Plan van aanpak I-Pass Project

Risk-Sniffer

Project voor Defensie, LeerDock Woensdrecht

Door Mick Luuring

Planning:

Ik ga door een semi iteratieve aanpak te hanteren mijn project aanpakken. Dit betekent dat ik een planning op ga stellen met (zeer waarschijnlijk) goedhaalbare deadlines, waar ik een extra marge voor neem mocht iets langer uitpakken dan gedacht. Dit zorgt ervoor dat ik eerst een deel af kan maken, voordat ik door kan met het volgende deel. Ik doe dit omdat ik vaak een bepaalde functie, of feature werkend moet hebben voordat ik door kan met het volgende onderdeel van dit project.

MIJN SCHEMA:

Ik ben van plan om een weekje eerder te beginnen met de voorbereiding van dit project, ik ga hier nog niet volledig aan de slag. Deze week is eigenlijk een week vakantie. Maar ik zelf vindt deze extra tijd een fijne bijkomstigheid in dit project. Hierdoor houd ik een 4 week durende planning aan in plaats van de 3 weken die er vanuit school voor gepland staan.

WEEK 0 (OPSTART + VOORBEREIDING):

- Onderzoek doen naar de mogelijkheid van een transparant proxy op meerdere systemen. (Windows, Linux)
- Sniffing/proxy framework testen en werkend krijgen op mijn 2 test laptops.
- Automatiseren van de installatie van deze framework voor makkelijk gebruik opdrachtgever.
- Netwerk schema uitdenken voor visualisatie van mijn gebruikte aanpak.

WEEK 1 (SNIFFING TOOL AF EN DATA LOGGEN):

Voorwaarden:

Ik heb de proxy framework werkend, en snap hoe ik deze bedien met python, ook moet ik een duidelijk inzicht hebben op hoe ik het netwerk op ga bouwen.

- Back log vorige week afmaken
- Documentatie week 0 net opstellen
- Programmeren van de data lees/log functie die websites moet loggen van http en hopelijk ook https.
- Log/leesfunctie optimaliseren zodat deze minder systeem resources gebruikt, zodat dit in de praktijk ook daadwerkelijk gebruikt kan worden.

WEEK 2 (DATA LOGGING AF EN RISICOANALYSE PROGRAMMA MAKEN)

Voorwaarden:

Ik heb de data logging/realtime analyse volledig werkend, waardoor ik minimaal de url van bezochte websites kan ontvangen, dit zorgt ervoor dat mijn programma zelf met de website kan verbinden en deze kan scrapen om deze te website te kunnen analyseren.

- Documentatie week 1 net opstellen
- Programmeren van de textmining / webmining functie

- Programmeren commandline interface (via ssh?) of in tijdsnood een config.txt file.
- Mits alles is afgerond en werkend kritiek vragen aan mijn opdrachtgever bij defensie.
- Locatie bezichtiging bij vliegbasis Woensdrecht

WEEK 3 (PROGRAMMA AF, KRITIEK VERWERKEN)

Voorwaarden:

Ik heb de programmatuur werkend (minimaal op basis niveau) en kan deze

- Functies testen op fouten / bug's
- Kritiek verwerken
- Installatie instructies maken
- Documentatie volledig
- Rapport afmaken

Punten van aandacht:

Ik moet de risicoanalyse die ik heb gedaan goed in acht nemen, hier heb ik rekening mee gehouden in mijn planning. Ook houd ik een Trello taskboard bij voor de visualisatie van mijn planning en taken die nog moeten gebeuren. Verder houd ik contact met mijn Ipass begeleider en mijn opdrachtgever bij defensie.

Bronnen die ik waarschijnlijk ga gebruiken voor informatie:

https://github.com/mitmproxy/mitmproxy

https://docs.mitmproxy.org/stable/

https://dl-acm-org.hu.idm.oclc.org/doi/abs/10.5555/954014.954024

https://dl-acm-org.hu.idm.oclc.org/doi/abs/10.1145/2888422.2888449

https://dl-acm-org.hu.idm.oclc.org/doi/abs/10.3115/1118149.1118160

https://dl-acm-org.hu.idm.oclc.org/doi/abs/10.1145/355214.355246

https://dl-acm-org.hu.idm.oclc.org/doi/abs/10.1145/1502650.1502728