Секция «Информационное общество, цифровая экономика и информационная безопасность»

Алгоритм тестирования на проникновение в корпоративную информационную систему с помощью специализированных программных продуктов

Научный руководитель – Уланов Алескей Александрович

Моргунов Александр Валерьевич

Студент (магистр)

Сибирский государственный университет путей сообщения, Новосибирск, Россия

E-mail: blimbablux@mail.ru

Для того, чтобы обеспечить эффективную защиту информационных ресурсов в корпоративной сети предприятия (далее - КИС), необходимо применять методы анализа эффективности ИБ предприятия. Одним из таких является периодическое тестирование на проникновение [1].

Актуальность данной работы основана на том факте, что с ростом информационных потоков и развитием технологий остро встал вопрос борьбы с киберпреступлениями, связанными с проникновением в КИС предприятий. Злоумышленники обнаруживают точечные уязвимости [2] в системе информационной безопасности и с её помощью получают несанкционированный доступ к данным разного рода и ценности.

Целью данной работы является создание алгоритма тестирования на проникновение с помощью программных продуктов (далее - ПП), позволяющий выявить актуальные угрозы. Также необходимо выполнить следующий перечень задач:

1. Анализ рынка и выбор подходящих ПП;
2. Создание тестового стенда и применение ПП;
3. Составление алгоритма тестирования;

4. Анализ полученных результатов.

В ходе мониторинга и анализа были выбраны следующие ПП: Nessus Vulnerability Scanner, Shadow Security Scanner, Armitage, XSpider, Nsauditor Network Security Auditor, Sparta, GFI Languard, Zenmap, Rapid 7 Nexpose.

Каждый из представленных выше ПП имеет определённый набор разнопрофильного функционала (утилиты, приложения, сетевые сервисы), позволяющего осуществлять: управление создаваемыми кибератаками, сканирование портов, анализ трафика, взлом паролей, детектирование уязвимостей системных служб, тестирование на проникновение локальных сетей.

После чего был создан тестовый стенд, на базе которого проводилось первичное тестирование выбранных ПП и в последствии созданного алгоритма. Более подробная топология стенда представлена на рис. 1.

Непосредственно алгоритм состоит из следующих этапов [3]:

1. Zenmap: с параметром nmap -A -T4 -v;

2. Sparta: с использованием Hydra, Nmap, Nikto и дополнительными модулями визуализации;

3. Armitage: use/auxiliary/scanner/portscan/(тип порта); set RHOSTS (ip-адрес); set THREADS (количество потоков); set PORTS (номера портов); use scanner/(выбор эксплойта).

4. GFI Languard: с детектированием уязвимостей CGI, DNS, FTP, электронной почты, UNIX/Windows семейств ОС, реестра, RPC, служб, сервисов и информации о слабо защищённых областях КИС;

5. Nsaudtor Network Security Auditor: с обнаружением TCP/UDP портов и служб; уязвимостей FTP, SMTP, TELNET, HTTP, POP3 и имён NetBIOS;

6. Shadow Security Scanner: с профилем «Complete Scan»;

7. XSpider: с профилем «Default».

8. Nessus Vulnerability Scanner: перейти по адресу https://localhost:8834/ и запустить тестирование с использованием режима «Basic Network Scan»;

9. Rapid 7 Nexpose: перейти по адресу https://localhost:3780/, создать «Site» с тестируемыми активами и запустить тестирование с использованием режима «Full Audit».

Исходя из вышеизложенного, можно сделать вывод о важности и необходимости проведения подобных исследований для обеспечения максимальной защиты информационных ресурсов и систем предприятий в условиях существующих посягательств в сфере киберпреступлений современного мира.

Источники и литература

1) Ситнов А.А. Аудит информационной инфраструктуры: учебно-практическое пособие. – М.: Изд. Центр ЕАОИ, 2011. – 144 с.

2) Бирюков А.А. Информационная безопасность: защита и нападение, - 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с.: нл.

3) Скабцов Н. Аудит безопасности информационных систем. – СПб.: Питер, 2018. – 272 с.

Иллюстрации

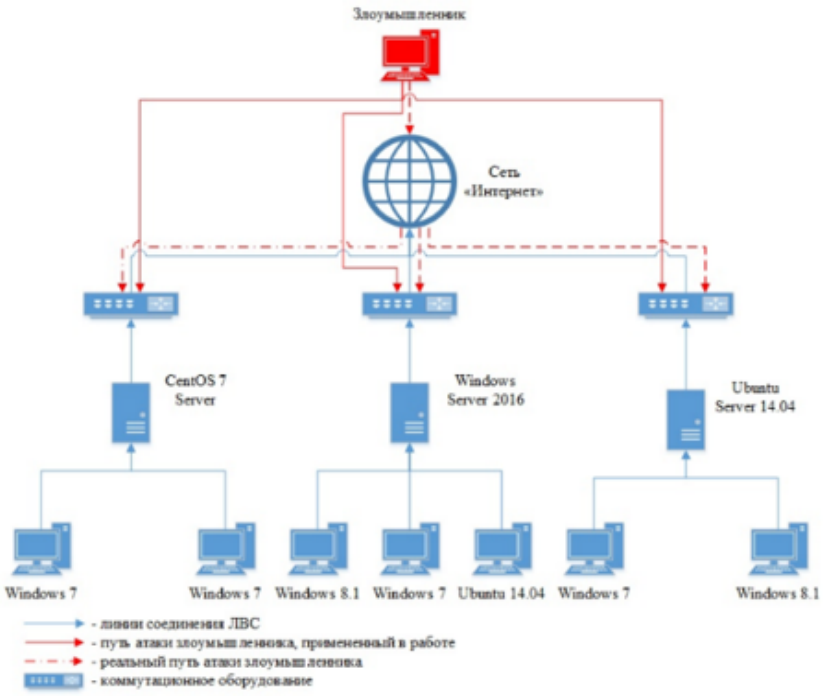

Рис. 1. Топология стенда для тестирования ПП