Zápisnica k 9. stretnutiu

Stretnutie sa konalo 31.1.2022 na Discorde.

Na stretnutí sa zúčastnili:

Účastník	Rola
Roderik Ploszek	Vedúci tímového projektu
Peter Švec	Vedúci tímového projektu
Pavol Sobota	Vedúci tímu za študentov
Samuel Hudák	Člen tímu
Andrej Tóth	Člen tímu
Martin Kudlačík	Člen tímu
Martin Bilka	Člen tímu
Michal Grznár	Člen tímu

Zápisnicu vypracoval Adam Štang

Vyhodnotenie úloh z predchádzajúceho stretnutia:

1. Andrej Tóth dokončil virtuálku – Je hotový image pre openstack.
2. Martin Bilka spravil research vzoriek ransomvéru – pripravil viacero vzoriek ktoré majú spravenú aj analýzu.

Opis stretnutia:

1. Dali sme návrh že na začiatok by sme chceli začať so vzorkami ktoré majú spravenú analýzu aby sme si mohli podľa toho skontrolovať správnosť výsledku.
2. Pavol Sobota navrhol začať so vzorkou ransomvéru z rodiny lockbit ktorý má vypracovanú dobrú analýzu ale nemá popísané metódy ako sa k danému výsledku autori dostali čiže by bola vhodná na začiatok.
3. Vedúci tímového projektu sa pýtali kde môžu tieto vzorky nájsť, zatiaľ sme ich nemali nikde tak sme sa dohodli že na to vytvoríme confluence a tam ich budeme dávať.
4. Rozprávali sme sa ako by mali vyzerať ďalšie vzorky na ktorých budeme pracovať, či môžu mať spravenú analýzu a podobne, na čo nám bolo povedané že môžu mať spravenú ale nie veľmi podrobnú analýzu aby sme sa mali od čoho odpichnúť.
5. Ďalej sme sa dohadovali o počte vzoriek ktoré by sme chceli stihnúť a dohodli sme sa že každý by mohol aspoň dve stihnúť.
6. Objasnili sme si na ktoré oblasti sa zameriame pri analýze jednotlivých vzoriek a to na – šifrovacie schémy, techniky obfuskácie, ukrývanie sa do cudzích procesov, ochrana voči technikám ladeniu, eskalácia privilégií a perzistencia.
7. Každý si musí vytvoriť účet na openstacku pre používanie virtuálky.

Rozdelenie úloh na nasledujúce dva týždne:

1. Každý z nás by sa mal pozrieť na jeden z ransomvérov.
2. Vedúci tímového projektu si pripravia ukážku ransomvéru.