СИМУЛИРАНЕ НА ПРОБИВИ В СИГУРНОСТТА И АНАЛИЗ НА РЕЗУЛТАТИТЕ ПО МЕТОДА “ZERO-TRUST”

Съдържание

(автоматично от headings)

Списък със съкращения

(сортиран по азбучен ред)

Увод

1-2 страници

Проактивното търсене на нови заплахи за информационната и комуникационна инфраструктура на организацията е важно. Освен „класическото“ сканиране за уязвимости в последните години се прилага и подхода за “breach attack simulation”- симулиране на атаки.

Оценката на сигурността може да се реализира с различени качествени и количествени методи. а в последните години се прилага и подхода “zero-trust”, който е динамичен и подходящ за актуалните фрагментирани инфраструктури.

Целта на дипломната работа е да се реализира симулиране на пробиви в сигурността на реална информационна и комуникационна инфраструктура, резултатите да се обработят и анализират по метода “Zero-trust” и да се обобщят препоръки за подобрение.

Глава 1

– “Zero-Trust” и “Breach Attack Simulation”

10-15 страници

Какво представлява zero-trust. Обобщена архитектура на модела. 5-Why/5-W. Защо “Zero-trust” е динамичен. Примерни системи.

Какво представлява “breach attack simulation”. Примерни системи. “Agent-based” и “agent-less’ подход. Силни и слаби страни.

Задължително се включват screen shots.

Глава 2 Платформа Infection Monkey

15-20 страници

Описание на Infection Monkey. Основни функционални характеристики. Системни изисквания. Приложение, силни и слаби страни. Включени методи за „атака“ и възможност за надграждане

Глава 3 – Симулиране на пробиви в сигурността на реална инфраструктура

15-20 страници

План за действие. Инсталиране на Infection Monkey и стартиране на анализ. Добавяне на нови модули и повторно стартиране на анализ.

Глава 4 – Обобщаване на резултатите

10-15 страници

Анализ на получените резултати от работата на Infection Monkey по метода “zero trust”.

Насоки за подобрение на сигурността.

Изводи

1-2 страници

Обобщение на целта на дипломната работа. Какво е постигнато в разработката и какво е бъдещото развитие.

Използвана литература

1. Zane Pokorny et. al, “The Threat Intelligence Workbook”, Second Edition, CyberEdge Press, 2019, ISBN: 978-1-948939-06-5.