Honeypot Anomaly Detection

Plan van aanpak

STAGE ITFactory

Alex Coulon – 3CCS02

Academiejaar 2021-2022

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

LID VAN ASSOCIATIE KU LEUVEN

THOMAS MORE

INHOUDSTAFEL

Inhoud

INHOUDSTAFEL 3
1 INLEIDING 4
2 STAGEBEDRIJF 5
3 OPDRACHT + AANLEIDING & ACHTERGROND 6
4 DOELSTELLING 7
5 INFORMATIE VERZAMELING & RAPPORTERING 8
6 PLANNING 9

1 INLEIDING

Gedurende 3 maanden zal ik een internationale Cyber Security stage afleggen bij Univerzita Tomáše Bati ve Zlíně. Op de faculteit 'Applied Informatics' zal je me terug vindend werkend aan het 'Honeypot Anomaly Detection' project dat ons is opgedragen samen met mijn 2 Belgische collega's Bram Geudens & Yannick Vandevenne.

Ik zou voor het begin van deze stage en het plan van aanpak graag Thomas More en hun personeelsleden willen bedanken voor het helpen met alles rondom deze internationale stage. Ook zou ik graag de UTB willen bedanken voor deze geweldige kans.

Dit plan van aanpak is opgesteld voor de afstudeerstage die ik gedurende 3 maanden zal ondergaan. Eerst zal de stageplaats beknopt voorgesteld worden samen met de opdracht omschrijving en de aanleiding hiervan. De doelstelling & toegevoegde waarde voor de UTB zal hierna aan bod komen. Hoe we dit gaan documenteren en rapporteren aan iedereen word uitgelegd en erna wordt onze planning nog even besproken.

2 STAGEBEDRIJF

Dit plan van aanpak is opgesteld voor een stage afgelegd bij Univerzita Tomáše Bati ve Zlíně, meer specifiek bij het departement voor Applied Informatics (U5).

Deze universiteit wordt afgekort als UTB in dit document. De UTB is gelokaliseerd doorheen heel Zlin (Czech Republic). Er zijn 6 faculteiten onder de UTB:

- Technologische Faculteit
- Faculteit voor Management en Economie
- Faculteit voor Multimediale Communicatie
- Faculteit voor Toegepaste Informatica
- Faculteit der Geesteswetenschappen
- Faculteit Logistiek en Crisismanagement

De UTB is een gemiddelde hogeschool in Tsjechië met maar liefst 190 cursussen in 115 verschillende programma's.

Wijzelf zijn onderdeel van de Faculteit Toegepaste Informatica / Applied Informatics in het gebouw U5. Hier hebben wij een internationaal kantoor gekregen met nog enkele andere stagairs in een IT laboratorium. Hier werken we voor David Malanik, een van de cybersecurity medewerkers en docent van onze faculteit.

Ik heb deze stageplaats gekozen door de interessante aanbiedingen binnen stageopdrachten. Doordat ze meerdere project voorstellen aangaven heb ik echt kunnen kiezen wat ik graag wou doen. Dit in combinatie met op een universiteit te kunnen werken en buiten de grootsteden was ik op slag verkocht.

Onze stage word mede mogelijk gemaakt, opgevolgd, beheerd en ondersteund door onderstaande personeelsleden:

UTB Stage Mentor: David Malaník

UTB Stage Supervisor: Marek kubalčík

UTB International Coördinator: Patrik foltýn

TMK Stage Begeleider: Liesbeth Kenens

TMK International Coordinator: Tinne Van Echelpoel

3 OPDRACHT + AANLEIDING & ACHTERGROND

De officiële opdracht omschrijving luid als volgt:

"Honeypot anomaly detection:

Main topic will be focused to implementation of honeypots techniques to computer network. Start with analyses of existing honeypot techniques and possibilities. Followed by the design of usable implementation for securing high value targets. Part of the solution will be implementation of communication between honeypots and central control node.

Second part will be focused to detect security anomalies in infrastructure. Testing solution will be compared with existing IDS/IPS system."

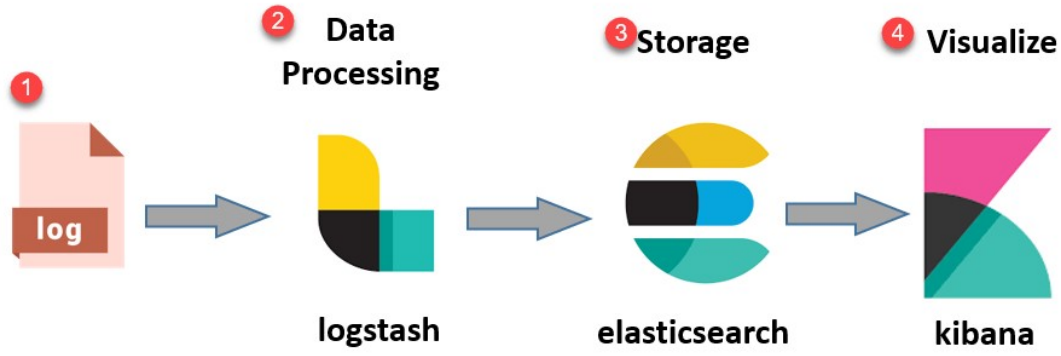
Na een verder uitbreidend gesprek over onze stageopdracht is het dus de bedoeling dat we 1 of meerdere honeypots soorten opzetten binnen het uitgebreide UTB netwerk (linux + windows + macos). Dit moeten we implementeren en hiervan ook een gepaste data output stream voorzien. Deze data van aanvallen moeten we op een webpagina visueel weergeven met alle informatie van bijvoorbeeld een IP adres met geolocatie en soort aanval.

Met de huidige situatie gaande in Rusland/Oekraïne merkt de UTB een serieuze aanvals-trafiek op hun netwerk (+- 20 000 aanvallen/maand). Momenteel zijn er geen honeypots actief binnen het netwerk, hier willen ze verandering in maken. Onze uitwerking zal dan ook gebruikt gaan worden in het UTB netwerk. Momenteel voorziet de ISP van de UTB een ids/ips oplossing. Dit geeft enkel aan dat er aanvallen gebeuren en vanaf welk ip, deze informatie is te beperkt. Met onze honeypots kunnen we de dat verder uitzoeken, analyseren en de nieuwste trends beter opvolgen. Een honeypot kan veel dieper ingaan op 1 bepaalde aanval, zo kan er beter uitgezocht worden wat het doel was van de aanval en hoe dit verkomen kan worden. Ook geeft een honeypot een veel betere datalogstream waarmee de data ook in een ELK stack gebruikt kan worden.

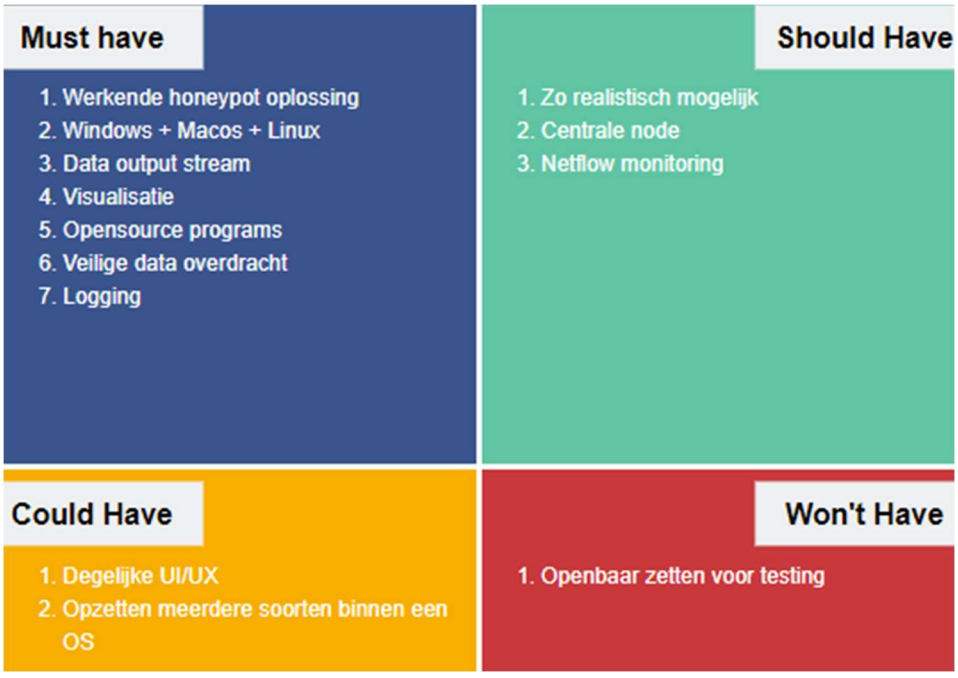
De stageopdracht is heel open gelaten zodat er ruimte is voor eigen inbreng, inspiratie & nieuwe mogelijkheden. Wel is er een serieuze voorkeur naar opensource software gegeven.

4 DOELSTELLING

Het einddoel van deze stage is om op het einde een volledig werkende honeypot implementatie te hebben draaien die in gebruik genomen kan worden in de UTB. De basis vereiste is een werkende honeypot met datastream naar buiten toe. Extra's zijn het weergeven van deze data op een ELK stack na een API call naar bijvoorbeeld een ip-information provider. Het vergelijken met welke aanvallen binnenkomen op onze honeypot als op die van een HAAS (honeypot as a service) zou een toegevoegde waarde hebben. De grootste vereiste is het gebruik van opensource software. Onze opzet zal dan ook het doel hebben om in productie een verbeterend effect achter te laten. Hiervan zal een beperkt verslag worden opgemaakt met de gekozen tools en finale documentatie over het proces en finaal product. Indien er tijd is kunnen we onze data trafiek vergelijken met al bestaande trafieken uit honeypot as a service via netflow monitoring. Hiernaast zou de oplossing kant en klaar moeten zijn zonder grote aanpassingen om over te stappen naar een productie omgeving.



De doelstellingen van ons project worden weergegeven in onderstaande MOSCOW analyse. We delen dit op in must have, should have, could have en won't have. Dit lijstje is opgesteld samen met de stagementor wat zijn eisen zijn en de doelstellingen van deze stage. Al deze items zijn in dit PVA besproken en verduidelijkt wat ze inhouden.



5 INFORMATIE VERZAMELING & RAPPORTERING

De UTB vraagt ons om gefaseerde verslagen in te dienen, maar niet al teveel tijd in lange documentatie te steken. Graag zouden ze een verslag hebben van onze onderzoeksfase en ons uiteindelijk besluit. Voor fase 2 willen ze een uitleg van onze proof-of-concept die we gaan maken. Ze willen geen technische uitleg tot op elke letter uitgelegd, in grote lijnen maar goed onderbouwd is wat ze wensen. Dit kan via de teams-chats gedeeld worden met de stagementor.

Voor onze stagebegeleider Liesbeth Kenens zullen we wekelijks een status-update bezorgen over onze prestaties deze week en plannen via het teams kanaal.

Intern zullen we een eigen documentatie bijhouden voor de info die we hebben verzameld en onderzocht. Hiernaast worden we 2wekelijks geacht een demo te doen met onze vooruitgang aan onze mentor.

6 PLANNING

Ons project splitsen we op in 5 fases.

1) Analysefase
2) Onderzoeksfase
3) POC-fase
4) Realisatiefase
5) Evaluatiefase

De eerste werkweek werken we aan geen enkele fase werken. Doorheen deze week zijn er meerdere meetings met onze mentor, supervisor, internationale dienst enzovoort. Het is een introductie week waar er niet verwacht word enig echt werk te kunnen verrichten.

In fase 1 gaan we onze opdracht analyseren, bespreken en verdere informatie vragen. Dit zal 1 week in beslag nemen om grondig te overleggen.

In fase 2 gaan we alle mogelijke opties onderzoeken, vergelijken en een besluit maken. De duratie van deze fase zal afhangen naargelang de mogelijkheden die beschikbaar zijn maar word geschat op 1-2weken.

In fase 3 gaan we een Proof of Concept opzetten met onze gekozen tools en applicaties uit fase 2. Dit zal vermoedelijk een 3 weken duren.

In fase 4 gaan we na goedkeuring van de UTB onze Proof of Concept ombouwen en verbeteren naar een volledig gebruiksklaar project met alles erop en eraan. Dit zal vermoedelijk een 2-tal weken duren om alles te optimaliseren.

In fase 5 gaan we ons werk evalueren samen met het team, mentor & supervisor en bijstellen waar nodig. Wanneer dit gebeurt zal vanaf hangen wanneer alle vorige fases afgerond zijn.

Er zullen 2 online terugkommomenten gepland worden. De eerste met als bedoeling een presentatie over het bedrijf en de opdracht te geven. Het 2de moment heeft als bedoeling het PVA te overlopen en een update over je vooruitgang te bespreken.

Om dit allemaal op een vlotte en duidelijke manier te laten werken zullen we Agile werken. S ’morgens vroeg beginnen we elke dag met een kleine scrum meeting wat we de vorige dag gedaan hebben, en wat onze plannen voor die dag zelf zijn. Tevens is dit een momentje om elkaars werkt te beoordelen en bij te sturen waar nodig. Op maandag houden we een grotere vergadering om de vorige week te evalueren en de volgende werk week te bespreken. Waar nodig zullen we geregeld samenkomen en overleggen.