Нижлукченко И.Д. Этичный хакинг и тестирование на проникновение: защита через наступление. введение в концепции этичного хакинга, роли и методики тестирования на проникновение для улучшения безопасности систем// Международный журнал информационных технологий и энергоэффективности.– 2024. –
Т. 9 № 5(43) с. 109–114

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ЭТИЧНЫЙ ХАКИНГ И ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ: ЗАЩИТА ЧЕРЕЗ НАСТУПЛЕНИЕ. ВВЕДЕНИЕ В КОНЦЕПЦИИ ЭТИЧНОГО ХАКИНГА, РОЛИ И МЕТОДИКИ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ ДЛЯ УЛУЧШЕНИЯ БЕЗОПАСНОСТИ СИСТЕМ

Нижлукченко И.Д.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: nizhluchenk@gmail.com

В статье "Этичный хакинг и тестирование на проникновение: защита через наступление" освещаются ключевые концепции и методологии, лежащие в основе этичного хакинга и тестирования на проникновение, как средств обеспечения кибербезопасности. В контексте постоянно растущего числа киберугроз, авторы рассматривают эти практики как необходимые инструменты для защиты информационных систем и сетей путем активного выявления и устранения уязвимостей. Статья начинается с обзора современного ландшафта киберугроз, подчеркивая важность превентивных мер безопасности. Далее, внимание уделяется философии и методологии этичного хакинга, представляющего собой легитимное исследование систем на наличие уязвимостей с целью их последующего укрепления. Разъясняется, как этичный хакинг отличается от нелегитимного проникновения и каковы его цели и принципы.

Ключевые слова: Этичный хакинг, тестирование на проникновение, кибербезопасность, уязвимости информационных систем, стратегии обеспечения безопасности, методики киберзащиты, этические и юридические аспекты в кибербезопасности, превентивные меры безопасности, защита информационных сетей, управление киберугрозами.

ETHICAL HACKING AND PENETRATION TESTING: PROTECTION THROUGH OFFENSIVE. AN INTRODUCTION TO THE CONCEPTS OF ETHICAL HACKING, THE ROLE AND METHODS OF PENETRATION TESTING TO IMPROVE SYSTEM SECURITY

Nizhlukchenko I.D.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: nizhluchenk@gmail.com

The article "Ethical Hacking and Penetration Testing: Protection through Offensive" highlights the key concepts and methodologies underlying ethical hacking and penetration testing as a means of ensuring cybersecurity. In the context of an ever-growing number of cyber threats, the authors consider these practices as necessary tools to protect information systems and networks by actively identifying and eliminating vulnerabilities. The article begins with an overview of the modern cyber threat landscape, emphasizing the importance of preventive security

measures. Further, attention is paid to the philosophy and methodology of ethical hacking, which is a legitimate study of systems for vulnerabilities in order to strengthen them later. It explains how ethical hacking differs from illegitimate penetration and what its goals and principles are.

Keywords: Ethical hacking, penetration testing, cybersecurity, information system vulnerabilities, security strategies, cyber defense techniques, ethical and legal aspects in cybersecurity, preventive security measures, protection of information networks, cyber threat management.

В эпоху глобализированных информационных технологий и всесторонней цифровизации общества, вопросы кибербезопасности выходят на первый план. С каждым днем растет число кибератак, угрожающих личным данным пользователей, корпоративной информации и даже критически важной инфраструктуре государств. В этой связи, особую важность приобретают методики превентивного обеспечения безопасности, среди которых выделяется этичный хакинг и тестирование на проникновение. Данные подходы, ориентированные на идентификацию и устранение уязвимостей в информационных системах, представляют собой фундаментальный инструментарий в арсенале современного специалиста по кибербезопасности.

Этичный хакинг, или так называемое "белое" взломание, представляет собой практику использования методов и техник взлома для анализа безопасности информационных систем с целью их укрепления. Отличительной чертой этичного хакинга является его легитимность: действия проводятся с разрешения владельцев систем и направлены на повышение их защищенности. Ключевыми принципами этичного хакинга являются целостность, конфиденциальность и доступность информации. Специалисты в данной области обладают глубокими знаниями в области IT и кибербезопасности, а также высокой степенью этической ответственности.

Этичный хакинг является уникальным и мощным инструментом в арсенале современной кибербезопасности, воплощающим в себе комплекс философских принципов и методологических подходов. Эта практика, ориентированная на использование методов и техник взлома для идентификации и устранения уязвимостей в информационных системах, отличается от прочих подходов своей фундаментальной целью – укреплением защищенности систем.[5] Основываясь на принципах целостности, конфиденциальности и доступности информации, этичный хакинг стремится не просто выявить слабые места, но и предложить решения для их устранения, тем самым повышая уровень безопасности.

Философия этичного хакинга уходит корнями в понимание того, что для эффективной защиты системы необходимо способность мыслить как потенциальный атакующий. Это предполагает не только глубокие технические знания и навыки в области информационных технологий и кибербезопасности, но и высокую степень этической осведомленности и ответственности. Этичный хакер должен действовать с разрешения владельца системы, следуя законам и нормам, и при этом направлять свои усилия на выявление уязвимостей, которые могут быть использованы злоумышленниками.

Методология этичного хакинга включает в себя не просто применение инструментов и техник взлома, но и разработку комплексных стратегий защиты, адаптированных под конкретные условия и потребности организации. Это означает адаптацию подходов к безопасности, чтобы обеспечить защиту не только на уровне технологий, но и на уровне процессов и людей. Использование симуляций атак, анализ уязвимостей и разработка

рекомендаций по устранению обнаруженных слабостей – все это входит в компетенцию этичного хакера.

Таким образом, этичный хакинг представляет собой сложное сочетание технической экспертизы, этических принципов и стратегического планирования. Этот подход не только способствует повышению безопасности информационных систем, но и способствует формированию более широкого понимания ценности и важности информационной безопасности в современном мире.

Тестирование на проникновение, или пенетрационное тестирование, представляет собой метод оценки безопасности компьютерной системы или сети путем моделирования атаки со стороны потенциального злоумышленника.[1] Этот метод включает в себя идентификацию доступных систем, исследование возможных точек входа, попытку проникновения и анализ полученных результатов для выявления уязвимостей. Тестирование на проникновение может быть проведено с различными уровнями знаний о системе: от полного незнания до полного понимания внутренней структуры тестируемой системы. Этот процесс не только выявляет слабые места, но и помогает в разработке рекомендаций по усилению защиты.

Тестирование на проникновение является одним из ключевых элементов стратегии обеспечения кибербезопасности, представляя собой комплексный и многоуровневый подход к выявлению уязвимостей в информационных системах и сетях. Этот процесс эмулирует действия потенциального атакующего с целью обнаружения и последующего устранения уязвимостей, которые могут быть использованы для незаконного проникновения или нанесения вреда системе. Суть тестирования на проникновение заключается не просто в поиске слабых мест, но и в понимании того, как эти слабые места могут быть использованы в реальных атаках, а также в разработке мер по их нейтрализации.

Основная стратегия тестирования на проникновение предполагает целенаправленное и планомерное исследование информационной системы с использованием различных методов и техник, варьируя от автоматизированного сканирования до ручного тестирования и анализа. Этот процесс требует от исполнителей не только глубоких технических знаний и практических навыков, но и креативного подхода к решению задач, поскольку каждая система уникальна и может требовать индивидуального подхода к тестированию.

Тактика тестирования на проникновение включает в себя подготовительный этап, на котором определяются цели тестирования, выбираются методы и инструменты, а также устанавливаются рамки допустимых действий во избежание непреднамеренного вреда тестируемым системам. Затем следует этап активного сканирования и идентификации потенциальных точек входа, который позволяет составить карту уязвимостей. После этого осуществляется непосредственное тестирование на проникновение с целью эксплуатации найденных уязвимостей, что дает представление о реальных рисках безопасности. Финальный этап предполагает анализ полученных данных, подготовку отчета с детальным описанием обнаруженных проблем и рекомендаций по их устранению.[3]

Тестирование на проникновение не является однократной акцией, а представляет собой часть непрерывного процесса управления кибербезопасностью, требующего регулярного повторения для эффективной защиты от новых и эволюционирующих угроз. Это стратегический инструмент, который позволяет организациям не только обнаруживать и

устранять существующие уязвимости, но и формировать устойчивую культуру безопасности, адаптируемую к постоянно меняющемуся ландшафту угроз.

В процессе этичного хакинга и тестирования на проникновение задействованы различные специалисты, каждый из которых играет уникальную роль в обеспечении кибербезопасности информационных систем. Эти профессионалы, работая как единая команда, применяют широкий спектр методик и стратегий для выявления и устранения уязвимостей, что требует от них не только глубоких технических знаний, но и понимания целей и бизнес-процессов организации.

Среди ключевых участников процесса этичного хакинга и тестирования на проникновение выделяются аудиторы безопасности, которые отвечают за оценку соответствия системы стандартам и требованиям кибербезопасности, и специалисты по кибербезопасности, которые непосредственно занимаются идентификацией уязвимостей и разработкой рекомендаций по их устранению.[4] Кроме того, в этот процесс могут быть вовлечены системные администраторы и разработчики, которые обеспечивают техническую поддержку тестирования и реализацию предложенных улучшений безопасности.

Методики, используемые в ходе этих действий, варьируются от автоматизированного сканирования систем на предмет известных уязвимостей до ручных тестов и анализа для выявления неочевидных слабых мест. Особое внимание уделяется анализу данных, получаемых в ходе тестирования, что требует от специалистов не только технических знаний, но и аналитических навыков для правильной интерпретации результатов.

Применяемые методики направлены на всестороннее исследование системы, начиная от внешнего периметра и заканчивая внутренними компонентами, что позволяет обеспечить комплексную защиту. Важной частью работы является и разработка стратегий по обеспечению безопасности, включающих в себя как немедленные меры по устранению обнаруженных уязвимостей, так и долгосрочные планы по повышению уровня безопасности системы в целом.

Эта командная и мультидисциплинарная работа требует от всех участников не только высокой квалификации и профессионализма, но и способности к творческому подходу в решении задач кибербезопасности. Использование разнообразных методик позволяет подходить к вопросам безопасности комплексно, что в свою очередь способствует созданию более защищенной и устойчивой к атакам информационной среды.

Этические и юридические аспекты этичного хакинга и тестирования на проникновение играют критически важную роль в обеспечении, чтобы эти практики проводились ответственно и в соответствии с законодательством. Основываясь на принципе, что цель этих действий заключается в улучшении безопасности, а не в нарушении конфиденциальности или целостности данных, профессионалы в этой области должны строго следовать как этическим, так и юридическим стандартам.

Важным этическим принципом в этих областях является получение явного разрешения от владельцев или управляющих системами перед проведением любых тестов на проникновение или хакинга.[3] Это гарантирует, что все действия выполняются в рамках согласованных условий и не превышают предоставленные полномочия. Более того, специалисты обязаны сохранять конфиденциальность всей полученной в ходе тестирования

информации, а также действовать с целью минимизации любого возможного вреда для тестируемой системы.

С юридической точки зрения, действия, связанные с этичным хакингом и тестированием на проникновение, могут натолкнуться на различные законодательные ограничения, связанные с несанкционированным доступом к компьютерным системам, злоупотреблением владельческими данными и другими аспектами кибербезопасности. В разных юрисдикциях существуют различные нормы и законы, регулирующие эти вопросы, и профессионалы должны обладать знаниями актуальных законодательных требований и следовать им для избежания юридических последствий.

Кроме того, этичный хакинг и тестирование на проникновение требуют четкого определения рамок и целей тестирования, чтобы убедиться, что все действия направлены на достижение конструктивных результатов в области безопасности. Это включает в себя документирование всех шагов и процедур, а также разработку и внедрение мер по устранению выявленных уязвимостей.

Таким образом, соблюдение этических и юридических норм не только обеспечивает легитимность и ответственность процесса этичного хакинга и тестирования на проникновение, но и поддерживает доверие между всеми заинтересованными сторонами, включая компании, их клиентов и общественность в целом. Это создает основу для ответственного и эффективного применения этих практик в рамках общей стратегии кибербезопасности.

Этичный хакинг и тестирование на проникновение являются неотъемлемой частью стратегии обеспечения кибербезопасности в современном мире. Они позволяют не просто реагировать на угрозы, но и активно предотвращать их, используя методы и техники, аналогичные тем, что применяют злоумышленники. Таким образом, "защита через наступление" обеспечивает глубокое понимание угроз и разработку эффективных мер по защите информационных систем от возможных атак. Важно, что все действия в рамках этичного хакинга и тестирования на проникновение проводятся с соблюдением высоких этических норм и юридических требований, что делает эти практики не только эффективными, но и легитимными инструментами защиты киберпространства.

Список литературы

1. Гельфанд А. М. и др. Разработка модели распространения самомодифицирующегося кода в защищаемой информационной системе //Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2018. – №. 8. – С. 91-97.
2. Красов А. В. и др. Способы коммутации пакетов в сетях CISCO //Материалы Всероссийской научно-практической конференции" Национальная безопасность России: актуальные аспекты" ГНИИ" Нацразвитие". Июль 2018. – 2018. – С. 31-35.
3. Штеренберг С. И., Москальчук А. И., Красов А. В. Разработка сценариев безопасности для создания уязвимых виртуальных машин и изучения методов тестирования на проникновения–Информационные технологии и телекоммуникации, 2021 //Т. – 2021. – Т. 9. –С. 1-2

4. Катасонов А. И., Штеренберг С. И., Цветков А. Ю. Оценка стойкости механизма, реализующего... Мандатную сущностно-ролевую модель разграничения прав доступа в операционных системах семейства gnu linux //Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2020. – №. 2. – С. 50-56.
5. Бударный Г. С. и др. Разновидности нарушений безопасности и типовые атаки на операционную систему //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2022). – 2022. – С. 406-411

References

1. Gelfand A.M. et al. Development of a model for the distribution of self-modifying code in a protected information system //Modern science: actual problems of theory and practice. Series: Natural and Technical Sciences. – 2018. – No. 8. – pp. 91-97.
2. Krasov A.V. et al. Packet switching methods in CISCO networks //Materials of the All-Russian scientific and practical conference "National Security of Russia: current aspects of the "GNII" National Development". July 2018. – 2018. – pp. 31-35.
3. Shterenberg S. I., Moskalchuk A. I., Krasov A.V. Development of security scenarios for creating vulnerable virtual machines and studying penetration testing methods–Information technologies and Telecommunications, 2021 //Vol. – 2021. – vol. 9. –pp. 1-2
4. Katasonov A. I., Shterenberg S. I., Tsvetkov A. Yu. Assessment of the stability of the mechanism implementing... The mandatory essential role model of access rights differentiation in gnu linux operating systems //Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences. – 2020. – No. 2. – pp. 50-56.
5. Budarny G. S. et al. Types of security breaches and typical attacks on the operating system //Actual problems of infotelecommunications in science and education (APINO 2022). – 2022. – pp. 406-411.