МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧОРНОМОРСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ПЕТРА МОГИЛИ

Костік Світлана Сергіївна

УДК 004.75

МЕТОДИ ТА ПІДХОДИ ДЛЯ ТЕСТУВАННЯ ВЕБ-СЕРВЕРІВ ПРИ НИЗЬКІЙ ПРОПУСКНІЙ ЗДАТНОСТІ КАНАЛУ ЗВ'ЯЗКУ

122 – Комп'ютерні науки

Автореферат
магістерської наукової роботи на здобуття освітньої кваліфікації
«Магістр комп'ютерних наук»

Миколаїв – 2019

Магістерська наукова робота є рукопис.

Робота виконана в Чорноморському національному університеті імені Петра Могили Міністерства освіти і науки України на кафедрі інтелектуальних інформаційних систем

Науковий керівник: к.т.н., доцент (б.в.з.) кафедри інтелектуальних інформаційних систем Сіденко Євген Вікторович

Рецензент: к.т.н., доцент, доцент кафедри комп'ютерної інженерії Журавська Ірина Миколаївна

Захист відбудеться 25 лютого 2019 р. о $9^{\underline{30}}$ год. на засіданні екзаменаційної комісії (ауд. 2-403) у Чорноморському національному університеті імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

З магістерською науковою роботою можна ознайомитися в бібліотеці Чорноморського національного університету імені Петра Могили за адресою: 54003, м. Миколаїв, вул. 68-ми Десантників, 10.

Автореферат представлений 25 лютого 2019 р.

Секретар
екзаменаційної комісії,
к.пед.н., доцент Н. М. Болюбаш

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Актуальність даної наукової роботи полягає в тому, що в останні роки все більше сервісів стають загальнодоступними у мережі Інтернет (веб-сайти, відеохостинги, соціальні мережі, тощо). Ними користуються все більше людей, а відтак все більше уваги мережевим сервісам приділяють зловмисники. Серед найпоширеніших загроз для мережевих сервісів є відмова в обслуговуванні (DoS, DDoS). В наш час DDoS-атаки збільшилися в силі, частоті та складності. Зловмисники постійно вдосконалюють свої навички та змінюють свій режим роботи, використовуючи новітні технології для запуску диверсифікованих DDoS-атак. Незважаючи на те, що дослідники запропонували багато рішень для виявлення, запобігання або пом'якшення DDoS-атак, але зловмисники все ще постійно розробляють нові методи і засоби, щоб обійти ці контрзаходи. Є ряд доступних інструментів, які можуть генерувати подібний, легітимний трафік, а також трафік атак і можуть легко обійти існуючі захисні рішення DDoS.

Метою магістерської наукової роботи є дослідження існуючих атак на веб-сервери на прикладному рівні, відтворення “повільних атак” на відмову в обслуговуванні за допомогою існуючих інструментів та знаходження оптимального значення мінімально низького каналу зв’язку для відмови в обслуговуванні веб-серверу.

Об’єкт досліджень – процес тестування веб-серверів на відмову в обслуговуванні при низькій пропускній здатності каналу зв’язку.

Предмет досліджень – методи та підходи для тестування веб-серверів на відмову в обслуговуванні.

Практичне значення отриманих результатів полягає в використанні отриманих знань з тестування веб-серверів на відмову веб-серверів в обслуговуванні, аби запобігти атаки на веб-сервер та веб-ресурси для захисту персональних та інших важливих даних від зловмисників.

Апробація результатів магістерської наукової роботи. Дана робота була представлена на XXI Всеукраїнській науково-методичній конференції “Могилянські читання – 2018”, яка була проведена в Миколаєві, 12 – 17 листопада 2018 року.

Публікації. Результати магістерської наукової роботи надруковані в “[УДК 004.75]. Могилянські читання – 2018 : Досвід та тенденції розвитку суспільства в Україні: глобальний, національний та регіональний аспекти : XXI Всеукр. наук.-метод. конф. : тези доповідей Комп’ютерні науки. Технічна науки, Миколаїв, 12 – 17 листоп. 2018 р. / ЧНУ ім. Петра Могили. – Миколаїв: Вид-во ЧНУ ім. Петра Могили, 2018. – 39 – 41 с.”

Структура магістерської наукової роботи. Магістерська наукова робота складається із вступу, шести розділів, висновків, додатків. Загальний обсяг роботи складає 135 сторінок, 54 рисунків, 24 таблиць та 57 посилань на літературні джерела.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі магістерської наукової роботи було окреслено актуальність даної роботи, її мету, предмет та об’єкт досліджень, а також практичне значення.

В першому розділі було оглянуто основні визначення та поняття, які використовуються в магістерській науковій роботі, проаналізовано публікації та дослідження для тестування веб-серверів на відмову в обслуговуванні при низькій пропускній здатності каналу зв’язку.

Мережеві сервіси - інструменти, що полегшують роботу мережі. Зазвичай це забезпечується сервером (який може виконувати одну або більше служб) на основі мережевих протоколів, що виконуються на прикладному рівні в моделі взаємодії відкритих систем (OSI) мережі. Наприклад, система доменних імен (DNS), протокол динамічної конфігурації хоста (DHCP), протокол голосового зв'язку через Інтернет (VoIP), тощо.

Пропускна здатність мережі – описує максимальну швидкість передачі даних по мережі або підключенню до Інтернету. Він вимірює, скільки даних можна надсилати за певним з'єднанням за певний проміжок часу. Наприклад, gigabit Ethernet-з'єднання має пропускну здатність 1000 Мбіт/с (125 мегабайт в секунду). Підключення до Інтернету через кабельний модем може забезпечити пропускну здатність 25 Мбіт/с.

Мережева модель ISO/OSI (International Standards Organization / Open System Interconnection) описана стандартом ISO 7498. Модель є міжнародним стандартом для передачі даних. Згідно еталонної моделі взаємодії ВВС виділяють сім рівнів, створюючих область взаємодії відкритих систем: 7 – Прикладний (Application), 6 – Представницький (Presentation), 5 – Сеансовий (Session), 4 – Транспортний (Transport), 3 – Мережевий (Network), 2 – Канальний (Data Link), 1 – Фізичний (Physical). Основна мета цієї моделі полягає у тому, що кожному рівню відводиться конкретна роль. Завдяки цьому загальна задача передачі даних розподіляється на окремі конкретні задачі. Кожен рівень визначається групою стандартів, які включають дві специфікації: протокол і сервіс.

Веб-сервер – це комп'ютерна система, на якій розміщено веб-сайти. Він запускає веб-серверне ПЗ, таке як Apache або Microsoft IIS, яке надає доступ до розміщених веб-сторінок через Інтернет.

В другому розділі було проведено аналіз існуючих атак на мережевому, транспортному та прикладному рівнях моделі OSI. Також було розглянуто існуючі методи та підходи для виявлення та тестування “повільних атак” на відмову в обслуговуванні – аномальну систему контролю трафіку розроблену Джейкван Кімом та Джі-Хайонг Лі та WebSOS архітектуру (О. Констянтинов, А. Камра).

Модель OSI була створена ISO, щоб допомогти стандартизувати зв'язок між комп'ютерними системами. Він розділяє комунікації на сім різних рівнів (рис. 1), кожен з яких включає декілька стандартів, протоколів або інших типів послуг.

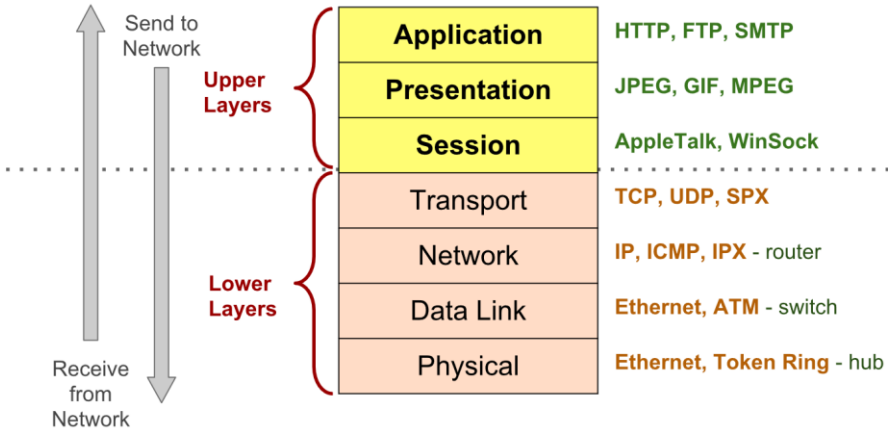

Рис. 1. Рівні моделі OSI

Модель OSI надає огляд того, як комп'ютерні системи спілкуються один з одним. Розробники ПЗ часто використовують цю модель під час написання ПЗ, яке вимагає підтримки мережі. Замість того, щоб відтворювати стек зв'язку з нуля, розробники програмного забезпечення повинні лише включати функції для певного рівня OSI, які використовують їх програми.

В третьому розділі було описано принцип роботи HTTP/HTTPS протоколів та їх вразливостей для подальшого тестування веб-серверів на відмову в обслуговуванні, було розглянуто архітектуру та принцип дії існуючих “повільних атак” DoS та DDoS на відмову в обслуговуванні на веб-сервери.

Протокол передачі гіпертексту (HTTP) – протокол прикладного рівня, необхідний для розподілених, спільних, гіпермедійних інформаційних систем. Це загальний об'єктно-орієнтований протокол, який може використовуватися для багатьох завдань, таких як сервери імен і розподілені системи управління об'єктами, через розширення методів запиту (команди). Особливістю HTTP є типізація подання даних, що дозволяє будувати системи незалежно від переданих даних.

HTTP використовується глобальною інформаційною ініціативою з 1990 року. Специфікація RFC1945 відображає загальне використання протоколу, який називається “HTTP / 1.0”.

Безпечний HTTP (S-HTTP) забезпечує захищені механізми зв'язку між HTTP-клієнт-сервер, щоб дозволити спонтанні комерційні транзакції для широкого колу додатків. Метою була розробка гнучкого протоколу, який підтримує кілька ортогональних режимів роботи, механізми керування ключами, моделі довіри, криптографічні алгоритми та формати інкапсуляції за допомогою узгодження опцій між сторонами для кожної транзакції.

В четвертому розділі було розглянуто існуючі веб-сервери та обрано веб-сервер для тестування на відмову в обслуговуванні. За допомогою R-U-Dead-Yet, Slowhttptest, Slowloris та OWASP Switchblade 4.0 інструментів було імітовано slowloris, slow post та slow read “повільні атаки ” на веб-сервер для тестування. Для знаходження мінімально низького каналу зв’язку для виведення з ладу веб-серверу був використаний інструмент Netlimiter 4.0. Результати досліджень, експериментів

були оформлені в таблиці. Після тестування було проаналізовано недоліки та переваги використаних інструментів та опис дій, які допоможуть попередити або полегшити “повільну атаку” на веб-сервер.

Для тестування було обрано тестовий веб-сайт, який знаходиться за посиланням http://mnr.info.tm/ на встановленому веб-сервері (рис. 1).

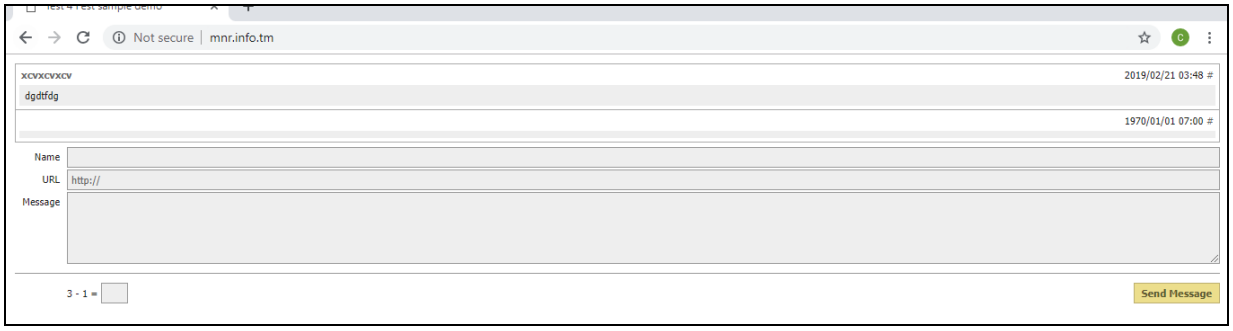

Рис. 1. Веб-сайт, обраний для тестування

На веб-сервер було розміщено даний веб-сайт за допомогою додавання конфігураційного файлу з налаштуваннями mnr.info.tm.conf в директорію apache2/sites-available. Зміст конфігураційного файлу mnr.info.tm.conf зображений на рис. 2.

```
root@Ubuntu-1504-vivid-64-minimal /home # cat /etc/apache2/sites-available/mnr.info.tm.conf
<VirtualHost *:80>
    ServerAdmin svitlana.kostik@globallogic.com
    ServerName mnr.info.tm
    DocumentRoot /var/www/html/demo
     <Directory /var/www/html/demo>
     AllowOverride All
     </Directory>

</VirtualHost>
```

Рис. 2. Зміст конфігураційного файлу mnr.info.tm.conf

Для регулювання пропускної здатності каналу зв’язку буде використано Netlimiter версії 4.0.37.0 для всіх обраних інструментів.

NetLimiter – утиліта, яка дозволяє збирати статистику про інтернет-трафік, що створюється будь-якими програмами, а також контролювати трафік: Netlimiter дозволяє виставляти обмеження на швидкості скачування/закачування для кожного додатка або з'єднання, здійснювати моніторинг їх мережевої активності. Програма веде детальну статистику в реальному часі, а при бажанні – за вказаний проміжок часу. Основні можливості:

1. Моніторинг трафіку додатків і підключень в реальному часі.

2. Можливість заблокувати обраним додаткам доступ в Інтернет.

3. Можливість заблокувати або обмежити передачу даних додатків, якщо було досягнуто заданий ліміт.

4. Довгострокова статистика інтернет-трафіку.

5. Обмеження максимальної швидкості передачі даних для будь-якої програми, запущеної на ПК.

6. Фільтри: трафік, протоколи, IP-адреса, додатки і т. д.

6. Планувальник завдань. Включення/Відключення обмежень і пріоритетів в заданий час.

7. Віддалене адміністрування.

8. Дозволи користувача. Призначення користувача, який зможе контролювати інтернет-трафік.

11. Схема трафіку. Швидкість завантаження/вивантаження даних для обраної програми або з'єднання.

Для того, щоб знайти найоптимальніше значення мінімально низького каналу зв’язку для відмови в обслуговуванні веб-серверу, будемо обмежувати швидкість завантаження за допомогою Netlimeter (рис. 3), змінюючи Limit-параметр для DL Limit (Download Level Limit) та UL Limit (Upload Level Limit).

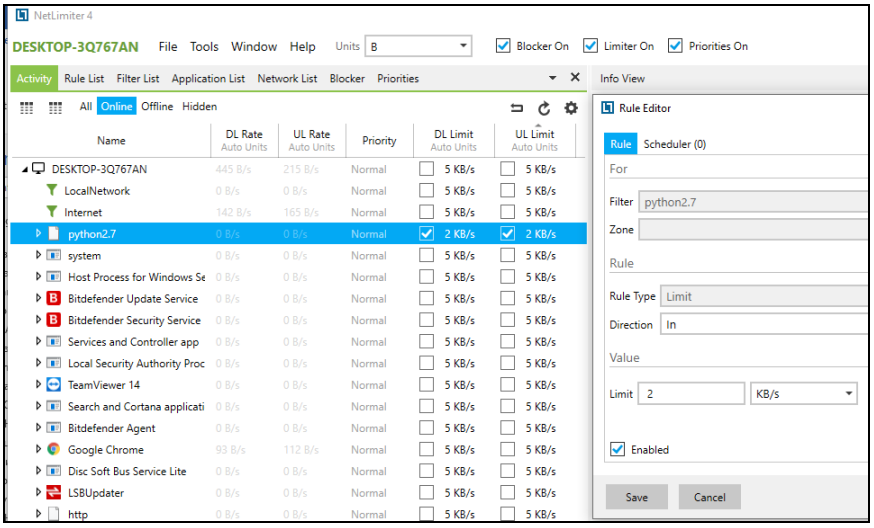

Рис. 3. Зміна параметрів DL та UL Limit

Застовані параметри для r-u-dead-yet інструменту продемонстровані на рис. 4.

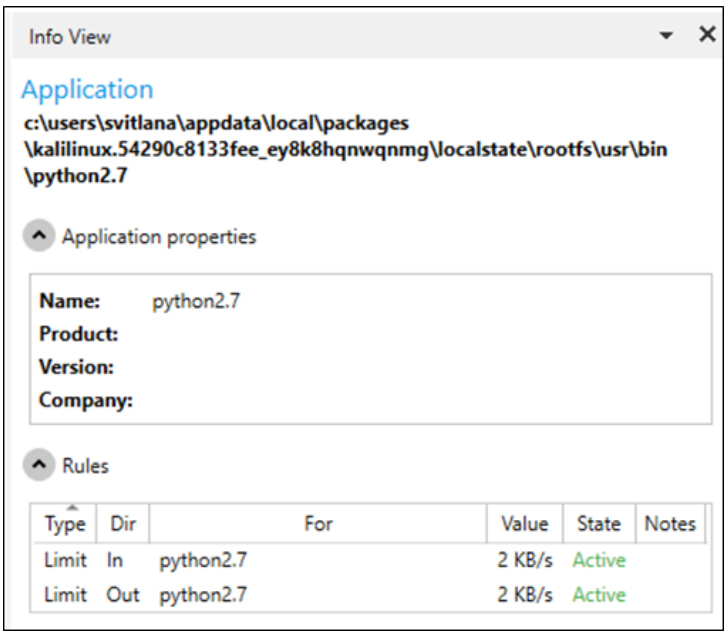

Рис. 4.10. Застосовані параметри ліміту рівня завантаження в Netlimiter

За допомогою інструментів slowhttptest, slowloris та OWASP Switchblade 4.0 було проведено імітацію атаки slowloris (slow headers) на веб-сервер. З табл. 1 видно, що OWASP Switchblade 4.0 виявив мінімально-можливий канал зв’язку для виведення веб-серверу з ладу.

Таблиця 1. Результати тестування веб-сервера на атаку slowloris (slow headers)

інструмент	атака	кількість з'єднань	мінміально низький канал зв'язку
slowloris	slowloris (slow headers)	150	512 байт/с
slowhttptest		300	3 кбайт/с
OWASP		**150**	**256 байт/с**

За допомогою інструментів slowhttptest, r-u-dead-yet та OWASP Switchblade 4.0 було проведено імітацію атаки slow post (rudy) на веб-сервер. З табл. 2 було виялено, що slowhttptest виявив мінімально-можливий канал зв’язку для виведення веб-серверу з ладу.

Таблиця 2. Результати тестування веб-сервера на атаку slow post (R-U-Dead-Yet)

інструмент	атака	кількість з'єднань	мінміально низький канал зв'язку
slowhttptest	slow post (rudy)	**150**	**512 байт/с**
OWASP		150	1.5 кбайт/с
RUDY		150	5 кбайт/с

За допомогою інструменту slowhttptest було проведено імітацію атаки slow read на веб-сервер. З табл. 3 було видно, що slowhttptest виявив мінімально-можливий канал зв’язку для виведення веб-серверу з ладу.

Таблиця 3. Результати тестування веб-сервера на атаку slow read

інструмент	атака	кількість з'єднань	мінміально низький канал зв'язку
slowhttptest	**slow read**	**600**	**5 кбайт/с**

При проведенні декількох досліджень, було виявлено, що інструменти slowhttptest та OWASP Switchblade 4.0 більш точно визначають оптимальне значення мінімального каналу зв’язку для атакування веб-серверу, оскільки вони можуть імітувати різні типи «повільних атак», мають багато параметрів для налаштування та стислий звіт про атакування та роботу веб-серверу.

У п’ятому розділі магістерської наукової роботи було розроблено вказівки до виконання лабораторних робіт із дисципліни - "Методи та системи тестування програмного забезпечення" .

У спеціальній частині магістерської роботи з «Охорони праці» було здійснено аналіз умов праці у офісному приміщенні ТОВ СП «НІБУЛОН», що займається транспортуванням, зберіганням, обробкою вантажів. Результатом є визначення мікрокліматичних умов, підбір спліт-системи кондиціонування, а також розробка інструктажу для забезпечення безпеки під час землетрусу на робочих місцях.

За результатами оцінки параметрів мікроклімату було з’ясовано, що такі параметри як температура, вологість та швидкість руху повітря у приміщенні знаходяться в межах оптимальних показників згідно з ДСН 3.3.6.042-99.

В результаті опрацювання правил поведінки під час землетрусу було розроблено інструктаж для працівників, яка описує дії у результаті виникнення землетрусу.

ЗАГАЛЬНІ ВИСНОВКИ

В даній магістерській роботі було проведено тестування веб-серверів на відмову в обслуговуванні при низькій пропускній здатності каналу зв’язку. Поставленими задачами при виконанні роботи були: ініціалізувати “повільні атаки” для тестового веб-серверу за допомогою існуючих інструментів; виявити необхідну кількість одночасних запитів різних типів атак для того, щоб привести сервер до відмови у обслуговуванні; для кожного типу атаки, в залежності від кількості необхідних одночасних запитів, визначити мінімальну пропускну здатність каналу зв’язку, достатню для проведення атаки на відмову веб-серверу в обслуговуванні.

В першому розділі було оглянуто основні визначення та поняття, які використовуються в магістерській науковій роботі. Також було проаналізовано публікації та дослідження для тестування веб-серверів на відмову в обслуговуванні при низькій пропускній здатності каналу зв’язку. Було сформульовано мету, предмет та об’єкт дослідження, актуальність наукової роботи.

В другому розділі було розглянуто рівні моделі OSI/ISO та проведено аналіз існуючих атак на третьому (Мережевому), четвертому (Транспортному) та сьомому (Прикладному) рівнях. Також було розглянуто існуючі методи та підходи для виявлення та тестування “повільних атак” на відмову в обслуговуванні, а саме Аномальна система контролю трафіку розроблену Джейкван Кімом та Джі-Хайонг Лі та WebSOS архітектуру (О. Констянтинов, А. Камра).

В третьому розділі було описано принцип роботи HTTP/HTTPS протоколів та їх вразливостей для подальшого тестування веб-серверів на відмову в обслуговуванні. Також було розглянуто архітектуру та принцип дії існуючих “повільних атак” DoS та DDoS на відмову в обслуговуванні на веб-сервери. Також було розглянуто інструменти для тестування веб-серверів, які в подальшому будуть використовуватися для тестування при низькій пропускній здатності каналу зв’язку.

В четвертому розділі було розглянуто існуючі веб-сервери та обрано веб-сервер для тестування на відмову в обслуговуванні. За допомогою R-U-Dead-Yet, Slowhttptest, Slowloris та OWASP Switchblade 4.0 інструментів було імітовано slowloris, slow post та slow read “повільні атаки ” на веб-сервер для тестування. Для

знаходження мінімально низького каналу зв’язку для виведення з ладу веб-серверу був використаний інструмент Netlimiter 4.0. Результати досліджень, експериментів були оформлені в таблиці. Після тестування було проаналізовано недоліки та переваги використаних інструментів та опис дій, які допоможуть попередити або полегшити “повільну атаку” на веб-сервер.

При виконанні магістерської наукової роботи були виконані поставлені задачі, крім імітації Slow SSL атаки на веб-сервер. Причиною була відсутність SSL сертифікату на тестовому середовищі.

АНОТАЦІЯ

Костік Світлана Сергіївна. Методи та підходи для веб-серверів при низькій пропускній здатності каналу зв'язку. – На правах рукопису.

Магістерська наукова робота на здобуття освітньої кваліфікації «Магістр комп'ютерних наук». – Чорноморський національний університет імені Петра Могили, Миколаїв, 2019.

Дана магістерська наукова робота спрямована на аналіз існуючих атак на веб-сервери на прикладному рівні, відтворення "повільних атак" на відмову в обслуговуванні та знаходження оптимального значення мінімально низького каналу зв'язку для відмови в обслуговуванні веб-серверу.

Об'єктом дослідження в даній роботі є процес тестування веб-серверів на відмову в обслуговуванні при низькій пропускній здатності каналу зв'язку.

Предмет досліджень – методи та підходи для тестування веб-серверів на відмову в обслуговуванні.

Проведені дослідження та розрахунки з тестування веб-серверів на відмову в обслуговуванні можуть бути використані для попередження та запобігання атак на веб-сервер та веб-ресурси для захисту персональних та інших важливих даних від зловмисників.

Магістерська робота складається з чотирьох розділів, методичної частини та спеціальної частини з охорони праці та безпеки у надзвичайних ситуаціях.

Розділ 1 містить наступні підрозділи:

– основні визначення та поняття;
– аналіз останніх публікацій та досліджень;
– постановка задачі.

Розділ 2 містить наступні підрозділи:

– аналіз існуючих атак на транспортному та мережевому рівнях, їх недоліки;
– прикладний рівень моделі OSI;
– аномальна система контролю трафіку;
– WebSOS.

Розділ 3 містить наступні підрозділи:

– принцип роботи HTTP/HTTPS протоколів;

– вразливості HTTP/HTTPS протоколів;

– протокол повільної передачі гіпертексту атаки на відмову в обслуговуванні;

– інструменти для тестування.

Розділ 4 містить наступні підрозділи:

– вибір веб-серверу для тестування;

– тестування за допомогою обраних інструментів:

– методи попередження атак.

У висновках наведено підсумки виконаної роботи.

В методичній частині до магістерської наукової роботи розроблено вказівки до виконання лабораторних робіт із дисципліни - "Методи та системи тестування програмного забезпечення" (Розділ 5).

В спеціальній частині "Охорона праці та безпека у надзвичайних ситуаціях" розглянуто охорону праці на робочих місцях відділу прикладного програмного забезпечення ТОВ СП «НІБУЛОН», опис обраного виробничого приміщення, робочих місць, їх обладнання та складання вихідних даних для кількісної оцінки умов праці, заходи щодо запобігання надзвичайних ситуаціях, пов’язаних з порушенням вимог пожежної безпеки (Розділ 6).

Робота має три додатки.

В цілому робота складається із 135 сторінок, 24 таблиць, 54 рисунків, в тому числі фахова частина складається із 96 сторінок, 19 таблиць, 37 рисунків.

Ключові слова: веб-сервер, мережева модель ISO/OSI, HTTP протокол, DoS, DDoS, Slow HTTP атаки, Slowloris, Slow Read, R-U-Dead-Yet, Slow SSL.

ABSTRACT

Kostik Svitlana. Методи та підходи для веб-серверів при низькій пропускній здатності каналу зв'язку. – On the rights of the manuscript.

Master's scientific work for obtaining an educational qualification "Master of Computer Science". – Petro Mohyla Black Sea National University, Nikolaev, 2019.

The given Master's Paper is directed at the analysis of existing attacks on web-servers at the application level, the reproduction of "slow attacks" on denial of service and finding the optimal value of the minimum low link for denial of service to the web server.

The object of research in this paper is the process of testing web servers for denial of service at low bandwidth communication channels.

The subject of research is methods and approaches for testing web servers for denial of service.

Researches and calculations for web server denial of service testing can be used to prevent and prevent attacks on the web server and web resources to protect personal and other important data from intruders.

The Master's Paper consists of four chapters, methodological part and a special part for labor protection and emergency safety.

Chapter 1 contains the following dubsections:

– basic definitions and concepts;

– analysis of recent publications and researches;

– formulation of the problem.

Chapter 2 contains the following subsections:

– analysis of existing Transport and Network Layers attacks, their disadvantages;

– Application Layer of OSI model;

– Abnormal Traffic Control System;

– WebSOS framework.

Chapter 3 contains the following subsections:

– the principle of HTTP/HTTPS protocols;
– HTTP/HTTPS protocols vulnerabilities;
– slow HTTP DoS attacks;
– tools for testing.

Chapter 4 contains the following subsections:

– the process of selection web-server for testing;
– testing web-server by selected tools;
– methods of preventing attacks.

The conclusions summarize the work done.

In the methodical part of the Master's Paper there were developed the instructions for implementation of practical works on discipline «Methods and systems of Software Testing» (Chapter 5).

In the special section «Occupational safety and security in emergencies» there are presented occupational safety at the workplaces of the application software division of NIBULON LLC, a description of the selected production facility, workplaces, their equipment and input data for quantitative assessment of working conditions, prevention measures Emergencies related to violations of fire safety requirements (Chapter 6).The work has three additions.

In general, the work consists of 135 pages, 24 tables, 54 figures, including the professional part consisting of 96 pages, 19 tables, 37 figures.

Keywords: web server, network model ISO/OSI, HTTP, DoS, DDoS, Slow HTTP attacks, Slowloris, Slow Read, R-U-Dead-Yet, Slow SSL