Hodnocení vedoucího bakalářské práce

Student: Pisk Jiří
Téma: Detekce bezpečnostních incidentů v počítačové síti nemocnice (id 25055)
Vedoucí: Matoušek Petr, doc. Ing., Ph.D., M.A., UIFS FIT VUT

1. **Informace k zadání**
   Cílem práce bylo nakonfigurovat v produkční síti nemocnice honeypoty, ověřit možnost detekce síťových incidentů a implementovat automatizovaného zpracování událostí. Práce zahrnovala nejen rešerši dostupných implementací honeypotu, ale také zpracování a klasifikaci velkého množství dat, které honeypoty. Návrhované řešení je vytvořeno tak, aby nezahlcovalo správce sítě velkým množství nepodstatných událostí.

   Student všechny zadané úkoly úspěšně vyřešil.
2. **Práce s literaturou**
   Student využíval doporučenou literaturu i manuály k jednotlivým nástrojům, které instaloval.
3. **Aktivita během řešení, konzultace, komunikace**
   Student byl během řešení projektu aktivní, svůj postup a výsledky pravidelně konzultoval. Navrhoval vlastní způsoby řešení, které pak ověřoval experimenty.
4. **Aktivita při dokončování**
   Práce byla dokončena včas a její obsah konzultován.
5. **Publikační činnost, ocenění**
   Práce nebyla publikována.
6. **Souhrnné hodnocení** **výborně (A)**
   Student odvedl dobrou práci při řešení zadaného problémy. Oceňuje zejména nasazení detekčního systému v reálném prostředí krajské nemocnice i kombinaci více nástrojů pro zpracování incidentů typu Kibana, Logstash, Gitlab s klasifikací pomocí IDS systému Surikata, což přesahuje běžný obsah bakalářských prací.

Prohlášení: Uděluji VUT v Brně souhlas ke zveřejnění tohoto hodnocení v listinné i elektronické formě.

V Brně dne: 1. června 2022

Matoušek Petr, doc. Ing., Ph.D., M.A.
vedoucí práce