

Tunneling 101

von überall ins Netz

André / strohi

25. Oktober 2015

Motivation

Historisches

Problemstellung und Konzepte

Tools

- SSH and remote Shell

- Singleport forwarding

- VPN

Fallstricke und Resumé

Wer?

ich.

Warum?

Viele Tools über die Jahre, die mir früher viel (g)e(r)sparrt hätten



Was??



Was??



Welche Netze?

Eigene Netze

- ▶ zu Haus
- ▶ mit Freunden
- ▶ Firma/Kundennetze

Welche Netze?

Eigene Netze

- ▶ zu Haus
- ▶ mit Freunden
- ▶ Firma/Kundennetze

Fremde Netze

- ▶ Fremde Länder
- ▶ *Darknets*

- ▶ Viele Tools, kaputte Netze

Motivation und Fokus

- ▶ Viele Tools, kaputte Netze
- ▶ Vorstellung verschiedener Ansätze

Motivation und Fokus

- ▶ Viele Tools, kaputte Netze
- ▶ Vorstellung verschiedener Ansätze
- ▶ Von unterwegs nach Haus, Fernwartungsgeschichten, Services anbieten

Motivation und Fokus

- ▶ Viele Tools, kaputte Netze
- ▶ Vorstellung verschiedener Ansätze
- ▶ Von unterwegs nach Haus, Fernwartungsgeschichten, Services anbieten
- ▶ Fokus: Konzepte grob Vorstellen

Szenarien

ÖK. UCLAN

SMARTY /) OT

Home Log'in

NATIPOST

anonym, schaden

Zensur umgehen

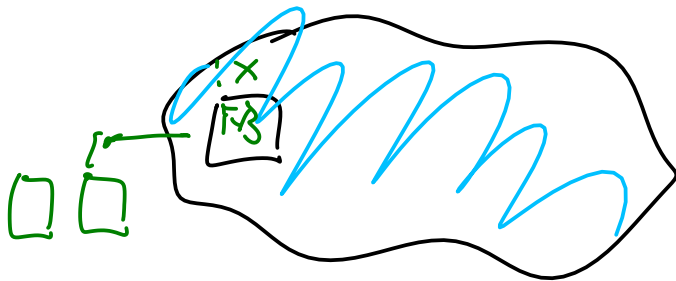
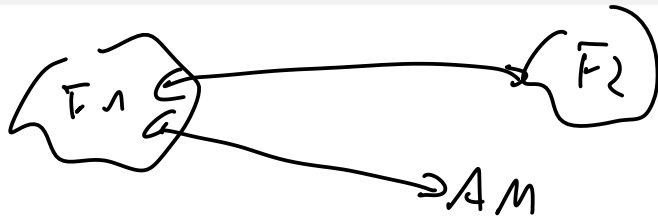
- ▶ Services anbieten
- ▶ Standorte Vernetzen
- ▶ Fernwartungszugriffe
- ▶ aus degradierten Netzen heraustunneln
- ▶ Dienste (ab)sichern

- ▶ DFÜ Einwahl
- ▶ leased lines
- ▶ Vor Ort sein
- ▶ Buch lesen/ spazieren(geocachen)

Warum Fortschritt?

- ▶ zu teuer
- ▶ Modemfarm + Leitungen
- ▶ Unwetter, Streiks ..
- ▶ heute eh immer mit Computer unterwegs

Skizze



site2site

services

Probleme?

Services direkt anbieten

- ▶ zu wenig IPs
- ▶ nicht alle Services public
- ▶ wechselnde IPs

Sicherheit

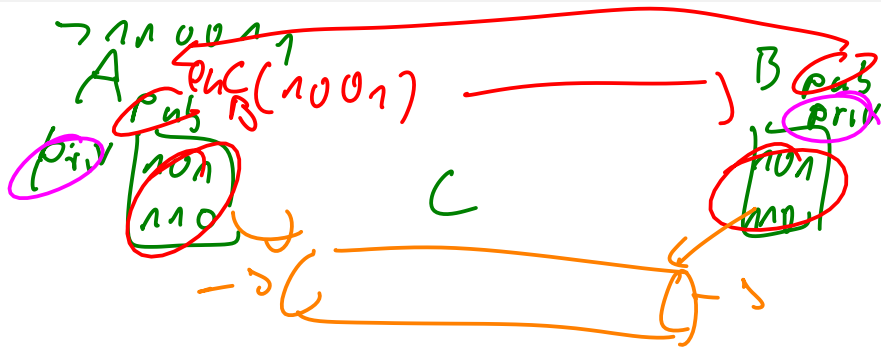
- ▶ viele lesen viel mit
- ▶ komische/alte Protokolle
- ▶ Compliance/Richtlinien

Lösungen

- ▶ Kryptographie: z.B. TLS
- ▶ Netzwerke in Netzwerke

skizze

Krypto Exkurs



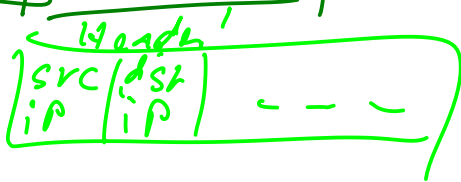
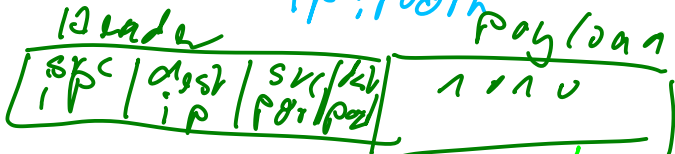
PKI

Netzwerk Exkurs

ip
port

ip
port
ip
port

ip:port



IP Paket

SSH 1

Socks

ssh -ND 33334 andre@tunnelbox

Webbrowser → Socksproxy

localhost:3333

http://weistmeineip.de → IP von Tunnelbox

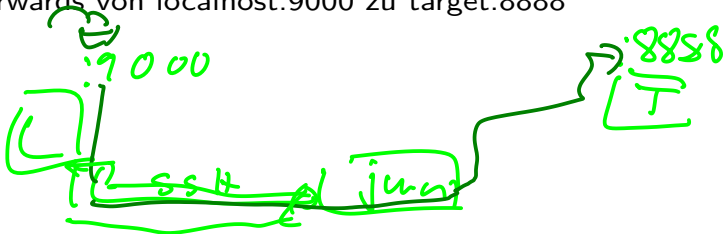
+ sockt \$ curl

SSH 2

Port Forwarding

```
ssh -L 9000:target:8888 andre@jumphost
```

forwards von localhost:9000 zu target:8888

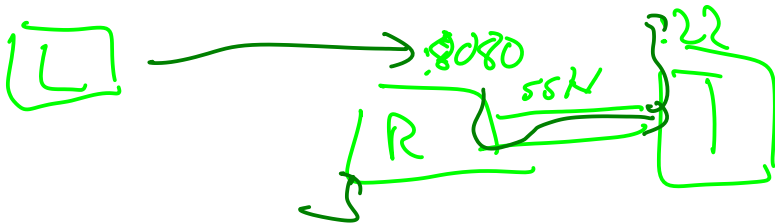


SSH 3

reverse Tunnel

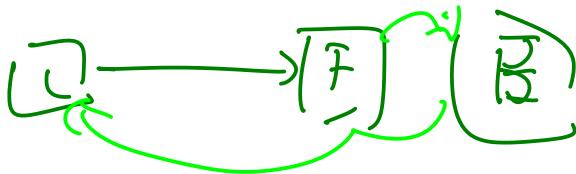
ssh -R 8080:localhost:22 reversehost

einkommend auf Reversehost:8080 geht an localhost 22



SSH Anmerkungen

- ▶ Key-Login
- ▶ signierte Keys?
- ▶ ssh -N
- ▶ -A /agent



Poor mans VPN mit SSH

Sshuttle

```
sshuttle -dns -r andre@jumphost 212.1.1.0\24
```

route Subnetze durch SSH

magic mit SSH und Iptables

in Python

robuste remote shell

```
mosh andre@jumphost
```

”Mobile shell that supports roaming and intelligent local echo”

locales feedback erlaubt korrekturen bevor es ausgeführt wird, synct später.

Socat (nc auf Steroiden)

Server

```
socat UDP-Listen:1337,fork,reuseddr stdio
```

Client


```
socat READLINE UDP:localhost:1337
```

Stunnel

TLS mit Zertifikaten davor schalten

```
foreground = yes  
pid =
```

```
[level1]  
accept = 13370  
exec = ./level1.py  
cert = level1-cert.pem  
key = level1-key.pem  
CAfile = level3-cert.pem  
verify = 2
```



- ▶ Server-Client
- ▶ Ein Server, mehrere Clients
- ▶ TLS basiert

▶ MeshVPN

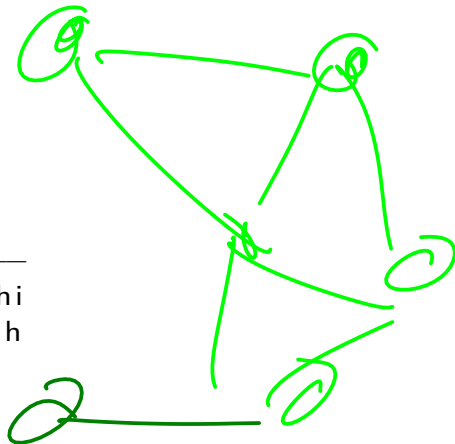
Subnet= 10.11.100.0/24

Adress = 10.11.100.3

-----BEGIN RSA PUBLIC KEY-----

hiwqefhUHFIUHWifquhiuwhfuiqwghi

fhqiuwhfuihfwiuhiuwqfiwqfhwqih



Was vergessen?

- ▶ iodine
- ▶ ..

Fallstricke



- ▶ MTU beachten, Fragmentierung
- ▶ DNS mittunneln falls gewollt
- ▶ Falls Browser: Cookies etc
- ▶ "internes" DNS
- ▶ <http://www.bralug.de/wiki/Overlaynetzwerke>



