Boosterweek 2 – Intelligence Gathering

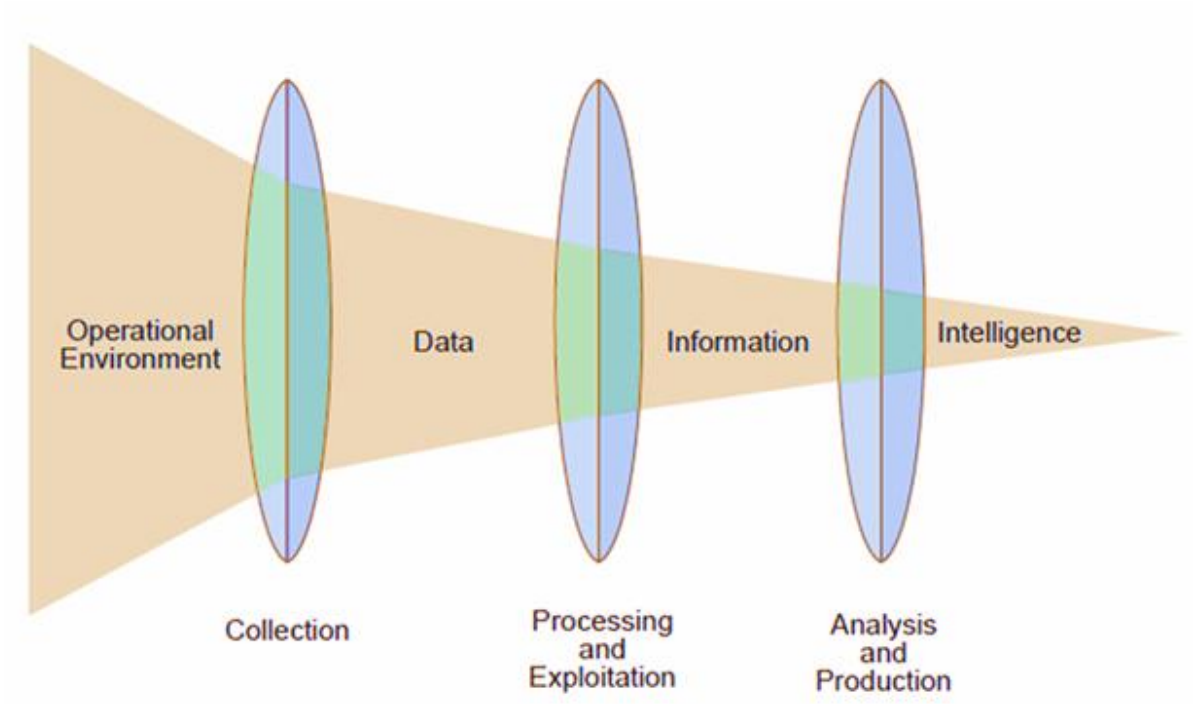
Werkcollege’s

Inhoud

PTES Fase 2 – Intelligence Gathering 3
OSINT (Open Source Intelligence) 3
Werkcollege 1 – Handmatig onderzoek 5
Leerdoelen 5
Opdrachten 5
Inhoud van de portfolio 8
Werkcollege 2a – Tools 9
Leerdoelen 9
Opdrachten 9
Inhoud van de portfolio 9
Werkcollege 2b – Documenteren 10
Leerdoelen 10
Opdrachten 10
Inhoud van de portfolio 10
Werkcollege 3 – Casus 11

PTES Fase 2 – Intelligence Gathering

Fase 2 van het PTE model is Intelligence Gathering. Hierbij is het doel om informatie te verzamelen over een systeem of doelwit. Echter is verzamelde informatie niet direct intelligence. De data die verzameld word moet namelijk eerst verwerkt en geanalyseerd worden om tot conclusies te kunnen komen. Deze conclusies worden de intelligence genoemd. De onderstaande afbeelding maakt dit visueel.



Figuur 1 De relatie tussen, data, informatie en intelligence

De informatie die tijdens deze fase wordt verzameld kan belangrijk zijn voor het uitvoeren van een pentest. Met deze informatie kan er namelijk bepaald worden waarop, waarmee en hoe de aanval uitgevoerd kan worden.

OSINT (Open Source Intelligence)

Een van de technieken die in de Intelligence Gathering fase wordt toegepast is Open Source Intelligence (OSINT). Dit is het zoeken naar openbaar beschikbare informatie wat kan lijden tot intelligence. Dit kan veel meer zijn dan wat er op het internet staat. Dit kan bijvoorbeeld ook een gesprek of een krant zijn.

Het is legaal om OSINT uit te voeren op een persoon of een bedrijf. Dit is omdat de informatie openbaar beschikbaar is. Echter zijn er ook veel uitzonderingen op deze regel. Op het moment dat er

sprake is van stelselmatig onderzoek, is OSINT wel strafbaar op dat moment is het namelijk een inbreuk op de privacy.

Bijvoorbeeld: Een x periode onderzoek uitvoeren naar de CEO van een grote organisatie is in de basis legaal omdat er geen sprake is van stelselmatigheid. Maar op het moment dat je elke week controleert of de informatie veranderd is er sprake van stelselmatigheid wat illegaal/strafbaar kan zijn.

Het uitvoeren van een OSINT onderzoek kan zowel handmatig als met tools. In beide gevallen zullen de resultaten ongeveer gelijk zijn. Een tool voert namelijk meestal een geautomatiseerde handeling uit die je ook handmatig zou kunnen doen (denk bijvoorbeeld aan automatisch scrollen). Een voordeel van tools is dat het sneller kan zijn dan handmatig onderzoeken als het gaat om grote hoeveelheden.

Echter hebben tools ook een nadeel; ontwikkelaars van websites/applicaties doen er alles aan om te voorkomen data automatisch verzameld kan worden. Veel ontwikkelaars proberen dit dan ook actief te blokkeren/tegen te gaan. Het nadeel hiervan is dat een tool die vandaag nog werkt morgen niet meer kan werken. Daarom is het altijd goed om eerst te weten hoe iets handmatig onderzocht wordt voordat je dit automatisch doet. Daarnaast kunnen tools sporen achterlaten die te herleiden zijn naar een gebruiker van de tool, denk voor gebruik dus goed na of het veilig is!

Werkcollege 1 – Handmatig onderzoek

Het maken van de vragen gaat aan de hand van de informatie die ontvangen is tijdens de presentatie van de gastles. Deze presentatie staat ook op DLO en kan bekeken worden voor verduidelijking/beantwoording van de vragen.

Op DLO staat een gezipt bestand met daarin alle media die nodig is voor het beantwoorden van de vragen. Voor deze opdrachten zijn de volgende mappen nodig uit de map '*Werkcollege 1*' EXIF data onderzoeken, Reverse Image Search en Geolocating.

Leerdoelen

De leerling moet na het volgen van de presentatie en beantwoorden van de vragen in staat zijn om de volgende dingen uit te voeren:

- Een zoekmachine te kiezen aan de hand van het onderzoek of wat er gezocht moet worden.
- Toepassen van Google Dorking.
- Uitvoeren van reverse image search.
- Het verschil tussen surface-, deep- en dark web kennen.
- Toegang verkrijgen tot dark web websites.
- Onderzoeken van EXIF data.
- Achterhalen van een locatie (geolocating)

Opdrachten

Hieronder volgende opdrachten die de beantwoord moeten worden. Dit kunnen kennisvragen zijn maar dit kunnen ook vragen zijn waarbij de student gevraagd word om een handeling uit te voeren.

Werkcollege 1 – opdracht 1

Voor een specifiek onderzoek kan het handig zijn om een specifieke browser te gebruiken om tot de gevraagde informatie te komen. Beantwoord hierover de volgende vragen.

Vraag 1: Je doet onderzoek naar een Russisch persoon, welke zoekmachine kan je hier het beste voor gebruiken?

Vraag 2: Je doet onderzoek naar een Aziatisch persoon, welke zoekmachine kan je hier het beste voor gebruiken?

Vraag 3: Je wilt een reverse image search zoekopdracht naar een persoon uitvoeren, welke zoekmachine kan je hier het beste voor gebruiken?

Vraag 4: Je wilt een locatie met streetview bekijken in een Europees land. Welke zoekmachine kan je hier het beste voor gebruiken?

Werkcollege 1 – opdracht 2

Voor het specifiek zoeken naar bepaalde zoekresultaten kan je gebruik maken van Google Dorking, dit gaat door middel van operators.

Vraag 1: Vul de onderstaande tabel aan om deze helemaal compleet te krijgen.

Operator	Toepassing
	Zoeken naar het een én het ander
	Zoeken het een of het ander combinaties
"…"	
	Uitsluiten van een woord
site:	Zoeken binnen een website
filetype:	
intitle:	
	Zoeken naar resultaat in een titel (meerdere woorden)
inurl:	Zoeken naar resultaten in een URL
allinurl:	
intext:	
	Zoeken naar resultaat in een tekst (meerdere woorden)

Vraag 2: Hieronder volgen een aantal zoekopdrachten waarvoor google operators nodig zijn om deze juist te beantwoorden. Van deze opdrachten moeten er minimaal 2 beantwoord zijn. Geef hierbij een screenshot van de resultaten en noteer welke zoekopdracht je hiervoor gebruikt. Het gaat hierbij voornamelijk om de zoekopdracht die je gebruikt om het gevraagde te vinden.

- Zoek een vertrouwelijk rapport voor het AZ Sint-Elisabeth op de website van de instantie.
- Zoek het CV van Marjolein Dohmen op de website van Universiteit van Twente.
- Zoek naar medewerkers van politie Nederland die op LinkedIn zitten.
- Zoek naar een document over geïmproviseerde explosieven op de website van Centurion University.
- Zoek een vertrouwelijk rapport van Deloitte en het Ministerie van Binnenlandse zaken.

Werkcollege 1 – opdracht 3

Voor deze opdracht zijn de afbeeldingen nodig die gedownload zijn vanuit DLO. Noteer ook waar je dit gevonden heb.

Vraag 1: Wie is het persoon op de foto?

Vraag 2: Hoe heet het bedrijf waar deze foto bij hoort en in welke plaats is dit?

Vraag 3: Wat is de naam van het bedrijf wat gevestigd is in dit gebouw?

Werkcollege 1 – opdracht 4

De volgende opdrachten gaan over het surface-, deep- en dark web.

Vraag 1: Wat is het belangrijkste kenmerk van een website op het surface web?

Vraag 2: Wat is het belangrijkste kenmerk van een website op het deep web?

Vraag 3: Wat is het belangrijkste kenmerk van een website op het dark web?

Vraag 4: Wat heb je nodig voor het bezoeken van het dark web?

Vraag 5: Omschrijf alle stappen die je nodig hebt om een dark web website te bezoeken (mag met screenshots en uitleg).

Werkcollege 1 – opdracht 5

De volgende opdrachten gaan over het onderzoeken van EXIF data. Voor een deel van deze vragen heb je de afbeeldingen nodig die je gedownload hebt uit DLO. (Tip, verschillende manieren van het onderzoeken van EXIF data kan het makkelijker maken).

Vraag 1: Waar staat de afkorting EXIF voor?

Vraag 2: Wanneer is de foto genomen?

Vraag 3: Met wat voor Camerafabrikant en cameramodel is de foto genomen?

Vraag 4: Wat is het Image Unique ID?

Vraag 5: Waar is het adres waar de foto genomen is?

Werkcollege 1 – opdracht 6

Voor deze opdracht zijn de bestanden nodig die gedownload zijn vanuit DLO. Uit de map Geolocating. (Denk om de afbreuk risico's)!

Vraag 1: Wat is het adres van het gebouw op de foto?

Vraag 2: In welke stad is deze foto genomen?

Vraag 3: Wat is de naam van de straat waar deze foto genomen is?

Vraag 4: Wat is het adres van het gebouw op de foto?

Vraag 5: Wat is het adres van de atleet (ongeveer)?

Inhoud van de portfolio

- Antwoorden op de vragen van opdracht 1.
- Ingevulde tabel van opdracht 2, vraag 1.
- Minimaal 2 van de zoekopdrachten zijn gedaan en gevonden, leg hierbij de zoekslag en het resultaat vast.
- Antwoord op de vragen van opdracht 3, leg het bewijs van de antwoorden vast.
- Antwoorden op de vragen van opdracht 4
- Antwoorden op de vragen van opdracht 5.
- Antwoorden op de vragen van opdracht 6, inclusief stappen hoe je hier tot gekomen bent.

Werkcollege 2a – Tools

Het maken van de vragen gaat aan de hand van de informatie die ontvangen is tijdens de presentatie van de gastles. Deze presentatie staat ook op DLO en kan bekeken worden voor verduidelijking/beantwoording van de vragen. Op DLO staat een gezipt bestand met daarin alle media die nodig is voor het beantwoorden van de vragen. Voor deze opdrachten zijn de volgende mappen nodig uit de map '*Werkcollege 2*' Autostitch.

Leerdoelen

De leerling moet na het volgen van de presentatie en beantwoorden van de vragen in staat zijn om de volgende dingen uit te voeren:

- Een video of meerdere foto's omzetten naar een panorama foto voor geolocating.
- Zoeken naar gekoppelde accounts met Holehe.
- Een onderzoek documenteren via Hunchly.

Opdrachten

Hieronder volgende opdrachten die de beantwoord moeten worden. Dit kunnen kennisvragen zijn maar dit kunnen ook vragen zijn waarbij de student gevraagd word om een handeling uit te voeren.

Werkcollege 2a – opdracht 1

Maak met Autostitch een panorama van de mp4 video uit de map 'Autostitch'. Sla deze panorama op en voeg deze toe aan de portfolio met uitleg waarom je de keuze gemaakt hebt om de panorama op die manier te maken.

Werkcollege 2a – opdracht 2

Installeer het programma Holehe en laat zien dat het werkt door te zoeken naar bert.janssen@gmail.com. Zet een screenshots van de installatie, het commando en het resultaat in je portfolio. Leg ook uit hoe Holehe handig kan zijn tijdens een onderzoek.

Werkcollege 2a – opdracht 3

Installeer de 30 day trial van Hunchly en de bijbehorende Chrome extensie. Voer een aantal zoekopdrachten uit en laat met screenshots zien dat het werkt. Leg ook in je eigen woorden waar Hunchly voor gebruikt kan worden en waarom dit handig kan zijn.

Inhoud van de portfolio

- De panorama die gemaakt is via Autostitch en onderbouwen waarom.
- Screenshot van de installatie, het gebruik en het resultaat van Holehe.
- Uitleg waarom Holehe handig kan zijn tijdens een onderzoek.
- Screenshot waarin je laat zien dat Hunchly werkt.
- Uitleg waarom Hunchly handig kan zijn tijdens een onderzoek.

Werkcollege 2b – Documenteren

Het maken van de vragen gaat aan de hand van de informatie die ontvangen is tijdens de presentatie van de gastles. Deze presentatie staat ook op DLO en kan bekeken worden voor verduidelijking/beantwoording van de vragen.

Leerdoelen

De leerling moet na het volgen van de presentatie en beantwoorden van de vragen in staat zijn om de volgende dingen uit te voeren:

- Een OSINT onderzoek rapporteren in Xmind.
- Een stappenplan kunnen maken in Xmind.
- Notities maken met markdown.
- Een markdown cheat sheet maken in Obsidian.
- Een OSINT onderzoek rapporteren in Obsidian.
- Een stappenplan maken in Obsidian.

Opdrachten

Hieronder volgende opdrachten die de beantwoord moeten worden. Dit kunnen kennisvragen zijn maar dit kunnen ook vragen zijn waarbij de student gevraagd word om een handeling uit te voeren.

Werkcollege 2b – opdracht 1

Download Xmind, maak hier vervolgens een stappenplan in om een persoon te onderzoeken. Zet een screenshot in je portfolio.

Denk bij het maken van het stappenplan onder andere aan de volgende dingen:

- Zijn er handmatige manieren om te zoeken?
- Zijn er tools waar je mee kan zoeken?
- Stel je vind een emailadres, wat kan je daar weer mee?

Werkcollege 2b – opdracht 2

Download Obsidian en maak een markdown cheat sheet voor jezelf. Maak vervolgens een stappenplan voor geolocating. Zet een screenshot in je portfolio en upload de .md bestanden in DLO.

Inhoud van de portfolio.

- Een screenshot van het stappenplan in Xmind.
- Een screenshot van het markdown cheat sheet in Obsidian.
- Een screenshot van het geolocating stappenplan in Obsidian.

Werkcollege 3 – Casus

Na de gastles heb je in groepjes van 4 personen een casus gemaakt. In deze casus staat vermeld dat er een tweetal documenten opgeleverd moet worden. Dit zijn de volgende documenten:

- Plan van aanpak voor het onderzoek.
- Rapportage van het onderzoek.

Deze bestanden moeten bijgevoegd worden aan de portfolio om dit werkcollege succesvol af te ronden. Hieronder volgt een opsomming van de eisen die deze documenten moeten hebben.

Plan van aanpak:

- Welke rol heeft iedereen tijdens het onderzoek?
- Welke informatie wil je vinden?
- Hoe en waar denk je deze informatie te gaan vinden?
- Zijn er risico's verbonden aan het onderzoek en waarom zijn deze risico's er?
- Hoe ga je om met de risico's?
- Wat ga je doen als het niet lukt om de informatie te vinden?

Rapportage:

- Wat voor soort informatie heb je gevonden?
- Waar heb je deze informatie gevonden?
- Hoe ben je bij deze informatie gekomen?
- Kan je bewijzen dat deze informatie juist is?

In een wereld die in toenemende mate digitaliseert, zorgt Cuccibu ervoor dat de onbegrensde mogelijkheden van deze wereld worden benut op een verantwoorde en veilige manier. Cuccibu helpt organisaties met vraagstukken op het vlak van informatiebeveiliging, privacy, cyber security en QHSE. Onze professionals op deze gebieden hebben de achtergrond en ervaring om met creatieve en heldere oplossingen iedere organisatie, groot of klein, te helpen!

www.cuccibu.nl | Cuccibu B.V. | Eindhoven - Rijswijk | KvK 61072923 | info@cuccibu.nl | +31 (0) 85 303 2984