Столыпинский вестник

Научная статья

Original article

УДК 004.424

METASPLOIT КАК ПРОЕКТ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

METASPLOIT AS A COMPUTER SECURITY PROJECT

Багдасаров Даниэль Михайлович, студент бакалавр, Донской государственный технический университет, г. Ростов-на-Дону (344003 Россия г. Ростов-на-Дону, Гагарина 1), baggggdass@rambler.ru

Bagdasarov Daniel Mikhailovich, bachelor student, Don State Technical University, Rostov-on-Don (344003 Russia, Rostov-on-Don, Gagarina 1), baggggdass@rambler.ru

Аннотации: Проект Metasploit — это проект компьютерной безопасности, который предоставляет данные об уязвимостях безопасности и помогает проводить тестирование на проникновение. Он принадлежит Rapid7, американской фирме по кибербезопасности. Примечательным подпроектом Metasploit является Metasploit Framework с открытым исходным кодом — инструмент, используемый для разработки и запуска кода эксплойта на удаленных целевых системах.

Annotations: The Metasploit project is a computer security project that provides data on security vulnerabilities and helps with penetration testing. It is owned by Rapid7, an American cybersecurity firm. A notable subproject of

Metasploit is the open source Metasploit Framework, a tool used to develop and run exploit code on remote target systems.

Ключевые слова: информационная безопасность, злоумышленник, анализ. Metasploit.

Key words: information security, intruder, analysis. Metasploit.

Проект Metasploit включает средства защиты от криминалистики и исправления, некоторые из которых встроены в Metasploit Framework. Metasploit предустановлен в операционной системе Kali Linux.

Одна из главных причин для принятия Metasploit заключается в том, что Metasploit имеет открытый исходный код и активно развивается. В отличие от многих других инструментов пентестинга, Metasploit обеспечивает широкие возможности настройки, предоставляя пентестерам полный доступ к исходному коду и возможность добавлять пользовательские модули.

Интеллектуальная генерация полезной нагрузки. Metasploit позволяет тестировщикам легко переключать полезные нагрузки с помощью команды setpayload. Это обеспечивает большую гибкость при попытке проникнуть в систему с помощью доступа на основе оболочки или meterpreter, динамического инструмента сценариев Metasploit. Тестировщики также могут использовать приложение MsfVenom для создания шелл-кода для эксплуатации вручную непосредственно из командной строки.

Чистые выходы и постоянство. Metasploit может закрыться без обнаружения, даже если целевая система не перезапустится после теста на проникновение. Он также предоставляет несколько вариантов для обеспечения постоянного доступа к целевой системе.

Визуальный интерфейс. Metasploit предоставляет несколько простых в использовании графических интерфейсов, в первую очередь Armitage. Эти графические интерфейсы позволяют выполнять стандартные функции тестирования на проникновение, такие как управление уязвимостями и создание рабочих областей, одним нажатием кнопки.

Metasploit Framework содержит большое количество инструментов, позволяющих пентестерам выявлять уязвимости в системе безопасности, проводить атаки и избегать обнаружения. Многие инструменты организованы в виде настраиваемых модулей. Вот некоторые из наиболее часто используемых инструментов:

MSFconsole — это основной интерфейс командной строки (CLI) Metasploit. Он позволяет тестировщикам сканировать системы на наличие уязвимостей, проводить сетевую разведку, запускать эксплойты и многое другое.

Модули эксплойтов — позволяют тестировщикам нацеливаться на конкретную известную уязвимость. Metasploit имеет большое количество модулей эксплойтов, в том числе эксплойты переполнения буфера и SQL-инъекций. Каждый модуль имеет вредоносную полезную нагрузку, которую тестеры могут выполнять на целевых системах.

Вспомогательные модули — позволяют тестировщикам выполнять дополнительные действия, необходимые при тестировании на проникновение, не связанные с прямой эксплуатацией уязвимостей. Например, фаззинг, сканирование и отказ в обслуживании (DoS).

Модули постэксплуатации — позволяют тестировщикам расширить свой доступ к целевой системе и подключенным системам. Например, перечислители приложений, сетевые перечислители и дампы хэшей.

Модули полезной нагрузки — предоставляют шелл-код, который запускается после того, как тестеру удастся проникнуть в систему. Полезные нагрузки могут быть статическими сценариями или могут использовать Meterpreter, расширенный метод полезной нагрузки, который позволяет тестировщикам писать свои собственные библиотеки DLL или создавать новые возможности эксплойта.

Генератор бездействия (NOPS) — создает случайные байты, которые могут заполнять буферы с целью обхода систем обнаружения и предотвращения вторжений (IDS/IPS).

Хранилище данных — центральная конфигурация, позволяющая тестировщикам определять поведение компонентов Metasploit. Он также позволяет задавать динамические параметры и переменные и повторно использовать их между модулями и полезными нагрузками. Metasploit имеет глобальное хранилище данных и отдельное хранилище данных для каждого модуля.

После установки Metasploit вы можете найти все модули Metasploit по одному из следующих путей к файлам: Установка из бинарника: /path/to/metasploit/apps/pro/msf3/modules. Клонирование репозитория с GitHub: /path/to/metasploit-framework-repo/modules. Инструменты, предлагаемые Metasploit.

MSFконсоль

MSFconsole — это интерфейс Metasploit по умолчанию. Он предоставляет все команды, необходимые для взаимодействия с фреймворком, а также автозавершение стандартных команд с помощью табуляции. Чтобы научиться использовать интерфейс командной строки, может потребоваться некоторое время, но когда вы ознакомитесь с инструментом, пользоваться им станет проще.

msfdb

msfdb — это инструмент управления базами данных, поддерживающий базы данных PostgreSQL. В базе данных msfdb хранится информация, включая данные хостов, результаты эксплойтов и добычу. Вы можете использовать msfdb для импорта результатов сканирования из внешних инструментов, таких как Nessus или Nmap. Он предоставляет список команд, которые можно использовать для экспорта и импорта результатов сканирования.

Msfvenom

Msfvenom позволяет создавать пользовательские полезные нагрузки для конкретных целей. Инструмент был создан путем объединения двух предыдущих инструментов Metasploit — msfencode и msfpayload.

Msfvenom может помочь обойти безопасность цели, защищенной брандмауэром или антивирусом. Вы можете использовать msfvenom для настройки полезной нагрузки для конкретной цели и достижения более высоких показателей успеха во время теста на проникновение.

Meterpreter

Meterpreter — это расширенная полезная нагрузка Metasploit. Как правило, полезные нагрузки Metasploit выполняют определенную функцию. Тем не менее, Meterpreter динамичен, что позволяет вам писать сценарии на лету. Как только вы успешно эксплуатируете систему, вы можете внедрить Meterpreter в качестве полезной нагрузки.

Вот что вы можете сделать после того, как успешно внедрили полезную нагрузку Meterpeter:

- Настройте зашифрованную связь между целью и вашей системой.
- Получить хэши паролей дампа из целевой системы
- Найдите файлы в файловой системе цели
- Скачать или загрузить файлы
- Делайте снимки с веб-камеры целевой системы

Meterpreter существует и работает из памяти цели. Эта скрытность Meterpeter делает его чрезвычайно трудным для обнаружения. Даже криминалистическим инструментам бывает сложно отследить Meterpreter.

Вы можете использовать Ruby для написания сценариев Meterpreter, которые выполняют пользовательские функции. Meterpreter также предоставляет модуль Python, который предоставляет дополнительные команды, которые вы можете использовать для выполнения скриптов Python на целевой машине.

Armitage

Armitage — это графический пользовательский интерфейс на основе Java. Основное преимущество этого интерфейса заключается в том, что он может визуализировать цели и рекомендовать эксплойты. Он также

поддерживает сценарии, что позволяет автоматизировать избыточные задачи, такие как обнаружение узлов.

Armitage идеально подходит для сценариев, включающих сети с большим количеством систем. Инструмент позволяет просматривать файлы, повышать привилегии, выгружать хэши паролей и многое другое.

Metasploit может легко интегрироваться с такими элементами, как перечисление исправлений Windows, сканирование SNMP на этапе сбора информации теста на проникновение. Он также обеспечивает связь со сканером уязвимостей Nessus компании Tenable. Metasploit интегрируется практически с любым инструментом разведки, позволяя вам определить нужную уязвимость.

Когда вы найдете уязвимость, вы можете поискать в расширяемой базе данных Metasploit эксплойт, который ее взломает. Например, Shadow Brokers выпустили эксплойт NSA EternalBlue в 2017 году, упакованный для Metasploit, который может помочь вам справиться с неисправленной устаревшей системой Windows.

Вы сопоставляете эксплойт с соответствующей полезной нагрузкой для задачи. Например, Meterpreter — это интерактивная оболочка, работающая только в памяти, что делает ее подходящей для атаки на систему Windows, учитывая, что большинству людей нужна оболочка. В зависимости от используемых эксплойтов существуют определенные шелл-коды для Linux-боксов.

После того, как вы взломали целевую машину, Metasploit предоставляет полный набор инструментов пост-эксплуатации с новыми функциями, добавляемыми каждый год. Например, один из вариантов — создать постоянный бэкдор, который останется на машине даже после перезагрузки. Другие инструменты включают перехват пакетов, эскалаторы привилегий, захват экрана, поворотные устройства и кейлоггеры. Metasploit также предлагает фаззер для выявления потенциальных недостатков безопасности в двоичном коде и расширяющийся выбор вспомогательных модулей.

Metasploit — это легко расширяемая модульная структура, поддерживаемая активным сообществом. Хотя это просто высокоуровневое описание возможностей Metasploit, вы почти всегда можете настроить его, чтобы выполнить именно тот пентест, который вам нужен, как только вы получите более глубокое понимание этого.

Как и любой другой инструмент безопасности, фреймворк Metasploit можно использовать как легально, так и нелегально. Пользователи несут ответственность за использование инструмента законным образом. В общем, если у вас нет контракта с организацией, позволяющей вам тестировать конкретную систему, не используйте на ней Metasploit. Даже во время утвержденного теста на проникновение убедитесь, что вы используете Metasploit в рамках утвержденной клиентом области и соблюдаете разрешенные условия использования инструмента.

Еще одна проблема, о которой следует помнить, заключается в том, что использование Metasploit может привести к нежелательным результатам. Многие эксплойты предназначены для применения переполнения буфера , состояния гонки или других уязвимостей программного обеспечения. Эти эксплойты представляют опасность, поскольку уязвимости могут дестабилизировать целевую систему. Многие эксплойты могут привести к неожиданному отказу в обслуживании, сбоям приложений, перезапускам системы и неожиданному поведению приложений. Убедитесь, что организация, заказывающая тест на проникновение, имеет план действий в чрезвычайных ситуациях для подготовки к таким ситуациям.

Наконец, примите во внимание, что хотя Metasploit предлагает более 2000 эксплойтов, это лишь малая часть реальных эксплойтов, доступных злоумышленникам. Всегда учитывайте наиболее актуальные угрозы, с которыми сталкивается ваш клиент или организация. При необходимости разработайте собственный модуль Metasploit или используйте дополнительные инструменты, чтобы убедиться, что вы охватываете все соответствующие угрозы.

Imperva предоставляет брандмауэр веб-приложений, который может предотвратить эксплойты и инъекции кода, например, протестированные Metasploit. WAF может перехватывать вредоносный трафик и блокировать его в режиме реального времени.

Кроме того, Imperva Runtime Application Self-Protection (RASP) обеспечивает обнаружение и предотвращение атак в режиме реального времени из среды выполнения вашего приложения. RASP может останавливать внешние атаки и инъекции и сокращать количество незавершенных уязвимостей.

Помимо защиты от эксплойтов, Imperva обеспечивает комплексную защиту приложений, API и микросервисов:

Безопасность API. Автоматическая защита API обеспечивает защиту ваших конечных точек API по мере их публикации, защищая ваши приложения от эксплуатации.

Расширенная защита от ботов. Предотвращайте атаки на бизнес-логику со всех точек доступа — веб-сайтов, мобильных приложений и API. Обеспечьте полную видимость и контроль над трафиком ботов, чтобы остановить онлайн-мошенничество путем захвата учетной записи или извлечения конкурентоспособных цен.

Защита от DDoS -атак — блокируйте атакующий трафик на периферии, чтобы обеспечить непрерывность бизнеса с гарантированным временем безотказной работы и отсутствием влияния на производительность. Защитите свои локальные или облачные ресурсы независимо от того, размещены ли вы в AWS, Microsoft Azure или Google Public Cloud.

Аналитика атак — обеспечивает полную видимость с помощью машинного обучения и экспертизы предметной области в стеке безопасности приложений, чтобы выявлять закономерности в шуме и обнаруживать атаки на приложения, позволяя изолировать и предотвращать кампании атак.

Защита на стороне клиента. Получите видимость и контроль над сторонним кодом JavaScript, чтобы снизить риск мошенничества в цепочке поставок, предотвратить утечку данных и атаки на стороне клиента.

Литература

1. Бабаш, А.В. Информационная безопасность: Лабораторный практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2019. - 432 с.
2. Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. - М.: КноРус, 2013. - 136 с.
3. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 400 с.
4. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2017. - 476 с.
5. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
6. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2008. - 400 с.
7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2010. - 324 с.

References

1. Babash, A.V. Information security: Laboratory workshop / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2019. - 432 p.
2. Babash, A.V. Information Security. Laboratory workshop: Textbook / A.V. Babash, E.K. Baranova, Yu.N. Melnikov. - M.: KnoRus, 2013. - 136 p.
3. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 400 p.

4. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2017. - 476 p.
5. Baranova, E.K. Information security and information protection: Textbook / E.K. Baranova, A.V. Babash. - M.: Rior, 2018. - 400 p.
6. Baranova, E.K. Information Security. History of special methods of cryptographic activity: Textbook / E.K. Baranova, A.V. Babash, D.A. Larin. - M.: Rior, 2008. - 400 p.
7. Biryukov, A.A. Information security: protection and attack / A.A. Biryukov. - M.: DMK Press, 2013. - 474 p.
8. Gafner, V.V. Information Security: Textbook / V.V. Gafner. - Rn / D: Phoenix, 2010. - 324 p.

Для цитирования: Багдасаров Д.М. Metasploit как проект компьютерной безопасности// Научный сетевой журнал «Столыпинский вестник», номер 4/2022.