Приложение 3

к документации о проведении конкурсного отбора

**Техническое задание**

**на оказание услуг** **по тестированию инфраструктуры**

**АО «Экспобанк»**

**Адреса оказания услуг:** г. Москва, Космодамианская наб., д. 52, стр. 7; Удаленно.

**Условия оплаты:**

## 100% предоплата в течение 10 (десяти) рабочих дней со дня получения Заказчиком счета на оплату, выставленного Исполнителем, после подписания Договора.

## Или

Предоплата 50% от стоимости услуг в течение 10 рабочих дней после выставления счета Исполнителем, окончательный расчет в течение 10 рабочих дней с момента подписания обеими Сторонами Акта оказанных услуг и получения Заказчиком соответствующего счета от Исполнителя

1. **Услуги по проведению тестирования на проникновение:**

**1.1 Цели и задачи**

Тестирование на проникновение проводится с целью выявления уязвимостей внутренней инфраструктуры Заказчика, а также получения объективной оценки ее текущего уровня защищенности. Достижение этих целей снижает вероятность наступления инцидента, вызванного действиями потенциального злоумышленника.

В рамках проекта Исполнитель решает следующие задачи:

* Идентификация уязвимостей сетевых служб и приложений;
* Идентификация уязвимостей и ошибок конфигурирования серверов, рабочих компьютеров, сетевого оборудования Заказчика.
* Поиск доступа к базам данных с конфиденциальной информацией и персональными данными сервисов Заказчика;
* Выявление недостатков в применяемых мерах кибербезопасности и оценка возможности использования их нарушителем;
* Практическая демонстрация эксплуатации уязвимостей (на примере наиболее критических);
* Выработка рекомендаций по устранению найденных уязвимостей или принятию компенсационных мер защиты;

**1.2 План оказания услуг**

Для решения поставленных задач Исполнитель выполняет для Заказчика работы в соответствии с табл. 1.

Таблица 1 — План оказания услуг

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№** | **Этап** | **Перечень работ** | **Срок оказания услуг** | **Стоимость, руб., с НДС** |
| **1** | Сбор информации об объекте исследования | Активный и пассивный сбор данных об инфраструктуре (используемые технологии, архитектура и оборудование сети), а также первичная идентификация уязвимостей в настройках граничного сетевого оборудования, сетевых службах и приложениях | 02.12.2024 – 28.12.2024 |  |
| **2** | Тестирование на проникновение | Поиск возможности получения НСД к конфиденциальным данным и защищенным сегментам сети, при отсутствии привилегированного доступа  | 02.12.2024 – 28.12.2024 |  |
| **3** | Эксплуатация обнаруженных уязвимостей | Эксплуатация обнаруженных уязвимостей и проверка наиболее вероятных векторов атаки, позволяющих получить НСД к конфиденциальным данным, защищенным сегментам сети или даже полный контроль над IT-инфраструктурой | 02.12.2024 – 28.12.2024 |  |
| **4** | Подготовка отчета | Подготовка и согласование итогового отчета в соответствии с формой, описанной в методике Исполнителя | 02.12.2024 – 28.12.2024 |  |
| Итого:  |  |

**1.3 Объекты тестирования**

Тестирование на проникновение проводится по отношению к Внутренней инфраструктуре Заказчика.

* Проведения тестирования методом “Black box”;
* Исследуемый объем внутреннего периметра – корпоративная сеть, сетевые хранилища, контролер домена.

Границы оказания услуг, а также полный список доступных для исследования подсетей и информационных систем согласовываются дополнительно перед началом проекта.

1. **Модель злоумышленника**

**2.1 Цель:** получение финансовой или другой личной выгоды, а также нанесение любого вреда Заказчику или его клиентам.

**2.2 Уровень квалификации:** высококвалифицированный специалист, обладающий навыками, сравнимыми с навыками Исполнителя.

**2.3 Привилегии при тестировании внутренней инфраструктуры:**

* привилегии во внутренней сети отсутствуют;
* в случае неудачи прохождения внешнего периметра, предоставляется пользовательская учетная запись в домене.

В ходе оказания услуг Исполнитель имитирует процесс анализа внешней и внутренней инфраструктуры потенциальным злоумышленником в соответствии с вышеописанной моделью. При этом действия, ведущие к возможности нанесения вреда Заказчику или его клиентам, Исполнитель выполняет исключительно по согласованию с Заказчиком.

1. **Состав оказываемых услуг**

Тестирование на проникновение проводится по методике Исполнителя и в соответствии со следующими международными стандартами и практиками:

* Penetration Testing Execution Standard (PTES);
* NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment;
* Open Source Security Testing Methodology Manual (OSSTMM);
* Open Web Application Security Project (OWASP) Testing Guide;
* Council of Registered Ethical Security Testers (CREST);
* Payment Card Industry Data Security Standard (PCI DSS).

**3.1 Услуги включают следующие этапы:**

* **Сбор данных об объекте исследования:**
* диапазоны IP-адресов;
* имена доменов и поддоменов;
* сетевые протоколы, используемые в локальной сети;
* сетевое оборудование;
* почтовые сервера;
* DNS-сервера;
* компоненты сети;
* средства защиты;
* внешние системы, отраженные во внутренней сети;
* типы и версии ОС;
* типы и версии ПО;
* типы и виды устройств.
* **Тестирование на проникновение:**
* проверка возможности преодоления сетевого периметра при не авторизованном подключении к локальной вычислительной сети;
* поиск способов получения НСД к операционным системам, телекоммуникационному оборудованию, приложениям и службам (CУБД, веб-приложения, клиент-серверные приложения, мобильное приложение и др.).
* **Эксплуатация обнаруженных уязвимостей:**
* анализ уязвимостей рабочих станций пользователей, компонентов Внутренней инфраструктуры, сетевого оборудования и сетевых средств защиты;
* моделирование атак на уровне приложений, сетевых сервисов и ОС с использованием специализированных средств, а также сведений об уязвимостях и ошибках конфигурации;
* эскалация привилегий пользователя — проверка возможности получения прав администратора;
* проверка возможности несанкционированного повышения привилегий в IT-сервисах авторизованными пользователями и получения доступа к закрытой информации;
* проверка возможности компрометации публичных сервисов c целью получения доступа к конфиденциальной информации или информации ограниченного пользования;
* проверка возможности получения доступа к контроллеру домена.
* **Подготовка отчета:**
* общая информация;
* экспертная оценка текущего уровня защищенности;
* сценарий компрометации;
* перечень обнаруженных уязвимостей;
* общие рекомендации по повышению уровня защищенности;
* подробная информация о найденных уязвимостях, включая подробное описание, уровень опасности, место обнаружения, пример эксплуатации и рекомендации по устранению.
1. **Требования к Исполнителю**

4.1 Исполнитель должен обладать следующими лицензиями:

лицензия ФСТЭК России на деятельность по технической защите конфиденциальной информации согласно п.п. б) ст.4 Положения введенного Постановлением Правительства РФ 2012 года №79 (подтверждается наличием копии лицензии)

4.2 Наличие профильных сертификатов у специалистов Исполнителя: KCFC, CHFI, OSCP, CWAP, CEH, CRTE, CRTP, RTO, eCPTX, OSEP, OSWE, OSCE3, eWPTX, SQLIM (подтверждается предоставлением копии сертификатов).

4.3 Опыт проведения работ по анализу защищенности и пентестам не менее 3 последних лет.

4.4 Участие специалистов Исполнителя в соревнованиях в сфере кибербезопасности - Pentestit Lab/Standoff и т.д. (подтверждается предоставление копии сертификатов об участии)

4.5 Опыт проведения работ по стандартам:

* PTES (Penetration Testing Execution Standard)
* OWASP Testing Guide
* OSSTMM (Open Source Security Testing Methodology Manual),
* NIST SP 800-115: Technical Guide to Information Security Testing and Assessment
* CREST (Council of Registered Ethical Security Testers)
* PCI DSS (Payment Card Industry Data Security Standard)"