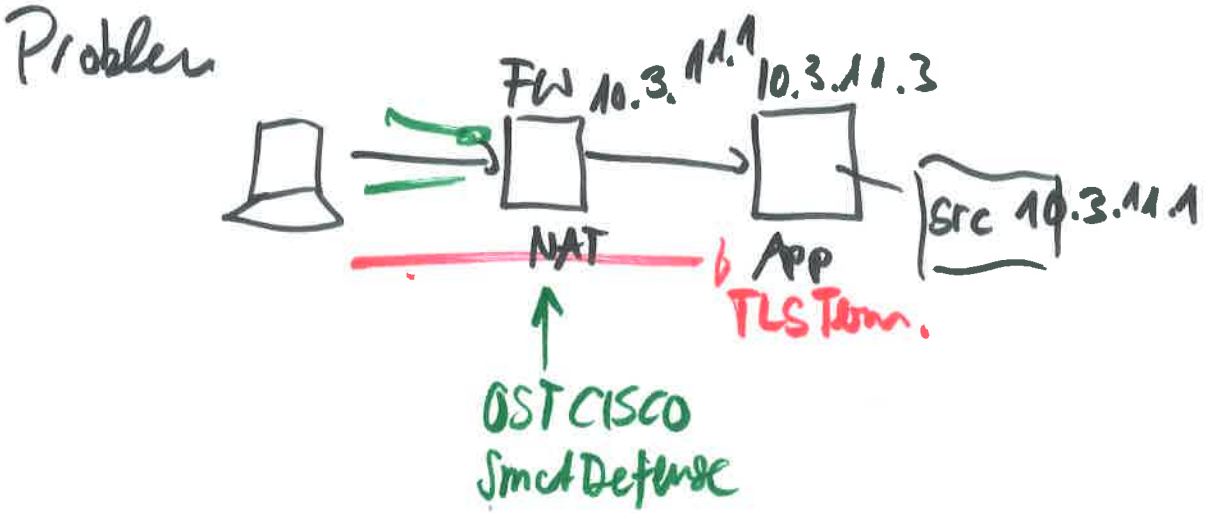
This attack can allow an attacker to execute arbitrary code with the same privileges as the application, potentially leading to data theft, system compromise, or unauthorized access. DLL hijacking is particularly effective because it takes advantage of trusted applications, making detection harder for security systems. It underscores the importance of secure application development practices and stringent system protections to prevent misuse.

DDoS

- Überlast generieren!

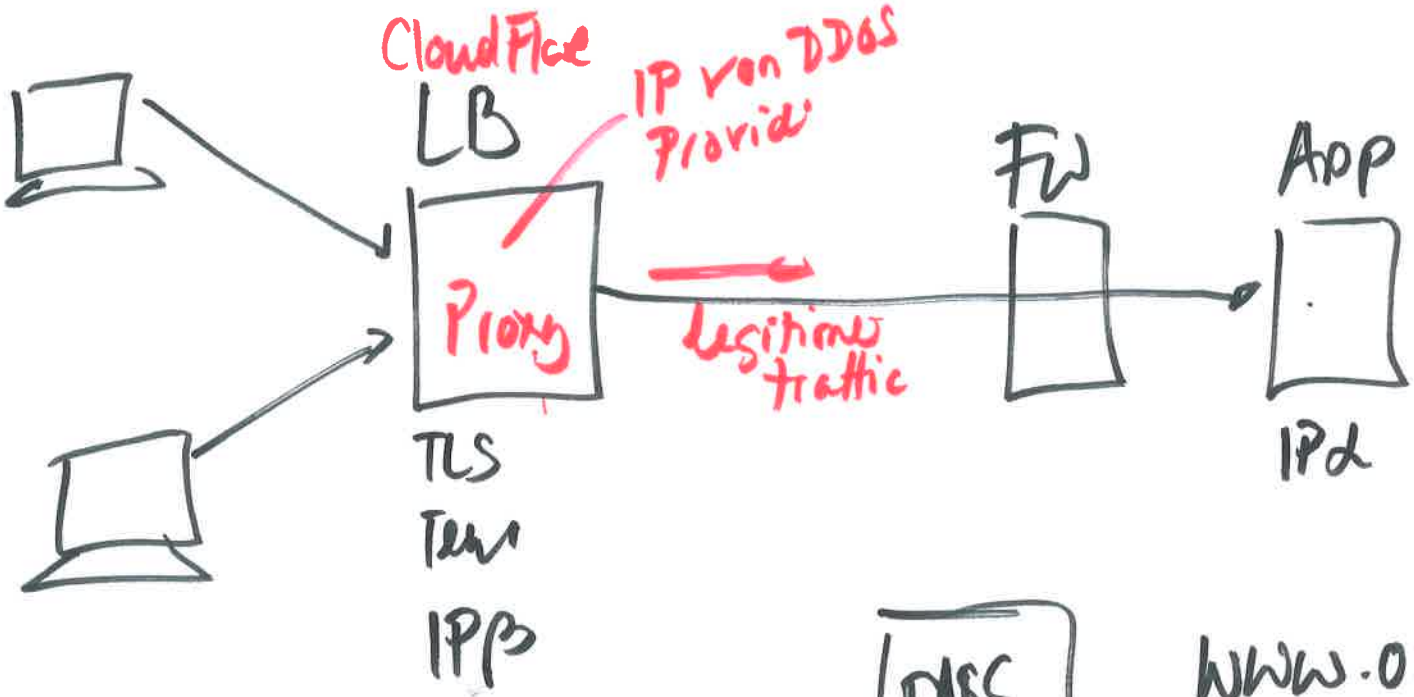


Frage / Diskussion Marco Kuoni aus Teams Chat



Wir diskutieren den DDoS Fall von Marco Kuoni (siehe MS Teams) und wie man präventiv vorbereiten kann, oder dann im Notfall via CloudFlare vorgeschalteten Proxy eine Lösung umsetzt. Problem bei selbst gemachten Lösungen, man braucht etwas was die Logs parst und dynamisch die Firewall konfiguriert. NAT könnte ein Problem darstellen, dann geht es auf dem HostOS nicht. Oder aber man macht einen API Call auf die Firewall und sperrt für ne Zeit ne IP, was aber die FW guys nicht so gerne sehen. Auf einem Linux kann man hierfür fail2ban einsetzen. Siehe auch https://pwspray.vm.vuln.land/ für ne fail2ban Umsetzung.

Cloud Flare [DDoS Lösung via Provider]



www.ost.ch
IPA → IPB

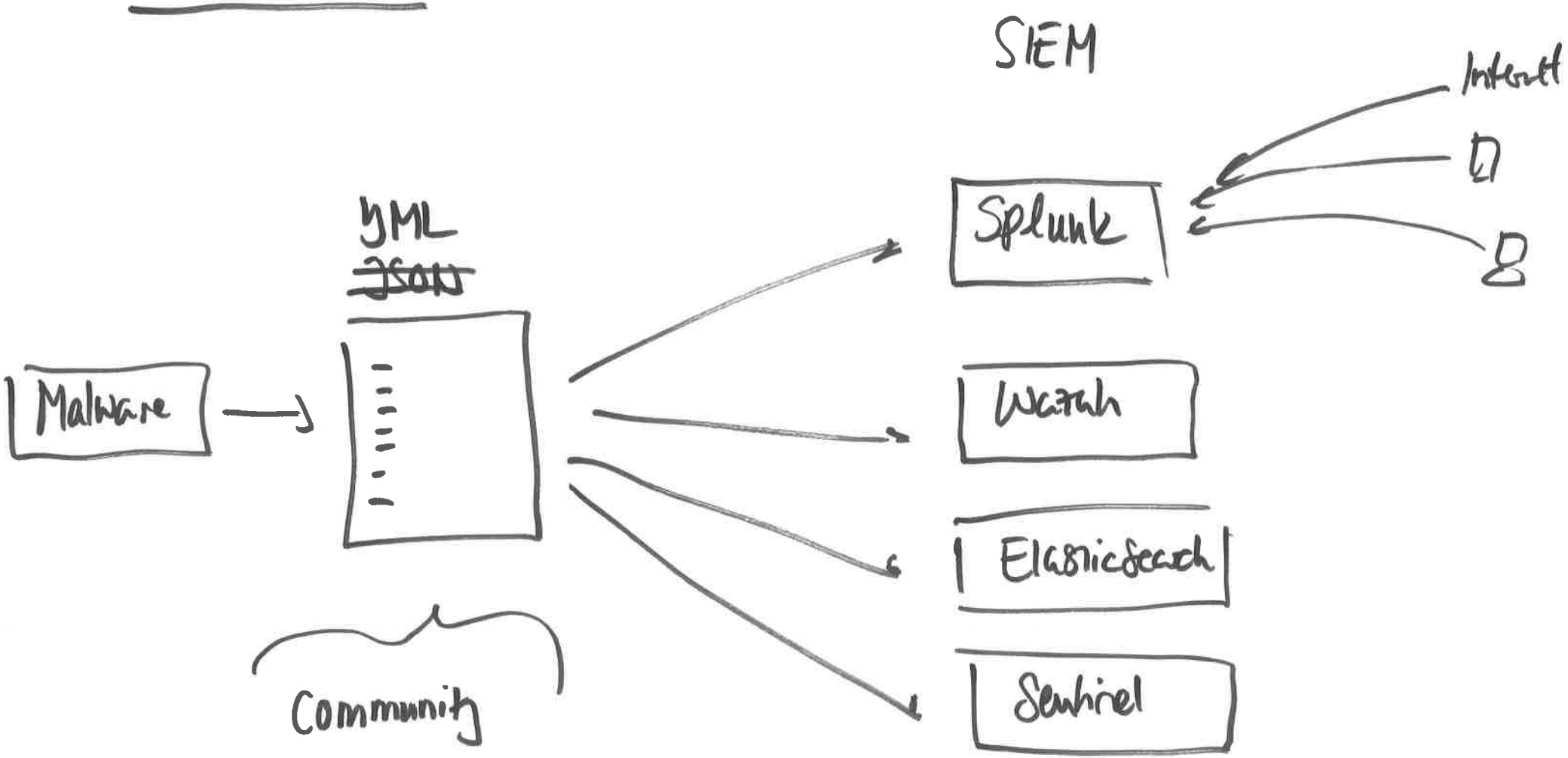
A record

ttl = 8h

Change IP → ttl ist wichtig
tiefe ttl ermöglicht raschen Wechsel.

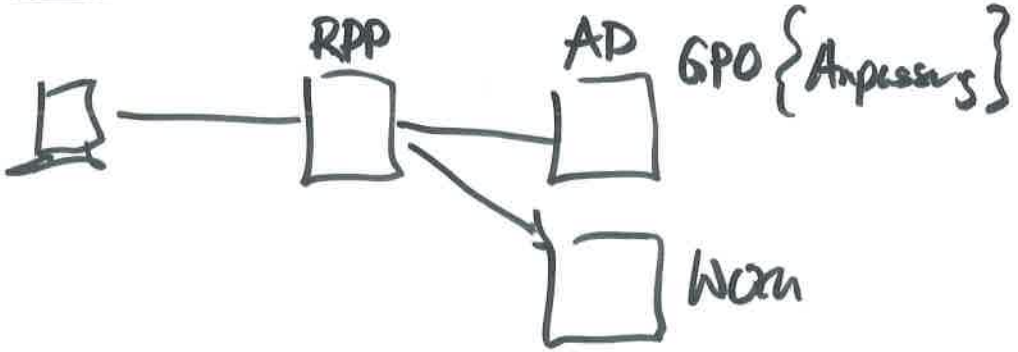
CloudFlare Load Balancer (LB) terminiert die TLS Verbindung, macht die DDoS Protection und schickt legitimen Traffic zur Anwendung. Somit verlagert man den DDoS Schutz zum DDoS Provider (CloudFlare oder andere). Machen viele, die sich vorher nicht genügend vorbereitet haben.

SIGMA



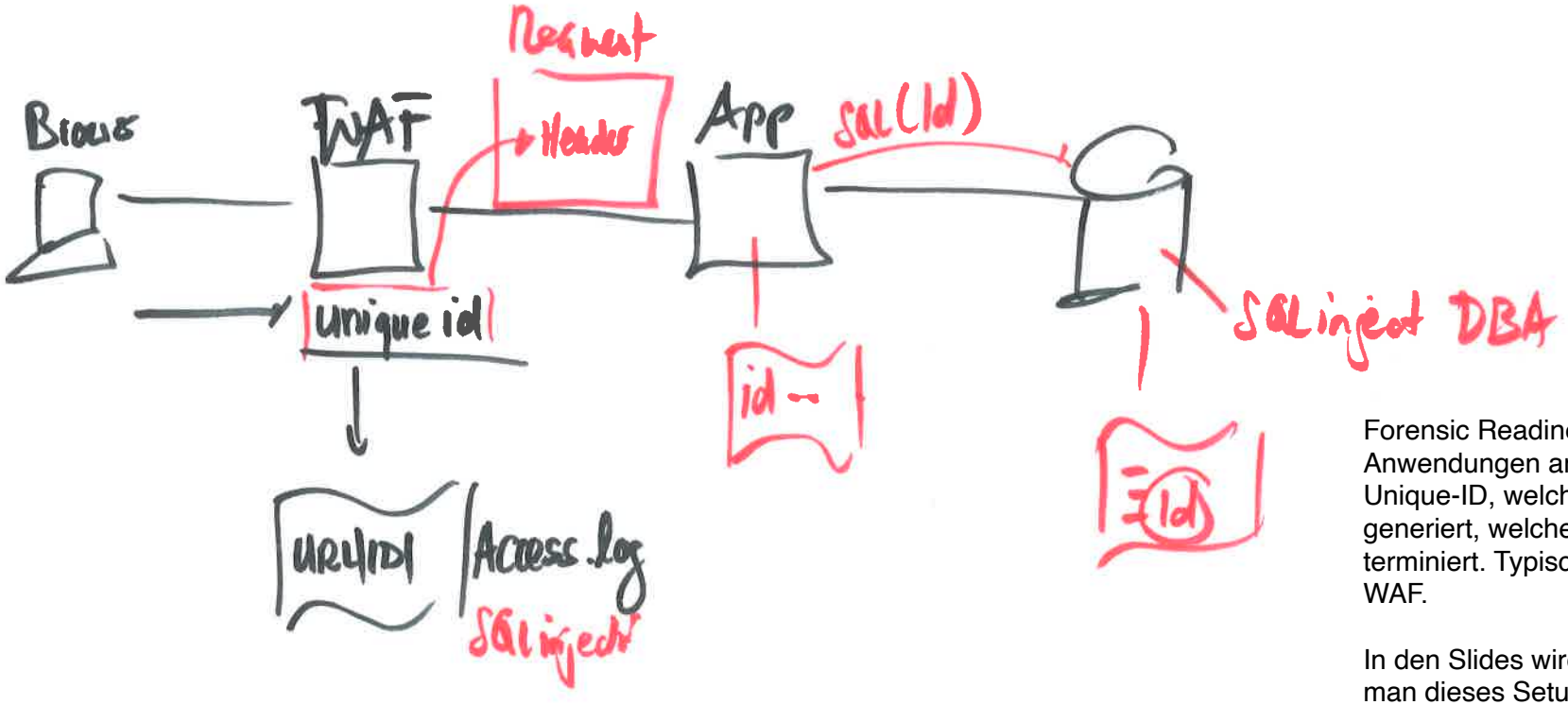
Einführung SIGMA. Generelles YML basiertes Rule File das man dann konvertieren kann in Splunk Format, oder ElasticSearch Format und weitere. EIne breite Community teilt SIGMA Rules für die Erkennung von Malware. Mehr dazu in den Slides.

Forensic Readiness



Windows

Forensic Readiness unter Windows heisst, dass man über die GPO die Logging Einstellungen so vorgibt, dass wichtige Events wie “failed login” oder “PowerShell Parameters” geloggt werden. Muss man vorab machen, um im Incident Fall diese Logs parat zu haben

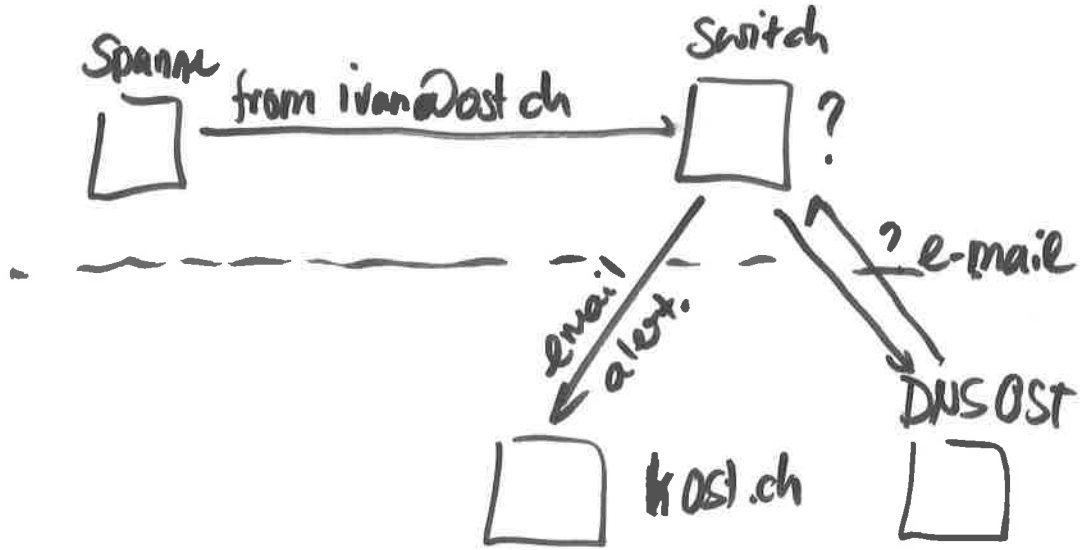


Forensic Readiness für Web Anwendungen arbeiten mit einer Unique-ID, welche das Device generiert, welchen TLS terminiert. Typischerweise eine WAF.

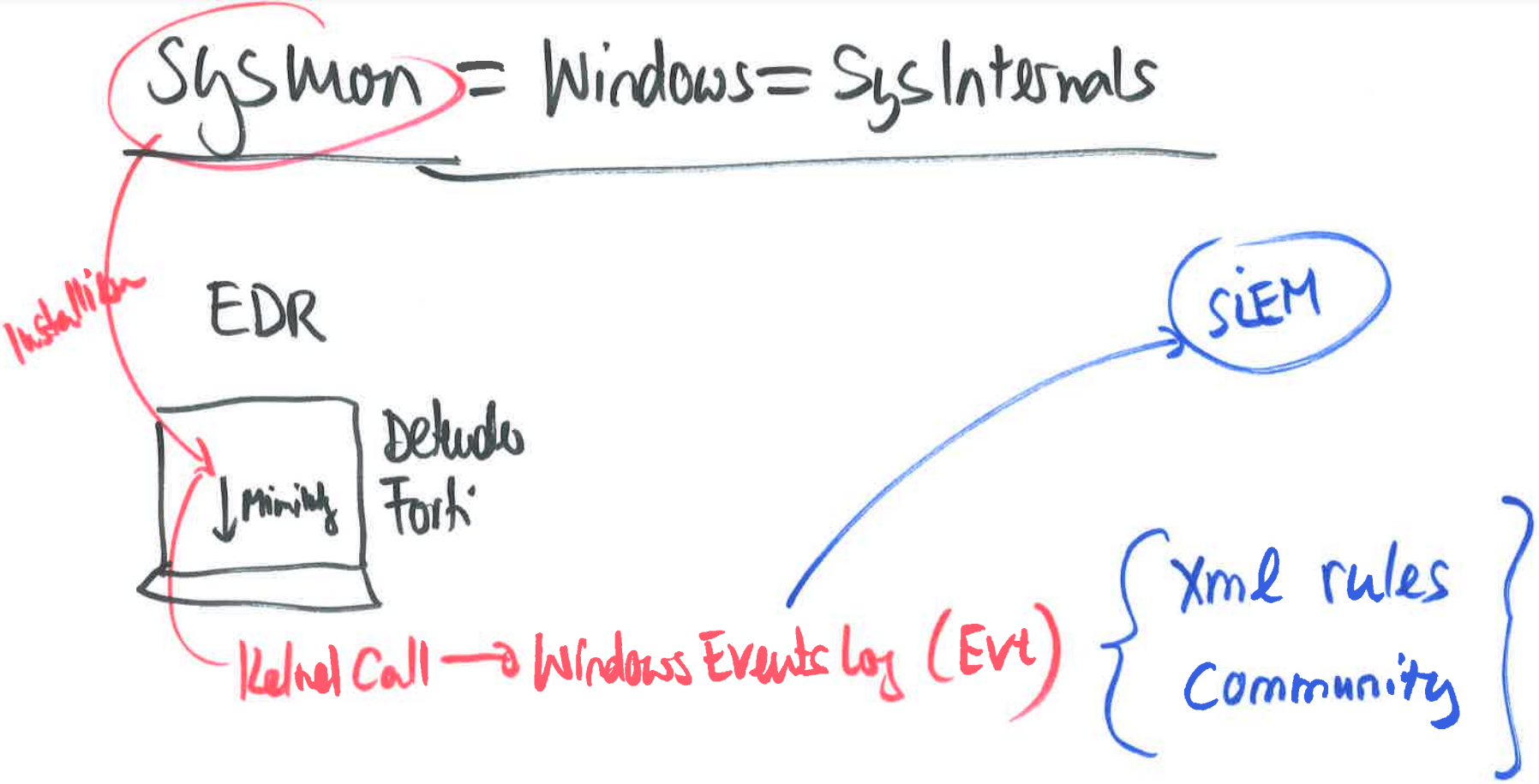
In den Slides wird erklärt, wie man dieses Setup mit einem Apache Webserver selbst umsetzt (diverse Module nutzen)

Viren → E-Mails SPF / DKIM / DMARC

- SPF Sender Policy Framework ≡ Whitelisting Sender MX → DNS
- DKIM Signaturen im SMTP Header
- DMARC



An der Prüfung wird vorausgesetzt, dass ihr SPAM Protection mit SPF, DKIM, DMARC versteht. Ist eine Wiederholung zu bereits gehabten Modulen. Die Slides zeigen einfach nochmals das Wichtigste auf. Sind nicht durch die Slides gegangen. Bitte selbst machen und bei Unklarheiten fragen.



Sysmon ist ein Windows SysInternal Tool das man auf einem Windows System installieren kann, welches Kernel API Calls überwacht und diese ins Event Log von Windows schreibt. Kann man sehr gut gebrauchen für Research Zwecke, wenn man auch verstehen will, was der Defender eigentlich macht.

Die Übung dient dazu, dass ihr 1x sysmon selbst ausprobiert habt und damit Mimikatz erkennt.