BYO-ASM
Building an Attack Surface Management Platform

Using Open Source to identify what an attacker is likely to exploit

Disclaimer, whoami, repo

ALL OPINIONS ARE MY OWN AND DO NOT REPRESENT ANY ORGANIZATION I'M RELATED

- @heryxpc - everywhere (no OSINT needed)
- Demo and slides:

https://github.com/heryxpc/byo-asm-recon

Agenda

- What is Attack Surface Management?
- How to implement Attack Surface Management?
- Demo: EASM tools
- Cloud Recon on ASM
- Demo: CloudQuery
- Demo: Cartography and NeoDash
- Mixing ASM and Vulnerability Management
- Demo: Visualize your attack surface
- Automation and next steps

What is Attack Surface Management

Attack Surface Management (ASM) is the process to identify and manage the sum of all places an attacker can...ATTACK.

This can be a network, a system, a web app or any other IT infra (or humans behind it...).

Google-it: https://letmegooglethat.com/?q=attack+surface+management

YouTube-it:
https://www.youtube.com/results?search_query=attack+surface+management

Why doing so?

- **Because someone else will do it...**
  a. Threat Actors, Bounty Hunters, etc.
- To know what is *(NOT)* protected
  a. **Do you know what you don't know?**
- To prioritize security efforts
  a. **You can't tackle everything, focus on the highest impact/likelihood = risk**

How to implement Attack Surface Management

The magic recipe or silver bullet
Spoiler: *doesn't exists*

1. **Discovery/Recon**: Find all the assets you own
2. **Inventory**: Keep an updated asset DB
3. **Prioritize**: Define what is critical and what is not
4. **Protect**: Apply security controls
5. **Monitor**: Repeat all over again

The choosing your vendor problem

- Each focus/strength is on different places
  - Specific Cloud Provider/Technology Stack
  - Asset Discovery (e.g. Shadow IT)
  - Threat Intelligence
  - Vulnerability Management
  - Data Enrichment
  - Monitoring

❏ Might be expensive
- ❏ By Organization Size
- ❏ By Business Model
- ❏ Due to Infrastructure Requirements

LOTS OF VENDORS: https://github.com/someengineering/cloud-security-list?tab=readme-ov-file

DIY, YOU LAZY HACKER!

THIS TALK IS NOT ABOUT PROMOTING VENDORS

IT'S ABOUT USING OPEN SOURCE TO PERFORM ATTACK SURFACE MANAGEMENT

The right tool for the right job

The tools landscape is huge as well:

- Web Recon: subfinder, amass, etc.
- Cloud Recon: CloudQuery, Cartography, etc.
- Network Recon: nmap, masscan, etc.
- Vulnerability Scanning: OpenVAS, Nessus, etc.
- Container Scanning: Clair, Trivy, etc.
- Git scanning: trufflehog, gitrob, etc.

```
How to do it right then?
* Choose your initial focus (Web, Cloud, Network)
* Set a minimal scope (e.g. one AWS accounts, one root domain)
* Automate as much as possible
* Iterate all over again
```

[DEMO] External Attack Surface Management

Cloud Recon for ASM

Cloud Infra ~= Network + Data + Access

- Multiple providers: AWS, Azure, GCP
- Services: EC2, S3, RDS, etc.
- Configuration: IAM, VPC, etc.

What discovering infra can help you with?

- Find misconfigurations
- Detect open ports
- Identify publicly exposed data (S3, etc.)
- **Perform Drift Detection**
- **Correlate infrastructure**

[DEMO] CloudQuery + Grafana

[DEMO] Cartography + NeoDash

Mixing ASM and Vulnerability Management

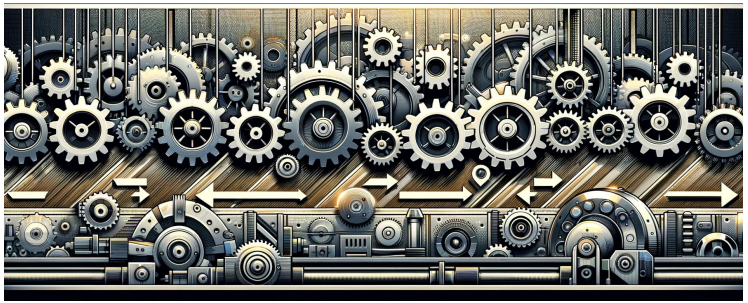
You mapped all your assets: now what?

1. Generate alerts based on configuration changes **(Drift Detection)**
2. Find the **path** an **attacker** would take
3. Identify **highests risk** assets (e.g. public facing, PII access, etc.)
4. **Identify Vulnerabilities in your assets**

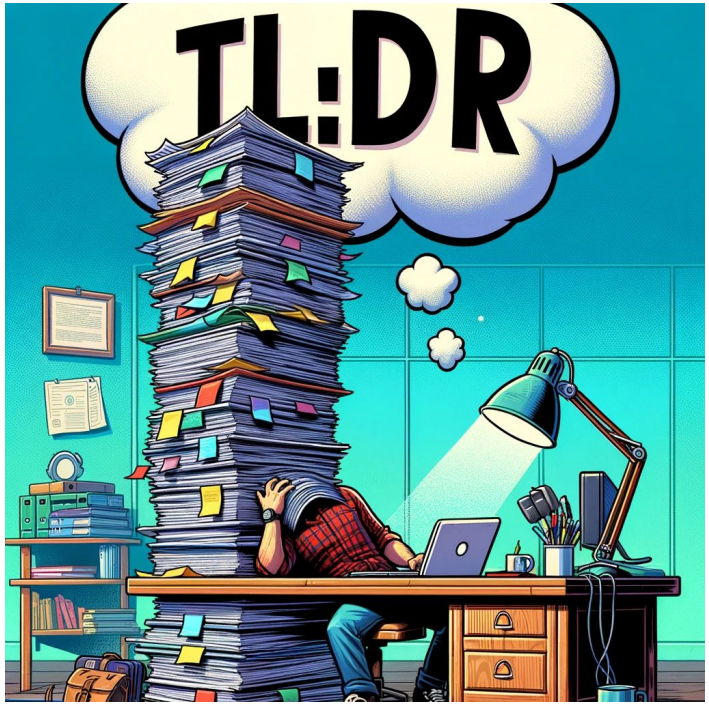
[DEMO] Visualize Your Attack Surface with risks

Next steps - Automation

- External attackers are running automated recon
  - BUT, only external surface.
- Red/Purple/Blue Teams *can* automate recon
  - AND, access internal information.



- Perform continuous recon
  a. **Automate discovery**
- Perform vulnerability scanning
  a. **Automate scanning**
- Create alerts for critical assets/vulnerabilities (**Monitoring**)
- **Automate remediation process**
- **Automate reporting process**



- ASM reduces the unknowns
  - Updated Asset Inventory
- Enables regular Vulnerability Reporting
- Helpful during Incident Response
- There is no silver bullet

➔ If you can pay for it:
- Understand what you are paying for
- Consider the limitations
- You still need to build a pipeline

➔ If you can build it:
- Build first a capable team
- Understand the tools you are using
- Balance the building vs buying cost