REFRACTED security

digital safety made accessible

Stageopdracht

Verslag

1 Inhoudstafel

Inhoud

2 Stageopdracht

2.1 OSINT Automation

- ***Basisrequirements***

Framework maken dat bestaande tools gebruikt en hun outputs combineert, met een enkele input zoveel mogelijk juiste* data verzamelen.

Op basis van een naam/username of email adres voor een persoon op te zoeken of op basis van bedrijfsnaam of URL om een bedrijf op te zoeken, hierbij ook lijst van werknemers + informatie.

Alle informatie gekoppeld en verwerkt naar CSV om dan te kunnen importen naar een visualisatie platform.

Gewenste format van results voor personen:

Index / Naam / Email / Telefoonnummer / Bedrijf / Adres / Social Media's / Andere Forums / Gevonden Accounts / Password Breaches / Password Breaches (Recent)

Gewenste format van results voor bedrijven:

Index / Naam Bedrijf / Locatie bedrijf / BTW-Nummer / Bedrijfsnummer / Domeinen / E-mail domain / Key Personnel / Financial Information / Partners / Intellect Property / Legal Issues / Past Breaches / Current security /

*False positives bevestigen en eruit halen

- ***Extra mogelijkheden/uitbreidingen:***

*VIP Protection module

**Zoeken naar intresses/persoonlijke dingen om social engineering simpeler te maken

3 Opzoekwerk bestaande OSINT Frameworks

*Gemarkeerde titels met * lijken mij interessant voor gebruik.*

3.1 Recon-ng *

Uitgebreid framework waar veel modules inzitten, met mogelijk om informatie van andere tools in te brengen en te exporten naar gewenste format. Mogelijkheid om een lijst van commando's in te brengen via script en zo te automatiseren.

Zowat alle tools die ik wil gebruiken zitten hier ook in, enkel dat het iets te uitgebreid is en alles moet manueel module per module worden ingesteld.

Sommige modules werken enkel met API keys, die niet te verkrijgen of betalend zijn.

3.2 Maltego

Betalend voor commercieel gebruik (duur). Zeer uitgebreid framework met eigen desktop app, verzamelt info via veel modules en heeft eigen visualisatie platform. Mogelijkheid om informatie van andere tools in te brengen en te exporten.

Visualisatie is goed en kan heel uitgebreid maar kan onduidelijk worden. Er is een optie om op bestaande informatie door te klikken en te gebruiken als input voor andere tools maar niet zo eenvoudig om informatie mee te verzamelen aangezien alles er op komt, misschien is betalende versie wel goed.

3.3 Spiderfoot *

Zeer uitgebreide tool, vrij duidelijke visualisatie. Results en export hiervan in web UI, nog geen manier gevonden om via CLI results op te slagen naar CSV.

Op dit moment resultaten enkel zichtbaar via web UI, en een hoop modules hebben API keys nodig waardoor er een hoop modules niet gebruikt worden.

Eerst opzetten van spiderfoot server en dan de cli openen en connecten naar die server, dan via cli mogelijk om alles op te slaan naar csv.

3.4 IntelTechniques *

Een hoop van online search tools op IntelTechniques site. Enkel online geen tool. Geen API voor queries automatisch te versturen naar hun site. Handige site maar lijkt onbruikbaar voor automatisering.

3.5 Shodan *

Er bestaat een API voor automatisering in script. Veel mogelijkheden om informatie te verzamelen via IP addressen, port numbers, locatie, services, AS nummerse en CVE nummers. Lijkt mij handig om te gebruiken met input van andere tools. Wel betalend voor meerdere pagina's results.

3.6 Conclusie

Een gebruik maken van Shodan en Spiderfoot om een framework opstellen zoals recon-ng lijkt mij het beste. Hierbij zelf tools selecteren die resultaten kunnen doorgeven aan elkaar.

4 Opzoekwerk bestaande OSINT tools

*Gemarkeerde tools met * lijken mij interessant.*

4.1 Sherlock *

Tool voor checken van usernames op sites. Kijkt na of er een account bestaat op deze sites. Kan exporten naar CSV. Handig voor checken social media accounts en vaak voorkomende sites.

4.2 Blackbird *

Zelfde als Sherlock maar andere websites, sommige overlappen. Exporteert naar JSON. Mogelijkheid om zelf Blackbird te herschrijven om een optie toe te voegen om te te exporteren naar CSV.

4.3 LinkedInt *

Kijkt LinkedIn bedrijven na en laat werknemers + naam + functie zien op html pagina + mogelijk email-adres binnen bedrijf. Heeft LinkedIn account nodig + hunter.io API key.

4.4 Nmap *

Scanner, geeft uitgebreid verslag terug van netwerk. Returned open poorten en banners etc. Zeker een must voor scanning van IP.

4.5 Dehashed *

Wordt hier al gebruikt. Zeer interessant, Zoekt op basis van email-adres, domain, ip, username om password breaches te checken.

4.6 HaveIBeenPwned

Zelfde als Dehashed maar aangezien Dehashed al gebruikt word niet van toepassing.

4.7 Crosslinked *

Tool die via LinkedIn zoekt naar mensen die gelinked zijn aan een bedrijfnaam. Returned lijst van email-adressen en link naar profielen en job beschrijving. Results in txt/csv.

4.8 WhoIs

Geeft domein info terug, van wie het domein is, nameservers. Lijkt nuttig maar er zijn andere tools die dit ook doen in combinatie met andere dingen.

4.9 TheHarvester *

Handige tool, gebruikt meerdere tools om informatie over een domein te verzamelen. Heeft API keys nodig van sommige tools. Kan geautomatiseerd worden. Verzamelt namen, emails, ip's, subdomeinen en urls. Dan ook DNS brute forcing doen en screenshots nemen. Mogelijkheid om op te slaan naar XML of JSON.

4.10 Whatsmyname

Word gebruikt in spiderfoot, zoekt via username naar matchende namen.

4.11 DNS Dump

Handige online tool, maar geen API of mogelijkheid om te automatiseren. Laat ook deel van WhoIs zien.

4.12 Dnsrecon *

Tool voert WhoIs, reverse IP, DNSSEC zone walk uit op domeinnaam. Resultaten worden opgeslagen naar keuze. Lange result dus moet nog gefilterd worden op wat nodig is.

Dig domain /zeer handig -> beste optie

Dnsrecon -d domain crasht VM en geen nuttige output

4.13 Whatweb *

Zeer handig, returned alles van de opgegeven website dat mogelijk nuttig kan zijn. Mogelijkheid om resultaten op te slagen naar keuze en hoe gedetailleerd.

4.14 Hosthunter

Stopt op 500 resultaten, en hele boel false positives. Exporteert wel naar txt of csv bestand. Automatisering is mogelijk.

4.15 Amass *

Word op dit moment gebruikt, handige tool met veel opties. Kan geautomatiseerd worden. Gebruikt andere tools om results te combineren. Heeft API keys nodig om volledig aan het werk te gaan. Het intel deel heeft veel opties zoals WhoIs, reverseIP, … maar de resultaten die hier uitkomen lijken mij

vooral false positive, als ik op organisatie zocht kwam er niks uit. Heeft een visualisatie functie die alle gevonden data uitgebreid laat zien. Kan wel onduidelijk worden als er veel data gevonden is. Bij de enum optie geeft deze wel een IP adress en ASN nummer terug.

4.16 Conclusie

Lijst van tools samen te voegen, voor personen en voor bedrijven andere tools nodig.

5 Opzoekwerk False Positives & combineren van data resultaten

*Gemarkeerde tools met * lijken mij interessant.*

5.1 OpenRefine *

Handige tool om meerdere bestanden samen te voegen, kan ook data filteren en combineren op bepaalde criteria, zeer interessant voor mijn opdracht. Nog manier zoeken om dit te automatiseren. Probleem is dat filters die nodig zijn op een project niet kunnen opgeslagen worden dus alle filters moeten telkens opnieuw worden toegevoegd aan nieuwe projecten.

5.2 Talend

Betalend, te groot en uitgebreid voor wat nodig is.

5.3 Alteryx APA

Betalend, te groot en uitgebreid voor wat nodig is.

5.4 Altair Monarch

Betalend, te groot en uitgebreid voor wat nodig is.

5.5 Trifecta

Betalend, te groot en uitgebreid voor wat nodig is.

5.6 Datameer

Betalend, te groot en uitgebreid voor wat nodig is.

5.7 Tableau Desktop

Betalend, te groot en uitgebreid voor wat nodig is.

5.8 Parsehub *

Zeer leuke tool maar alles moet handmatig worden ingesteld en dat is het tegenovergestelde van mijn opdracht. Tool kan gebruikt worden om data te scrapen van een website. Zelf website in kaart brengen en dan omzetten naar CSV of JSON bestand.

5.9 Scrapy *

Tool werkt wel maar output file blijkt leeg te zijn. Elke mogelijke spider werkt wel maar de output files blijven leeg.

5.10 ConvertCSV *

Betalend maar lijkt op dit moment de enigste tool die zijn werk echt doet. Zet JSON resultaten om naar CSV. Heeft API.

5.11 Dasel *

cat test.json | dasel -r json -w csv > test.csv kan gebruikt worden om json bestanden om te zetten naar CSV.

Confidentiality & Liability

This document contains information that is confidential to the customer, Refracted and third parties officially involved in this project. Information from this document may only be shown to other parties with the written permission of Refracted. The document is issued to the recipient in strict confidence and may be used solely for the internal business purposes of the recipient. It may not be sold, copied ore reproduced or provided to any third party in whole or in part in any matter or form without the prior written consent of Refracted.

Refracted has made every effort to ensure that the information contained in this report is accurate. However, the information may be based on data provided by third parties and/or their software products and as such Refracted is not liable for any problems that may occur as a result of any inaccuracies in this document.

Refracted Security
2500 Lier
Belgium

www.refracted.eu
info@refracted.eu

REFRACTED security
digital safety made accessible