УДК 004.056.5

КИБЕРПОЛИГОН КАК СОВРЕМЕННОЕ РЕШЕНИЕ ДЛЯ ОБУЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ И МОДЕЛИРОВАНИЯ АТАК

Волкорезов С.В. (ИГУ), **Королькова М.Д.** (ИГУ), **Чанков Р.А.** (ИГУ)
Научный руководитель –кандидат технических наук, доцент Петрушин И.С.
(ИГУ)

Введение. Киберполигоны позволяют решать ряд задач, связанных с моделированием кибератак и тестированием защитных мер в безопасной среде, которые актуальны в связи с распространением киберинцидентов в коммерческих и государственных инфраструктурах. Данная технология также применяется для обучения специалистов, создавая условия, приближенные к реальной атаке, имитируя продвижение злоумышленников по системе и злонамеренные действия с информацией [1].

Основная часть. Основные этапы создания киберполигона включают проектирование виртуального стенда с взаимодействием машины-жертвы (на базе ОС Windows 10), атакующей машины (на базе ОС Kali Linux) и сервера для сбора системныхлогов. Далее используются специализированные инструменты, такие как Metasploit и Atomic Red Team, для проведения атак и построения их цепочек. Завершающим этапом является настройка и развертывание механизма сбора журналов системы с использованием ELK-стека (Elasticsearch, Winlogbeat, Kibana) для их последующего анализа.

С помощью киберполигона решаются следующие два типа задач:

1) Задачи моделирования кибератак и выявления уязвимостей в системах информационной безопасности. Например, моделирование DDoS-атак на серверную инфраструктуру с целью выявления устойчивости системы к перегрузкам. Также направления включают использование известных уязвимостей в программном обеспечении (таких как EternalBlue) для несанкционированного доступа.
2) Задачи обучения специалистов кибербезопасности при взаимодействии с киберполигоном [2]. В условиях, приближенных к реальным атакам, таким как использование злоумышленниками PowerShell для выполнения вредоносных или подозрительных действий (вызов утилиты mimikatz или манипуляции с учетными данными).

Выводы. Создан учебный киберполигон в виде комлпекса виртуальных машин, позволяющий моделировать реальные кибератаки, анализировать системные журналы и оценивать актуальность мер защиты. Проведенные эксперименты с эмуляцией кибератак подтвердили возможность применения развернутого стенда для практического обучения и исследования киберугроз.

Список использованных источников:

1. Как мы построили виртуальную инфраструктуру для киберучений промышленных предприятий // Ростелеком-Солар : сайт. – URL: https://habr.com/ru/companies/solarsecurity/articles/515626/ (дата обращения: 15.01.2025)
2. Коваленко А.П., Тимаков А.А., Жанкевич А.О., Фадеев М.М. Обучение методам обнаружения компьютерных атак на базе киберполигона кафедры "Информационной безопасности" РТУ (МИРЭА) // Методы и технические средства обеспечения безопасности информации. 2021. № 30. С. 39-44.