МЕТОДИКА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ ДЛЯ ПОДРАЗДЕЛЕНИЙ КИБЕРБЕЗОПАСНОСТИ

Михайловский С.Г., студенты гр.461403

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Белоусова Е.С. – канд. техн. наук, доцент

Аннотация. В статье рассматривается роль методики тестирования на проникновение в деятельности подразделений кибербезопасности. Раскрываются ключевые этапы разработанной методики: разведка, сканирование, анализ уязвимостей, эксплуатация, закрепление в системе и нагрузочное тестирование. Особое внимание уделяется современным инструментальным средствам, включая AI-first сканеры, технологии эксплуатации уязвимостей и автоматизации обработки данных. Подход ориентирован на практическое использование атакующими и защищающими командами для объективной оценки защищенности корпоративных информационных систем.

Ключевые слова. тестирование на проникновение, пентест, методика, эксплуатация уязвимостей, импланты, C2-каналы, автоматизация, AI-безопасность, команда кибербезопасности, Red Team, Blue Team.

Современные корпоративные информационные системы представляют собой сложные распределенные комплексы с облачными платформами, виртуализацией, микросервисами и множеством внешних интеграций. В условиях роста кибератак обеспечение информационной безопасности требует регулярной оценки эффективности средств защиты, ключевым инструментом которой выступает тестирование на проникновение. В крупных организациях функции могут быть разделены между «красными» (Red Team) и «синими» (Blue Team) командами, а эффективное взаимодействие между ними невозможно без формализованной методики. Настоящая статья посвящена разработке комплексной методики тестирования на проникновение, включающей этапы проведения, инструментальное обеспечение на базе AI-first сканеров и автоматизацию. Предлагаемый подход ориентирован на практическое применение подразделениями кибербезопасности для объективной оценки защищенности корпоративных информационных систем [1].

Разработанная методика базируется на модели Cyber Kill Chain и включает шесть последовательных этапов, обеспечивающих полноту охвата всех стадий атаки: от сбора информации до закрепления в системе.

Этап планирования и подготовки, формализует цели, объем и правила взаимодействия. Определяются объекты оценки: внешний периметр (веб-приложения, шлюзы), внутренняя инфраструктура (серверы приложений, БД, СХД), сетевая архитектура (VLAN, межсетевые экраны, микросегментация), человеческий фактор. На данном этапе формируется команда, распределяются роли, разрабатывается план взаимодействия с заказчиком, включая информирование о критических находках и механизмы экстренного прекращения тестирования.

Этап разведки делится на пассивные и активные методы, при этом пассивная разведка включает анализ IP-адресов, DNS-имен, соцсетей, архивов сайтов с использованием theHarvester (сбор email и поддоменов), Maltego (визуальный анализ связей), Shodan (поиск устройств в глобальной сети). Активная разведка, это этап сканирование портов, определение версий сервисов, определение топологии сети. Автоматизация обеспечивается скриптами, которые выполняют последовательный запуск OSINT-инструментов, парсинг данных, формирование списков активных хостов и подготовку отчетов для импорта в другие системы [2].

Этап сканирования и анализа уязвимостей, обеспечивается применением Masscan, который позволяет осуществлять высокоскоростное обнаружение активных узлов и портов (до миллионов пакетов в секунду). Nmap выполняет детальный анализ версий сервисов, ОС и специализированные скрипты безопасности. Nmap с набором скриптов vulners автоматически сопоставляет версии ПО с CVE и оценивает критичность по CVSS. AI-first сканер MEDUSA (открытая платформа, 76+ анализаторов, 7300+ правил) выявляет классические уязвимости (SQL-инъекции, XSS) и риски AI-компонентов, LLM-интеграций. Преимущества сканера AI-first в снижении ложных срабатываний до 74 %, контекстная приоритизация рисков, поддержка более 42 языков (Python, JavaScript, Terraform, Docker, конфигурации AI-агентов) [3].

Этап эксплуатации уязвимостей и закрепления в системе позволяет моделировать действия злоумышленника. Как правило, эксплуатация выполняется с использованием публичных эксплойтов Metasploit для получения начального shell-доступа. Ключевое отличие методики в обязательном закрепление в системе для оценки способности средств защиты обнаруживать активность после получения доступа. Для этого используется платформа Sliver, позволяющая генерировать импланты на сервере C2 с обфускацией, что делает каждый экземпляр уникальным, усложняя сигнатурный анализ. Архитектура импланта включает ядро агента на Go, поддерживает протоколы C2 (HTTPS,

DNS, mTLS, WireGuard), модульная структура снижает вероятность обнаружения. После установления C2 выполняются сбор информации, повышение привилегий и горизонтальное перемещение для оценки сетевой сегментации и принципа минимальных привилегий.

Этап тестирования устойчивости и доступности, проводится на трех уровнях модели OSI: сетевом (hping3 для реализации SYN-flood, UDP-flood или проверки межсетевых экранов, IPS, SYN Cookies), транспортном (thc-ssl-dos для проверки устойчивости TLS/SSL к атакам, связанным с повторным согласованием соединения, выявление некорректных конфигураций веб-серверов), прикладном (siege для нагрузочного тестирования веб-сервисов, оценки кэширования, балансировщиков, отказоустойчивости). Автоматизация достигается скриптами, стандартизирующими параметры тестирования и формирующими сводные отчеты [3].

Этап анализа результатов и формирования рекомендаций, базируется на документировании уязвимостей с указанием методов эксплуатации, использованных инструментов и доказательной базы (логи C2, скриншоты). Формируется матрица рисков по CVSS с учетом бизнес-контекста. Предлагаются меры по совершенствованию СЗИ (формируется дорожная карта повышения защищенности).

Реализация представленной методики требует применения систематизированного набора инструментов, охватывающих все этапы тестирования. В таблице 1 представлены основные категории инструментов и их роль в методике.

Таблица 1 – Инструменты обеспечение методики тестирования на проникновение

Категория	Инструменты	Назначение
Базовая платформа	Kali Linux	Унифицированная операционная среда с предустановленным набором инструментов безопасности
Разведка и OSINT	theHarvester, Maltego, Shodan	Сбор информации из открытых источников, визуальный анализ связей, поиск устройств и сервисов
Сканирование портов	Masscan, Nmap	Высокоскоростное обнаружение активных узлов, детальное определение версий и операционных систем
Анализ уязвимостей	Nmap (скрипт vulners), MEDUSA	Поиск известных уязвимостей (CVE), AI-first статический анализ кода и конфигураций
Эксплуатация уязвимостей	Metasploit Framework	Выполнение эксплойтов, автоматизация атак
Закрепление и C2	Sliver	Генерация имплантов, управление каналами C2, пост-эксплуатация
Нагрузочное тестирование	hping3, thc-ssl-dos, siege	SYN-флуд, SSL renegotiation, нагрузочное тестирование веб-приложений
Социальная инженерия	GoPhish	Моделирование фишинговых кампаний, оценка человеческого фактора
Автоматизация процессов	Скрипты Python/Bash	Автоматизация сбора данных, обработки результатов, формирования отчетов

В ходе разведки скрипты последовательно собирают данные через OSINT-инструменты, фильтруют результаты, формируют списки активных хостов, поддоменов и email-адресов, подготавливают структурированные отчеты (JSON, XML) для импорта в системы анализа. Обеспечивается воспроизводимость и сравнительный анализ изменений атакуемой поверхности.

Скрипты выполняют двухэтапное сканирование: высокоскоростное обнаружение активных узлов Masscan, затем детальный анализ Nmap с определением версий и поиском уязвимостей. Результаты агрегируются в единый отчет. Дополнительно инициируется сканирование AI-first сканером MEDUSA, который выявляет уязвимости в коде и конфигурациях, снижая ложные срабатывания до 74 % [2].

Нагрузочное тестирование реализуется скриптами, последовательно запускающими различные типы атак (SYN-флуд, атаки на TLS/SSL, нагрузочное тестирование веб-сервисов), собирающими метрики производительности и формирующими сводные отчеты. Стандартизация параметров обеспечивает воспроизводимость результатов и сравнение показателей до и после изменений [3].

Скрипты агрегируют результаты всех этапов, формируют матрицу рисков с оценкой критичности уязвимостей и подготавливают итоговый отчет для передачи заказчику и интеграции с системами управления уязвимостями. Это сокращает время подготовки документов и обеспечивает единообразие результатов при повторных тестированиях.

Разработанная методика тестирования на проникновение повышает эффективность Red Team и Blue Team.

Для Red Team она обеспечивает системность, воспроизводимость и накопление знаний. Автоматизация высвобождает ресурсы для нестандартных задач, требующих глубокого понимания архитектуры.

Для Blue Team результаты тестирования позволяют приоритизировать устранение уязвимостей и настраивать системы обнаружения инцидентов. Автоматизированная отчетность ускоряет идентификацию критических рисков.

Взаимодействие команд строится на совместном планировании. Информированное тестирование оценивает не только возможность эксплуатации уязвимостей, но и способность службы ИБ их своевременно обнаружить. Совместный анализ предоставляет детальную информацию о методах, инструментах и тактиках для настройки систем обнаружения.

Особую ценность имеет этап закрепления в системе с использованием платформы Sliver. Развертывание обфусцированного импланта и установление скрытого канала C2 подтверждает неспособность средств защиты блокировать полиморфные нагрузки, доказывая необходимость поведенческого анализа и XDR. DNS-туннелирование для управления и эксфильтрации данных выявляет недостаточную глубину анализа служебных протоколов сетевой защитой [2].

Разработанная методика представляет собой систематизированный подход к оценке защищенности корпоративных информационных систем, интегрирующий ключевые этапы тестирования на проникновение, современные инструментальные средства и автоматизацию процессов. Ее реализация обеспечивает системность и воспроизводимость оценки, объективную оценку эффективности средств защиты, выявление не только наличия уязвимостей, но и реальной возможности их эксплуатации, формирование обоснованных рекомендаций.

Для команд Red Team и Blue Team методика создает основу системной работы и накопления знаний, а автоматизация позволяет сосредоточиться на сложных задачах. Для подразделений кибербезопасности результаты становятся объективной основой приоритизации защитных мероприятий и оценки эффективности внедренных средств.

Список использованных источников:

1. Бегаев А.Н., Бегаев С.Н., Федотов В.А. Тестирование на проникновение. – СПб: Университет ИТМО, 2018. – 45 с.

2. Парасрам Ш. Kali Linux. Тестирование на проникновение и безопасность / Шива Парасрам. – Москва : ДМК Пресс, 2021. – 432 с.

3. Efe A. A risk assessment on usage of Kali tools to hack and manipulate web-based MIS and ERP applications // Yönetim Bilişim Sistemleri Dergisi. – 2025. – Vol. 11, № 1. – P. 62–80.