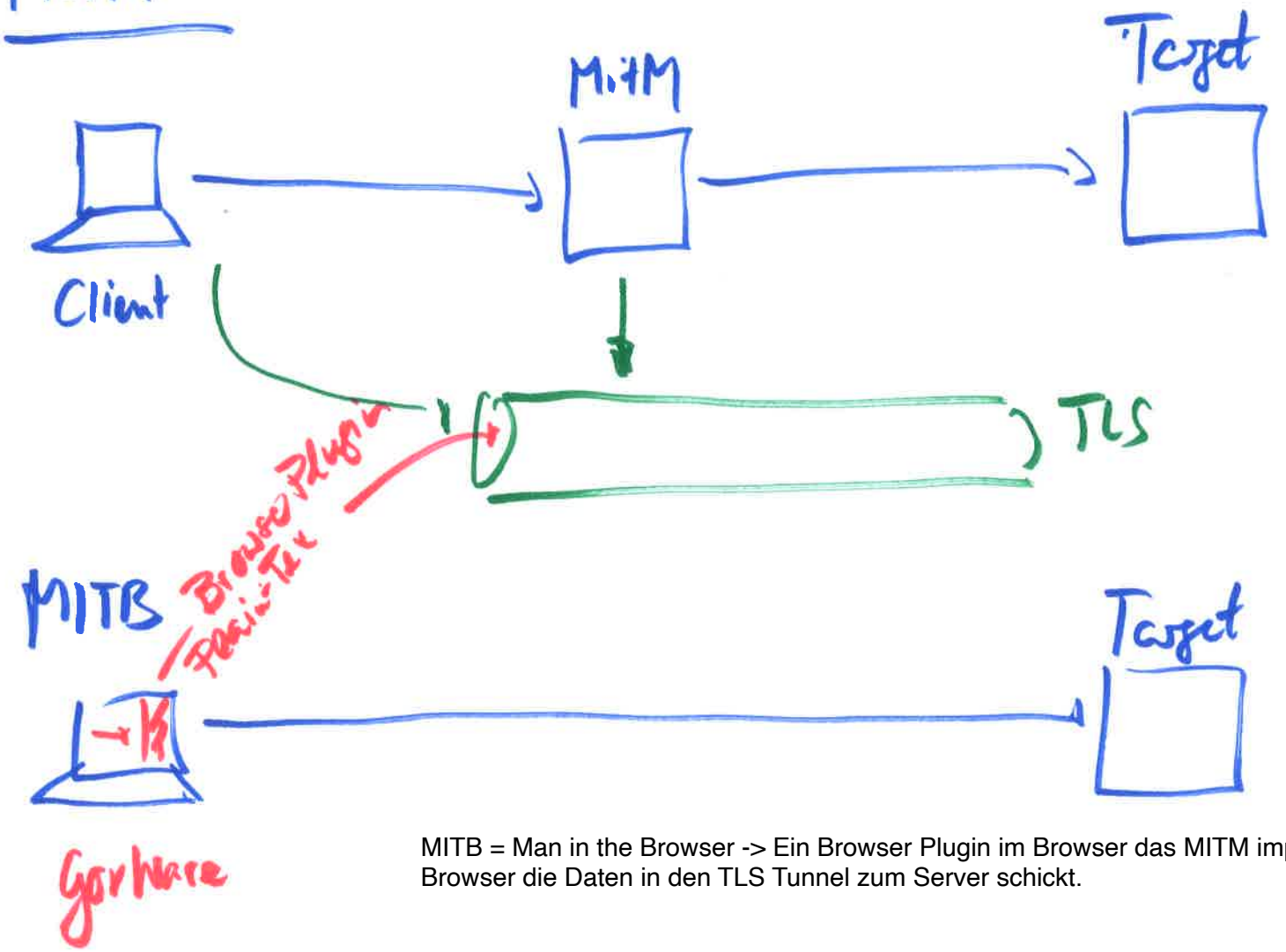
Cyber Defense

30.10.2024

MitM



MITB = Man in the Browser -> Ein Browser Plugin im Browser das MITM implementiert, bevor der Browser die Daten in den TLS Tunnel zum Server schickt.

MitM – Wie wird man, kommt man zwischen Client + Server

- ARP Spoofing
- DNS Spoofing
- DHCP Attack
- Rogue Access Point (Wifi)
- Glasfaser Splitter
- Switch Port Mirroring
- Malware (/etc/hosts / Proxy)
- IMSI Catcher (G3, G4, G5)
- BGP
- NFC
- Bluetooth

Wie kommt jemand in eine MitM Position? Siehe auch die Slides wo alle diese Varianten kurz vorgestellt werden.

Was kann ein MitM Angreifer tun?

Unverschlüsselte Protokolle

bootp

DNS, DHCP, tftp, http, telnet, ftp

- Mitlesen
- Andern Request/Response

Was kann ein Angreifer machen, wenn man in einer MitM Position unverschlüsselte Protokolle “sieht”

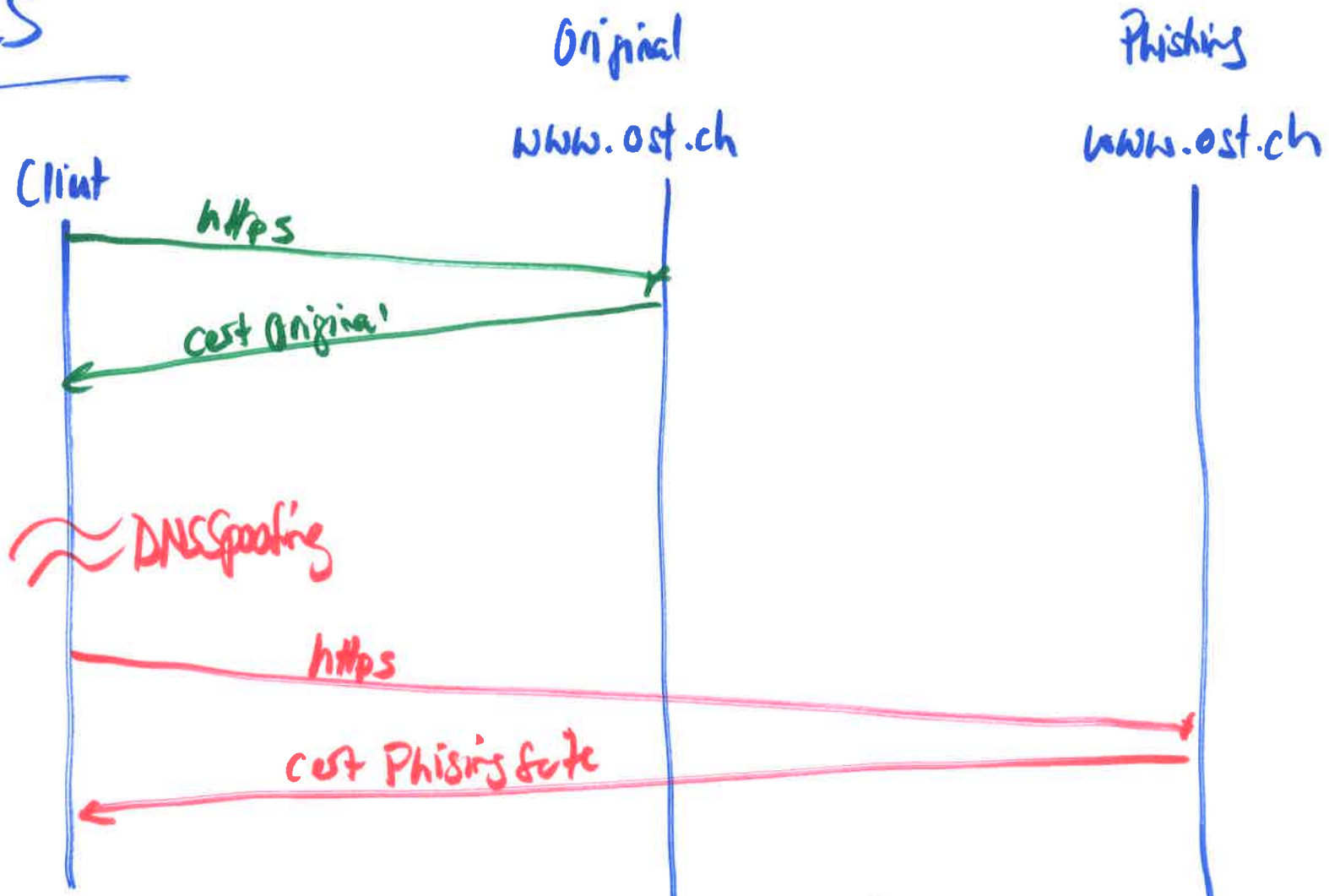
Verschlüsselte Protokolle

TLS, IPSec,

- Terminieren (TLS Warnung) → neue Verbindung
  - Burp, ZAP
- Downgrade Attacke
  - SMB Relay

Was kann ein Angreifer machen, wenn man in einer MitM Position verschlüsselte Protokolle “sieht”

TLS



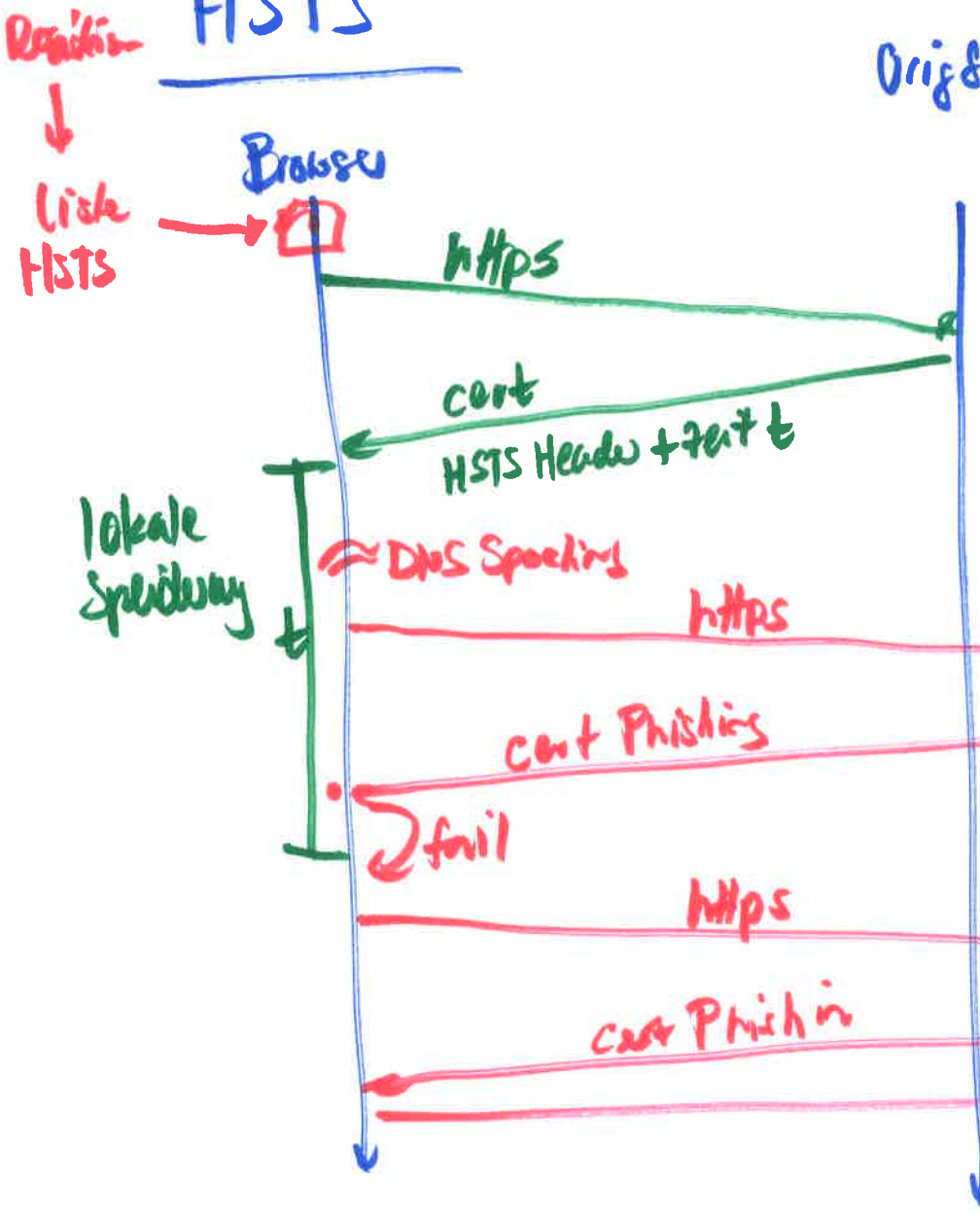
gegenmassnahme Mobileapps → Certificate Pinning (Cert des Servers oder Intermediate Cert)
in App ausliefern

↓

Browser → HPKP ⇒ abgeschafft → hsts

HTTP Strict Transport Security

HSTS



Wir diskutieren im Kontext von Man in the Middle, wie sich http-strict-transport-security (HSTS) auswirkt

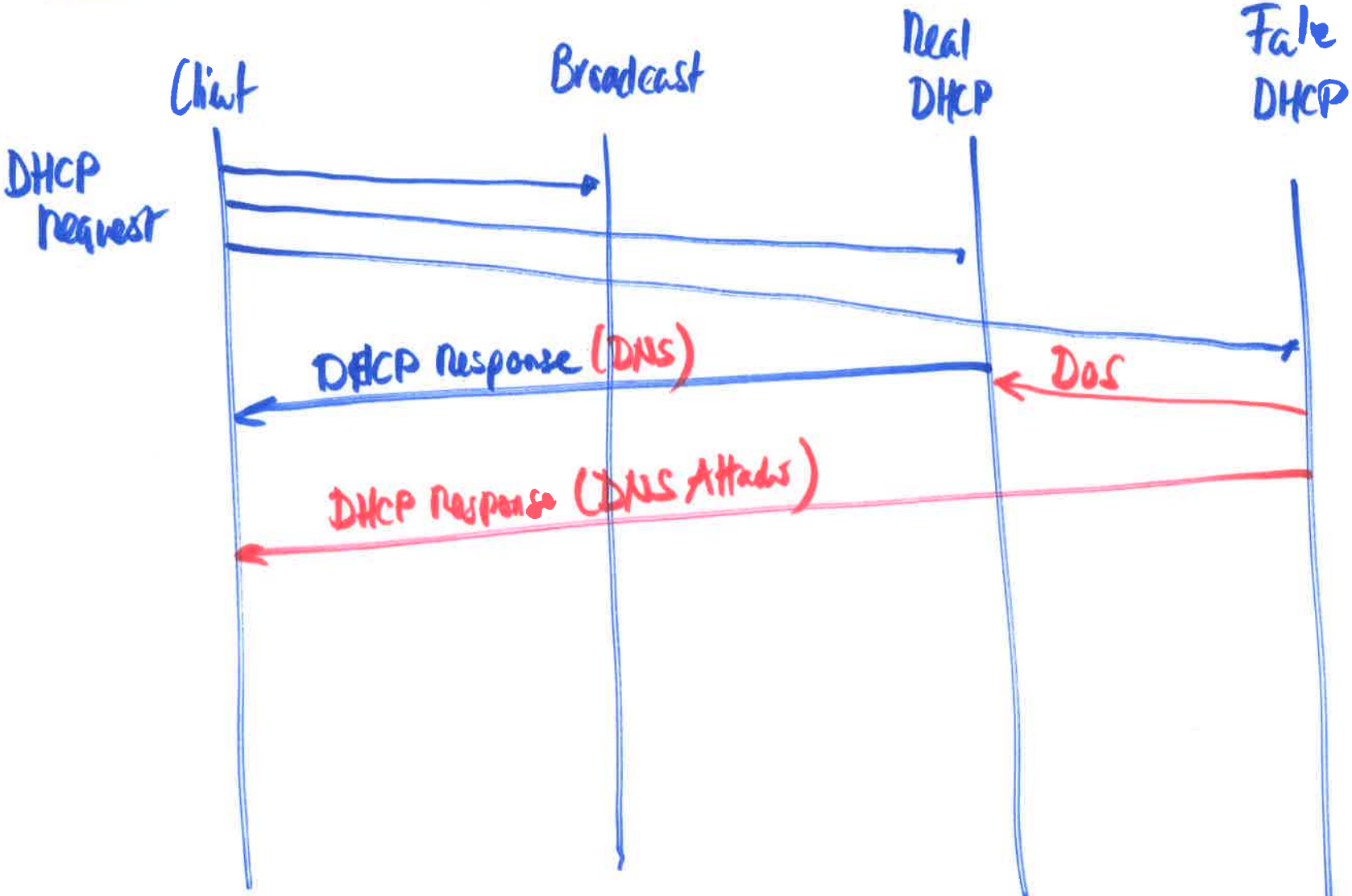
Wenn eine Domain nicht in der HSTS preload Liste eingetragen ist, dann schützt HSTS nur, wenn das Opfer einmal ohne MitM auf der Seite war und man während der Gültigkeit des HSTS auf eine Phishing Seite verbindet

Hier habe ich 3 Demos gemacht
a) www.ost.ch mit neuem Browser Profil, danach MitM und mein Button (Accept Risk)

b) www.ost.ch mit neuem Browser Profil, danach via MitM und ein Accept Risk Button ist dort, welches der User klicken kann

c) www.compass-security.com mit neuem Browser, danach MitM und trotzdem kein Accept Risk Button, weil Compass Security Domain in der hsts preloaded Liste drin ist

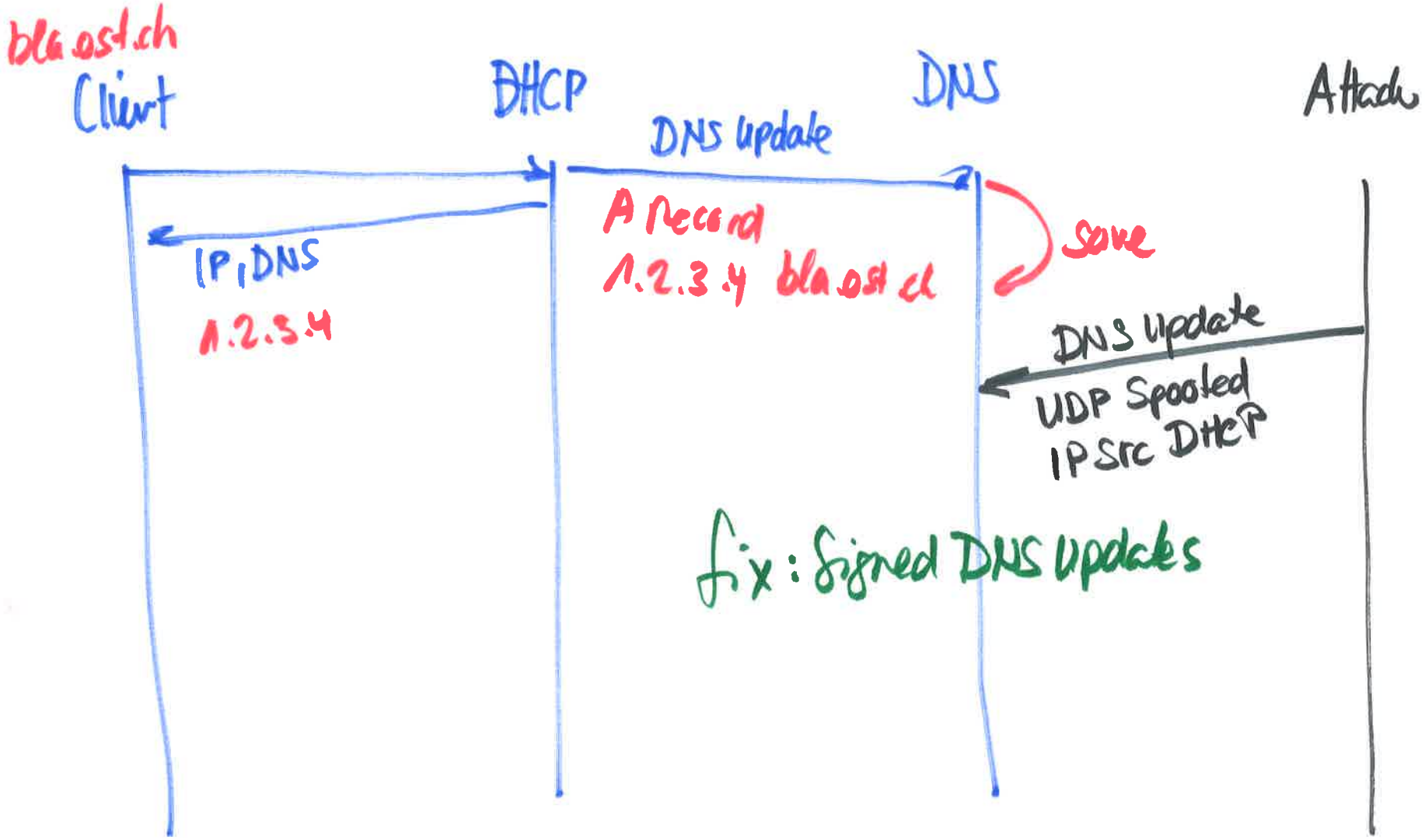
DHCP Poisoning



DHCP funktioniert über die Broadcast Adresse und die schnellere DHCP Response wird vom Client akzeptiert. Sprich der Fake DHCP erhöht durch DoS auf den Real DHCP seine Chancen, zuerst ne Antwort an den Client senden zu können.

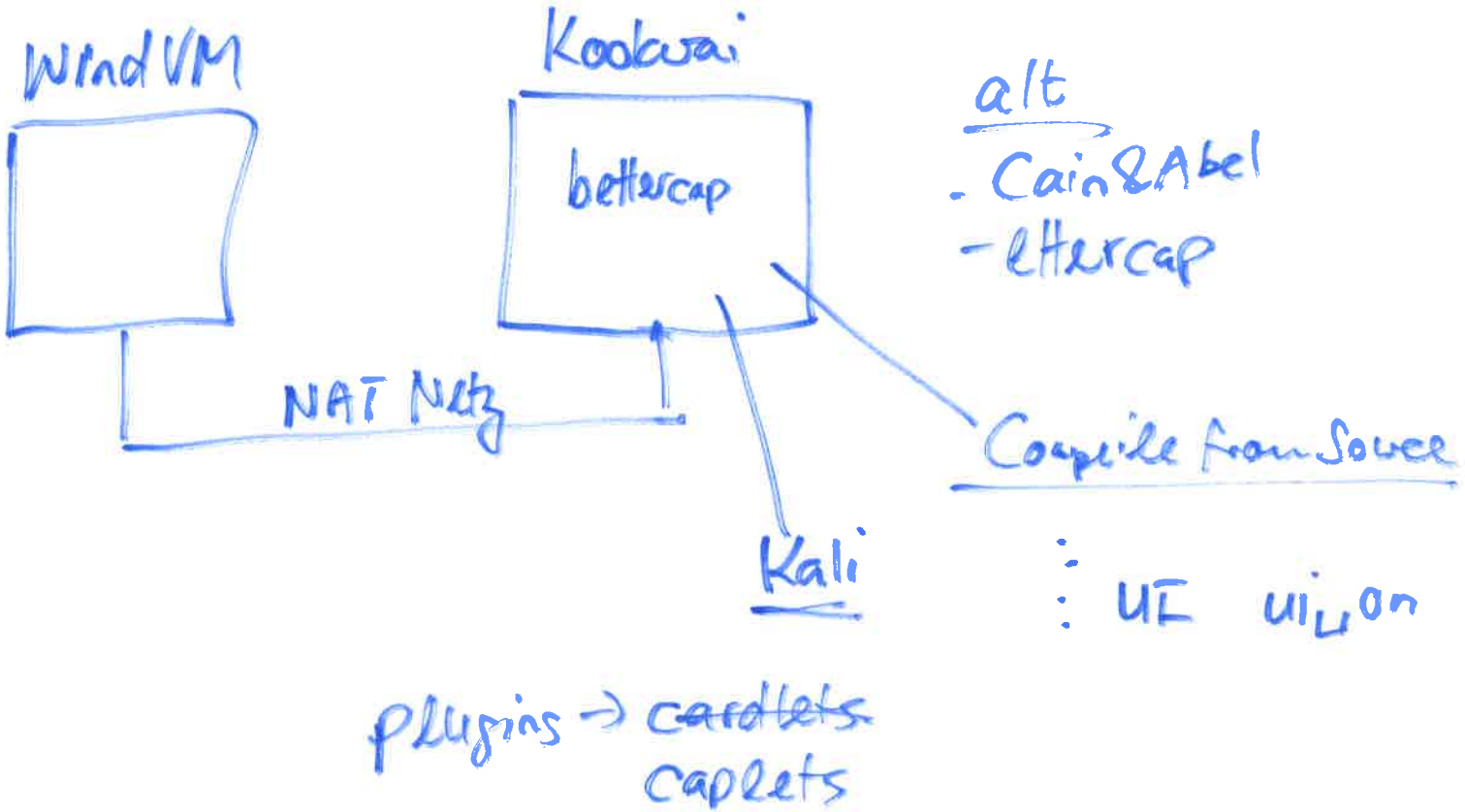
Im Fake DHCP Request ist der DNS falsch eingetragen, nämlich der DNS des Angreifers (damit man DNS Spoofing machen kann)

DNS Update



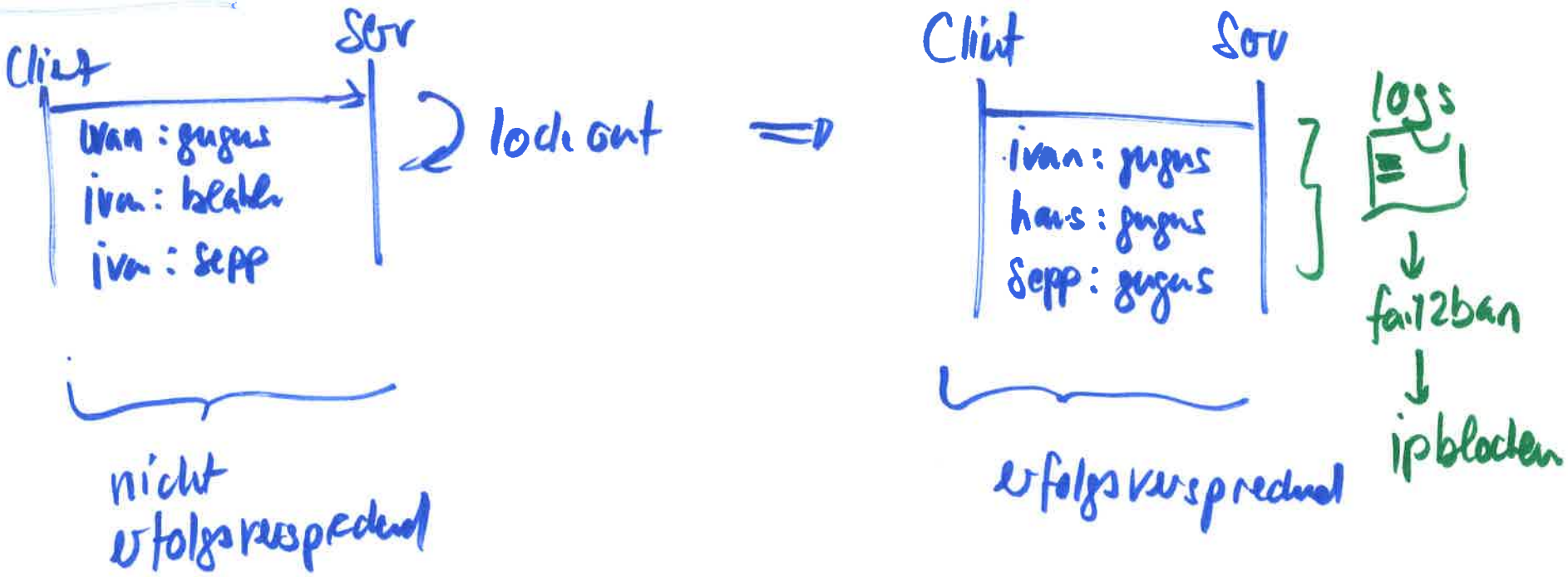
DNS Update wird gebraucht, wenn der DHCP eine IP rausgibt und den Host der die IP kriegt beim DNS eintragen will. Das macht das Active Directory so. Nicht sehr wahrscheinlicher Angriff, da AD heutzutage Signed DNS Update Packets schickt.

ARP Spoofing (Lab 02)



Kurze Erwähnung von bettercap, das in der Übung für MitM mittels ARP Spoofing eingesetzt wird. Hier war nur die Idee zu sagen, dass wir bettercap einsetzen und vom Source Code her nutzen, weil die Kali Version in früheren Jahren Probleme machte.

PW Spray



Hier gehen wir der Frage nach, was PW Spraying bedeutet. Angreifer lassen das PW konstant und iterieren den Usernamen. Der PW Spray Server im Hacking-Lab kann hierfür verwendet werden. Der Server wurde während dem Unterricht kurz gezeigt.

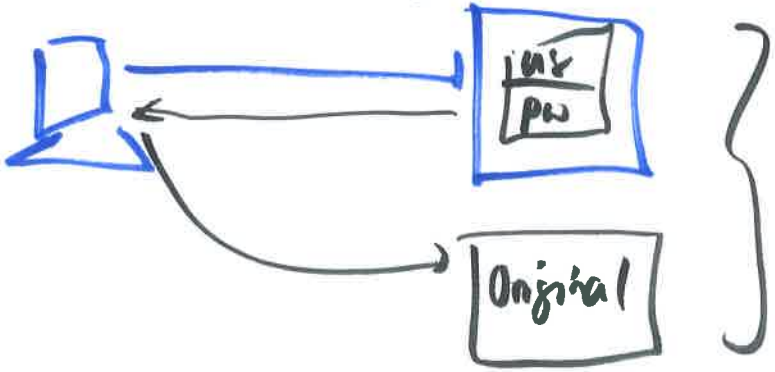
Dieser Server nur daher kurz erwähnt, weil dieser für die HTTPS MitM eingesetzt wird, der HTTPS Reverse Proxy Übung im HL

HTTP(S) MitM (Phishing)

Variante 1

www.remmer.ch (Original)

www.remmer.ch (Holograph) Proxy



GoPhish (Übung 9)

= 1 Schutz = 2FA

GoPhish stellt eine Phishing Platform bereit, die gleich aussieht wie das Original

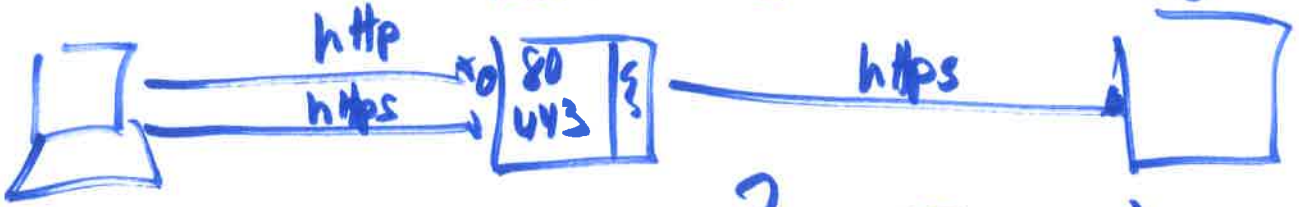
Erklärt als Vorbereitung für die Übung im HL

Variante 2

pwdprog.vm.vuln.lan

Original

↓ ReverseProxy



http2https

https2https

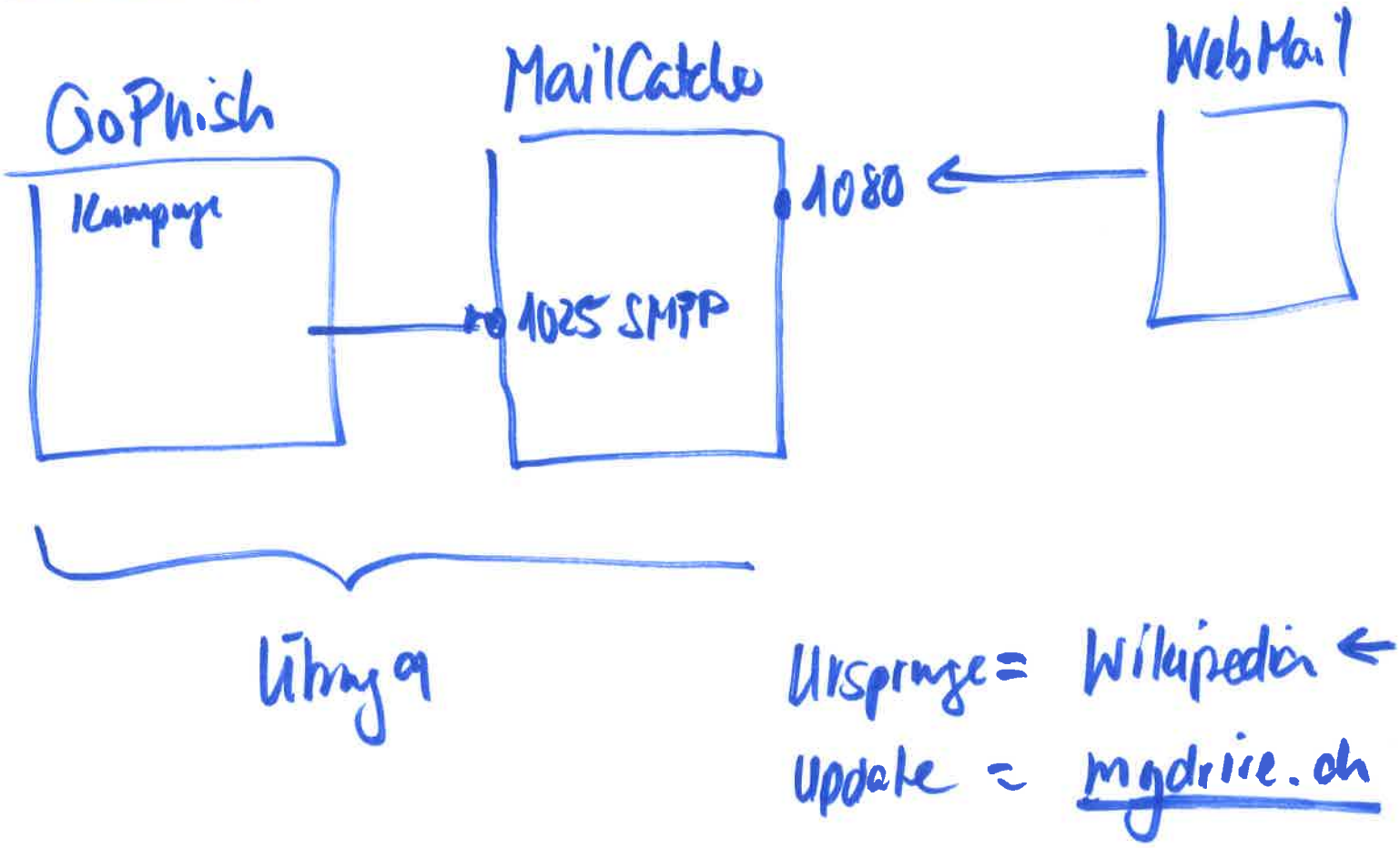
= ✓ (Übung 6)

= Bypass 2FA

Hierbei agiert die Phishing Seite als Reverse Proxy und leitet alle Requests zum Original Server

Hat für den Angreifer den Vorteil, dass 2FA nichts bringt. (Ausser FIDO2)

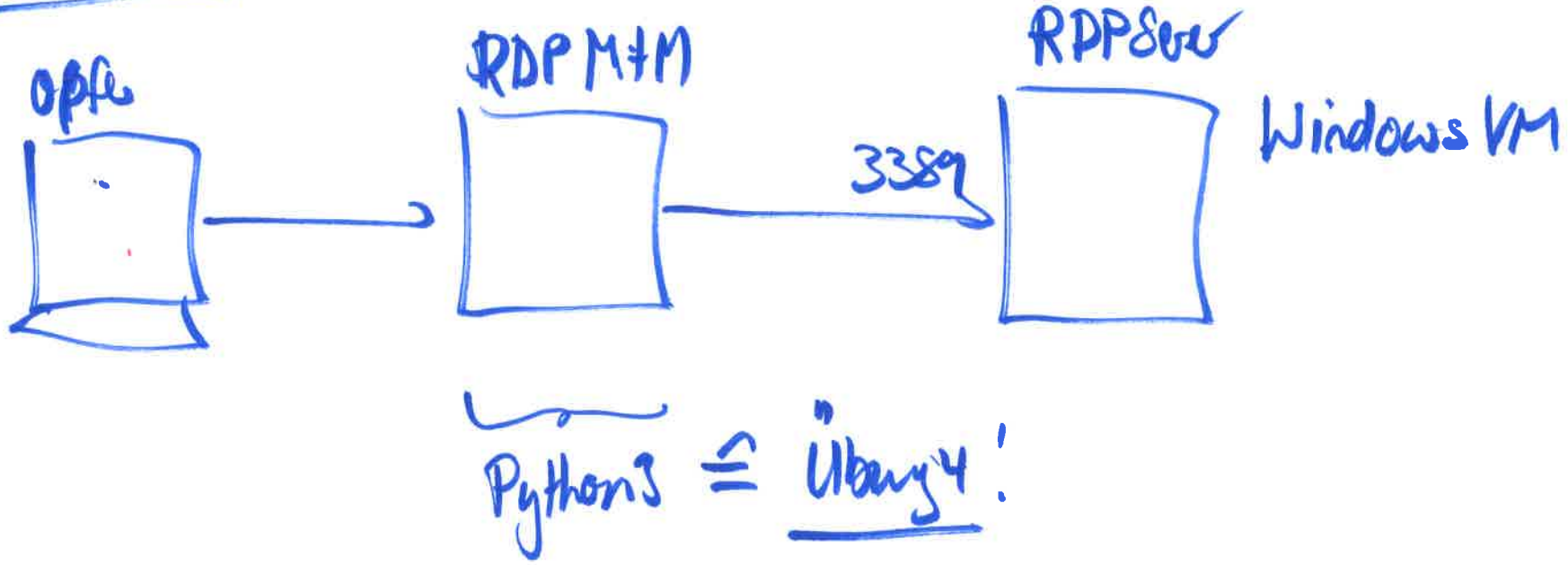
Mailserver



Kleiner Trick erklärt, falls man mal kurz nen Mailserver fürs Testen benötigt. MailCatcher ist ein Docker, der einen SMTP Port öffnet der alle Mails entgegen nimmt und ein WebUI wo man die Mails dann betrachten kann.

Brauchen wir, weil GoPhish einen Mailserver braucht um die SW auszutesten.

RDP

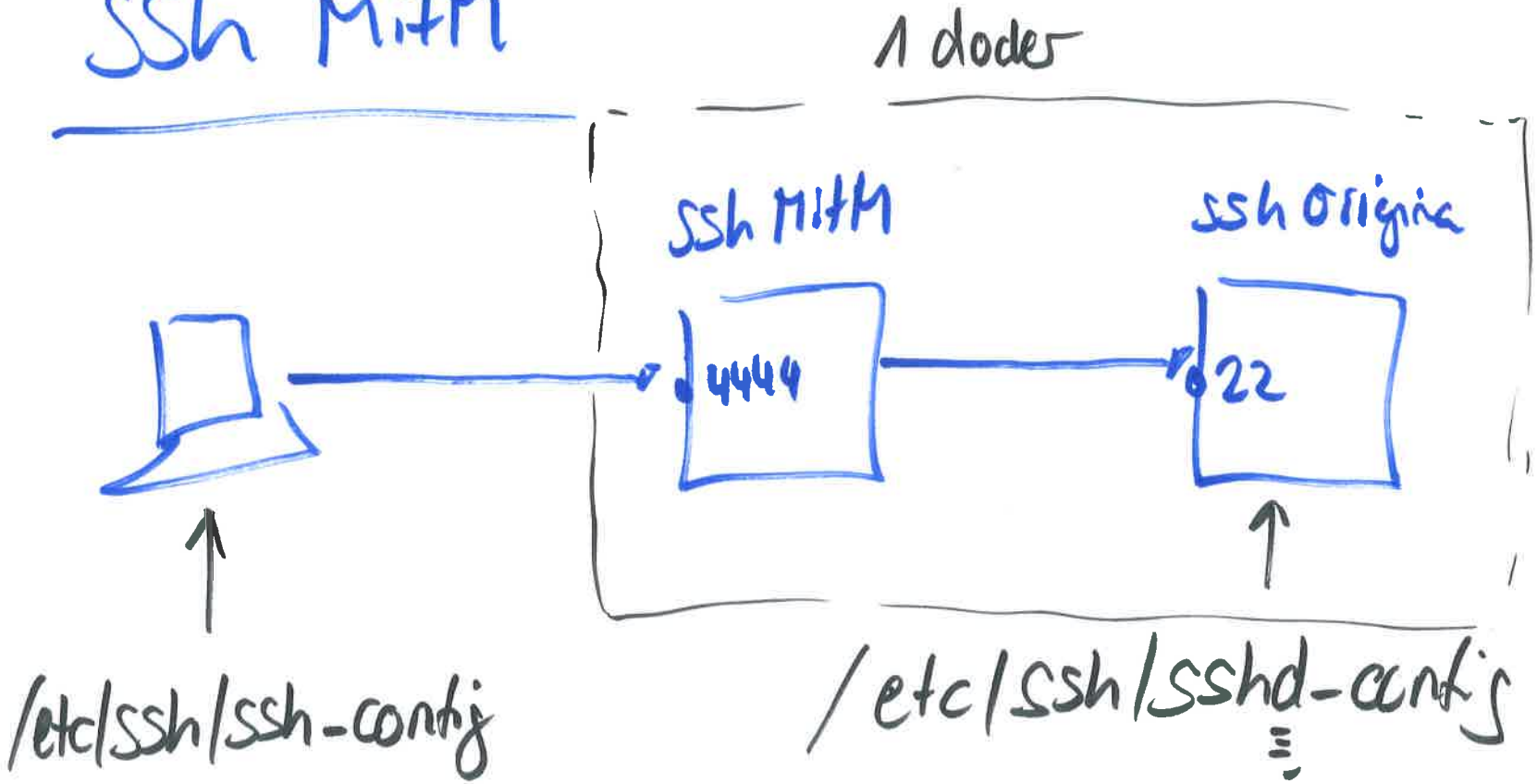


MitM ohne NLA ⇒ Network level Authentication → möglich!

MitM mit NLA → nicht möglich (Default)

NLA (Network Layer Authentication) schützt vor RDP Man in the Middle. Erklärung als Vorbereitung der Übung im HL.

SSH MitM



PasswordAuth deaktivieren

~/home/.ssh/config → Default *
→ HostEintrag

sshd_config = SSHD Daemon Konfig
ssh_config = SSH Client Config

Man kann im Client konfigurieren, keine UN/PW Verbindungen aufzubauen. Schützt davor, dass ein SSH MitM Server danach fragt.