Fakulta Informatiky a Informačných Technológii
Slovenská Technická Univerzita

ZÁPISNICA 7

22.11.2022

Monitoring of LoRa IoT Devices

Tím č. 3 Molid

Miestnosť 1.19

Prítomní Ing. Alexander Valach

Bc. Michal Greguš

Bc. Adrián Ondov

Bc. Adam Melicher

Bc. Matej Laš

Bc. Dorota Gajdošová

Bc. Michal Minár

Neprítomní -

Obsah stretnutie

- Prezentácia úprav UDP packet forwarderu
- Ukážky zdrojového kódu udp packet forwarderu na vytváranie syslogov, zdrojový kód spĺňa definovanú metodiku písania zdrojového kódu
- Ukážka spôsobu pripojenia sa na jednotlivé nakonfigurované LoRa brány prostredníctvom lorafiit serveru + dokumentácia daného postupu pre ostatných členov tímu, prípadne iných používateľov
- Prezentácia zachytených syslogov v frontende systému SIEM (Kibana)
- Vygenerované logy sú zaznamenávané do /var/log/molid.log súboru
- Vedúci navrhol implementovať log rotation, aby logy nezaberali príliš veľa diskového priestoru
- Zaznamenané logy sú pomocou filebeatu odosielané do logstashu, ktorý ich spracuje a následne je možné ich prehliadať prostredníctvom Kibany
- V kibane je vytvorený index súbor každý deň
- Matej vytvára bashskript na pridanie ďalšej LoRa brány do siete
- V podstate došlo k ukončeniu implementácie systému SIEM a tým pádom je možné začať realizovať prípravu útokov a spôsoby detekcie v SIEMe
- Logy budú rotované týždenne a po dobu 4 týždňov budú uchovávané v rámci backupu

Úlohy a poznámky

1. Príprava inžinierskeho diela (Dorka, Michal, Adrián)
2. Príprava metodiky riadenia (Dorka, Michal, Adrián)

Autor Bc. Michal Greguš