БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра телекоммуникаций и информационных технологий

Аннотация к дипломной работе

АНАЛИЗ ЗАЩИЩЕННОСТИ СЕГМЕНТА СЕТИ НА ОСНОВЕ СКАНЕРОВ ЗАЩИЩЕННОСТИ

Поляков Роман Игоревич

Научный руководитель – кандидат физико-математических наук,

доцент Резников Г.К.

2018

РЕФЕРАТ

Дипломная работа 74 страницы, 20 рисунков (схемы, диаграммы), 5 таблиц, 16 источников, 3 приложения.

СЕТЕВОЙ СКАНЕР; АДАПТИВНАЯ БЕЗОПАСНОСТЬ СЕТИ; СЕТЕВОЙ ПОРТ; УЯЗВИМОСТЬ; СЕТЕВАЯ АТАКА; СПОСОБЫ ЗАКРЫТИЯ УЯЗВИМОСТЕЙ;

Объект исследования – сканер защищенности. В работе было исследовано 8 сетевых сканеров последних версий – «LanSpy 2.0», «Xscan v3.3», «Superscan 4.1», «Network Scanner», «NMap», «LanState Pro», «10-Страйк Сканирование Сети», «Nessus».

Цель работы - определить функциональности сетевого сканера как инструмента адаптивной безопасности сети, провести сравнительный анализ представленных на рынке программ данной категории. На основании полученных данных определить уязвимости исследуемой локальной сети. Произвести проверку по международным сертифицированным базам данных. Оценить степень риска уязвимостей, предложить методы решения

В работе проведен анализ быстродействия, информативности, функциональности и оптимизированности отчетной информации к дальнейшему использованию, пригодности сканера к построению карты исследуемой сети. Сканеры тестировались на операционных системах семейств Windows, Linux, Linux Server, а также на работающем сетевом окружении с количеством компьютеров более 150. Приведены и классифицированы по степени важности обнаруженные уязвимости, предложены действующие способы их закрытия, также приведены наиболее уязвимые к сетевым атакам порты TCP и UDP, для каждого сканера защищенности определен наиболее подходящий сценарий использования, а также оптимальные параметры.

РЭФЕРАТ

Дыпломная работа 74 старонкі, 20 малюнкаў (схемы, дыяграмы), 5 табліц, 16 крыніц, 3 дадатку.

СЕТКАВЫ СКАНЕР; АДАПТЫЎНАЯ БЯСПЕКА СЕТКІ; СЕТКАВЫ ПОРТ; СЕТКАВАЯ ПРАБОІНА; СЕТКАВАЯ АТАКА; СПОСАБЫ ЗАКРЫЦЦЯ СЕТКАВЫХ ПРАБОІН;

Аб'ект даследавання –сканер абароненасці сеткі. У дыпломнай рабоце было даследавана 8 сеткавых сканераў апошніх версій – «LanSpy 2.0», «Xscan v3.3», «Superscan 4.1», «Network Scanner», «NMap», «LanState Pro», «10-Страйк Сканирование Сети», «Nessus».

Мэта работы - вызначыць функцыянальнасці сеткавага сканера як інструмента адаптыўнай бяспекі сеткі, правесці параўнальны аналіз прадстаўленых на рынку праграм дадзенай катэгорыі. На базе атрыманых дадзеных вызначыць прабоіны доследнай лакальнай сеткі. Ажыццявіць праверку прабоін па міжнародным сертыфікаваным базам дадзеных. Вызначыць ступень рыска сеткавых прабоін, прапанаваць метады іх закрыцця.

У працы праведзены аналіз хуткадзейнасці, інфарматыўнасці, функцыянальнасці і аптымізаванасці справаздачнай інфармацыі сканераў да далейшага выкарыстання, прыдатнасці сканера да пабудовы карты доследнай сеткі. Сканеры тэставаліся на аперацыйных сістэмах сямейства Windows, Linux, Linux Server, а таксама на лакальным сеткавым асяроддзі з колькасцю камп'ютараў больш за 150. Прыведзены і класіфікаваны па ступені важнасці выяўленыя сеткавыя прабоіны, прапанаваныя дзейсныя спосабы іх закрыцця Таксама прыведзены найбольш важныя у кантэксце сеткавых атак TCP і UDP парты, для кожнага сканера вызначаны найбольш прыдатныя спосабы выкарыстання і асяроддзі, а таксама аптымальныя параметры.

ABSTRACT

The degree work 74 pages, 20 figures (diagrams, diagrams), 5 tables, 16 sources, 3 applications.

NETWORK SECURITY SCANNER; ADAPTIVE NETWORK SECURITY; NETWORK PORT; VULNERABILITY; NETWORK ATTACK; METHODS OF CLOSING VULNERABILITIES;

The object of the work is a network security scanner. The current work conducts research of 8 scanners of their latest versions: «LanSpy 2.0», «Xscan v3.3», «Superscan 4.1», «Network Scanner», «NMap», «LanState Pro», «10-Страйк Сканирование Сети», «Nessus».

The purpose of the research is to determine the functionality of a security scanner in context of being an instrument of the adaptive network security. Also this work includes the comparative analysis of network scanners available on the market. Based on the data, collected during the first two stages it was possible to determine the vulnerabilities in the targeted networks, classify them by risk and suggest the ways to close them. This is what the last part of the research is oriented on.

I conducted the research of scanners' performance, speed, functionality and the usability of each scanner's report to be a source of preferences for the further scans. Also I researched how the scanners can build a network topology based on their scan results. To test the scanners, I used several operation system families-Windows, Linux, Linux Server. The scans were conducted both on a specially created virtual local network environment and the real enterprise network with more than 150 hosts. As a result of the researches I show the comparative data for all the scanners and offer the best using scenario and parameters for each of them. Also I list typical vulnerabilities that can be found a regular LAN and group them by importance and. For each vulnerability I describe the ways to close it and the TCP/UDP port, through which the vulnerability can be exploited.