

Übungsaufgaben

Phase Aufklärung / Information Gathering

Dieses Dokument beinhaltet die Versuchsanleitung für die Durchführung des Laborversuches Phase Aufklärung / Information Gathering.

Bei Fragen zur Versuchsanleitung wenden Sie sich bitte direkt an das Laborpersonal.

Autoren: M. Moro, R. Wyss, C. Banzer, T. Jösler, N. Neher, B. M. Hämmerli

Version: 2.3XO

Letzte Änderung: 27.09.2023

Inhaltsverzeichnis

Vorwort	4
Feedback.....	4
Legende	4
Bemerkungen / Rechtlicher Hinweis.....	4
1 Vorbereitung.....	5
1.1 Theorie.....	5
1.2 Fragen zur Theorie	5
1.3 Benötigte Mittel.....	7
2 Was wir heute lernen	7
3 Information Gathering – Eigene Persönlichkeit (120min)	8
3.1 Informationsbeschaffung /-gestaltung (80min)	8
3.1.1 Informationsquellen.....	8
3.1.2 Datenanspruch	9
3.1.3 Datenbeschaffung.....	9
3.2 Informationsverarbeitung (40min)	9
3.2.1 Datenrepräsentation.....	9
3.2.2 Datenanalyse /-interpretation.....	10
4 Information Gathering – öffentliche Personen (120min).....	11
4.1 Informationsbeschaffung /-gestaltung (80min)	11
4.1.1 Informationsquellen.....	11
4.1.2 Datenanspruch	12
4.1.3 Datenbeschaffung	12
4.2 Informationsverarbeitung (40min)	12
4.2.1 Datenrepräsentation.....	12
4.2.2 Datenanalyse /-interpretation.....	13
5 Information Gathering – Hochschule Luzern (135min)	14
5.1 Webauftritt der HSLU (15min)	14
5.2 Social Media Auftritt der HSLU (15min)	15
5.3 Technische Analyse der HSLU (105min)	16
5.3.1 Google Direktiven und GHDB.....	16
5.3.2 FOCA	17
5.3.3 Shodan.io.....	20
5.3.4 Maltego CE.....	23
6 Anhänge.....	27
6.1 Anhang A – Mögliche Informationsquellen.....	27
6.1.1 Vorwissen zur Zielperson.....	27
6.1.2 Social Networks – erste Anlaufstelle für persönliche Informationen.....	27
6.1.3 Persönliche Webseite / Blog.....	31
6.1.4 Google Suche – Korrekte Anwendung entscheidend.....	32
6.1.5 Weitere Informationsquellen – OSINT Framework.....	33
6.2 Anhang A – OVA Datei in VirtualBox importieren.....	34
6.3 Anhang B – FOCA	36
6.4 Anhang C - Shodan.io	42
6.5 Anhang D – Maltego CE	46

Abbildungsverzeichnis

Abbildung 1: FOCA: auszuwählende Dateiendungen.....	18
Abbildung 2: Einstellungen FOCA Network Search	19
Abbildung 3: XING – Einsatz Personensuche	29
Abbildung 4: XING – Persönliches Profil als CV.....	29
Abbildung 5: XING People Search by Company.....	30
Abbildung 6: LinkedIn People Search	30
Abbildung 7: LinkedIn People Search by Company	31
Abbildung 8: inurl Google Search.....	32
Abbildung 9: OSINT Framework.....	33
Abbildung 10: VirtualBox Appliance importieren.....	34
Abbildung 11: VirtualBox Appliance auswählen.....	34
Abbildung 12: VirtualBox Appliance-Übersicht.....	35
Abbildung 13: FOCA: Projektübersicht	36
Abbildung 14: FOCA: Dokumentsuche	36
Abbildung 15: FOCA: Logeinträge anhand von Fuzzing	36
Abbildung 16: FOCA: Metadatendetails zu einem Dokument.....	37
Abbildung 17: FOCA: Dokumentenliste.....	38
Abbildung 18: FOCA: Aggregierte Daten von Dokumenten (1 / 215 Dokumenten analysiert)	38
Abbildung 19: FOCA: Network-Suche Einstellungsmöglichkeiten	39
Abbildung 20: FOCA: Dokumentenscan auf einzelnen Hosts	39
Abbildung 21: FOCA: Übersicht der gefundenen Server (unvollständig)	40
Abbildung 22: FOCA: Aggregierte Metadaten der Mail-Adressen	40
Abbildung 23: FOCA: Aggregierte Metadaten der Betriebssysteme	40
Abbildung 24: FOCA: Proxy-Einstellungsmöglichkeiten.....	41
Abbildung 25: Shodan: Suchfeld	42
Abbildung 26: Shodan: Resultatübersicht	42
Abbildung 27: Shodan: HTTP-Antworten auf Requests	43
Abbildung 28: Shodan: Zertifikatsinformationen	43
Abbildung 29: Shodan: Unternehmens-Informationen wie GPS; ISP, etc.....	44
Abbildung 30: Shodan: gefundene, offene Ports.....	44
Abbildung 31: Shodan: Service-Details (Port-Informationen).....	45
Abbildung 32: Shodan: Search Filters.....	45
Abbildung 33: Maltego: Transformhub.....	46
Abbildung 34: Maltego: Plugin-Settings (bspw. API-Key für Shodan).....	46
Abbildung 35: Maltego: Entity Palette.....	47
Abbildung 36: Maltego: Domain Entity Konfiguration	47
Abbildung 37: Maltego: Suche nach Related TLD Domains	48
Abbildung 38: Maltego: Ansichts-Optionen	48

Abkürzungsverzeichnis

Abkürzung	Beschreibung
API	Application Programming Interface
GHDB	Google Hacking Database
ISP	Internet Service Provider
OSINT	Open-Source Intelligence
Proxy	Software/System zur Vermittlung zwischen dem Endpunkt
TLD	Top Level Domain

Vorwort

Diese Laborübungen sollen den Studierenden die Phase «Aufklärung» näherbringen. Diese Aufgaben befassen sich daher primär mit den Themen Informationsbeschaffung und -verarbeitung rund um öffentlich verfügbaren Informationen. Es wird im Rahmen der Übungen somit ausschliesslich auf frei zugänglich Informationen zurückgegriffen.

Die vorliegende Übung setzt grundlegendes Netzwerk-Knowhow (vgl. Modul NS – Network & Cloud Services / Computer Network Architecture) und die Verwendung von Tools/Methoden für die Informationsverwaltung (z.B. EverNote, OneNote oder diverse MindMap-Tools) voraus.

Feedback

Mit Ihrer Mithilfe kann die Qualität des Versuches laufend den Bedürfnissen angepasst und verbessert werden.

Falls in diesem Versuchsablauf etwas nicht so funktioniert wie es beschrieben ist, melden Sie dies bitte direkt dem Laborpersonal oder erwähnen Sie es in Ihrem Laborbericht oder Protokoll. Bei Problemen wenden Sie sich bitte an das Laborpersonal, idealerweise über Discord.

Legende

In den Versuchen gibt es Passagen, die mit den folgenden Zeichen markiert sind. Diese sind wie folgt zu verstehen:



Dringend beachten. Was hier steht, unbedingt merken oder ausführen.



Beantworten und dokumentieren Sie die Antworten im Laborprotokoll.



Ergänzender Hinweis / Notiz / Hilfestellung.



Weiterführende Informationen. Dies sind Informationen, die nicht zur Ausführung der Versuche benötigt werden, aber bekannt sein sollten.

Bemerkungen / Rechtlicher Hinweis

Die vorliegenden Übungen beinhalten sowohl Einzelarbeiten als auch Partnerarbeiten. Es ist daher vorteilhaft, in 2er Teams zu arbeiten.

Im Rahmen der Laborübungen dürfen Personenprofile unter Genehmigung der entsprechenden Person erstellt, jedoch nicht anderweitig verwendet werden. Bitte beachten Sie, dass Sie im Rahmen dieser Übungen ggf. mit besonders schützenswerten Daten in Kontakt kommen und diese entsprechend rechtskonform/adäquat behandeln.



Bitte seien Sie sich bewusst, dass die Anwendung dieser Techniken gegenüber den genannten Personen / Systeme ausserhalb der Laborübung ggf. strafrechtliche Konsequenzen mit sich bringen kann.

1 Vorbereitung


Dieses Kapitel beschreibt die Vorbereitungsmaßnahmen, die Sie vor Beginn des Laborversuches durchführen müssen und soll ebenfalls kurz die theoretischen Grundlagen reflektieren.

1.1 Theorie

Lesen Sie Kapitel 2 «Aufklärung» in Patrick Engebretsons «Hacking Handbuch».

1.2 Fragen zur Theorie

Beantworten Sie die folgenden Fragen im Formular unten.


 Welche Phasen gibt es in einem Cyber Angriff?

.....

.....

.....

.....


 Gibt es unterschiedliche Modelle zur Gliederung eines Cyber Angriffs? Wenn ja, welche?

.....

.....

.....

.....

 Wieso werden unterschiedliche Modelle verwendet?

.....

.....

.....

.....



Was ist der ungefähre Zeithorizont eines Cyber Angriffs?

.....

.....

.....

.....



Welche Informationsquellen können für einen Cyber Angriff verwendet werden? Nennen Sie Beispiele?

.....

.....

.....

.....



Wie könnten die gesammelten Informationen kategorisiert werden?

.....

.....

.....

.....



Erklären Sie den Begriff OSINT.

.....

.....

.....

.....

1.3 Benötigte Mittel

Für eine grafische Darstellung der Informationen bietet sich beispielsweise das OpenSource Tool XMind¹ oder das kommerzielle Tool «Mindjet MindManager» (für Studenten der HSLU kostenlos über Softwarekiosk) an. Es ist Ihnen aber freigestellt, wie Sie die Informationen visualisieren möchten.

Die Anwendungen FOCA und Maltego CE, welche im zweiten Teil der Laborübung benötigt werden, werden Ihnen auf einer virtuellen Maschine zur Verfügung gestellt.



Die Maltego-Version in der 50GB Installation funktioniert leider so nicht. Sie können entweder das Tool selbst installieren, oder die neue bereitgestellte VM verwenden.

2 Was wir heute lernen

Der vorliegende Laborversuch deckt primär die Themen rund um die Phase «Aufklärung» der «Zero-Entry-Hacking»-Methodik ab. Es wird dabei das Thema der Informationsbeschaffung & -strukturierung behandelt. Das Ziel für die Studierenden ist dabei, sich mit den Möglichkeiten der Informationsbeschaffung auseinander zu setzen. Neben der Informationsbeschaffung wird ebenfalls erlernt, wie diese Informationen visualisiert und interpretiert werden können.

Während in einem ersten Teil nach personenbezogenen Informationen gesucht werden, steht im zweiten Teil der Übung die Analyse von Unternehmensinformationen im Fokus.

Im Laborumfeld wird hierfür die Hochschule Luzern als entsprechendes Ziel / Unternehmen verwendet.

¹ Verfügbar unter: <http://www.xmind.net/de/>

3 Information Gathering – Eigene Persönlichkeit

In dieser Übung sollen Sie sich bewusst werden, welches Wissen über eine Persönlichkeit mittels öffentlich (oder zumindest kostenlos) verfügbaren Informationen eruiert werden kann. Ausserdem soll durch die Erarbeitung dieses Wissens, «Awareness» in Bezug auf das eigene Verhalten erzeugt werden.

Ziel ist es, möglichst viele wertvolle Informationen zum Laborpartner über öffentliche Informationsquellen zu erfahren und diese aufzuzeigen. Der Einsatz von speziellen OSINT-Tools ist nicht vorgesehen, kann aber bei Bedarf additiv verwendet werden.



Fragen Sie zuerst ihren Laborpartner um Einverständnis und klären Sie den Rahmen der Erlaubnis ab. Ohne Einverständnis oder wenn Sie einzeln Arbeiten, nehmen Sie an, Ihr Laborpartner wäre «Bernhard Hämmerli» und führen die Schritte entsprechend durch.



Der Einsatz von Google Search Operators kann Ihnen helfen, einfacher an Informationen zu gelangen. Sehen Sie sich deshalb diese Operatoren unter dem Link http://www.googleguide.com/advanced_operators_reference.html genau an.

3.1 Informationsbeschaffung /-gestaltung

Bevor Sie mit der eigentlichen Recherchetätigkeit starten, sollten Sie sich Gedanken zum Vorgehen und den möglichen Informationen machen. Eine gute Vorbereitung hilft strukturiert vorzugehen und den Fokus nicht zu verlieren!

3.1.1 Informationsquellen



Welche Informationen könnten über Ihren Laborpartner in öffentlichen Quellen gefunden werden und welche Darstellungsform würde sich für die Informationsbeschaffung anbieten? Sammeln Sie Ihre Ideen in einem separaten Dokument.

.....

.....

.....

.....

.....


.....

.....



Bedenken Sie, dass auch eine eher unwahrscheinliche Quelle trotzdem wertvolle Informationen liefern kann und beschränken Sie sich daher nicht nur auf die offensichtlichen Punkte.

3.1.2 Datenanspruch

-  Welche Ansprüche / Anforderungen müssen Sie an die gesammelten Informationen stellen, damit Sie diese weiterverarbeiten können?
Gehen Sie von einem generellen Motiv aus, d.h.: Suche nach möglichst vielen Informationen.

.....

.....

.....


.....

.....

.....

.....

3.1.3 Datenbeschaffung


-  Der nächste Schritt besteht darin, die Informationen zum Laborpartner zu suchen. Ziehen Sie hierbei die möglichen Informationsquellen aus dem Anhang «Anhang A – Mögliche Informationsquellen» bei. Weitere Quellen können nach Belieben verwendet werden. Strukturieren Sie die Daten schon bei der Beschaffung anhand ihrer oben überlegten Darstellungsform.

3.2 Informationsverarbeitung

Dieser Übungsteil befasst sich mit der Verarbeitung der gewonnenen Informationen und wie diese interpretiert werden können.


3.2.1 Datenrepräsentation

Nach der Informationsbeschaffung stellt sich häufig die Herausforderung, die eruierten Informationen entsprechend zu visualisieren. Verfeinern Sie hier Ihre vorher erarbeitete Struktur, indem Sie Ihrer Meinung nach wichtige Informationen hervorheben und Zusammenhänge aufzeigen.

-  Versuchen Sie innerhalb von max. 20min die Daten **im separaten Dokument** aufzubereiten. Laden Sie dieses Dokument zusätzlich zur Abgabe auf Ilias hoch (z.B. in einem Zip File).

3.2.2 Datenanalyse /-interpretation

Nach der Informationsaufbereitung sollten Sie in der Lage sein, die wichtigsten Informationen bzw. die persönlich interessantesten Informationen innert überschaubarer Zeit zu extrahieren.

 *Lassen sich persönliche Informationen, welche von einem Angreifer ausgenutzt werden könnten, finden? Wenn ja, begründen Sie.*

.....

.....


.....

.....

.....

.....

.....

 *Aufgrund der bekannten Informationen: Welche konkreten Tipps bezüglich schützenswerter Informationen würden Sie Ihrem Laborpartner geben?*

.....

.....


.....

.....

.....

.....

.....

 *Wie schätzen Sie Ihren eigenen Online-Footprint ein? Besteht Handlungsbedarf? Wenn ja, welcher? Begründen Sie!*

.....

.....

.....

4 Information Gathering – öffentliche Personen

In diesem Kapitel einigen Sie sich in der Gruppe auf eine interessante Person des öffentlichen Lebens, und führen die Suche über diese Person durch.



Der Einsatz von Google Search Operators kann Ihnen helfen, einfacher an Informationen zu gelangen. http://www.googleguide.com/advanced_operators_reference.html

4.1 Informationsbeschaffung /-gestaltung

Bevor Sie mit der eigentlichen Recherchetätigkeit starten, sollten Sie sich Gedanken zum Vorgehen und den möglichen Informationen machen. Eine gute Vorbereitung hilft strukturiert vorzugehen und den Fokus nicht zu verlieren!

4.1.1 Informationsquellen



Welche öffentliche Person haben Sie ausgewählt?

Welche Informationen erwarten Sie zu finden und wie könnten diesen Informationen strukturiert dargestellt werden?

.....

.....

.....

.....

.....

.....

.....



Über welche Kanäle bzw. Informationsquellen können Informationen zu öffentlich aktiven Personen gefunden werden? Sehen Sie sich hierzu die in «Anhang A» aufgeführten Informationsquellen genauer an und erweitern Sie diese Auflistung, in Bezug auf Personen des öffentlichen Lebens, mit eigenen Ideen zu Informationsquellen.

.....

.....

.....

.....


.....

.....



Bedenken Sie, dass auch eine eher unwahrscheinliche Quelle trotzdem wertvolle Informationen liefern kann, und beschränken Sie sich daher nicht nur auf die offensichtlichen Punkte.

4.1.2 Datenanspruch

-  Welche Ansprüche / Anforderungen müssen Sie an die gesammelten Informationen stellen, damit Sie diese weiterverarbeiten können? Können Sie zwischen privaten und geschäftlichen Daten unterscheiden?

.....

.....


.....

.....

.....

.....

4.1.3 Datenbeschaffung


-  Suchen Sie nun Informationen zur gewählten öffentlichen Person und strukturieren Sie diese, in der vorher gewählten Darstellungsform. Ziehen Sie bei der Beschaffung die Informationsquellen aus «Anhang A», sowie Ihre selbst gewählten Informationsquellen als Hilfe bei.

4.2 Informationsverarbeitung

Dieser Übungsteil befasst sich mit der Verarbeitung der gewonnenen Informationen und wie diese interpretiert werden können.

4.2.1 Datenrepräsentation

Nach der Informationsbeschaffung stellt sich häufig die Herausforderung, die eruierten Informationen entsprechend zu visualisieren. Verfeinern Sie hier Ihre vorher erarbeitete Struktur, indem Sie Ihrer Meinung nach wichtige Informationen hervorheben und Zusammenhänge aufzeigen.

-  Versuchen Sie innerhalb von max. 20min die Daten im separaten Dokument aufzubereiten. Schenken Sie dabei vor allem auch der Unterscheidung zwischen privaten bzw. geschäftlichen Informationen Aufmerksamkeit und markieren Sie diese entsprechend. Geben Sie dieses Dokument mit ab!

4.2.2 Datenanalyse /-interpretation

Nach der Informationsaufbereitung sollten Sie in der Lage sein die wichtigsten Informationen bzw. die persönlich interessantesten Informationen innert überschaubarer Zeit zu extrahieren.



Wie beurteilen Sie die gefundenen Informationen? Inwiefern divergiert das Profil zwischen dem privaten und geschäftlichen Umfeld?

.....

.....

.....

.....

.....

.....



Lassen sich Informationen finden, welche von Angreifern ausgenutzt werden könnten? Wenn ja, welche? Begründen Sie!

.....

.....

.....

.....

.....


.....




Dieses Vorgehen wird im Falle von Social Engineering in detaillierterem Umfang verwendet. Die gefundenen Informationen helfen dabei, eventuelle Schwächen der untersuchten Person zu identifizieren, und Sie zur Herausgabe von Daten zu verlocken.

5 Information Gathering – Hochschule Luzern

Ziel in dieser Übung ist, die Hochschule Luzern in der Phase «Information Gathering» zu untersuchen. Durch diese Übung soll das Vorgehen aufgezeigt werden, wie in der Phase «Information Gathering» mögliche Schwachstellen, bzw. Angriffsoberflächen zu einer Unternehmung gesucht werden können. Ebenso werden Tools eingeführt, welche häufig in der Phase «Information Gathering» benutzt werden.

 *Der professionelle Umgang mit diesen Tools erfordert einigen Aufwand, und ist teilweise auch mit finanziellen Kosten verbunden (Lizenzen). Es wird lediglich eine Einführung in die Tools im Rahmen der kostenlos erhältlichen Tools durchgeführt. Es ist möglich, dass einige Aufgaben nicht im vorgegebenen Zeitraum detailliert lösbar sind.*


Sammeln, strukturieren und visualisieren Sie die Informationen sinnvoll in einem separaten Dokument. Es interessieren grundsätzlich sämtliche Informationen, welche für einen potenziellen Angriff verwendet werden können.

 *Beachten Sie, dass die Informationen ständigem Wandel unterliegen. Es kann sein, dass in einigen Bereichen keine aktuellen Informationen vorliegen.*

Die vorliegenden Aufgaben sind mit dem Gedanken erstellt, die vorgestellten Tools kennen zu lernen und eventuell selber einige Versuche mit diesen durchzuführen.

5.1 Webauftritt der HSLU


Durchsuchen Sie die Webseite der HSLU auf wertvolle Informationen. Verwenden Sie dazu Methoden wie «Google Hacking», also die Suche mit Google Search Operatoren. Weitere Details zu diesen finden Sie unter dem Link (http://www.googleguide.com/advanced_operators_reference.html).

 *Vergleichen Sie die Eingabe von «**jobs hslu.ch**» und «**jobs site:hslu.ch**». Wie unterscheiden sich die Suchergebnisse?*

.....

.....

.....

 *Welche weiteren Google Operatoren lassen sich finden? Testen Sie zwei weitere, welche im Zusammenhang mit dem Webauftritt der HSLU Sinn ergeben und dokumentieren Sie diese hier.*


.....

.....

.....

.....

.....

-  Suchen Sie nach Stelleninseraten der HSLU. Welche Informationen finden Sie darin? Legen Sie besonderes Augenmerk auf Kontaktinformationen und Qualifikationsprofil/Anforderungen (bspw. eingesetzte Technologie-Kenntnisse).


.....

.....

.....

.....

.....

-  Durch die Analyse von Stelleninseraten können wertvolle Informationen, wie beispielsweise verwendete Produkte, eingesetzte Technologien und Verantwortliche gefunden werden. Im Falle der Übung erhalten Sie eine Momentaufnahme, die eventuell keine Informationen preisgeben. Denken Sie daher daran, dass bei einem gezielten Angriff sämtliche Informationen über längere Zeit verglichen werden.

5.2 Social Media Auftritt der HSLU

Analysieren Sie die Social Media Auftritte der HSLU.

-  Wie ist der Auftritt der HSLU auf Social Media Portalen gestaltet? Durchsuchen Sie hierfür Facebook, Twitter, LinkedIn, und weitere Social Media Plattformen. Analysieren Sie, welche Social Media Profile der HSLU welche Informationen besitzen.

.....

.....

.....

.....

.....


.....

.....

.....

.....

Sammeln Sie die Informationen aus Beiträgen, Veranstaltungen, Jobprofilen und weiteren Inhalten und dokumentieren Sie diese Informationen kurz in der von Ihnen gewählten Darstellungsform. Legen Sie dabei speziell Wert auf Informationen, welche für einen Angriff interessant sein könnten (z.B. Mail-Adressen, Telefonnummern, Aktivitäten, Veranstaltungen, ...)

 Für welche spezielle Angriffsmethode eignen sich vor allem Informationen aus Sozialen Medien und wieso?

.....

.....


.....

.....

.....

.....

5.3 Technische Analyse der HSLU

 Als Erinnerung: Der professionelle Umgang mit diesen Tools erfordert einigen Aufwand, und ist teilweise auch mit finanziellen Kosten verbunden (Lizenzen). Es wird lediglich eine Einführung in die Tools im Rahmen der kostenlos erhältlichen Tools durchgeführt. Es ist möglich, dass einige Aufgaben nicht im vorgegebenen Zeitraum detailliert lösbar sind.

Wenn bestimmte Teile auf Grund technischer Beschränkungen nicht lösbar sind, dokumentieren Sie dies bitte.


In diesem Kapitel wird die Webseite der HSLU erneut (siehe Kapitel 5.1) analysiert. Diesmal kommen neben den in der vorhergehenden Übung besprochenen Google Operatoren auch die Werkzeuge FOCA, Shodan.io und Maltego CE zum Einsatz.

Bitte laden Sie eine neue VM hierfür:

<https://filesender.switch.ch/filesender2/?s=download&token=4562d9a9-cd81-4928-9dab-9a54d80140cf>

5.3.1 Google Direktiven und GHDB

Wie in der oberen Übung verwenden Sie auch hier wieder Google Search Operatoren. Studieren Sie diese nochmals unter http://www.googleguide.com/advanced_operators_reference.html

 Stellen Sie eine Suche zusammen, die auf der Webseite «hslu.ch» nach den Dokumenttypen von PDF; Word und Excel-Dokumenten sucht. Die Zusammenstellung muss nicht abschliessend sein, und dient lediglich des Vergleichs.

.....

.....


.....

.....

.....

Die Direktiven erlauben auch die Suche nach spezifischen Geräten / Dokumenten etc. Die Google Hacking Database (GHDB) unterhält dabei eine Vielzahl von spezifischen Direktiven: <https://www.exploit-db.com/google-hacking-database/>

Auf der Webseite der GHDB können Sie die Suchoperationen finden, jedoch nicht direkt anwenden. Für die Anwendung müssen Sie die Operation direkt in die Google Suchmaschine eingeben.

 *Sehen Sie sich die verschiedene Kategorien der GHDB an: Aus welchen Kategorien können Sie relativ schnell einen potenziellen Angriff vorbereiten?*

.....

.....

.....


.....

.....

5.3.2 FOCA

Mit FOCA durchsuchen wir die Webseite der HSLU und deren verwandte Webseiten nach nützlichen Informationen wie IP-Adressen, Domains, Dokumenten, Benutzernamen, eingesetzten Software usw.

Studieren Sie Anhang B der das FOCA GUI erklärt.

 *Können Inventarisierungstools wie FOCA von den Webseitenbetreibern erkannt werden und wenn ja, wie?*

.....

.....

.....

.....

Erstellen Sie ein neues Projekt und fügen Sie die Domain «hslu.ch» als ‘Domain website’ ein. Wechseln Sie zu den Metadaten.

Die Suche und der Download der Dokumente dauert relativ lange. Um Zeit zu sparen und die HSLU Webseite nicht übermässig zu strapazieren, wurden die zu findenden Dateien vor kurzem vom Labor Team heruntergeladen und auf dem Desktop Ihrer VM platziert. Folgende Parameter waren bei der Suche angewählt.

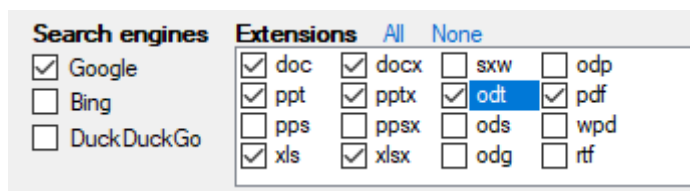



Abbildung 1: FOCA: auszuwählende Dateieindungen

Um an die Metadaten der gefundenen Dokumente zu gelangen, müssen Sie diese zuerst importieren. Ziehen den Ordner auf Ihrem Desktop in die Applikation und extrahieren Sie die Metadaten mittels Kontextmenüpunkt. Als nächstes analysieren Sie die Daten über das gleiche Kontextmenü.

 Sehen Sie sich die Metadaten an. An welche verschiedenen Informationen sind sie dadurch gekommen?

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Als nächstes Starten Sie eine Suche im Network-Menu. Benutzen Sie hierfür die Websearch. Aus zeitlichen Gründen verzichten wir darauf, die Findings mit Informationen von Robtex und Shodan.io anzureichern. Verwenden Sie die folgenden Einstellungen. Achtung: Bei sehr vielen Request kann Google die Anfragen blockieren, vor allem wenn dies aus dem HSLU Netz ausgeführt wird. Hier einfach später probieren, oder einen anderen Dienst auswählen.

Select search type

☒ WebSearch
Using a web searcher like Google or Bing the program searches for links pointing to the domain site to identify new subdomains.

Google Web limitations
-Max 1000 results for each search
-Max 32 words in a search string

☒ Google
☐ DuckDuckGo
☐ Bing

☒ Dictionary Search
The program uses a common DNS names list to find new subdomains.

Abbildung 2: Einstellungen FOCA Network Search



Wie verändern sich die Informationen durch die Network-Suche? Was ist neu hinzugekommen?

.....

.....

.....

.....

.....

.....



Analysieren Sie nun die gefundenen Daten der Network-Suche. Welche gefundenen Informationen finden Sie besonders interessant, um einen Angriff zu planen?

.....

.....

.....

.....

.....

.....

Dokumentieren Sie die Ergebnisse und werten Sie diese aus (Eingesetzte Tools, Häufigkeit und Zeitraum des Einsatzes, Autoren, etc...).

5.3.3 Shodan.io und Censys.io


Shodan.io ist eine Search Engine, welche anders als Google und Co. nicht nach Daten auf Webseiten sucht, sondern das Internet abscannt und die resultierenden Banner für die Suche in einer Datenbank indexiert. Unter einem Banner werden jene Metadaten verstanden, welche vom Server an den Aufrufer zurückgesendet werden und Informationen über die laufenden Services, Betriebssysteme und deren Versionen enthalten. Dadurch können mit Shodan.io spezifische Nodes (Desktops, Server, Router, Switches, etc...), welche direkt aus dem Internet ansprechbar sind, gefunden werden.

Leider ist Shodan kostenpflichtig für eine vernünftige Suche geworden. Hinweise zur alten Oberfläche von Shodan.io finden Sie im Anhang C.


Eine in der kostenlosen Variante sehr interessante Alternative ist Censys.io unter <https://search.censys.io/>



Sinnvollerweise verlässt sich ein Angreifer niemals auf eine einzige Quelle. Ein Abgleich mit anderen gefundenen Informationen lässt oft neue Verknüpfungen zu.

 *Recherchieren Sie, wie Shodan.io oder Censys.io funktioniert und probieren Sie die Webseiten aus.*

Starten Sie in Shodan.io und Censys.io eine Suche eine Suche nach der Domain «hslu.ch» und vergleichen Sie die gefundenen Resultate auch mit denen von FOCA.

 *Welcher Dienst liefert mehr Informationen? Welche Art von Informationen lassen sich finden?*

.....

.....

.....

.....

.....

.....

.....

.....

.....

Sehen Sie sich die Suchergebnisse von Censys.io im Detail an, ggfs. beschränkt auf eine IP Adresse. Dokumentieren Sie die gefundenen Ergebnisse. Legen Sie Wert auf folgende Punkte:

- *Aktive Services*
- *Protokoll-Versionen*
- *Verwendete Technologien*
- *Zertifikatdetails*
- *ISP-Informationen*


[illegible]

5.3.4 Maltego CE

Mit Maltego CE (Community Edition) werden nun zusätzliche Informationen gesucht und in grafischer Form dargestellt. Verwenden Sie die Community Edition (gratis erhältlich: <https://www.maltego.com/downloads/>). Maltego CE unterstützt die Transformation von bis zu 12 Resultaten. Hinweise zur Oberfläche von Maltego CE finden Sie im Anhang D.

Maltego CE benötigt für die Nutzung einen Account, den Sie sich auf der Website erstellen können. Wir haben einmalig einen shared HSLU-Account erstellt, dieser funktioniert so lange wie Sie verantwortungsvoll damit umgehen. (Nutzer: hans.muster.hslu@gmail.com PW: Ha3cK1ng.HS17).

Starten Sie Maltego CE und melden Sie sich an. Schliessen Sie die geöffneten Start-Fenster in Maltego CE, so dass Sie den «Transform Hub» sehen. Der Transform Hub ist eine Sammlung von Erweiterungen, die Sie direkt aus Maltego CE installieren und nutzen können.


 Starten Sie nun einen neuen Graph indem Sie links oben auf den Kreis klicken und «New» auswählen. Schaffen Sie sich eine Übersicht über die «Entity Palette» (linke Seite) und notieren Sie sich mindestens 3 Paletten, welche interessante Informationen für einen Angriff liefern könnten.

.....

.....

.....

.....

 Starten Sie eine Transformation für die Domain «hslu.ch». Ziehen Sie dazu die Entity «Domain» in den Graphen und editieren Sie diese. Starten Sie dann die Transformation «TO Domain (Find other TLDs) mit einem Rechtsklick auf die Entität. Welche Ergebnisse liefert die Transformation?

.....

.....

.....

.....

Die Ergebnisse können unterschiedlich angeordnet werden. Im Menüpunkt «View» können Sie die Ansicht ändern. Wählen Sie dazu die eben erstellten Ergebnisse aus, und schauen Sie sich die unterschiedlichen Optionen an.

- Verwandte TLDs
- Welche Mail-Server verwenden die HSLU-Mailserver
- E-Mail-Adressen der Domain
- Telefon-Nummern
- Server Technologie
- Übersicht der IP-Adressen

[illegible]

Notizen

[illegible]

[illegible]

6 Anhänge

6.1 Anhang A – Mögliche Informationsquellen

Die folgende Auflistung zeigt mögliche Informationsquellen für die Eruiierung von Informationen in der Phase «Aufklärung». Es handelt sich dabei um keine abschliessende oder vollständig korrekte Auflistung und kann bei Bedarf ergänzt werden. Aufgrund der grösseren Informationsbasis wird empfohlen, die Notizen / Erkenntnisse in einem separaten Dokument / Notizbuch festzuhalten.

6.1.1 Vorwissen zur Zielperson

In einem ersten Schritt soll das bekannte Vorwissen zur Zielperson schriftlich festgehalten sein. Das Vorwissen ist nicht immer in gleicher Ausprägung gegeben:

Das Vorwissen kann bspw. vollständiger Name, Wohnort, Telefonnummer, Email-Adresse, bestimmte Hobbies, Fotos etc. sein und soll in digitaler Form festgehalten werden.

6.1.2 Social Networks – erste Anlaufstelle für persönliche Informationen

Bitte beachten Sie, dass der Zugriff auf ein Social Media Profil unter Umständen durch die Zielperson zurückverfolgt werden kann und daher grundsätzlich mit direkt öffentlichen Informationen oder mittels Fake-Profilen auf die Zielperson zugegriffen wird. (Reminder: Oberstes Ziel bei Phase «Aufklärung»!).

Notieren Sie sich zu den untenstehenden Profilen immer folgende Informationen:

- URL auf Profil
- Benutzername / Pseudonym
- Wichtigkeit / Relevanz des Profils und der gefundenen Informationen
- Festhalten der Inhalte durch PrintScreen, da die Inhalte ggf. später nicht mehr verfügbar sind

6.1.2.1 Facebook

Facebook ist immer noch eine der populärsten Social Media Plattform und u.U. hat die Zielperson ein Profil auf der genannten Plattform.

6.1.2.2 Instagram

Die meisten Beiträge werden mittels Geo-Tagging hochgeladen und ein Instagram-Profil ist standardmässig offen bzw. öffentlich zugänglich. Dies bietet Informationspotenzial. In den meisten Fällen wird Instagram mit dem Facebook-Account verlinkt, weshalb meistens schnell das dazugehörige Profil gefunden wird.

Vorgehen:

1. Auf Instagram mittels Facebook-Login aus Liste einloggen
2. Profilinformationen zu Zielperson eruiieren
3. Bilder auf Geotagging überprüfen und thematische, inhaltliche Bilder eruiieren (zeigt ebenfalls Interessen auf)
 - a. Notieren Sie sich die thematischen Hintergründe der Bilder (z.B. Hobbies)
 - b. Notieren Sie sich die Standorte der Bilder und den Inhalt des Bildes
 - i. Können Sie ggf. erkennen, wo sich die Person für welche Aktivität aufhält?
 - ii. Sind auf den Bildern noch andere Personen «getaggt» / verlinkt? Welchen Bezug hat die verlinkte Person zur Zielperson?

Advanced (optional):

Aktuell sind Online nur beschränkt bzw. keine grafischen Tools vorhanden, um anhand eines spezifischen Users die Geolocation-Daten der Bilder auf Instagram aufzubereiten und in einer Map darzustellen:

1. Konsultiere die Instagram API und beachten Sie ebenfalls die Limitierungen/Restriktionen
2. Entwickeln Sie eine simple Webseite, welche die Geodaten der Instagram-Bilder auf einer Map (Google, Bing, etc.) anzeigt.
3. Interpretieren Sie erhaltenen Daten und notieren Sie Ihre Erkenntnisse

Tipp zu Punkt 2: Ein Ansatz für die Erstellung mit PHP:

<https://shareurcodes.com/blog/instagram%20user%20image%20fetcher%20in%20php>

6.1.2.3 Twitter

Twitter wird als äusserst informative Datenbasis gesehen, dass v.a. weil die zur Verfügung gestellten Information meistens mit Geodaten angereichert sind und so interessant herauszufinden, wo genau Twitter Nachrichten gesendet werden. Dies ermöglicht z.B. den Rückschluss, wo eine Person wohnt und/oder arbeitet (Anzahl Tweets)

- Geo-Daten anhand User
- Inhalt der Tweets und die thematischen Followers verrät Interessen

Vorgehen:

- Auf Twitter mittels eigenem oder «Fake»-Profile einloggen/registrieren
- Über <https://tinfoleak.com/> eine graphische Aufbereitung der vorhandenen Tweets ausführen und die möglichen «Hotspots» eruieren. Es besteht neben den Online-Reports auch ein Python-Script, dass auch mehrere Abfragen hintereinander zulässt.
- Tweets inhaltlich prüfen – «Interessen» erkennen und ggf. meist genutzt Hashtags in Erfahrung bringen
- Sind die Tweets mit Geo-Informationen versehen? Wenn ja, an welchen Standorten werden die meisten Tweets publiziert? Können Sie dadurch ggf. feststellen, wo die Person arbeitet / lebt?
- Followers prüfen – Notieren Sie sich dabei die thematische «Interessen» der Person

6.1.2.4 XING

Obwohl XING einen geschäftlichen Charakter aufweist, werden über XING zu einer Person folgende Informationen gerne Preis gegeben:

- Arbeitgeber und Ausbildung
- Fachliche Interessen / Zertifizierungen / Forenbeiträge
- (geschäftliche) Kontaktdaten
- Organigramm

Vorgehen:

1. Auf XING <https://www.xing.com> mittels eigenem oder HSLU-Profil einloggen/registrieren

2. Personensuche über die XING Suche starten

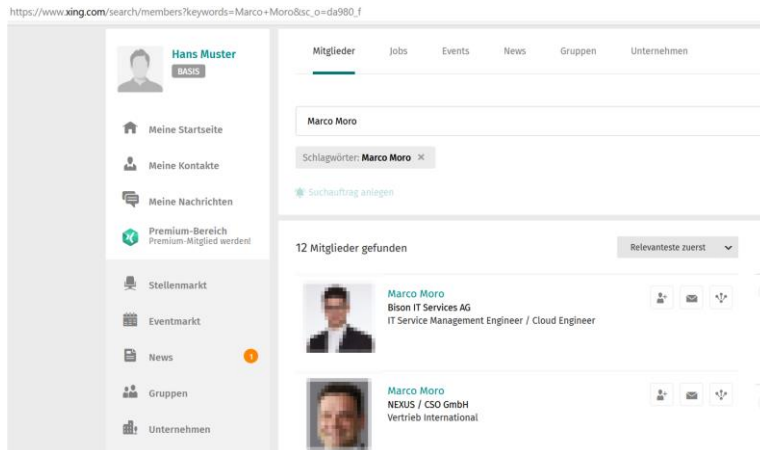


Abbildung 3: XING – Einsatz Personensuche

3. Direkte Informationen aus Profilseite entnehmen (Sektionen «Ich suche/biete», «Arbeitgeber», «Ausbildung»/»Qualifikationen».

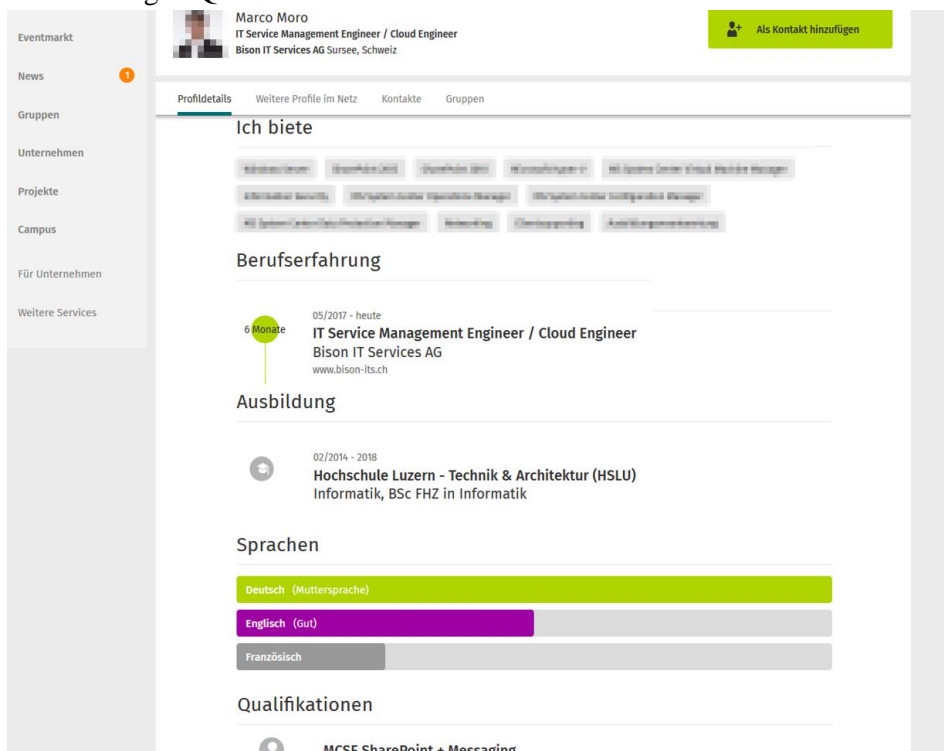


Abbildung 4: XING – Persönliches Profil als CV

Beachten Sie auch die Informationen unter «Weitere Profile im Netz», «Gruppen». Unter Gruppen können die thematischen Interessen der Person eruiert werden. Prüfen Sie ebenfalls, ob der Benutzer in den Gruppen aktiv ist. Wenn ja, zu welchen konkreten Themen äussert sich die Person in den Gruppen. Sie können hierzu in den Gruppen einfach nach der Person suchen.

4. Falls die Person nicht gefunden werden kann und das Unternehmung bekannt ist, so kann über Unternehmensprofil die Mitarbeiterliste überprüft werden:

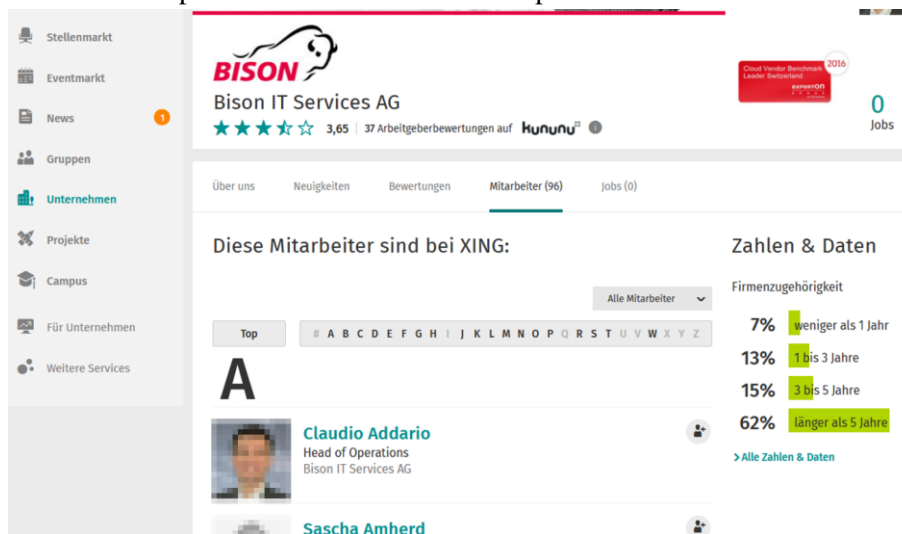


Abbildung 5: XING People Search by Company

5. Geschäftliche Kontakte geben ggf. auch Aufschluss über aktuelle / frühere Arbeitgeber, indem unter «Kontakte» die Häufigkeit der unternehmerischen Zugehörigkeit der Kontakte betrachtet wird.
 - a. Sind sowohl aktuelle Firma und Kontakte bekannt, so kann geprüft werden, ob ggf. Teamkollegen (siehe hierzu Jobbezeichnung) bekannt sind.

6.1.2.5 LinkedIn

Analog zu XING ist LinkedIn auf einen geschäftlichen Fokus ausgelegt, jedoch eher auf internationaler Ebene. Die möglichen Informationen sind daher gleich wie bei XING. Das Vorgehen ist dabei ebenfalls gleich gestaltet.

Vorgehen:

1. Auf LinkedIn <https://www.linkedin.com> mittels eigenem oder HSLU-Profil einloggen/registrieren
2. Personensuche über die LinkedIn Suche starten

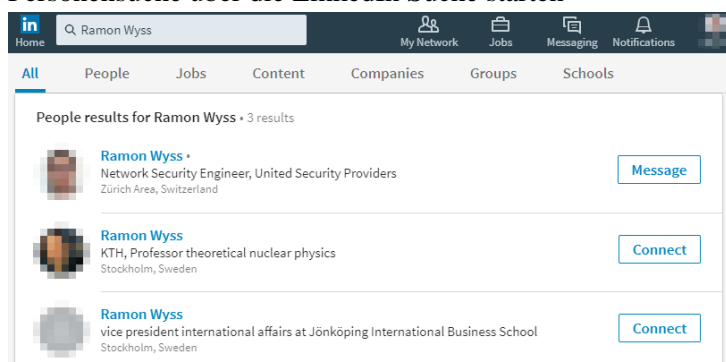


Abbildung 6: LinkedIn People Search

3. Direkte Informationen aus Profilsseite entnehmen (Sektionen «Experience», «Skills / Accomplishments» und v.a. «Interests»)

4. Falls die Person nicht gefunden werden kann und das Unternehmen bekannt ist, so kann ggf. über Unternehmensprofil die Mitarbeiterliste überprüft werden:
Hierzu nach Firma suchen und über Link «View all employees» die Auflistung erhalten:

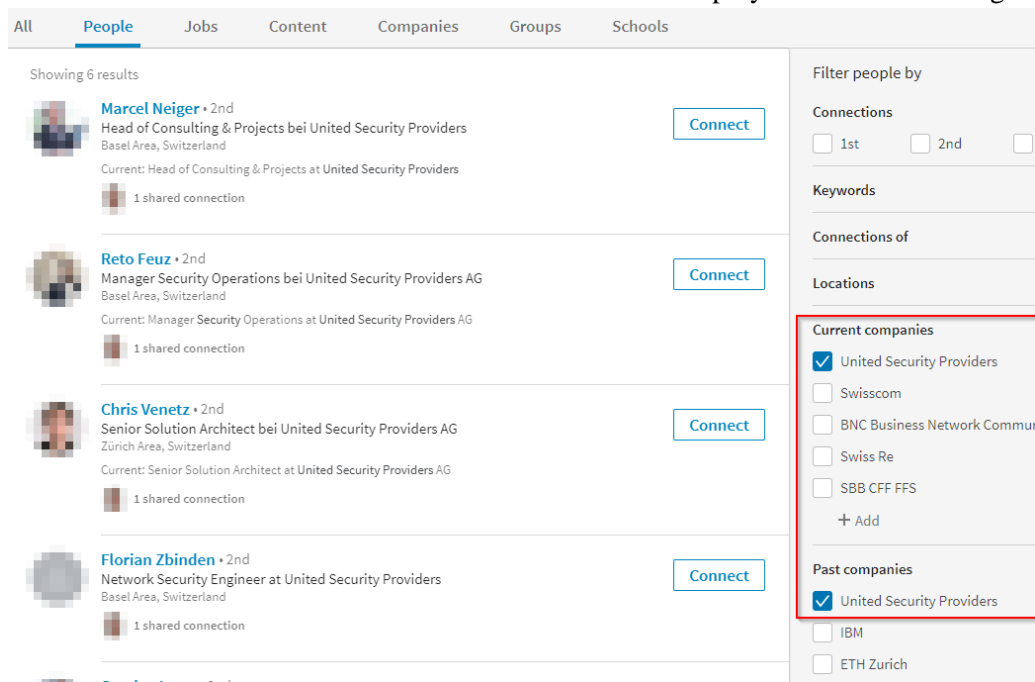


Abbildung 7: LinkedIn People Search by Company

5. In den Filtermöglichkeiten kann auch nach Mitarbeitern gefiltert werden, welche früher beim genannten Arbeitgeber tätig war und ggf. im gleichen Team wie die Zielperson gearbeitet hat.
6. Anhand der Jobbezeichnung können ggf. Teamkollegen eruiert werden.

6.1.3 Persönliche Webseite / Blog

Unter Umständen besitzt die Zielperson eine persönliche Webseite und/oder Blog und bietet Informationen aus erster Hand. Auch die Tatsache, dass einmal ein Blog oder Webseite existierte, kann interessante Informationen liefern.

Vorgehen:

1. Suchen Sie über Google nach einer möglichen Webseite der Person mittels simpler Suche nach dem Namen der Person
2. Hat die Person eine persönliche Webseite, so kann über eine WHOIS-Abfrage Details zur Person (z.B. Wohnort, Adresse) erlangt werden. Einige Personen präsentieren sich auf der Webseite unter «Über mich» / «About me» oder «Kontakt»
3. Ist bekannt, dass die Person eine Webseite hatte oder ggf. früher weitere Informationen auf der Webseite publizierte, so kann über die «Internet Archive Wayback Machine» <https://archive.org/web> über die URL der Webseite, die Webseite zu früheren Zeitpunkten betrachtet werden.

4. Mittels der Google-Suchdirektive `inurl` / `intitle` können bspw. auch Blogs gefunden werden. Konkret kann z.B. nach `<vorname nachname inurl:blog>` gesucht werden:

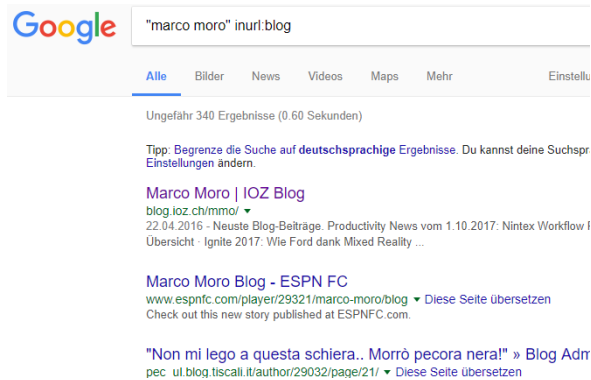


Abbildung 8: inurl Google Search

5. Für die `intitle`-Suche empfiehlt es sich auch die bekannten «Benutzernamen / Pseudonyme der Zielperson zu verwenden. Wenn durch die Profile der Arbeitgeber eruiert werden konnte, so findet man ggf. einen Blog des Unternehmens und ggf. auch einzelne Post pro Person. Dabei können persönliche Posts das Arbeitsgebiet der Person verraten (siehe Abbildung oben).

6.1.4 Google Suche – Korrekte Anwendung entscheidend

Machen Sie sich mit den «Google Search Operators» vertraut. Die korrekte Anwendung der grössten Suche-Engine findet Unmengen von Seiten, wenn die Suchparameter nicht zielgerichtet verwendet werden. Als Kurzübersicht dient die Webseite <https://moz.com/learn/seo/search-operators> und jene von Google selbst: <https://support.google.com/websearch/answer/2466433>.

6.1.5 Weitere Informationsquellen – OSINT Framework

Auf GitHub wird ein «OSINT Framework»² aktiv gepflegt, indem mögliche Informationsquellen zusammengetragen und aktuell gehalten werden.

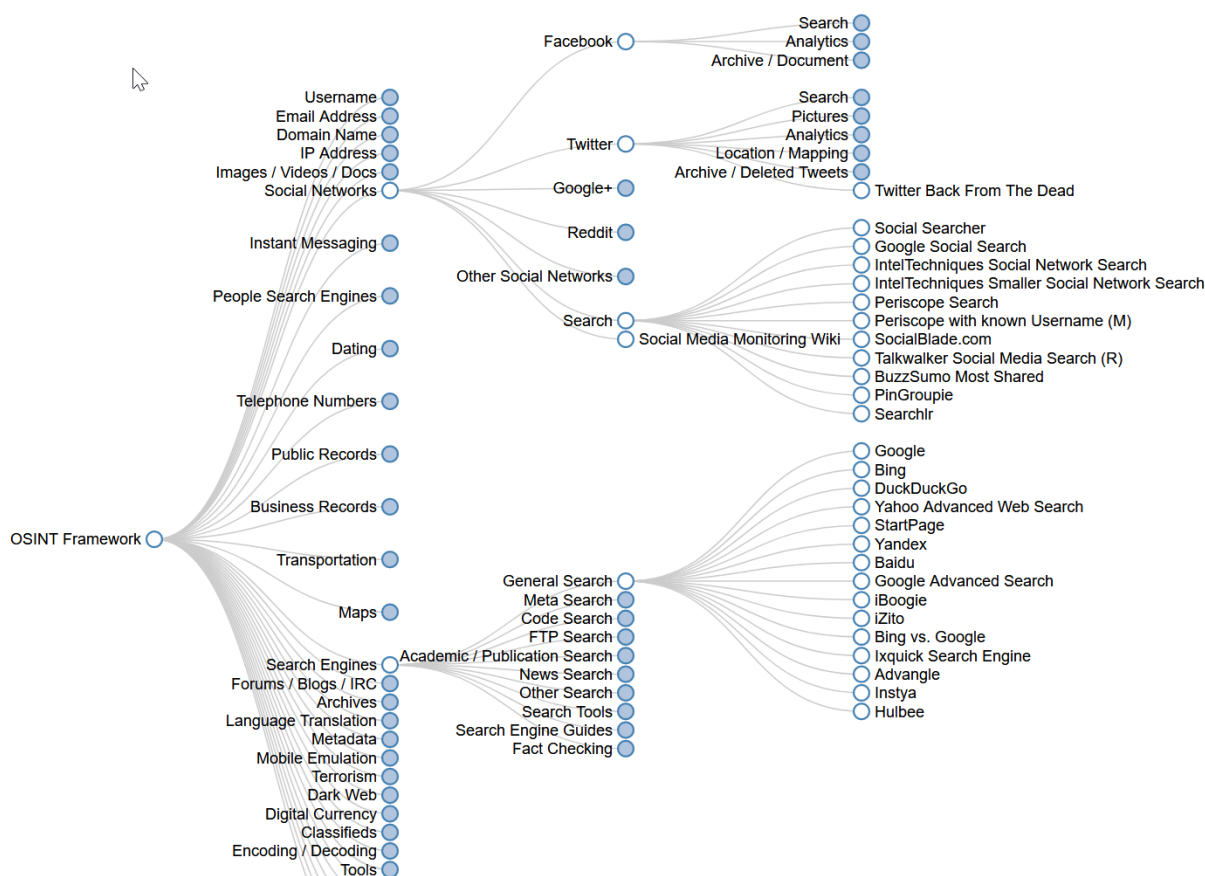


Abbildung 9: OSINT Framework

Für weitere Informationsbeschaffung eignet sich das OSINT Framework optimal und bietet zu vielen thematischen Aspekten entsprechend konkrete Hilfsmittel (Webseiten, Tools, etc.).

² Unter <http://osintframework.com/> zu finden

6.2 Anhang A – OVA Datei in VirtualBox importieren

Folgende Anleitung zeigt, wie eine OVA Datei in VirtualBox importiert werden kann.

1. Öffnen Sie über die Menüleiste Datei -> Appliance importieren ...

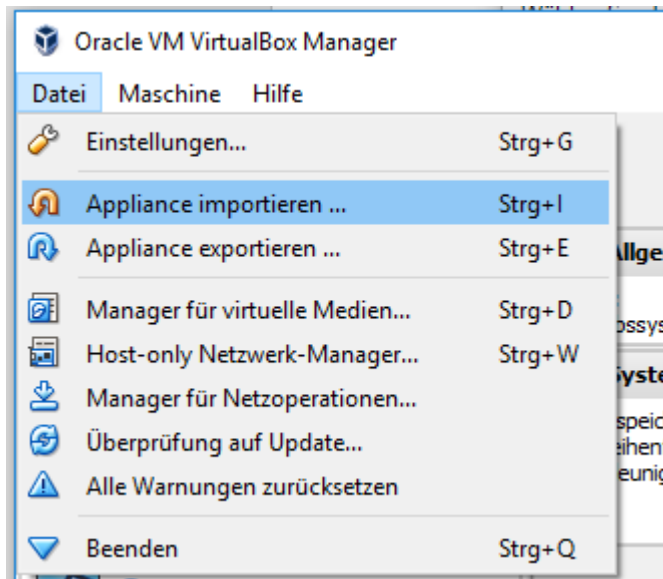


Abbildung 10: VirtualBox Appliance importieren

2. Navigieren Sie zum gewünschten OVA File und wählen Sie dieses aus.

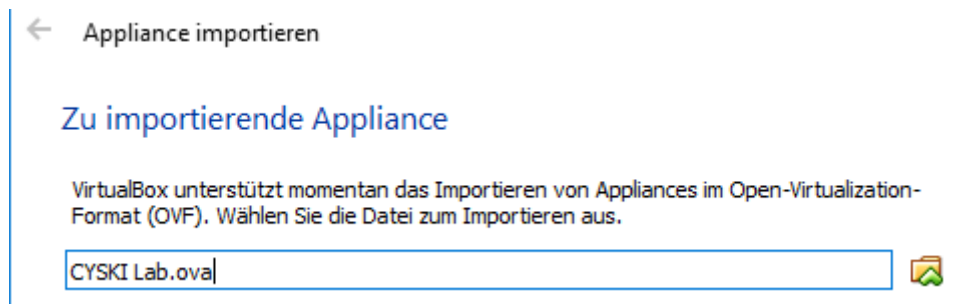








Abbildung 11: VirtualBox Appliance auswählen

3. Belassen Sie die Standardeinstellungen und importieren sie die virtuellen Maschinen. Dies kann einige Minuten dauern.

Appliance-Einstellungen

Dies sind die in der Appliance beschriebenen virtuellen Maschinen mit den entsprechenden Abbildungen für den Import in VirtualBox. Sie können Änderungen an vielen dieser Einstellungen mittels Doppelklick bzw. durch Auswahl der entsprechenden Checkbox ändern.

Virtuelles System 1	
 Name	Windows10
 Gast-Betriebssystem	 Windows 10 (64-bit)
 CPU	1
 RAM	2048 MB
 DVD-Laufwerk	<input checked="" type="checkbox"/>
 USB-Controller	<input checked="" type="checkbox"/>
 Soundkarte	<input checked="" type="checkbox"/> Intel HD Audio

☐ Zuweisen neuer MAC-Adressen für alle Netzwerkkarten

Appliance ist nicht signiert

Abbildung 12: VirtualBox Appliance-Übersicht

6.3 Anhang B – FOCA

Start-Bildschirm in FOCA eines gespeicherten und leeren Projekts.

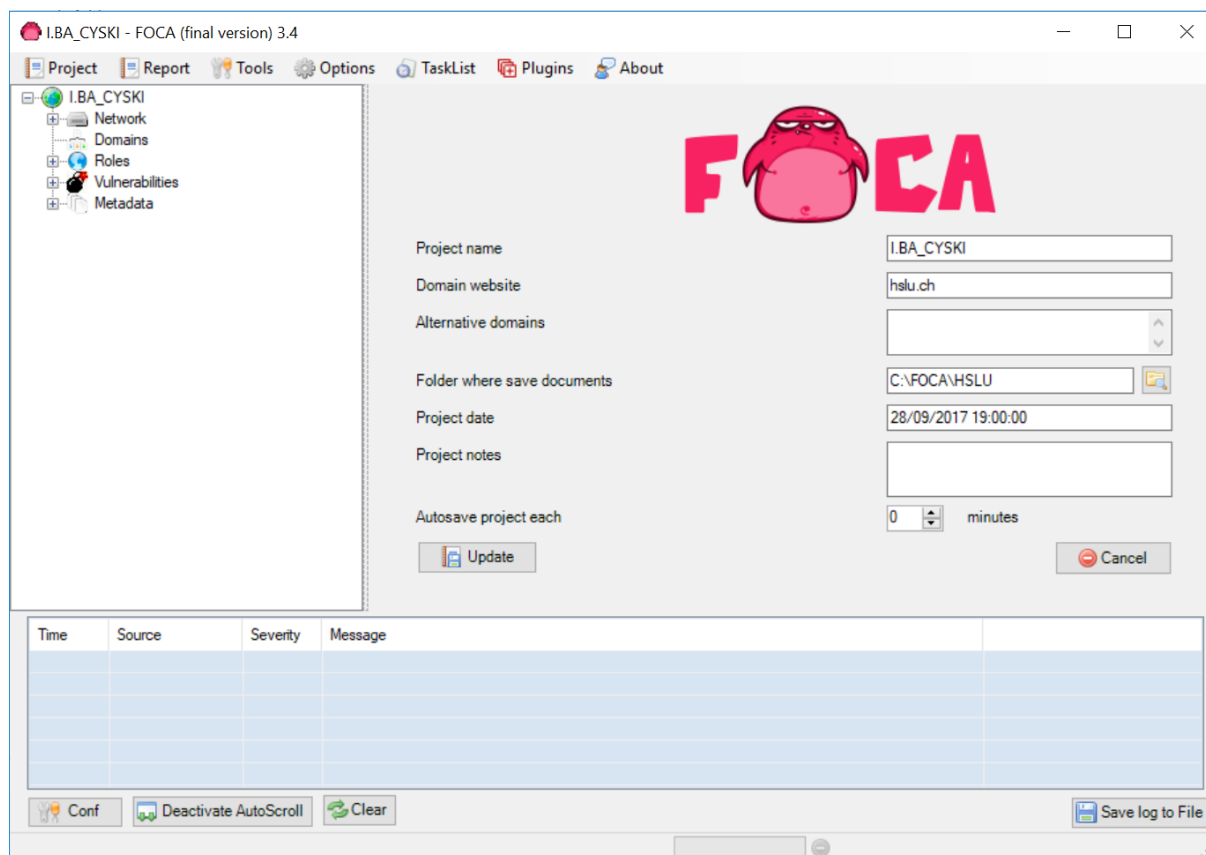


Abbildung 13: FOCA: Projektübersicht

Such-Option nach Dokumenten. Unter «Custom search» kann ein eigenes Query nach den Google Direktiven definiert werden. Für unseren Anwendungsfall reichen die bestehenden Filter.

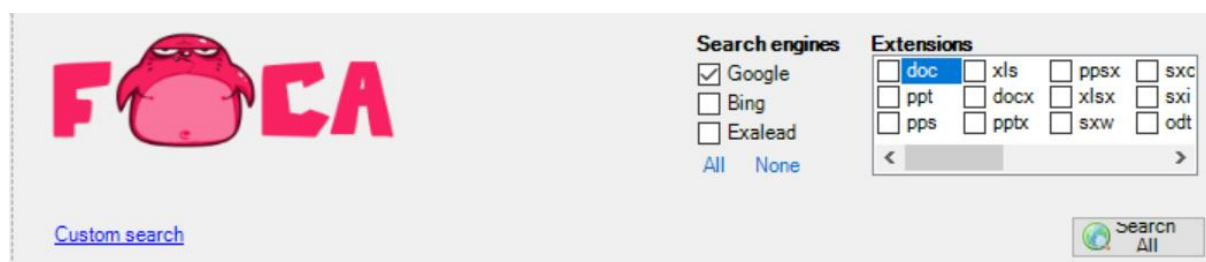


Abbildung 14: FOCA: Dokumentsuche

Prozess-Liste. Das Fuzzing sucht gleichzeitig nach unsicheren Methoden der untersuchten Domain.

Time	Source	Severity	Message
19:10:51	Fuzzer	high	Directory Listing found on https://ppdb.hslu.ch:443/images/hilfe/
19:10:51	Fuzzer	high	Insecure methods found (trace) on https://ppdb.hslu.ch:443/images/
19:10:51	Fuzzer	high	Insecure methods found (trace) on https://ppdb.hslu.ch:443/images/hilfe/

Abbildung 15: FOCA: Logeinträge anhand von Fuzzing

Detail-Informationen zu einem analysierten Dokument:

Attribute	Value
File Information	
URL	https://blog.hslu.ch/ikwerkzeugkasten/files/2012/01/zhb-info-citavineu1012061-1.doc
Local path	C:\FOCA\HSLU\zhb-info-citavineu1012061-1.doc
Download	Yes
Analyzed	Yes
Download date	28/09/2017 19:15:52
Size	465.5 KB
Users	
Username	Ursula Baumann
Username	Chrisitan Matlage
Folders	
Folder	\Zhb-vorl\
Folder	G:\Zhb-vorl\
Folder	http://www.citavi.ch/de/download/
Folder	http://www.citavi.com/
Folder	http://zhbluzem.wordpress.com/citavi-an-der-universitat-luzern/
Folder	http://zhbluzem.wordpress.com/
Folder	https://www.citavi.com/de/service/
Dates	
Creation date	07/02/2012 17:44:00
Printed date	16/05/2010 15:17:00
Modified date	07/02/2012 17:44:00
Other Metadata	
Application	Microsoft Office for Mac
Encoding	Unknown
Company	ZHB Luzern
Statistics	Pages: 4 Words: 1298 Characters: 7402 Bytes: 342016 Lines: 61 Paragraphs: 14
Revisions	2
Template	\Zhb-vorl\B_Info_A4_hoch.dot
Operating system	Mac OS
Title	Citavi Literaturverwaltungsprogramm
Software	
Microsoft Office for Mac	

Abbildung 16: FOCA: Metadatendetails zu einzeltem Dokument

Ergebnis-Liste von PDFs. Die Dokumente sind noch nicht gedownloadet und extrahiert.

site.hslu.ch filetype pdf, doc, docx, xls,xlsx							
Id	Type	URL	Download	Download Date	Size	Analyzed	Modified Date
181	pdf	https://blog.hslu.ch/ffz/files/2012/08/29_Bitterli_Sonder...	✗	-	449.47 KB	✗	-
182	pdf	https://blog.hslu.ch/holz/files/2013/06/stummat.pdf	✗	-	5.55 MB	✗	-
183	pdf	https://blog.hslu.ch/backstein2012/files/2012/03/Prod...	✗	-	3.4 MB	✗	-
184	pdf	https://blog.hslu.ch/summerschooltanzania/files/2014/0...	✗	-	309.42 KB	✗	-
185	pdf	https://blog.hslu.ch/designforschung/files/2010/01/ZH...	✗	-	-	✗	-
186	pdf	https://blog.hslu.ch/training/files/2009/09/flyer_celm_ta...	✗	-	414.89 KB	✗	-
187	pdf	https://blog.hslu.ch/ffz/files/2012/07/16_Birrer_Sonder...	✗	-	518 KB	✗	-
188	pdf	https://blog.hslu.ch/beton2014/files/2014/04/Dickhaut...	✗	-	4.9 MB	✗	-
189	pdf	https://blog.hslu.ch/ffz/files/2012/07/4_Emy_Sonderdr...	✗	-	611.43 KB	✗	-
190	pdf	https://blog.hslu.ch/ikwerkzeugkasten/files/2012/07/k...	✗	-	579.12 KB	✗	-
191	pdf	https://blog.hslu.ch/ffz/files/2012/08/14_Rupp_Kull_So...	✗	-	494.8 KB	✗	-
192	pdf	https://blog.hslu.ch/retailbanking/files/2015/04/Digitale...	✗	-	1.01 MB	✗	-
193	pdf	https://blog.hslu.ch/ffz/files/2012/06/Jusletter10310de1...	✗	-	493.96 KB	✗	-
194	pdf	https://blog.hslu.ch/product/files/2010/10/FormaleFunk...	✗	-	8.46 MB	✗	-
195	pdf	https://blog.hslu.ch/ffz/files/2010/09/Erwartungswert_T...	✗	-	39.18 KB	✗	-
196	pdf	https://blog.hslu.ch/financialmanagement/files/2017/03...	✗	-	129.49 KB	✗	-
197	pdf	https://blog.hslu.ch/ffz/files/2012/08/12_Schmidiger_S...	✗	-	290.69 KB	✗	-
198	pdf	https://blog.hslu.ch/neohslu/files/2015/01/141124_w_i...	✗	-	54.83 KB	✗	-
199	pdf	https://blog.hslu.ch/bibliothek/files/2014/11/ML_Brosc...	✗	-	1.22 MB	✗	-
200	pdf	https://blog.hslu.ch/beton2014/files/2014/04/These23...	✗	-	1.69 MB	✗	-
201	pdf	https://blog.hslu.ch/designforschung/files/2011/08/SN...	✗	-	-	✗	-
202	pdf	https://blog.hslu.ch/product/files/2014/03/Pap_MA1_2...	✗	-	4.48 MB	✗	-
203	pdf	https://blog.hslu.ch/bibliothek/files/2013/06/IDS_Info...	✗	-	405.27 KB	✗	-
204	pdf	https://blog.hslu.ch/holz/files/2013/07/Thesenpapier_0...	✗	-	1.71 MB	✗	-
205	pdf	https://blog.hslu.ch/financialmanagement/files/2017/05...	✗	-	147.44 KB	✗	-
206	pdf	https://blog.hslu.ch/klasse/files/2016/06/Fee_schedule...	✗	-	87.43 KB	✗	-
207	pdf	https://blog.hslu.ch/expandedcinema/files/2014/04/int...	✗	-	1.12 MB	✗	-
208	pdf	https://blog.hslu.ch/backstein2014/files/2014/06/Thes...	✗	-	1.64 MB	✗	-
209	pdf	https://blog.hslu.ch/beton2014/files/2014/03/Thesep...	✗	-	1.64 MB	✗	-
210	pdf	https://blog.hslu.ch/ffz/files/2011/01/IFRS_SWISSGAA...	✗	-	64.74 KB	✗	-
211	pdf	https://blog.hslu.ch/ffz/files/2011/05/273813_KPMG_Jo...	✗	-	2.22 MB	✗	-
212	pdf	https://blog.hslu.ch/madesign10/files/2010/11/Beobac...	✗	-	199.2 KB	✗	-
213	pdf	https://blog.hslu.ch/files/2010/09/110328_Best_Practic...	✗	-	201.91 KB	✗	-
214	pdf	https://blog.hslu.ch/investments/files/2017/02/Analyse...	✗	-	259.97 KB	✗	-

Abbildung 17: FOCA: Dokumentenliste

Bei analysierten Dokumenten werden die Informationen im rechten Menu aufbereitet angezeigt.

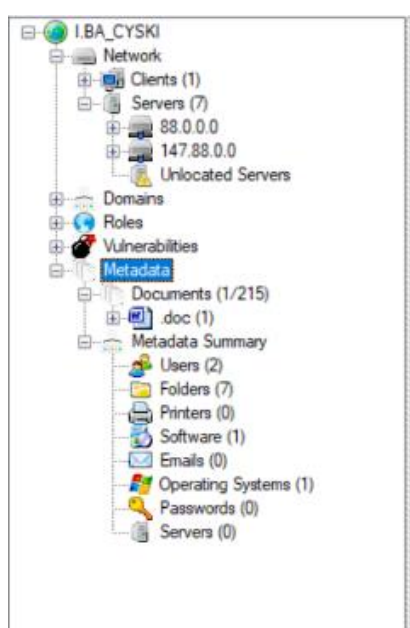


Abbildung 18: FOCA: Aggregierte Daten von Dokumenten (1 / 215 Dokumenten analysiert)

Übersicht der Network-Suche mit Einstellungsmöglichkeiten für Suchmaschinen, Host-Listen, etc...

Select search type

☒ WebSearch ☒ Also, improve results with Robtex
Using a web searcher like Google or Bing the program searches links pointing to the domain site to identify new subdomains.

Google Web limitations
-Max 1000 results for each search
-Max 32 words in a search string

☒ DNS Search ☒ ZoneTransfer
DNS Search performs queries to DNS Servers searching for well-known records. The following queries will be done:
NS, SOA, Primary, Master, MX, SPF, Domainkeys Records, DKIM Records, SRV Records for VoIP, IM and Active Directory, Kerberos, LDAP and Web Proxy Autodiscovery.

☒ Dictionary Search
The program uses a common DNS names list to find new subdomains. This list is the same used by Fierce tool.
C:\FOCA\hosts.txt

☒ IP Bing ☒ Bing Web ☐ Bing API
Bing allows search links located in a particular IP address. This functionality can be used to find domains that share IP Address.

Bing Web limitations
-Max 1000 results for each search
-Max 49 words in a search string

☒ PTR Scan
When the program discovers an IP address, it can make a reverse resolution over the entire IP range in DNS internal. Just reserve resolution contained in the domain will be added.

Current search: None

Abbildung 19: FOCA: Network-Suche Einstellungsmöglichkeiten

Die Network-Suche ermöglicht es auch, einen Dokumenten-Scan durchzuführen.

Attribute	Value
Domain - Source	
sta.hslu.ch	WebSearch
IP Addresses - Source	
147.88.201.201	WebSearch > DNS resolution [147.88.201.201]
Server Roles	
147.88.201.201	Http
147.88.201.201	Https

Technology recognition | Crawling | Exploiting | **Files** | Log

☒ Google ☒ doc ☒ pps ☒ docx ☒ ppsx ☒ sxw ☒ sxi ☒ ods

☒ Bing ☒ ppt ☒ xls ☒ pptx ☒ xlxs ☒ sxc ☒ odt ☒ odg

☒ Exalead

Finished

Domain: sta.hslu.ch

Files (1 found) | Folders (5 found) | Documents published (1 found) | Backups (0 found) | Parametrized (0 found) | S...

File	Extension
http://sta.hslu.ch/wp-content/uploads/2015/04/Antragsformular-Festbeitrag.docx	.docx

Abbildung 20: FOCA: Dokumentenscan auf einzelnen Hosts

Die Ergebnisse der Network-Suche werden direkt in einzelne Subnetzen zusammengefasst.

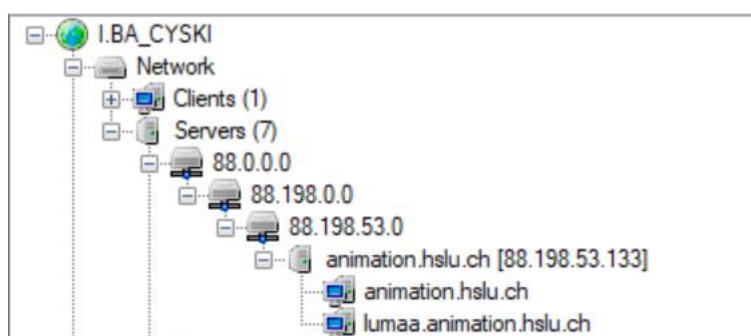


Abbildung 21: FOCA: Übersicht der gefundenen Server (unvollständig)

Analysierte E-Mail-Adressen der Dokumente, die in den Meta-Daten vorhanden sind.

Attribute	Value
All emails found (10) - Times found	
simone.rosenkranz@zhbluzern.ch	1
info@womensbusiness.ch	1
inno@zinno.ch	1
soner.yaprak@stud.hslu.ch	1
transfer.wirtschaft@hslu.ch	1
international-i@hslu.ch	3
exchange.business@hslu.ch	1
energy-systems@hslu.ch	1
roland.lymann@hslu.ch	1
international.business@hslu.ch	1

Abbildung 22: FOCA: Aggregierte Metadaten der Mail-Adressen

Verwendete Betriebssysteme anhand der Metadaten der Dokumente

Attribute	Value
All operating systems found (3) - Times found	
Mac OS	2
Windows XP	3
Windows 7	38

Abbildung 23: FOCA: Aggregierte Metadaten der Betriebssysteme

FOCA-Options zum Konfigurieren eines Proxys. Der Custom User Agent sollte, wenn möglich, auch auf einen «gültigen User Agent» gesetzt werden. Moderne WAF's können den Zugriff von speziellen User Agents blockieren.

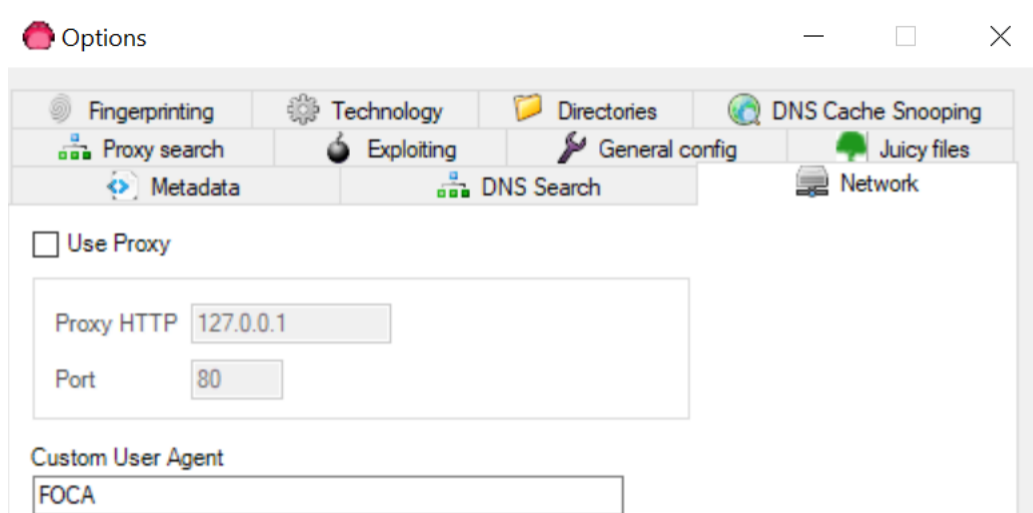


Abbildung 24: FOCA: Proxy-Einstellungsmöglichkeiten

Die User Agents sollten, wenn möglich angepasst werden. Einige Sicherheitsmechanismen filtern «unbekannte» User Agents heraus, um Automatisierung zu verhindern. User Agents können Beispielsweise hier eingesehen werden: <https://udger.com/resources/ua-list> (Stand, 23.11.2017)

6.4 Anhang C - Shodan.io

Die Suchleiste von Shodan.io. Hier können Domains, IP-Ranges, Technologien, etc. gesucht werden

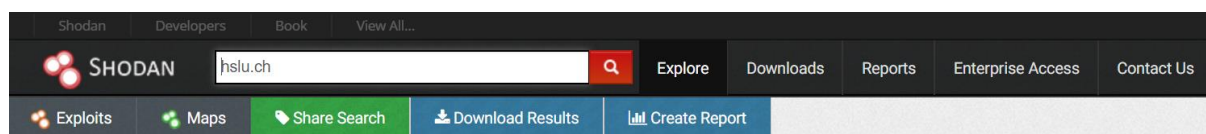


Abbildung 25: Shodan: Suchfeld

Die Übersicht der Suchanfrage bietet eine Zusammenfassung der wichtigsten Erkenntnisse.

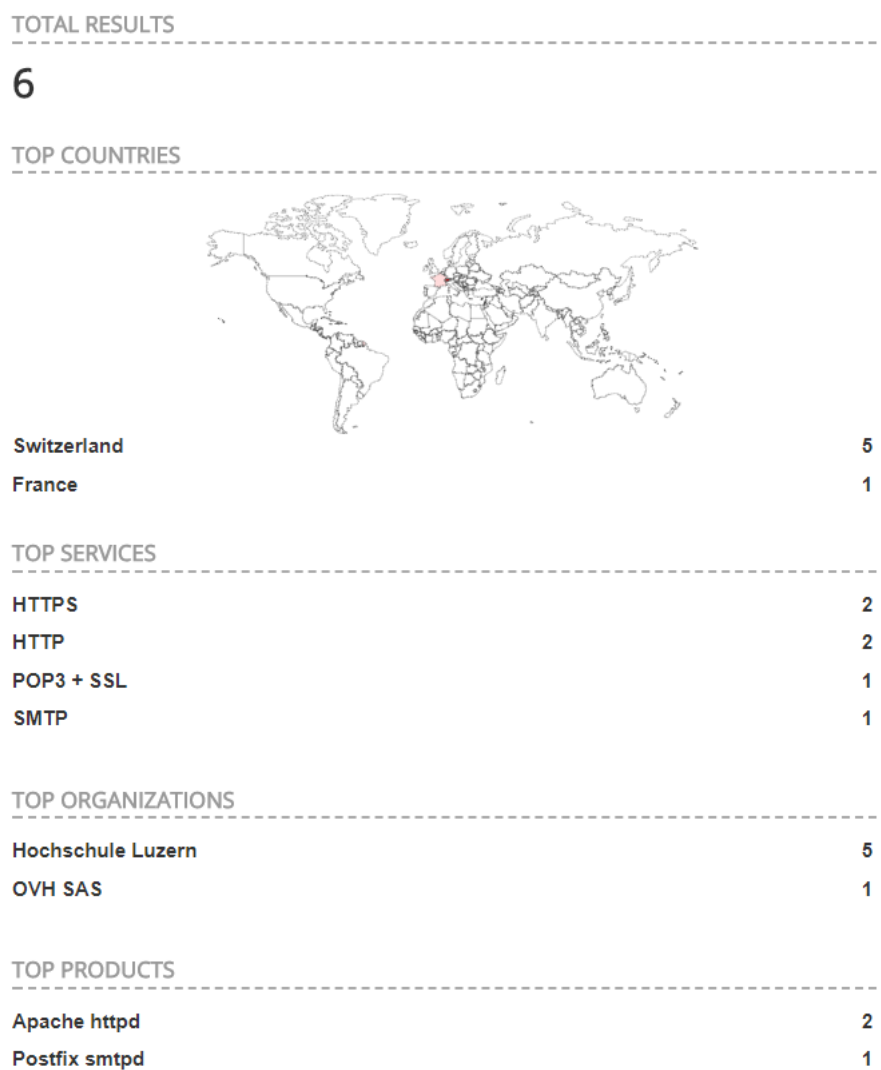


Abbildung 26: Shodan: Resultatübersicht


Ein Auszug des durchgeführten Aufrufs zeigt, wie genau der Zielserver auf die Anfrage reagiert hat. In diesem Beispiel hat der Server mit einem HTTP 301 Redirect geantwortet.

301 Moved Permanently

147.88.201.129

Hochschule Luzern

Added on 2017-09-22 03:55:20 GMT

 Switzerland, Horw

Details

HTTP/1.1 301 Moved Permanently

Date: Fri, 22 Sep 2017 03:55:13 GMT

Server: Apache

Location: <https://stage-elearning.hslu.ch/>

Content-Length: 304

Content-Type: text/html; charset=iso-8859-1


301 Moved Permanently

147.88.201.119

elearning.hslu.ch

Hochschule Luzern

Added on 2017-09-20 15:55:53 GMT

 Switzerland, Horw

Details

HTTP/1.1 301 Moved Permanently

Date: Wed, 20 Sep 2017 15:55:53 GMT

Server: Apache

Location: <https://elearning.hslu.ch/>

Content-Length: 298

Content-Type: text/html; charset=iso-8859-1

Abbildung 27: Shodan: HTTP-Antworten auf Requests


Zertifikats-Informationen wie CN, Aussteller, etc... sind ebenfalls ersichtlich.

147.88.201.201

hosting.hslu.ch

Hochschule Luzern

Added on 2017-09-14 15:52:13 GMT

 Switzerland, Horw

Details

SSL Certificate

Issued By:

| Common Name: QuoVadis Global SSL

ICA G2

| Organization: QuoVadis Limited

Issued To:

| Common Name: hosting.hslu.ch

| Organization: Hochschule Luzern

Supported SSL Versions

TLSv1, TLSv1.1, TLSv1.2

+OK Dovecot ready. <5436.1.59baa5a4.z8ggQXiaz9UYcwDXDqe0+g==@ws14.hslu.ch>

+OK

CAPA

TOP

UIDL

RESP-CODES

PIPELINING

AUTH-RESP-CODE


USER

SASL PLAIN LOGIN DIGEST-MD5 CRAM-MD5

.

Abbildung 28: Shodan: Zertifikatsinformationen

Über einige Server sind sogar GPS-Koordinaten oder ISP-Infos wie ASN-Nummern erhältlich



147.88.201.201 hosting.hslu.ch

City	Horw
Country	Switzerland
Organization	Hochschule Luzern
ISP	Hochschule Luzern
Last Update	2017-10-03T09:46:01.573439
Hostnames	hosting.hslu.ch
ASN	AS559

Web Technologies

Prototype

Abbildung 29: Shodan: Unternehmens-Informationen wie GPS; ISP, etc...

Die aufgelisteten Ports sind offen für Requests aus dem Internet. Das Beispiel zeigt eine IP-Adresse, die anscheinend für unterschiedliche Zwecke verwendet wird (FTP, SSH, HTTP, Mail, DNS)

Ports



Abbildung 30: Shodan: gefundene, offene Ports

Zusätzlich zu den Port-Informationen sind sogar noch die Produkte, bzw. die eingesetzten Protokoll-Versionen angezeigt. In diesem Falle ein ProFTPD-Server der Version 1.3.5d

Services

Port	Protocol	Service
21	tcp	ProFTPD Version: 1.3.5d
21	ftp	ProFTPD Version: 1.3.5d

```
220 ProFTPD 1.3.5d Server (ProFTPD) [147.88.201.201]
530 Login incorrect.
214-The following commands are recognized (* =>'s unimplemented):
CWD      XCWD      CDUP      XCUP      SMNT*     QUIT      PORT      PASV
EPRT     EPSV      ALLO*     RNFR      RNT0      DELE      MDTM      RMD
XRMD     MKD        XMKD     PWD       XPWD      SIZE      SYST      HELP
NOOP     FEAT       OPTS      AUTH      CCC*      CONF*     ENC*      MIC*
PBSZ     PROT       TYPE      STRU      MODE      RETR      STOR      STOU
APPE     REST      ABOR      USER     PASS      ACCT*     REIN*     LIST
NLST     STAT       SITE      MLSD      MLST
214 Direct comments to root@127.0.0.1
211-Features:
MFMT
SIZE
PROT
CCC
PBSZ
AUTH TLS
MFF modify;UNIX.group;UNIX.mode;
REST STREAM
MLST modify*;perm*;size*;type*;unique*;UNIX.group*;UNIX.mode*;UNIX.owner*;
LANG en-US.UTF-8*
UTF8
EPRT
EPSV
MDTM
SSCN
TVFS
211 End
```

Abbildung 31: Shodan: Service-Details (Port-Informationen)

Shodan.io unterstützt auch Filter, wie bspw. Netzwerk, Betriebssystem, Port, und weiteren.

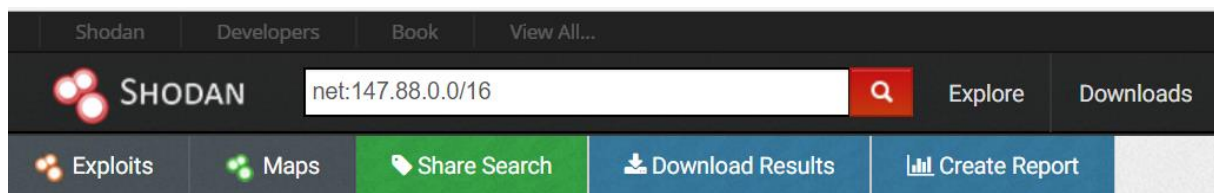


Abbildung 32: Shodan: Search Filters

6.5 Anhang D – Maltego CE

Die Ansicht des Transform Hubs als Startseite



Abbildung 33: Maltego: Transformhub

Die Konfiguration des API-Keys.

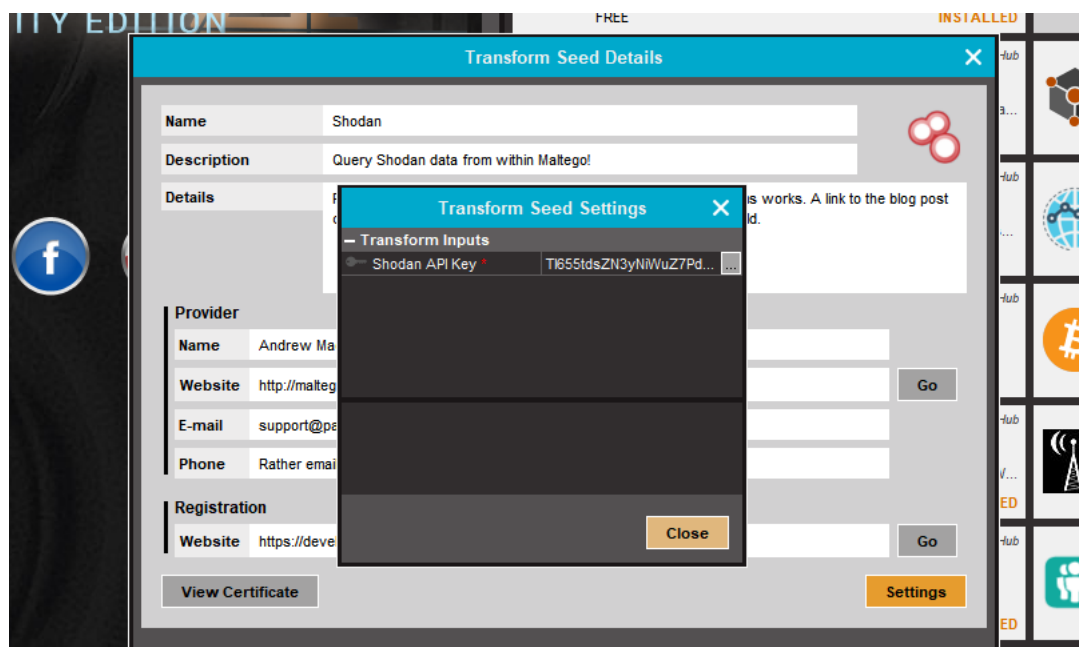


Abbildung 34: Maltego: Plugin-Settings (bspw. API-Key für Shodan)

Die Entity-Palette

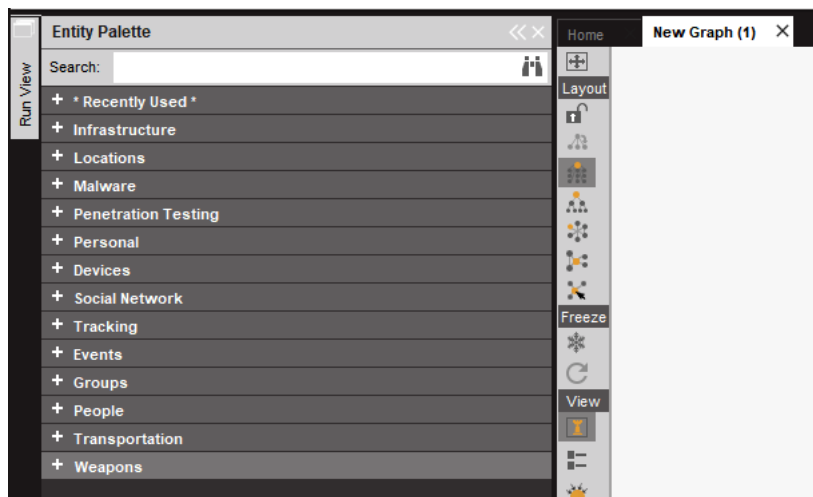


Abbildung 35: Maltego: Entity Palette

Die Domain-Konfiguration der Entität Domain

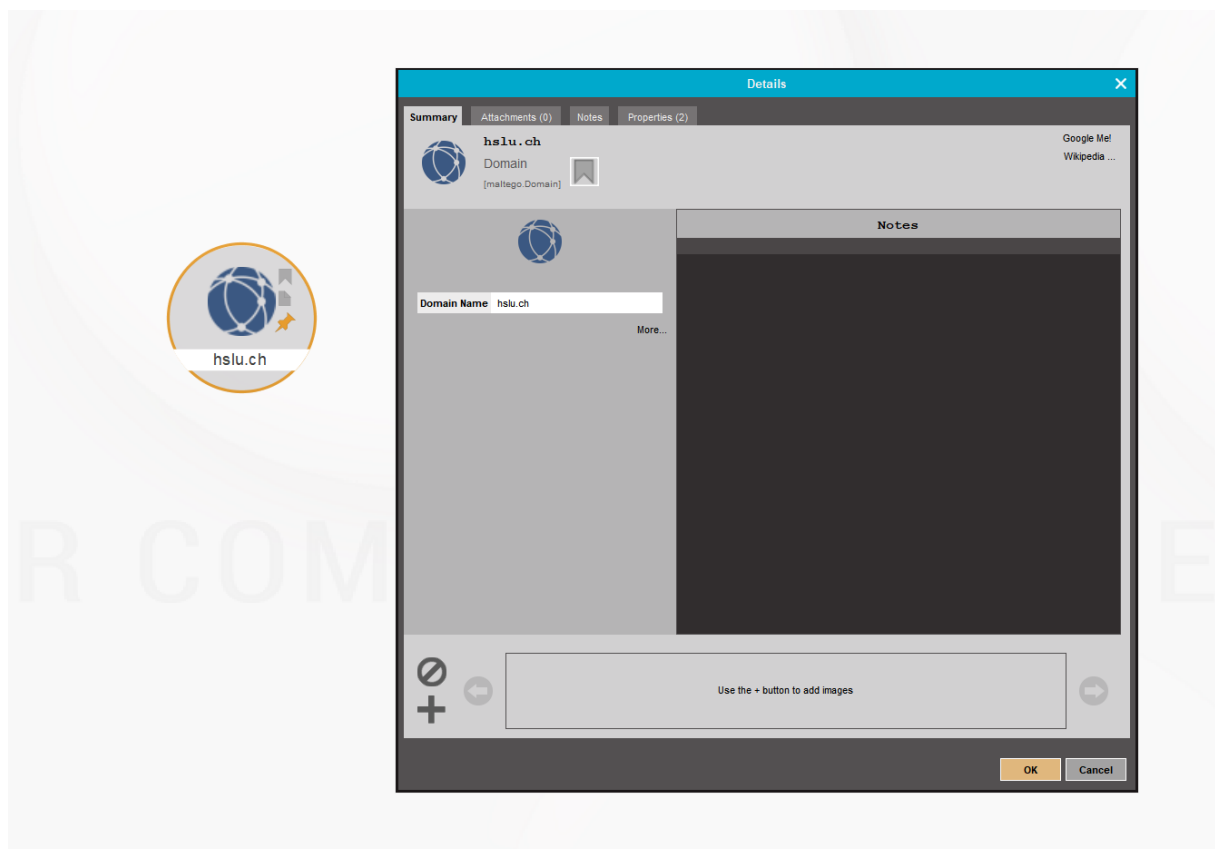


Abbildung 36: Maltego: Domain Entity Konfiguration

Die Transformationsauswahl

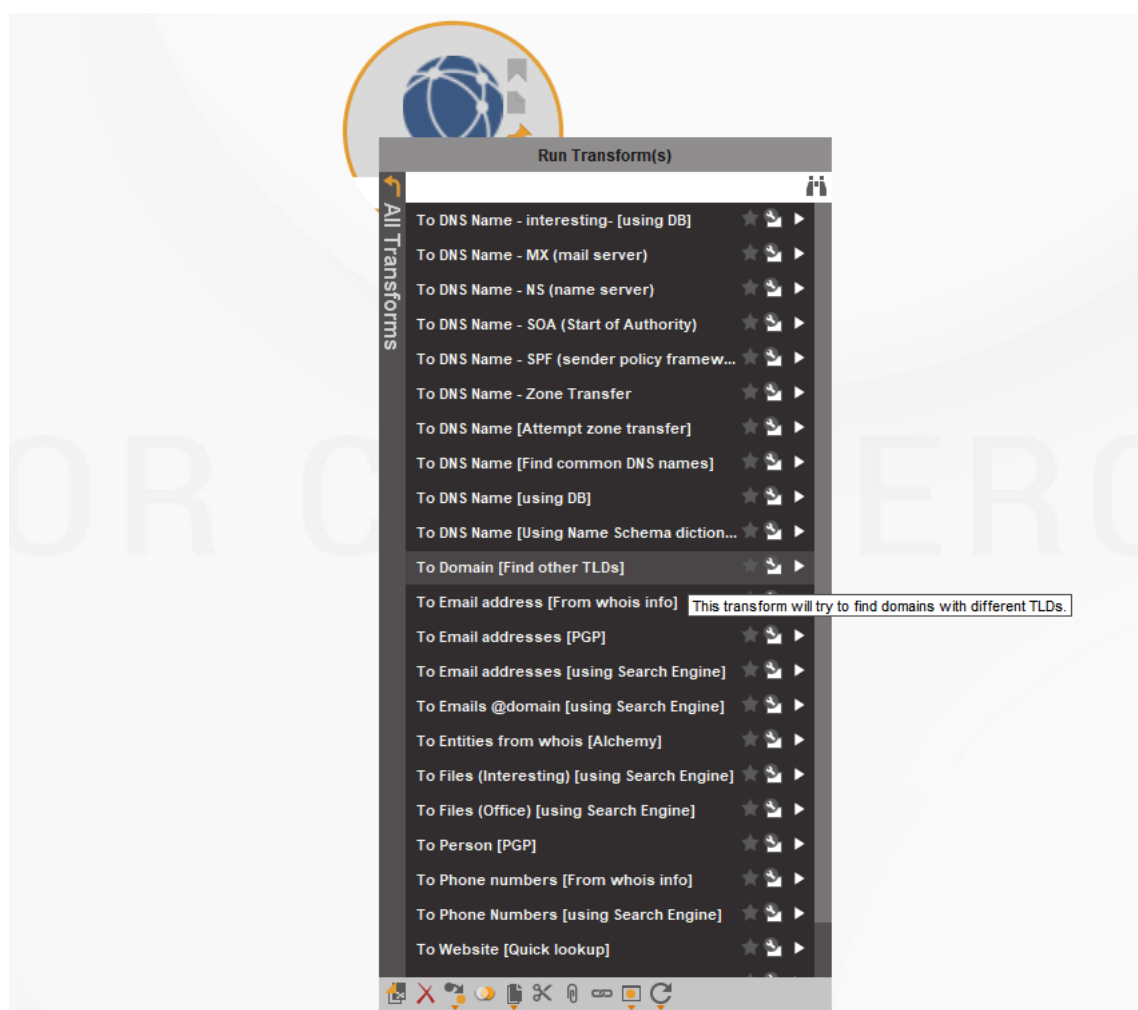


Abbildung 37: Maltego: Suche nach Related TLD Domains

Die graphische Aufbereitung

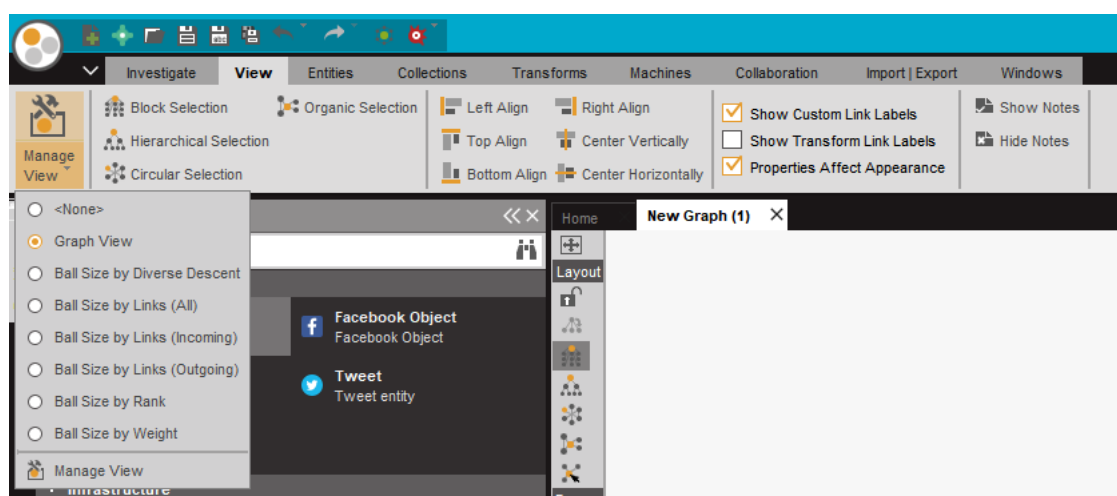


Abbildung 38: Maltego: Ansichts-Optionen