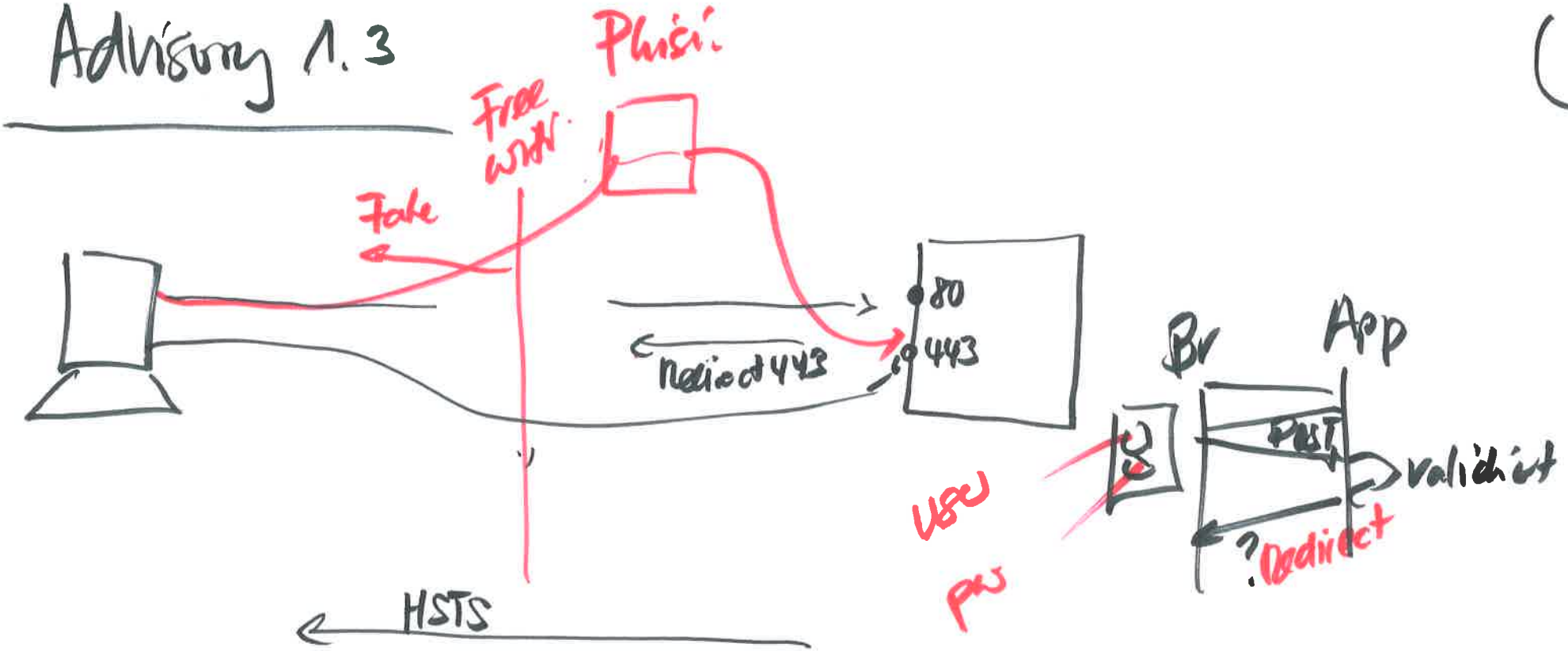
Cyber Defense

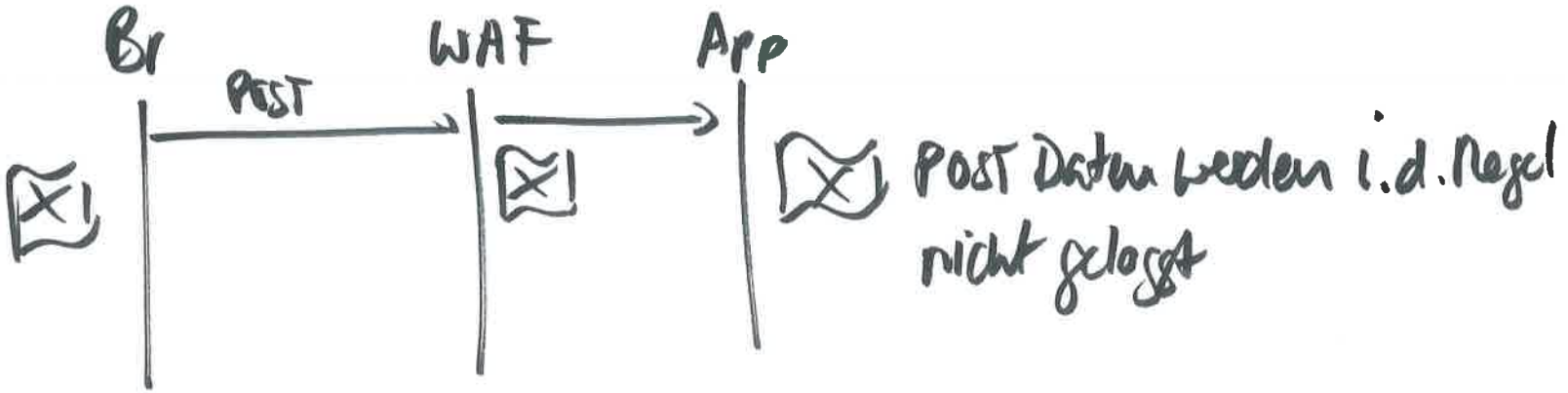
27.11.24

CVSS, CVE, CWE

Adrisonios Suchn

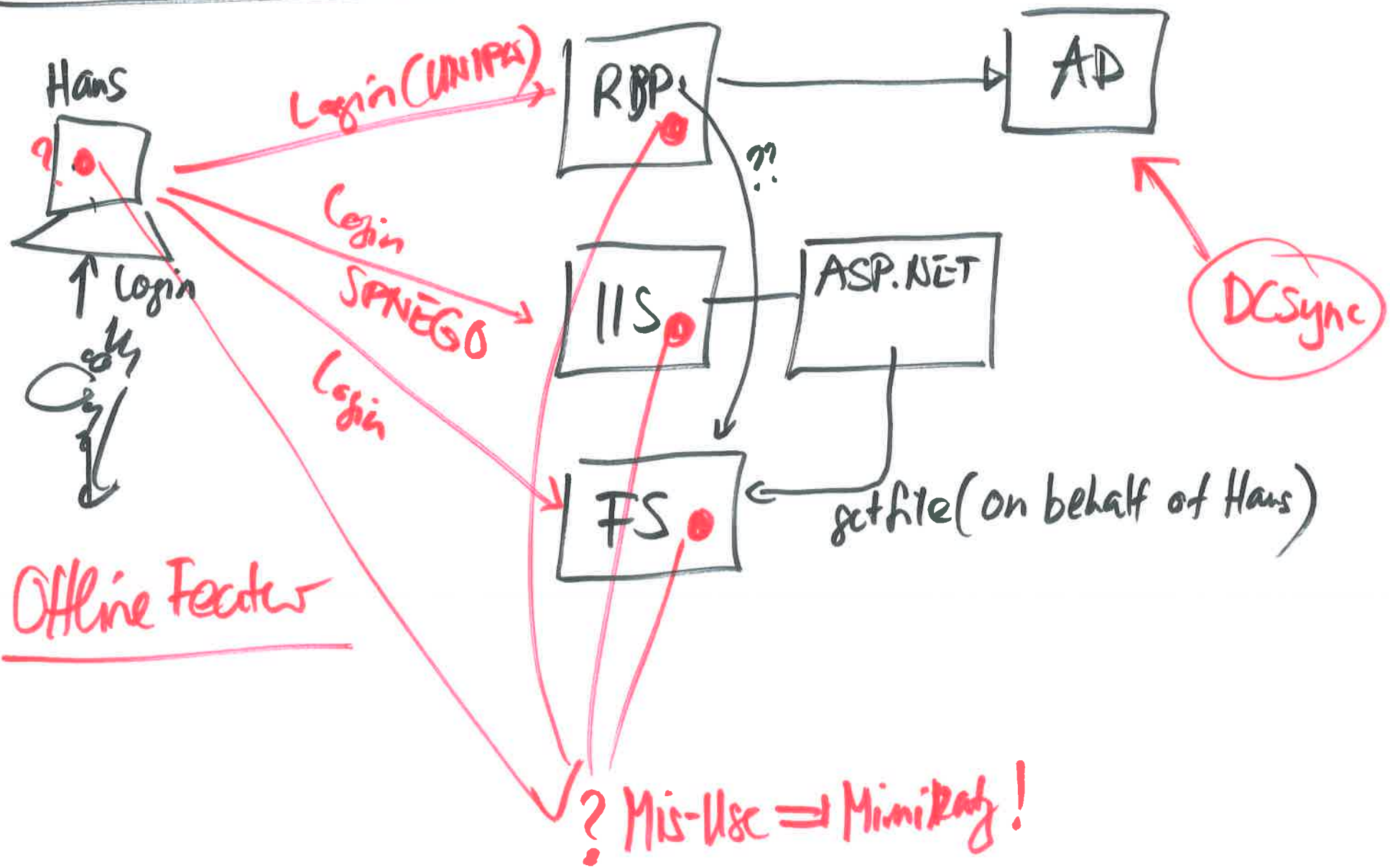
Aufgabe 1.3





Redirect von Port 80 auf 443 ist zwar ne korrekte Antwort, aber die erwartete Antwort wäre HSTS. Der Redirect ist daher ungünstig, da der MitM die Response manipulieren kann und auf eine Phishing Seite redirecten kann. Daher ist das nicht so ideal.

Microsoft Authentisierungen



Microsoft unterstützt diverse Auth Methoden. Ein RDP Login verhält sich anders als ein Kerberos Ticket via Browser (SPNEGO) und nochmals anders als ein Network Login für Fileserver Zugriff. Metasploit zu verstehen bedeutet, dass man den Gesamtzusammenhang hier erkennen muss.

Mimikatz → POST Exploitation Tool

Was ist es nicht!

- man wird nicht Admin, weil Mimikatz Local Admin Rechte braucht

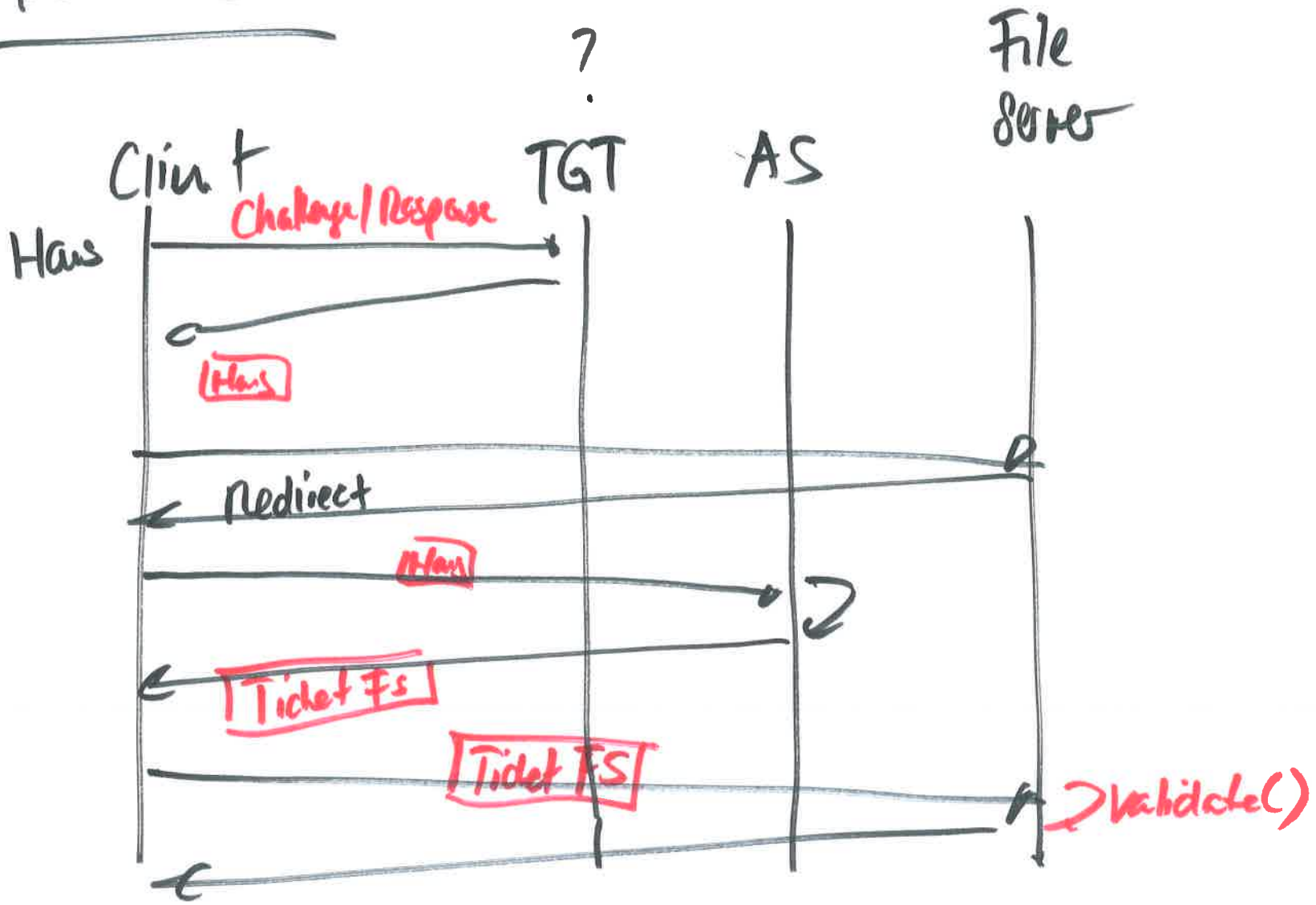
Es ist ein Tool um die diversen Auth Möglichkeiten weiter auszunutzen

→ Domain Admin Rechte erlangen

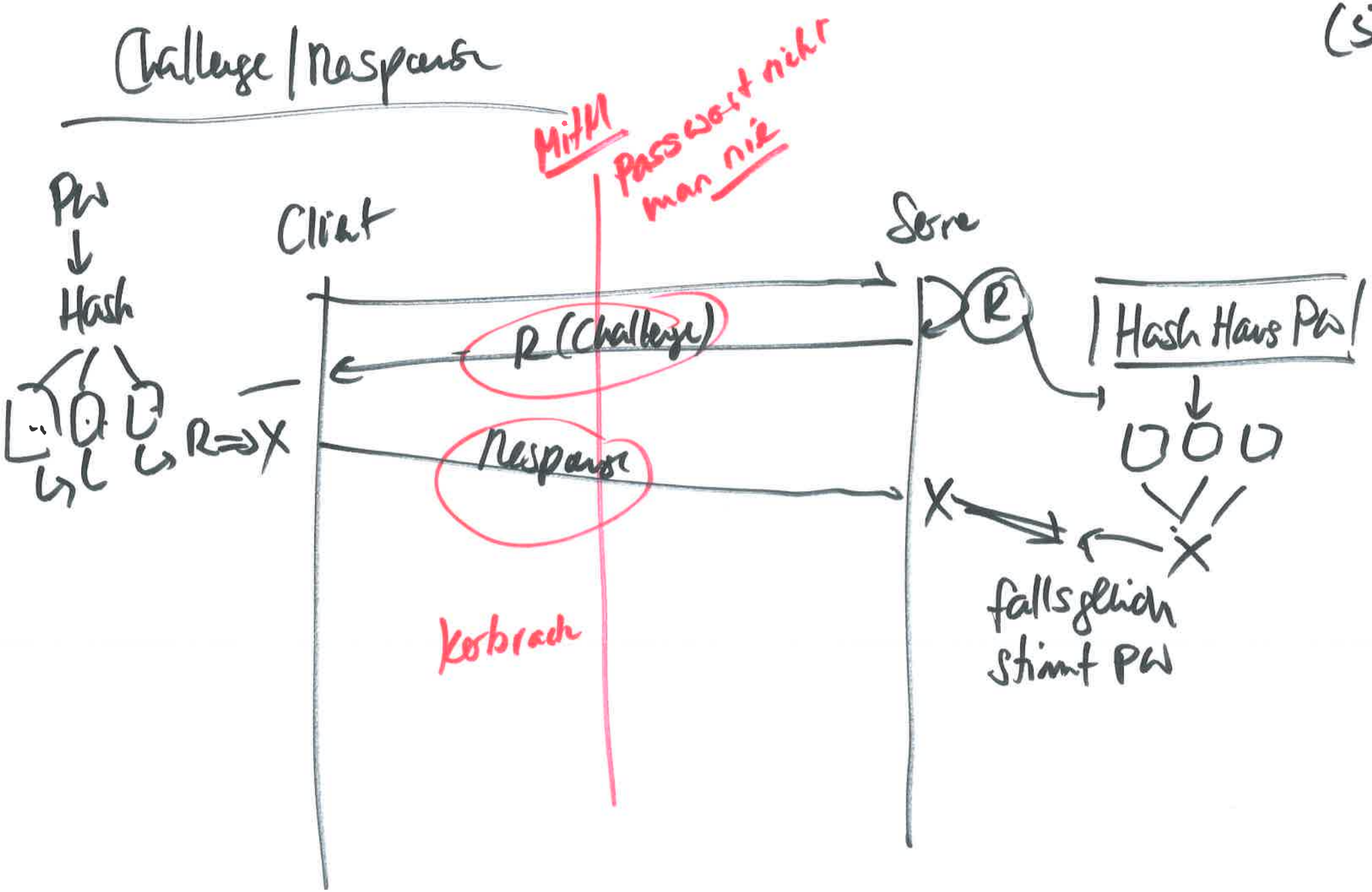
→ Privilege Escalation + Lateral Movement

Mimikatz ist extrem mächtig (wird durch alle Anti-Viren Produkte erkannt), mit welchem man mit Tokens, Cached Credentials, DPAPI rumspielen kann. Die in den Folien gezeigten Zusammenhänge sind aus Reverse Engineering Arbeiten resultiert. Folien stammen nicht aus der offiziellen Microsoft Doku.

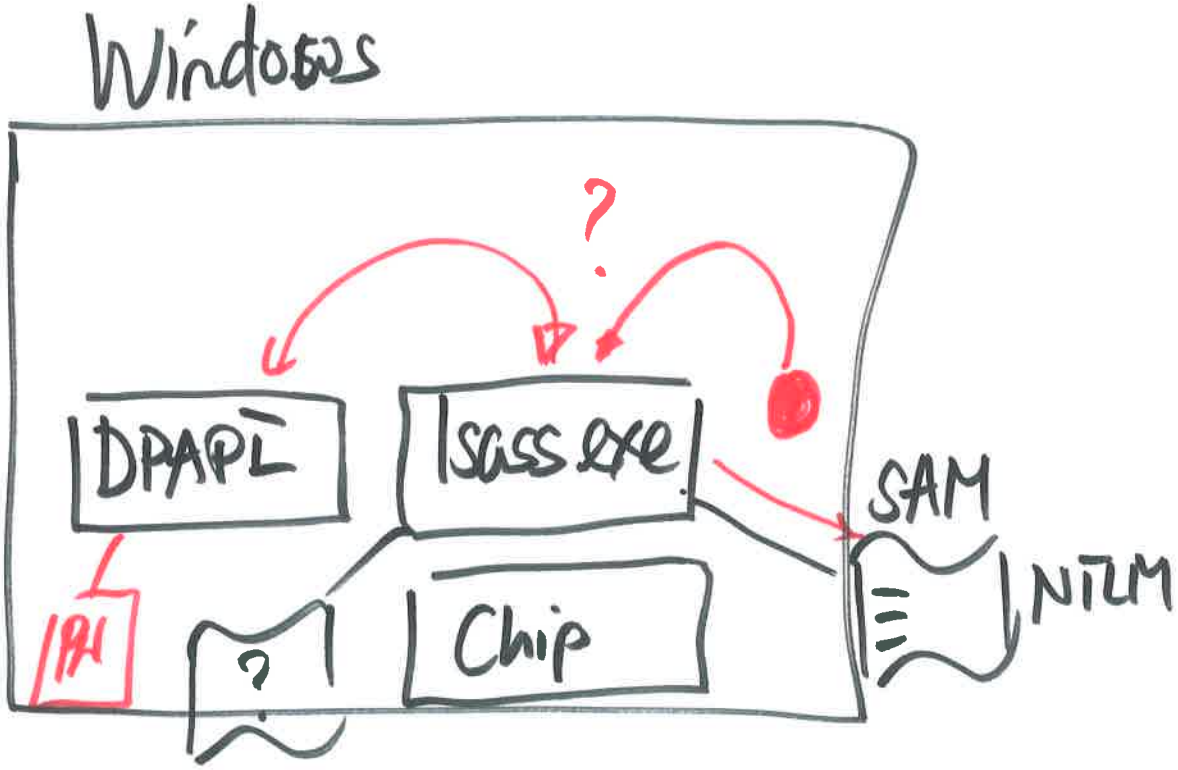
Kerberos



Kerberos basiert auf einem Challenge/Response Verfahren. Hinsichtlich Mimikatz wichtig, weil Mimikatz dann keine Credentials kennt. Obere Zeichnung ist vereinfacht und zeigt, dass man mit einem TGT ein Master Ticket erhält, mit welchem man beim AS weitere Service Tickets beziehen kann. Alle Tickets natürlich mit Asymetrischer Krypto abgesichert (Pub/Priv Key, Signaturen, Timestamp)



Man in the Middle kann bei Kerberos lediglich die Challenge und Response sniffen und dann mit Brute-Force versuchen den Key zu finden, mit welchem die Response berechnet wurde (siehe Tool “kerbcrack”)



Heute geht es um Windows und wie Windows die Credentials und Tokens der User verwaltet.

a) gegenüber SSO
b) gegenüber DPAPI

Der lsass.exe ist der zentrale und einzige Prozess den Microsoft erlaubt, die entsprechenden Kernel Aufrufe zu machen