8. Is VoIP Secure? The Ultimate Guide to VoIP Security & Call Encryption Ethnography / Cameron Johnson. — URL: https://www.nextiva.com/blog/voip-security.html/ (date of the application: 20.05.2022). — Text : electronic.

Д. А. Ромейко, Т. И. Паюсова
Тюменский государственный университет, г. Тюмень

УДК 004.056

ОБЗОР ВОЗМОЖНОСТЕЙ СРЕДЫ METASPLOIT FRAMEWORK

Аннотация. *В данной статье приведены материалы, которые позволят студентам, изучающим информационную безопасность, освоить теоретические основы тестирования на проникновение. Понимание основ эксплуатации уязвимостей помогает студентам осознать важность и необходимость комплексной системы защиты, позволяющей снизить риск наличия недекларированных возможностей. Результатом работы стала серия лабораторных работ, посвященных эксплуатациям уязвимостей.*

Ключевые слова: *metasploit framework, эксплойт, payload, kali linux, metasploitable3, meterpreter, reverse shell, msfvenom, уязвимость, кибератака.*

Введение. Тестирование на проникновение позволяет ответить на вопросы о том, как злоумышленники могут вмешиваться в информационную инфраструктуру. Используя инструменты пентеста, «белые хакеры» и эксперты по информационной безопасности могут проникнуть в систему и проверить наличие сетевых и прикладных дефектов и уязвимостей на любом этапе разработки или развертывании.

Одним из инструментов пентеста является проект Metasploit Framework. Это платформа с открытым исходным кодом, которая позволяет выполнять тестирование системы на проникновение с помощью командной строки или графического интерфейса.

Проблема исследования. Статистика «Лаборатории Касперского» показывает, что в организациях наиболее серьезными последствиями кибератак являются невозможность доступа к критически важной бизнес-информации (59% российских компаний

заметили этот фактор), ущерб репутации (50%) и потеря бизнес-возможностей и важных деловых контактов (34%) [1].

На рис. 1 представлена статистика от Positive Technologies основных последствий целевых кибератак на российские компании за 2021 г. в процентном соотношении [2].

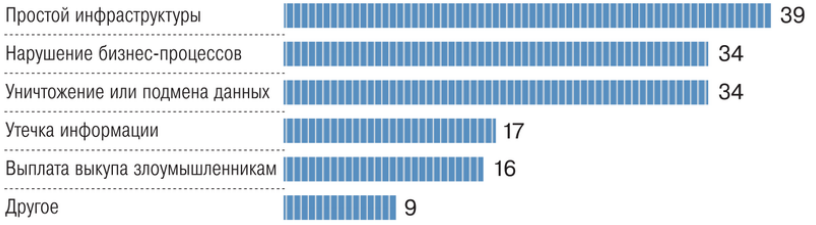

Рис. 1. Статистика последствий кибератак на российские компании (по данным Positive Technologies)

Материалы и методы. *Metasploit Framework.* Платформа Metasploit Framework — это модульная платформа тестирования на проникновение, основанная на языке программирования Ruby, которая позволяет вам писать, тестировать и выполнять код эксплойта. Платформа Metasploit содержит набор инструментов, которые можно использовать для проверки уязвимостей в системе безопасности, перечисления сетей, выполнения атак и уклонения от обнаружения. Ядром платформы Metasploit является набор часто используемых инструментов, которые обеспечивают полную среду для тестирования на проникновение и разработки эксплойтов [3].

Как показано на рис. 2, ядром Metasploit является библиотека Rex. Она обеспечивает работу с сокетами, протоколами, текстовыми форматами и т. д. Она основана на библиотеке MSF Core и предоставляет базовые функции и «низкоуровневый» API. В свою очередь, она использует библиотеку MSF Base, которая, предоставляет API для подключаемых модулей, пользовательских интерфейсов (консольных и графических) и подключаемых модулей.

Meterpreter. Meterpreter — это полезная нагрузка для атаки на платформе Metasploit, которая позволяет злоумышленнику управлять компьютером жертвы и перемещаться по командной оболочке.

Когда дело доходит до тестирования на проникновение, он может оказаться очень универсальным инструментом. Это инструмент после эксплуатации, основанный на встраивании библиотеки DLL в память, что означает, что он может запускать встроенную библиотеку DLL, создавая новый процесс и вызывая систему для запуска встроенной библиотеки DLL. Он позволяет получить доступ к невидимой командной оболочке на компьютере жертвы, позволяет запускать исполняемые файлы и профилировать сеть [4].

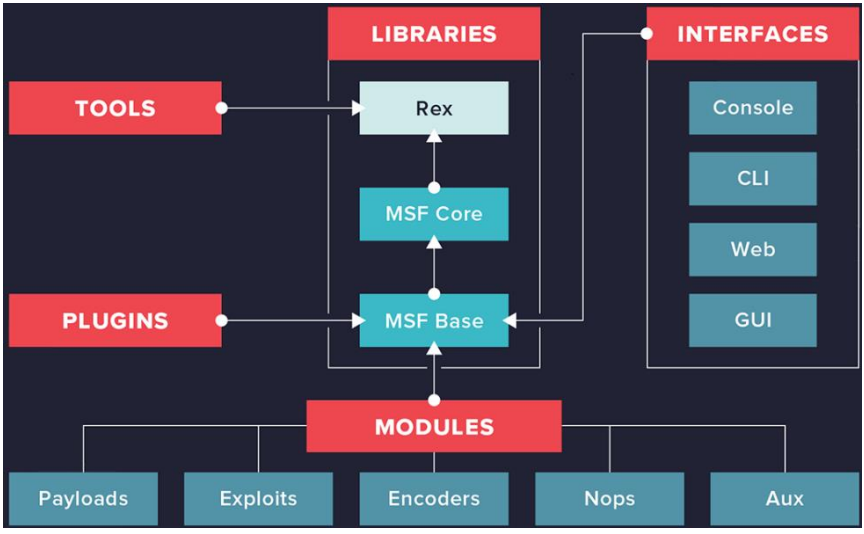

Рис. 2. Архитектура Metasploit

Полезная нагрузка в Metasploit — это модули, то есть фрагменты кода в Metasploit, которые запускаются в удаленной системе нашей цели. Сначала отправляется в систему модуль эксплойта, в котором установлен модуль полезной нагрузки. Затем полезная нагрузка предоставляет злоумышленнику доступ, ограниченный или полный, в зависимости от содержимого полезной нагрузки.

На рис. 3 показана наглядная иллюстрация того, как работает эксплуатация с помощью Meterpreter.

Рис. 3. Эксплуатация целевой машины с помощью Meterpreter

Reverse Shell. Существует два популярных типа оболочек: Bind shell и Reverse Shell.

Bind Shell — открывает новую службу на целевой машине и требует от злоумышленника подключения к ней, чтобы получить сеанс.

Reverse Shell — обратная оболочка также называется обратным соединением. Эта оболочка требует, чтобы злоумышленник сначала установил прослушиватель на свой компьютер. В это время целевая машина действует как клиент, подключающийся к этому прослушивателю. В результате злоумышленник получает клиентскую оболочку [5].

На рис. 4 показан процесс установки обычного и обратного соединения компьютера атакующего с компьютером жертвы.

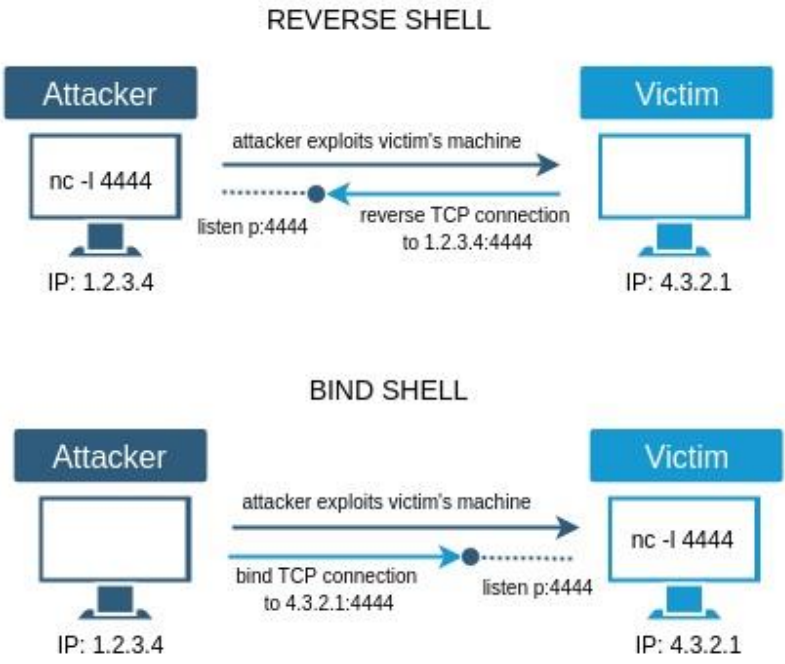

Рис. 4. Процесс соединения с помощью Bind Shell и Reverse Shell

Если вы окажетесь в одной из следующих ситуаций, вы можете использовать обратную оболочку:

- целевая машина расположена за другой частной сетью;
- брандмауэр целевого компьютера предотвращает входящие попытки подключения к вашей командной оболочке Bind;
- по какой-то причине ваша полезная нагрузка не может быть привязана к нужному порту.

MSFvenom

MSFvenom — это продукт, который сочетает в себе “MSF payload” и “MSF Encode”. Эти методы особенно полезны для генерации полезных данных в различных форматах и их кодирования с использованием различных модулей кодировщика. Объединив эти два инструмента в один, можно использовать единую платформу

для оптимизации параметров командной строки и ускорения процесса [6].

Эта утилита также поддерживает все стандартные полезные нагрузки Metasploit.

Синтаксис данной утилиты выглядит следующим образом: msfvenom -p (payload type) lhost=(Listening's_IP) lport=(Listening_Port) -f (Filetype) > (Output Filename).

Ниже приведены параметры, которые используются для настройки модуля:

1. «-p» — определяет тип полезной нагрузки.

2. Lhost — определяет адрес локального хоста, для получения обратного соединения.

3. Lport — определяет порт Localhost, на котором соединение прослушивает жертву.

4. «-f» — определяет тип выходного файла.

5. Output filename — определяет имя выходного файла.

После того, как был создан вредоносный файл, как показано на рис. 5, необходимо любыми способами установить и запустить данный вредоносный файл на компьютере жертвы. Помимо этого, необходимо запустить Netcat в качестве листенера для захвата обратного соединения, с помощью команды «nc–lvp (lport)».

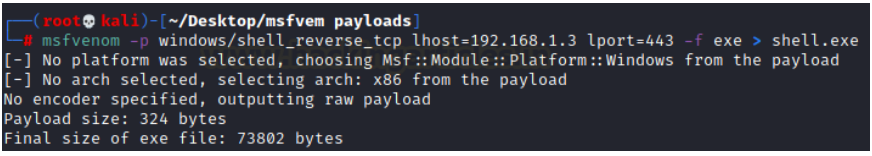

Рис. 5. Создание вредоносного «exe» файла с помощью MSFvenom

После запуска данного вредоносного файла будет захвачено обратное соединение и будет получен доступ к шеллу командной строки атакуемой цели.

Результаты

Лабораторная работа № 1.

В лабораторной работе № 1 было предложено получить доступ к целевой машине с помощью эксплойта «EternalBlue», после

эксплуатации провести повышение привилегий Meterpreter, запуск Кейлоггера и похитить хэши паролей учетных записей.

Лабораторная работа № 2.

В лабораторной работе № 2 было предложено создать с помощью MSFvenom вредоносные файлы, затем необходимо было либо самостоятельно запустить данные файлы на целевой машине, либо заставить жертву самой запустить их с помощью социальной инженерии. Вследствие чего был бы совершен захват обратного соединения и получен доступ к целевой машине.

Заключение. Данная тема останется актуальной, так как злоумышленники совершенствуют навыки применения и разработки эксплойтов, и всегда подобные среды как Metasploit Framework будут актуальны. Злоумышленники также будут продолжать применять подобные среды и эксплойты для атак. Следовательно, специалистам по информационной безопасности также нужно знать данную тему для пентеста систем, чтобы повторять действия злоумышленников в благих целях.

Результатом данной работы стала подготовленная серия лабораторных работ по эксплуатации уязвимых машин с помощью среды Metasploit Framework.

Серия лабораторных работ, которая посвящена эксплуатации уязвимостей, поможет студентам по информационной безопасности освоить теоретические основы тестирования на проникновение и попрактиковаться в их выполнении.

СПИСОК ЛИТЕРАТУРЫ

1. Левцов В. Анатомия таргетированной атаки. Ч. 2 / В. Левцов, Н. Демидов. — Текст : электронный // Information Security. — 2016. — № 3. — URL: https://lib.itsec.ru/articles2/Oborandteh/anatomiya-targetirovannoy-ataki-chast-2 (дата обращения: 25.05.2022).
2. Криптовалютные вымогательства добрались до России. — 2021. — URL: https://ru.beincrypto.com/kriptovalyutnye-vymogatelstva-rossia (дата обращения: 25.05.2022). — Текст : электронный.

3. RAPID7, Metasploit Framework. — URL: https://docs.rapid7.com/metasploit/quick-start-guide (date of the application: 26.05.2022). — Text : electronic.
4. Пост-эксплуатация с помощью Meterpreter — подсказка для Linux. — URL: https://ciksiti.com/ru/chapters/1260-post-exploitation-with-meterpreter--linux-hint (дата обращения: 26.05.2022). — Текст : электронный.
5. How to use a reverse shell in Metasploit | Metasploit Documentation Penetration Testing Software, Pen Testing Security. — URL: https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-a-reverse-shell-in-metasploit.html (date of the application: 27.05.2022). — Text : electronic.
6. How to exploit any android device using msfvenom and Metasploit Framework / Archana Tulsiyani. — URL: https://archanatulsiyani21.medium.com/how-to-exploit-any-android-device-using-msfvenom-and-metasploit-framework-9e90af4a4d7b (date of the application: 27.05.2022). — Text : electronic.

А. И. Левченко, А. С. Нестеров, М. С. Двинский, А. В. Широких
Тюменский государственный университет, г. Тюмень

УДК 004.056

РАЗРАБОТКА ЗАЩИЩЕННОГО ЛИЧНОГО КАБИНЕТА ДЛЯ ЧАСТНОЙ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

Аннотация. *В статье обсуждаются процесс разработки и средства для защиты данных пользователей личного кабинета частной медицинской организации. Приведено обоснование стойкости выбранных криптографических методов. Представлена демонстрация работы готового приложения.*

Ключевые слова: *цифровизация, разработка, безопасность, защита данных, ФСТЭК, Blowfish, bcrypt, Java, React.*

Введение. Актуальность темы обусловлена фактом того, что в современном мире происходит стремительная цифровизация и автоматизация бизнес-процессов, сфера здравоохранения при этом не исключение. Подтверждением данного факта является указ Президента Российской Федерации от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года» [1].