Weekly status raport

Stage

Nagels Viktor
R0840938
3ITF – CCS01

Academiejaar 2022-2023

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

Table of Content

1 WEEK 1 (27/02 - 03/03)

1.1 Maandag 27/02

Vandaag was het de allereerste stagedag. Deze is goed verlopen! Eerst kreeg ik een rondleiding en werd er mij een bureau aangewezen. Vervolgens mochten we ons zelf installeren en onze gekregen accounts instellen. Hierna werd er me al direct gevraagd om een carkey duplicator te onderzoeken, of er een mogelijkheid was om de logging ervan uit te lezen.

Na de middag kregen we de uitleg over onze stageopdracht. Deze gaat over het gebruik van telegram en het uitlezen ervan. Tot slot had ik nog samen met de andere stagiaires een Webinar gevolgd over SIMP.

1.2 Dinsdag 28/02

Vandaag ben ik begonnen aan de onderzoeksfase van mijn stageproject. Ik heb de hele dag onderzoek gedaan naar wat is telegram, hoe werkt het, hoe werkt de encryptie, welke alternatieven zijn er. Ook heb ik gezocht welke cachegegevens er werden opgeslagen op verschillende apparaten. Ten slotte had ik nog enkele telegram OSINT-tools opgezocht om op donderdag te testen

1.3 Woensdag 01/03

Jobbeurs

1.4 Donderdag 02/03

Vandaag in de voormiddag heb ik onderzoek gedaan naar de verschillende OSINT-tools voor telegram. Er moest een API aangemaakt worden om de tools te activeren. Deze tools kunnen GEO-locaties van mensen en groepen terugvinden. In de namiddag had ik mijn les Windows Server

1.5 Vrijdag 03/03

Vandaag ben ik gestart met het documenteren van alles van de voorbije week. Ook heb ik nog onderzoek gedaan naar verschillende tools, die we kunnen gebruiken in dit onderzoek. Daarna ben ik nog eens dieper gedoken in de beveiliging van telegram. Hier had ik dan nog een schema van gemaakt. Mijn dag sloot af met het installeren en configureren van een Kali vm. Deze gaat worden gebruikt in de volgende weken.

2 WEEK 2 (06/03 – 10/03)

2.1 Maandag 06/03

Vandaag heb ik in de voormiddag samen met de andere stagairs samengezeten om ons onderzoek van vorige week te overlopen en hierover een presentatie te maken. Tijdens de middag hebben we deze dan voorgesteld aan onze stagementor en de collega's. Hierna ben ik dan verder op de tip van een collega ingegaan. Zo is er een kans dat we live kunnen meelezen in telegram chats. Tenslotte kreeg ik nog een vraag van mijn collega Gunther. Hij vroeg me om eens te kijken of er een manier bestaat om crypto wallets makkelijk op te zoeken en hun Balance uit te lezen. Ik had dit makkelijk gevonden via een API. Hier zou nog enkel een frontend voor moeten gemaakt worden en dan zou dit zijproject af moeten zijn

2.2 Dinsdag 07/03

Vandaag ben ik begonnen aan de tip van gisteren in werkelijkheid toe te passen. Eerst moest ik van mijn systeem een image maken. Daarna moest deze image omgezet worden naar TFK. Vervolgens moest deze gecoverd worden naar een. Vmdk bestand. Echter liep er hier iets met mis. Na lang zoeken naar de fout lijkt het erop dat de oorzaak een corrupt bestand is. Ik ben de dag geëindigd met een image maken, maar dan via een andere manier. Omdat dit alles heel lang wachten was. Heb ik mijn basistool zoals nmap, … herhaald en versterkt. Deze kunnen namelijk nog van pas komen in het verloop van dit project.

2.3 Woensdag 08/03

Vandaag hebben we onze telegram telefoon uitgelezen. Hier hadden we eerst al de verschillende soorten beveiliging en berichten gestructureerd gestuurd. Zo konden we achteraf nakijken welke er nog waren en welke niet. Tijdens de middag is ook onze stagementor langsgekomen om te zien hoe het met ons was. Daarnaast deden we ook nog onderzoek over de telegram OSINT-tools. Tenslotte had ik nog onderzoek gedaan naar telegram op de blockchain.

2.4 Donderdag 09/03

In de voormiddag heb ik mijn inhaal les gevolgd

Vanaf de namiddag ben ik bezig geweest met het onderzoeken van de source code van telegram, daarnaast ook de verschillen tussen de web, app & desktop versie. Ook heb ik nog onderzoek gedaan naar de hun API. Om 15u hadden we een gesprek om te overlopen hoever we staan in het project. Tot slot heb ik nog onderzoek gedaan naar MISP. Hier ga ik morgen op verder.

2.5 Vrijdag 10/03

Vandaag heb ik me beziggehouden met MISP installeren. Dit ging heel moeizaam. Dit kwam omdat ik verschillende problemen had met mijn virtual box. In de namiddag was ik hier verder met bezig. Ook had ik een collega geholpen met het onderzoeken of er ergens een database was met al de verschillende crypto wallet nummers. Deze bestond niet, maar je kan die wel maken met zelf een big query uit te voeren. Hiervoor moet je wel de blockchain zelf handmatig downloaden. Hiermee sloten we de dag ook af.

3 WEEK 3 (13/03 – 17/03)

3.1 Maandag 13/03

Vandaag kregen we de opdracht om rocket.chat te onderzoeken. Hier hebben we de hele voormiddag aan gezeten. Tijdens deze voormiddag heb ik rocket.chat ook online gezet en de server ook opgezet. Zo kon een collega deze vm's overnemen voor eigen onderzoek. In de namiddag ben ik bezig geweest met de complete installatie van MISP. Omdat dit met lang wachten is, heeft dit ook de volle namiddag gekost. Tot slot hebben we nog een gsm uitgelezen om de data van telegram eruit te halen

3.2 Dinsdag 14/03

Vandaag heb ik het hele MISP-platform onderzocht. Ook heb ik openCTI gedownload om zo te kijken wat het verschil ertussen is. Vervolgens heb ik onderzoek gedaan naar de MISP-feeds. Om te kijken wat dit juist is.

In de namiddag heb ik 2 windows 11 vm's aangemaakt. Deze heb ik gebruikt om te proberen een actieve telegram sessie overzetten van de ene vm naar de andere. Dit is me uiteindelijk gelukt naar een paar keer proberen. Dit was ook een Lucky shot, want we wisten niet of dat wel degelijk ging werken.

3.3 Woensdag 15/03

Vandaag heb ik meer onderzoek gedaan naar MISP. T.O.V gisteren heb ik meer geavanceerde stukken van MISP onderzocht. Hiervoor maakte ik gebruik van YouTube video's. Deze waren zeer gedetailleerd maar duurde wel lang.

In de namiddag heb ik me weer gefocust op de source code van telegram. Ik ben stelselmatig door de code gegaan zodat ik een globaal beeld erover kreeg. Tot slot heb ik ook geprobeerd een actieve Android sessie proberen overzetten via een externe apk extracten. Dit was echter niet gelukt.

3.4 Donderdag 16/03

In de voormiddag heb ik voor Windows server gewerkt. In de namiddag heb ik van thuis gewerkt. Ik heb me beziggehouden met de documentatie van de afgelopen week uit te schrijven en te verbeteren. Dit was mijn stagedag

3.5 Vrijdag 17/03

Vandaag heb ik onderzoek gedaan naar de community databases van MISP. Met meer nadruk op die van CIRCL. Omdat er zoveel van zijn, is het moeilijk om deze te snappen en implementeren. Vervolgens heb ik een md5 database gedownload en deze uitgelezen. Hiervoor had ik mysqlite geïnstalleerd. Ook heb ik XAMPP geïnstalleerd voor phpmyadmin. Tot slot sloot ik de week af met mijn documentatie weer in orde te maken.

4 WEEK 4 (20/03 – 24/03)

4.1 Maandag 20/03

Ik ben de week begonnen met mijn documentaties na te kijken en aan te passen waar nodig. Vervolgens heb ik mee een OSINT-tool getest namelijk: "Universal search bot Telegram". Deze tool zorgt ervoor dat je gemakkelijk aan OSINT kunt doen. Na de middag ben ik verdergegaan met het onderzoeken van de telegram protocollen. Tot slot had ik nog wat tijd over en heb het SharePoint portaal eens onderzocht. Hier had ik daarvoor nog geen tijd.

4.2 Dinsdag 21/03

In de voormiddag ben ik bezig geweest met het opzoeken van publieke hash code databases voor Android, iOS en windows device. In de namiddag hadden we een meeting over het verder verloop van onze stageopdracht. Hieruit kwam het volgende:

-Minder teksten, meer feiten
-Onderzoek eigen hash codes
–Publieke hash codes
-cryptografie

Na de meeting ben ik begonnen aan een Android hash database in te laden en te bekijken. Tot slot heb ik nog een meeting meegevolgd i.v.m. een telegram groep waar pornografische/pesterijen beelden in werden gedeeld. Hier werd er besproken hoe ze dit gingen aanpakken.

4.3 Woensdag 22/03

Vandaag hebben we in de voormiddag onderzoek gedaan naar een honeypot en canary tokens. Dit moesten we testen om te kijken of het mogelijk is dit samen met telegram te onderzoeken. Hierna hadden we een korte meeting om alle ideeën bij elkaar te leggen. Na de middag ben ik begonnen met het nakijken van hash codes online ne die van de IOS-device lokaal. Tot slot hebben we nog gewerkt aan de presentatie voor morgen

4.4 Donderdag 23/03

Vandaag moesten we in de voormiddag naar school om een tussentijdse presentatie te geven over ons stagebedrijf. Deze presentatie had ik samen met Jentel gedaan. Onze stagementor was erg content over ons resultaat en onze visie over het verder verloop van de stage.

In de namiddag heb ik van thuis gewerkt Hier heb ik onderzoek gedaan naar het overzetten van een actieve sessie van een Android toestel

4.5 Vrijdag 24/03

Vandaag heb ik me beziggehouden met het schrijven van een query om de databases met hashes te vergelijken. De query uitvoeren heeft in totaal 6.5u geduurd. Tijdens deze tijd kon ik niet te veel zware activiteiten uitvoeren op mijn laptop. Daarom ben ik verder opzoek gegaan naar de communicatie van telegram. Hiervoor heb ik wireshark gebruikt. Tot slot heb ik nog samen met Jentel een gsm-toestel uitgelezen.

5 WEEK 5 (27/03 – 31/03)

5.1 Maandag 27/03

In de voormiddag ben ik verdergegaan met de vergelijkingen van de hash databases. Eerst had ik een kleine test database aangemaakt. Om zo mijn query's te testen. Daarna heb ik indexeringen gedaan van de onlinedatabase waardes. Zo moet ik niet meer 6.5u wachten tot een resultaat. Uiteindelijk kwam ik tot de conclusie dat de databases geen enkel dezelfde hash waardes bevatten

In de namiddag ben ik bezig geweest met mijn documentatie te verkorten. Daarna heb ik me beziggehouden met het onderzoeken waarom de hashes niet overeenkomen.

5.2 Dinsdag 28/03

Vandaag heb ik in de voormiddag me weer beziggehouden met het onderzoeken van de hash codes. Ook had ik nog een indexering gedaan in de publieke database. Deze is echter corrupt geraakt en daarom moest ik deze opnieuw installeren.

In de namiddag hebben we een sessie gevolgd over wat je allemaal moet doen, om bij de politie te starten. Deze heeft 4 uur geduurd. Ik vond het een interessante uitleg en sta er zeker voor open om er te starten. Echter wil ik eerst nog bijstuderen.

5.3 Woensdag 29/03

Deze voormiddag hebben we samengezeten met onze collega Lieven. Hier hadden we een gesprek over de stand van zaken. Ook had Lieven onze stageopdracht nog verder in detail uitgewerkt. Zo is hebben we nu weer meer werk dat we kunnen doen. Hierna heb ik een python script geschreven om de hash database juist te formateren. In hun database stonden al de hashes van 1 app samen in 1 kolom, verdeeld met een ',’. Ik had deze dan allemaal uit elkaar getrokken en mooi in allemaal verschillende rijen laten zetten. Zo kon ik de query uitvoeren op de publieke database. Uiteindelijk bleek het dat deze dus wel degelijk overeenkwamen met de onlinedatabase. Vervolgens had ik me meer verdiept over hashcat en John the ripper. Deze tools zullen in een later stadia van pas komen voor onze opdracht.

5.4 Donderdag 30/03

Deze voormiddag hadden we ons tussentijdse examen over windows server. Tegen dat ik weer thuis was, ben ik weer kunnen beginnen aan mijn stage om 14u. Dan heb ik me weer verder verdiept in hashcat en John the ripper. Het laatste uur van mijn dag heb ik me nog beziggehouden met het beter snappen van 'Salt' op data.

5.5 Vrijdag 31/03

Vandaag heb ik mijn hele dag besteed aan het installeren van een telegram server + client. De server is uiteindelijk gelukt om te installeren. De client kreeg op het einde nog een error melding die ik niet meer op tijd heb kunnen

oplossen. Dit was eigenlijk mijn hele dag, daarom dat het zo een korte uitleg is voer mijn stagedag.

6 WEEK 6 (03/04 – 07/04)

6.1 Maandag 03/04

Vandaag ben ik begonnen met opzoekwerk naar de wet. Voor telegram ligt de wat moeilijk. Wanneer er een gsm wordt in beslag genomen, wordt deze in vliegtuigstand geplaatst. Vanaf dan kan het toestel niet meer aan het internet. Om een telegram account uit te lezen, moet eerst dat account online gezet worden. Zo kunnen al de berichten weer inladen. Deze manier val dus tussen 3 wetten. Hiervoor zijn we met collega's gaan praten die hier meer verstand van hadden. Zij wisten het echter ook niet. Op het einde van de dag hadden we het ongeveer gevonden. We moeten het nog wel eens gaan navragen bij het parket.

6.2 Dinsdag 04/04

Vandaag heb ik een dagje van thuis gewerkt. Eerst heb ik me beziggehouden met documenteren wat ik de afgelopen dagen had gedaan. Hierna heb ik weer eens een stapje teruggenomen om zo opnieuw opzoek te gaan naar andere programma's. Ik had er enkele gevonden en allemaal getest. Uiteindelijk bleek het dat deze programma's niet echts meer doen dan die we al hadden gevonden. Hierna heb ik mijn dag afgesloten met dit ook te documenteren

6.3 Woensdag 05/04

Vandaag zaten we samen met iedereen over hoe ons stageproject gaat. Waar we met bezig zijn. Waar we aan vastlopen. Ook hadden we nieuwe specifieke taken gekregen die nu tot op het bot van telegram gaan. Hierna was het nog 1 uur tot aan de middag en hebben we de taken onderling verdeeld.

Na de middag ben ik begonnen met mezelf te verdienen in telegram bots. Eerst en vooral heb ik zitten opzoeken via welke taal je allemaal een telegram bot kunt maken. De opties waren Java en Python. Omdat mijn python skills beter zijn dan die van telegram. Heb ik hiervoor gekozen. Ik heb me ook beziggehouden met het juist installeren van de library en ineens gekoppeld aan GitHub. Zo heb ik versioning op mijn code.

6.4 Donderdag 06/04

Vandaag heb ik me een hele dag beziggehouden met het schrijven/ ontdekken van de telegram bot. De bot kan nog niet veel, dit komt omdat ik eerst de library zo goed mogelijk wil kennen. Zo kan ik een bot schrijven die 100% goed werkt. Ik heb hiervoor veel kennis opgedaan via YouTube en GitHub. Ook deed mijn laptop even moeilijk met python. Hierdoor ben ik 2u kwijtgespeeld, maar ik heb het wel opgelost gekregen. Op het einde van de dag had ik een telegram bot die je bijna alle basisfuncties kon vragen die er ter beschikking waren.

6.5 Vrijdag 07/04

Omdat ik me gisteren had beziggehouden met het leren van een telegram bot schrijven, heb ik me vandaag kunnen bezighouden met de effectieve bot ui te werken. Ik heb eerst zitten zoeken naar al een bestaand voorbeeld om zo een goede basis te hebben. Nadat ik er ongeveer eentje gevonden had ben ik beginnen met coderen. Tegen de middag was de basis van de bot af. Na mijn middagpauze ben ik bezig geweest met de lay-out van de bot beter te maken. Ook had ik kort een bootstrap website online gegooid. Zo kon de bot hierna

verwijzen. In deze website zit ook een canarytoken. Dit wil zeggen als iemand de website bezoekt, krijg ik een bericht hiervan met zijn locatie en IP-adres.

Na de bot schrijven heb ik me nog het laatste half uur beziggehouden met een alternatief van de broncode te zoeken. Dit was geen succes

7 WEEK 7 (10/04 – 14/04)

7.1 Maandag 10/04

Paasmaandag

7.2 Dinsdag 11/04

Vandaag heb ik mijn volledige dag gevuld met het bestuderen van de broncode van "thelethon". Hier heb ik een volledige analyse gedaan van de code om te kijken dat er nergens een functie inzit waar de Keys worden opgeslagen. Daarnaast heb ik ook een client geïnstalleerd. Deze heb ik dan via debug mode proberen uitlezen. Echter heb ik niks bijzonders gevonden

7.3 Woensdag 12/04

Vandaag had ik in de voormiddag me nog kort 2u op de broncode gezet. Daarna hadden we een meeting met iedereen om een onderzoek op gang te zetten. Tegen da middag was deze gedaan. Vervolgens. Vervolgens had ik via teleclient een connectie proberen opzetten via de CLI. Daarna had ik mijn tussentijdse evaluatie. Mijn stagementor was tevreden over het werk dat ik lever. Ze hadden geen grote werkpunten. Het enige dat ik meer moest doen, was meer documenteren wat mijn resultaten zijn. Na dit gesprek hadden we nog een brainstorm over welke technologieën we konden toep passen. Hierna was de dag voorbij

7.4 Donderdag 13/04

Vandaag heb ik me een hele dag beziggehouden met mezelf Vue.JS aan te leren. Dit doe ik via een Udemy cursus. Dit was het enige wat ik vandaag heb gedaan. Ik heb in totaal 10% van de cursus kunnen afronden.

7.5 Vrijdag 14/04

Vandaag heb ik me weer verdiept op de Udemy cursus. In totaal ben ik tot aan 20% geraakt. Omdat de cursus veel oefeningen vraagt, duurt het lang voordat je verder kan naar het volgende hoofdstuk. Echter is de cursus wel goed en zorgt hij ervoor dat ik vue.js begrijp. Hierna had ik nog kort verschillende dingen gedocumenteerd en dan was de dag voorbij

8 WEEK 8 (17/04 – 21/04)

8.1 Maandag 17/04

Vandaag ben ik begonnen met eerst al mijn mails te lezen. Daarna hebben we samen met de 3 stagairs samengezeten om elkaar op de hoogte te brengen van wie wat allemaal gedaan heeft. Daarna ben ik de rest van de dag verder bezig geweest met mijn VUE.JS cursus. Op het einde van de dag was zat ik aan 29% van de hele cursus. Dit wil zetten dat ik al basiscomponenten van Vue nu heb gezien. Ook heb ik nog samen met Jentel een fake googledrive account aangemaakt

8.2 Dinsdag 18/04

Vandaag heb ik samen met Jentel onderzoek gedaan naar googledrive. Vervolgens heb ik nog onderzoek gedaan naar Snapchat, Dropbox en OneDrive. We moesten zoeken wat de beste manier was om iemand terug te vinden wanneer je met zijn account een folder hebt gedeeld. Dit was een heel interessant onderzoek, uit de conclusie komt dat googledrive de beste manier is om iemand achteraf terug te vinden.

Na de middag had ik les.

8.3 Woensdag 19/04

Vandaag hebben we in de voormiddag een presentatie gemaakt met daarin de vergelijking van onze ondervindingen. Hierna hadden we onze technologieën nog eens opnieuw beken en nagekeken. Zo weten we 100% zeker dat wat we op onze meeting gaan zeggen. Wel degelijk klopt. In de namiddag hadden we dan met zijn alle

8.4 Donderdag 21/04

Vandaag is mijn dag begonnen met weer mijn vue.js cursus. Vervolgens hebben we tot de middag met onze docent een meeting gehad. Deze ging over het verloop van de stage. In de namiddag ben ik weer bezig geweest met de vue.js cursus. Ik zit op het moment op 36% van de volledige cursus. Vandaag ging de cursus over childs, sister methods, events. Tot slot heb ik nog een collega geholpen met het overzetten van een tesseract file. Als specifieke file moesten ze een Albania language hebben. Hierna was mijn dag gedaan.

8.5 Vrijdag 21/04

Vandaag heb ik van thuis gewerkt. Als eerstes ben ik begonnen met wat mails te bekijken en te beantwoorden. Vervolgens kreeg ik nog de vraag van een collega i.v.m. een wetgeving. Hij zei me om dat eens op te zoeken op hun web portaal. Zo kon ik ook het portaal nog wat beter aanleren. Hierna ben ik dan bezig geweest het bekijken van de broncode van de telegram app. Deze moest eerst nog worden ge decompiled. Hier besefte ik dat ik kennis tekortkwam. Daarom had ik met behulp van chat-GPT verder onderzoek gedaan. Dit alles zonder succes. Hierna zat de dag erop

9 WEEK 9 (24/04 – 28/04)

9.1 Maandag 24/04

Vandaag zijn we de week begonnen met het proberen samenvatten van MTproto. Hierna heb ik een nieuw googleaccount en Hotmail account aangemaakt voor ons lopend onderzoek op een telegram groep. Dit moest via een VPN-connectie en een VM. Zo is er geen manier om mijn toestel eraan te herleiden. Na de middag hebben we met zijn alle samengezeten voor een korte briefing. Na deze briefing heb ik het googleaccount gevuld met AI gegenereerde content. Zo lijkt het een echt account. Tot slot heb ik mijn dag geëindigd met het verder onderzoeken van MTproto

9.2 Dinsdag 25/04

Vandaag had ik me weer eens een dagje gefocust op het mezelf aanleren van vue.js Omdat ze gisteren toch vermelde dat we dit nog konden gebruiken. Ik ben tot 54% geraakt. Het was de eerste keer in de cursus dat we een hele single page webapp hadden gemaakt. Na veel vloeken en knoeien was het me dan toch gelukt en had ik de website zelfstandig kunnen nabouwen. Dit heeft heel de dag geduurd

9.3 Woensdag 26/04

Vandaag ben ik verdergegaan met het onderzoeken van het sequence diagram van MTproto. In de namiddag had ik samen met Lieven en Silas een meeting van 3u over MTproto en de client to server. Deze was zeer productief. We waren opzoek gegaan naar de IP-adressen van telegram, de publieke en private RSA Keys, noem maar op. Hierna ging ik zelf verder met de eigen client en server opzetten. Sturen ik een script geschreven dat ik via mijn script berichten kan sturen in de echte telegram app en ook berichten kan lezen.

9.4 Donderdag 27/04

Vandaag had ik in de voormiddag les.

In de namiddag heb ik van thuis gewerkt. Ik heb me beziggehouden met mijn cursus over vuejs. Er was woensdag gezegd dat er nog een kans was da we dit nodig zouden hebben. Als dat het geval is. Moet ik dan ook een website proberen nabouwen. Ik ben tot 44% geraakt van de cursus. Hierna was mijn dag al om.

9.5 Vrijdag 28/04

Vandaag heb ik me beziggehouden met opnieuw proberen installeren van de telegram client. Dit is een externe client gemaakt door teamgram. De basis installaties zijn niet goed voor wat we nodig hebben. Daarom heb ik deze proberen installeren via docker. Echter duurde de docker build zo lang, dat ik hem op het einde van de dag heb moeten stoppen. Natuurlijk heb ik niet heel de dag zitten kijken naar een installatie. Tijdens is er me gevraagd geweest om een script te schrijven voor het exporteren van enkel en alleen mediabestanden uit een specifieke telegram groep. Na een uurtje had ik deze volledig af. In de

middag hadden we nog een informatief gesprek met de collega’s over het gaan werken bij de politie.

10 WEEK 10 (01/05 – 05/05)

10.1 Maandag 01/05 (feestdag)

/

10.2 Dinsdag 02/05

Vandaag ben jammer genoeg herbegonnen met de docker build installatie, voor de teamgram client. Tijdens de installatie heb ik me beziggehouden met het bouwen/ samenvoegen van de sequence diagram van de voorbije weken. Ik geloof nu dat ik een volledig beeld heb kunnen blootleggen van de telegram connectie. Hierna heb ik me beziggehouden met mijn vorig python bestand van afgelopen vrijdag. Ik ben nu een user interface aan het toevoegen om zo het programma gebruiksvriendelijk te maken voor iedereen. Ook vroeg er een collega of ik een oud pythonbestand kon aanpassen zodat het voor hem gebruiksvriendelijker is om te gebruiken. Hey python bestand leest SSID's uit van de routers en het opzoeken welke mobiele apparaten er zijn geconnecteerd met deze specifieke ssid. Nu wil mijn collega dit niet meer allemaal manueel doen. Hij wil dat de SSID's worden uitgelezen en dan automatische de mobiele toestellen worden gekoppeld. Deze info wil hij dan geëxporteerd hebben naar een CSV-bestand. Echter mag ik de database nog niet zien, want het is een lopend onderzoek. Hij gaat donderdag een nieuwe uitlezing doen en ervoor zorgen dat ik mee in het dossier zit. Zo krijg ik de toestemming om deze uit te bekijken en het bestand te bouwen.

10.3 Woensdag 03/05

Vandaag is eindelijk de dag dat we in contact gegaan zijn met de administrator van de telegramgroep. Nu was het moment om scenario 2 uit te voeren. We hadden rond 9u30 ons bericht verzonden. Om 10u30 heeft de persoon gereageerd. Toen hadden we onze credentials gestuurd. Sindsdien had hij niet meer gereageerd. Nu moesten ik wel heel de tijd opletten of er op het googleaccount iets veranderede. Tijdens het wachten heb ik nog een python script geschreven. Dit script zorgt ervoor dat je de chat historie van 1 specifiek persoon naar keuze kan exporteren. Tegen het einde van de dag hebben we telegram en het googleaccount gelaten voor wat het is. Het laatste uur heb ik me nog beziggehouden met het documenteren. Conclusie, vandaag was het een dag met lang wachten.

10.4 Donderdag 04/05

Vandaag had ik in de voormiddag les windows server. In de namiddag heb ik van thuis gewerkt. Ik heb me beziggehouden met mijn python scripts te verbeteren. Zo heb ik de kleine foutjes uit mijn programma's gehaald en heb ik me nog beziggehouden met de user interface van 1 van de 2 programma's. Hierna was eigenlijk mijn werkdag al voorbij.

10.5 Vrijdag 05/05

Vandaag was het een minder productieve dag, Dit kwam omdat ik me wat ziek voelde. Echter ben ik bezig geweest met het uitzoeken naar een goede manier om pythonscripts gebruiksvriendelijker te maken. Na wat opzoekwerk kwam ik uit op tkinter. Hier had ik dan een tutorial van gevolgd die ongeveer 2u duurde. Daarna ben ik bezig geweest met deze te implementeren in mijn code. Ook heb

ik me nog beziggehouden met een nieuw script schrijven dat verschillende dingen kon exporteren aan de hand van een keuzemenu. Na dit script zat mijn werkweek er alweer op.

11 WEEK 11 (08/05 – 12/05)

11.1 Maandag 08/05

Vandaag ben ik de dag begonnen met mijn mails lezen en ongeopende berichten te beantwoorden. Vervolgens heb ik me beziggehouden met het analyseren van de telegram exports. Wat bleek nu, deze exports zijn heel goed voor het eenvoudig bekijken van foto's en chats. Maar er is veel belangrijke data dat niet mee wordt geëxporteerd. Zoals message_ids, user_ids, etc.…

Na de middag heb ik me beziggehouden met het proberen exporteren van een lijst met al de user_ids. Echter lijkt dit niet mogelijk voor meer dan 1000 gebruikers in een groep. Er staat een max op het aantal bevragingen dat je kan doen in telegram. Normaal gezien kan je hier rondt werken, maar met user_ids heb je geen andere parameters om dat toe te passen. Tot slot heb ik al mijn code nog opgeschoond en universeel gemaakt. Zo worden credentials niet meer opgeslagen in de scripts. Maar in een .env bestand.

11.2 Dinsdag 09/05

Vandaag ben ik mijn dag begonnen met het documenteren van wat ik gisteren had gedaan. Hierna hadden we een meeting over het verdere verloop van de stage. Ze waren zeer positief over ons en hebben ons de laatste taken gegeven die we nog moesten doen om onze stage of te werken. Na de middag hadden we een meeting i.v.m. de exposure groepen. Hier werd de stand van zaken besproken en het verdere verloop. Tot slot heb ik me nog beziggehouden met een docker-compose file te schrijven om een telegram-bot op een server te zetten.

11.3 Woensdag 10/05

-Vandaag heb ik van thuis gewerkt. Dit omdat ik me niet 100% goed voelde. Daarom ben ik in de voormiddag niet super productief geweest. In de namiddag heb ik tijd gestoken in nieuwe OSINT tools te vinden voor telegram. Ik had op reddit een tool gevonden en heb deze uitgetest. Echter was deze tool outdated

11.4 Donderdag 11/05

Voormiddag les

In de namiddag heb ik me beziggehouden met het schrijven van een docker bestand voor de telegram bot. Dit is me op het einde van de dag gelukt met behulp van youtube en chatGPT

11.5 Vrijdag 12/05

Vandaag heb ik me volledig gefocust op het namaken van een website via vue.js. Dit heeft me een hele dag gekost. Op het einde van de dag was de website frontend volledig af. Ik heb gebruik gemaakt van vue, bootstrap en font-awsome. Ik moet enkel de site nog opdelen in verschillende componenten. Om zo de website deftig te laten werken.

12 WEEK 12 (15/05 – 19/05)

12.1 Maandag 15/05

Vandaag heb ik me beziggehouden met 2 dingen. In de voormiddag ben ik bezig geweest met een telegram bot via java. Dit om te kijken of er een groot verschil is tussen java en python.

In de namiddag heb ik me weer beziggehouden met mijn vue.js cursus.

12.2 Dinsdag 16/05

Vandaag heb ik de website onderverdeeld in componenten, zo kon ik routing toevoegen en de website gebruik vriendelijk maken. Naast dit ben ik nog verder gegaan aan mij vue.js cursus. Om zo de laatste aspecten aan de website te kunnen toevoegen

12.3 Woensdag 17/05

Vandaag heb ik me een hele dag beziggehouden met het nog eens proberen van de telegram server. Ik had een ander manier gevonden om dit via een windows client te proberen. Dit heeft me een hele dag gekost, maar jammer genoeg weeral zonder resultaat

12.4 Donderdag 18/05 (feestdag)

/

12.5 Vrijdag 19/05 (Brug)

/

13 WEEK 13 (22/05 – 26/05)

13.1 Donderdag 25/05

Vandaag hebben we heel de dag aan onze presentatie gewerkt. We hebben het werk verdeeld en onze documentatie nagekeken. Tegen Het einde van de dag was de presentatie eindelijk af.

13.2 Vrijdag 26/05

Vandaag hebben we onze presentatie gegeven over Telegram. Deze presentatie hadden we aan onze collega's gegeven. In de voormiddag hadden we nog wat geoefend en in de namiddag was dan de presentatie. Na de presentatie hebben we gegeten en heb ik nog geholpen met de IVI waar ik niks verder over mag vertellen. Tot slot heb ik eens gekeken naar let's encrypt.

14 WEEK 14 (29/05 – 02/06)

14.1 Maandag 29/05 (feestdag)

/

14.2 Dinsdag 30/05

Vandaag ben ik in de voormiddag naar school gegaan voor de uitleg van onze bachelor proef. In de namiddag heb ik me beziggehouden met het laatste aan te passen aan de website en de telegram bot. Hierna heb ik nog in de avond tijd gestoken in het SSL certificaat aan de webserver te koppelen.

14.3 Woensdag 31/05

In de voormiddag heb ik me beziggehouden met van het schrijven van documentatie. In de namiddag zijn we in interactie gegaan met de admin van de telegram groep. Echter mag ik hier niets meer over vertellen. Omdat dit vertrouwelijk is.

14.4 Donderdag 01/06

Teambuilding

14.5 Vrijdag 02/06

Vandaag was het de laatste stagedag, in de voormiddag heb ik vooral al mijn documentatie nog eens nagekeken en aangepast waar nodig. Vervolgens hebben Jentel en ik al de documenten verzameld zodat we deze samen konden afgeven. Na de middag hebben we nog een presentatie gegeven over telegram aan de mobfor. Zei konden de vorige keer er niet bij zijn. Tot slot heb ik nog al mijn materiaal gereset en alles achtergelaten aan hoe ik het heb gekregen. De dag eindigede met iedereen nog eens te bedanken.