SLOVENSKÁ TECHNICKÁ
UNIVERZITA V BRATISLAVE
FAKULTA INFORMATIKY
A INFORMAČNÝCH TECHNOLÓGIÍ

Návrh zadania diplomovej práce

Predbežná verzia (vytváraná) [1]

Študent:

Meno, priezvisko, tituly:	Tomáš Belluš, Bc.
Študijný program:	Informačná bezpečnosť
Kontakt:	tomas.bellus@gmail.com

Výskumník:

Meno, priezvisko, tituly:	Tibor Csóka, Ing. PhD.

Projekt:

Názov:	Sledovanie zlovoľných činiteľov nástržným systémom
Názov v angličtine:	Bait network based monitoring of malicious actors
Miesto vypracovania:	Ústav počítačového inžinierstva a aplikovanej informatiky, FIIT STU
Oblasť problematiky:	Mitigačné a detekčné nástroje v informačnej bezpečnosti

Text návrhu zadania[2]

Úplné ochránenie produkčných systémov exponovaných do verejných sietí proti zlovoľným činiteľom neexistuje. Preto sa diplomová práca zameriava na výskum v oblasti informačnej bezpečnosti na detekciu a mitigáciu zlovoľnej aktivity za účelom zvyšovania bezpečnosti týchto systémov. Aktuálny výskum využíva nástroje (napr. honeynet, honeypot a sandbox) ako prostriedky pre oklamanie zlovoľného činiteľa s cieľom donútiť ho využiť ľubovoľné dostupné prostriedky pre realizáciu jeho agendy. Vysoká sofistikovanosť zlovoľných činiteľov kladie zvýšené nároky na nástroje používané pri výskume ich aktivity. Z toho dôsledku je potrebné na strane výskumníkov v informačnej bezpečnosti disponovať schopnosťou vytvárať vierohodne klamlivé ciele, ktoré motivujú činiteľov realizovať pokus o kompromitáciu nastraženého systému. V súčasnosti je možné vďaka širokému spektru open-source technológií realizovať systémy pre pozorovanie zlovoľnej aktivity i na úrovni vytvorenia samostatnej a uzavretej infraštruktúry. Analyzujte možnosti nástrojov typu honeynet, honeypot a sandbox a popíšte ich možné využite v skúmanej oblasti. Analyzujte možnosti realizácie systému honeynet tak, aby zbieral relevantnú telemetriu a dáta z pozorovanej aktivity zlovoľného činiteľa od vstupu do systému po jeho výstup zo systému predchádzjúci realizáciou zlovoľného cieľa. Navrhnite vhodné metódy, algoritmy alebo postupy s použitím open-source technológií vyplývajúcich z analýzy, ktoré umožnia následné pozorovanie a telemetriu uchovávať a dodatočne analyzovať. Navrhnuté metódy implementujte a aplikujte do honeynet systému a overte jeho použiteľnosť vo výskumnej oblasti.

[1] Vytlačiť obojstranne na jeden list papiera

[2] 150-200 slov (1200-1700 znakov), ktoré opisujú výskumný problém v kontexte súčasného stavu vrátane motivácie a smerov riešenia

Literatúra[3]

- Wenjun Fan, David Fernández, Zhihui Du, Adaptive and Flexible Virtual Honeynet, Tsinghua University, 2015
- Christian Abdelmassih, Container Orchestration in Security DemandingEnvironments at the Swedish Police Authority, Diplomová práca, 2018

V Bratislave dňa 10.12.2019

_____

Podpis študenta

[3] 2 vedecké zdroje, každý v samostatnej rubrike a s údajmi zodpovedajúcimi bibliografickým odkazom podľa normy STN ISO 690, ktoré sa viažu k téme zadania a preukazujú výskumnú povahu problému a jeho aktuálnosť (uveďte všetky potrebné údaje na identifikáciu zdroja, pričom uprednostnite vedecké príspevky v časopisoch a medzinárodných konferenciách)