НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

ФАКУЛЬТЕТ КІБЕРБЕЗПЕКИ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інформаційних технологій

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«СИСТЕМНИЙ АНАЛІЗ ПОТОКІВ КОМП'ЮТЕРНИХ АТАК В РОЗПОДІЛЕНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ»

Виконав: студент 2 курсу

Рівень: магістр

Галузь знань 12 «Інформаційні технології»

спеціальність 124 «Системний аналіз»

Базаров Дмитро Андрійович

Керівник: к.т.н., доцент

Щербина Юрій Володимирович

Рецензент: к.т.н., доцент

Задерейко Олександр Владиславович

Одеса – 2024

АНОТАЦІЯ

Базаров Д. А. Системний аналіз потоків комп’ютерних атак в розподілених інформаційно-комунікаційних системах – Кваліфікаційна робота студента 2-го курсу магістратури за спеціальності 124 «Системний аналіз», освітньою програмою «Аналіз та безпека даних».

В секторі безпеки розподілених інформаційно-комунікаційних систем існує велика проблема розподілених «атак на відмову в обслуговувані». Останні роки спостерігається стрімке зростання кількості таких атак, але способи попереджень та блокування цих атак доволі складні і потребують досліджень. Цим і зумовлена актуальність теми кваліфікаційної роботи.

Об’єктом дослідження є вплив розподілених «атак на відмову в обслуговувані» на ресурси розподілених інформаційно-комунікаційних систем. Предметом дослідження є способи організації захисту від DoS та DDoS атак.

Метою проведеного дослідження є аналіз розподілених «атак на відмову в обслуговувані» на ресурси розподілених інформаційно-комунікаційних систем та методів захисту від них.

В кваліфікаційній роботі розглядаються підходи до системного аналізу впливу розподілених «атак на відмову в обслуговувані» на мережні ресурси. Зроблено огляд сучасних нормативно-правових актів України, що регулюють організацію захисту в комп’ютерних мережах. Визначено складові частини системного підходу до аналізу впливу атак на працездатність системи. Проаналізовано основні види атак на відмову в обслуговувані та визначені слабкі місця стеку протоколів TCP/IP, що використовуються для подолання захисту. Розглянуто способи попереджень та блокування розподілених «атак на відмову в обслуговувані» та зроблено вибір систем захисту IDS/IPS та тестового середовища. Проведено аналіз ефективності та продуктивності систем запобігання вторгненням.

Ключові слова: інформаційно-комунікаційна система, DDoS атака, IDS/IPS система, стек протоколів TCP/IP, затримка сигналу.

ABSTRACT

Bazarov D. System analysis of computer attack flows in distributed information and communication systems - Qualification work of a 2nd-year master's student in the specialty 124 "System Analysis", educational program "System Analysis".

In the security sector of distributed information and communication systems, there is a big problem of distributed "Denial of Service attacks". In recent years, there has been a rapid increase in the number of such attacks, but the methods of warning and blocking these attacks are quite complex and require research. This determines the relevance of the subject of the qualification work.

The object of the study is the influence of distributed "Denial of Service attacks" on the resources of distributed information and communication systems. The subject of the study is methods of organizing protection against DoS and DDoS attacks.

The purpose of the conducted research is the analysis of distributed "Denial of Service attacks" on the resources of distributed information and communication systems and methods of protection against them.

In the qualification work, approaches to the system analysis of the impact of distributed "Denial of Service attacks" on network resources are considered. An overview of modern normative legal acts of Ukraine regulating the organization of protection in computer networks was made. The components of the system approach to analyzing the impact of attacks on system performance are defined. The main types of Denial-of-Service attacks on the served and identified weak points of the TCP/IP protocol stack used to overcome protection are analyzed. Methods of warnings and blocking of distributed "Denial of Service attacks" were considered, and a selection of IDS/IPS protection systems and a test environment was made. An analysis of the efficiency and productivity of intrusion prevention systems was carried out.

Keywords: information and communication system, DDoS attack, IDS/IPS system, TCP/IP protocol stack, response time, latency

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

КСЗІ (Complex System Information Protection) – комплексна система захисту інформації

СЗІ (Information Security System) – система захисту інформації

СУІБ (Information Security Management System) Система управління інформаційною безпекою

ISO (International Organization for Standardization) – Міжнародна організація по стандартизації

IEC (International Electrotechnical Committee) – Міжнародний електротехнічний комітет

DoS (Denial-of-Service attack) – Атака типу “відмови в обслуговуванні”

SYN (synchronize) – Запит на підключення по протоколу TCP.

ACK (acknowledges) – Відповідь з флагом на SYN запит “SYN-ACK”.

DNS (Domain Name System) – Система доменних імен

IDS (Intrusion detection system) – Система виявлення вторгнень

IPS (Intrusion prevention system) – Система запобігання вторгненням

DDoS(Distributed Denial of Service) – Розподілена атака типу “відмови в обслуговуванні”

TCP/IP(Transmission Control Protocol/Internet Protocol) – Набір інтернет-протоколів забезпечує наскрізну передачу даних

SMTP (Simple Mail Transfer Protocol) – Мережний простий протокол для передавання поштових повідомлень

SSL/TLS (Secure Sockets Layer/Transport Layer Security) – Протокол з’єднання з виконанням процедур автентифікації

ВСТУП

Сучасні досягнення в області інформаційно-комунікаційних технологій суттєво змінили способи доступу до даних, що передаються і обробляються в Internet-середовищі та зробили Web-сервіси дуже популярними у повсякденних бізнесових відносинах. Переважна більшість сучасних компаній з різних сегментів ринку, повністю переходять на роботу в онлайн-режимі. Цей тренд значно підсилюється процесами, пов'язаними з платіжними онлайн-операціями. У той самий час, навіть коротке переривання користувачам доступу до таких сервісів, приводить не тільки до втрати довіри їх постачальникам, але й може викликати суттєві матеріальні втрати.

На даний момент, одною з головних проблем інформаційної безпеки, є захист корпоративних інформаційних веб-ресурсів від зовнішніх атак. Досвід показує, що у подібних ситуаціях використання організованого системного захисту є критичним та необхідним.

Дуже важливим є дослідження найбільш розповсюджених мережних атак, та способів обмеження їх впливу. Значною часткою таких атак є розподілені «атаки на відмову в обслуговувані», кількість таких атак зросла в 2023 році на 117%, порівнюючи с 2022 роком. Впровадження в інформаційно-комунікаційні системи ефективних способів боротьби з DoS і DDoS-атаками потребує постійних досліджень. В силу військової агресії з боку Росії, загострилась актуальність дослідження розподілених «атак на відмову в обслуговувані» та створення та реалізація методів захисту інформаційно-комунікаційних систем від таких атак. Цим і зумовлена актуальність теми кваліфікаційної роботи.

Для рішення даної проблеми можливо використати декілька підходів. В кваліфікаційний роботі досліджено шлях впровадження в інформаційно-комунікаційних системи додаткового обладнання, яке може попередити та блокувати DoS і DDoS-атаки.

Проведене дослідження стосовно потоків комп'ютерних атак в розподілених інформаційно-комунікаційних системах базується на системному аналізі

результатів сучасних розробок вітчизняних та іноземних науковців. В даної кваліфікаційній роботі використовувалися наукові публікації наступних авторів: Матусяк І.В., Козак Р.О., C. Douligeris, A. Mitrokotsa, Christos D., Aikaterini M. та ін.

Метою проведеного дослідження є аналіз розподілених «атак на відмову в обслуговувані» на ресурси розподілених інформаційно-комунікаційних систем та методів захисту від них.

Для досягнення поставленої мети в кваліфікаційній роботі необхідно вирішити наступні **завдання**:

– провести дослідження предметної області з точки зору системного аналізу;

– проаналізувати теоретичні аспекти системного підходу до вирішення проблем забезпечення захисту мережних інформаційних ресурсів;

– визначити вразливості стеку протоколу TCP/IP на його різних рівнях, з точки зору їх використання для організації «атак на відмову в обслуговувані»;

– провести аналіз існуючих показників ефективності системи та на його основі обрати метод оцінки захисту;

– провести дослідження впливу «атак на відмову в обслуговуванні» в різних тестових середовищах та проаналізувати результати дослідження.

Об'єктом дослідження є вплив розподілених «атак на відмову в обслуговувані» на ресурси розподілених інформаційно-комунікаційних систем.

Предметом дослідження є способи організації захисту від DoS та DDoS атак.

В кваліфікаційній роботі використовувалися загальнонаукові та спеціальні методи наукового дослідження такі, як системний аналіз, моделювання, порівняння, класифікації тощо.

Теоретичне значення проведеного дослідження полягає в тому, що було узагальнено наукові знання щодо питань організації «атак на відмову в обслуговуванні».

Практичне значення одержаних результатів полягає у розробці тестової системи захисту від «атак на відмову в обслуговуванні» та отримано і проаналізовано результати тестування.

Структура кваліфікаційної роботи відповідає меті та завданням дослідження і складається зі вступу, основної частини з трьох розділів, висновків та списку використаних джерел. Робота викладена на 58 сторінках, містить 26 рисунків, 2 таблиці. Список використаних джерел включає 29 джерел.

ВИСНОВКИ

Кваліфікаційна робота була присвячена аналізу проблеми розподілених «атак на відмову в обслуговувані».

В ході дослідження були отримані наступні результати:

1. Проведено аналіз проблеми захисту мережних інформаційних ресурсів від «атак на відмову в обслуговуванні» та визначено підходи системного аналізу для оцінки їх впливу.

2. На основі системного підходу визначено, що складовими напрямами створення систем захисту є нормативно-правове забезпечення захисту, організаційні міри та програмно-технічне забезпечення.

3. Виконано аналіз актуальних на даний час в Internet-середовищі DoS і DDOS-атак на програмні додатки, розміщені на Web-сайтах копаній. Визначено цілі таких атак та розглянуто і виявлено слабкі місця у стеку протоколів обміну даними TCP/IP.

4. Проаналізовано основні сценарії поширених розподілених DDOS-атак з використанням Internet-ботів, і зрблено висновок про те, що виявлення розподілених DDOS-атак відбувається тільки після скоєння нападу, і основна задача захисту полягає у зменшені негативних наслідків шляхом перекриття доступу Internet-ботам мережних програмно-апаратних ресурсів Web-сайту, що є об’єктом атаки. З урахуванням цього, ефективна система захисту від розподілених DDOS-атак потребує використання фільтрації вхідного трафіку або підключення зовнішнього захисту на транспортному і прикладному рівнях.

5. Розглянуті способи попереджень та блокування розподілених мережних атак та проведено порівняльний аналіз вільних програмних рішень запобігання розподіленим мережним атакам IDS/IPS Snort і Suricata.

6. Проведено дослідження ефективності та продуктивності систем запобігання розподіленим мережним атакам та виконано порівняльний аналіз впливу IDS/IPS Snort і Suricata на ефективність мережної системи протягом атаки та при відсутності атак.