УДК 004.56

МЕТОДОЛОГИЯ СОЗДАНИЯ ВИРТУАЛЬНОЙ ЛАБОРАТОРИИ ДЛЯ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ

Москальчук А.И., СПбГУТ им. проф. М. А. Бонч-Бруевича
Научный руководитель – К.т.н, ассистент Штеренберг С.И.
СПбГУТ им. проф. М. А. Бонч-Бруевича

В статье рассматривается создание виртуальной лаборатории для тестирования на проникновение в домашних условиях. Данная лаборатория обладает всем необходимым функционалом, благодаря которому специалист в области информационной безопасности может оттачивать свои навыки и реализовывать новые методы, не нарушая при этом закон и безопасность реальных информационных систем. Целью является создание такой среды, в которой возможно понимать действия злоумышленника и анализировать природу «конкретных» уязвимостей.

Поскольку кибернетическая среда продолжает активно развиваться, и нарушения становятся более распространенным явлением, все больше внимания уделяется защите информационных активов. Одним из способов обеспечения информационной безопасности является тестирование на проникновение (пентест) – метод оценки безопасности путем моделирования атаки злоумышленника, благодаря которому организация может выявить уязвимости в системе безопасности и принять соответствующие меры.

Когда идет речь об обучении тестированию на проникновение, необходима среда, в которой можно практиковаться, не нарушая закон и целостность компьютерных сетей или систем. Именно для этих целей и создается лаборатории для тестирования. Пентест лаборатория - это небольшая локальная сеть, специально созданная для реализации всех возможных атак, которые можно выполнять в реальном мире. Кроме того, если говорить о виртуальной среде, то можно тщательно отслеживать поведение каждой системы во время атаки, что дает дополнительное представление о том, что и как ставит под угрозу безопасность системы.

Целью данной работы является: создание виртуальной пентест лаборатории с использованием VirtualBox Kali Linux, Ubuntu и Metasploitable 2 и демонстрация работоспособности на конкретных примерах.

Основными преимуществами созданной лаборатории являются быстрота, доступность и легкость развертывания, по сравнению с более сложными лабораториями, для функционирования которых необходимо более одного ПК. Также, немаловажным фактором является то, что она позволяет наглядно демонстрировать, из-за чего возникают уязвимости в информационных системах, что дает практическое понимание того, как комплексно обеспечивать защиту от них. Помимо этого, созданная лаборатория является экономной для системы и поддерживает стабильную работу на среднем по мощности ПК, так как основными компонентами являются Unix-подобные операционные системы на базе ядра Linux, которые обладают небольшими системными требованиями наряду с другими операционными системами. Это позволяет разворачивать данную лабораторию на ноутбуках или в компьютерных классах для использования в обучающих целях. Также, на базе ядра Linux находится подавляющее число серверной части систем, что делает данную лабораторию актуальной.

Результатом данной работы является пошаговый алгоритм создания виртуальной пентест-лаборатории. В качестве примера эксплуатации лаборатории был продемонстрирован алгоритм тестирования на проникновение при помощи уязвимой машины Metasploitable 2 и произведён экспериментальный взлом уязвимой версии Drupal. Созданная лаборатория является универсальной и может быть использована для

моделирования собственных сценариев взлома и, в частности, для тестирования конкретных систем или приложений в условиях изолированной среды.

Москальчук А.И. (автор)
Штеренберг С.И. (научный руководитель)