06 / 2023

IT-S NOW

TÜV TRUST IT
TÜV AUSTRIA Group

T SECURITY

Die Macht des OSINT

Wie man öffentliche Daten effektiv nutzt

Workshop

WORKSHOP **SPEAKERS**

Fabio Birnegger BSc

Penetration Tester &
MSc Student

Fatih Varli BSc

Security Analyst &
MSc Student

TÜV TRUST IT
TÜV AUSTRIA Group

T SECURITY

06 / 2023

IT-S NOW

TÜV TRUST IT
TÜV AUSTRIA Group

T SECURITY

01

ÜBERSICHT

Was ist OSINT?

- Open Source Intelligence
- Analyse von Informationen aus öffentlichen Quellen
- Erkenntnisgewinnung
  - Manuell
  - Automatisch (Tools)

Nutzen für einen Angreifer

- Informationen über Target
- Vorbereitung auf einen Angriff
- Beispiele:
  - Persönliche Daten
  - Technische Daten
  - Unternehmens Daten

Use Case

- Mitarbeiter Name über Website des Unternehmens
- Finden des Mitarbeiters über LinkedIn
- Finden von weiteren Kollegen und Beziehungen
- Craften einer Spear Phishing E-Mail anhand von
  - Unternehmens Daten
  - Persönlichen Daten
  - Beziehungen zwischen Mitarbeitern
  - ...

02

TOOLS & TECHNIKEN

Reverse Bildersuche

- Zum entdecken visuell ähnlicher oder gleicher Fotos
- Kann in Investigationen genutzt werden:
  - Wo wurde das Bild geschossen?
  - Gibt es ähnliche Fotos?
  - Wurde das Foto manipuliert?
- Je nach Tool verschiedene Ergebnisse:
  - verschiedene Ansätze zum Analysieren der Bilder
  - verschiedene Datenbanken

Reverse Bildersuche - Tools

- Yandex Visual Search - https://yandex.com/images/
- Google Images Search by Picture - https://www.google.com/imghp
- PimEyes - https://pimeyes.com/en
  - Ideal für: Gesichter
- Tineye - https://tineye.com/
- DupliceChecker - https://www.duplichecker.com/reverse-image-search.php
  - Speist die gesuchten Bilder in mehrere Tools ein
- Deepware - https://scanner.deepware.ai/
  - Ideal für: Detektieren von Deepfake Videos

Metadaten - EXIF

- Exchangeable Image File Format (EXIF)
- Gibt Informationen zu einem Bild, unter anderem:
  - Kameraeinstellungen (Shutter Speed, ISO speed, …)
  - Bild Metriken
  - GPS Standort
- Hin und wieder findet man online Bilder, die EXIF-Daten beinhalten …
- Tool: https://exif.tools/

Google Dorks

- Operatoren für effektivere Google Suchen
  - Bspw. Filtern von Web-Seiten. (“-” Operator)
- Sensitive Informationen über Google erreichbar
  - Selbst nach dem Löschen der jeweiligen Seiten, könnten diese weiterhin im Google Cache gespeichert sein! (“cache:” Operator)
- Basic und Advanced Operators
  - Basic Operators: +, -, “”, ~, ., *
  - Advanced Operators: nächste Seite

Google Dorks

- Gängige Advanced Operators:
- cache: zeigt die gecachte Version einer Website,
  - z.B. *cache:fh-campuswien.ac.at*
- inurl: sucht Seiten mit einem bestimmten Keyword in der URL
  - z.B. *inurl:admin*
  - Für mehr als ein Wort soll der Operator allinurl: verwendet werden
- filetype: nach bestimmten File Extensions suchen
  - z.B. *filetype:pdf*
- site: nach Ergebnissen von einer bestimmten Seite suchen
  - z.B. *site:linkedin.com*
- intitle: nach bestimmten Wörtern

Advanced Operators

Advanced Operators	Meaning	What To Type Into Search Box *(& Description of Results)*
site:	Search only one website	**conference site:www.sans.org** *(Search SANS site for conference info)*
[#]...[#] or numrange:	Search within a range of numbers	**plasma television $1000...1500** *(Search for plasma televisions between $1000 and $1500)*
date:	Search only a range of months	**hockey date: 3** *(Search for hockey references within past 3 months; 6 and 12-month date-restrict options also available)*
safesearch:	Exclude adult-content	**safesearch: sex education** *(Search for sex education material without returning adult sites)*
link:	linked pages	**link:www.sans.org** *(Find pages that link to the SANS website)*
info:	Info about a page	**info:www.sans.org** *(Find information about the SANS website)*
related:	Related pages	**related:www.stanford.edu** *(Find websites related to the Stanford website)*
intitle:	Searches for strings in the title of the page	**intitle:conference** *(Find pages with "conference" in the page title)*
allintitle:	Searches for all strings within the page title	**allintitle:conference SANS** *(Find pages with "conference" and "SANS" in the page title. Doesn't combine well with other operators)*
inurl:	Searches for strings in the URL	**inurl:conference** *(Find pages with the string "conference" in the URL)*
allinurl:	Searches for all strings within the URL	**allinurl:conference SANS** *(Find pages with "conference" and "SANS" in the URL. Doesn't combine well with other operators)*
filetype: or **ext:**	Searches for files with that file extension	**filetype:ppt** *(Find files with the "ppt" file extension. ".ppt" are MS PowerPoint files.)*
cache:	Display the Google cache of the page	**cache:www.sans.org** *(Show the cached version of the page without performing the search)*
phonebook: or **rphonebook:** or **bphonebook**	Display all, residential, business phone listings	**phonebook:Rick Smith MD** *(Find all phone book listing for Rick Smith in Maryland. Cannot combine with other searches)*
author:	Searches for the author of a newsgroup post	**author:Rick** *(Find all newsgroup postings with "Rick" in the author name or email address. Must be used with a Google Group search)*
insubject:	Search only in the subject of a newsgroup post	**insubject:Mac OS X** *(Find all newsgroup postings with "Mac OS X" in the subject of the post. Must be used with a Google Group search)*
define:	Various definitions of the word or phrase	**define:sarcastic** *(Get the definition of the word sarcastic)*
stock:	Get information on a stock abbreviation	**stock:AAPL** *(Get the stock information for Apple Computer, Inc.)*

Cheat-Sheet Auszug

Source: https://www.sans.org/posters/google-hacking-and-defense-cheat-sheet/

Wayback Machine

- Internet Archive
- Tool zum Abruf archivierter Websites
- Snapshots werden durch Web Crawler erstellt
- Nicht alles wird archiviert!

Source: archive.org/web/

Website Scanning

- Ermitteln verwendeter Technologien
- Durch bestimmte “Signale”
- Speziell als Vorbereitung für einen Angriff über Website
- Tools:
  - Wappalyzer - https://www.wappalyzer.com/
  - BuiltWith - https://pro.builtwith.com/
  - …

Maltego

- Daten Analyse Software
- Verknüpft Informationen
- Visuelle Darstellung mittels Graphen
- Unterstützte Suchquellen:
  - Suchmaschinen
  - Websites
  - Social Media
  - Öffentliche Datenbanken

Source: Maltego Technologies

03

CHALLENGES

Praktische Challenges

Level I bis III

Bist du bereit?

https://www.github.com/fbirn/ITSNOW_OSINT_WS/

Vielen Dank für die Aufmerksamkeit !

Bei weiteren Fragen:

Fabio Birnegger: fabio.birnegger@stud.fh-campuswien.ac.at

Fatih Varli: fatih.varli@stud.fh-campuswien.ac.at