Projekt č. 3

PENETRAČNÍ TESTOVÁNÍ SONDY SONIOT

B0B32KTI- Komunikační technologie pro IoT

Ing. Bc. Marek Neruda, Ph.D., Ing. Tomáš Straka

Datum: 9 / 2022

1. Zadání projektu **3**

2. Doporučení k projektu **5**

1. Zadání projektu

Studenti si nastudují možnosti penetračního testování koncových zařízení skrze telekomunikační síť, např. článek[1] či článek[2] a další. Z rešerše vytvořené na základě nastudovaných poznatků si připraví sadu testů, resp. útoků a ty v rámci předem předpřipravené infrastruktury aplikují na sondu a to v libovolné variantě, tj. IDS nebo IPS. Studenti zároveň kontrolují logy z nástroje Suricata a identifikují ty, které značí zachycený test/útok.

Pro různé druhy útoků je požadováno zaznamenání těchto parametrů:

- typ útoku,
- zdroj a cíl útoku,
- byl útok zaznamenán? ANO/NE (v případě nejasného výsledku slovní zhodnocení),
- hardwarové využití sondy na typy útoků.

Studenti následně slovně zhodnotí a číselně vyhodnotí efektivnost detekce.

Pro tento projekt je připraven PC s předinstalovaným OS Kali Linux, který se standardně využívá jako nástroj pro digitální forenzní analýzu a penetrační testy. Každý tým má přístup k jednomu účtu v OS a tento PC vidí na všechny sondy. Z toho plyne, že každý tým dbá na to, aby aplikoval sadu útoků pouze na svoji sondu a v žádném případě nevyužíval tuto infrastrukturu k útokům mimo ní.

Výsledky měření vynesou studenti do protokolu v jasné a přehledné formě s patřičnými náležitostmi (za využití standardního formátování dokumentu včetně číslování) a to především:

- 1. strana: logo, název protokolu, jména osob, datum, místo, stručný závěr protokolu
- 2. a další strany: cíl projektu, měřené parametry, tabulkové stavy jednotlivých komponent, případně grafy se správně označenými osami
- popis testbedu/ů (veškeré souvislosti s měřením, tj. např. “měřeno bez provozu”, “měřeno při konstantním provozu 20Mbit/s” atd.)
- blokové schéma testbedu/ů
- literární zdroje a SW nástroje, které byly využity pro měření
- pokud byla provedena vlastní invence, tak zadokumentovat postup
- práce v týmu: rozdělení rolí, rozdělení zodpovědností, návrh časového plánu projektu, vybrané způsoby komunikace
- výsledky měření

[1] T. Zitta et al., "Penetration Testing of Intrusion Detection and Prevention System in Low-Performance Embedded IoT Device," 2018 18th International Conference on Mechatronics - Mechatronika (ME), 2018, pp. 1-5.

[2] SHIVAYOGIMATH, Chaitra N. An overview of network penetration testing. *International Journal of Research in Engineering and Technology*, 2014, 3.07: 5.

- zhodnocení: dosaženého plánu včetně časové alokace, plnění zodpovědností, plnění rolí, způsoby komunikace
- závěrečné zhodnocení výsledků testu obsahující dosažené hodnoty a statistické zhodnocení měřených hodnot, zhodnocení práce v týmu

Studenti zároveň navrhnou v závěru protokolu možné způsoby optimalizace na základě zjištěných poznatků, tj. např. odstranění nepotřebného SW a jiné.

2. Doporučení k projektu

Projekt je navržen tak, aby se studenti naučili hledat relevantní zdroje, tj. literaturu, zdrojové kódy, příkazy, SW a HW komponenty. Zároveň si osvojí základy penetračního testování v telekomunikační síti. Studenti na projektu pracují v laboratoři, nebo v domácím prostředí, ale vždy dbají na pravidla bezpečnosti a bezpečného užití HW a nevyužijí sondu k nekalé či trestné činnosti. Projekt je vypracováván s vědomím, že výsledky budou krom výstupního protokolu prezentovány na konci semestru před cvičícími a budou hodnoceny.

Doporučené otázky, které by si studenti měli klást následují.

- Jaké nástroje či příkazy, které jsou standardní součástí distribuce Kali Linux 2022.3 lze využít k získání odpovědí?
- Potřebuji na sondu instalovat další SW? Pokud ano, nevyužívá příliš HW zdrojů?
- Pokud vyžaduji pro testování více koncových stanic, nestačila by virtualizace, např. s využitím open-source nástroje VirtualBox[3]??
- Je námi vytvořený protokol reprodukovatelný jiným týmem?

[3] https://www.virtualbox.org/