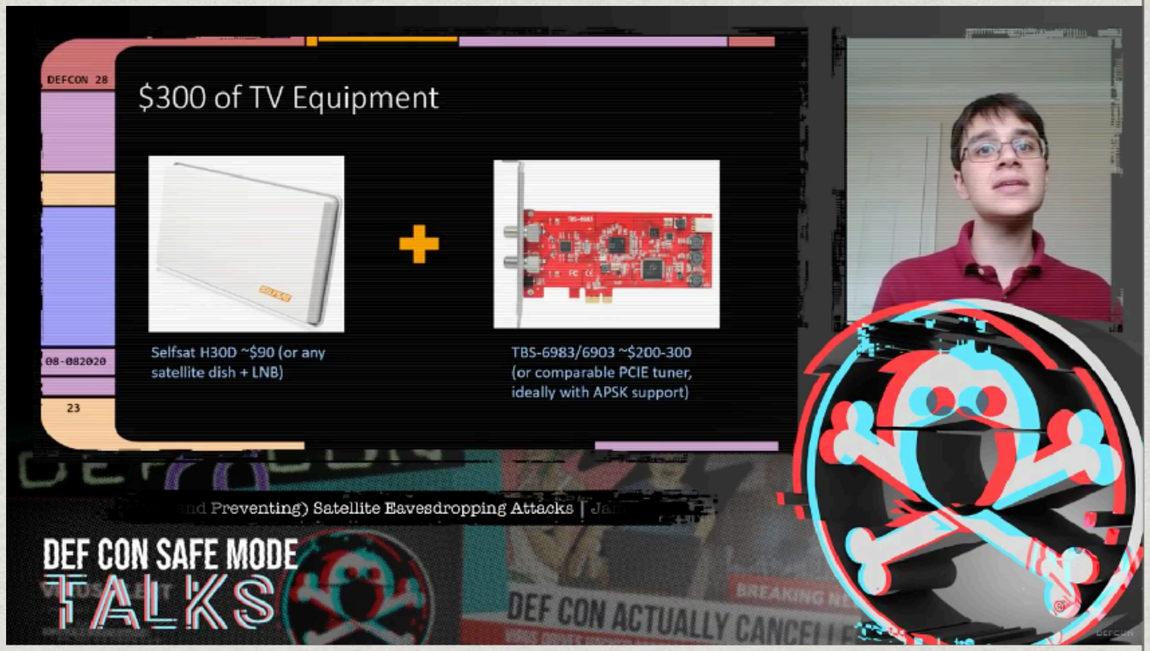
# DEF CON 28

## TALK RECAPS

# James Pavur
# **Whispers Among the Stars**

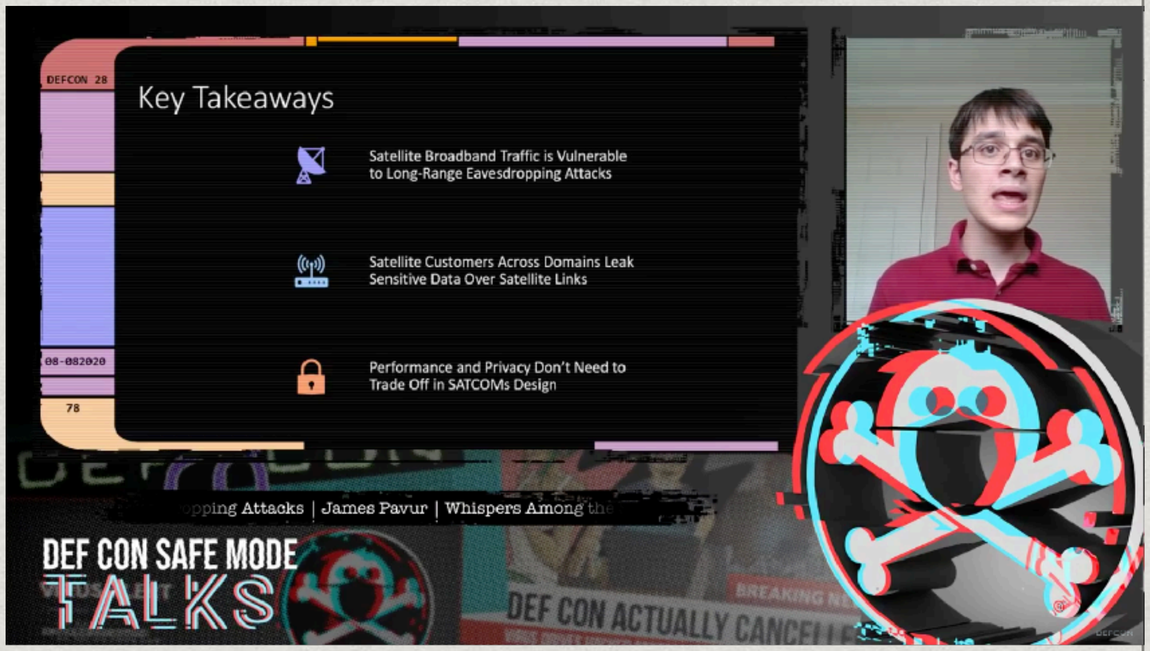
- Geostationäre TV-Sats, die auch Internetservices vermitteln
- Traffic für Subscriber für jeden im Ausleuchtgebiet mit billigem Equipment empfangbar.
- Verschlüsselung nicht Standard, nur wenn Anwendung verschlüsselt. (DNS, SMTP, POP3, FTP, …)
- Im Talk: Protokolle und die passenden Toolpfade bis zu Wireshark




https://www.youtube.com/watch?v=ku0Q_Wey4K0

# James Pavur
# **Whispers Among the Stars**

- Nutzer: Frachtschiffe, Kreuzfahrtschiffe, Flugzeuge, Remote OT (Windräder, etc.)
- Viele gute Anekdoten!
- PHP Session Tokens, offene FTP Server für Karten-Updates auf Frachtschiffen, Session Hijacking, nicht nachverfolgbare Datenexfiltration, …




https://www.youtube.com/watch?v=ku0Q_Wey4K0

# Jeff Foley (Caffix)
# OWASP Amass Red Team Village Training

- OWASP Tool für OSINT zur Identifikation von potentiellen Zielen mit Domainname als Startpunkt
- Command Line Tool mit einer eigenen Graph DB

```
$ amass enum -d DOMAIN :
```

Finde assets/subdomains mit Hilfe offener, freier Quellen (manche brauchen einen API Key), DNS, etc.

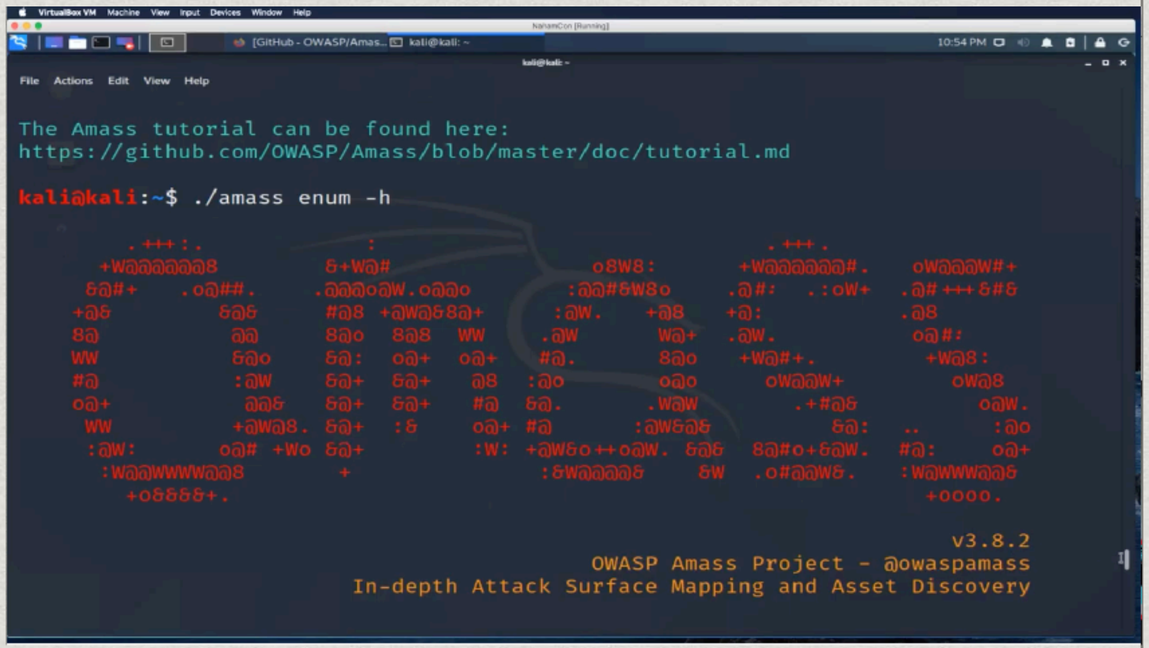
➡ Hosts (mit ASN und Quelle) landen in der Graph DB (.config/amass)

```
$ amass db -names -d DOMAIN
```

➡ Zeige alle Hosts in der DB

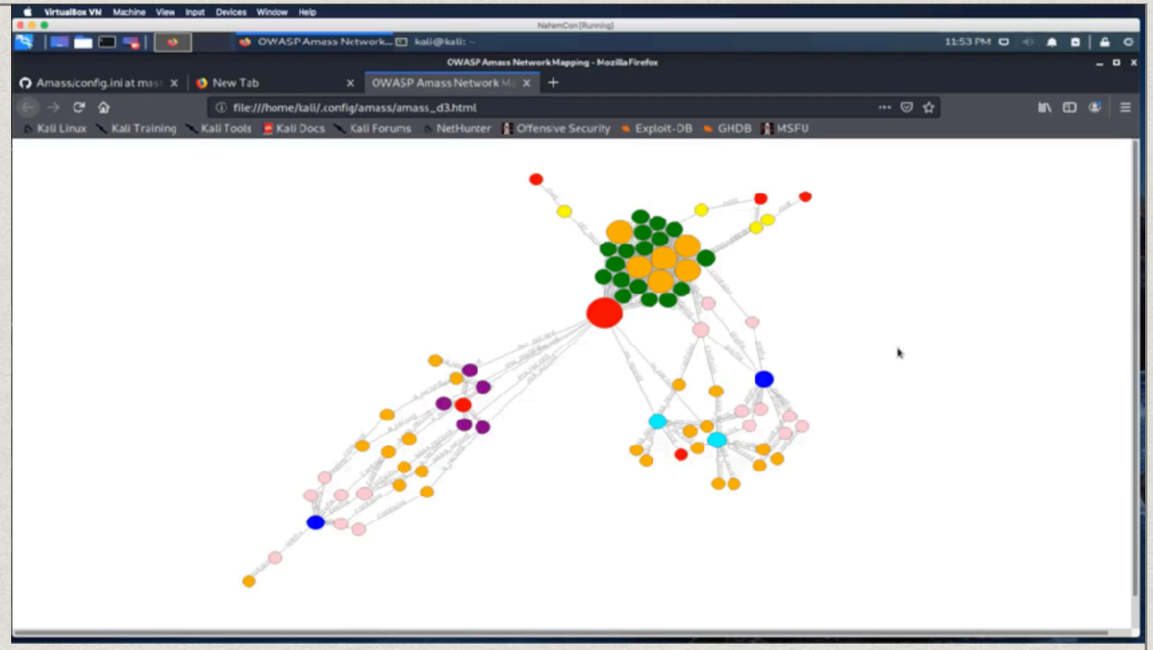
```
$ amass db -summary -d DOMAIN
```

➡ Summary der Daten in der DB




https://youtu.be/0ZSsiH2-AwA

# Jeff Foley (Caffix)
# OWASP Amass Red Team Village Training




https://youtu.be/0ZSsiH2-AwA

`$ amass intel -whois -d DOMAIN:`

Findet noch mehr Domainnamen, die mit der Organisation in Verbindung stehen *könnten*, z.B. basierend auf WHOIS Informationen. Diese Domains dann wieder mit "`enum`" abfragen.

`$ amass track -d DOMAIN:`

Zeige die beim letzten Lauf festgestellten Änderungen (neu, removed) an, nützlich bei längerfristigen Projekte.

`$ amass intel -active -asn ASN:`

Sammle Informationen über eine ASN

`$ amass enum -brute -w WORDLIST -d DOMAIN:`

Finde Hostnames/Subdomains mit einer Wordlist

`$ amass viz -d3 -d DOMAIN:`

Hübsche grafische Darstellung

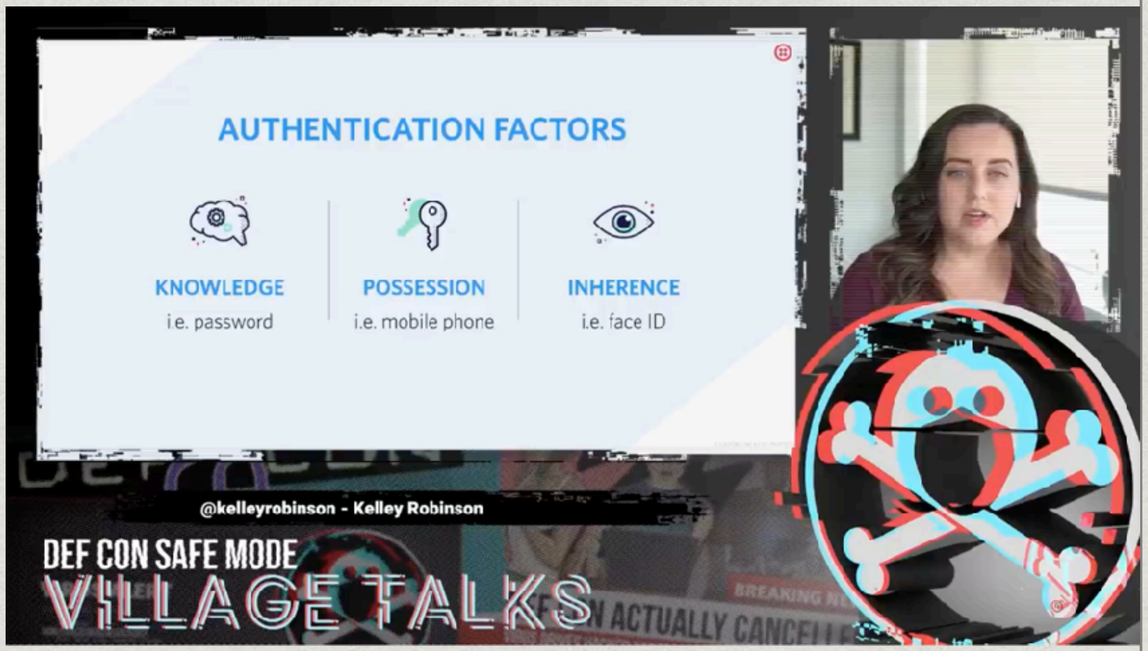
`$ amass enum -include CUSTOMSCRIPT -d DOMAIN`

Eigene Skripts können zum Einbinden von Datenquellen eingebunden werden (z.B. externes Command)

# Kelley Robinson
# 2FA in 2020 and Beyond - AppSec Village

- Kurzer Talk (25 Min) über Zwei-Faktor Authentifizierung
- Stellt die aktuell üblichen Zweiten Faktoren vor und bewertet Sie.
- Details im Talk, vieles auch mit Quellen (Studien zu Usability, Effectiveness, Adoption)

**SPOILER ALERT!**




https://youtu.be/8blsM0UV44E

# Kelley Robinson
# 2FA in 2020 and Beyond - AppSec Village

| | |
|---|---|
| SMS One-Time Passwords | „Convenient, but insecure“ |
| Soft Token - TOTP (Apps) | „Pretty good option, but not perfect“ |
| Pre-generated Codes | „Option for backups, less practical for ongoing use“ |
| Push Authentication | „Convenient and secure, but maybe too convenient?“ |
| U2F / WebAuthn | „Secure but not always convenient. Will become more common.“ |


https://youtu.be/8blsM0UV44E

# David Waldrop
# The DevOps & Agile Security Toolkit - AppSec Village

- Erklärt kurz Agile und DevOps, und
- dass Security in diesen Konzepten **zu spät** eingebunden wird.
- Sein Werkzeugkasten das zu fixen:

  - Agile Staffing
  - The 8 simple questions...
  - Security Champions Program
  - Developer Training
  - Security in the SDLC
  - Static Code Analysis
  - Dynamic Code Analysis
  - Open Source Analysis
  - Let's Automated This!!!


https://youtu.be/pF9l5AeUv9g

David Waldrop

# The DevOps & Agile Security Toolkit - AppSec Village

## Agile Staffing

Jemanden von InfoSec in Teams integrieren funktioniert nicht.

Stattdessen: Guidelines auf Enterprise Level und InfoSec Representative aus dem Agile Team

## The 8 simple questions...

Wann sollte das Agile Team das InfoSec Team "anrufen"? Fragen sollte jede Org für sich definieren und stets anpassen.

## Security Champions Program

Virtuelles Team, in das jedes agile Team genau einen Developer entsendet, der sich für Security interessiert und sich freiwillig gemeldet hat.

Vierteljährliche Treffen in lockerer Umgebung (Mittagessen) als Gelegenheit sich auszutauschen.

## Security in the SDLC

In welcher Phase des SDLC sollten welche Security Aktivitäten stattfinden?

## Developer Training (sein Lieblingsthema)

Von InfoSec organisierte Lunch & Learns, sollen Spaß machen.

Von InfoSec organisierte Secure Coding Trainings oder Trainingdays durch externe Instructors

InfoSec nimmt ein paar Devs mit zu Sicherheitsevents

## Static Code Analysis

automatisierte Codeprüfung alleine auf Basis des Quellcodes

## Dynamic Code Analysis

automatisierte Codeprüfung durch Beobachtung von laufendem Code

## Open Source Analysis

Welche Open Source Komponenten sind in einem Projekt eingebunden? Passen Lizenzen? Bekannte Schwachstellen?

## Let's Automated This!!!

Static/Dynamic/Open Source Analysis clever in die Build Pipeline einbauen.

https://youtu.be/pF9l5AeUv9g