ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

Чем отличаются исследования

	Пентест	**Анализ защищённости**	**Аудит**
Цель	Достижение поставленной задачи. При этом вопрос полноты обнаруженных уязвимостей не стоит. Определить, может ли текущий уровень защищённости выдержать попытку вторжения потенциального злоумышленника с определённой целью.	Найти все известные и неизвестные уязвимости и недостатки, способные привести к нарушению конфиденциальности, целостности и доступности информации. Сформировать рекомендации по повышению уровня защищённости.	Проверить, насколько информационная система (или её компоненты) и процессы соответствуют требованиям, лучшим практикам или рекомендациям нормативных актов, стандартов и документации производителей оборудования и ПО.
Примеры задач	Получить несанкционированный доступ к информации о клиентах, их средствах и другим данным. Проникнуть из офисного сегмента в боевой, где расположены рабочие серверы. Нарушить доступность определённого сервиса. Получить доступ к файловой системе с некими правами.	Провести комплексный анализ защищённости IT-ресурсов: веб-приложений, СУБД, ДБО, мобильных приложений и т.д.	Проверить соответствие информационной системы PCI DSS. Проверить соответствие информационной системы СТО БР ИББС. Проверить соответствие информационной системы Приказу №21 ФСТЭК России. Проверить веб-серверы на соответствие рекомендациям CIS.
Фокус	Важнее глубина исследования, чем ширина.	Важнее ширина исследования, чем глубина.	Важен объём выполнения требований и рекомендаций.
Уровень зрелости	Высокий.	От низкого до среднего.	От низкого до высокого.
Критерии завершения	Проект заканчивается, как только поставленная цель будет достигнута. Или не достигнута из-за тех или иных причин, например, закончилось время, выделенное на проект.	Проект заканчивается по факту завершения проверок на наличие уязвимостей всех типов во всех подсистемах.	Проект заканчивается по факту завершения всех проверок, предусмотренных методикой.
Методы достижения цели	Все доступные методы и средства, удовлетворяющие ограничениям, поставленным заказчиком (в т. ч. социальная инженерия, атаки перебором и др.). Исследователи ищут кратчайший и самый дешёвый путь достижения целей.	Исследования методом «чёрного / белого / серого ящика», анализ исходного кода, анализ структуры, функций, используемых технологий, подтверждение обнаруженных уязвимостей.	Ручное или автоматизированное проведение проверок в соответствии с выбранной методикой.

План работ	Получить предварительную информацию об объекте, используются все доступные источники информации. Составить карту сети, определить типы и версии устройств, ОС, сервисов, приложений по реакции на внешнее воздействие. Выявить уязвимости сетевых служб, сервисов и приложений (включая базовый анализ веб-приложений с детектированием уязвимостей, способствующих достижению поставленной цели). Проанализировать уязвимости внутренних и внешних ресурсов. Подготовить подходящие сценарии атак. Провести атаки, связанные с социальной инженерией и/или атаками типа отказа в обслуживании (по согласованию). Осуществить проникновение.	Определить метод, который целесообразно использовать для анализа защищённости. Построить модель угроз и нарушителя, если необходимо. Провести инструментальные и ручные проверки для отдельных типов уязвимостей (отсечение ложных срабатываний и выявление уязвимостей, которые не обнаруживаются автоматизированными средствами). Исследовать уязвимости, чтобы подтвердить их наличие и возможность эксплуатации. Проэксплуатировать ряд наиболее критичных уязвимостей (по согласованию).	Адаптировать методику под объект исследования. Составить список проверок. Провести ручные и/или автоматизированные проверки.
Результат	Факт и/или вероятность взлома (проникновения) и получения информации злоумышленником.	Максимально полный перечень обнаруженных уязвимостей.	Заключение о соответствии требованиям / рекомендациям.
Отчёт содержит	Выводы для руководства, содержащие общую оценку текущего уровня защищённости. Описание выявленных недостатков системы управления информационной безопасностью. Оценку возможностей злоумышленника ими воспользоваться. Описание сценариев, при помощи которых проводилось проникновение. Подробное описание структуры объектов тестирования. Описание полного хода тестирования (воспроизводимость) с информацией по всем выявленным уязвимостям и результатам их эксплуатации. Рекомендации по повышению текущего уровня защищённости.	Методику проведения анализа защищённости. Модель угроз и нарушителя. Выводы для руководства, содержащие оценку уровня защищённости по результатам анализа. Подробное описание всех обнаруженных уязвимостей и их подтверждение. Оценку уровня рисков (оценка вероятности эксплуатации уязвимости и степени влияния на бизнес процессы Заказчика). Возможные сценарии атаки с учётом различных моделей нарушителя. Подробные рекомендации по устранению выявленных уязвимостей. В зависимости от используемого при анализе подхода рекомендации могут включать и примеры корректного кода и т.д.	Описание методики аудита. Перечень критериев аудита. Заключение о соответствии информационной системы критериям аудита. Рекомендации по устранению выявленных несоответствий и недостатков.
От чего зависит стоимость	От комплексной сложности архитектуры, поставленных задач, сроков и ограничений на работу (например, работа только в выходные или ночное время).	От количества исследуемых сервисов, служб, приложений и протоколов, а также от модели угроз и нарушителя, методики проверки.	От архитектуры и масштаба информационной системы, методики аудита и набора критериев.