

Supervisor assessment of Master's Thesis

Student: Sedlo Ondřej, Bc.

Title: Improvement of Adversarial Classification in Behavioral Analysis of Network Traffic Intended for Targeted Attack Detection (id 22643)

Supervisor: Homoliak Ivan, Ing., Ph.D., DITS FIT BUT

1. Assignment comments

Zadanie hodnotím ako nadpriemerne obtiažne a z môjho pohľadu bolo splnené vo všetkých bodoch. Zadanie vyžadovalo detailné pochopenie problematiky klasifikácie ako aj jej adversariálneho variantu, s ktorým študent experimentoval v rozsiahlej miere. Práca tiež zahrňovala obstaranie si vlastných vzoriek zraniteľných služieb a ich exploitov, čo vyžadovalo manuálne otestovanie a vyladenie exploitovania týchto zraniteľností na desiatkach virtualných mašín.

2. Literature usage

Študent si študijné pramene získaval samostatne na základe vlastného uváženia ale aj na základe doporučení vedúceho.

3. Assignment activity, consultation, communication

Aktivita behom tvorby práce bola na veľmi dobrej úrovni. Na schôdzky chodil študent dobre pripravený a priebežne podával informácie o stave práce. Na pripomienky študent vždy reagoval.

4. Assignment finalisation

Značná časť práce bola dokončená v dostatočnom predstihu a bola aj dôkladne konzultovaná. No niektoré experimenty boli dokončené až tesne pred odovzdaním čo bolo spôsobené ich vysokou časovou náročnosťou a opakovaného (niekoľko sto násobného) uskutočňovania z dôvodu štatistickej významnosti.

5. Publications, awards

Publikačná aktivita nie je známa, no v blízkej budúcnosti je v pláne dosiahnuté výsledky opublikovať v spolupráci s vedúcim práce.

6. Total assessment

excellent (A)

Prácu hodnotím stupňom A (**výborne**) pretože študent svedomito pracoval celý akademický rok, vzniknuté problémy riešil aj samostatne aj s využitím konzultácií. Študentovi sa podarilo vyrobiť novú verziu ASNМ datasetov zahrňujúcich adversariálne modifikácie, ktoré boli následne aj otestované naprieč rôznymi verziami datasetov.

In Brno 29 June 2020

Homoliak Ivan, Ing., Ph.D.
supervisor