Zápisnica k 2. stretnutiu

Stretnutie sa konalo 18.10.2021 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
Andrej Tóth	Člen tímu
Adam Štang	Člen tímu
Samuel Hudák	Člen tímu
Martin Bilka	Člen tímu
Michal Grznár	Člen tímu

Zápisnicu vypísal Adam Štang.

Vyhodnotenie úloh z predchádzajúceho stretnutia:

1. Pavol sobota vypracoval ponuku a poslal ju Ing. Eugenovi Antalovi, PhD.
2. Andrej Tóth vytvoril Flare Virtual Machine ktorá slúži na analýzu ransomwérov , penetračné testy a podobne.
3. Všetci členovia tímu si pozreli cvičenia z predmetu Počítačová kriminalita z tohto roku zamerané na reverzné inžinierstvo, a Crackovanie ktoré sú dostupné na Youtube kanáli a tým si rozšírili poznatky v tejto problematike.
4. Pavol Sobota našiel skupinu reverzných inžinierov na discorde a pokúšal sa ich kontaktovať, avšak neúspešne ale poskytol nám link na túto skupinu odkiaľ môžeme čerpať nejaké informácie a tutoriály.
5. Všetci členovia tímu si prečítali knihu Márie Bielikovej – Ako úspešne riešiť projekt, ktorý nám pomôže bližšie pochopiť na aké zručnosti je tento predmet zameraný popri zadanej téme.
6. Pavol Sobota vytvoril tasky v JIRE.

Opis stretnutia:

1. Pavol Sobota ako vedúci tímu za študentov odprezentoval vedúcim tímu našu prácu od posledného spoločného stretnutia.
2. Následne začala diskusia kde sme rozoberali problémy a otázky ktoré sa vyskytli od posledného stretnutia.
3. Pre vytvorenie virtuálneho priestoru na spoločnú analýzu a vzdialené pripojenie sme prediskutovali dve alternatívy. Prvá bola využitie študentského účtu na Azure serveroch a vytvorenie virtuálneho stroja tam. Druhá alternatíva sa týkala

vytvorenia virtuálneho stroja na školských výpočtových zariadeniach (server alebo desktop)

4. Zhodli sme sa že je potreba založiť spoločné úložisko dát kde si budeme zhromažďovať materiály k nášmu projektu. Nakoniec sme sa dohodli že využijeme služby Google Disku čo si zobral na starosti Martin Bilka.
5. Mysleli sme trochu dopredu tak sme rozobrali aj otázku ohľadne jazyka ktorým má byť písaný finálny dokument nášho projektu pretože sme nevedeli či je potrebné ho písať v anglickom jazyku. Zistili sme že môže ale nemusí.
6. Pre písanie finálneho dokumentu sme prebrali rôzne možnosti. Vedúci tímu nám odporučili program LaTech avšak zatiaľ sme za nedohodli v čom budeme dokument písať.
7. Na prácu s ransomwérom potrebujeme zhromaždiť vzorky na testovanie. Diskutovali sme o dostupnosti vzoriek na internete. Vedúci tímu nám poradili aby sme si prešli nejaké blogy o ransomwéroch kde sa často nachádzajú spomínané vzorky.
8. Dohodli sme sa že nazbierané vzorky budeme posielať cvičiacim na github ktorý majú vytvorený na tento účel.
9. Prediskutovali sme aj dostupné programy na analýzu malwérov ako ANY.RUN, Hybrid Analysis, Malware center, Virus Total avšak prvé dve spomínané nám boli odporučené a nakoniec sme sa zhodli na Hybrid Analysis.
10. Taktiež nám bolo odporučené si najprv vybrať dekompilátor ktorým prevedieme binárny kód ransomwéru na kód v jayzku C aby sme následne daný ransomwér mohli analyzovať. Spomenuli sme dekompilátory ako RedDeads, Binary ninja, Cutter.re a Rada.re z ktorých si jeden vyberieme v priebehu tohto týžna.
11. Prebrali sme knihu Márie Bielikovej - Ako úspešne riešiť projekt, ktorej link sme dostali minulú konzultáciu aby sme si ju prečítali. Pochopili sme bližšie princípy práce na tímovom projekte.
12. Na koniec sme dostali odporúčanie od vedúcich projektu aby sme postup analýzy ransomwéru vykonali najprv staticky a postupne začať kombinovať s dynamickým postupom pre lepšie pochopenie a oboznámenie.

Rozdelenie úloh na nasledujúce dva týždne:

ID	Úloha	Kto	Do kedy
1	Organizácia Scrumu	Andrej Tóth	1.11.2021
2	Naďalej získavať informácie	Michal Grznár	1.11.2021
3	Pokračovať v rešerši článkov	Martin Bilka	1.11.2021
4	Urobiť zápisnicu	Adam Štang	1.11.2021
5	Úprava tímovej webstránky	Adam Štang	1.11.2021
6	Rozšíriť poznatky z reverzného inžinier.	Martin Kudlačík	1.11.2021

7	Naďalej sa oboznamovať s obfuskáciou	Samuel Hudák	1.11.2021
8	Vytvorenie úložiska pre materiály	Martin Bilka	1.11.2021
9	Vytvoriť Confluence	Pavol Sobota	1.11.2021