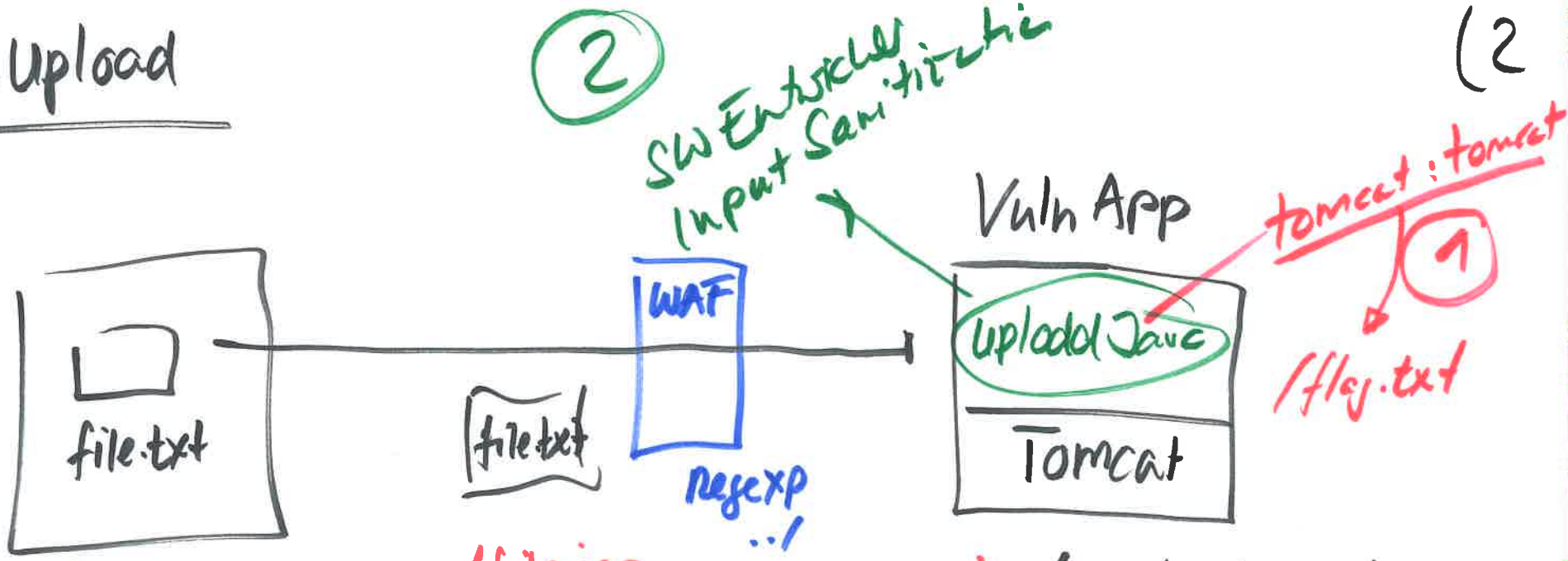
Cyber Defense

2.10.2024

Heute ist das Thema DNS Tunneling, Proxy Requests und Metasploit

PLUpload



Alte Attacke IIS

%255c..%255c../winnt/system32/cmd.exe

↓

../../../winnt/system32/cmd.exe

%25 = Hex Zeichen = %

↓

%5c = Hex Zeichen = \

1 Gegenmassnahe Hardening System-Technik

/~~var/upload.class~~

/bla.class

/upload/...

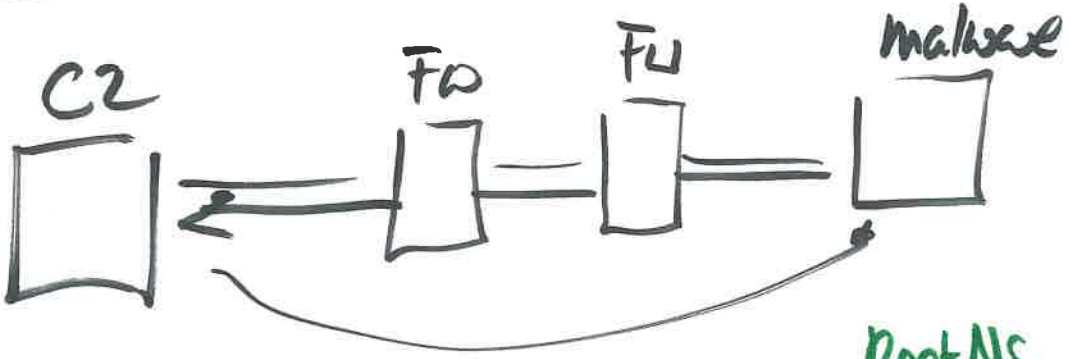
file.txt

nur Leserechte!

Read/Write! nötig

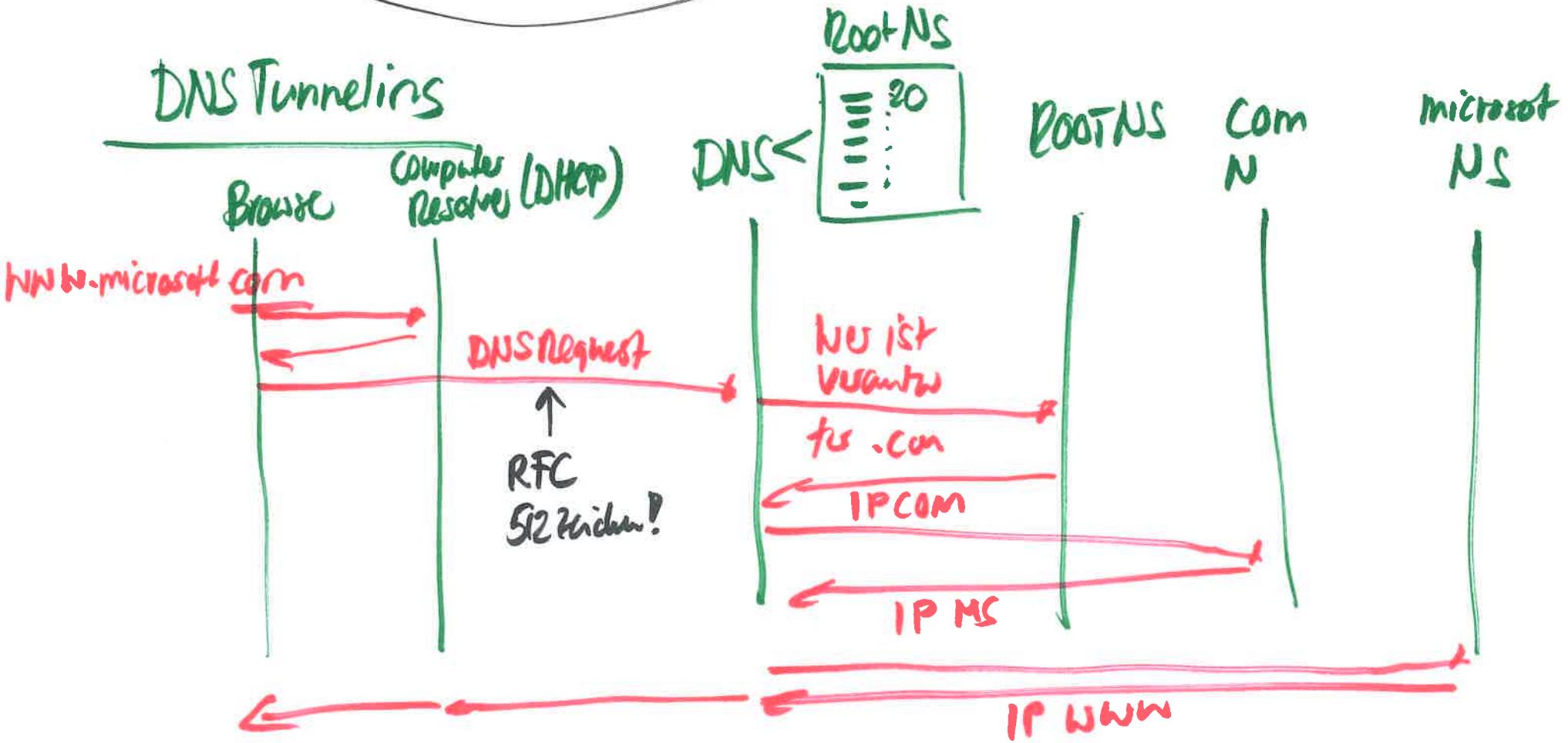
Auflösung Fragen PLUpload Challenge

Paradigma C2 / C&C / CovertChanel



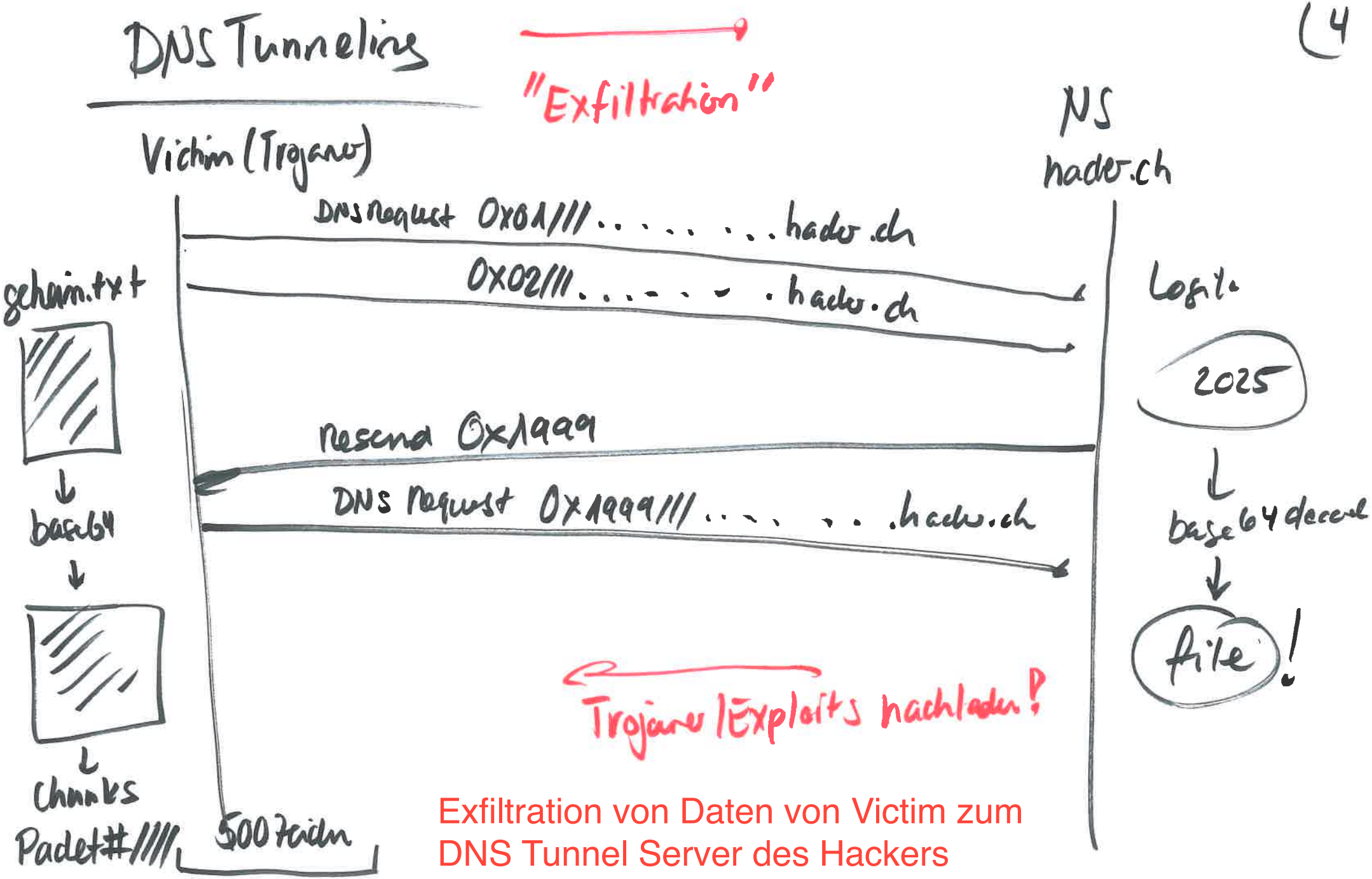
DNS Auflösung mit Root Nameserver für Erklärung von DNS Tunneling nötig

DNS Tunneling



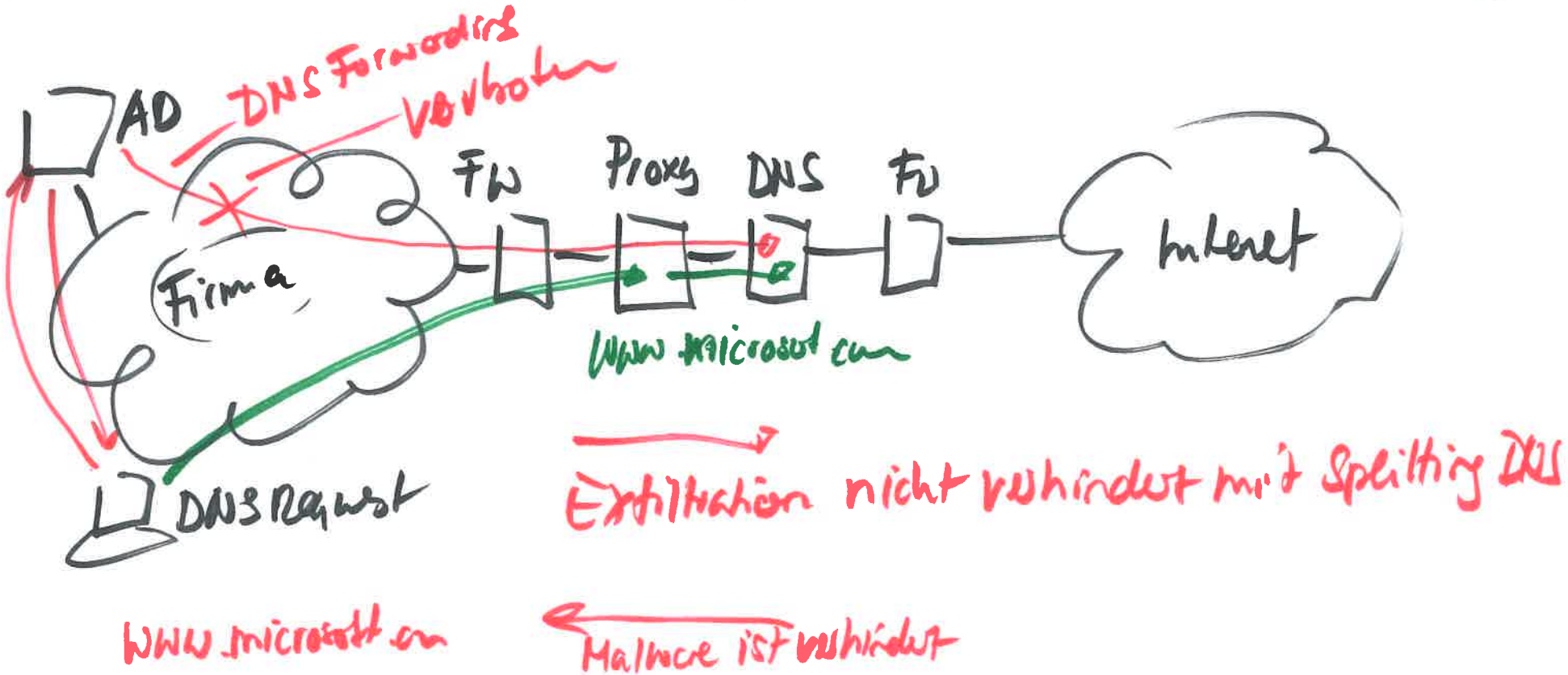
DNS Tunneling

"Exfiltration"



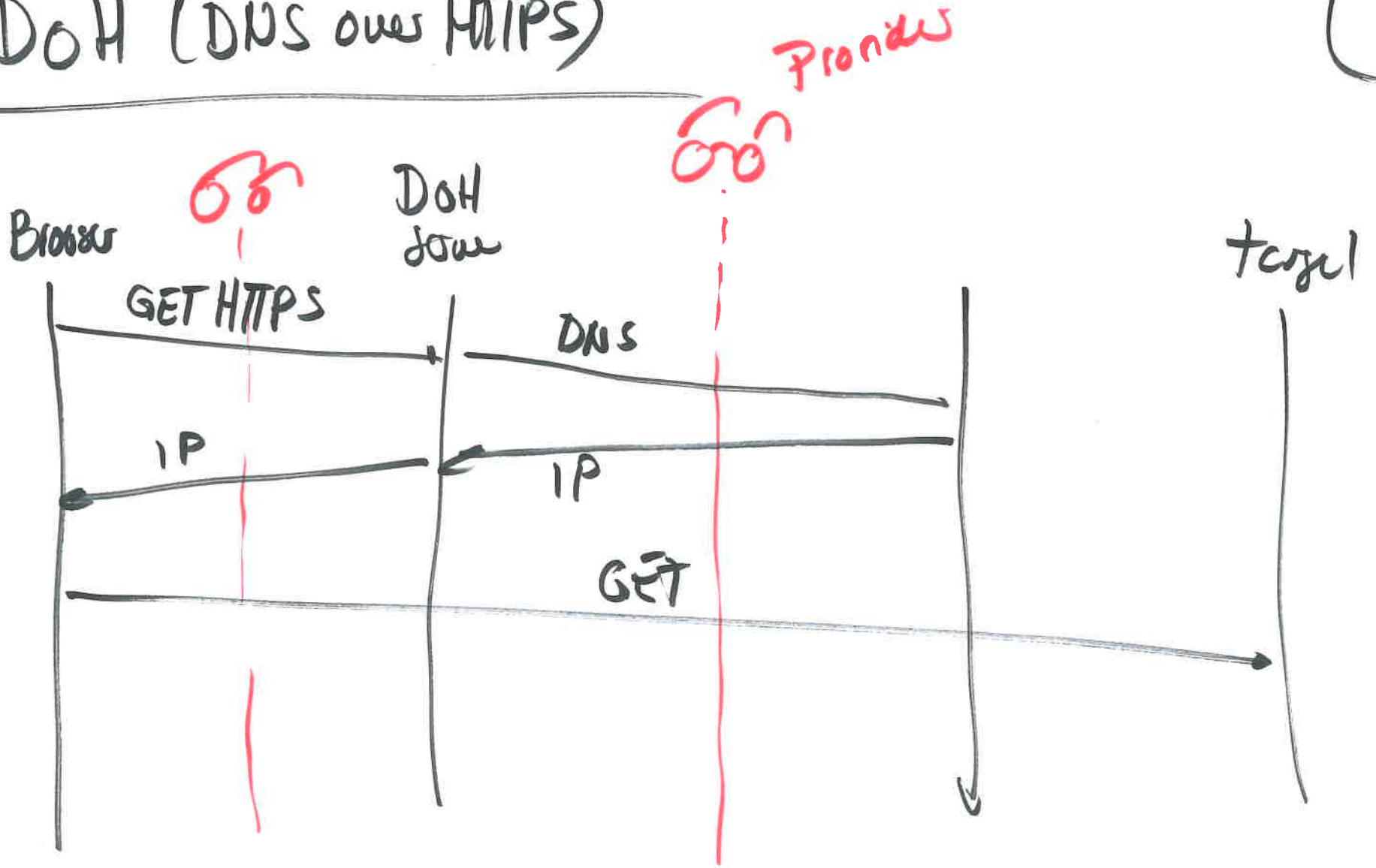
Exfiltration von Daten von Victim zum
DNS Tunnel Server des Hackers
Viele hundert DNS Requests sind nötig

Splitted DNS Zone (Solution)



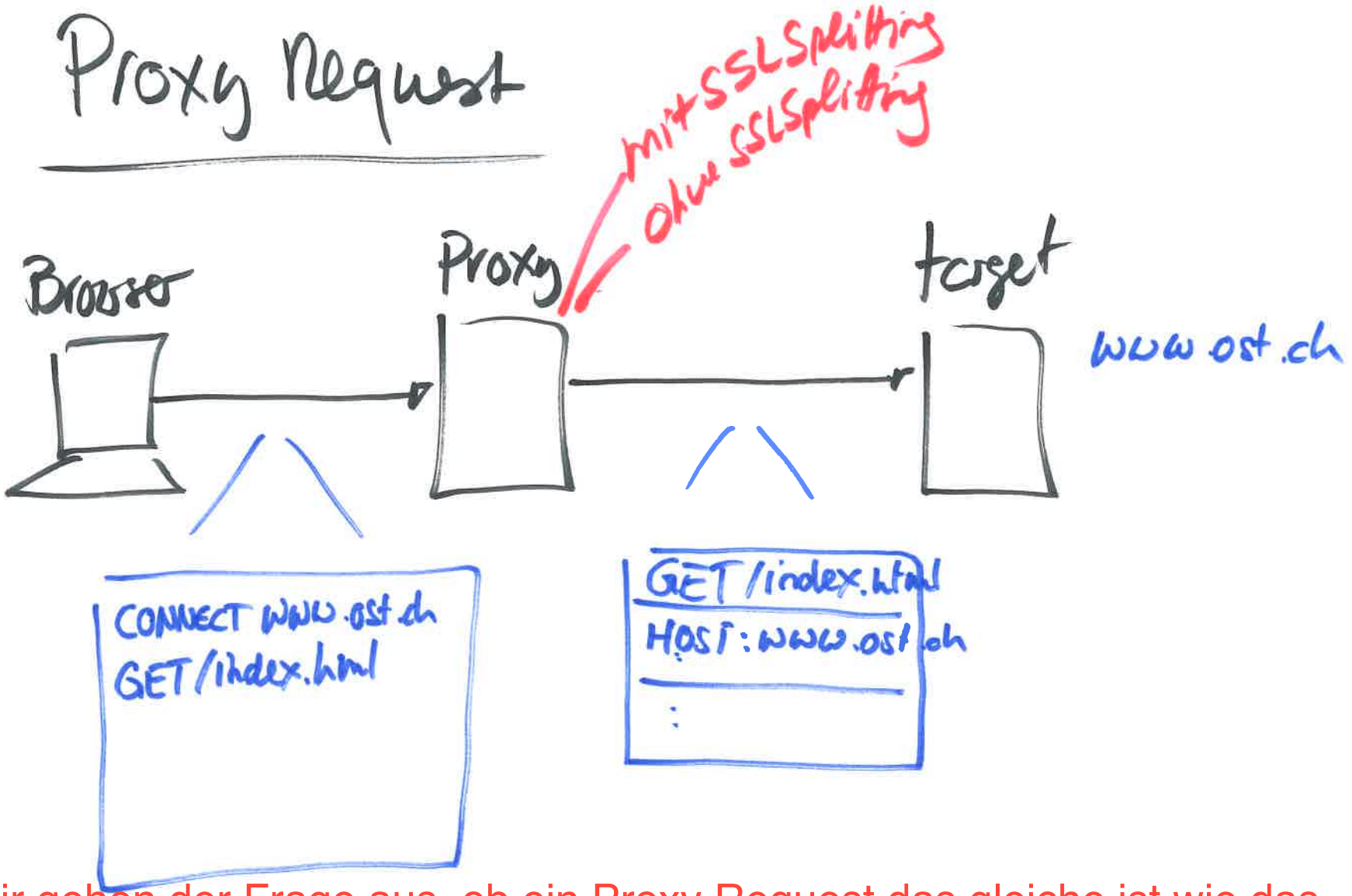
Einige Firmen erlauben ihren Clients nicht, FQDN Auflösung direkt ab dem Client ins Internet. Splitted DNS nennt sich das. Aber auch hier ist eine Exfiltration allenfalls über Web Requests und DNS möglich

DoH (DNS over HTTPS)



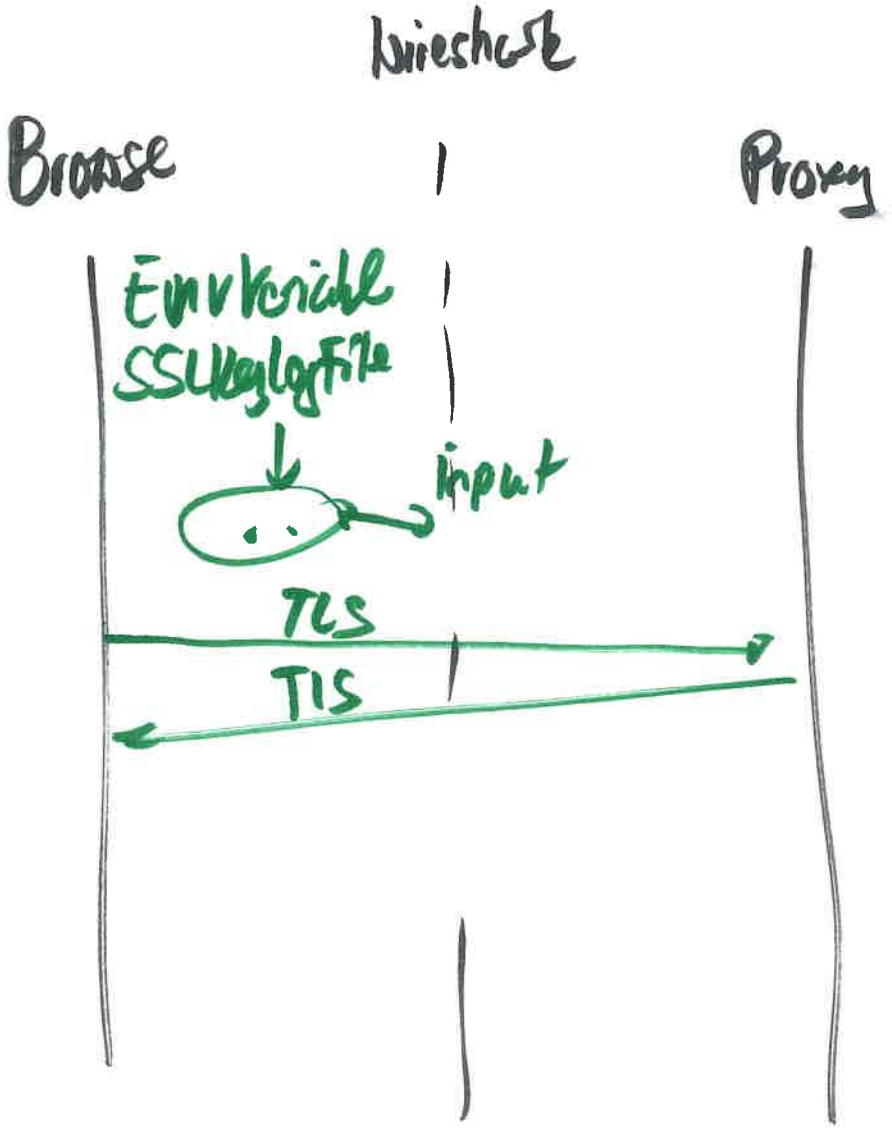
Splitted DNS ist eh ein wenig obsolet seit der Einführung von DoH
DNS over HTTP. Siehe auch https://en.wikipedia.org/wiki/DNS_over_HTTPS

Proxy Request



Wir gehen der Frage aus, ob ein Proxy Request das gleiche ist wie das, was der Proxy dem Target Webserver schickt. Die Antwort ist NEIN, denn ein Proxy Request schaut anders aus. Wir diskutieren das Sniffing mit Wireshark zwischen Browser und Proxy mittels SSLKEYLOGFILE

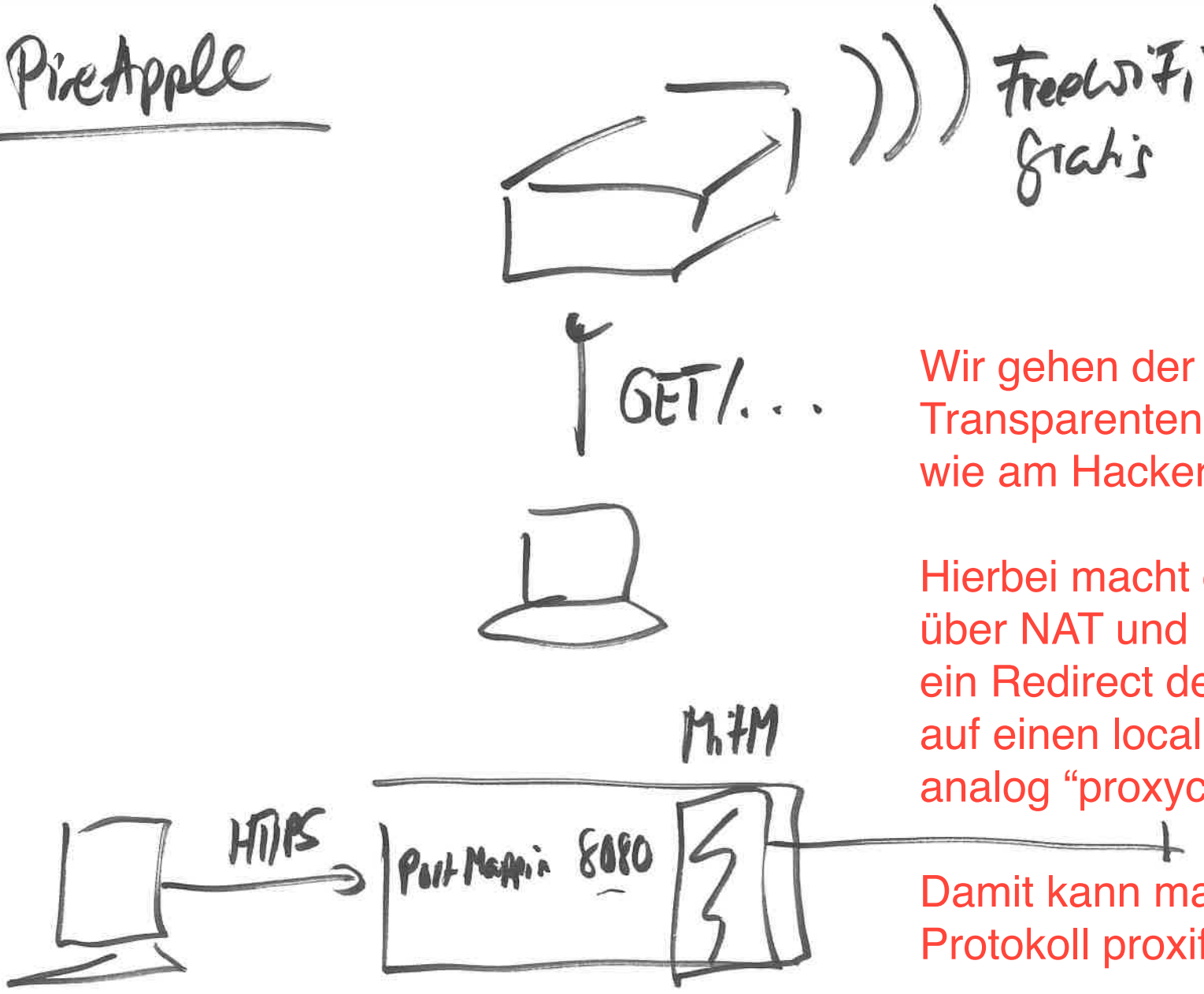
Lab in Optionaler Kachel im HL verfügbar für diejenigen, die wollen



Mit SSLKEYLOGFILE setzt man als User eine ENV Variable und dann werden die TLS Keys in ein File gespeichert

Dieses File kann man Wireshark angeben und dann kann Wireshark auch den TLS Traffic on the fly decrypten

PineApple



Wir gehen der Frage nach
Transparenten Proxies nach,
wie am Hacker Tool PineApple

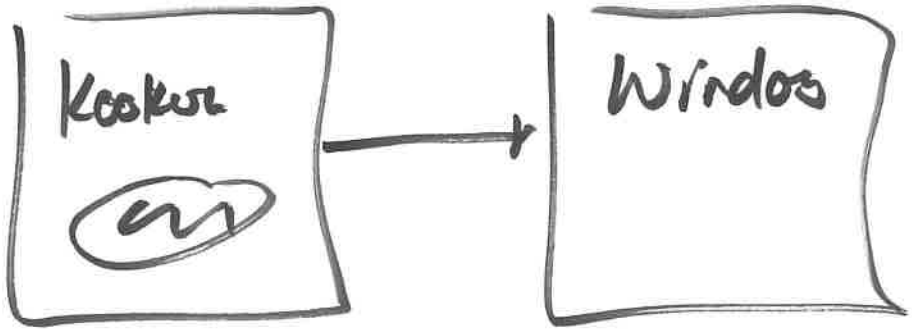
Hierbei macht das Gerät
über NAT und Port Forwarding
ein Redirect des Traffic
auf einen localhost service
analog “proxychain” Tool

Damit kann man jedes TCP
Protokoll proxifizieren

https://shop.hak5.org/products/wifi-pineapple

metasploit → payload (Malware)

msfvenom → AVP Bypass



Wir werden heute im Lab ein paar Metasploit Labs lösen. Hier geht es darum zu prüfen, ob Viren die mit Metasploit generiert sind, auf der Windows VM erkannt werden

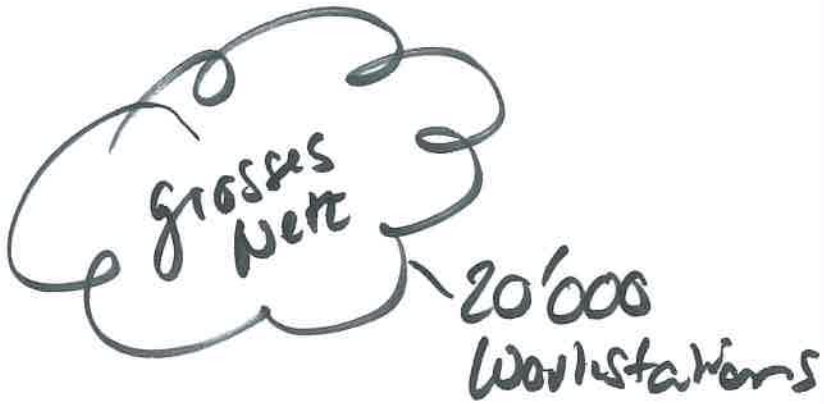
Tipp: vom Linux her über “python -m http.server” das Filesystem via Web Server dem Windows gegenüber öffnen, so dass man die Trojaner nicht über das HostOS kopieren muss (da würde die Anti Viren Software sicher blocken)

Hunting

Incident!

- Registry Key → Evidence
- Process
- File
- Device Drives

Indu!
Hunting



Wir gehen der Frage nach, was “Hunting” ist. Cyrill Brunschwiler wird in 2 Wochen die Vorlesung für Ivan halten und hierbei geht er dann mit Euch das Thema Hunting mit Velociraptor durch.

https://docs.velociraptor.app/docs/gui/hunting/