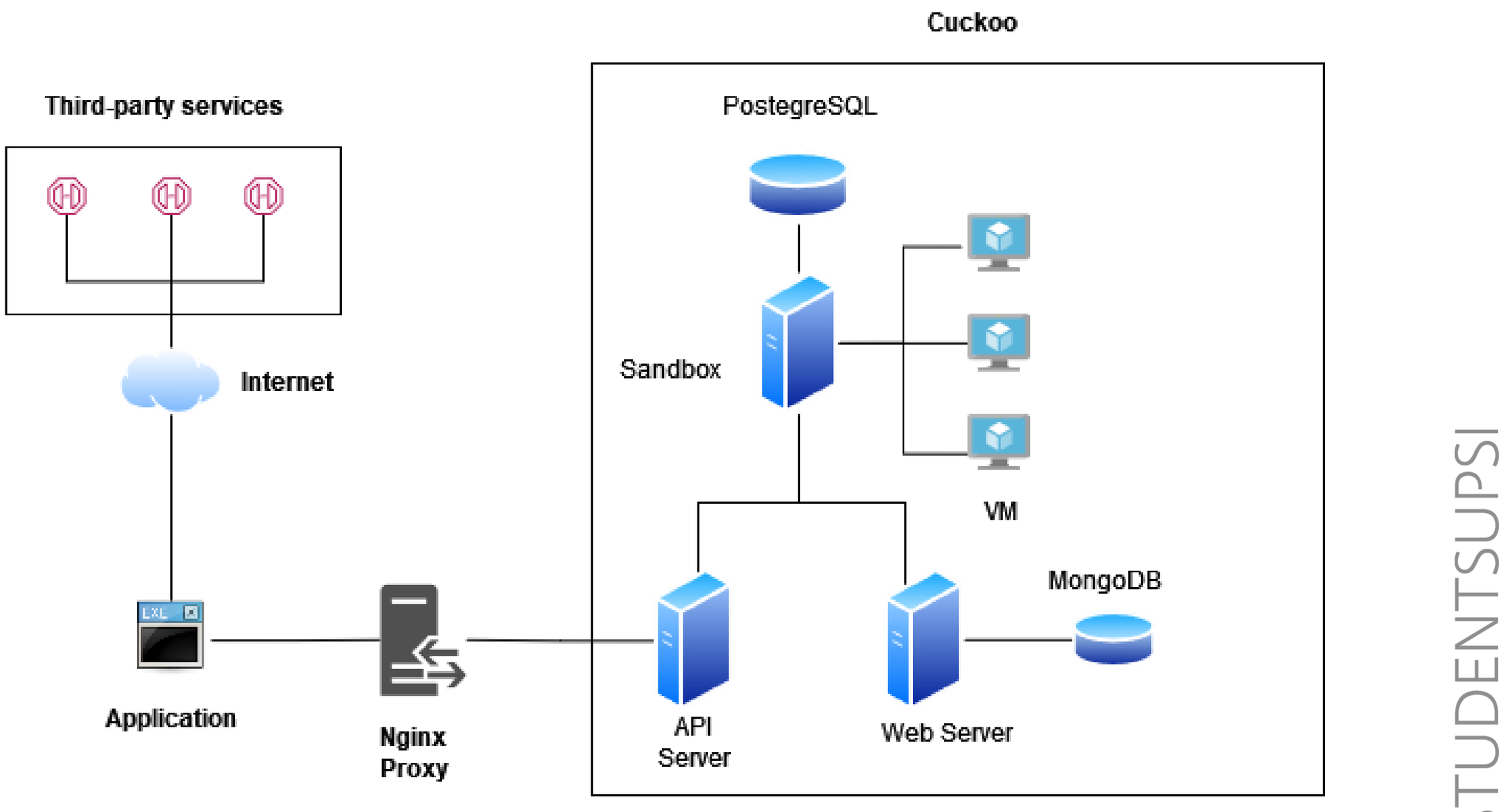
Scuola universitaria professionale della Svizzera italiana
Dipartimento tecnologie innovative

SUPSI

Malware Analysis and CTI Attribution Techniques

Studente/i	Relatore	Correlatore	Committente
Gregori Nicolas	Consoli Angelo - Mariotti Nesurinii Alice	Consoli Angelo	Consoli Angelo

Corso di laurea	N° Progetto	Anno	Data
Ingegneria informatica	C10463	2021/2022	20.06.2022



Abstract

Con la diffusione massiva di Internet, la circolazione di minacce informatiche in questi ultimi decenni è incrementata notevolmente. I malware, spesso generati da aggregati di codici malevoli, infettano sistemi informatici cercando di lasciare il più possibile un loro segno anche a causa degli utenti più inermi. L'unica metodologia di prevenzione è affidata all'analisi di file sospetti, nata allo scopo di mitigare sempre e più questo fenomeno. I processi di analisi statica e dinamica spesso vengono combinati in sistemi di analisi automatizzata, che permettono di analizzare il comportamento di un malware all'interno di un sistema isolato denominato sandbox. Ne esistono diversi in commercio: in particolare Cuckoo Sandbox: case-study del presente lavoro e che ha fornito un buon spunto per lo sviluppo di un portale web con funzioni simili. Il sistema sviluppato è in grado di fornire un banco di analisi del malware, appoggiandosi a servizi di terze parti per l'esecuzione dell'analisi tramite l'utilizzo di API. Il presente lavoro ha permesso di sviluppare una maggior consapevolezza e sensibilità a queste tematiche, sperando che anche in futuro numerose persone prestino più attenzione per evitare la diffusione di queste insidie.

Obiettivi

Il presente lavoro ha come scopo di fornire un sistema in grado di fornire un banco di analisi del malware, cercando di trarre più informazioni possibili. In particolare:

- Documentare le varie tecniche di analisi del malware, sia di tipo statico che dinamico.
- Effettuare un benchmarking di diverse sistemi di sandboxing
- Installare un sistema di sandboxing quale Cuckoo.
- Sviluppare un'infrastruttura, che mediante l'utilizzo di sistemi di sandboxing, sia in grado di estrarre più informazioni possibili sui campioni analizzati.
- Effettuare dei test del sistema utilizzando malware noti.
- Documentare tutto il sistema.

Conclusione

Il progetto ha permesso di acquisire più competenze professionali in questo ambito e una maggio sensibilità a queste tematiche. Tutto sommato il lavoro soddisfa i requisiti stipulati all' inizio, , anche se con alcune piccole criticità. Purtroppo a causa delle limitazioni imposte dalle versioni premium delle API, non è stato possibile raccogliere tutte le informazioni possibili e in modo molto dettagliato, ma comunque in grado di determinare la natura esatta del target in analisi. Si spera in futuro di riuscire ad integrare gli aspetti mancanti e di allargare l'utilizzo dell'applicativo su un'utenza più larga.