МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра телекоммуникаций и информационных технологий

АЛЕКСАНДРОВА
Диана Владимировна

РАЗРАБОТКА И АПРОБАЦИЯ МЕТОДИК ТЕСТИРОВАНИЯ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ НА ПРОНИКНОВЕНИЕ

Аннотация к дипломной работе

Научный руководитель – кандидат физ.-мат. наук,
доцент Ю.И. Воротницкий

Минск, 2023

РЕФЕРАТ

Дипломная работа: 55 с., 21 рис., 1 табл., 29 источника, 1 прил.

ЭКСПЛУАТАЦИЯ УЯЗВИМОСТЕЙ, АТАКИ, ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, МЕТОДИКИ ТЕСТИРОВАНИЯ, КИБЕРПОЛИГОН, ЗАЩИТА ДАННЫХ

Объектом исследования является корпоративная информационная система (киберполигон) и анализ ее потенциальных уязвимостей.

Цель работы – исследование различных методов, этапов, стандартов тестирования на проникновение и применение полученных знаний в процессе реализации тестирования корпоративной информационной системы (киберполигона) на проникновение.

В процессе выполнения дипломной работы был разработан киберполигон с помощью сетевого симулятора EVE-NG, который предоставляет набор инструментов для работы с виртуальными устройствами, построением сетей, коммутацией и управлением оборудования. Сам киберполигон представляет собой виртуальную среду, разработанную для отработки практических навыков выявления компютерных атак, расследования инцидентов информационной безопасности, отработки проведения аудита безопасности инфраструктуры, тестирования на проникновение, проведения киберобучений и соревнований.

После завершения разработки и настройки киберполигона было проведено тестирование на проникновение с использованием специально подобранных инструментов, включая Nmap и Metasploit Framework. Так же был произведен анализ результатов тестирования и были выделены рекомендаций по устранению повышению уровня защищенности корпоративной информационной системы.

РЭФЕРАТ

Дыпломная работа: 55 с., 21 мал., 1 табл., 29 крыніц, 1 дад.

ЭКСПЛУАТАЦЫЯ ЎРАЗЛІВАСЦЯЎ, АТАКІ, ТЭСТАВАННЕ НА ПРАНІКНЕННЕ, ІНФАРМАЦЫЙНАЯ БЯСПЕКА, МЕТОДЫКІ ТЭСТАВАННЯ, КІБЕРПАЛІГОН, АБАРОНА ДАНЫХ

Аб’ектам даследвання з’яўляецца карпаратыўная інфармацыйная сістэма (кіберпалігон) і аналіз яе патэнцыйных уразлівасцяў.

Мэта працы – даследаванне розных метадаў, этапаў, стандартаў тэставання на пранікненне і карыстанне атрыманых ведаў у працэсе рэалізацыі тэставання карпаратыўнай інфармацыйнай сістэмы (кіберпалігона) на пранікненне.

У працэсе выканання дыпломнай працы быў распрацаваны кіберпалігон з дапамогай сеткавага сімулятара EVE-NG, які прапануе набор прылад для працы з віртуальнымі ўстройствамі, пабудовай сетак, камутацыяй і кіраваннем абсталявання. Сам кіберпалігон уяўляе сабою віртуальнае асяроддзе, распрацаванае для адпрацоўкі практычных навыкаў выяўлення камп'ютарных атак, расследаванні інцыдэнтаў інфармацыйнай бяспекі, адпрацоўкі правядзення аўдыту бяспекі інфраструктуры, тэставання на пранікненне, правядзенні кібернавучанняў і спаборніцтваў.

Пасля завяршэння распрацоўкі і налады кіберпалігона было праведзена тэставанне на пранікненне з выкарыстаннем спецыяльна падабраных інструментаў, уключаючы Nmap і Metasploit Framework. Таксама быў зроблены аналіз вынікаў тэставання і былі дадзены рэкамендацый па павышэнні ўзроўню абароненасці карпаратыўнай інфармацыйнай сістэмы.

ABSTRACT

Thesis: 57 pages, 21 drawings, 1 table, 29 sources, 1 app.

VULNERABILITY EXPLOITATION, ATTACKS, PENETRATION TESTING, INFORMATION SECURITY, TESTING METHODOLOGIES, CYBER RANGE, DATA PROTECTION

The object of research is a corporate information system (cyber range) and analysis of its potential vulnerabilities.

The aim of this work is to explore various methods, stages, and standards of penetration testing and apply the acquired knowledge in the process of implementing penetration testing of the corporate information system (cyber range).

During the execution of the thesis, a cyber range was developed using the network simulator EVE-NG, which provides a set of tools for working with virtual devices, network construction, switching, and equipment management. The cyber range itself represents a virtual environment designed for practicing practical skills in detecting computer attacks, investigating security incidents, conducting security infrastructure audits, penetration testing, cyber training, and competitions.

After the development and configuration of the cyberpolygon was completed, distribution testing was carried out using special tools, including Nmap and the Metasploit Framework. An analysis of the test results was also carried out and identification was made to eliminate the increase in the level of security of the corporate information system.