И.Р. Зулькарнеев, А.С. Новожилов

Тюменский государственный университет, г. Тюмень

УДК 004.056

КОНЦЕПЦИЯ ТРЕНИРОВОЧНОЙ ПЛОЩАДКИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация. В статье описывает подход к созданию тренировочной площадки с заданиями по информационной безопасности в формате task-based CTF. Показана необходимость такой площадки и пути ее развития и применения. Предложена модель технической реализации.

Ключевые слова: CTF, обучение, пентестирование, информационная безопасность, подготовка специалистов, тренировочная площадка

Одним из недостатков современной учебной программы по компьютерной безопасности является отсутствие предоставления учащимся возможности приобретения практических навыков поиска уязвимостей и проактивного анализа информационных систем в условиях, приближенных к реальным. Разработка специальной площадки, в основе которой лежат соревнования по информационной безопасности Capture the flag (CTF) для студентов и школьников с доступом к обучающему материалу, совмещенному с заданиями в формате task-based или pentest должна решить данную проблему. Как показали исследования, задания такого рода с возможностью моделирования кибератак в условиях, максимально приближенных к реальным, повышают интерес студентов к кибербезопасности [1,2]. Несмотря на то, что соревнования по кибербезопасности представляют интерес для студентов, эффективность данного подхода при подготовке профессионалов высокого уровня ограничена. Одна из причин заключается в том, что необходимость обладать достаточным уровнем подготовки и знаний, зачастую оказывается барьером для участия в этих соревнованиях.

Ценность приближенных к реальности заданий соревнований CTF для подготовки специалистов по информационной безопасности является неоспоримой. Однако непосредственно сами соревнования CTF предоставляют очень мало возможностей для обучения. Гораздо важнее то, что вокруг соревнований можно организовать мастер-классы, проводить специализированные лекционные занятия и рассматривать некоторые сложные для самостоятельного понимания и освоения моменты [3,4]. Большинство функционирующих в настоящее время открытых площадок подобного рода разбиты на 2 категории: предоставляющие задания в формате task-based, требующие поиска и сдачи флага, и сервисы, предоставляющие образы виртуальных машин для самостоятельного развертывания и поиска уязвимостей, повышения прав доступа и пр.

Тест на проникновение (далее – пентест) — это процесс тестирования, в ходе которого специалист по защите информации может практическим путем проверить защищенность той или иной информационной системы от посягательств на ее конфиденциальные данные и других угроз для информации. За рубежом также часто встречается термин этический хакинг. Построение нашей системы планируется таким образом, что на начальном этапе будет возможность прохождения и добавления заданий в формате task-based, в будущем же планируется расширение с предоставлением возможностей по полноценному пентестированию. Именно поэтому особенно важно учесть архитектурные особенности на этапе проектирования.

Знание векторов атак даст возможность подготовиться к ним и снизить негативные последствия. В современных условиях будущий специалист по информационной безопасности, обладающий практическими навыками пентестирования будет более востребован на рынке труда.

Для достижения поставленных целей будет разработана обучающая площадка на базе Тюменского государственного университета для приобретения практических навыков анализа, выявления и тестирования известных уязвимостей. Для студентов будет реализован личный кабинет, с

помощью которого студент сможет просматривать назначенные ему задачи, отслеживать свой прогресс, потраченное и оставшееся время, а также обмениваться личными сообщениями с преподавателем. В результате окончательного внедрения площадки, учащимся высших учебных заведений будет предоставлена возможность регистрации для доступа к заданиям. В качестве испытаний студенту будут предложены задания в формате task-based, разбитые на категории:

- Osint — поиск и анализ информации на основе данных из открытых источников;
- Reverse — исследование программ без исходного кода, декомпиляция, реверс-инжиниринг;
- Stegano — стеганография, сокрытие информации;
- PPC — задачи на программирование;
- Crypto — криптография, кодирование и шифрование информации;
- Web — задачи на веб-уязвимости, такие как SQL injection, XSS и другие.

Эти задания позволяют поддерживать в актуальном состоянии знания, получаемые в учебном заведении, и углубленно изучать различные разделы информационной безопасности и информатики. Помимо основного функционала для пользователей, необходимо реализовать администраторский модуль с возможностью добавления, редактирования и управления заданиями и обучающим материалом. Также преподаватели должны иметь возможность объединять студентов в группы, классифицировать созданные задания по категориям, добавлять необходимые файлы, указывать количество баллов за выполнение и устанавливать время начала и окончания доступа к задаче.

В ходе работы над заданиями нет каких-либо ограничений на используемый инструментарий (сканеры, отладчики, специальные пакеты программ и т.п.) и методы. Главной задачей работы площадки является

получение новых, а также закрепление уже имеющихся знаний, умений и навыков.

Результатом выполнения определенного задания формата task-based является найденный флаг — набор символов или произвольная фраза. Каждое задание оценивается различным количеством фиксированных баллов, в зависимости от сложности. Для мониторинга общих результатов будет реализована рейтинговая таблица, отображающая количество баллов, набранных студентом за пройденные им задания.

В настоящее время на кафедре информационной безопасности ведется разработка системы, основной функционал которой направлен на проведение соревнований в формате CTF, ограниченных по времени. В данной системе уже реализованы механизмы по приему флагов, начислению баллов, быстрое реагирование при неполадках, а также возможность обслуживания большого количества одновременных подключений. В отличии от существующей системы, разрабатываемая тренировочная площадка предоставляется не для командных соревнований, а для индивидуального использования, доступ к определенным заданиям может быть ограничен в условиях образовательной программы. В будущем эти две системы будут интегрированы друг с другом.

Для реализации возможности преподавателем устанавливать временные рамки выполнения задания необходим планировщик задач, функционирующий на сервере Cron. Для хранения загружаемых файлов необходимо использовать отдельное файловое хранилище с генерируемыми алиасами и соответствующими записями в базе данных. При загрузке файлов будет учитываться их расширение и максимальный допустимый объем. Предотвращение основных атак на систему будет осуществляться с помощью валидации форм площадки, проверке и фильтрации данных при помощи экранирования символов и др. При развертывании системы планируется использовать два сервера, на одном из которых будет функционировать web-сервер, основная база данных(master) и файловое хранилище. На другом

сервере будет находиться база данных(slave) с возможностью репликации данных БД(master) и резервное файловое хранилище.

Для возможности реализации некоторых типов задач потребуется развертывание отдельных сервисов, которые должны быть изолированы от основной системы и соответствовать возможностям ресурсоемкости. Решением данной задачи выступит средство программной виртуализации – Docker, который прост в эксплуатации и хорошо зарекомендовал себя с точки зрения стабильности. Также необходимо реализовать систему логирования, с помощью которой можно не только вести журнал действий, но и впоследствии анализировать индивидуальные особенности студентов с целью улучшения методов обучения. Отдельное внимание стоит уделить вопросу защиты от возможности сдачи флага путем перебора(bruteforce), а также от DDoS-атак с целью вывода из строя основных компонентов системы.

В данной статье рассмотрена важность и необходимость расширения учебного инструмента при подготовке специалистов в области защиты информации, а также описана предполагаемая архитектура разрабатываемого приложения с учетом возможности дальнейшего масштабирования. В дальнейшем планируется реализация площадки в форме web-приложения и расширение ее функционала до полноценной системы тренировок по пентестированию.

СПИСОК ЛИТЕРАТУРЫ

1. Cheung R., Cohen J., Lo H., Elia F., Carrillo-Marquez V. Effectiveness of Cybersecurity Competitions [Электронный ресурс] // Proceedings of International Conference on Security and Management, Las Vegas, Nevada. 2012 URL: http://josephpcohen.com/papers/seccomp.pdf (дата обращения 14.04.2018).

2. Werther J., Zhivich M., Leek T., Zeldovich N. Experiences in cyber security education: The MIT Lincoln laboratory capture-the-flag exercise. 2011 URL: https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2011_08_08_Werther_CSET_FP.pdf (дата обращения 14.04.2018).

3. Eagle C., Clark J. L. Capture-the-Flag: Learning Computer Security Under Fire. [Электронный ресурс] // Proceedings of the Sixth Workshop on Education in Computer Security (WECS). 2004.
URL: http://calhoun.nps.edu/bitstream/handle/10945/7203/wecs6_ch04.pdf (дата обращения 14.04.2018).

4. Mansurov A., A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia [Электронный ресурс] // Modern Applied Science, vol. 10, no. 11, p. 159, 2016.
URL: http://ccsenet.org/journal/index.php/mas/article/view/60685/33468 (дата обращения 14.04.2018)