реалізованим за допомогою ApacheDS є LDAP. LDAP — відносно простий протокол, що використовує TCP/IP і дозволяє проводити операції авторизації, пошуку та порівняння, а також операції додавання, зміни або видалення записів. ApacheDS виступає як LDAP-сервер, очікує запити та координується із внутрішнім стрижнем служби каталогу для відповіді на запити LDAP. При використанні LDAP відпадає необхідність у використанні спеціальних драйверів, можна реалізувати гнучку схему обробки, орієнтуватися на користувача (аутентіфикація, аудит, створення груп, паролі, сертифікати тощо) і ефективно визначати його контекст безпеки. Інтеграцію у веб-додаток можна здійснити у вигляді сервлета, що витягає з веб-запиту необхідну інформацію.

Список використаних джерел:

1. Краткий обзор Spring Security. URL: https://habrahabr.ru/post/203318/ (дата звернення: 18.10.2017).
2. ApacheDS-official site. URL: http://directory.apache.org/ (дата звернення: 28.12.2016).

Одержано 27.10.2017

УДК 004.056

Юрій Петрович ГОРЕЛОВ,
кандидат технічних наук,доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ЗАХОДИ ПРОТИДІЇ АТАКАМ З ВИКОРИСТАННЯМ ВРАЗЛИВОСТЕЙ АРХІТЕКТУРИ HTTP- ПОВІДОМЛЕНЬ

Однією з актуальних завдань забезпечення кібербезпеки є захист веб-серверів і веб-додатків. Серед десятків видів атак на веб-сервери та додатки високий пріоритет мають атаки, у ході яких відбувається експлуатація вразливостей архітектури повідомлень HTTP при роботі за схемою клієнт-проксі-сервер. Наявність проміжних вузлів, таких, як кешуючий сервер, міжмережних екранів або проксі серверів, що працюють у режимі «reverse proxy», робить обмін даними небезпечним.

Різні види атак цього класу мають свої особливості, але їхньою загальною рисою є порушення структури http-запитів або http-відповідей, що дозволяє втручатися в роботу веб-серверів або додатків.

До основних заходів протидії даним видам атак можна віднести:

- установка екранів для веб-додатків;
- застосування стійких технік керування сесіями та завершення сесій після кожного запиту;
- відключення розподілу TCP-з'єднань на проміжних пристроях;
- активізація заборони на кешування всіх сторінок;
- використання технології SSL для захисту сайтів;
- повне усунення XSS-вразливостей;
- блокування запитів по протоколі HTTP/1.0 на рівні веб-сервера;
- фільтрація уведених користувачем даних з метою видалення послідовностей CRLF.

Одержано 27.10.2017

УДК 651. 34

Світлана Юріївна ГАВРИЛЕНКО,
кандидат технічних наук, доцент кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Ілля Валентинович ШЕВЕРДІН,
аспірант кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

РОЗРОБКА ЕКСПЕРТНОЇ СИСТЕМИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ АНАЛІЗУ ВІРУСУ PETYA

Найпомітнішою подією першого літнього місяця 2017 року на Україні стала епідемія вірусу-шифрувальника Trojan.Encoder.12544, що згадується в ЗМІ як Petya.A або mbr locker 256. Під удар «вірусу-вимагача» потрапили українські державні структури і приватні компанії: Кабінет Міністрів, «Ощадбанк», «Укренерго», «Нова пошта», аеропорт Бориспіль, Чорнобильська АЕС та інші організації. Ця шкідлива програма заразила комп'ютери безліч організацій і приватних осіб в 60 країнах світу.

В роботі проаналізовано даний вірус та описано етапи поширення, а саме встановлено наступні шляхи зараження:

1) шляхом експлуатації вразливості в SMB MS17-010 (аналогічно вірусу Wanna Cry);

2) шляхом спрямованої відправки шкідливого програмного забезпечення за електронною поштою;