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

БЫКОВ Георгий Алексеевич

РАЗРАБОТКА ПРОГРАММНО-АППАРАТНОЙ ЛОВУШКИ ДЛЯ КИБЕРПРЕСТУПНИКА

Аннотация к дипломной работе

Научный руководитель – старший преподаватель
А. М. Соболь

Минск, 2024

РЕФЕРАТ

Дипломная работа: 51 с., 27 рис., 1 табл., 9 источников.

КИБЕРБЕЗОПАСНОСТЬ, СИСТЕМЫ HONEYPOT, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЛОВУШКИ ДЛЯ КИБЕРПРЕСТУПНИКОВ, ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Объект исследования – средства для защиты и обнаружения от проникновения в информационные системы и разработка ловушки для киберпреступников.

Цель работы – изучение и анализ ловушек для киберпреступников как средств обнаружения проникновений в информационные системы, исследование существующих программных реализаций ловушек, разработка и тестирование системы-ловушки.

В работе рассматриваются общая характеристика Honeypot-систем, их классификация по различным параметрам: по степени интерактивности, по цели применения, по уровню адаптивности, по способу размещения, по типам атак. Описаны существующие реализации Honeypot-систем с низким и высоким уровнем взаимодействия, изучены их принципы работы и выделены основные преимущества и недостатки. Разработана собственная Honeypot-система для защиты от киберпреступников и для выявления новых типов уязвимостей и атак. Разработанная ловушка для киберпреступников имитирует реальную операционную систему Ubuntu 20.04 LTS, к которой реализована возможность подключения через SSH соединение, а также созданы уязвимости, эксплуатировав которые злоумышленники могут получить несанкционированный доступ к ловушке. Результатом дипломной работы является тестирование разработанной ловушки, которое представляет из себя имитацию атаки на проникновение в систему-ловушку и включает в себя следующие этапы атаки: сканирование системы, получение доступа к системе, сбор данных внутри системы и атака отказа в обслуживании.

Таким образом удалось разработать ловушку для киберпреступников, целью которой является стать полезным инструментом в руках пользователя для изучения новых типов атак.

РЭФЕРАТ

Дыпломная работа: 51 с., 27 мал., 1 табл., 9 крыніц.

КІБЕРБЯСПЕКА, СІСТЭМЫ HONEYPOT, ПРАГРАМНАЕ ЗАБЕСПЯЧЭННЕ ПАСТКІ ДЛЯ КІБЕРЗЛАЧЫНЦАЎ, ТЭСТАВАННЕ НА ПРАНІКНЕННЕ

Аб'ект даследавання – сродкі для абароны і выяўлення ад пранікнення ў інфармацыйныя сістэмы і распрацоўка пасткі для кіберзлачынцаў.

Мэта работы – вывучэнне і аналіз пастак для кіберзлачынцаў як сродкаў выяўлення пранікненняў у Інфармацыйныя сістэмы, даследаванне існуючых праграмных рэалізацый пастак, распрацоўка і тэставанне сістэмы-пасткі.

У працы разглядаюцца агульная характарыстыка Honeypot-сістэм, іх класіфікацыя па розных параметрах: па ступені інтэрактыўнасці, па мэты прымянення, па ўзроўні адаптыўнасці, па спосабе размяшчэння, па тыпах нападаў. Апісаны існуючыя рэалізацыі Honeypot-сістэм з нізкім і высокім узроўнем ўзаемадзеяння, вывучаны іх прынцыпы працы і вылучаны асноўныя перавагі і недахопы. Распрацавана ўласная Honeypot-сістэма для абароны ад кіберзлачынцаў і для выяўлення новых тыпаў уразлівасцяў і нападаў. Распрацаваная пастка для кіберзлачынцаў імітуе рэальную аперацыйную сістэму Ubuntu 20.04 LTS, да якой рэалізавана магчымасць падлучэння праз SSH злучэнне, а таксама створаны ўразлівасці, эксплуатаваўшы якія зламыснікі могуць атрымаць несанкцыянаваны доступ да пастцы. Вынікам дыпломнай працы з'яўляецца тэставанне распрацаванай пасткі, якое ўяўляе з сябе імітацыю атакі на пранікненне ў сістэму-пастку і ўключае ў сябе наступныя этапы атакі: сканаванне сістэмы, атрыманне доступу да сістэмы, збор дадзеных ўнутры сістэмы і атака адмовы ў абслугоўванні.

Такім чынам атрымалася распрацаваць пастку для кіберзлачынцаў, мэтай якой з'яўляецца стаць карысным інструментам у руках карыстальніка для вывучэння новых тыпаў нападаў.

ABSTRACT

Thesis: 51 pages, 27 drawings, 1 table, 9 sources.

CYBERSECURITY, HONEYPOT SYSTEMS, CYBERCRIMINAL TRAP SOFTWARE, PENETRATION TESTING

The object of research – means to protect and detect against penetration into information systems and the development of a trap for cyber criminals.

Objectives – the study and analysis of traps for cybercriminals as a means of detecting intrusions into information systems, the study of existing software implementations of traps, the development and testing of a trap system.

The paper considers the general characteristics of Honeypot systems, their classification according to various parameters: by the degree of interactivity, by the purpose of application, by the level of adaptability, by the method of placement, by the types of attacks. The existing implementations of Honeypot systems with low and high levels of interaction are described, their principles of operation are studied and the main advantages and disadvantages are highlighted. A proprietary Honeypot system has been developed to protect against cybercriminals and to identify new types of vulnerabilities and attacks. The developed trap for cybercriminals simulates the real Ubuntu 20.04 LTS operating system, to which the ability to connect via SSH connection is implemented, and vulnerabilities have been created, exploiting which attackers can gain unauthorized access to the trap. The result of the thesis is testing of the developed trap, which is a simulation of an attack to penetrate a trap system and includes the following stages of the attack: scanning the system, gaining access to the system, collecting data inside the system and a denial of service attack.

Thus, it was possible to develop a trap for cybercriminals, the purpose of which is to become a useful tool in the hands of the user to study new types of attacks.