ТЕХНИЧЕСКОЕ ОПИСАНИЕ КИБЕРПОЛИГОНА

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Наименование

Полное наименование: «Система моделирования киберугроз и ликвидации компьютерных инцидентов в информационных инфраструктурах «Cyber Range».

Сокращенное наименование: «Киберполигон».

1.2. Назначение

Киберполигон предназначен для тренировок персонала, повышения практических навыков и уровня командного взаимодействия специалистов информационной безопасности по предотвращению компьютерных атак, ликвидации компьютерных инцидентов, а также для тестирования средств защиты информации.

1.3. Основные возможности

Киберполигон представляет собой учебную базу для проведения занятий со специалистами команды Security Operation Center (SOC) и команды Blue Team по предотвращению, обнаружению, реагированию, расследованию и устранению последствий инцидентов.

Программная платформа позволяет моделировать сетевые ИТ инфраструктуры с имитацией ИТ технологий, сервисов и средств защиты информации (СЗИ). Это позволяет анализировать безопасность сети в тестовой среде, не затрагивая «боевой» контур.

Киберполигон обладает атакующим ядром, который позволяет осуществлять атаки в автоматизированном режиме. База сценариев атак может регулярно пополняться.

Киберполигон представляет собой программно-аппаратный комплекс позволяющий:

– имитировать виртуальные сетевые ИТ инфраструктуры с использованием программного конструктура;

– симулировать компьютерные атаки в автоматизированном режиме с помощью программного модуля хакерской активности или в ручном режиме специалистом Red Team путем подключения или web-доступа к атакуемой сетевой инфраструктуре;

– имитировать информационные потоки с помощью программного модуля генерации белого трафика;

– организовывать виртуальные рабочие места руководителей, администратора и специалистов информационной безопасности (команды SOC и команды Blue Team) для отработки практических навыков по обнаружению и реагированию на компьютерные инциденты;

– организовывать и проводить киберучения и тренировки персонала в целях отработки практических навыков защиты информационных инфраструктур от внешнего и внутреннего нарушителей.

2. СОСТАВ КИБЕРПОЛИГОНА

2.1. Состав аппаратной части

Аппаратная часть киберполигона состоит из серверного оборудования, персональных компьютеров (ноутбуков) пользователей, средств отображения и вспомогательного сетевого оборудования. Минимальные требования к оборудованию приведены в Спецификации. При необходимости расширения функциональности киберполигона состав оборудования может увеличиваться кратно.

Указанное оборудование позволяет реализовать базовые виртуальные шаблоны учебных инфраструктур (около 40 хостов) с возможностью обучения группы 10-15 человек.

При необходимости обучения нескольких групп одновременно, состав оборудования потребуется увеличить кратно.

В базовый комплект поставки входят opensource решения для построения шаблонов отраслевых инфраструктур не требующие закупки лицензий.

2.2. Состав программной платформы

Программная платформа содержит серверную часть (ядро платформы), набор программных модулей и клиентскую часть.

Серверная часть (ядро) содержит:

1. Сервер моделирования киберугроз и ликвидации инцидентов безопасности в информационных инфраструктурах «Server Cyber Range».
2. Сервер баз данных «Cyber Range DB».
3. Веб-Сервер «WebServer».

Набор системных программных модулей содержит:

1. Программный генератор сетевого трафика «Network Activity Generator»
2. Программный модуль имитации хакерской активности «Hacker Activity Generator».
3. Программный модуль скоринга и статистики «Scoring And Statistics Software Module».
4. Программный модуль генерации отчетов «Report Generator».

Клиентская часть содержит:

1. Программный модуль АРМ администратора киберполигона «Admin Cyber Range».
2. Программный модуль АРМ инструктора «Instructor Workplace».
3. Программный модуль АРМ специалиста SOC «SOC Specialist Workplace».
4. Программный модуль АРМ специалиста BlueTeam «BlueTeam Specialist Workplace».

Количество клиентских автоматизированных мест определяется исходя из потребностей Заказчика.

Сервер моделирования киберугроз и ликвидации инцидентов безопасности в информационных инфраструктурах «Cyber Range Server» содержит набор шаблонов инфраструктур, сценариев атак и средств обнаружения компьютерных инцидентов. Обеспечивает управление и взаимодействие программных модулей киберполигона.

Сервер баз данных «Cyber Range DB» предназначен для накопления информации о пользователях, хранения статистических данных и отчетов о проведенных киберучениях.

Посредством единого интерфейса Web-Сервера «WebServer» осуществляется взаимодействие с киберполигоном внешних пользователей через web-браузер.

Программный генератор сетевого трафика «Network Activity Generator» осуществляет имитацию по заданным параметрам действий легитимных пользователей внутри учебной ИТ инфраструктуры.

Программный модуль имитации хакерской активности «Hacker Activity Generator» предназначен для симуляции действий атакующего с целью проникновения в ИТ инфраструктуру по выбранным сценариям.

Программный модуль скоринга и статистики «Scoring And Statistics» позволяет обрабатывать данные по проведенным киберучениям, получать статистику по каждому из обучаемых, оценивать рейтинг, сравнивать и оценивать специалистов и отслеживать прогресс обучения.

Программный модуль генерации отчетов «Report Generator» позволяет обработать статистические данные о проводимом обучении и посредством подготовленных шаблонов предоставлять структурированную информацию (отчет) в виде документа.

Программный модуль АРМ администратора киберполигона «Cyber Range Admin» содержит web-интерфейс с набором настроек, позволяющим осуществлять взаимодействие с программной платформой и управление системными свойствами комплекса.

Программный модуль АРМ инструктора «Instructor Workplace» позволяет посредством web-интерфейса управлять киберучением, взаимодействовать с обучаемыми и проводить мониторинг процесса обучения.

Программный модуль АРМ специалиста SOC реализует набор функций, позволяет посредством web-интерфейса выполнять управляющие воздействия на имитируемую сетевую ИТ инфраструктуру, управлять работой средств защиты, сетевой СЗИ, осуществлять мониторинг сетевой активности, имитировать инциденты в информационной безопасности, взаимодействовать с инструктором и с другими участниками тренировки.

Программный модуль АРМ специалиста BlueTeam реализует набор функций, позволяющий посредством web-интерфейса воздействовать на элементы имитируемой ИТ инфраструктуры с целью устранения обнаруженных уязвимостей, взаимодействовать с инструктором и с другими участниками тренировки.

Программное обеспечение киберполигона является российской разработкой, построено на открытом программном обеспечении (open-source software), включает базовые средства защиты информации Security Onion и имеет возможности подключения проприетарных решений заказчика типа WAF, FW, Antivirus, IDS/IPS, SIEM.

2.3. Используемые технологии

В программном обеспечении киберполигона используются следующие технологии (языки программирования и фреймворки):

Backend: Django (Python), PostgreSQL.

Frontend: Vue.js.

Атакующий модуль: Python, PowerShell, Bash, Ruby.

Виртуализация: Proxmox.

Основным преимуществом используемых технологий является использование программного с открытым кодом (opensource).

3. АРХИТЕКТУРА КИБЕРПОЛИГОНА

Базовая модель киберполигона схематически представлена на рис. 1.

Архитектурно программная платформа построена на основе технологии виртуализации типа Proxmox VE (KVM, LXC).

Реализован единый интерфейс управления платформой.

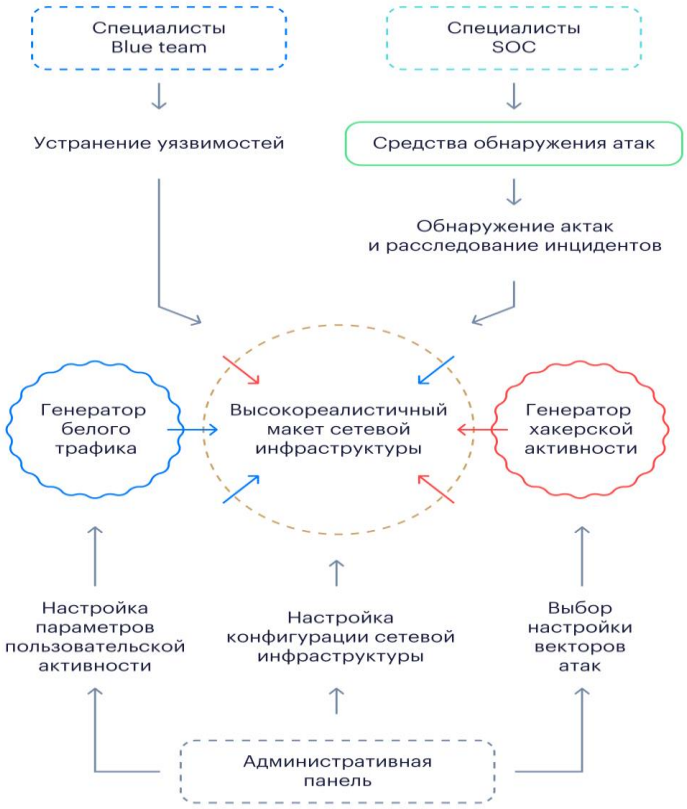

Рис.1. Базовая модель киберполигона

Базовая модель развертывается с помощью следующих продуктов:

Серверная часть (Backend) построена на Python, фреймворк – на Django, база данных типа PostgreSQL

Клиентская часть (Frontend) содержит фреймворки типа vue.js, vuetify, nuxt.js.

Обработчик событий построен на основе базы данных TinyDB и набора скриптов.

Атакующий модуль содержит набор скриптов на PowerShell, Ruby, Python, Bash.

Интерфейс администратора осуществляет запуск, scoreboard, управление учетными записями.

Интерфейс инструктора (преподавателя) содержит: индикатор прохождения киберучений (Progress bar), чат с участниками, планирование и запуск киберучений, табло с результатами (scoreboard), управление учетными записями на уровне групп.

Интерфейс специалиста (обучаемого) включает: карту сети, доступ к средствам защиты информации (СЗИ) и серверам, чат, ведение карточек обнаруженных и устраненных уязвимостей, приборная панель с вспомогательными элементами (Dashboard).

Сценарии реализации программной платформы могут включать:

- базовые шаблоны сценариев;
- сети SCADA;
- WMI (внутренний злоумышленник);
- EIS Takeover – Advanced (внутренний злоумышленник);
- Social Engineering (внешний злоумышленник);
- No 0day (внешний злоумышленник);
- Data Compressed Exfiltration (внутренний злоумышленник: сотрудник);

- Remote File Copy (внешний злоумышленник);
- Server Corruption (внешний злоумышленник).

Программная платформа реализует модульность сценариев и возможность кастомизации сценариев.

4. ФУНКЦИИ ПО МОДЕЛИРОВАНИЮ ИНФРАСТРУКТУР И АТАК

4.1. Компоненты моделирования сетевой инфраструктуры

Моделирование сетевых ИТ инфраструктур осуществляется с использованием платформы виртуализации Proxmox, содержащей гипервизоры типа KVM и LXC.

Платформа виртуализации Proxmox поддерживает операционные системы Linux, *BSD и другие, с минимальными потерями производительности. Операционная система Linux поддерживается без потери производительности.

Платформа виртуализации Proxmox способна моделировать поддерживаемые KVM операционные системы. Практически может моделировать широкий спектр оборудования и систем, используемых в современных ИТ инфраструктурах.

Базовая поставка включает 3 шаблона сети, до 40 хостов в каждом шаблоне.

Количество и состав моделируемых систем и оборудования Заказчика сверх базовой поставки согласовывается с Заказчиком.

Максимальное количество моделируемого оборудования определяется возможностями серверного оборудования.

Добавление сети может осуществляться как в виде VLAN, так и путем физического подключения.

SCADA-сеть представлена комбинацией программно-определяемых сетей и эмуляцией сетевого оборудования для проведения атак.

Инструменты моделирования сетевой ИТ инфраструктуры позволяют осуществлять:

- настройку сети под требования обучения;
- имитирование до 6 подсетей, разделенных на уровне L2\L3 модели OSI;
- добавление и/или исключение ИТ-компонентов;
- добавление и/или исключение средств защиты информации.

4.2. Генерация сетевого трафика и компоненты сетевых атак

Комплект базовой поставки включает 9 сценариев атак по 3 сценария на каждый шаблон имитируемой сети.

Генерация сетевого трафика осуществляется генератором (на уровнях L2-L7 модели OSI) в виде скриптов на рабочих станциях. Генератор позволяет получить web-трафик, почтовый трафик; трафик технологической сети, трафик вредоносной активности; трафик Интернета вещей; трафик взаимодействия с сетевыми хранилищами, подключением по RDP, обращением к DC и т.п.

Имеется возможность комбинирования нескольких видов трафика вручную, включая проигрывание собственного трафика или направление копии реального трафика корпоративной или технологической сети.

4.3. Компоненты сетевых атак и защиты

Обучаемые участвуют в процессе обучения посредством подключения к внутренней рабочей станции киберполигона через web-интерфейс по протоколу http.

Возможно физическое подключение к внутренней сети и/или подключение посредством VPN.

Позиции в команде защиты сети разделяются на команду SOC и команду Blue Team. Внутри каждой команды возможно произвольное распределение ролей участников по решению инструктора-руководителя.

Обучение по защите от атак включает практическую отработку следующих типовых задач:

- обнаружение аномалий в сетевом трафике;
- распространенные техники эксплуатации уязвимостей;
- журналирование, обработка журналов логирования;
- анализ SMTP, DNS, HTTP(S);
- анализ процессов на рабочих станциях и серверах;
- отработка взаимодействия команды реагирования и SOC.

В базовой поставке для команды защиты предусмотрено использование средств защиты компьютерных сетей типа SIEM, Firewall, Antivirus software, Security Onion.

Возможно подключение иных проприетарных средств защиты.

4.4. Участие атакующей команды

Атакующие участвуют в процессе обучения посредством подключения к внутренней рабочей станции киберполигона через web-интерфейс по протоколу http.

Возможно физическое подключение к внутренней сети и/или подключение посредством VPN.

Распределение позиций в команде сетевых атак определяет инструктор – руководитель на этапе планирования обучения.

Возможно назначение типовых позиций (ролей): reverse, pwn, web и т.п.

Команда сетевых атакующих может использовать инструменты из дистрибутива Kali Linux, а также иные инструменты.

Сценарии атак также реализованы в виде скриптов.

Киберполигон позволяет моделировать многовекторные сценарии атак. Набор векторов атак в каждом сценарии может быть разнообразным и формироваться из перечня: Web, binary exploitation, password attacks, bruteforcing, DoS/DDoS, exfiltration, lateral movement, client side attacks и др.

При выборе векторов атаки учитываются актуальные угрозы.

4.5. Компоненты поддержки обучения

Инструктор отслеживают процесс обучения посредством web-интерфейса, через панель управления обучением.

После каждого обучения оформляется отчет с отражением общих и индивидуальных результатов обучаемых.

Команды и обучающиеся оцениваются в зависимости от степени достижения поставленных целей и выполнения отдельных задач.

Итоговая оценка складывается из частных оценок по количеству правильно обнаруженных и оформленных инцидентов, по количество корректно устраненных уязвимостей, по время реакции и др.

Процесс обучения осуществляется через web-интерфейс. Сценарии атак реализованы виде скриптов на языке Python с возможностью клонирования и модификации.

Управление тренировкой (киберучением) включает:

- автоматизированное добавление обучающихся;
- режим самостоятельного обучения (без инструктора);
- обучение команд Red Team против Blue Team;
- обучение команд в режиме Team против Blue Team;
- ведение записи процесса обучения;
- параллельное обучение нескольких классов;
- интерфейса системы обучения (RU\ENG\VET);
- формирование отчетов и описаний задач и сценариев;
- web-подключение обучающихся к платформе киберполигона;
- инструменты оценки результатов в ручном и автоматическом режиме.

Предусмотрена визуализация и отчетность киберучений, включающая:

- визуализацию компонентов сетевой ИТ инфраструктуры;
- визуализацию процесса обучения;
- интерактивные отчеты и дашборды в ходе обучения и по итогам обучения;
- встроенные инструменты статистики и коэффициента эффективности (KPI).