

Технические правила и требования к решению Хакатона

1. Трек и Задача Хакатона

1.1. Основной Трек

Разработка инструмента оценки безопасности информационных систем и ИТ-инфраструктуры.

1.2. Задача

Участникам предлагается разработать **работоспособный прототип или минимально жизнеспособный продукт (MVP)**, предназначенный для автоматизированной проверки защищённости инфраструктуры и информационных систем (тестирования на проникновение – пентест). Инструмент должен помогать специалистам по ИБ в оценке безопасности, поиске и устранении уязвимостей, а также предоставлять практические рекомендации по их исправлению.

1.3. Рекомендованный функционал решения

Решение должно включать, но не ограничиваться следующими ключевыми возможностями:

- Режимы Сканирования:** Поддержка сканирования в различных режимах, включая "чёрный ящик" (без исходных данных), "серый ящик" (с частичными привилегиями) и "белый ящик" (с полным доступом).
- Имитация Атак:** Реализация сценариев атак, направленных на поиск и эксплуатацию уязвимостей, сетевую разведку, попытку компрометации учетных записей или поиск мисконфигураций.
- Анализ и Реагирование:** Автоматизированный анализ конфигураций и уязвимостей с предложением вариантов реагирования на потенциальные угрозы.
- Автоматизация:** Упрощение и автоматизация рутинных операций пентестеров и аналитиков ИБ.
- Построение Вектора Атаки:** Возможность построения подтвержденных цепочек атак и эксплуатации уязвимостей с переиспользованием полученных данных.
- Отчетность:** Составление детализированных отчетов с доказательствами обнаруженных уязвимостей и четкими инструкциями/рекомендациями для их исправления.

1.4. Сквозные цифровые технологии

Приветствуется интеграция следующих технологий для повышения инновационности решения:

- Искусственный интеллект и машинное обучение.
- Новые коммуникационные интернет-технологии.

2. Технические требования и ресурсы

2.1. Технологический стек (Рекомендованный)

Участники могут использовать любые технологии, но рекомендуется обратить внимание на:

- **Языки программирования:** Python, JavaScript, TypeScript, Go, C/C++.
- **Базы данных:** MySQL, PostgreSQL.
- **Веб-технологии:** HTML, CSS, Nginx.
- **Инструменты ИБ:** Утилиты разведки, анализа и эксплуатации уязвимостей, специализированные инструменты анализа (например, Kali Linux, PT Exploit Explorer).
- **Источники данных:** CVE, БДУ ФСТЭК России.

2.2. Ограничения разработки

- **Оригинальность:** запрещено использовать готовые коммерческие решения или решения, разработанные до начала Хакатона. Допускается использование открытых библиотек и фреймворков.
- **Безопасность:** все разработанные решения должны быть протестированы в изолированной среде, предоставленной Организатором, или на собственном оборудовании без нарушения законодательства и прав третьих лиц.
- **Контроль:** решение должно предусматривать возможность контроля оператора, который может остановить процесс в любой момент.

3. Критерии оценки:

Новизна подхода: насколько оригинальна идея.

Эффективность: насколько хорошо прототип справляется с поиском, анализом и эксплуатацией уязвимостей.

Удобство использования (UI/UX): насколько интуитивно понятен и прост в работе инструмент.

Практическая ценность: насколько полезен и применим на практике результат работы вашего решения.