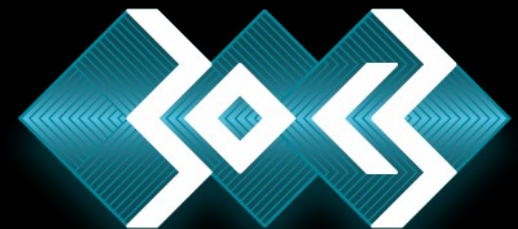


DHCXSSP



DHCXSSP



About me

- Moritz 'momo' Frenzel
- Linux Admin
- shackspace
- @momorientes
- m@hackathon.de

Imagine you're at a hackerspace...
and it's getting late...

so back to the hackerspace



so back to the hackerspace





So let's break it!

- We have a webinterface
- We could look for XSS, XSRF, ...
- We could test the underlying OS

Active Wireless Users

Filter by AP

↕ Name/MAC Address	↕ IP Address	↕ WLAN	↕ Access Point	↕ Signal	▼ Down
android-[REDACTED]	10.42.12.213	shack	DergrossePig	72% 	22.5K
Sch[REDACTED]	10.42.10.109	shack	DergrossePig	72% 	1.12K

1 - 2 / 2


```
dhcpcd -h '<script>alert(1)</script>' wlan0
```

Things to make your life easier

- A dot might be regexed away, use dword!
- Avoid weird caching, change your MAC on every try

And now what

- ~15 vendors affected
 - e.g. CVE-2013-3572
- Go out and pentest ALL webinterfaces
- If you find something:
 - Disclose responsibly
 - Let me know!
 - You owe me a tschunk



CVE-2013-2572

Questions?

- m@hackathon.de
- @momorientes
- DECT: 6421
- Infodesk or shackspace assembly

Thank You!