МЕТОДОЛОГИЯ ПРОВЕДЕНИЯ СТРЕСС ТЕСТИРОВАНИЯ НА ЦЕЛЕВОЙ ВЕБ-СЕРВЕР

И. В. Давыдович[1], В. С. Зурахов[1], И. А. Ушаков[2*]

[1]Санкт-Петербургский государственный университет промышленных технологий и дизайна, Санкт-Петербург, 191186, Российская Федерация

[2]Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

*Адрес для переписки: ushakovia@gmail.com

Аннотация—**Предмет исследования.** В статье рассматриваются методы злоумышленника для проведения атаки на веб-сервер и способы защиты от них. **Метод.** Данная методология содержит описание этапов подготовки атаки и описание способов защиты от них. Целью работы является составление такой методологии, с помощью которой можно предотвращать большинство хакерских атак. Поскольку в последнее время интернет-технологии развиваются стремительными темпами, и компании переносят свой бизнес в Интернет, вопрос информационной безопасности как никогда актуален. Одним из методов защиты от атак злоумышленников является понимание методологии атаки на веб-сервер. Понимание того, как будет действовать злоумышленник при атаке, позволяет своевременно предотвратить её и как следствие избежать последствий. Целью данной работы является: описание этапов, которые злоумышленник проходит во время атаки на веб-сервер и составление рекомендаций по его защите. Для понимания методов защиты веб-сервера от взлома, важно знать концепцию его устройства, то, как он функционирует и другие элементы, связанные с ним.

Ключевые слова—Nmap, Burp Suite, хакерские атаки, Directory Monitor, DMZ, pentest.

Информация о статье
УДК 004.56
Язык статьи – русский.
Поступила в редакцию 02.03.2021, принята к печати 24.03.2021.

Ссылка для цитирования: Давыдович И. В., Зурахов В. С., Ушаков И. А. Методология проведения стресс тестирования на целевой веб-сервер // Информационные технологии и телекоммуникации. 2021. Том 9. № 1. С. 79–86. DOI 10.31854/2307-1303-2021-9-1-79-86.

METHODOLOGY FOR CONDUCTING STRESS TESTING ON A TARGET WEB SERVER

I. Davydovich[1], V. Zurakhov[1], I. Ushakov[2*]

[1]Saint-Petersburg State University of Industrial Technologies and Design, St. Petersburg, 191186, Russian Federation

[2]The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, St. Petersburg, 193232, Russian Federation

*Corresponding author: ushakovia@gmail.com

Abstract—This article discusses the methods of an attacker to conduct an attack on a web server and how to protect against them. This methodology contains a description of the stages of preparing an attack and a description of how to protect against them. The aim of the work is to draw up such a methodology, with the help of which it is possible to prevent the majority of hacker attacks. Since Internet technologies have been developing at a rapid pace lately, and companies are moving their businesses to the Internet, the issue of information security is more urgent than ever. One of the methods to defend against malicious attacks is to understand the methodology for attacking a web server. Understanding how an attacker will act in an attack allows you to prevent it in a timely manner and, as a result, avoid consequences. The purpose of this work is: description of the stages that an attacker goes through during an attack on a web server and making recommendations for its protection. To understand the methods of protecting a web server from hacking, it is important to know the concept of its device, how it functions and other elements associated with it.

Keywords— Nmap, Burp Suite, hacker attacks, Directory Monitor, DMZ, pentest.

Article info
Article in Russian.
Received 02.03.2021, accepted 24.03.2021.

For citation: Davydovich I., Zurakhov V., Ushakov I.: Methodology for conducting stress testing on a target web server // Telecom IT. 2021. Vol. 9. Iss. 1. pp. 79–86 (in Russian). DOI 10.31854/2307-1303-2021-9-1-79-86.

Введение

Поскольку в последнее время интернет-технологии развиваются стремительными темпами, и компании переносят свой бизнес в Интернет, вопрос информационной безопасности как никогда актуален. Одним из методов защиты от атак злоумышленников является понимание методологии атаки на веб-сервер. Понимание того, как будет действовать злоумышленник при атаке, позволяет своевременно предотвратить её и как следствие избежать последствий.

Целью данной работы является: описание этапов, которые злоумышленник проходит во время атаки на веб-сервер и составление рекомендаций по его защите.

Одним из важнейших методов поддержания информационной безопасности распределённых информационных систем (РИС) [1], наряду с разработкой политики безопасности и применением средств защиты, является знание методологии проведения атаки на веб-сервер. Хорошим решением в этом случае будет созданная в данной статье методологии, благодаря которой можно понять, какие этапы выполняет злоумышленник во время атаки.

Уникальность данной методологии заключается в ряде преимуществ, которые она обеспечивает, по сравнению с коммерческими аналогами. Также уникальности нашей статье придает тот факт, что среди цитируемой литературы мы не смогли найти аналоги данной методологии. Основными её достоинствами являются доступность и простота в понимании. Данная методология включает в себя основные этапы проведения взлома веб-сервера. Это позволяет пресекать большую часть атак. Стоит также отметить, что данную методологию можно, и даже нужно, использовать в обучающих целях.

Концептуальное представление веб-сервера

Для понимания методов защиты веб-сервера от взлома, важно знать концепцию его устройства то, как он функционирует и другие элементы, связанные с ним. Веб-сервер представляется собой операционную систему, чаще всего Unix-подобную, которая имеет древовидную структуру каталогов, выполняющую ряд функций: хранение информации и веб-страниц, её обработку и доставку глобальным клиентам по средствам протокола передачи гипертекста (HTTP)[1]. Веб-сервер состоит из следующих основных компонентов:

- **Корневой каталог** – один из корневых каталогов веб-сервера, на котором хранятся важные файлы HTML, связанные с веб-страницами доменного имени, которые будут отправляться в ответ на запросы пользователей.
- **Корневой каталог сервера** – каталог верхнего уровня в дереве каталогов, в котором хранятся конфигурация сервера и файлы ошибок, исполняемые файлы и файлы журналов. Корневой каталог, как правило, состоит из четырех файлов. Один файл предназначен для кода, реализующего сервер, а остальные три являются подкаталогами, а именно -conf, -logs, -cgi-bin, которые используются для информации о конфигурации, журналов и исполняемых файлов.

[1] Веб-серверы: информация для начинающих [Электронный ресурс]. URL: https://arduinoplus.ru/web-servers-nachinauschim/ (дата обращения: 01.02.2021)

• **Виртуальное дерево документов** – обеспечивает хранение на другом компьютере или диске после заполнения основного диска. Данный компонент может использоваться для обеспечения безопасности на уровне объектов.

• **Виртуальный хостинг** – метод размещения нескольких доменов или веб-сайтов на одном сервере. Этот метод позволяет разделять ресурсы между различными серверами.

На рис. 1 наглядно показано концептуальное файловое устройство веб-сервера, его иерархию.

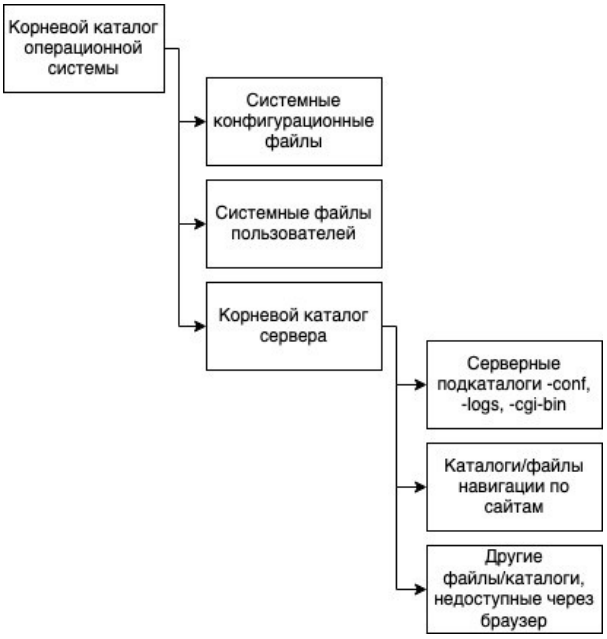

Рис. 1. Концептуальное устройство веб-сервера

Общие цели взлома веб-сервера

Цели, которые преследуют злоумышленники, атакуя веб-сервер, могут быть техническими и нетехническими. Например, хакеры могут нарушить безопасность веб-сервера и украсть конфиденциальную информацию с целью получения финансовой выгоды или просто из любопытства.

Проведя аналитику наиболее известных атак за последние три года, мы можем выделить следующие цели, которые преследуют хакеры:

- Кража данных кредитной карты или других конфиденциальных данных;
- Интеграция сервера в ботнет для выполнения атаки типа «отказ в обслуживании» (DoS) или распределенных DoS-атак (DDoS) [2];
- Взлом базы данных, с целью похищения учетных записей;
- Получение приложений с закрытым исходным кодом;
- Повышение привилегии.

Также кроме финансовых целей есть ещё и личные мотивы, такие как:

- Простое любопытство или достижение цели, поставленной перед собой;
- Нанесение ущерба репутации целевой организации.

Методология проведения атаки на веб-сервер

Атака на веб-сервер обычно включает заранее запланированные действия, называемые методологией атаки, которой злоумышленник следует для достижения цели. Хакеры атакуют веб-сервер в несколько этапов, на каждом из которых они пытаются собрать информацию о слабых местах веб-сервера и получить несанкционированный доступ к нему. Ниже приведены этапы методологии атаки на веб-сервер [3]:

- Сбор информации;
- Создание «слепка» веб-сервера;
- Зеркальное отображение веб-сайта;

- Сканирование уязвимостей;
- Перехват сессионных данных;
- Взлом паролей веб-серверов.

Для более четкого представления методологии атаки на веб-сервер, необходимо рассмотреть каждый пункт подробнее.

Это первым и одним из самых важных шагов на пути к взлому целевого веб-сервера является **сбор информации**. На этом этапе злоумышленник собирает как можно больше информации о целевом сервере, используя различные инструменты и методы, такие как сервис Whois.net и Whois Lookup. Эти инструменты позволяют узнать сетевую информацию веб-сервера, например, доменное имя и IP-адрес. Данные, полученные на данном этапе, позволяют злоумышленнику оценить состояние безопасности веб-сервера. Немало важным является тот факт, что на этом этапе появляется возможность установить связи целевого веб-сервера с другими веб-серверами.

Кроме специализированных инструментов для сбора информации злоумышленник использует веб-сайт, который установлен на целевом веб-сервере. Владелец сайта создает файл robots.txt, чтобы перечислить файлы и каталоги, которые браузер должен индексировать для предоставления результатов поиска. Плохое написание такого файла может привести к полной индексации файлов и каталогов веб-сервера. Если конфиденциальные файлы и каталоги проиндексированы, злоумышленник может легко получить такую информацию, как пароль, e-mail адрес, скрытые ссылки.

Следующим немало важным этапом на пути к взлому целевого веб-сервера является **footprinting веб-сервера.** На данном этапе злоумышленник как бы «снимает отпечаток» веб-сервера для того, чтобы получить ценные данные на уровне системы, например, сведения об учётной записи, ОС, версии программного обеспечения и др. Для данного этапа используются такие инструменты, как Nmap[2], Netcraft, ID Serve, httprecon и другие. Эти инструменты используют встроенные шаблоны для того, чтобы узнать следующую информацию о целевом веб-сервере:

- Имя сервера;
- Тип сервера;
- Операционную систему;
- Запущенные приложения.

Следующим шагом является **зеркальное копирование веб-сайта**, на котором злоумышленник копирует весь веб-сайт и его содержимое на локальный диск. Такой способ позволяет показать полный профиль структуры каталогов веб-сайта, файловой структуры, внешних ссылок, изображений, веб-страниц и т. п. С помощью «отзеркаленного» веб-сайта хакер может легко сопоставить его каталоги и получить ценную информацию об их устройстве на целевом веб-сервере. Кроме того, злоумышленник может получить полезную информацию путем поиска комментариев и других элементов в исходном HTML-коде, скаченных веб-страниц. Для данного этапа могут подойти такие инструменты, как NCollector Studio, HTTPrack Web Site Copier, WebCopier Pro и Website Ripper Copier.

[2] Nmap. Documentation [Электронный ресурс]. URL: https://nmap.org/docs.html (дата обращения: 02.02.2021)

Наиболее важным, на наш взгляд, этапом в данной методологии является **сканирование на уязвимости**. На этом шаге появляется возможность обнаружения уязвимостей и неправильных настроек на целевом веб-сервере или в сети. Сканирование уязвимостей выявляет возможные слабые места на целевом веб-сервере, которые можно использовать при атаке. На этапе сканирования уязвимостей злоумышленник использует методы сниффинга для получения данных о сетевом трафике для определения активных систем, сетевых служб и приложений. Для данного этапа очень хорошо подходит инструмент Acunetix Web Vulnerabolity Scanner.

Но для успешного взлома веб-сервера недостаточно найти уязвимость, нужно найти способ её реализовать, т. е. проэксплуатировать. Зачастую злоумышленники ищут и эксплуатируют уже известные уязвимости. При поиске эксплоитов для таких уязвимостей злоумышленники используют сайты SecurityFocus и Exploit-DB. Использование этих уязвимостей позволяет злоумышленнику исполнить команду или двоичный файл для повышения привилегий на целевом веб-сервере и получить полный контроль над атакуемым веб-сервером.

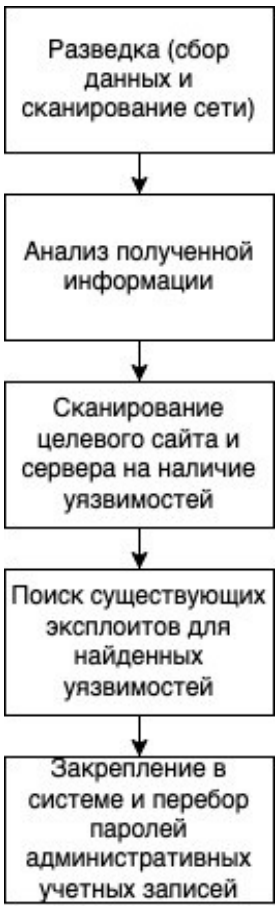

Рис. 2. Алгоритм хакерской атаки

Также стоит отметить важность такого этапа, как **перехват сессионных данных**. Он опасен тем, что злоумышленник, используя методы социальной инженерии, атаки Cross-site scripting (XSS) или специального инструмента, например, Burp Suite может получить несанкционированный доступ к целевому веб-серверу. Перехваченные сессионные данные, хакер может использовать для получения привилегий и совершения более серьезных атак.

Самым ресурсоемким из представленных нами этапов является **взлом паролей** для целевого веб-сервера. На этом этапе атаки на веб-сервер злоумышленник пытается взломать пароли, которые смог обнаружить на предыдущих этапах, либо закрепившись в системе. Хакер может использовать всевозможные методы взлома паролей, начиная от простого угадывания пароля и заканчивая радужной атакой и вычислением хэша пароля. Для упрощения работы злоумышленник использует автоматизированные средства такие, как Hashcat, THC Hydra и Ncrack. Подытожив выше сказанное, мы предлагаем алгоритм поведения хакера при атаке на целевой веб-сервер (рис. 2).

Методы защиты веб-сервера

Существует множество мер по защите веб-сервера от взлома, например, установка антивируса или парольная политика, мы в свою очередь предлагаем **альтернативные**, не менее действенные средства защиты:

- Сегментации сети. Идеальная сеть веб-хостинга должна иметь три сегмента: интернет-сегмент, сегмент безопасности защищенного сервера (DMZ)

и внутренняя сеть (рис. 3). Первым шагом в обеспечении безопасности веб-сервера является его отдельное размещение в DMZ, которая изолирована от общей и внутренней сети веб-хостинга. Такое разделение позволяет администраторам устанавливать брандмауэры и применять контроль доступа на основе правил безопасности для внутренней сети, а также интернет-трафика в направлении DMZ. В сегментированной сети злоумышленник, взломавший один сегмент сети, не сможет поставить под угрозу безопасность других сегментов.

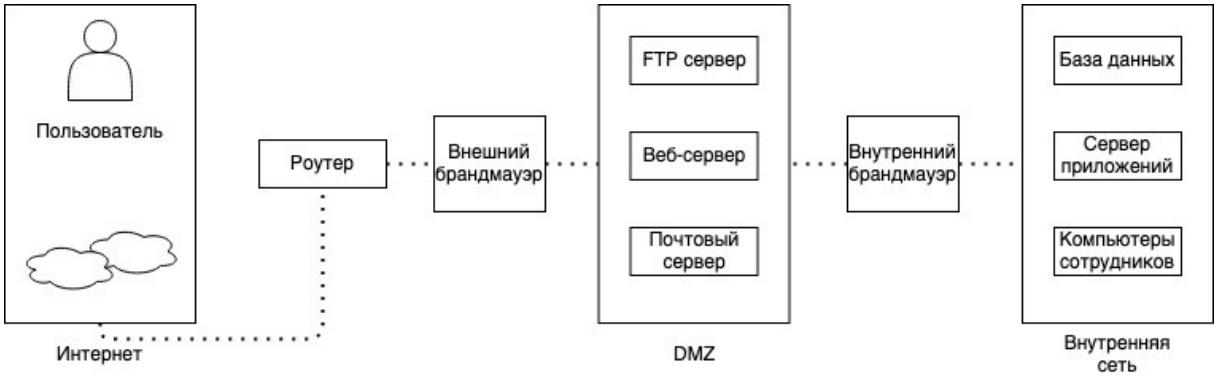

Рис. 3. Сеть веб-хостинга с использованием DMZ

- Обнаружение попытки взлома. Злоумышленник, который получил доступ к веб-серверу, ставя под угрозу безопасность с помощью известных уязвимостей, имеющихся на веб-сервере, может попытаться установить бэкдоры (скрипты), которые позволят злоумышленнику нанести ещё больший урон бизнесу компании. Когда хакер устанавливает бекдор на веб-сервер, размер зараженных файлов, автоматически увеличивается. Мы предлагаем использовать систему обнаружения изменений веб-сайта (WDS). WDS – это сценарий, который запускается на сервере для обнаружения изменений, внесенных в любой исполняемый файл, либо наличия нового файла на веб-сервере и предупреждает пользователя о необходимости предпринять необходимые меры. Примером такой системы является Directory Monitor от одноименной компании[3].
- Своевременное проведение аудита безопасности с помощью тестирования на проникновение (пентест). Данный метод позволяет выявить недостатки безопасности веб-сервера до того, как злоумышленник попытается проникнуть в сеть. Пентест – максимально приближенный к реальным атакам метод тестирования безопасности веб-сервера [4]. Для его проведения желательно привлечь специалистов по информационной безопасности, однако некоторые тести можно проделать самостоятельно.

Заключение

Таким образом, в данной статье была выработана методика атаки на веб-сервер, благодаря которой можно предотвращать большинство атак ещё

[3] Directory Monitor [Электронный ресурс]. URL: https://directorymonitor.com/ (дата обращения: 03.03.2021)

на начальном этапе их формирования. В качестве защитный мер были предоставлены альтернативные способы защиты веб-сервера, кроме тех, что уже существуют.

Из этого можно сделать вывод, что, зная методы взлома веб-сервера можно предотвратить атаки ещё на стадии создания веб-сервера, соблюдая вышеуказанные меры защиты. Созданная методология является универсальной и может быть использована при создании собственного веб-сервера.

Литература

1. Москальчук А. И., Красов А. В., Штеренберг С. И. Методология создания виртуальной лаборатории для тестирования безопасности распределенных информационных систем // Вестник Брянского государственного технического университета. 2020. №3 (88). С. 38–46. DOI 10.30987/1999-8775-2020-3-38-46.

2. Шемякин С. Н., Гельфанд А. М., Холоденко В. Ю., Орлов Г. А., Ходжаев Ш. А. У. Описание разнообразных ddos атак с использованием botnet // Colloquium-journal. 2019. № 23-2 (47). С. 52–53.

3. Котенко И. В., Дойникова Е. В., Чечулин А. А. Общее перечисление и классификация шаблонов атак (CAPEC): описание и примеры применения // Защита информации. Инсайд. 2012. № 4 (46). С. 54–66.

4. Давыдович И. В., Степанова А. А., Добрянский Д. Э., Кузева В. В. Разработка пентест лаборатории с использованием Raspberry PI // Молодежная научная школа кафедры «Защищенные Системы Связи». 2020. Т. 1. № 1. С. 39–42.

References

1. Moskal'chuk A., Krasov A., Shterenberg S. Virtual laboratory creation for distributed information system safety testing // Bulletin of Bryansk State Technical University. 2020. Vol. Iss. 3 (88). pp. 38–46 (in Russian). DOI 10.30987/1999-8775-2020-3-38-46.

2. Shemyakin S. N., Gelfand A. M., Kholodenko V. Y., Orlov G. A., Khojaev Sh. A. U. Description of various ddos attacks using botnet // Colloquium-journal. 2019. Iss. 23-2 (47). pp. 52–53 (in Russian).

3. Kotenko I. V., Dojnikova E. V., CHechulin A. A. Obshchee perechislenie i klassifikaciya shablonov atak (CAPEC): opisanie i primery primeneniya // Zaŝita informacii. Inside. 2012. Iss. 4 (46). pp. 54–66 (in Russian).

4. Davydovich I. V., Dobriansky D. E., Stepanova A. A., Kuzeva V. V. Development of a pentest laboratory using Raspberry PI // Youth scientific school of the department "Secured Communication Systems". 2020. Vol. 1. Iss. 1. pp. 39–42 (in Russian).

Давыдович Илья Владимирович
студент, Санкт-Петербургский государственный университет промышленных технологий и дизайна, davydovich.2014@mail.ru

Davydovich Ilja V.
student, Saint-Petersburg State University of Industrial Technologies and Design, davydovich.2014@mail.ru

Зурахов Владимир Сергеевич
кандидат технических наук, доцент кафедры Санкт-Петербургского государственного университета промышленных технологий и дизайна, ziegfried@mail.ru

Zurakhov Vladimir S.
candidate of engineering sciences, associate professor, Saint-Petersburg State University of Industrial Technologies and Design, ziegfried@mail.ru

Ушаков Игорь Александрович
кандидат технических наук, доцент кафедры Санкт-Петербургского государственного университета телекоммуникаций им. проф. М. А. Бонч-Бруевича, ushakovia@gmail.com

Ushakov Igor A.
candidate of engineering sciences, associate Professor, The Bonch-Bruevich Saint-Petersburg State University of Telecommunications, ushakovia@gmail.com