# Приложение №1

|  |  |  |  |
| --- | --- | --- | --- |
|  | **УТВЕРЖДАЮ:** | | |
|  | | |
| Начальник отдела ИБ | | |
| *(должность начальника подразделения – Инициатора)* | | |
| Савченко С.Ю. | | |
| *(Ф. И. О. Начальника подразделения – Инициатора)* | | |
|  | | |
| *(подпись)* | | |
|  | | |
| **ТЕХНИЧЕСКОЕ ЗАДАНИЕ**  **для ДОГОВОРА ВОЗМЕЗДНОГО ОКАЗАНИЯ УСЛУГ**  **ПО ПРОВЕДЕНИЮ ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ** | | | |
|  | | | |
| Требования к предмету Закупки | | | |
|  | | | |
| Общие требования к качеству | | | |
| В соответствии с данным техническим заданием Исполнитель оказывает услуги по проведению тестирования на проникновение, в соответствии с требованиями и в объеме, указанным в п.1.6 данного Технического задания. | | | |
|  | | | |
| Требования к техническим характеристикам | | | |
| Отсутствуют | | | |
|  | | | |
| Требования к размерам (заполняется для товаров) | | | |
| Отсутствуют | | | |
|  | | | |
| Требования к упаковке (заполняется для товаров) | | | |
| Отсутствуют | | | |
|  | | | |
| Требования к отгрузке (заполняется для товаров) | | | |
| Отсутствуют | | | |
|  | | | |
| Количество товара, объем работ, услуг | | | |
| Исполнитель оказывает услуги по проведению комплексного тестирования на проникновение в следующем объеме:   * внешнее тестирование на проникновение в режиме черного ящика, включая сервисы удаленного доступа, веб-приложения и сайты, почтовые сервисы, прочие сетевые сервисы; * внутреннее тестирование на проникновение по модели гостя и инсайдера; * анализ защищенности беспроводных сетей; * оценка осведомленности сотрудников в вопросах информационной безопасности (социотехнические атаки); * повторное тестирование на наличие выявленных уязвимостей после их устранения Заказчиком.   Для следующей инфраструктуры Заказчика:   * количество публично доступных IP-адресов для тестирования – 33; * количество веб-сервисов области тестирования – 5; * количество сервисов собственной разработки – 1; * примерное количество серверов в области тестирования – 350; * примерное количество рабочих станций в области тестирования – 1100; * примерное количество сетевых сегментов – 500; * количество беспроводных сетей – 3.   C возможностью организации защищенного удаленного доступа для проведения работ.  В состав работ должно быть включено:   * определение типов и версий устройств, ОС, сетевых сервисов и приложений по реакции на внешнее воздействие; * идентификация уязвимостей серверов, сетевого оборудования и сетевых средств защиты. Идентификация уязвимостей должна производится для всех хостов, входящих в границы работ и доступных (или ставших доступными в ходе работ) из сети Интернет (в том числе, сервисы HTTP и DNS, VPN-сервисы, web-приложения, сервис электронной почты, системные и прикладные сервисы). Должно производится выявление как уязвимостей, связанных с некорректной реализацией, так и уязвимостей, связанных с некорректной конфигурацией сетевых сервисов, ОС, приложений, сетевых устройств и средств защиты; * экспертный анализ защищенности (проникновение), включающий моделирование атак, с использованием специализированных средств и сведений об известных уязвимостях, в отношении целевых систем; * проведение социотехнических атак.   При проведении работ необходимо (включая, но не ограничиваясь):   1. Определить список сервисов для конкретного хоста: IP-адрес, порт и протокол взаимодействия посредством:  * сканирования всех адресов по всем портам с помощью специализированных утилит, с различными настройками скрытности; * для доступных веб-ресурсов определения способа обращения к ним - URL, включая домен и путь; * определения версии сервиса по сетевому баннеру с использованием специализированных сканеров; * установления используемого продукта/платформы с помощью поисковых систем; * попыток определить и подтвердить протокол сервиса на основе порта; * определения наличия мобильных приложений для подключения к веб-ресурсу.  1. Выявить технические недостатки во внешней и внутренней сети на сетевом уровне (при необходимости), а именно:  * ошибки в настройке сетевого оборудования, ОС, веб-серверов, систем управления базами данных и других компонентов инфраструктуры; * ошибки межсетевого экранирования (сегментирования); * ошибки в организации удаленного доступа; * использование недостаточно защищенных протоколов передачи данных, а также служебных протоколов (telnet, snmp, и т.д.); * уязвимости, связанные с использованием устаревших версий ПО/прошивок на доступных текущему нарушителю ресурсах; * использование слабых или словарных паролей на служебных сервисах, а также прикладных сервисах и приложениях, недостатки парольной политики; * возможность доступа к сетевым хранилищам конфиденциальной информации, хранение важных данных в незащищенном или недостаточно защищенном виде.  1. Выявить недостатки проектирования, реализации и эксплуатации веб сервисов, используемых в локальной сети, а именно:  * некорректная настройка прикладного программного обеспечения (CMS, Фреймворков, веб-сервера, сервера приложений и т. п.); * небезопасная эксплуатация и/или администрирование веб-компонентов (слабые пароли, пароли по умолчанию, доступ к служебным компонентам в файловой системе веб-сервера, доступ к архивным копиям приложения, доступ к исходному коду веб-приложения через служебные файлы системы контроля версий (.cvs, .svn, .git)); * некорректная обработка входных данных в веб-компонентах, некорректная обработка пользовательского ввода, которая позволяет проводить следующие виды атак:   + внедрение операторов языка SQL (SQL injection), в том числе межмодульное;   + включение локальных и удаленных файлов (LFI/RFI);   + внедрение кода на языке, интерпретируемом на стороне клиента (XSS), в том числе межмодульное и клиентское;   + внедрение команд, интерпретируемых средой выполнения (Eval injection/EL inejction);   + внедрение команд, интерпретируемых ОС сервера (OS command injection);   + внедрение разметки на языке XML;   + внедрение заголовков (Header Injection), в том числе позволяющих разделить HTTP ответ;   + внедрение сериализованных объектов (Object Injection);   + подключение внешних XML-сущностей (XML External Entity);   + прочие атаки, целью которых является выполнение кода на стороне сервера (например, загрузка файлов (Unrestricted Upload of File with Dangerous Type)).  1. Провести эксплуатацию недостатков, перспективных с точки зрения увеличения уровня доступа/перечня доступных ресурсов/расширения (повышения) привилегий, а именно:  * подбор паролей; * использование эксплойтов для удаленного повышения привилегий на узлах, использующих стандартное ПО с известными уязвимостями; * эксплуатация недостатков в веб-приложениях для получения доступа в административную панель с целью получения возможности выполнения команд операционной системы или доступа к учетным данным пользователей веб-приложения; * использование эксплойтов для локального повышения привилегий на захваченных узлах с целью получения прав суперпользователя (root, SYSTEM и т. п.); * переконфигурирование сетевых устройств с целью преодоления правил межсетевого сегментирования; * проведение атак на рабочие места администраторов с целью получения доступа к учетным записям, используемым ими для управления сетевыми, системными и прикладными ресурсами (доступ к SSH-ключам, к менеджерам паролей, к локальным файлам со списками паролей и т. п.); * эксплуатация производится в соответствии с согласованным с Заказчиком планом в отведенное время. Исполнителем предоставляется информация по возможному влиянию на эксплуатируемый сервис; * повышение привилегий производиться по согласованию с Заказчиком в отведенное время. Превышение привилегии должно осуществляться не менее тремя способами с гарантированным не прерыванием доступности эксплуатируемого средства и ПО; * развитие атаки осуществляется по заранее спланированному и согласованному с Заказчиком плану в отведенное временя. Цель проникновения - получение прав доменного администратора/компрометация домена. Атака может быть остановлена по решению Заказчика;  1. Провести анализ защищенности беспроводных сетей, а именно:  * обнаружение точек доступа и сбор информации с использованием автоматизированных средств; * для сетей с защитой WPA2-Enterprise проведение атак с фальшивой точкой доступа, в рамках которых Исполнитель пытается вынудить жертв подключиться к его точке доступа и получить их аутентификационные данные; * для гостевых беспроводных сетей выполнение проверок возможности проникновения во внутреннюю сеть Заказчика с их использованием; * при возможности проведение других распространенные атаки на беспроводные сети стандарта 802.11x.  1. Провести социотехнические атаки в части:  * проверки наличия в сети Интернет сведений, часто используемых при социотехнических атаках, в том числе - проверка публичных «утечек данных»; * проверки настроек используемого программного обеспечения для противодействия социотехническим атакам; * рассылки электронных писем с вложением с активным содержимым/исполняемым файлом; * рассылки электронных писем со ссылкой на тестовый фишинговый ресурс; * телефонных звонков сотрудникам Заказчика с целью получения конфиденциальной информации или удаленного доступа; * подбрасывания внешних носителей информации (USB-накопителей) с тестовым вредоносным приложением.   Cоциотехническое тестирование должно проводиться в следующем порядке:   * сбор информации (адресов электронной почты и иных контактных данных работников, сведений об их интересах и т.п.) о работниках Заказчика в общедоступных источниках; * формирование и согласование с Заказчиком перечня проводимых проверок и перечня тестируемых пользователей; * проведение тестов и обработка их результатов.   По результатам выполнения работ Заказчику должны быть предоставлены документы, содержащие рекомендации по устранению выявленных уязвимостей, включающие:  1. описание проведённых работ с детализацией действия – сценариев атак, которые приводили к выявлению уязвимостей или изменению возможностей атакующего;  2. перечень выявленных уязвимостей, ошибок конфигурации и других недостатков;  3. результаты эксплуатации наиболее критичных уязвимостей, включая информацию о полученном уровне привилегий в системе;  4. оценку степени критичности всех выявленных уязвимостей, оценку возможного влияния реализации уязвимостей на ИТ-инфраструктуру Заказчика, ранжирование выявленных недостатков по уровню риска (согласно метрикам CVSS или OWASP Risk Rating Calculator), вероятности их использования, описание последствий реализации выявленных уязвимостей;  5. подробные рекомендации по повышению уровня защищённости и устранению выявленных уязвимостей, включая рекомендации по изменению конфигурации и настроек оборудования, используемых защитных механизмов и программных средств, принятию дополнительных мер и применению дополнительных средств защиты, по установке необходимых обновлений для используемого программного обеспечения и т.п.  6. инвентаризация выявленных недочетов на русском языке, включая ссылки на международные стандарты, оценку степени критичности, пошаговые рекомендации по устранению.  7. верхнеуровневое резюме для руководства на русском языке;  8. структурированное описание полученных данных о целевой инфраструктуре (видение целевой инфраструктуры с позиции потенциального злоумышленника);  9. комплексное заключение с описанием принятых мер и экспертной оценкой текущего состояния ЗИ и принятых мерах ЗИ;  10. перечень скомпрометированных в ходе работ компонент.  11. отчет о результатах оценки осведомленности сотрудников в вопросах информационной безопасности, статистику по каждому из типов атаки и действиям пользователей, перечень сотрудников, недостаточно осведомленных в вопросах информационной безопасности.  12. выводы об эффективности средств и систем ИБ Заказчика, их достаточности для обеспечения противодействия проведенным атакам. Анализ проводится совместно специалистами Исполнителя, имеющими соответствующую квалификацию и опыт оценки систем ИБ и процессов реагирования на инциденты ИБ.  Работы Исполнителя на каждом из этапов должны предварительно согласовываться с ответственными представителями Заказчика. | | | |
|  | | |
| Место, сроки (периоды), иные условия Закупки | | |
|  | | |
| Место поставки товара, выполнения работ, оказания услуг | | |
| г. Санкт-Петербург, Пулковское шоссе, д. 41, лит. ЗА;  г. Санкт-Петербург, Пулковское шоссе, д. 41, лит. А;  г. Санкт-Петербург, Пулковское шоссе, д. 41, лит. ЗИ. Контактное лицо: Савченко Сергей ЮрьевичE-mail: S.Savchenko@pulkovo-airport.com | | |
|  | | |
| Сроки (периоды, стадии) поставки товара, выполнения работ, оказания услуг Согласно коммерческому предложению потенциального поставщика, но не позднее 30.12.2024г. | | |
|  | | |
| Иные условия поставки товара, выполнения работ, оказания услуг | | |
|  | | |
| Требования к Поставщику | | |
|  | |  |
| наличие прав на осуществление определенных действий (деятельности): | |  |
|  | |  |
| лицензии: Лицензия на деятельность по технической защите конфиденциальной информации ФСТЭК РФ. Действие лицензии должно распространяться на услуги по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации; проектированию в защищенном исполнении средств и систем информации. | |  |
|  | |  |
| участие в профессиональных объединениях (например, саморегулируемых организациях) [указать, каких]; | |  |
|  | |  |
| допуски, разрешения [указать, какие]; | |  |
|  | |  |
| сертификаты, декларации [указать, какие]; | |  |
|  | |  |
| договор об осуществлении деятельности от имени третьих лиц (например, в качестве официального дилера, поставщика и т. д.) [указать, какой]; | |  |
|  | |  |
| права на результаты интеллектуальной деятельности (лицензионные договоры, патенты, свидетельства и т. д.) [указать, какие]; | |  |
|  | |  |
| иные: | |  |
| Исполнитель должен иметь в штате и привлечь при проведении работ не менее 3 (трех) компетентных специалистов, имеющих сертификаты OSCP (Offensive Security Certified Professional), CEH (Certified Ethical Hacker), OSWE (Offensive Security Web Expert), OSWP (Offensive Security Wireless Professional).  Исполнитель должен обладать опытом проведения вышеуказанных работ в объеме не менее 20 успешных проведенных тестирований на проникновение за 2 календарных года до момента начала подачи заявок, один из договоров должен быть на сумму не менее 1 500 000 руб. и быть заключен в рамках 44-ФЗ или 223-ФЗ.  Исполнитель должен предоставить подтверждение в момент подачи заявки. | |  |
| квалификационные требования: | |  |
|  | |  |
| требования к персоналу: | |  |
|  | |  |
| требования к производственным мощностям, технологиям, оборудованию [указать, какие]; | |  |
|  | |  |
| иные: | |  |