INTEGRÁCIA MANAŽMENTU RIZÍK DO INFORMAČNÉHO SYSTÉMU

P3: Bc. Štefan Čulík; P1: Bc. Bruno Dvořák, Bc. Roman Ďurajka
Vedúca: Mgr. Jana Uramová, PhD.

Aplikované sieťové inžinierstvo

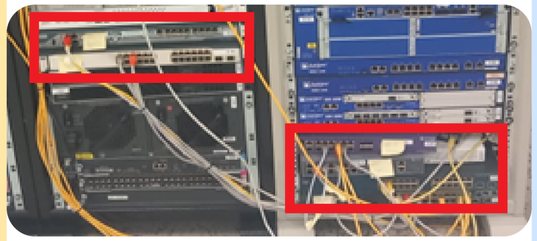
ŽILINSKÁ UNIVERZITA V ŽILINE
Fakulta riadenia
a informatiky

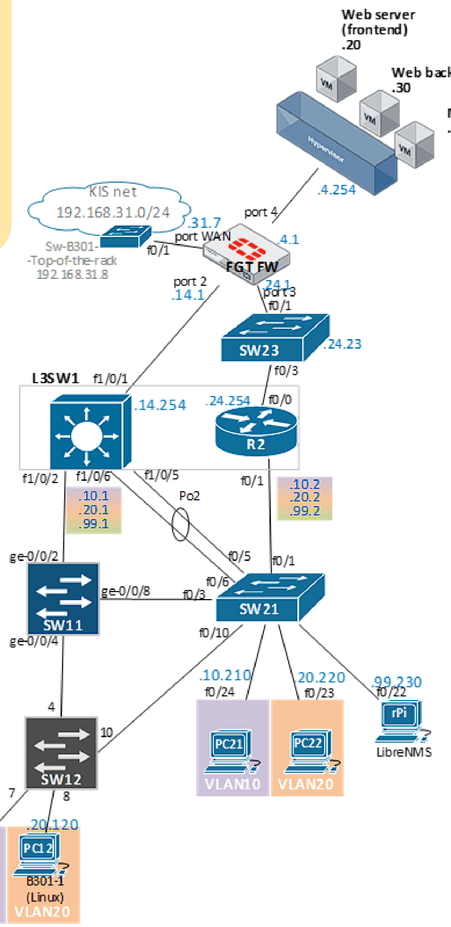
Motivácia

Prvým krokom informačnej bezpečnosti je identifikácia aktív. Na tento krok nadväzuje proces mapovania zraniteľností, hrozieb, rizík a ich následné riešenie. Po tomto nasleduje proces monitoringu aktív. O týchto krokoch pojednáva rodina štandardov ISO 27000. Tieto kroky sú veľmi dôležité pre informačnú bezpečnosť a zvyčajne sa vykonávajú manuálne.

Projekt a jeho ciele

Cieľmi projektu je viacero, ale dajú sa rozdeliť do štyroch kategórií: automatické skenovanie medziľahlých a koncových zariadení, skenovanie aplikácií na koncových zariadeniach, vylepšenie vizualizácie zhromaždených dát.





Výsledky

Pre testovacie účely sme si vytvorili topológiu, ktorá obsahuje medziľahlé zariadenia od rôznych výrobcov. Bolo nutné pridať aj koncové zariadenia. Na týchto zariadeniach beží aj operačný systém Windows a na iných beží Linux. Automatické skenovanie vykonávame pomocou aplikácie LibreNMS, ktorá využíva na zber dát protokol SNMP.
Táto aplikácia je schopná vykresliť aj mapy topológie.
V priebehu projektov sme si vytvorili skripty na skenovanie aplikácií na koncových zariadeniach. Tieto skripty sú vyrobené pre Bash (Linux) a PowerShell (Windows).
Ďalej spolupracujeme s externou firmou, ktorá využíva naše znalosti na vývin sondy.
Napokon vytvárame aplikáciu s GUI (React) na vylepšené zobrazenie topológií.

culik3@stud.uniza.sk