

Light Footprint

A decorative white line graphic consisting of two horizontal segments connected by a diagonal line, with small circles at the endpoints.

Ein Tool zur erkundung von Subdomains einer Domain

Agenda



- 1 Herausforderung
- 2 Was wird gemacht
- 3 Kurze Demo
- 4 Weitere Ideen
- 5 Fazit

Herausforderung

Cyber Angriffe nehmen mehr und mehr zu. Firmen brauchen zwingend einen Überblick über ihre Domain.

Viele Quellen

Um sich einen Überblick der Domain zu verschaffen gibt es zahlreiche Quellen welche unterschiedliche Ergebnisse liefern. Ein Ziel des erstellten Tools ist es diese an einem Ort zu sammeln und auszuwerten.

Erster Schritt zur Analyse

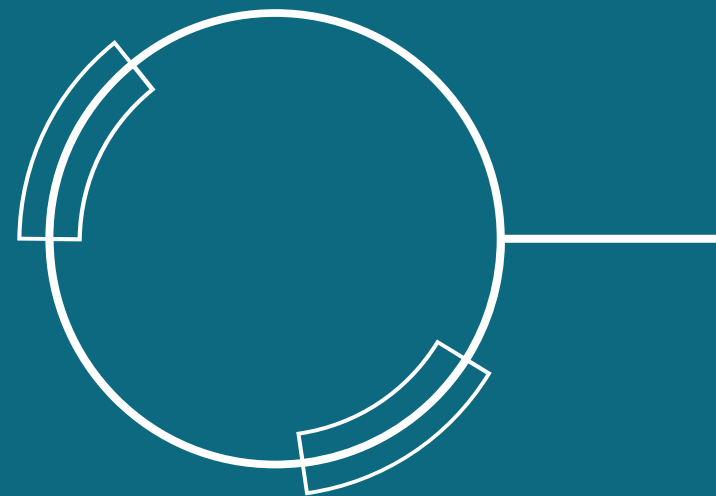
Ein guter Anfang für Firmen ist es ihre eigene IT-Domain von außen zu betrachten um ein Verständniss zu bekommen was ein Angreifer potentiell als Schwachstelle erkennt. Dies dient als Einstieg in Threat Intelligence.

Die meisten Analysetool sind kostenpflichtig

Leider sind die meisten Tools/ Quellenplattformen kostenpflichtig, das bedeutet Firmen werden abwägen müssen welches die effizienteste Vorgehensweise für sie ist. Und welche Ergebnisse sinnvoll kombiniert werden können ohne zu hohe Entwicklungskosten und Datenpeicherung zu verursachen.



Was wird gemacht




Python Script

- Sammeln von Subdomains aus verschiedenen Quellen
- CRT, VirusTotal, RapidDNS
- Python GUI zur einfachen Nutzung der Skripte
- Nutzen einer SQLite Datenbank für performanten und änderbaren Umgang mit den gesammelten Daten.

Externe Tools

- Subdomains, Services, IPs: Shodan, VirusTotal, Censys
- Ports: Nmap Port Scanner (Hacker Target)
- Grafische Darstellung der Komponenten: Maltego

 Subdomains

Inser Subdomains and Values

Show specific results

Search Subdomain results

DB

Choos Database

Subdomain Eingabe

Subdomain Name:

Subdomain Quelle:

Add Subdomain

IP-Adressen Eingabe

Subdomain Name:

IP Address:

IP Quelle:

Add IP

Ports Eingabe

IP Address:

Port:

Port Quelle:

Add Port

Services Eingabe

IP Address:

Port:

Service:

Version:

Service Quelle:

Add Service

Demo

Eine kurze Vorstellung des Programms:
<https://github.com/ttschan/SubdomainsIPs/tree/main/ConstantLightweightScan>



Weitere Ideen

Das Programm ist noch vielseitig erweiterbar. Die Struktur der Daten lassen nun weitere Analysen zu

1

Aktiven Scann optional mit einfügen

2

Services und Version mit anderen Datenbanken abgleichen

3

Analyse der Daten über einen längeren Zeitraum

4

Einfügen kostenpflichtiger Tools (Shodan, Censys, Portscanningtools)

Fazit

- Erste Übersicht der eigenen Domain
- Benutzeroberfläche mit Python nicht schön - könnte darüber nachdenken das Programm in Angular umzusetzen.
- Programm ist vielseitig erweiterbar.