
# OSINT Automation

## Plan van aanpak

**Siebe Van Rompay**

Academiejaar 2022-2023

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

# INHOUDSTAFEL

## Inhoud

# VOORWOORD

Ik ben student Cloud & Cyber security in het derde jaar IT-Factory aan de Thomas More Geel, dit plan van aanpak gaat over mijn stage opdracht. Ik loop mijn stage bij Refracted, een bedrijf dat gespecialiseerd is in Penetration testing.

Ik wil graag mijn begeleiders van Refracted bedanken, Ben, Karel en Stijn. Maar ook Patrick Dielens mijn stagesupervisor.

# 1 INLEIDING

Mijn stage gaat over het onderwerp OSINT, meer specifiek over het automatiseren hiervan. Ik moet een framework of script opstellen om bepaalde OSINT technieken, tools en frameworks automatisch toe te passen en zoveel mogelijk juiste resultaten terug te krijgen.

Eerst zal ik het probleem kort beschrijven met de huidige manier van werken dan het doel, de planning en tenslotte de conclusie.

In het onderzoek zal ik eerst zoeken naar bestaande frameworks en tools om zo te zien wat nuttig en van toepassing is voor mijn stageopdracht. Dan zal ik hiervan testresultaten genereren om zo te zien welke echt gebruikt kunnen worden. Daarna ga ik de gewenste tools samen brengen in een script of framework om zo dit te automatiseren. Met verder de bedoeling om de resultaten hiervan te visualiseren.

# 2 PROBLEEMSTELLING

Het huidige probleem met OSINT onderzoek is dat er heel veel verschillende tools en frameworks bestaan maar deze geven allemaal een deel van de gewenste resultaten. Bijvoorbeeld: Spiderfoot geeft heel veel resultaten, zowat alle juiste resultaten staan erin maar er zijn nog een hele berg false positives, deze moeten eruit.

Aan de andere kant zijn aparte OSINT tools zeer goed maar deze geven maar een deel van de resultaten, minder false positives maar enkel op specifiek gebied gezocht.

Het probleem blijft dus om alle OSINT tools apart te laten werken wat dus handmatig is en veel tijd kost. Of een OSINT Framework zijn werk te laten doen maar dan zit je weer met een hoop false positives en moet je die handmatig deze eruit halen.

# 3 STAGE BESCHRIJVING

In het onderzoek zal ik eerst zoeken naar bestaande frameworks en tools om zo te zien wat nuttig en van toepassing is voor mijn stageopdracht. Dit bestaat uit alle bestaande tools en frameworks opzoeken en zelf testen op meerdere scenario's.

Dan zal ik hiervan testresultaten genereren om zo te zien welke echt gebruikt kunnen worden. Dit bestaat dus op meerdere manieren de tools en frameworks runnen om zo meerdere resultaten genereren en dan bekijken of de tools van toepassing zijn op mijn opdracht.

Daarna ga ik de gewenste tools samen brengen in een script of framework om zo dit te automatiseren. Waarschijnlijk een framework in een Github Repository met daarin alle benodigde tools en een script om deze tools samen te brengen.

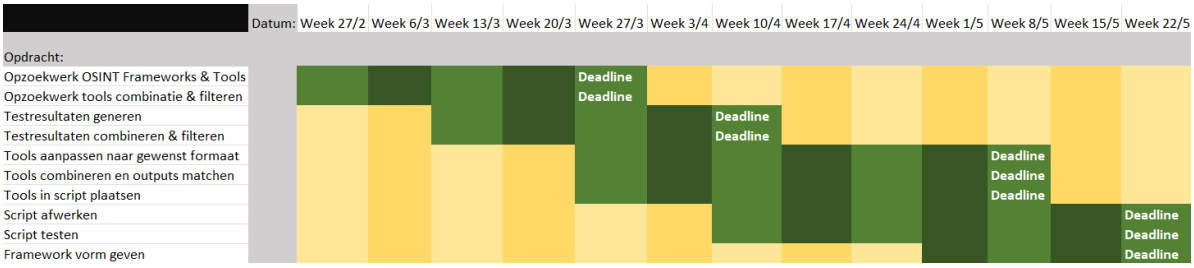
Verder zoek ik de mogelijkheid om de resultaten hiervan te visualiseren. Liefst in een spin-diagram maar op eender welke mogelijke manier die duidelijk is.

# 4 DOELSTELLING

Het doel van mijn opdracht is dat ik op het einde een framework heb gemaakt waarbij je simpelweg een persoon naam of bedrijf naam kan ingeven en zo alle informatie terug krijgt. Deze resultaten worden zo goed mogelijk gefilterd en verder gevisualiseerd op een duidelijke manier. Het eindresultaat moet simpel, duidelijk en zo juist mogelijk zijn. Wat dus wilt zeggen dat er zo weinig mogelijk false positives in de resultaten mogen zitten. Dit zorgt ervoor dat je simpelweg mijn framework kan gebruiken en voor de rest amper tot niks meer moet doen.

# 5 PROJECTPLANNING

*Zie ProjectPlanningStage.xlsx*



# 6 CONCLUSIE

Het eindresultaat van de opdracht zou het gemakkelijker moeten maken voor Refracted om zo snel en zo juist mogelijk data te verzamelen. OSINT kan heel uitgebreid zijn en daarom zou deze opdracht voor het grootste deel het manuele aspect achter OSINT, dus alles zelf opzoeken en elke tool apart gebruiken, uit handen moeten nemen. Waardoor er tijd is voor andere manuele acties die wel echt manueel moeten gebeuren.

# 7 BIJLAGEN

ProjectPlanningStage.xlsx