Linux Am Dienstag

Podcast & Videostammtisch

TLS Attacke: ALPACA

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

„Per Bande zum Ziel“

Wie ein Angriff auf das Web unschuldige Dienste nötigt.

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

FireFox

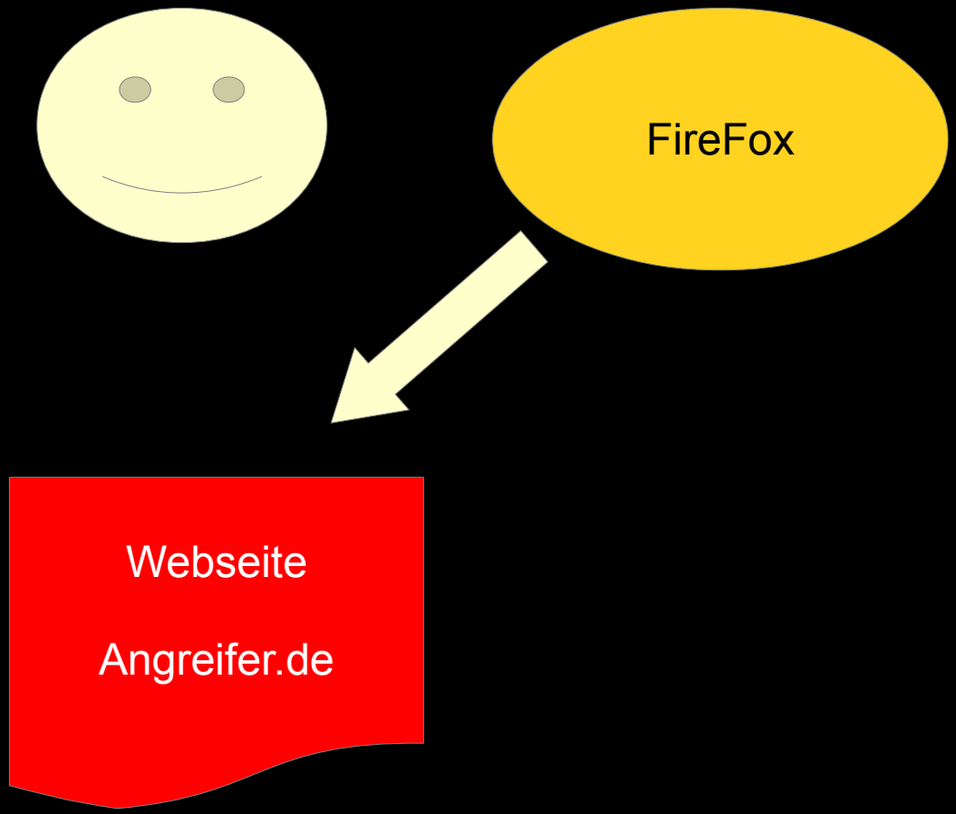
Webseite

Angreifer.de

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

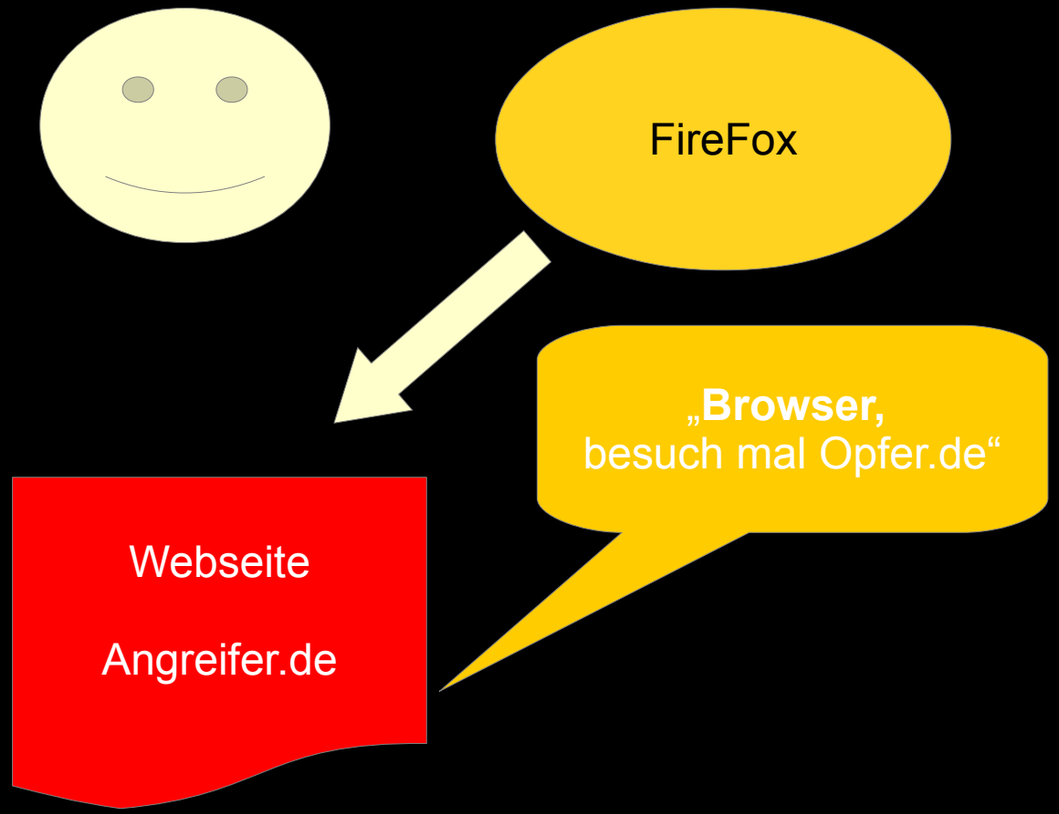
Podcast & Videostammtisch



© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

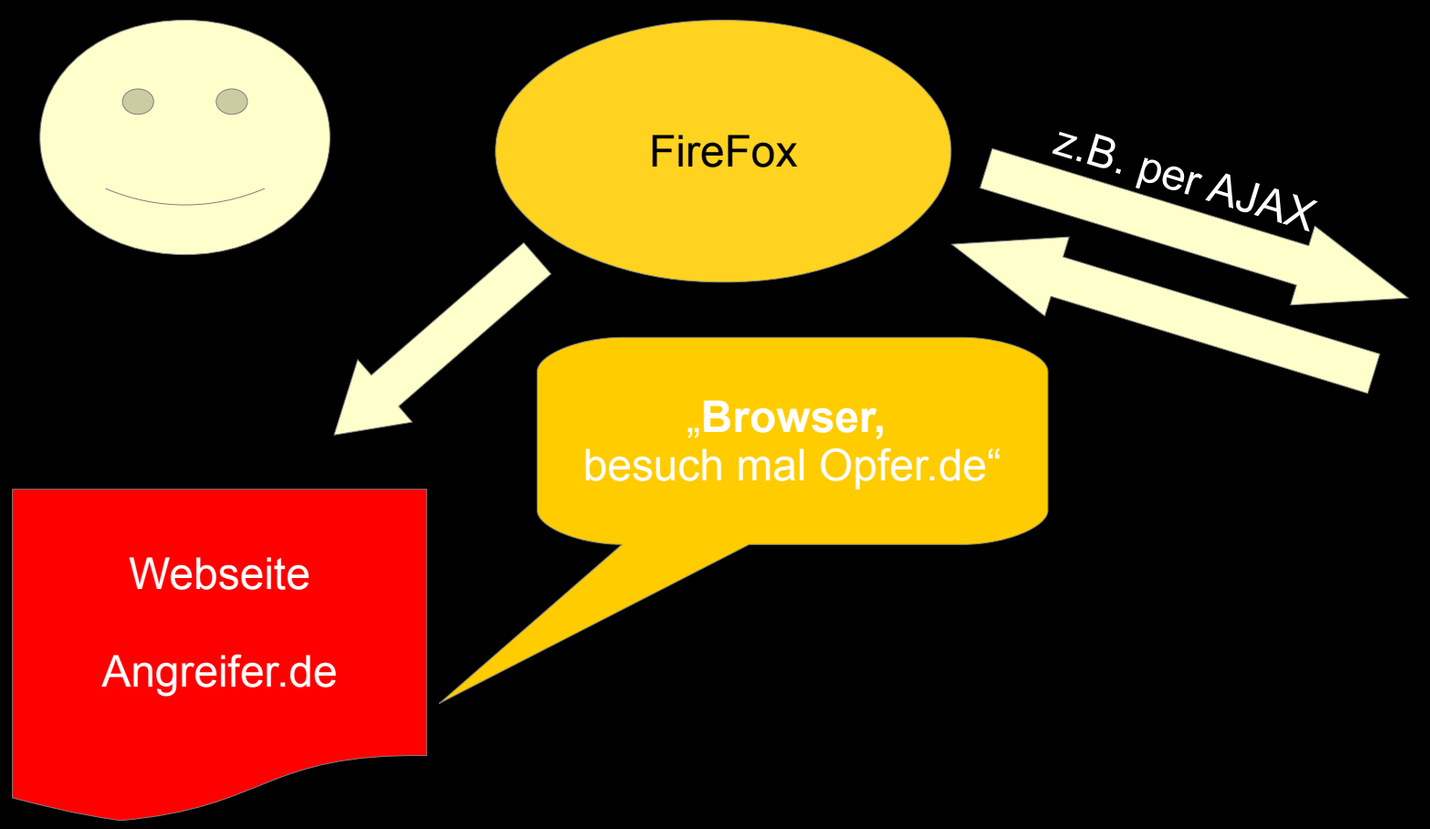
Podcast & Videostammtisch



© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch



Domain: opfer.de

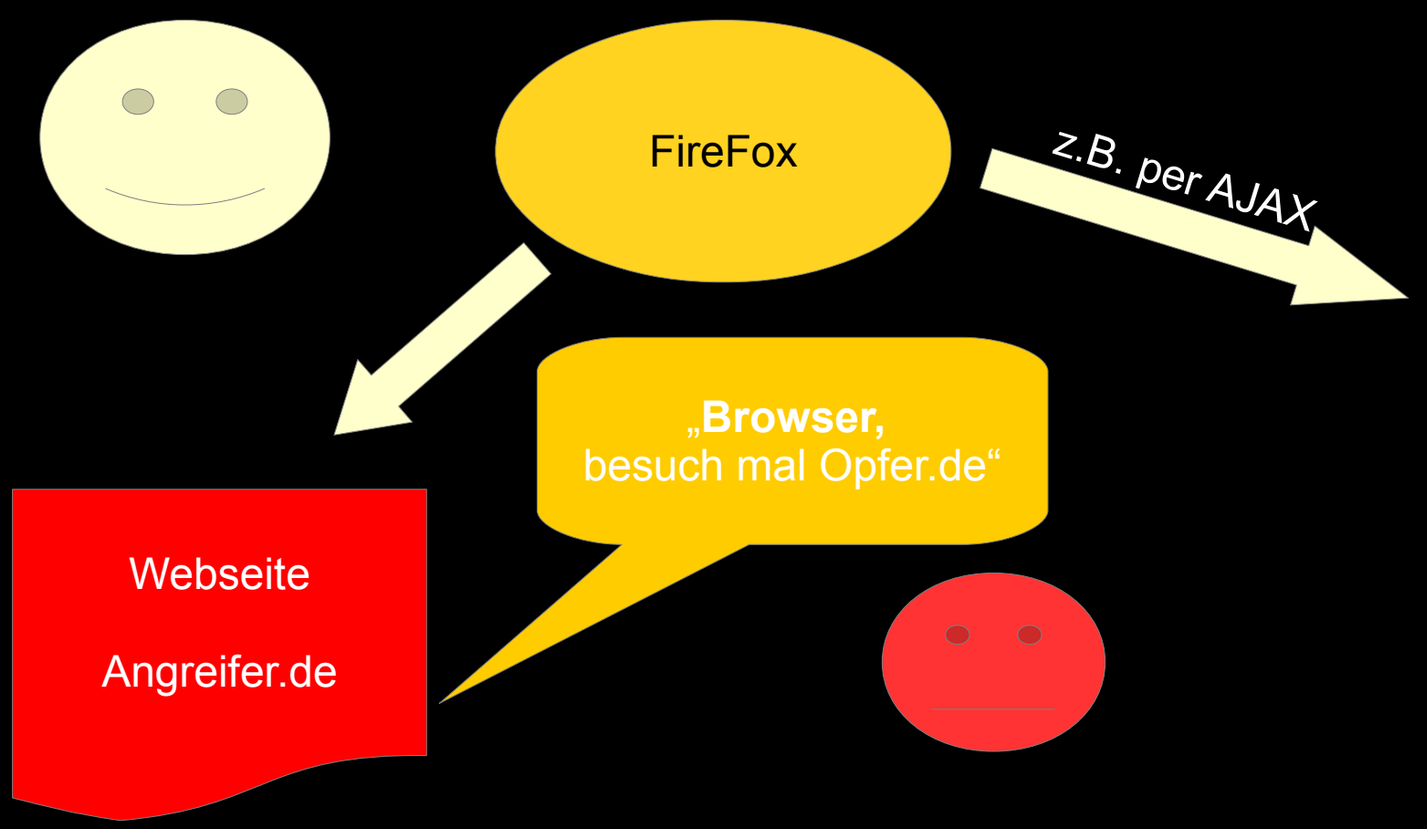
Webserver Port 443

FTP – Server Port 21
SMTP – Server Port 25
POP3 – Server Port 110
IMAP – Server Port 143

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch



Domain: opfer.de

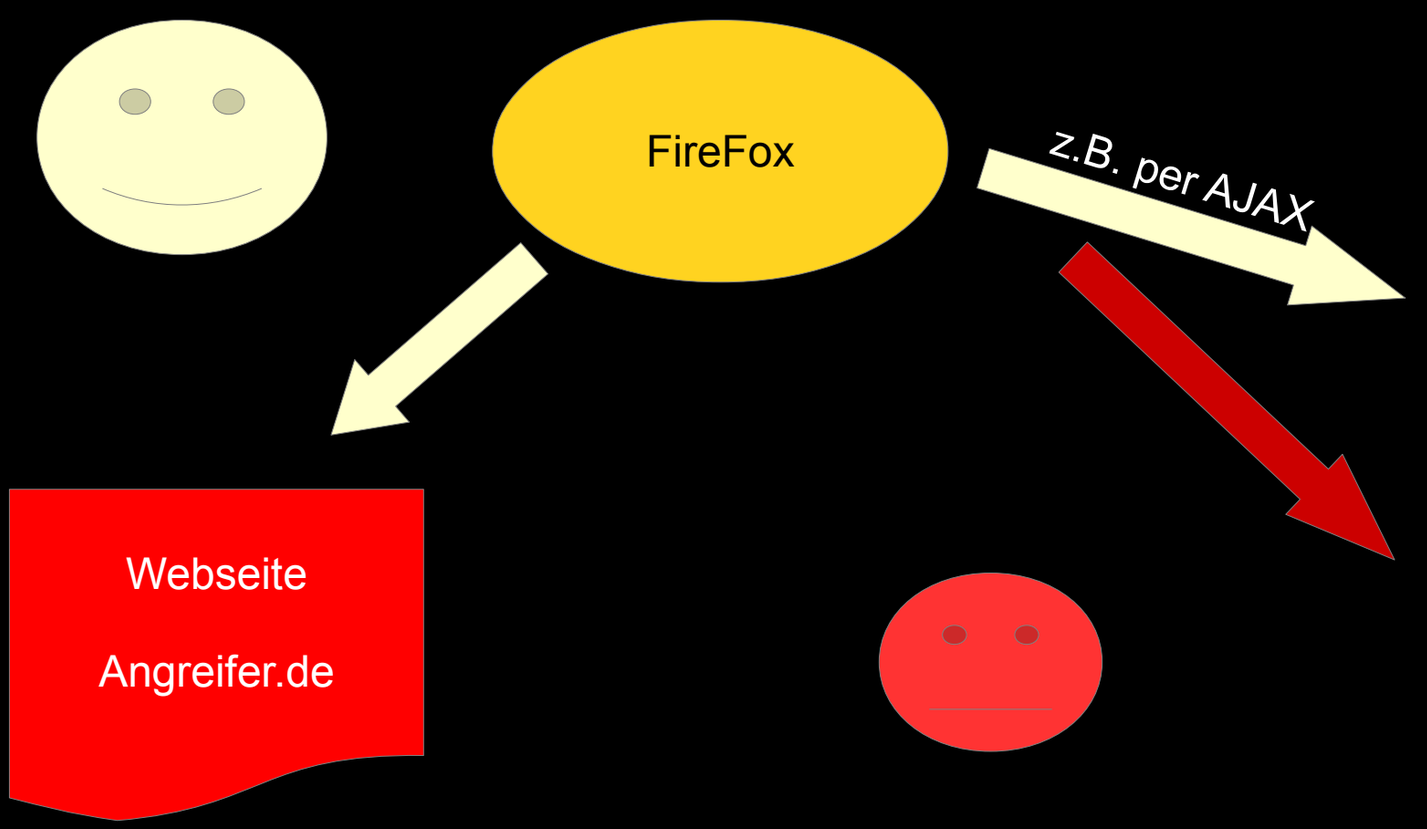
Webserver Port 443

FTP – Server Port 21
SMTP – Server Port 25
POP3 – Server Port 110
IMAP – Server Port 143

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch



Domain: opfer.de

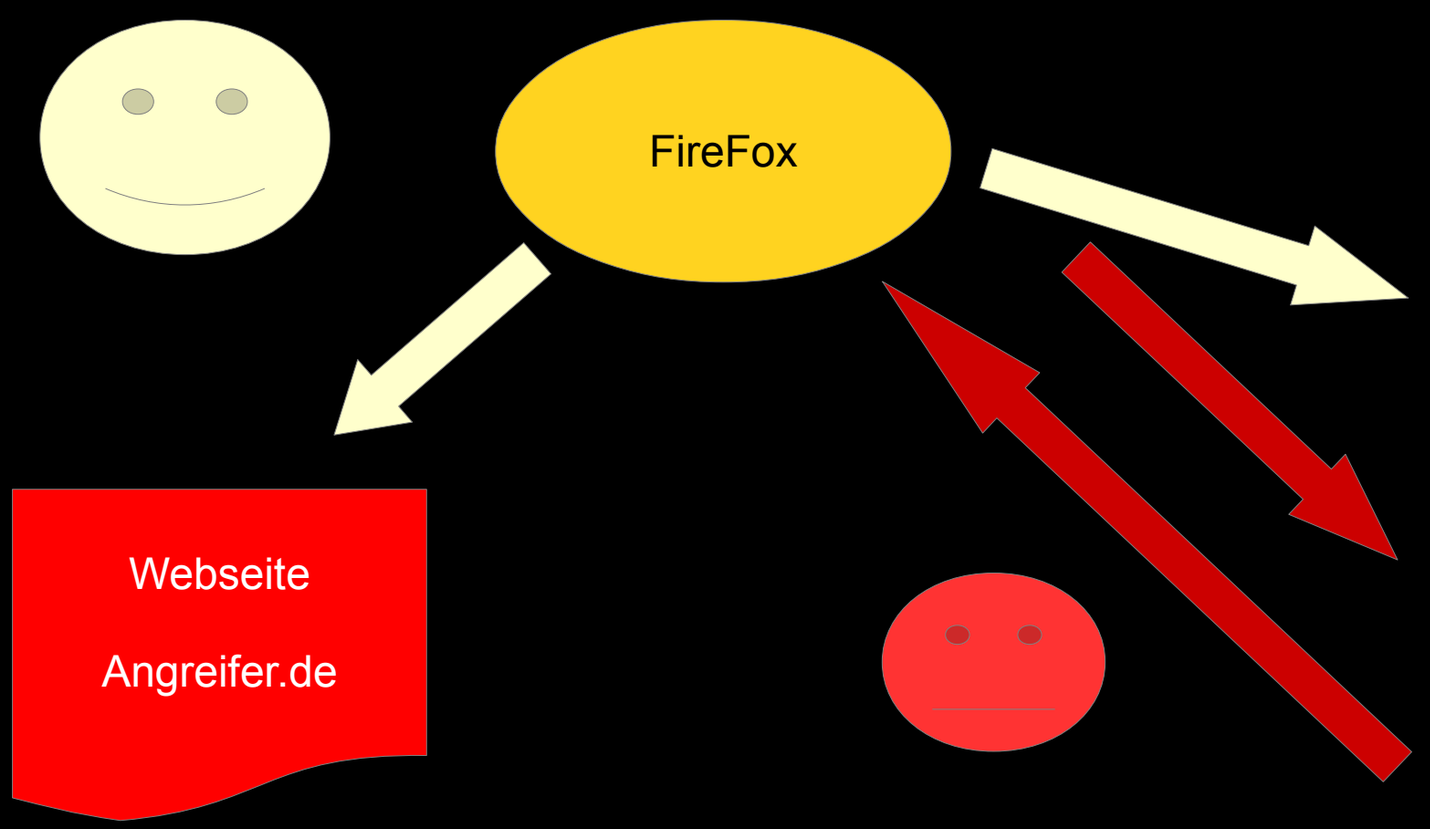
Webserver Port 443

FTP – Server Port 21
SMTP – Server Port 25
POP3 – Server Port 110
IMAP – Server Port 143

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch



Domain: opfer.de

Webserver Port 443

FTP – Server Port 21
SMTP – Server Port 25
POP3 – Server Port 110
IMAP – Server Port 143

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

Was ist jetzt so schlimm daran,

einen anderen Dienst zu belästigen?

© Marius Schwarz, Linux Am Dienstag, 2021

Beispiel: SMTP → Exim

© Marius Schwarz, Linux Am Dienstag, 2021

reales Beispiel:

```
# nc localhost 25
220 x.de ESMTP Exim 4.94 Tue, 15 Jun 2021 16:40:31 +0200
GET /index.html HTTP/1.1
500 unrecognized command
Host: opfer.de
500 unrecognized command
MAIL FROM: <script>alert(1);</script>
501 <script>alert(1);</script>: malformed address: alert(1);</script> may not follow <script>

500-unrecognized command
500 Too many syntax or protocol errors
```

© Marius Schwarz, Linux Am Dienstag, 2021

Dem Angreifer geht es dabei nicht darum den Mailserver zu kompromittieren,

sondern die Antwort an den Browser zu bekommen,

so daß dieser im Kontext der Webseite ausgeführt werden kann.

© Marius Schwarz, Linux Am Dienstag, 2021

```
$ nc c1 25
220 c1.x.de ESMTP Exim 4.94.2 Tue, 15 Jun 2021 16:22:10 +0200
MAIL FROM: <script>alert(1);</script>
501-<script>alert(1);</script>: malformed address:
alert(1);</script> may not follow <script>
501 Too many syntax or protocol errors
```

© Marius Schwarz, Linux Am Dienstag, 2021

Damit das klappt, müssen einige Voraussetzungen erfüllt sein:

Man-In-The-Middle-Attacke möglich
Pakete müssen punktgenau umgeleitet werden

© Marius Schwarz, Linux Am Dienstag, 2021

Damit das klappt, müssen einige Voraussetzungen erfüllt sein:

Man-In-The-Middle-Attacke möglich
Pakete müssen punktgenau umgeleitet werden

Ein Server, der das Gewollte in der Antwort mitschickt

© Marius Schwarz, Linux Am Dienstag, 2021

Damit das klappt, müssen einige Voraussetzungen erfüllt sein:

Man-In-The-Middle-Attacke möglich
Pakete müssen punktgenau umgeleitet werden

Ein Server, der das Gewollte in der Antwort mitschickt
Ein Browser der das mit sich machen lässt

© Marius Schwarz, Linux Am Dienstag, 2021

Damit das klappt, müssen einige Voraussetzungen erfüllt sein:

Man-In-The-Middle-Attacke möglich
Pakete müssen punktgenau umgeleitet werden

Ein Server, der das Gewollte in der Antwort mitschickt
Ein Browser der das mit sich machen lässt
Es muß das gleiche TLS Zertifikat in Benutzung sein.

© Marius Schwarz, Linux Am Dienstag, 2021

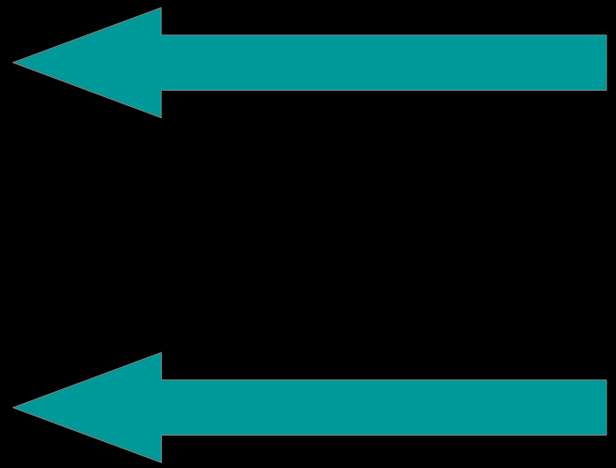
Linux Am Dienstag

Podcast & Videostammtisch

Domain: opfer.de

Webserver Port 443

FTP – Server Port 21
SMTP – Server Port 25
POP3 – Server Port 110
IMAP – Server Port 143



SSL-Zertifikat

Authority Information Access:
OCSP - URI:http://r3.o.lencr.org
CA Issuers - URI:http://r3.i.lencr.org/

X509v3 Subject Alternative Name:
DNS:opfer.de, DNS:www.opfer.de

X509v3 Certificate Policies:
Policy: 2.23.140.1.2.1
Policy: 1.3.6.1.4.1.44947.1.1.1
CPS: http://cps.letsencrypt.org

0 s:CN = opfer.de
i:C = US, O = Let's Encrypt, CN = R3
1 s:C = US, O = Let's Encrypt, CN = R3
i:C = US, O = Internet Security Research Group, CN = ISRG Root X1
2 s:C = US, O = Internet Security Research Group, CN = ISRG Root X1
i:C = US, O = Internet Security Research Group, CN = ISRG Root X1

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

Warum ist das TLS-Zertifikat wichtig?

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

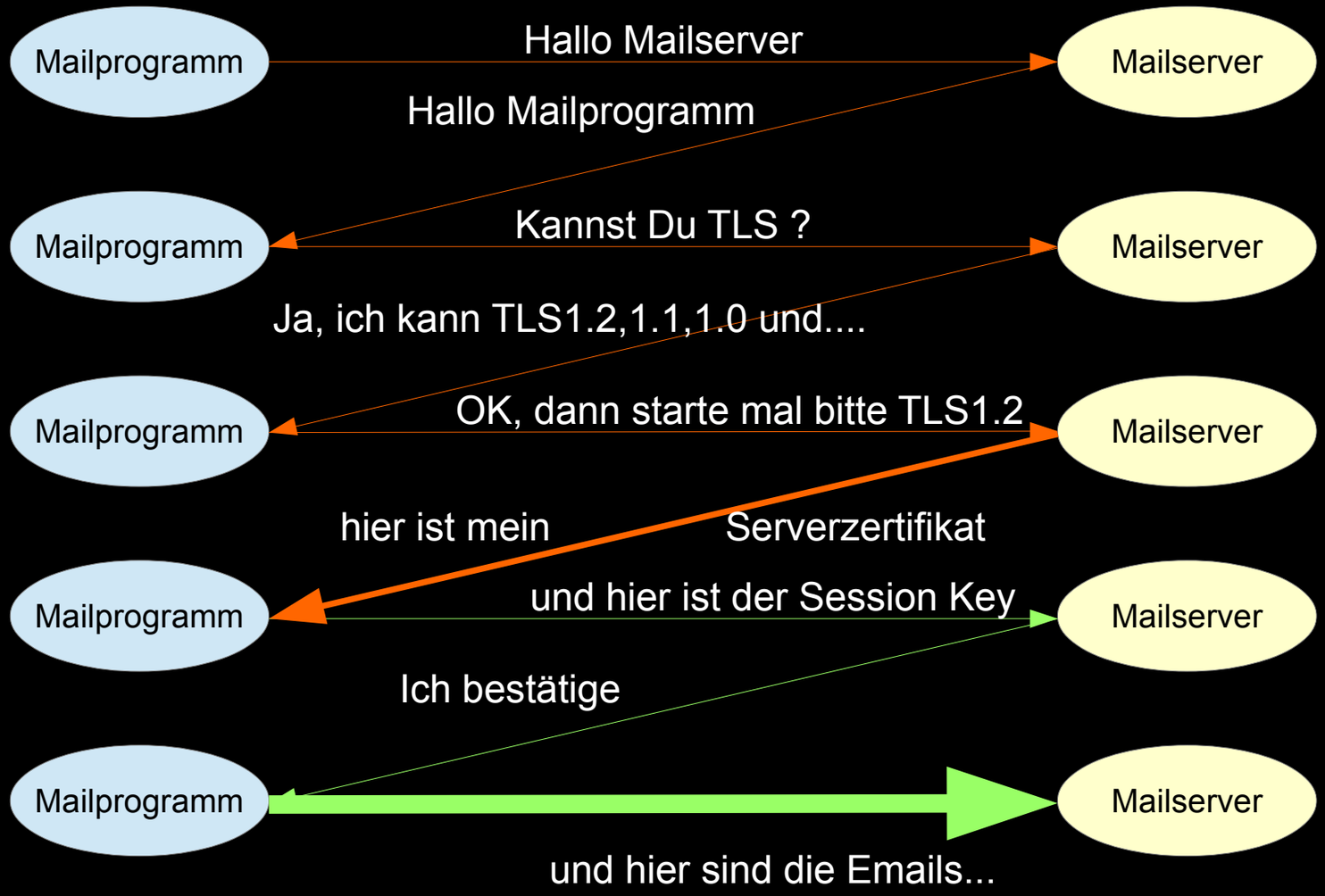
Der Verbindungaufbau einer TLS gesicherten Verbindung

ist in einzelne Abschnitte aufgeteilt.

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch



© Marius Schwarz, Linux Am Dienstag, 2021

Der Angreifer muß jetzt an der richtigen Stelle eingreifen,

damit er die Pakete vom Browser an den anderen Service umlenken kann ohne, daß es auf TLS-Ebene zu einem Fehler kommt.

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

ATTACKE!

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

2021-06-12 13:46:07 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "\026\003\001\001\236\001?\001\232\003\003\233\340/Q^EV\320\205\177\302\271\375\036\373Z\367\\366u\363@\201\212-s\220Y\007V\265^
R\343J\357\301\262?\375\027\342\027\304\266\026\374\345#\375\336 \346x", NULL)
2021-06-12 13:46:08 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "\026\003\001\001\265\001?\001\261\003\003s\022P\241K\301z\317\213\337\327\242g\027\353>\310?6\273\270\352k\fNi\274\355\316W\305\036 \
301W\347\025\355\352j\006\252\f\347\351c\257E]\346\277\035~\270\247\276\340\336cc\234-
H\3719?\214jj\300\022\300\023\300\007\300'\314\024\300/\023\001\300\024\023\002\300(\314\251\3000\300s\300`\300r\300a\300,\300v\300\257\300w\300\255\314\250\300$\023\005\300", NULL)
2021-06-12 13:46:08 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "", C=EHLO,STARTTLS)
2021-06-12 13:46:39 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "", C=EHLO,STARTTLS)
2021-06-12 13:46:40 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "", C=EHLO,STARTTLS)
2021-06-12 13:46:40 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "", C=EHLO,STARTTLS)
2021-06-12 13:46:40 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "\026\003\001\001E\001?\001A\003\003\306\247\305\026l\376\365m\301\246\205\303\345$\232:(\261\177\305\222\375\214\025\344?\017\020\017\367i\254??\266\3000\300,\300(\300$\300\024\300", NULL)
2021-06-12 13:46:40 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "", C=EHLO,STARTTLS)
2021-06-12 13:46:41 SMTP call from [193.37.255.114] dropped: too many syntax or protocol errors (last command was "\026\003\001?\214\001??\210\003\003 \027\206\364\254", NULL)
2021-06-12 21:01:58 SMTP call from [104.140.188.18] dropped: too many syntax or protocol errors (last command was "GET / HTTP/1.1", NULL)
2021-06-12 23:28:31 SMTP call from [89.248.165.106] dropped: too many syntax or protocol errors (last command was "\003??+&\340?????Cookie: mstshash=hello", NULL)
[root@c1 ~]# grep dropped /var/log/exim/main.log-20210613 |grep HTTP
2021-06-10 15:46:53 SMTP call from [83.135.88.244] dropped: too many syntax or protocol errors (last command was "GET /index.html HTTP/1.1", NULL)
2021-06-10 17:09:54 SMTP call from [134.122.7.20] dropped: too many syntax or protocol errors (last command was "HEAD / HTTP/1.0", NULL)
2021-06-10 17:09:55 SMTP call from [134.122.7.20] dropped: too many syntax or protocol errors (last command was "GET /system_api.php HTTP/1.1", NULL)
2021-06-10 17:09:56 SMTP call from [134.122.7.20] dropped: too many syntax or protocol errors (last command was "GET /c/version.js HTTP/1.1", NULL)
2021-06-10 17:09:58 SMTP call from [134.122.7.20] dropped: too many syntax or protocol errors (last command was "GET /streaming/clients_live.php HTTP/1.1", NULL)
2021-06-10 17:09:59 SMTP call from [134.122.7.20] dropped: too many syntax or protocol errors (last command was "GET /stalker_portal/c/version.js HTTP/1.1", NULL)
2021-06-10 17:10:01 SMTP call from [134.122.7.20] dropped: too many syntax or protocol errors (last command was "GET /stream/live.php HTTP/1.1", NULL)
2021-06-10 17:17:30 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "HEAD / HTTP/1.0", NULL)
2021-06-10 17:17:31 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "GET /system_api.php HTTP/1.1", NULL)
2021-06-10 17:17:32 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "GET /system_api.php HTTP/1.1", NULL)
2021-06-10 17:17:34 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "GET /c/version.js HTTP/1.1", NULL)
2021-06-10 17:17:35 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "GET /streaming/clients_live.php HTTP/1.1", NULL)
2021-06-10 17:17:37 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "GET /stalker_portal/c/version.js HTTP/1.1", NULL)
2021-06-10 17:17:39 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "GET /client_area/ HTTP/1.1", NULL)
2021-06-10 17:17:40 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "GET /stalker_portal/c/ HTTP/1.1", NULL)
2021-06-10 17:17:42 SMTP call from [138.197.154.233] dropped: too many syntax or protocol errors (last command was "GET /stream/live.php HTTP/1.1", NULL)
2021-06-10 19:08:50 SMTP call from [46.101.86.104] dropped: too many syntax or protocol errors (last command was "HEAD / HTTP/1.0", NULL)

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

Das war noch gar kein ALPACA Angriff,

sondern nur das weiße Rauschen im Netz :D

© Marius Schwarz, Linux Am Dienstag, 2021

Linux Am Dienstag

Podcast & Videostammtisch

Fragen?

© Marius Schwarz, Linux Am Dienstag, 2021