1. **Общая информация об организации**

|  |  |  |
| --- | --- | --- |
| **1.** | **Полное наименование организации** |  |
| **2.** | **Контактное лицо в организации**  **(подразделение, должность, ФИО, конт. тел., email)** |  |

1. **Внешний периметр. Перечень систем, подлежащих обследованию:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Тип сервиса** | | **Перечень “белых“ IP с указанием сервисов** | **Пример** |
| **1.** | **Сетевые сервисы** |  | 82.141.14.15:http,https,ftp;  29.172.19.11:http, smtp, openvpn. |
| **2.** | **Веб-сервисы** |  | 82.141.14.15: веб-сайт. Сайт-визитка.  29.172.19.11: Веб-сервис обмена документами между сотрудниками и контрагентами. Присутствует авторизация пользователей. Сервис хранит конфиденциальную информацию. |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1.** | **Требуемые к проведению работы на перечисленных внешних ресурсах**  **(поставьте отметку, где необходимо)** | |  |  |  | | --- | --- | --- | | 1. | Да | **“Базовое тестирование”.** Позволяет получить понимание общей степени защищенности перечисленных ресурсов и показывает, каких результатов добьется злоумышленник в первые дни своей работы. Отчет содержит выявленные в ходе работ уязвимости и примеры их использования.  Является лучшим выбором для компаний, в которых ранее не проводился тест на проникновение\анализ защищенности. | | 2 | Да | **Тест на проникновение.** Работы, которые проводятся до достижения поставленной цели. Цель – получить доступ в закрытую область, получить доступ к конфиденциальной информации. Отчет содержит описание одной успешной атаки и перечень уязвимостей, которые были для этой атаки задействованы.  Является лучшим выбором для компаний, которым требуется показать, текущий уровень информационной безопасности должен быть повышен в связи с уязвимостью целевых систем. | | 3. | Да | **Анализ защищенности.** Цель работ – выявить как можно большее число уязвимостей на целевых системах.  Данные работы обычно проводятся для конкретных критически-значимых ресурсов, для которых требуется обеспечить повышенный уровень защищенности. | |

1. **Внутренний периметр. Перечень систем, подлежащих обследованию:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Тип сервиса** | | **Перечень IP с указанием сервисов** | **Пример** |
| **1.** | **Сетевые сервисы** |  | Внутренние сервера:  172.16.16.2:http,https,ftp, AD;  10.10.0.15:http, smtp, DNS-server. |
| **2.** | **Веб-сервисы** |  | 192.168.100.25: веб-сайт. Сайт-визитка.  192.168.23.41: Веб-сервис обмена документами между сотрудниками и контрагентами. Присутствует авторизация пользователей. Сервис хранит конфиденциальную информацию. |
| **3.** | **Рабочие станции пользователей.** |  | 172.16.0.1\24 – рабочие станции сотрудников. Типовая настройка. |

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **1.** | **Требуемые к проведению работы на перечисленных внутренних ресурсах**  **(поставьте отметку, где необходимо)** | |  |  |  | | --- | --- | --- | | 1. | Да | **“Базовое тестирование”.** Позволяет получить понимание общей степени защищенности перечисленных ресурсов и показывает, каких результатов добьется злоумышленник в первые дни своей работы. Отчет содержит выявленные в ходе работ уязвимости и примеры их использования.  Является лучшим выбором для компаний, в которых ранее не проводился тест на проникновение\анализ защищенности. | | 2 | Да | **Тест на проникновение.** Работы, которые проводятся до достижения поставленной цели. Цель – получить доступ в закрытую область, получить доступ к конфиденциальной информации. Отчет содержит описание одной успешной атаки и перечень уязвимостей, которые были для этой атаки задействованы.  Является лучшим выбором для компаний, которым требуется показать, текущий уровень информационной безопасности должен быть повышен в связи с уязвимостью целевых систем. | | 3. | Да | **Анализ защищенности.** Цель работ – выявить как можно большее число уязвимостей на целевых системах.  Данные работы обычно проводятся для конкретных критически-значимых ресурсов, для которых требуется обеспечить повышенный уровень защищенности. | |

**Дополнительные вопросы.**

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **Вопрос** | **Ответ** | **Пояснения** |
| **1.** | **Возможно ли организовать VPN туннель для исполнителей до внутренней сети?** |  | Целью данного вопроса является выяснение возможности снижения накладных расходов исполнителя (снижение стоимости проекта для Заказчика), вследствие проведения работ удаленно. Для проведения работ клиент может создать туннель (туннели) до площадок, на которых находятся обследуемые системы.  Необходимо указать, возможно ли это, либо возможно частично (тогда указать в каком объеме). |
| **2.** | **Укажите расположение объектов, на которых планируется проведение внутреннего теста на проникновение.** |  | Если до всех обследуемых систем нет возможности создать удаленный доступ исполнителей, необходимо указать территориальное расположение объектов с привязкой по количеству, либо перечню IP из п.3. |

1. **Тест на проникновение с использованием социальной инженерии.**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Вопрос | Ответ | Пояснения |
| **1.** | **Укажите к-во человек, которые входят в область тестирования с применением методов социальной инженерии?** |  | Стоимость работ рассчитывается по количеству человек. Зачастую, есть необходимость во включении в область обследования топ-менеджмента, персонала службы help-desk, и выборочного контроля обычных сотрудников. |
| **2.** | **Укажите месторасположение офисов, в которых находятся сотрудники из пункта выше.** |  | Необходимо указать в каком офисе находится сколько человек из области обследования. |
| **3.** | **Какие тесты социальной инженерии должны быть проведены (поставьте отметку, где необходимо)** | |  |  |  | | --- | --- | --- | | 1. | Да | Безадресные рассылки писем, с вредоносными ссылками. | | 2 | Да | Адресные фишинговые рассылки писем, с вредоносными ссылками. | | 3. | Да | Безадресные рассылки писем, с вредоносным вложением. | | 4. | Да | Адресные фишинговые рассылки писем, с вредоносным вложением. | | 5. | Да | Звонки из службы техподдержки. | | 6. | Да | Атаки через “забытые” флеш-накопители | | Пункты 1-5 выполняются удаленно.  Пункт 6 требует выезда аудиторов в офисы компании и проведении атак “на-месте”. |
| **4.** | **Какие политики есть в организации, связанные с предотвращением действий с использованием социальной инженерии?** |  | Указать есть ли такие политики, и если они есть, приложить их к анкете (если не возможно приложить, указать краткое содержание). |

1. **Информация о технических средствах защиты организации**

|  |  |  |  |
| --- | --- | --- | --- |
| № | Вопрос | Ответ | Пояснения |
| **1.** | **Используется ли в организации WAF (Web Application Firewall)** | |  |  | | --- | --- | | Да | Укажите какой: | | Нет |  | | Примеры WAF: Imperva SecureSphere, Citrix NetScaller, DenyAll rWeb, SourceFire 3D, F5 ASM, Barracuda и др. |
| **2.** | **Используется ли в организации IPS (Intrusion Prevention System)** | |  |  | | --- | --- | | Да | Укажите какой: | | Нет |  | | Примеры IPS: CheckPoint IPS, StoneSoft IPS, Cisco IPS, McAfee IPS, Fortinet IPS, Palo Alto Networks IPS и др. |
| **3.** | **Используется потоковый антивирус?** | |  |  | | --- | --- | | Да | Укажите какой: | | Нет |  | |  |
| **4.** | **Используется ли фильтр SPAMa?** | |  |  | | --- | --- | | Да | Укажите какой: | | Нет |  | |  |
| **5.** | **Используется ли средство мониторинга и корреляции событий (SIEM)?** | |  |  | | --- | --- | | Да | Укажите какой: | | Нет |  | | Примеры SIEM: HP-Q1 Labs, HP-ArcSight, Splunk, McAfee, EMC-RSA, Tenable, Symantec и д.р. |

1. **Если вы хотите сообщить какие-либо дополнительные сведения, либо добавить комментарии, пожалуйста, сделайте это в поле ниже.**

|  |
| --- |
|  |