СОВРЕМЕННЫЕ ИНСТРУМЕНТЫ АВТОМАТИЗИРОВАННОГО ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В ПОДГОТОВКЕ СПЕЦИАЛИСТОВ ПО КИБЕРБЕЗОПАСНОСТИ

Хамидов Шерзод Жалолдин угли[1]

[1] Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий, старший преподаватель, кафедра "Криптология"
sherzod.hamidov@tuit.uz
DOI: 10.61587/mmit.tiue.uz.v1i1.330

Аннотация: В статье рассматриваются современные инструменты автоматизированного тестирования на проникновение, используемые при подготовке специалистов по кибербезопасности. Проанализированы возможности и особенности таких инструментов, как Nmap, Metasploit, SQLmap, Burp Suite, PentestGPT, Nuclei и Pentera. Показано, что их применение способствует развитию практических навыков и повышению качества подготовки специалистов.

Ключевые слова: *кибербезопасность, тестирование на проникновение, автоматизированный пентест, Nmap, Metasploit, SQLmap, Burp Suite, PentestGPT, Nuclei, Pentera, искусственный интеллект.*

MODERN AUTOMATED PENETRATION TESTING TOOLS IN CYBERSECURITY TRAINING

Khamidov Sherzod Jaloldin ugli[1]

[1] Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Department "Cryptology" teacher
sherzod.hamidov@tuit.uz

Abstract. This paper discusses modern automated penetration testing tools used in cybersecurity education. The capabilities and applications of Nmap, Metasploit, SQLmap, Burp Suite, PentestGPT, Nuclei, and Pentera are analyzed. The study shows that these tools improve practical skills and enhance the effectiveness of cybersecurity training.

Keywords: *cybersecurity, penetration testing, automated pentesting, Nmap, Metasploit Framework, SQLmap, Burp Suite, PentestGPT, Nuclei, Pentera, artificial intelligence.*

Введение

Цифровая трансформация экономики и государственных услуг сопровождается постоянным ростом количества киберугроз. Согласно международным исследованиям, значительная часть успешных атак связана с эксплуатацией известных уязвимостей, которые могли быть обнаружены и устранены на этапе аудита информационной безопасности. В связи с этим возрастает потребность в специалистах по кибербезопасности, обладающих практическими навыками выявления и анализа уязвимостей информационных систем. Одним из наиболее эффективных методов подготовки таких специалистов является обучение технологиям тестирования на проникновение (Penetration Testing). Традиционный ручной анализ требует значительных временных затрат и высокой квалификации специалиста. Поэтому в образовательном процессе все чаще используются автоматизированные инструменты

тестирования на проникновение, позволяющие ускорить процесс поиска уязвимостей и сформировать у студентов практические навыки работы с современными средствами защиты информации.

Тестирования на проникновение

В условиях открытого Интернета инциденты в области кибербезопасности происходят все чаще, а различные виды кибератак уже представляют серьезную угрозу для безопасного функционирования сетевых сервисов. В связи с этим вопросы предотвращения атак и их оперативного обнаружения стали одним из наиболее актуальных направлений исследований в области информационной безопасности.

Для минимизации рисков безопасности и снижения вероятности несанкционированного проникновения необходимо проводить тестирование на проникновение до ввода системы в эксплуатацию, заранее моделируя возможные атаки на систему. Тестирование на проникновение играет ключевую роль в выявлении уязвимостей информационных систем и занимает важное место в современной системе кибербезопасности.

Тестирование на проникновение представляет собой процесс проверки и оценки безопасности информационных систем посредством моделирования методов атак или имитации действий, используемых злоумышленниками. Его основная цель заключается в выявлении уязвимостей, проверке возможности их эксплуатации и оценке потенциального ущерба, который может быть нанесен системе. Такой подход позволяет определить фактический уровень защищенности информационной инфраструктуры и эффективность существующих механизмов безопасности. В отличие от традиционного сканирования уязвимостей, которое преимущественно ориентировано на обнаружение известных слабых мест, тестирование на проникновение уделяет особое внимание анализу полной цепочки атаки.

Это включает проверку возможностей повышения привилегий, горизонтального перемещения внутри сети, несанкционированного доступа к данным и их утечки, а также других последствий успешной компрометации системы. Благодаря этому тестирование на проникновение максимально приближено к реальным сценариям кибератак и является одной из ключевых технологий оценки уровня информационной безопасности и эффективности защитных мер.

Основными этапами являются предварительный сбор информации, получение сведений об операционной системе, целевых IP-адресах, открытых портах, предоставляемых сервисах, SQL-уязвимостях и точках возможной инъекции.

После этого собранная информация анализируется и обрабатывается, определяются внешние и внутренние IP-адреса, а затем выполняются операции по тестированию на проникновение, повышению привилегий и другие действия.

На заключительном этапе на основе большого объема проведенного анализа автоматически формируется отчет о результатах тестирования на проникновение. В отчете содержится информация обо всех выявленных уязвимостях, включая утечку HTTP-заголовков, раскрытие файлов, XSS-уязвимости, возможность кликджекинга (Clickjacking), успешность SQL-инъекций, наличие или отсутствие заголовка X-Content-Type-Options, а также сведения об открытых портах и работающих службах. Кроме того, выполняется оценка уровня опасности обнаруженных уязвимостей хоста.

Итоговый отчет способствует проведению комплексного анализа безопасности системы и позволяет максимально снизить риск несанкционированного проникновения и компрометации ресурсов [1].

Традиционные методы тестирования на проникновение в значительной степени основаны на ручной работе специалистов. Несмотря на высокую гибкость и возможность адаптации к конкретным условиям, такие подходы имеют ряд существенных недостатков: длительный цикл выполнения, ограниченный охват проверяемых объектов и сильная зависимость от квалификации экспертов. В результате они уже не в полной мере соответствуют требованиям крупных и сложных информационных систем, нуждающихся в эффективной и интеллектуальной оценке уровня безопасности.

В последние годы активно развивается направление автоматизированного тестирования на проникновение (Automated Penetration Testing), которое позволяет повысить эффективность проверок за счет стандартизации процессов и интеграции специализированных инструментов.

Современные системы автоматизированного тестирования охватывают не только этапы сбора информации и выявления уязвимостей, но и процессы эксплуатации обнаруженных недостатков, проверки их воздействия на систему, а также выполнение действий на этапе постэксплуатации (post-exploitation). Благодаря этому такие системы становятся более близкими по своим возможностям к комплексным сценариям оценки безопасности, применяемым в рамках учений типа Red Teaming.

В настоящее время развитие автоматизированного тестирования на проникновение направлено на внедрение интеллектуальных методов моделирования цепочек атак, оптимизацию стратегий принятия решений, адаптивное планирование действий и обход современных механизмов защиты. Эти направления создают основу для формирования высокоэффективных и интеллектуальных систем кибербезопасности, способных осуществлять комплексное моделирование атак и противодействие современным киберугрозам [2].

Современные инструменты тестирования на проникновение

Nmap (Network Mapper) является популярным инструментом для обнаружения сетевых узлов и аудита безопасности. Он позволяет выявлять активные устройства, открытые порты, сетевые службы и используемые операционные системы. Благодаря поддержке NSE-сценариев Nmap также обеспечивает автоматизированный анализ потенциальных уязвимостей. Инструмент широко применяется на этапе сбора информации и поддерживает различные методы сканирования, включая TCP, SYN, UDP и OS Fingerprinting.

Metasploit Framework является одной из наиболее популярных платформ для тестирования на проникновение. Она предоставляет набор эксплойтов, полезных нагрузок и средств автоматизации для проверки уязвимостей и моделирования кибератак. Благодаря модульной архитектуре Metasploit поддерживает эксплуатацию уязвимостей, постэксплуатационный анализ, сбор системной информации и оценку возможных последствий компрометации системы [3].

SQLmap представляет собой инструмент с открытым исходным кодом для автоматизированного обнаружения и эксплуатации уязвимостей типа SQL Injection в веб-приложениях. Он поддерживает большинство современных СУБД, автоматически определяет тип базы данных, выявляет уязвимые параметры и позволяет анализировать структуру баз данных. Благодаря поддержке различных техник SQL-инъекций SQLmap значительно упрощает и ускоряет процесс тестирования безопасности веб-приложений.

Burp Suite является одним из наиболее популярных инструментов для анализа безопасности веб-приложений. Он позволяет перехватывать, анализировать и модифицировать HTTP/HTTPS-трафик между клиентом и сервером, обеспечивая детальное исследование веб-запросов. Благодаря встроенным модулям Burp Suite поддерживает как автоматизированное, так и ручное выявление уязвимостей, включая

SQL Injection, XSS, CSRF и ошибки аутентификации, что делает его востребованным как в профессиональной деятельности, так и в образовательном процессе [4].

Intruder представляет собой облачную платформу для автоматизированного сканирования уязвимостей и непрерывного мониторинга безопасности. Инструмент поддерживает более 140 000 проверок, включая уязвимости OWASP Top 10, SQL Injection и XSS. Благодаря постоянному мониторингу и автоматическим уведомлениям о новых угрозах Intruder позволяет своевременно выявлять риски и повышать уровень защищённости информационных систем.

Acunetix является инструментом автоматизированного анализа безопасности веб-приложений, использующим методы DAST и IAST для выявления уязвимостей в режиме реального времени. Платформа обнаруживает SQL Injection, XSS, SSRF, ошибки конфигурации и недостатки аутентификации, а также поддерживает тестирование сложных динамических веб-интерфейсов. Благодаря автоматизированному сканированию и подробной отчётности Acunetix повышает эффективность оценки безопасности веб-приложений [5].

Qualys представляет собой облачную платформу для управления уязвимостями и мониторинга безопасности информационных систем. Она обеспечивает автоматизированное обнаружение угроз, анализ конфигураций и непрерывное сканирование сетевой инфраструктуры, веб-приложений и облачных сред. Благодаря централизованному управлению, приоритизации рисков и аналитической отчётности Qualys помогает своевременно выявлять и устранять уязвимости, повышая уровень кибербезопасности организации [6].

PlexTrac представляет собой платформу для управления результатами тестирования на проникновение и уязвимостями, использующую технологии искусственного интеллекта для автоматизации отчётности и анализа рисков. Система обеспечивает централизованное управление обнаруженными уязвимостями, их классификацию и приоритизацию, а также поддерживает полный цикл устранения недостатков и повторного тестирования. Это позволяет повысить эффективность управления киберрисками и сократить время подготовки отчётов.

PentestGPT представляет собой платформу с открытым исходным кодом, использующую большие языковые модели (LLM) для интеллектуальной поддержки тестирования на проникновение. Инструмент анализирует результаты работы других средств безопасности, выявляет возможные векторы атак и предлагает рекомендации по

дальнейшим действиям. Благодаря использованию искусственного интеллекта PentestGPT помогает ускорить анализ сложных инфраструктур и повысить эффективность принятия решений в процессе тестирования безопасности [7].

Nuclei представляет собой высокопроизводительный инструмент автоматизированного поиска уязвимостей, основанный на использовании YAML-шаблонов. Он позволяет быстро выявлять известные уязвимости, ошибки конфигурации и признаки компрометации в веб-приложениях, сетевых сервисах и облачных средах. Благодаря высокой скорости работы, поддержке искусственного интеллекта для генерации шаблонов и интеграции с CI/CD-процессами Nuclei является эффективным средством оперативного управления уязвимостями [8].

Pentera представляет собой платформу автоматизированной проверки безопасности, предназначенную для моделирования реальных кибератак и оценки защищённости информационных систем. Используя технологии искусственного интеллекта, платформа автоматически выявляет уязвимости, формирует цепочки атак и имитирует действия Red Team. Благодаря поддержке корпоративных, облачных и промышленных инфраструктур Pentera позволяет непрерывно контролировать уровень безопасности и оценивать эффективность существующих мер защиты [9].

Таблица 1

Сравнительный анализ современных инструментов тестирования на проникновение

Инструмент	**Основное назначение**	**Этап тестирования**	**Поддержка ИИ**	**Преимущества**
Nmap	Сетевое сканирование и разведка	Сбор информации	Нет	Быстрое обнаружение узлов, портов и сервисов
Metasploit	Эксплуатация уязвимостей	Эксплуатация, Post-Exploitation	Частично	Большая база эксплойтов и модулей
SQLmap	Выявление SQL Injection	Анализ веб-приложений	Нет	Полная автоматизация проверки SQL-инъекций
Burp Suite	Анализ безопасности веб-приложений	Тестирование веб-приложений	Частично	Гибкое ручное и автоматизированное тестирование
Intruder	Мониторинг уязвимостей	Непрерывный контроль	Нет	Более 140 000 автоматизированных проверок
Acunetix	Сканирование веб-приложений	Анализ веб-безопасности	Нет	Поддержка DAST и IAST
Qualys	Управление уязвимостями	Мониторинг и аудит	Нет	Централизованное управление безопасностью
PlexTrac	Управление результатами тестирования	Отчётность и анализ рисков	Да	Автоматизация отчётов и управления уязвимостями

Инструмент	Основное назначение	Этап тестирования	Поддержка ИИ	Преимущества
PentestGPT	Интеллектуальная поддержка пентеста	Анализ и планирование атак	Да	Использование LLM для рекомендаций
Nuclei	Автоматизированный поиск уязвимостей	Сканирование и анализ	Да	Высокая скорость и генерация шаблонов
Pentera	Automated Security Validation	Полный цикл тестирования	Да	Моделирование реальных цепочек атак

Заключение

Автоматизированные инструменты тестирования на проникновение играют важную роль в подготовке специалистов по кибербезопасности, обеспечивая формирование практических навыков выявления и анализа уязвимостей информационных систем. Проведённый анализ показал, что такие инструменты, как Nmap, Metasploit, SQLmap, Burp Suite, Qualys, Acunetix, PentestGPT, Nuclei и Pentera, позволяют эффективно автоматизировать различные этапы оценки безопасности, начиная от сбора информации и заканчивая моделированием сложных сценариев кибератак.

Особый интерес представляют современные решения на основе искусственного интеллекта, которые повышают скорость анализа, улучшают качество принимаемых решений и позволяют выявлять сложные цепочки атак. Использование данных инструментов в образовательном процессе способствует развитию практических компетенций студентов и повышению качества подготовки кадров в области информационной безопасности.

Таким образом, внедрение современных автоматизированных средств тестирования на проникновение является важным направлением совершенствования подготовки специалистов по кибербезопасности и повышения эффективности противодействия современным киберугрозам.

Список литературы:

1. Weidman G. Penetration Testing: A Hands-On Introduction to Hacking. San Francisco: No Starch Press, 2023.
2. Allen J., Williams J. Automated Penetration Testing Techniques for Modern Cybersecurity Education // IEEE Access. 2024.
3. Kennedy D., O'Gorman J., Kearns D., Aharoni M. Metasploit: The Penetration Tester's Guide. No Starch Press, 2023.
4. Burp Suite Professional Documentation. PortSwigger Ltd., 2025.

5. Acunetix Web Vulnerability Scanner Documentation. Invicti Security, 2025.
6. Qualys. Vulnerability Management and Detection Response User Guide. 2025.
7. Deng G., Liu Y., Mayoral-Vilches V., Wang X. PentestGPT: An LLM-Empowered Automatic Penetration Testing Tool // USENIX Security Symposium. 2024.
8. Project Discovery. Nuclei Documentation and Security Templates. 2025.
9. Pentera. Automated Security Validation Platform Documentation. 2025.