УДК 004.051:004.492.3

ОЦЕНКА БЕЗОПАСНОСТИ СЕТИ С ПОМОЩЬЮ ONLINE-ПЕНТЕСТОВ

А.Д. МИХЕЙЧИК

Белорусский государственный университет информатики и радиоэлектроники, Республика Беларусь

Поступила в редакцию 5 ноября 2018

Аннотация. Предложено использовать online-пентесты для повышения информационной безопасности в корпоративных сетях. Рассмотрены основные инструменты, с помощью которых можно осуществить мониторинг безопасности сети.

Ключевые слова: безопасность, пентест, сетевые атаки.

Введение

В настоящее время наблюдается непрерывное совершенствование механизмов реализации сетевых атак. В связи с этим системные администраторы и специалисты по защите информации должны периодически проверять на эффективность применяемые в их организации средства обеспечения сетевой безопасности.

Существует большое количество программных и программно-аппаратных средств, предназначенных для мониторинга безопасности корпоративных сетей. К недостаткам таких средств можно отнести дороговизну и сложность в реализации (при самостоятельной настройке). Поэтому многие специалисты часто прибегают к бесплатным online-инструментам, которые дают возможность понять, насколько защищена сеть от актуальных сетевых атак. К таким online-инструментам относятся пентесты.

Под пентестом понимается мониторинг безопасности сети с помощью проведения испытаний на проникновения. Испытания основаны на сетевых атаках, реализуемых с целью обнаружения уязвимостей и недостатков [1].

Целью работы является исследование эффективности работы online-пентестов, направленных на межсетевые экраны, антивирусные программы и веб-сайты.

Мгновенная проверка безопасности

Для проверки защищенности межсетевого экрана часто применяется сервис Check Point CheckMe [2]. Представленный сервис включает в себя несколько тестов, с помощью которых выполняется анализ компьютера пользователя и сети на предмет наличия уязвимостей, связанных с вредоносными программами, удаленным доступом, утечкой данных, кражей конфиденциальной информации, атак нулевого дня, эксплойтами и использованием анонимайзеров. Следует учитывать, что при проведении тестов на проникновения сеть не подвергается реальному риску. Для того чтобы увидеть работу сервиса Check Point CheckMe, следует выполнить следующее.

1. Зайти на сайт http://www.cpcheckme.com.
2. Запустить процесс сканирования на Интернет-браузере.
3. Просмотреть отчет о завершении сканирования после того, как произошел обмен данными между Интернет-браузером и сервисом (рис. 1).

Рис.1. Результаты работы сервиса Check Point CheckMe

Сервис Check Point CheckMe осуществляет различные сценарии, которые соответствуют следующим сетевым атакам.

1. Вредоносные программы – программы, которые могут существенно повлиять на работу компьютера и всей корпоративной сети организации.
2. Атака нулевого дня – атака, заключающаяся в неожиданном использовании злоумышленником найденной им уязвимости, о которой не было известно ранее.
3. Эксплойт – специальная программа или код, с помощью которых можно провести атаку на сеть, используя уязвимости в программном обеспечении.
4. Удаленный доступ – возможность нелегитимному пользователю дистанционно получить доступ к серверу, повысив тем самым свои привилегии.
5. Анонимайзеры – средства, предназначенные для скрытия сведений о компьютере или пользователе в сети от удаленного сервера.
6. Утечка данных – возможность для злоумышленника получить служебную информацию, циркулирующую в сети организации.
7. Кража информации – получение конфиденциальной информации (логин/пароль) с помощью поддельных веб-сайтов (фишинг).

При тестировании межсетевого экрана может возникнуть ситуация, при которой данное устройство не выполняет возложенные на него задачи (рис. 1). Это может быть связано с тем, что системные администраторы или специалисты по информационной безопасности неправильно используют функциональные возможности устройства. Например, межсетевой экран может быть настроен на фильтрацию по протоколам транспортного уровня, вместо фильтрации по приложениям. Сервис Check Point CheckMe позволяет установить и пересмотреть функционал межсетевого экрана, после чего настроить устройство и осуществить повторный тест с использованием сервиса Check Point CheckMe.

Проверка работоспособности антивирусных программ

В последнее время разработчики антивирусных программ начали использовать такие файлы, которые могут определяться антивирусным средством как вредоносные, но таковыми не являться. Это было сделано для того, чтобы пользователи смогли увидеть работу установленный ими антивирусной программы [3]. Также разработчики используют данные файлы для проведения тестов, с помощью которых осуществляется проверка работоспособности антивирусных программ. Одним из таких тестов является EICAR-Test-File [4].

Главная задача представленного теста заключается в том, чтобы показать пользователю работоспособность антивирусной программы, а также продемонстрировать, какие объекты она может проверить (происходит блокировка вирусного файла), а какие – нет (загружается вредоносный файл). Для проверки антивирусов EICAR-Test-File использует файлы формата txt, zip, а также протоколы http и https (рис. 2).

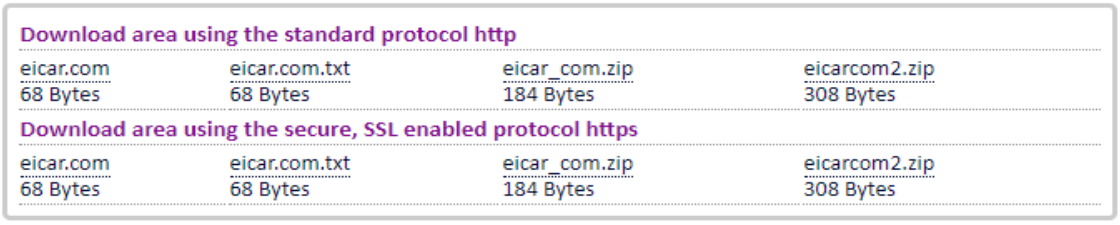

Рис. 2. Форматы файлов теста EICAR-Test-File

Для проведения тестов использована антивирусная программа Microsoft Windows 10. Перед началом проведения тестов была выполнена загрузка txt-файла. Далее была запущена антивирусная программа, после чего проверена ее работоспособность путем загрузки того же txt-файла. В конце испытаний в Интернет-браузере выполнена проверка истории загрузок (рис. 3).

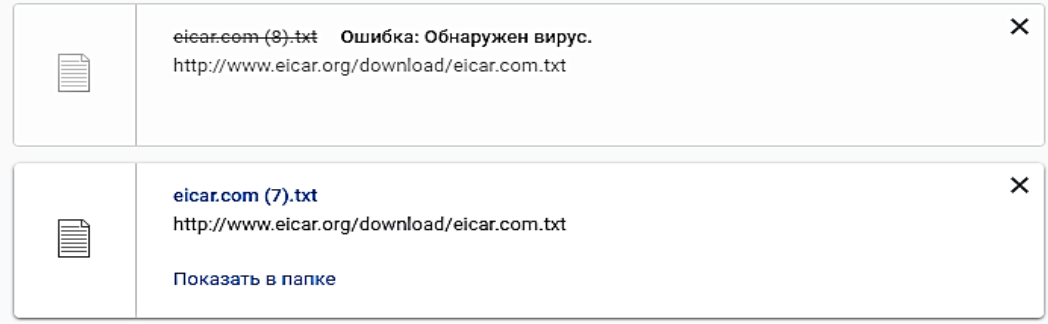

Рис. 3. Результаты проверки работоспособности антивируса Microsoft Windows 10

Как видно из рис. 3, при отключенной антивирусной программе тестовый файл загружался из Интернет-браузера на компьютер пользователя. При запущенной антивирусной прорамме тестовый файл блокировался. Таким образом, было установлено, что тестируемая антивирусная программа является работоспособной.

Проверка безопасности веб-сайтов

Одной из самых популярных сетевых атак является инъекция. Под инъекцией следует понимать возможность злоумышленником осуществить взлом сайта, внедряя в его данные произвольный код. Многие системные администраторы пренебрегают специализированными программами, которые предназначены для анализа сайтов.

На сегодняшний день существует большое количество программных средств, предназначенных для мониторинга безопасности веб-сайтов. Одним из таких средств является online-инструмент Pentest-tools [5]. Данный инструмент предназначен для проведения тестирования безопасности веб-сайта путем проведения тестов на проникновения. В качестве тестируемого веб-сайта был выбран сайт БГУИР (bsuir.by) (рис. 4). Согласно счетчику Яндекс.Метрика, среднее количество посетителей сайта bsuir.by 6100 хостов в сутки, при этом количество просмотров веб-сайта приблизительно равно 21 000 в сутки [6].

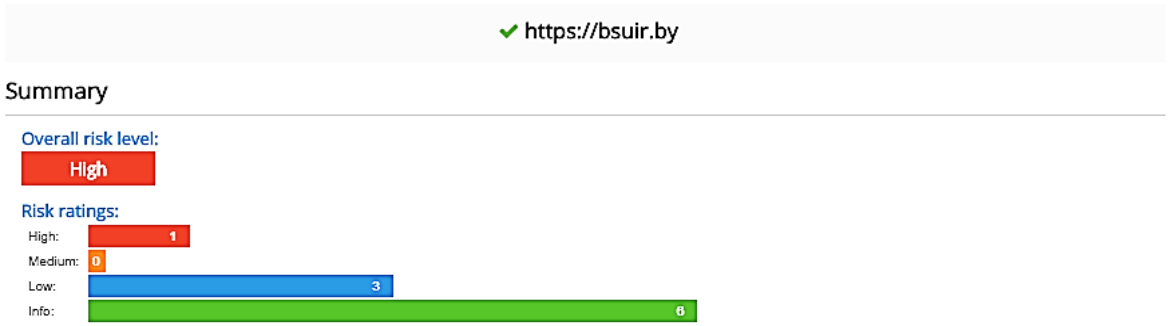

Рис. 4. Результаты анализа безопасности сайта bsuir.by, полученные с помощью Pentest-tools

Как видно из рис. 4, безопасность веб-сайта характеризуется высокой степенью риска. При более подробном анализе отчета можно прийти к выводу, что найденные уязвимости связаны с установленным веб-сервером Apache 2.4 (рис. 5).

Vulnerabilities found for server-side software

Risk Level	CVSS	CVE	Summary	Exploit	Affected software
●	7.5	CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.	N/A	http_server 2.4
●	7.5	CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.	N/A	http_server 2.4
●	7.5	CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.	N/A	http_server 2.4
●	7.5	CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.	N/A	http_server 2.4
●	7.5	CVE-2013-2249	mod_session_dbd.c in the mod_session_dbd module in the Apache HTTP Server before 2.4.5 proceeds with save operations for a session without considering the dirty flag and the requirement for a new session ID, which has unspecified impact and remote attack vectors.	N/A	http_server 2.4

Рис. 5. Перечень уязвимостей сайта bsuir.by

Под CVE понимается база данных известных на сегодняшний день уязвимостей [7]. Анализируя данные из рис. 5, можно сказать, что для решения проблемы безопасности веб-сайта следует обновить Apache HTTP Server до последней версии.

Заключение

Предложено использовать online-пентесты для проведения оценки безопасности корпоративной сети. Проведен анализ online-инструментов, направленных на межсетевые экраны, антивирусные программы и веб-сайты. В работе рассмотрены следующие online-пентесты: сервис Check Point CheckMe, тест EICAR-Test-File и online-инструмент Pentest-tools.

NETWORK SECURITY ASSESMENT WITH ONLINE PENTEST

A.D. MIHEYCHIK

Abstract. It is proposed to use online-pentest to improve information security in corporate networks. The main online-tools that can be used to monitor network security are reviewed.

Keywords: security, pentest, network attacks.

Список литературы

1. Пентестинг. [Электронный ресурс]. URL: http://www.tadviser.ru/index.php/Статья:Pentesting (дата обращения: 13.10.2018).
2. Check Point CheckMe. [Электронный ресурс]. URL: http://www.cpcheckme.com/checkme/?source=Tssolution (дата обращения: 14.10.2018).
3. Тестовый вирус eicar. [Электронный ресурс]. URL: https://support.kaspersky.ru/general/products/7399 (дата обращения: 15.10.2018).
4. EICAR-Test-File. [Электронный ресурс]. URL: http://www.eicar.org/85-0-Download.html (дата обращения: 15.10.2018).
5. Pentest-tools. [Электронный ресурс]. URL: https://pentest-tools.com/home (дата обращения: 16.10.2018).
6. Яндекс.Метрика. [Электронный ресурс]. URL: https://metrika.yandex.ru (дата обращения: 16.10.2018).
7. CVE. [Электронный ресурс]. URL: https://cve.mitre.org (дата обращения: 16.10.2018).