Смирнов Борис Андреевич, студент,
Финансовый университет при Правительстве РФ,
г. Москва

Власов Михаил Викторович, студент,
Финансовый университет при Правительстве РФ,
г. Москва

Резниченко Сергей Анатольевич,
кандидат технических наук, доцент кафедры
информационной безопасности Финансового
университета при Правительстве РФ,
Финансовый университет при Правительстве РФ,
г. Москва

СРЕДСТВА, ИСПОЛЬЗУЕМЫЕ ПРИ ПРОВЕДЕНИИ ПЕНЕТРАЦИОННОГО ТЕСТИРОВАНИЯ ВНУТРЕННЕЙ ИНФРАСТРУКТУРЫ

Аннотация: В данной статье рассматриваются основные этапы и цели пенетрационного тестирования, включая объяснение понятия, обзор основных целей, программные и аппаратные средства пентестинга, а также роль сканирования, эксплуатации и поддержания доступа.

Ключевые слова: Пенетрационное тестирование, пентест, внутренний аудит ИБ

1. Введение

1.1 Понятие пенетрационного тестирования

Пенетрационное тестирование (или пентестинг) представляет собой методологию проверки безопасности информационных систем и сетей путем имитации атак со стороны злоумышленников.

1.2 Цели и задачи пентеста в рамках аудита ИБ

Ниже приведены основные цели и задачи, которые решаются при проведении пенетрационного тестирования:

– Одной из основных задач пентестинга является обнаружение уязвимостей в информационной системе или сети. Это может включать в себя поиск слабых мест в конфигурации систем, недостатков в коде программного обеспечения, неправильно настроенных прав доступа и других потенциальных угроз для безопасности.

– После выявления уязвимостей пентестеры оценивают степень риска, которую эти уязвимости могут представлять для организации. Оценка риска включает в себя анализ вероятности эксплуатации уязвимости злоумышленниками и возможных последствий для бизнеса.

– Пентестинг также направлен на проверку эффективности существующих мер безопасности. Это включает в себя оценку работы средств защиты, таких как брандмауэры, системы обнаружения вторжений, антивирусные программы и другие механизмы защиты.

2. Категории средств для пенетрационного тестирования

Для проведения пенетрационного тестирования изначально проводится разведка. Под разведкой здесь понимается OSINT – поиск IP-адресов, имен учетных записей, доменных имен и так далее по открытым источникам. Сканирование, соответственно, подразумевает исследование уже найденных IP-адресов.

Основные методологии, которые используются для проведения пентеста:

– ISSAF (Information Systems Security Assessment Framework) – по сути является 1000-страничной инструкцией. Каждый этап атаки в этой методологии сопровождается конкретными командами;

– PTES (Penetration Testing Execution Standard) – в нем преобладает теория, но приводятся ссылки на инструменты, которые можно использовать в работе;

– OSSTMM (Open-Source Security Testing Methodology Manual) – представляется наиболее актуальным на сегодняшний день, разработанный Институтом безопасности и открытых методологий (ISECOM);

– MITRE ATT&K – представляет собой интерактивную матрицу, описывающую техники и тактики злоумышленников, делит свою методологию на техники, тактики и процедуры:

○ тактика – это тактическая цель злоумышленника, причина совершения действия. Всего в матрице существует 14 техник, каждая из которых отвечает на вопрос «почему?»;

○ техника отвечает на вопрос «как?» – как злоумышленник достигает тактической цели, выполняя определенное действие;

○ процедура – конкретная реализация техники.

Для реализации пентеста всегда нужно подобрать требуемые для той или иной работы дистрибутивы операционных систем, были выделены основные, а также определены их преимущества:

– Kali Linux – один из лучших безопасных дистрибутивов для разработчиков. Он не оставляет никаких следов после использования пользователем, которые могли бы привести к утечке информации. Имеет большое количество утилит в базовой версии.

– Windows – знакомая всем система, основным ее преимуществом является то, что большинство инструментов для проведения пентеста написаны среде.NET, разработанной компанией Microsoft.

Кроме перечисленных операционных систем используются и иные модификации, однако для проведения внутреннего инфраструктурного аудита именно они наиболее востребованы.

Программное обеспечение, используемое для проведения аудита, имеет очень большой спектр, поэтому были выбраны инструменты для работы с сетью:

– Платформа Metasploit – одно из лучших средств сетевой безопасности для разработки и выполнения кода эксплойта на удаленной целевой машине. Другие важные подпроекты включают базу данных кодов операций, архив шелл-кодов и соответствующие исследования;

– Nmap – это бесплатная утилита с открытым исходным кодом для сетевого обнаружения и аудита безопасности;

– Zeek (ранее Bro) – это мощная платформа сетевого анализа с открытым исходным кодом;

– HoneyPy – это открытое программное обеспечение, которое используется для обнаружения и сбора информации о злоумышленниках и их атаках. ПО позволяет пользователям создавать виртуальные слушатели для различных протоколов, таких как HTTP, FTP, Telnet и т.д. и отслеживать их взаимодействие со злоумышленниками. Это позволяет получить информацию об IP-адресах, идентификаторах сессий и используемом ПО злоумышленников для дальнейшей аналитики и защиты системы;

– Wireshark – это бесплатный анализатор пакетов с открытым исходным кодом. Инструмент используется для устранения неполадок в сети, анализа, разработки программного обеспечения и коммуникационных протоколов, а также обучения. Wireshark очень похож на tcpdump, но имеет графический интерфейс, а также некоторые встроенные опции сортировки и фильтрации.

Кроме программного обеспечения для получения начального доступа используются аппаратные средства, подключаемые к сканируемому устройству посредством соответствующих разъемов. Некоторые из них:

– Shark Jack – портативное устройство, которое позволяет проводить аудит в локальных сетях и за их периметром. Подключается к сетевой розетке и за 15 минут работы от аккумулятора сканирует сеть. Имеет внутреннюю память.

– LAN Turtle представляет собой USB-Ethernet-адаптер – имплант в LAN сеть, который подключается в разрыв между сетевым кабелем и компьютером. Так он обеспечивает скрытый удаленный доступ, сбор сетевых данных. Питается от USB, имеет слот для SIM-карты и может оставаться незамеченным достаточно долго.

– Screen Crab – устанавливается в разрыв, между компьютером и монитором. Он перехватывает и ретранслирует по Wi-Fi сигнал, идущий по HDMI-кабелю. Имеет антенну и два разъема: USB-C и HDMI.

– Bash Bunny – представляет собой USB-накопитель, который полезен для проведения проверок посредством атаки вида «Дорожное яблоко», жертва подбирает лежащее устройство и при подключении оно выполняют определенную полезную нагрузку.

– Wi-Fi Pineapple для перехвата и атак на Wi-Fi. Собирает данные о сети и устройствах в ней, поддерживает атаки на WPA. Имеет собственный веб-интерфейс и экосистему дополнительных загружаемых приложений.

3. Основные фазы пенетрационного тестирования

3.1 Сканирование

В этой фазе пентестеры исследуют информационную инфраструктуру организации с целью обнаружения открытых портов, сервисов, идентификации устройств и сетевых элементов, а также выявления потенциальных уязвимостей. Подробнее рассмотрим основные аспекты сканирования:

– Сетевое сканирование: Пентестеры используют специализированные инструменты для сканирования сети с целью определения активных устройств, открытых портов и доступных сервисов. Это позволяет составить карту сети и получить представление о том, как организована инфраструктура.

– Пассивное сканирование: это может включать в себя мониторинг трафика с помощью инструментов, таких как Wireshark или tcpdump, для анализа сетевой активности и обнаружения потенциальных уязвимостей.

– Оценка конфигурации: это включает в себя поиск недостатков в настройках безопасности, необходимых для предотвращения атак, таких как слабые пароли, открытые доступы к административным интерфейсам и другие конфигурационные ошибки.

3.2 Эксплуатация

Фаза эксплуатации в пенетрационном тестировании представляет собой процесс активного использования выявленных уязвимостей с целью получения несанкционированного доступа к информационной системе или сети. Рассмотрим подробнее основные аспекты эксплуатации:

– Выбор уязвимости для эксплуатации: Это могут быть уязвимости, позволяющие выполнить удаленное выполнение кода, получить несанкционированный доступ к системе или сети, обойти аутентификацию и т. д.

– Получение доступа к системе: Пентестеры могут использовать эксплойты для получения доступа к административным интерфейсам, исполнения команд на удаленной машине, перехвата сеансов аутентификации и других методов.

– Поддержание доступа: Это может включать в себя установку вредоносного ПО для обхода средств обнаружения вторжений или создание скрытых учетных записей.

– Анализ результатов: После эксплуатации уязвимостей пентестеры проводят анализ результатов атаки, оценивают полученный доступ и его потенциальные последствия. Это позволяет оценить уровень риска и разработать рекомендации по устранению выявленных уязвимостей.

3.3 Поддержание доступа и тестирование

После успешного получения доступа к информационной системе или сети на этапе эксплуатации, фаза поддержания доступа и тестирования становится необходимой для оценки стабильности и долгосрочных последствий атаки. Рассмотрим основные аспекты этой фазы:

– Поддержание доступа: Это может включать в себя создание скрытых учетных записей, установку вредоносного программного обеспечения (например, троянов), использование бэкдоров и другие техники для обхода механизмов обнаружения и удаленного управления системой.

– Тестирование безопасности: Включает в себя проверку наличия и работоспособности средств обнаружения вторжений, антивирусных программ, систем мониторинга безопасности и других механизмов защиты.

– Тестирование реакции на инциденты: Пентестеры могут также проверять реакцию организации на обнаружение инцидентов безопасности. Это может включать в себя симуляцию атак и наблюдение за реакцией персонала на алармы и инциденты, а также оценку эффективности процедур реагирования на инциденты.

– Документирование результатов: По завершении этапа поддержания доступа и тестирования пентестеры документируют все обнаруженные уязвимости, проведенные атаки, реакцию системы на инциденты безопасности и другие важные аспекты тестирования. Эта информация используется для подготовки отчета и предоставления рекомендаций по улучшению безопасности.

4. Заключение

В заключение, проведение пенетрационного тестирования является неотъемлемой частью стратегии обеспечения информационной безопасности для любой организации. Анализ уязвимостей и оценка уровня защиты помогают выявить слабые места в инфраструктуре и принять меры по их устранению, что существенно снижает риски возможных кибератак и утечек данных.

В результате пенетрационного тестирования выявляется не только текущее состояние безопасности, но и демонстрируются потенциальные последствия успешной атаки. Это позволяет руководству и специалистам по информационной безопасности принимать обоснованные решения по внедрению дополнительных мер защиты и обеспечению безопасности информационных активов организации.

Следует отметить, что пенетрационное тестирование должно рассматриваться как часть непрерывного процесса обеспечения безопасности, а не как одноразовое событие. Регулярное тестирование и обновление мер безопасности в соответствии с новыми угрозами и технологиями помогают организациям оставаться устойчивыми к возрастающему уровню киберугроз.

Список литературы:

1. Макаренко Сергей Иванович, Смирнов Глеб Евгеньевич МЕТОДИКА ОБОСНОВАНИЯ ТЕСТОВЫХ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ, ОБЕСПЕЧИВАЮЩИХ РАЦИОНАЛЬНУЮ ПОЛНОТУ АУДИТА ЗАЩИЩЕННОСТИ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ // Вопросы кибербезопасности. 2021. №6 (46). URL: https://cyberleninka.ru/article/n/metodika-obosnovaniya-testovyh-informatsionno-tehnicheskih-vozdeystviy-obespechivayuschih-ratsionalnuyu-polnotu-audita.

2. Макаренко Сергей Иванович, Смирнов Глеб Евгеньевич Анализ стандартов и методик тестирования на проникновение // Системы управления, связи и безопасности. 2020. №4. URL: https://cyberleninka.ru/article/n/analiz-standartov-i-metodik-testirovaniya-na-proniknovenie.

3. Шкрадюк А.Д. Оценка безопасности информационных систем с помощью тестирования на проникновение // Умная цифровая экономика. 2022. №4. URL: https://cyberleninka.ru/article/n/otsenka-bezopasnosti-informatsionnyh-sistem-s-pomoschyu-testirovaniya-na-proniknovenie.

4. Абидарова Александра Алексеевна КИБЕРАТАКИ НА ИНФОРМАЦИОННЫЕ И АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ И КОМПЛЕКСЫ // Известия ТулГУ. Технические науки. 2020. №11. URL: https://cyberleninka.ru/article/n/kiberataki-na-informatsionnye-i-avtomatizirovannye-sistemy-i-kompleksy.

5. Макаренко Сергей Иванович КРИТЕРИИ И ПОКАЗАТЕЛИ ОЦЕНКИ КАЧЕСТВА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ // Вопросы кибербезопасности. 2021. №3 (43). URL: https://cyberleninka.ru/article/n/kriterii-i-pokazateli-otsenki-kachestva-testirovaniya-na-proniknovenie.