КИБЕРБЕЗОПАСНОСТЬ В ОБРАЗОВАНИИ: АТАКА ЗАЩИТА И АНАЛИЗ ИНФОРМАЦИИ ИЗ КОМАНДНОЙ СТРОКИ LINUX В ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЯХ

Чугаев М.А., Гусаков П.Б.

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь, Timon02maks@mail.ru

Abstract. Bash and Cybersecurity: attack, protection and analysis from the Linux command line.

Современное образование играет огромную роль в подготовке обучающих к требованиям современного рынка труда. Однако, в контексте использования Bash и кибербезопасности существуют определенные проблемы, которые влияют на качество образовательного процесса [1]:

1. Одной из основных проблем является недостаток преподавателей, обладающих необходимыми знаниями и опытом в области Bash и кибербезопасности. Сфера кибербезопасности является быстро развивающейся и требует постоянного обновления знаний. Многие учебные заведения не всегда могут привлечь преподавателей, которые обладают актуальной экспертизой. Решение этой проблемы состоит в организации программ повышения квалификации для преподавателей, проведении специализированных курсов и семинаров, а также привлечении практикующих специалистов из индустрии для проведения лекций и мастер-классов. Такие меры помогут обеспечить наличие квалифицированных преподавателей, способных передать актуальные знания обучающим.

2. Устаревшие учебные программы является проблемой в области кибербезопасности и использования Bash. Быстрое развитие технологий требует обновления программ обучения, чтобы они отражали последние тенденции и вызовы в сфере кибербезопасности. Для решения этой проблемы необходимо пересматривать и обновлять учебные программы с учетом современных вызовов в области кибербезопасности, а также включать практические задания, реальные сценарии и проекты, которые помогут обучающим применить свои знания на практике. Такое обновление учебных программ поможет обучающим получить актуальные знания и навыки, необходимые для работы в сфере кибербезопасности.

3. Недостаток практических занятий и реальных сценариев. Одной из ключевых составляющих обучения кибербезопасности и использованию Bash является практическая работа. Однако, многие образовательные программы не предоставляют достаточное количество практических занятий и реальных сценариев. Это может ограничить обучающих получить практический опыт и применить свои знания на практике. Решение этой проблемы состоит в интеграции практических лабораторных занятий, симуляционных тренировок и проектных заданий в учебные программы. Такие задания должны быть основаны на реальных сценариях атак, защиты и анализа из командной строки LINUX.

4. Отсутствие доступа к современным инструментам и ресурсам. Сфера кибербезопасности и использование Bash требуют доступа к современным инструментам и ресурсам. Для решения этой проблемы необходимо обеспечить доступ к современным программным средствам, симуляторам и оборудованию, которые позволят обучающим проводить анализ, тестирование и защиту систем из командной строки LINUX. Кроме того, обучающим также необходимо предоставить доступ к актуальным источникам информации, например, электронным журналам, онлайн-курсам и специализированным форумам, чтобы они могли быть в курсе последних тенденций и разработок в области кибербезопасности. Использование методов защиты и анализа из командной строки Linux может значительно повысить качество образовательного процесса в области кибербезопасности и использования Bash. Методы, которые могут быть применены:

1. Использование мощных инструментов командной строки: Командная строка Linux предоставляет широкий спектр инструментов для анализа и защиты системы.

2. Скриптинг на Bash: Bash является мощным языком сценариев, который позволяет автоматизировать множество задач в Linux.

3. Анализ лог-файлов: лог-файлы содержат ценную информацию о действиях и событиях в системе, которые могут использоваться для обнаружения атак и аномалий.

4. Тестирование на проникновение: Обучающие могут использовать инструменты командной строки Linux для проведения тестирования на проникновение и оценки уровня защищенности системы.

5. Мониторинг безопасности: мониторинг системы, обнаружения подозрительной активности, анализа угроз и принятия соответствующих мер по обеспечению безопасности.

Объединение всех этих методов и подходов позволит значительно повысить качество образовательного процесса в области использования Bash, кибербезопасности, атак и анализа из командной строки Linux. Обчающие получат не только теоретические знания, но и ценные практические навыки, которые помогут им успешно применять эти методы в реальных ситуациях.

Литература

1. Bash и кибербезопасность: атака, защита и анализ из командной строки Linux [2020] Олбинг Карл, Тронкон Пол.