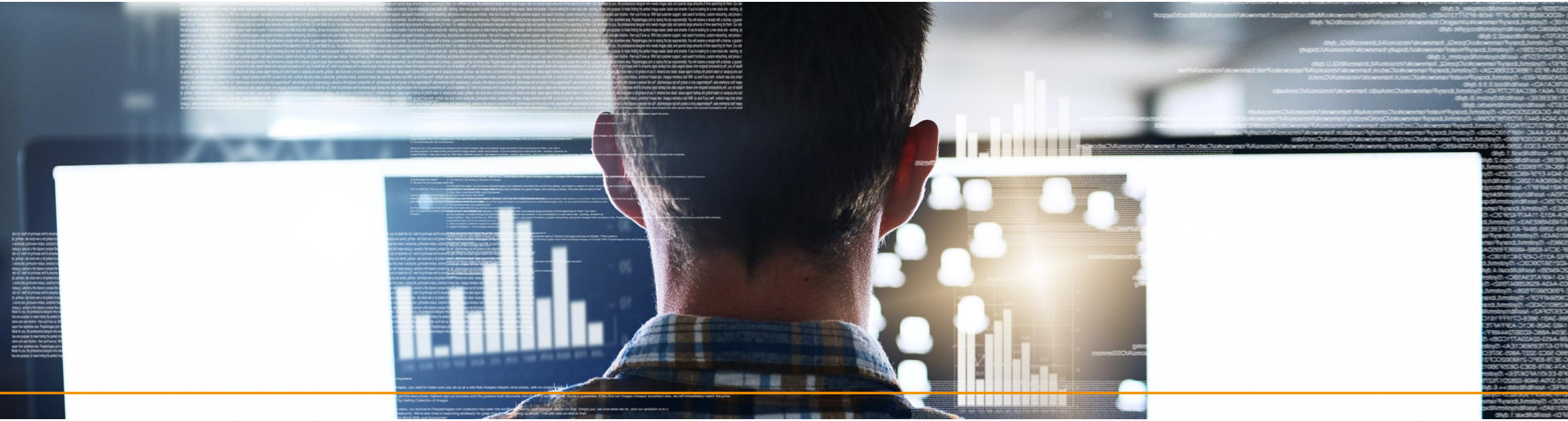


Passwort vergessen?

DNS-Schwachstellen in Webapplikationen

SEC Consult

an atos company

SEC Consult

an atos company

Timo Longin
Vienna, Austria
Security Consultant & Researcher
t.longin@sec-consult.com

Berlin | DE
Bochum | DE
München | DE
Nürnberg | DE

UAB Critical Security | LT

SEC Services | RU

Montreal | CA

Luxemburg | LX
Zürich | CH

Santa Cruz| US | HQ AMER

Wien | AT | HQ EMEA
St. Pölten | AT
Linz | AT
Wiener Neustadt | AT

Bangkok | TH
Kuala Lumpur | MY
Singapur | SG | HQ APAC

Hier bin ich!

- SEC Consult Niederlassungen
- SEC Consult Kunden
- SEC Consult Partner

8 Länder | 3 Kontinente

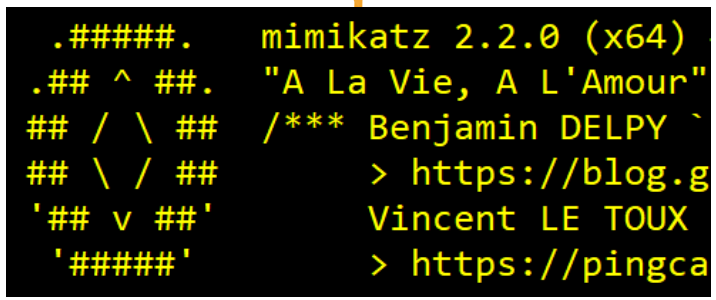
Übersicht

1. Es war einmal…
2. DNS-Schwachstellen in Webapplikationen?
3. DNS-Schwachstellen und wie diese zu finden sind
4. DNS-Schwachstellen!
5. (Andere Angriffsvektoren)

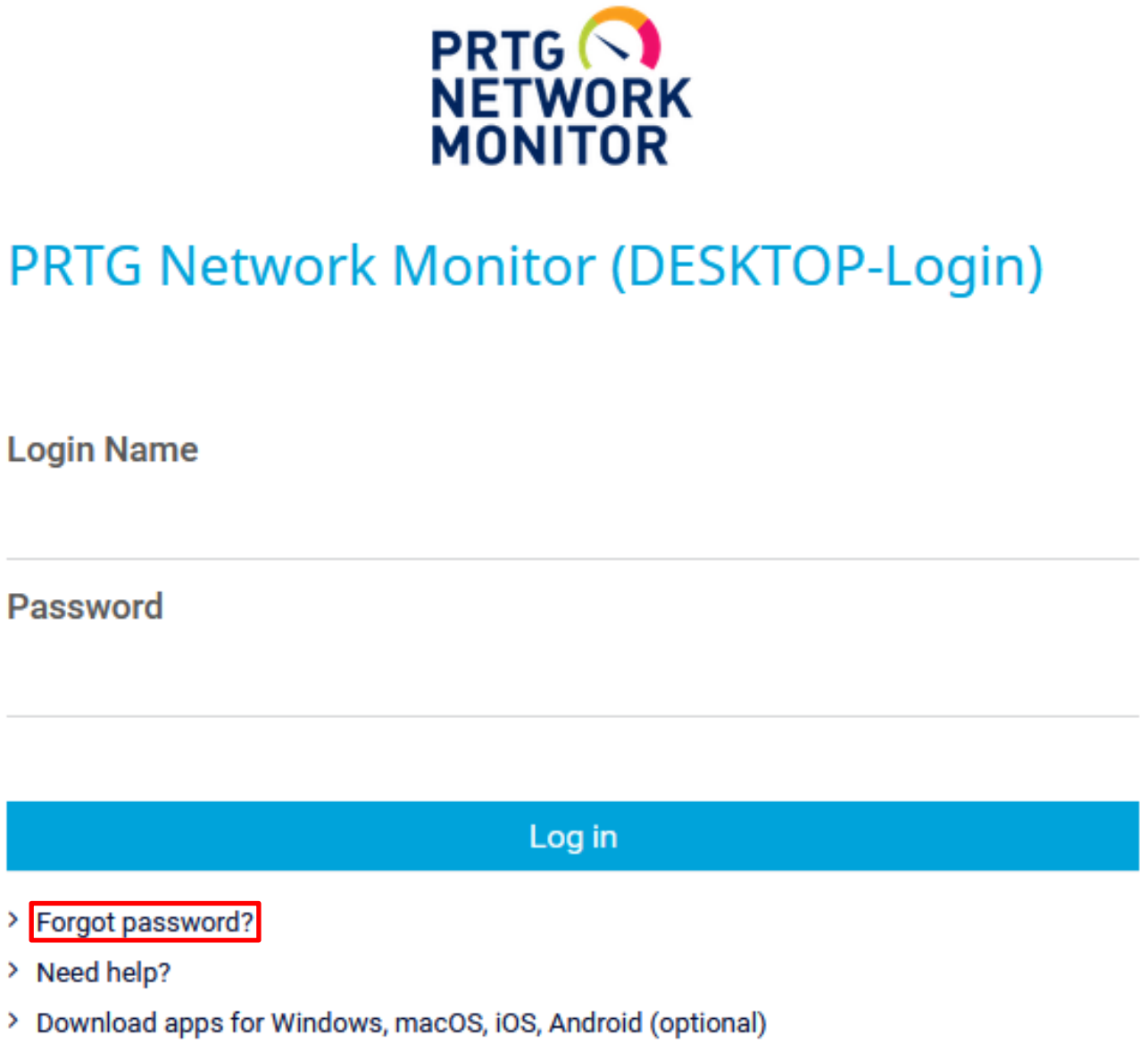
Es war einmal… – Exploit-Chain zum Domain Admin

PRTG NETWORK MONITOR

CVE-2018-9276

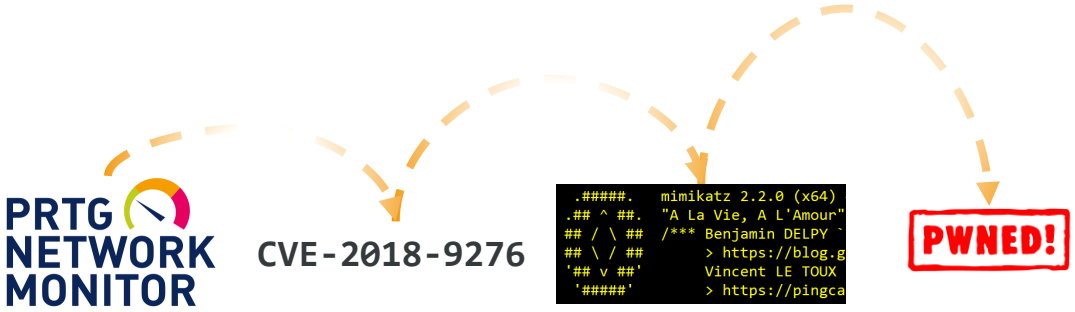


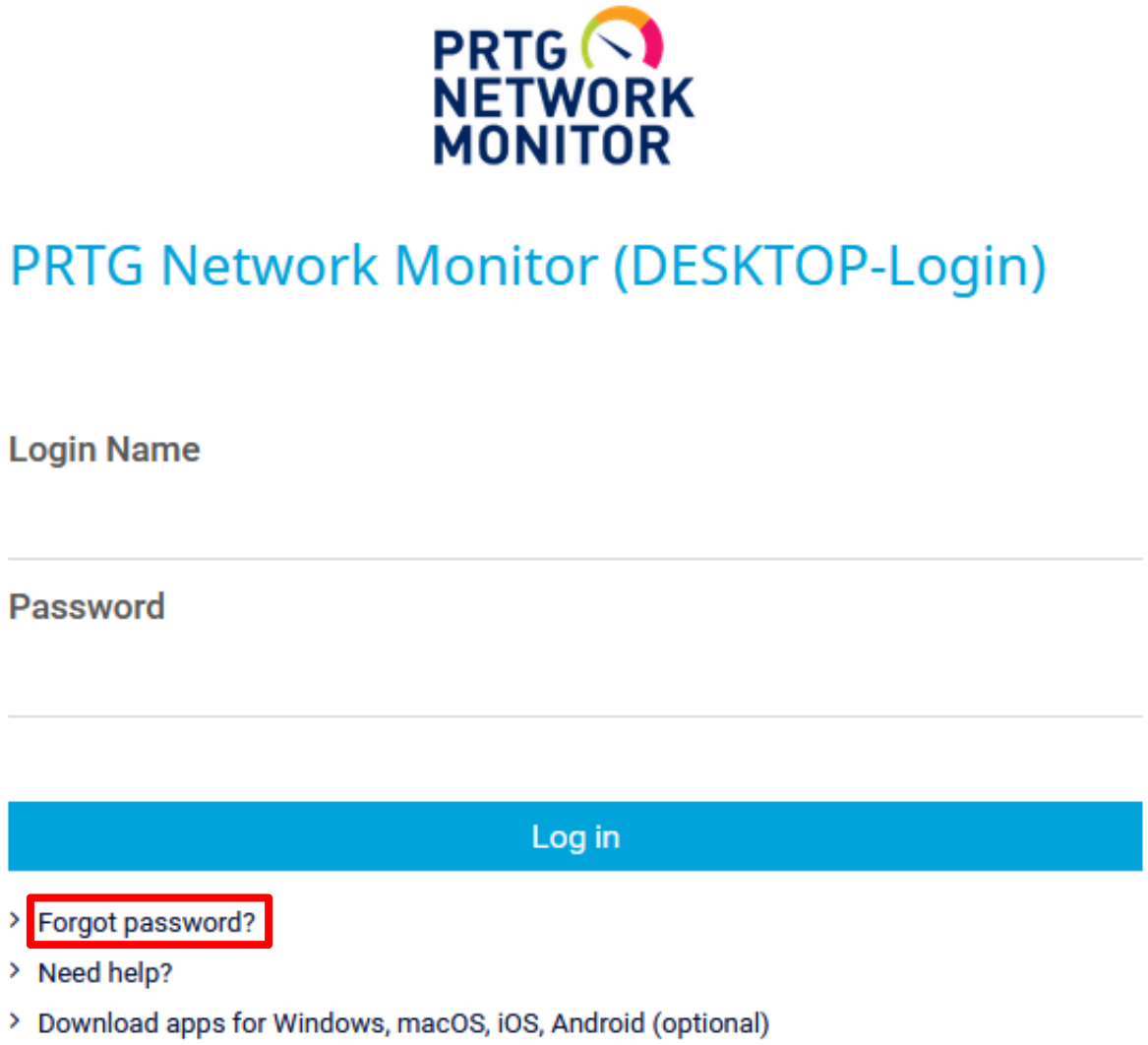
Es war einmal… – Passwort vergessen?



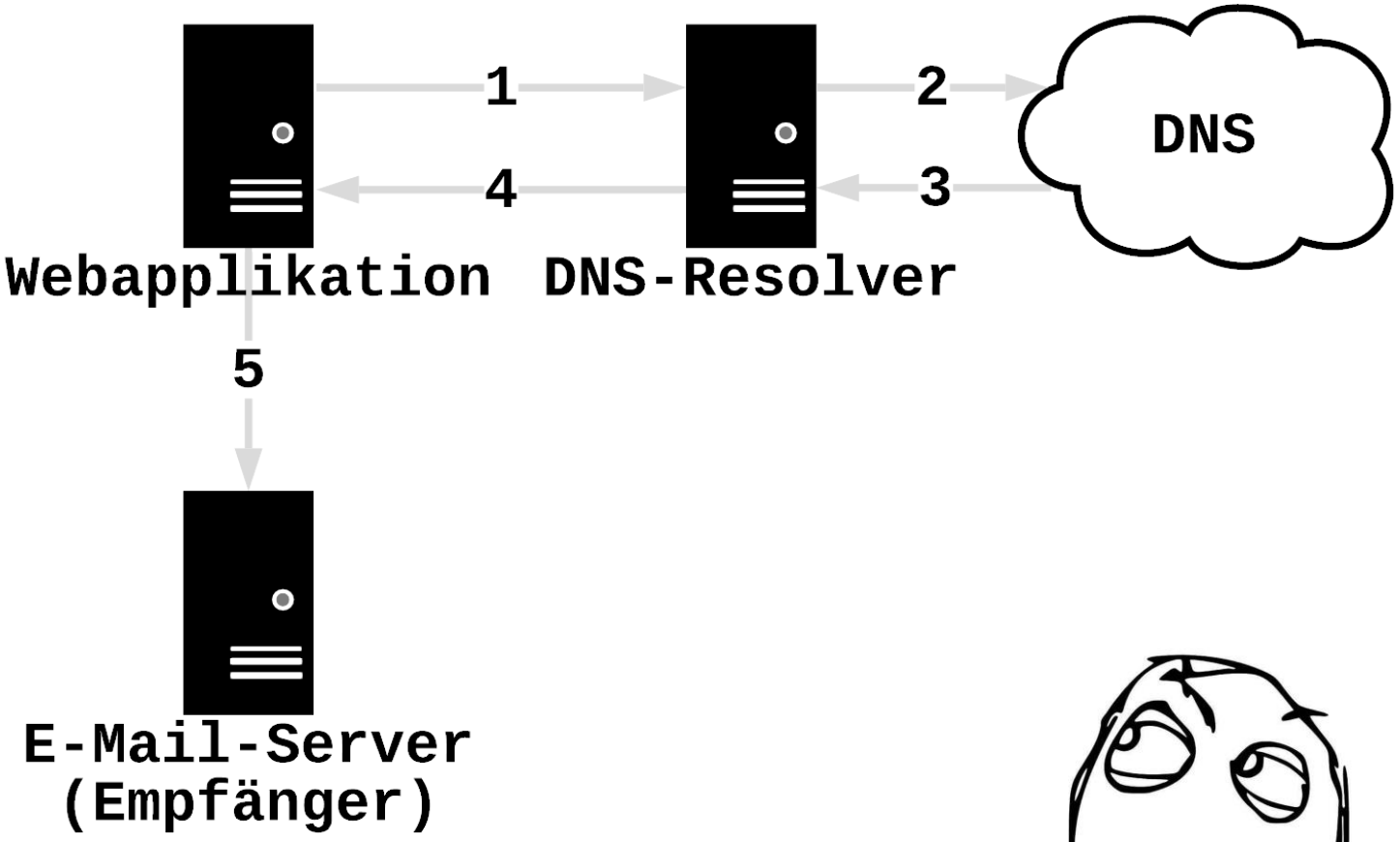
Es war einmal… – Exploit-Chain zum Domain Admin

- ARP-Spoofing
- Passwort vergessen
- Rücksetzungs-URL erhalten
- Admin-Passwort zurücksetzen
- CVE-2018-9276 – RCE
- NTLM-Hash von Domain Admin auslesen
- ???
- **Profit**





DNS-Schwachstellen in Webapplikationen? – E-Mail-Versand



1. -> DNS-Resolver:
   ```
   gmail.com    IN MX
   ```

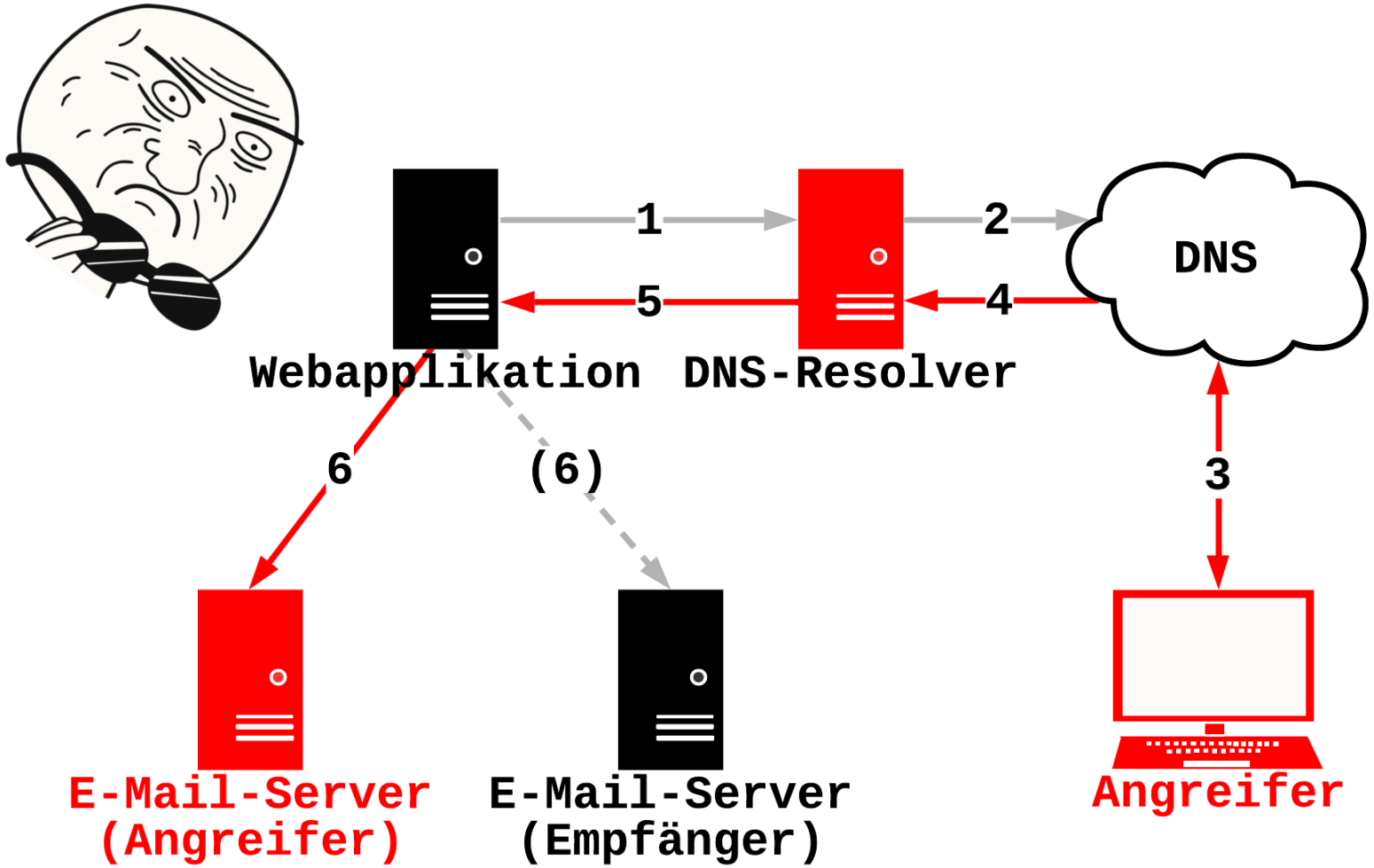
2. -> DNS:
   ```
   gmail.com    IN MX
   ```

3. -> DNS-Resolver (Cache):
   ```
   gmail.com    IN MX mx.gmail.com
   mx.gmail.com IN A  1.2.3.4
   ```

4. -> Webapplikation:
   ```
   gmail.com    IN MX mx.gmail.com
   mx.gmail.com IN A  1.2.3.4
   ```

5. E-Mail an 1.2.3.4

DNS-Schwachstellen in Webapplikationen? – E-Mail-Versand + Angreifer



1. -> DNS-Resolver:
   gmail.com IN MX

2. -> DNS:
   gmail.com IN MX

3. -> DNS:
   gmail.com IN MX mx.bad.com
   mx.bad.com IN A 13.33.33.37

4. -> DNS-Resolver (Cache):
   gmail.com IN MX mx.bad.com
   mx.bad.com IN A 13.33.33.37

5. -> Webapplikation:
   gmail.com IN MX mx.bad.com
   mx.bad.com IN A 13.33.33.37

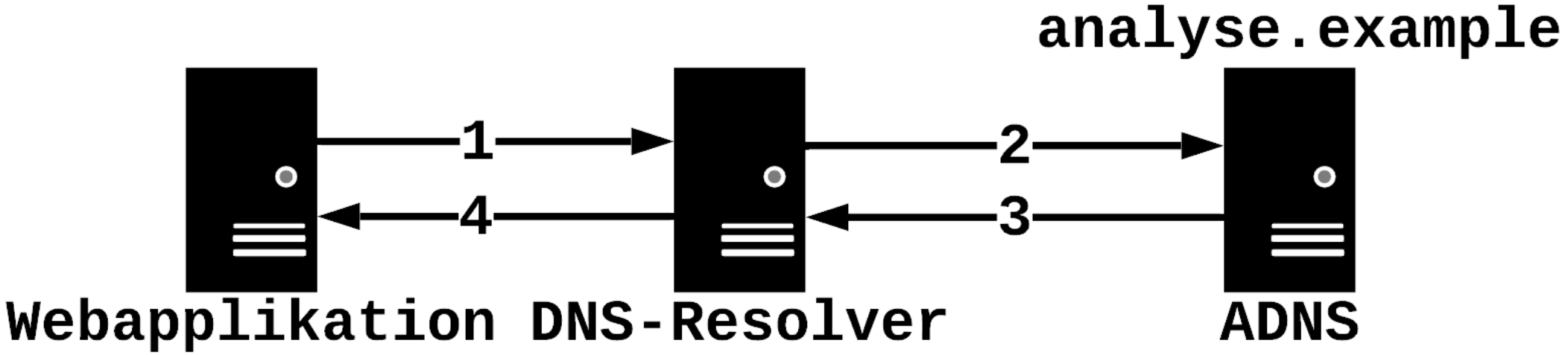
6. E-Mail an 13.33.33.37

DNS-Schwachstellen in Webapplikationen? – Dan Kaminsky

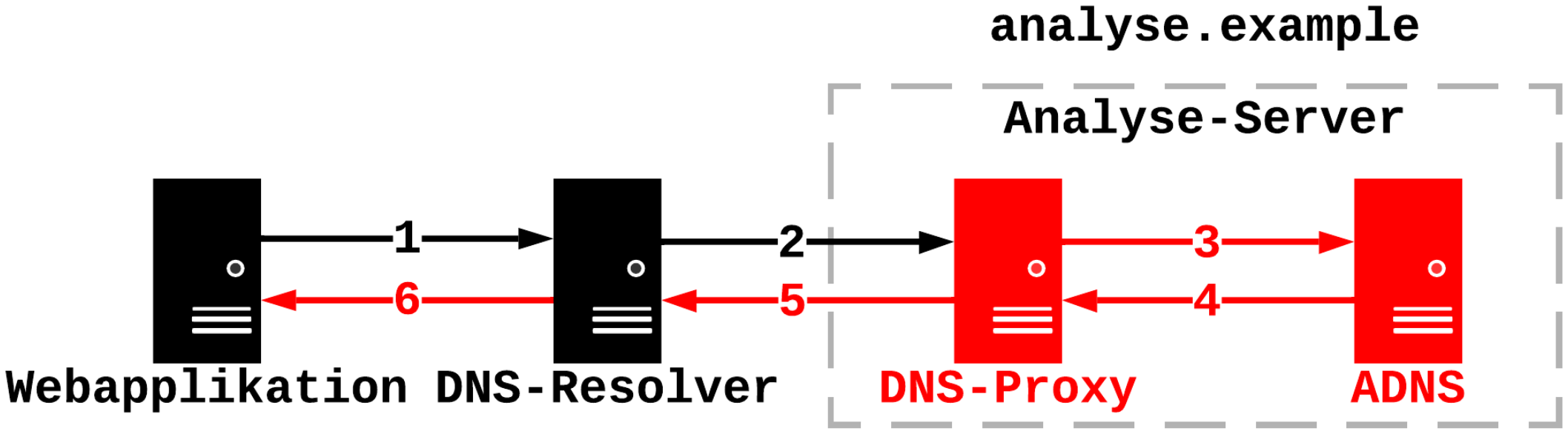
Dan Kaminsky:

- Black Ops 2008: It's The End Of The Cache As We Know It
- Kaminsky-Angriff

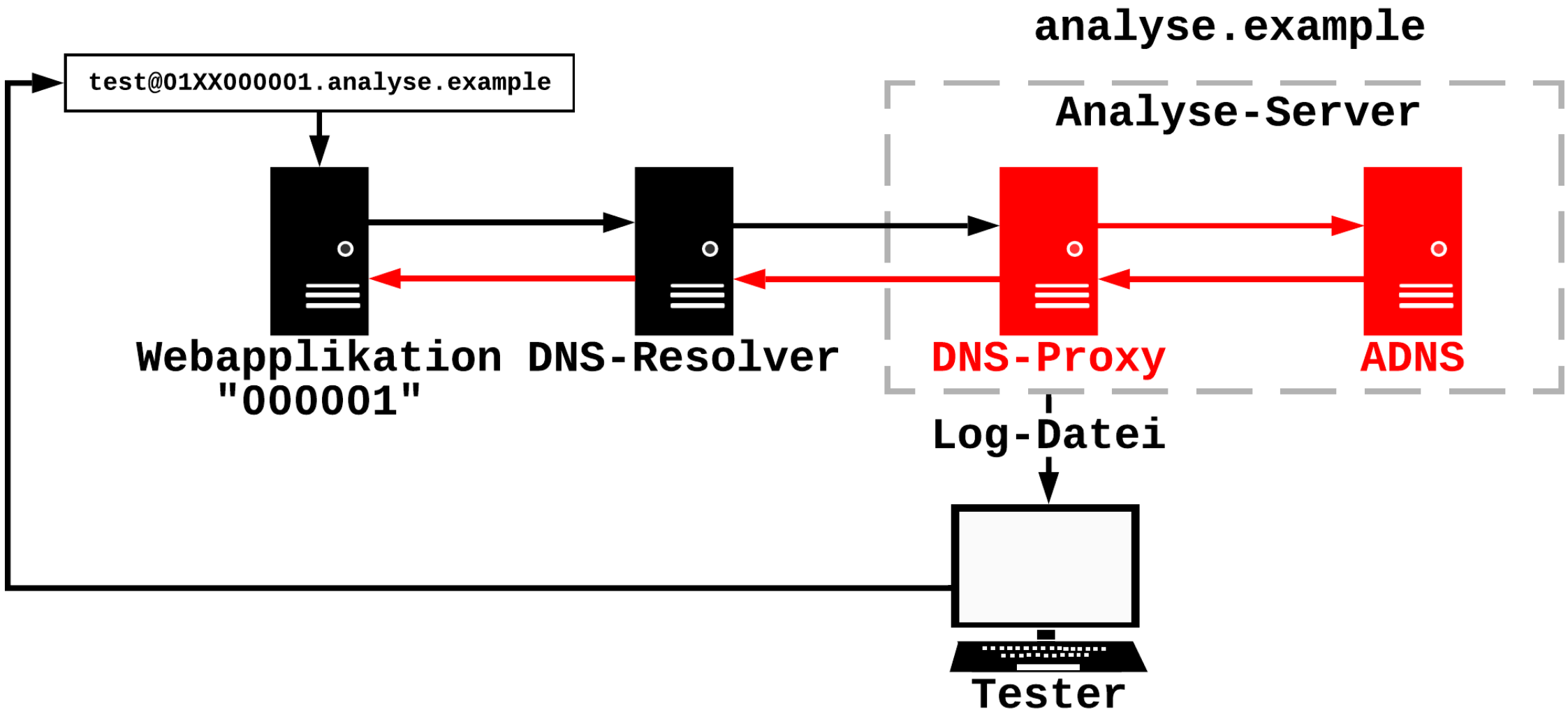
DNS-Schwachstellen und wie diese zu finden sind – Analyse-Server



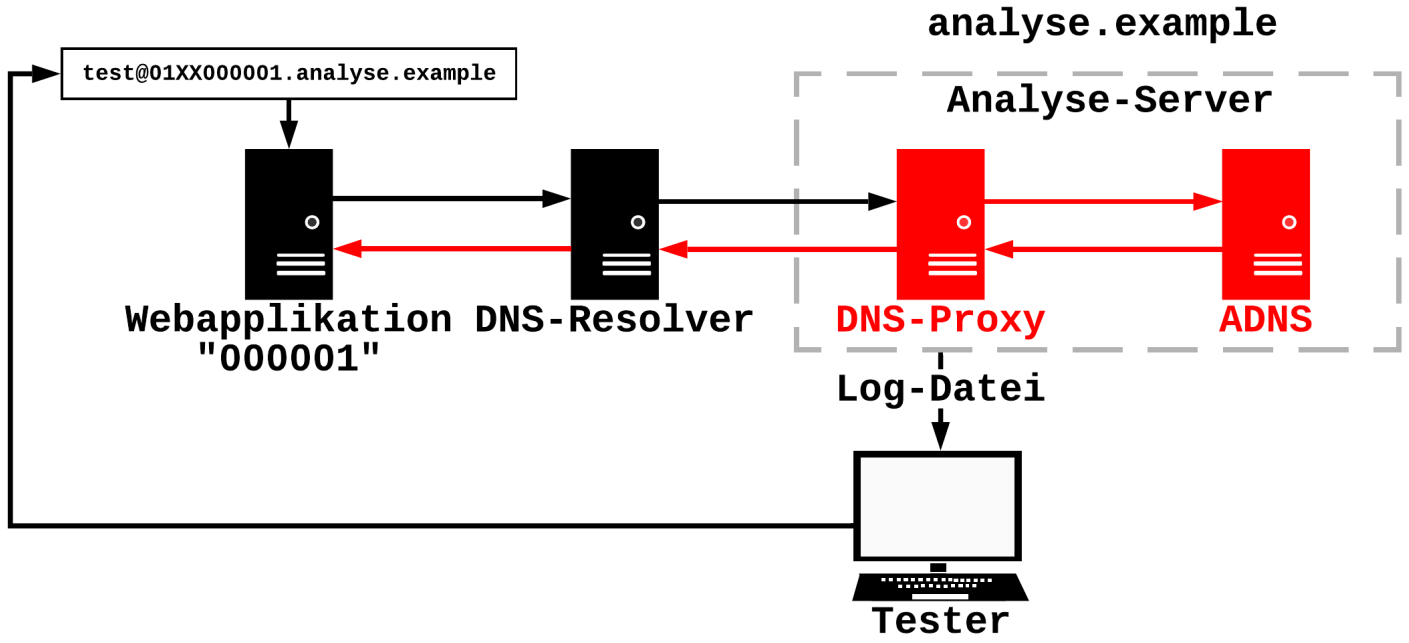
DNS-Schwachstellen und wie diese zu finden sind – Analyse-Server



DNS-Schwachstellen und wie diese zu finden sind – Testablauf



DNS-Schwachstellen und wie diese zu finden sind – Angriffsvoraussetzungen



Aktiv:

- IP-Fragmentierung
- Bailiwick-Tests
- Query-Loops
- …

Passiv:

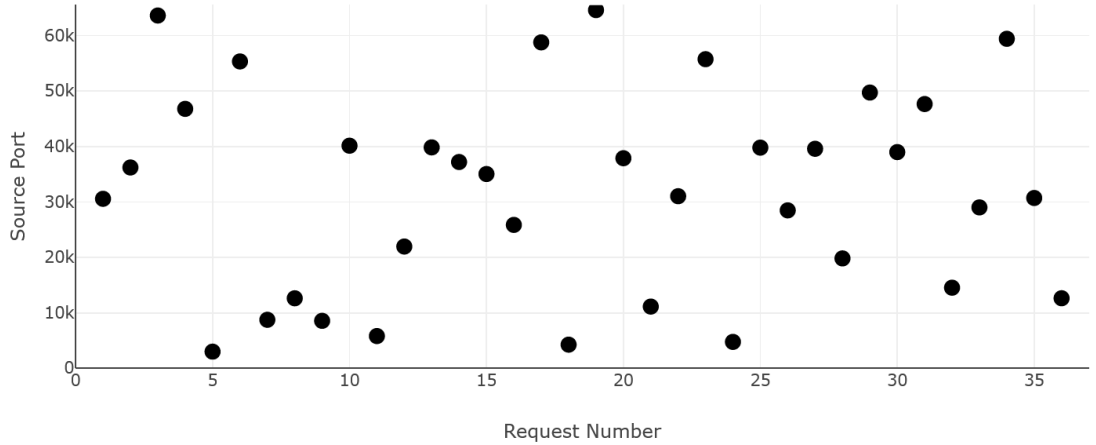
- UDP-Source-Ports
- DNSSEC
- DNS-Cookies
- EDNS-Max-Size
- 0x20-Enkodierung
- TCP
- Verwendete IP-Adressen
- …

DNS-Schwachstellen und wie diese zu finden sind – DNS Reset Checker

DNS-Reset-Checker

Tools to assess the DNS security of web applications

HTML 98 15

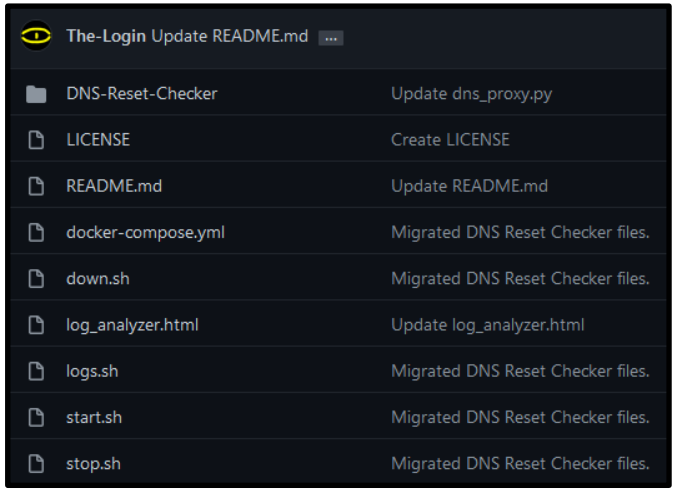


https://github.com/The-Login/DNS-Reset-Checker

Analysis of domain identifier: 001337

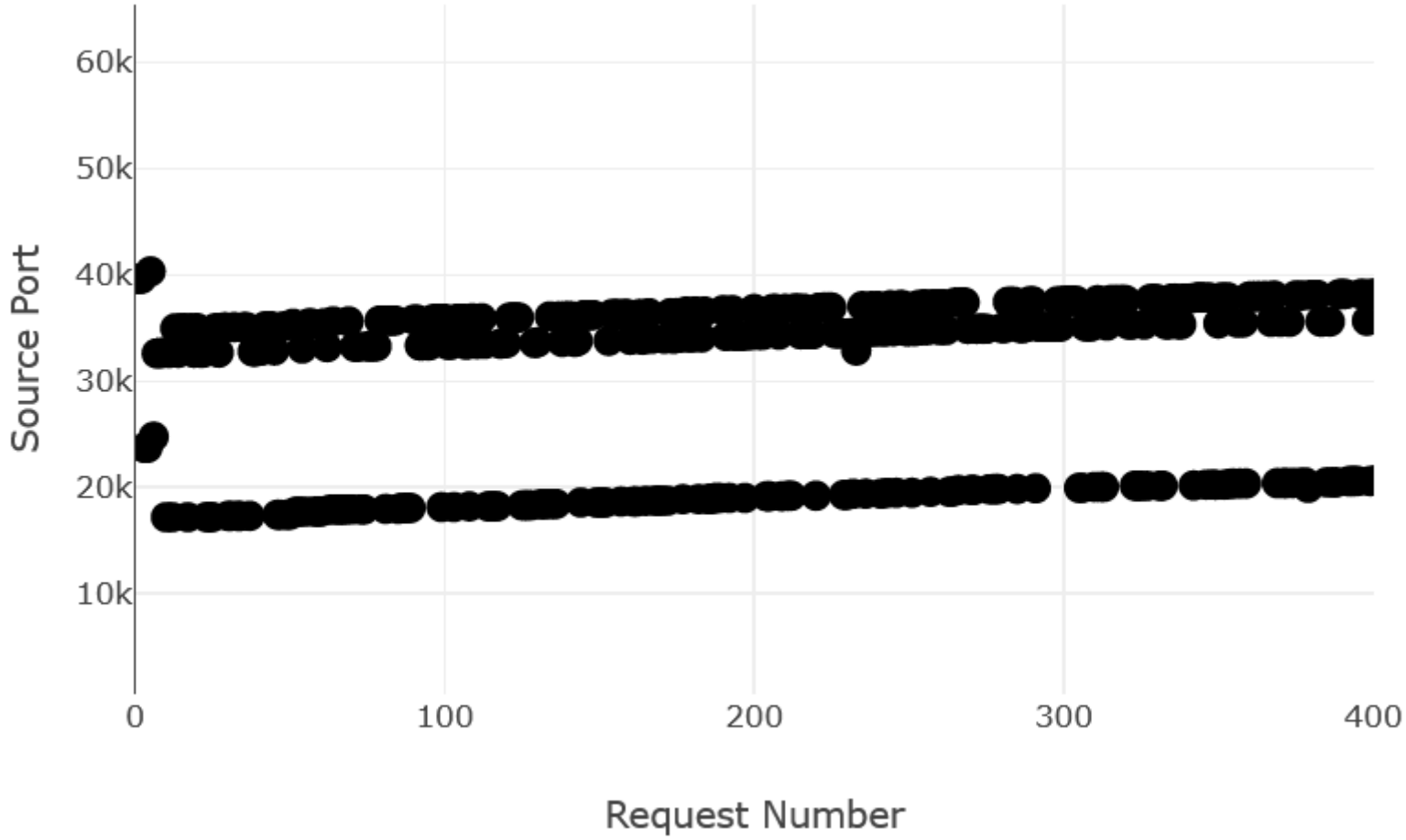
General Info

- **Number of DNS resolver IPs:** 3
- **Public DNS resolvers:** Outgoing IP addresses of big public DNS resolvers: 0 / 3
- **Number of queries received:** 62
- **Active methods probed:** ip_fragmentation, edns_removal
- **EDNS maximum size:** Not all DNS requests specified a response size.
- **DNS cookies:** At least one DNS query did not include a DNS cookie.
- **DNSSEC:** At least one DNS query did not require DNSSEC.
- **Removal of EDNS (OPT):** A response with a missing EDNS record was returned by the server and accepted by the resolver.
- **IP fragmentation:** An IP fragmented response was returned by the server but denied by the resolver.
- **0x20 Encoding:** At least one DNS query did not use 0x20 encoding.

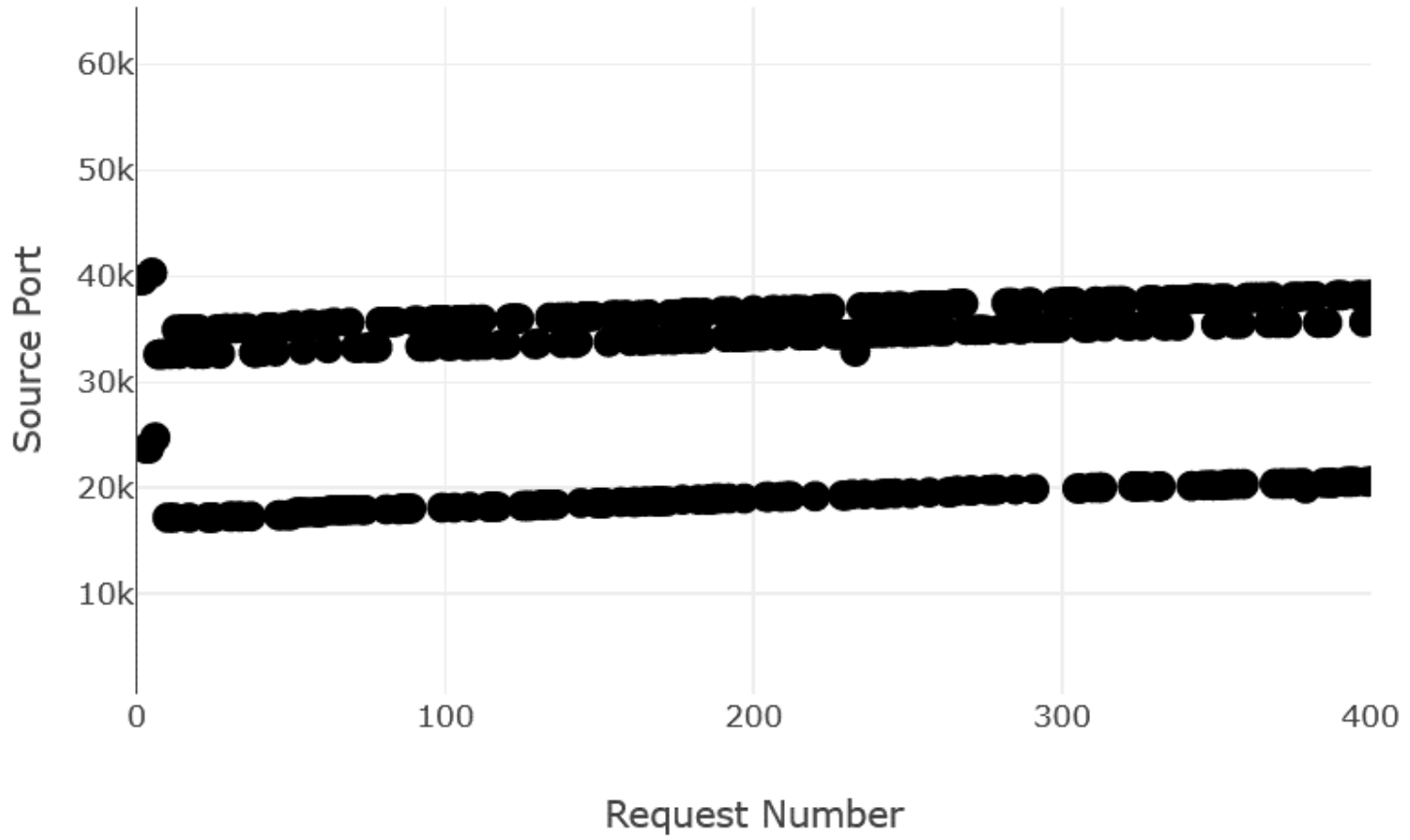


DNS-Schwachstellen und wie diese zu finden sind – Jetzt registrieren!

DNS-Schwachstellen! – Inkrementelle Source-Ports

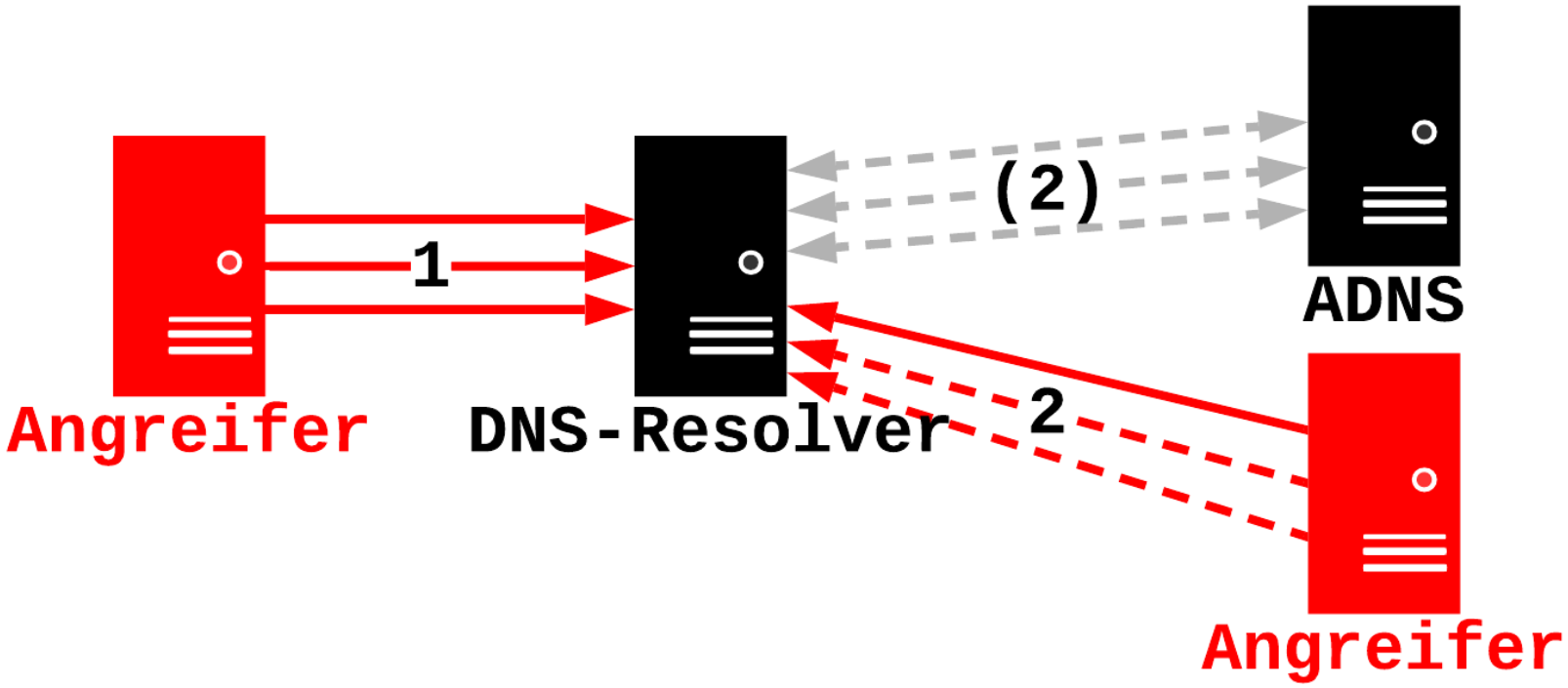


DNS-Schwachstellen! – Inkrementelle Source-Ports



- Erratbare Source-Ports
- Kaminsky-Angriff möglich

DNS-Schwachstellen! – Kaminsky-Angriff

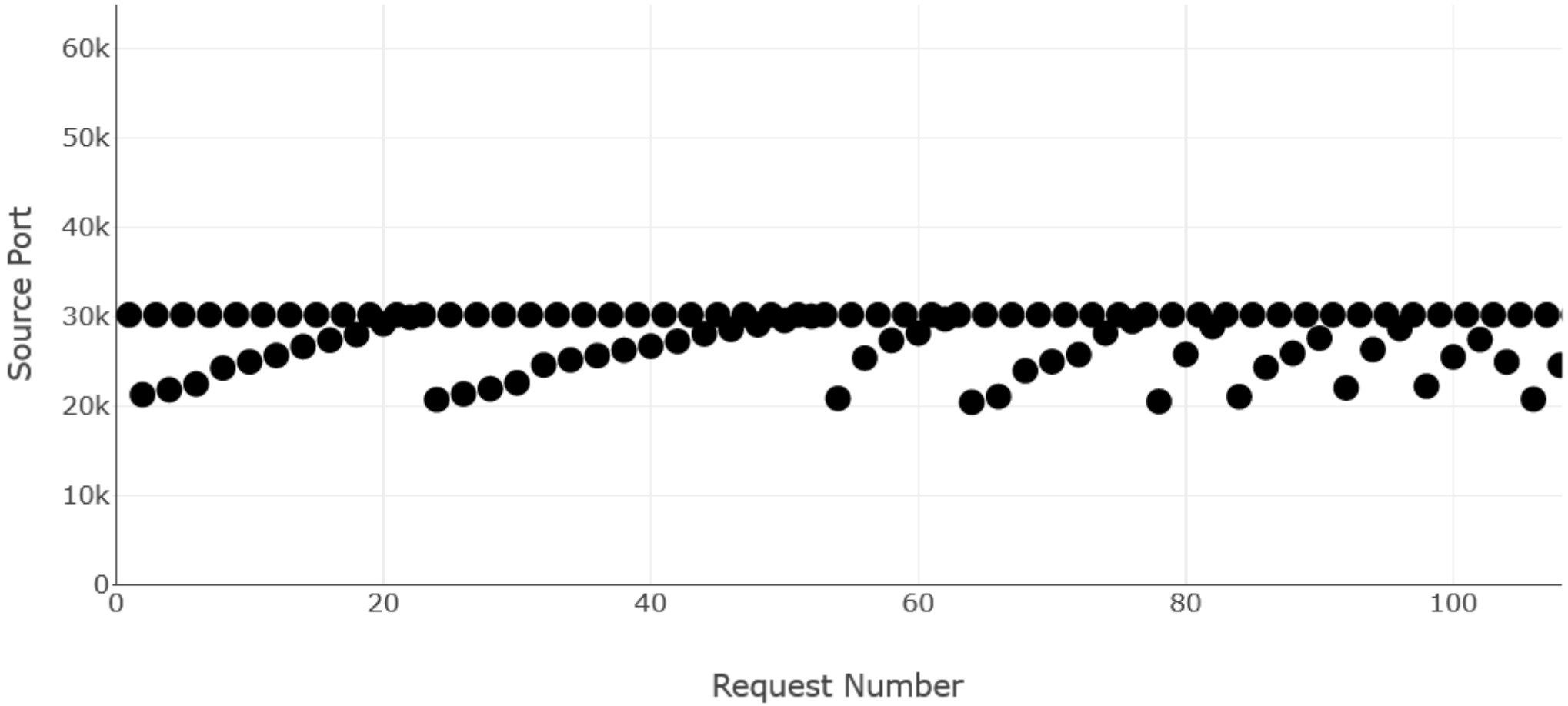


- 16 Bit Source-Port
- 16 Bit DNS-ID
- ~4,294 Mrd. Möglichkeiten

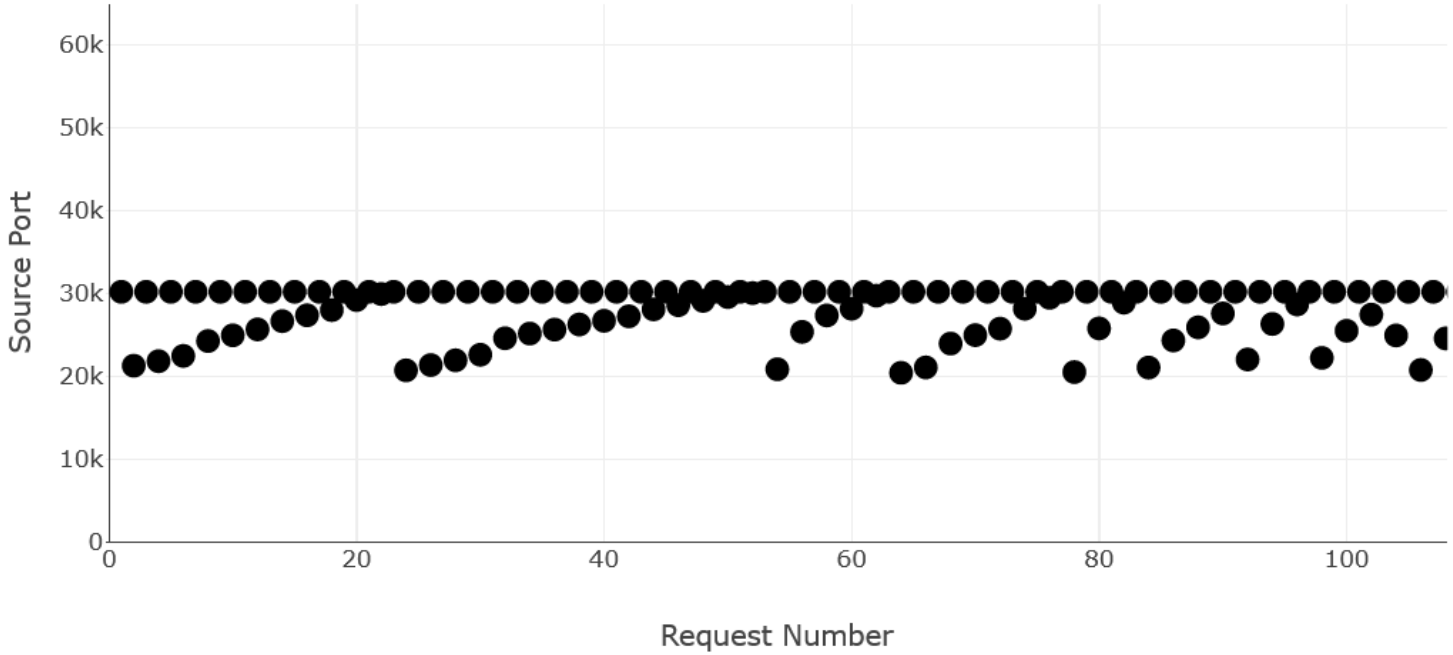
vs.

- 0 Bit Source-Port
- 16 Bit DNS-ID
- ~65000 Möglichkeiten

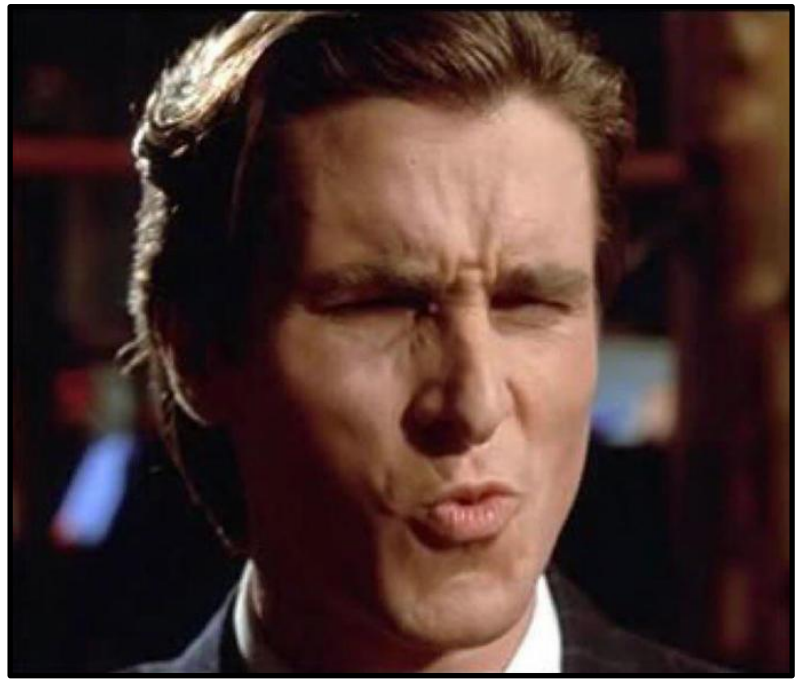
DNS-Schwachstellen! – Statische Source-Ports



DNS-Schwachstellen! – Statische Source-Ports



- Erratbare Source-Ports
- Kaminsky-Angriff möglich



DNS-Schwachstellen! – Ergebnisse

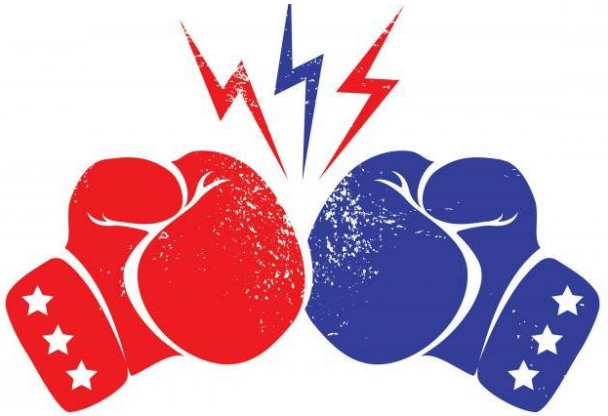
Kaminsky-Angriff: 2 von 146

IP-Fragmentierungs-Angriff: 62 von 146

DNS-Schwachstellen! – Finden und verhindern

Finden von DNS-Schwachstellen:

- DNS Reset Checker
- TBD: Burp Collaborator



Gegenmaßnahmen für DNS-Angriffe:

- DNSSEC und Best Practices
- Große DNS-Provider (Google, Cloudflare, Cisco, etc.)

Gegenmaßnahmen für erfolgreiche DNS-Angriffe:

- TLS (“No need for black chambers: Testing TLS in the e-mail ecosystem at large”)
- 2FA

Fragen?

Andere Angriffsvektoren

Alles was das DNS verwendet:

- “Passwort vergessen”-Funktion
- Domain Validation
- NTP
- Und vieles mehr!

Amit Klein

Markus Brandt

Tianxiang Dai

Domain Validation++ For MitM-Resilient PKI

Michael Waidner

Haya Shulman