Zápisnica k 5. stretnutiu

Stretnutie sa konalo 29.11.2021 na Discorde.

Na stretnutí sa zúčastnili:

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

Zápisnicu vypracoval Adam Štang

Vyhodnotenie úloh z predchádzajúceho stretnutia:

1. Andrej Tóth zazdielal obrazovku z JIRou, aby sa mohol každý vyjadriť ku svojej úlohe.
2. Andrej Tóth upratal Overleaf – dohodli sme sa že bude robiť poriadok na Overleaf
3. Andrej Tóth dopísal tému šírenie po sieti
4. Andrej Tóth začal robiť na cloud image na Flare – Je vytvorená VM - je to rozpracované
5. Pavol Sobota začal spisovať tému Obfuskácie a spôsoby deobfuskácie + v úvode doplnil text o malware analýzu, ciele, motiváciu
6. Samuel Hudák dokončil témy injection
7. Martin Kudlačík popísal šifrovanie - AS šifru, rozdelenie ransomvéru podľa šifier, generovanie kľúčov, nedostatky známych ransomvérov
8. Michal Grznár rozšíril a upravil text témy sandbox

Opis stretnutia:

1. Rozprávali sme sa čo by mala teória ešte obsahovať keďže už jej máme celkom dosť a nenapadali nás už iné témy, tak nám vedúci tímového projektu poradili že by sme mohli doplniť ešte témy Privilege escalation a Persistenciu.
2. Ďalej sme sa rozprávali že koľko toho očakávame v teoretickej časti dokumentácie a dohodli sme sa že ešte dopíšeme navrhnuté témy a prejdeme na prax.

3. Taktiež sme sa bavili či do teoretickej časti injection máme vkladať kód čo nám nebolo odporučené, ale aby sme namiesto toho vložili len všeobecný obrázok.
4. Spýtali sme sa či je potreba opísať nejaký konkrétny sandbox alebo poprípade porovnať sandboxy. Bolo nám povedané že môžeme ale aby to nebolo príliš dlhé oproti ostatným častiam.
5. Viedli sme debatu ohľadne virtuálky či ju spojazdniť už teraz alebo najprv dokončiť teóriu a zhodli sme sa že bude lepšie keď bude čím skôr aby sme si mohli testovať veci.
6. Boli nám povedané pripomienky k úvodu ako sa má písať a členiť.
7. Bolo nám odporučené formátovať text – aby sme zapojili aj tučné písmo a kurzívu na zvýraznenie.
8. Rozprávali sme sa ako treba vkladať obrázky, že musíme k nemu dať popis, pozičné značky, odkaz a podobne.

Rozdelenie úloh na nasledujúce dva týždne:

ID	Úloha	Kto	Do kedy
1	Spojazdniť virtuálku na Flare	Andrej Tóth	13.12.2021
2	Sandox - dokončiť	Michal Grznár	13.12.2021
3	Packer - dokočiť	Martin Bilka	13.12.2021
4	Urobiť zápisnicu	Adam Štang	13.12.2021
5	Úprava tímovej webstránky	Adam Štang	13.12.2021
6	Spracovať tému Privilege Escalation	Martin Kudlačík	13.12.2021
7	Injection - dokončiť	Samuel Hudák	13.12.2021
8	Spracovať tému Perzistencie	Pavol Sobota	13.12.2021