**ОПРОСНЫЙ ЛИСТ
< ТЕХНИЧЕСКИЙ АУДИТ БЕЗОПАСНОСТИ (Пентест/тестирование на проникновение)/>**

|  |
| --- |
|  |
| Наименование организации |  |
|  |
| Контактное лицо |  |
|  |
| Телефон |  |
|  |
| Email |  |
|  |
| Дата заполнения |  |
|  |

**Общие сведения**

|  |
| --- |
| 1. Цель проведения
 |
|  |
| [ ]  Требования законодательства о защите информации в государственных информационных системах (ФЗ-149, Приказ ФСТЭК России №17) |
| [ ]  Требования Положения ЦБ РФ 382-П/683-П об анализе уязвимостей в прикладном ПО (ОУД4) |
| [ ]  Требования Положения ЦБ РФ 382-П/683-П о ежегодном тестировании на проникновение и анализе уязвимостей |
| [ ]  Оценка действующей системы информационной безопасности |
| [ ]  Другое |  |
|  | *(указать)* |
|  |
| 1. Имеется ли в Вашей организации служба безопасности (в т.ч. информационной)?
 |
|  |
| [ ]  Да |
| [ ]  Да. Также есть отдельная служба/сотрудник информационной безопасности |
| [ ]  Нет |
| [ ]  Затрудняюсь ответить |
|  |
| 1. Все ли объекты информационного взаимодействия в границах исследования (компьютеры, серверы, сетевое и периферийное оборудование) объединены в одну локальную сеть?
 |
|  |
| [ ]  Да, все компьютеры «видят друг друга» |
| [ ]  Нет |
| [ ]  Затрудняюсь ответить |
| [ ]  Другое |  |
|  | *(указать)* |
|  |
| 1. Используется ли в границах исследования - Active Directory Domain/LDAP?
 |
|  |
| [ ]  Да, все компьютеры в едином Домене |
| [ ]  Да, используется несколько взаимосвязанных Доменов |
| [ ]  Да, но используется несколько несвязанных Доменов |
| [ ]  Нет, не используется |
| [ ]  Затрудняюсь ответить |
|  |
| 1. Имеется ли подключение к сети Интернет внутри границ исследования?
 |
|  |
| [ ]  Да, множество точек входа |
| [ ]  Да, единственная точка входа |
| [ ]  Нет |
|  |
| 1. Имеется ли DMZ?
 |
|  |
| [ ]  Да |
| [ ]  Нет |
| [ ]  Затрудняюсь ответить |
|  |
| 1. У всех ли пользователей есть выход в Интернет?
 |
|  |
| [ ]  Да | [ ]  Нет |
|  |
| 1. Ограничен ли доступ к ресурсам сети Интернет?
 |
|  |
| [ ]  Не ограничен |
| [ ]  Настроен «чёрный список» ресурсов |
| [ ]  Настроен «белый список» ресурсов |
|  |
| 1. Применяются ли в границах исследования средства защиты информации?
 |
|  |
| [ ]  Да, применяются повсеместно |
| [ ]  Да, но только отдельные решения |
| [ ]  Нет |
| [ ]  Затрудняюсь ответить |
| Какие СЗИ точно имеются (тип)? Например, антивирусы, средства корреляции (SIEM), DLP и пр. (**не указывается в случае** Red Team, AppSec) |  |
|  | *(указать)* |
|  |
| 1. Находятся ли объекты исследования в зоне ответственности какого-либо SOC?
 |
|  |
| [ ] Да |
| [ ]  Нет |
| [ ]  Затрудняюсь ответить |
|  |
| 1. Количество внешних IP-адресов, подлежащих тестированию
 |
|  |
| Количество адресов |  |
|  | *(указать их общую ёмкость)* |
| [ ]  Внешнее тестирование не требуется |
|  |
| 1. Количество WEB-ресурсов в границах исследования
 |
|  |
| Количество ресурсов |  |
|  | *(указать)* |
| [ ] В границах исследования WEB-ресурсы отсутствуют |
|  |
| 1. Количество серверов (вирт + физ, имеющих свои IP) в границах исследования
 |
|  |
| Количество серверов |  |
|  | *(указать)* |
| [ ]  В границах исследования серверы отсутствуют |
|  |
| 1. Количество рабочих станций в границах исследования
 |
|  |
| Количество APM |  |
|  | *(указать)* |
| [ ]  В границах исследования рабочие станции отсутствуют |
|  |
| 1. Используемые типы линий связи в границах исследования
 |
|  |
| [ ]  Затрудняюсь ответить |
| [ ]  Ethernet |
| [ ]  SFP |
| [ ]  Wi-Fi |
|  |
| 1. Используемые протоколы передачи информации внутри границ исследования
 |
|  |
| Протоколы передачи |  |
|  | *(указать)* |
| [ ]  Затрудняюсь ответить |
|  |

**Подход к проведению аудита безопасности**

|  |
| --- |
| 1. Формат проведения аудита безопасности
 |
|  |
| [ ]  Тестирование на проникновение |
| [ ]  Purple Team |
| [ ]  Red Team (APT) |
| [ ]  Эвристический анализ ПО (AppSec) |
|  |
| 1. Формат социальной инженерии (при необходимости)
 |
|  |
| [ ]  Email |
| [ ]  Телефон |
| [ ]  Очно |
|  |
| 1. Желаемая форма взаимодействия (**не указывается в случае** Red Team, AppSec)
 |
|  |
| [ ]  Очная форма проведения |
| [ ]  Удалённый доступ с предоставлением необходимых полномочий |
| [ ]  Удалённый доступ без прав доступа |
| [ ]  Другое |  |
|  | (указать) |
|  |
| 1. Формат проведения аудита безопасности
 |
|  |
| [ ]  Black Box (метод «чёрного ящика») |
| [ ]  Gray Box (метод «серого ящика») |
| [ ]  White Box (метод «белого ящика») |
|  |
| 1. Сценарии взаимодействия со службой безопасности (при её наличии, **не указывается в случае** Red Team)
 |
|  |
| [ ]  Black Hat | [ ]  White Hat |
|  |
| 1. Необходимость/желание тестирования защищенности беспроводных протоколов обмена (при их наличии)
 |
|  |
| [ ]  Да | [ ]  Нет |
|  |
| 1. Необходимость/желание проведения стресс-тестирования (DDoS)
 |
|  |
| [ ]  Да | [ ]  Нет |
|  |

↓ ↓ ↓ продолжение ↓ ↓ ↓

**Состав и содержание процедур**

|  |
| --- |
| 1. Желаемая «глубина» аудита безопасности (**не указывается в случае** Red Team, AppSec)
 |
|  |
| [ ]  По требованиям НПА |
| [ ]  Сбор данных из открытых источников |
| [ ]  Оценка привлекательности для кибератак |
| [ ]  Тестирование конфигураций DNS |
| [ ]  Поиск незащищенных информационных каналов |
| [ ]  Активное сканирование |
| [ ]  Идентификация сервисов/служб/приложений |
| [ ]  Анализ внутренней инфраструктуры |
| [ ]  Автоматизированный поиск уязвимостей |
| [ ]  Эвристический ручной анализ |
|  |
| 1. Желаемые техники проведения эвристического анализа ПО (**не указывается в случае** AppSec)
 |
|  |
| [ ]  По требованиям НПА (ОУД) |
| [ ]  Функциональное тестирование |
| [ ]  Нагрузочное тестирование |
| [ ]  Фаззинг |
| [ ]  Сигнатурный анализ кода |
| [ ]  Динамический анализ кода |
| [ ]  Обратная разработка |
| [ ]  Анализ реализованных механизмов |
|  |

Благодарим за уделенное время!