Уведомление о проведении закупочной процедуры

АО «ОХК «УРАЛХИМ» (далее - «Организатор») настоящим объявляет о проведении закупочной процедуры в форме запроса предложений (далее – «процедура») на оказание услуг по комплексному тестированию на проникновение корпоративной информационной системы.

Цель: Проведение независимой внешней оценки защищенности ИТ-инфраструктуры.

Выполнение работ по поиску путей проникновения внешнего нарушителя в ИТ-инфраструктуру Компании, анализу защищенности ИТ-инфраструктуры Компании от атак со стороны внутреннего нарушителя, анализ защищенности корпоративных беспроводных сетей и оценку осведомленности сотрудников в вопросах информационной безопасности в соответствии с приложенным Техническим заданием.

Для участия в процедуре юридическим лицам (далее – «Участник») необходимо зарегистрироваться в Ariba Network или войти в свою существующую учетную запись воспользовавшись ссылкой и следуя инструкциям http://www.uralchem.ru/purchase/tenders_Ariba/

После прохождения регистрации необходимо проинформировать организатора конкурентной процедуры для добавления Вашей компании в список участников.
Мосиенко Роман Борисович
по телефону: +7 (495) 721-89-89 (доб.12029) или
по электронной почте: roman.mosienko@uralchem.com.

Настоящее уведомление о проведении конкурентной процедуры в форме запроса предложений не является извещением о проведении конкурса (публичного конкурса) и не регулируется статьями 447—449, 1057—1061 Гражданского кодекса РФ.

Участник самостоятельно несет все расходы, связанные с подготовкой и подачей Предложения. Организатор не несет перед Участниками обязательств по компенсации понесенных расходов и по заключению договора по результатам проведения запроса предложений.

Для участия в закупочных процедурах, проводимых предприятием Группы «УРАЛХИМ» на портале SAP Ariba, Ваша компания соглашается с положениями и условиями «Соглашения участника», размещённого в Ariba Network.

Дата и время окончания приема Предложений: до 14.05.2021 г., 13-00 МСК.
Предложения, полученные позже установленного выше срока, будут отклонены Организатором процедуры без рассмотрения по существу, независимо от причин нарушения срока.
При необходимости Организатор, с уведомлением всех Участников, имеет право продлить срок окончания приема Предложений или изменить условия проведения конкурентной процедуры.

Требования, предъявляемые к участникам конкурентной процедуры:
• Участник должен предоставить подтверждение наличия необходимых компетенций для проведения соответствующих работ. В рамках данного требования оценивается наличие у участника конкурса квалифицированных специалистов, которых он предполагает привлекать для выполнения работ.
• Стоимость предложения указывается в рублях;
• Оплата работ по внедрению производится в течение 30 дней по факту приемки работ;
• Соответствие ТКП техническому заданию и критериям технической оценки.
• Участник должен иметь опыт оказания аналогичных услуг:
- в компаниях со штатной численностью персонала от 5000 человек за последние 3 года.
- в размере не менее 70 (пятидесяти) процентов от начальной (максимальной) цены договора, подлежащих оказанию за последние 3 года.

Перечень документов, которые должны предоставить участники конкурентной процедуры:
1. Коммерческое предложение с указанием стоимости работ по реализации требований ТЗ
2. План работ в соответствии с ТЗ по этапам с указанием трудозатрат, ставок и категорий привлекаемых специалистов
3. Подтверждение опыта оказания аналогичных услуг;

Сроки поставки/выполнения работ/услуг: 01.07.2021.

По всем дополнительным вопросам по проекту, просьба обращаться
Файзуллин Александр Игоревич – Руководитель управление информационной безопасности
по телефону: +7 (495) 721-89-89 (доб. 12060) или
по электронной почте: Alexander.Faizullin@uralchem.com

Приложения:
Техническое задание «Проведение работ по комплексному тестированию на проникновение ИТ-инфраструктуры АО «ОХК «УРАЛХИМ».

ТЕХНИЧЧЕСКОЕ ЗАДАНИЕ

ПРОВЕДЕНИЕ РАБОТ ПО КОМПЛЕКСНОМУ ТЕСТИРОВАНИЮ НА ПРОНИКНОВЕНИЕ ИТ-ИНФРАСТРУКТУРЫ АО «ОХК «УРАЛХИМ»

СОСТАВ РАБОТ

Для оценки защищенности ИТ-инфраструктуры Заказчика необходимо провести анализ защищенности, включающий следующие работы:

Внешнее тестирование на проникновение

Необходимо выполнить работы, направленные на поиск путей проникновения внешнего нарушителя в локальную вычислительную сеть (ЛВС) Заказчика с использованием уязвимостей и ошибок конфигурации сетевых устройств, а также доступных из сети Интернет сетевых служб и приложений. Внешнее тестирование на проникновение необходимо выполнить методом черного ящика, то есть со стороны нарушителя, не обладающего никакими сведениями и логическим доступом к информационным системам Заказчика. В ходе внешнего тестирования на проникновение требуется выполнить следующие работы:

- Собрать сведения о сетевом периметре на основе источников информации, доступных потенциальному нарушителю (поисковые системы, новости, конференции и т. п.);
- Выполнить сканирование узлов сетевого периметра, определить типов устройств, операционных систем, приложений по реакции на внешнее воздействие;
- Идентифицировать уязвимости сетевых служб;
- Выполнить анализ защищенности сервисов сетевой инфраструктуры и электронной почты, в том числе с использованием средств автоматического поиска уязвимостей;
- Выполнить анализ защищенности внешних корпоративных веб-приложений методом черного ящика, то есть со стороны нарушителя, не обладающего никакими сведениями и логическим доступом к системе.
- Выполнить анализ защищенности систем совместной работы (SharePoint, OWA, Confluence и др.)
- Провести квалифицированные bruteforce-атаки.

- Провести ручную верификацию уязвимостей и анализ защищенности доступных ресурсов (в том числе — анализ возможности эксплуатации известных уязвимостей устаревших версий ПО и сетевых служб, выявление чувствительных данных, хранящихся в открытом виде, выявление небезопасных конфигураций сетевого оборудования и серверов);
- Провести эксплуатацию уязвимостей с целью преодоления сетевого периметра, эскалации привилегий, получения несанкционированного доступа к информации;
- Провести тестирование сайтов и web-приложений:
    - Выполнить анализ веб приложения от имени аутентифицированного и анонимного пользователя.
    - Провести сканирование веб-приложения с использованием инструментальных средств (Acunetix WVS, BurpSuite Pro, W3AF, Nikto, sqlmap и др.)
    - Выполнить перебор значений параметризованных запросов.
    - Выполнить проверку обработки входных данных в веб-компонентах и возможности проведения следующих типов атак:
        - Внедрение операторов языка SQL (SQL Injection);
        - Включение локальных и удалённых файлов (LFI/RFI);
        - Внедрение кода на языке, интерпретируемом на стороне клиента (XSS);
        - Внедрение команд, интерпретируемых средой выполнения (Eval injection/Command injection);
        - Внедрение разметки на языке XML;
        - Внедрение заголовков (Header Injection)
        - Внедрение сериализованных объектов (Object Injection);
        - Подключение внешних XML-сущностей (XML External Entity);
        - Прочие атаки, целью которых является выполнение кода на стороне сервера.
    - Выполнить подбор паролей пользователей веб-приложения.
- Определить и описать меры противодействия, необходимые и достаточные для предотвращения успешно реализованных специалистами Исполнителя атак на ИТ-ресурсы и сервисы Заказчика со стороны внешнего нарушителя.

Внутреннее тестирование на проникновение

Необходимо выполнить анализ защищенности ИТ-инфраструктуры Заказчика от атак со стороны внутреннего нарушителя, обладающего правами и привилегиями рядового работника Заказчика и находящегося в пользовательском сегменте корпоративной ЛВС. Внутреннее тестирование на

проникновение осуществляются либо удаленно (с использованием ПО TeamViewer) либо непосредственно в офисе Заказчика специалистами Исполнителя. В рамках данного тестирования должны быть выполнены следующие работы:

- Собрать информации о доступных узлах внутренней сети;
- Провести сканирование узлов, доступных из заданного сегмента ЛВС, определить тип доступных устройств, операционных систем, приложений;
- Выполнить идентификацию уязвимостей сетевых служб;
- Выполнить анализ защищенности сервисов сетевой инфраструктуры;
- Оценить защищенности сети от атак на канальном уровне;
- Провести перехват и анализ сетевого трафика;
- Выявить явные недостатки в управлении доступом;
- Повести подбор паролей;
- Осуществить эксплуатацию наиболее опасных уязвимостей с целью выхода за границы пользовательского сегмента и дальнейшего развития атаки вплоть до получения привилегированного (административного) доступа к целевым компонентам ИТ-инфраструктуры Заказчика, таким как служба каталогов Active Directory, Сетевая инфраструктура, Инфраструктура открытого ключа, Системы обеспечения ИБ, СУБД, файловые серверы;
- Определить и описать меры противодействия, необходимые и достаточные для предотвращения успешно реализованных специалистами Исполнителя сценариев эскалации привилегий и реализации несанкционированного доступа к компонентам ИТ-инфраструктуры Заказчика со стороны внутреннего нарушителя.

Анализ защищенности беспроводных сетей

Анализ защищенности беспроводных сетей проводится на территории центрального офиса Заказчика (г. Москва, пресненская наб., д. 6 сроен. 2). В ходе этих работ необходимо выявить недостатки в использовании технологий беспроводного доступа (стандарты 802.11a/b/g/n/ac для диапазонов 2,4 и 5 ГГц) к ИТ-ресурсам Заказчика, а также недостатков в архитектуре и организации беспроводного доступа. При проведении анализа защищенности беспроводных сетей необходимо выполнить следующие работы:

- выявить недостатки в организации беспроводных сетей и недостатков конфигурации точек доступа и иного сетевого оборудования, позволяющие проводить атаки на сетевое оборудование, сети и клиентов сетей Заказчика;

- Установить наличие возможности получения неправомерного доступа к ресурсам ЛВС Заказчика со стороны пользователя беспроводных сетей Заказчика;
- Выявить несанкционированные точки доступа, функционирующие в офисе Заказчика;
- Провести анализ доступности беспроводных сетей Заказчика за пределами контролируемой зоны
- Определить и описать меры противодействия, необходимые и достаточные для предотвращения успешно реализованных специалистами Исполнителя сценариев получения несанкционированного доступа к компонентам ИТ-инфраструктуры Заказчика из обследованных беспроводных сетей.

Оценка осведомленности сотрудников в вопросах информационной безопасности

В рамках оценки осведомленности сотрудников в вопросах информационной безопасности необходимо провести тесты, эмулирующие распространенные сетевые атаки с использованием методов социальной инженерии:

- Проверка наличия в сети Интернет сведений, часто используемых при социотехнических атаках, в том числе - проверка публичных «утечек данных».
- Проверка настроек используемого программного обеспечения для противодействия социотехническим атакам.
- Рассылка сотрудникам электронных писем с приложенным офисным документом с активным содержимым.
- Рассылка сотрудникам электронных писем с приложенным исполняемым файлом.
- Рассылка сотрудникам электронных писем со ссылкой на фишинговый ресурс.
- Целевое общение с сотрудниками Заказчика через социальные сети, переход по ссылке [до 10 контактов].
- Телефонные звонки сотрудникам Заказчика с целью получения конфиденциальной информации или удаленного доступа [до 30 контактов].

МЕТОДИКА ПРОВЕДЕНИЯ РАБОТ

Работы должны проводиться методом черного ящика. Операции выполняются специалистами Исполнителя, находящимися в тех же условиях, что и потенциальный нарушитель. При выполнении работ необходимо основываться на следующих типах нарушителя:

- Высококвалифицированный внешний нарушитель
    - Действует из сети Интернет
    - не имеет легитимного доступа к каким-либо компонентам ИТ-инфраструктуры Заказчика
    - реализует атаки, направленные на получение доступа к одному или несколькими компонентам ИТ-инфраструктуры с возможностями, достаточными для организации атак на внутренние компоненты
- Высококвалифицированный внутренний нарушитель
    - имеет непривилегированный доступ некоторым компонентам ИТ-инфраструктуры Заказчика (в соответствии с типовыми задачами рядового работника Заказчика).
    - реализует атаки, направленные на получение несанкционированного привилегированного доступа к ключевым компонентам и функциям управления ИТ-инфраструктурой, несанкционированного доступа к защищаемой информации либо на вывод компонентов ИТ-инфраструктуры из строя
- Высококвалифицированный нарушитель беспроводного доступа
    - Имеет доступ к территории Заказчика
    - не имеет доступа к ЛВС Заказчика
    - не имеет привилегий в ИТ-инфраструктуре Заказчика
    - реализует атаки, направленные на получение доступа к одному или несколькими узлам ЛВС Заказчика с возможностями, достаточными для организации атак на внутренние компоненты ИТ-инфраструктуры.

Модель нарушителя «Высококвалифицированный внутренний нарушитель» применяется на этапе «Внутреннее тестирование на проникновение».

Модель нарушителя «Высококвалифицированный внешний нарушитель» применяется на этапе «Внешнее тестирование на проникновение».

Модель нарушителя «Высококвалифицированный беспроводного доступа» применяется на этапе «Анализ защищенности беспроводных сетей»

При проведении работ по тестированию на проникновение специалисты Исполнителя не располагают какими-либо предварительными данными об информационных системах Заказчика и используемой инфраструктуре.

Для каждого из этапов Заказчиком обеспечивается доступность всех исследуемых компонентов ИТ-инфраструктуры в соответствии с применяемой моделью нарушителя, а также организуется взаимодействие со специалистами Исполнителя и согласование временных рамок при проведении работ.

Работы по тестированию на проникновение должны проводится в период времени, согласованный с Заказчиком. Все действия Исполнителя, которые могут привести к нарушению функционирования ИТ-инфраструктуры Заказчика или другим негативным последствиям, должны в обязательном порядке согласовываться с ответственным представителем Заказчика.

Эксплуатация обнаруженных специалистами Исполнителя уязвимостей не должна приводить к уничтожению, блокированию, модификации, принадлежащей Заказчику, или к нарушению функционирования компонентов ИТ-инфраструктуры, если это отдельно не согласовано с Исполнителем.

При отсутствии успеха в преодолении защиты соответствующий этап завершается после исчерпания специалистами Исполнителя всех потенциально применимых в рамках данного этапа методов проведения атаки. В любом случае Заказчику должна предоставляться полная информация о действиях, выполнявшихся в ходе анализа защищенности, применявшихся методах атаки, выявленных недостатках, результатах использования наиболее серьезных недостатков и объективные свидетельства, подтверждающие как наличие недостатков, так и результаты их использования специалистами Исполнителя.

СОСТАВ РАБОТ

Ниже перечислен минимально-необходимый состав работ. Для достижения поставленных перед Исполнителем задач и повышения качества выполняемых работ данный перечень может быть существенно расширен.

Внешнее тестирование на проникновение

1. Анализ, систематизация и уточнение полученных от Заказчика исходных данных об области

исследования;

2. Конкретизация модели нарушителя для внешнего периметра;
3. Сбор информации о внешнем периметре (OSINT):
    a. Выявление связанных автономных систем (BGP ASN);
    b. Получение данных из поисковых систем общего назначения;
    c. Получение данных из специализированных поисковых систем;
    d. Определение используемых доменных имен;
    e. Поиск поддоменов;
    f. Анализ публичных утечек данных;
4. Автоматизированное сетевое сканирование:
    a. Выявление открытых сетевых портов;
    b. Идентификация сетевых устройств;

    c. Идентификация используемых сервисов и их версий;
    d. Идентификация используемых типов и версий ОС;
    e. Первичное выявление потенциальных уязвимостей;
5. Анализ результатов сканирования;
6. Выявление сетевых сервисов, допускающих утечку информации;
7. Выявление административных и привилегированных интерфейсов сервисов;
8. Сбор данных о взаимодействии хостов и их сервисов;
9. Обнаружение сервисов и анализ их функциональности;
10. Выявление и проверка общеизвестных уязвимостей;
11. Выявление и проверка ошибок конфигурации;
12. Анализ защищенности интерфейсов и средств удаленного доступа;
13. Анализ защищенности используемых сетевых устройств;
14. Анализ защищенности корпоративных ресурсов и сервисов:
    a. Почтовые службы;
    b. Средства удаленного доступа (VPN);
    c. Средства администрирования;
    d. Службы файлообмена;
    e. Информационные порталы;
    f. Бизнес-приложения;
    g. IP-телефония и прочие средства корпоративной коммуникации;
15. Анализ защищенности обнаруженных веб-приложений:
    a. Поиск общеизвестных уязвимостей в веб-приложениях;
    b. Проверка с использованием специализированных средств;
    c. Проверка с использованием методик OWASP;
16. Анализ защищенности иных сервисов, выявленных на сетевом периметре;
17. Проверка стойкости аутентификационных данных для обнаруженных сервисов:
    a. Перебор стандартных учетных данных;
    b. Составление контекстных словарей для перебора;
    c. Проведение атак перебора по словарю;
18. Выявление фактов переиспользования скомпрометированных учетных записей;
19. Выявление специфичных свойств инфраструктуры, негативно влияющих на безопасность;
20. В случае компрометации сервисов на внешнем периметре проводится:
    a. Проверка возможности получения доступа уровня пользователя ОС;
    b. Проверка возможности повышения привилегий;
    c. Проверка возможности развития атаки на связанные сервисы и ресурсы;

    d. Проверка возможности развития атаки на внутреннюю инфраструктуру Компании;
21. Разработка возможных сценариев атаки на основании выявленных уязвимостей;
22. Проверка возможности реализации разработанных сценариев;
23. Анализ полученных результатов, оценка критичности выявленных уязвимостей;
24. Разработка рекомендаций по устранению выявленных недостатков безопасности системы;
25. Составление отчета о выполненной работе.

Внутреннее тестирование на проникновение

1. Анализ, систематизация и уточнение полученных от Заказчика исходных данных о внутренней инфраструктуре;
2. Анализ внутренней сети и элементов инфраструктуры:
    a. Анализ правил сегментации и структуры сети;
    b. Поиск и сканирование доступных хостов;
    c. Поиск и сканирование сетевых устройств;
    d. Сканирование и идентификация сервисов, анализ их функциональности;
    e. Выявление административных или иных привилегированных интерфейсов сервисов;
    f. Определение общедоступных сетевых ресурсов;
    g. Выявление версий ОС и ПО на доступных хостах.
3. Выявление наиболее опасных факторов и значимых угроз информационной безопасности, воздействующих на систему;
4. Конкретизация модели нарушителя для внутренней инфраструктуры;
5. Разработка возможных сценариев атаки;
6. Поиск возможных утечек информации:
    a. Конфигурация серверов, сетевых устройств и других компонентов сети;
    b. Учетные данные пользователей;
    c. Конфиденциальная информация на сетевых ресурсах.
7. Поиск общеизвестных уязвимостей для выявленных версий ОС и ПО, в том числе автоматизированными методами;
8. Выявление ошибок конфигурации серверов, сетевых устройств и других компонентов сети;
9. Проверка выявленных уязвимостей и ошибок конфигурации;
10. Сбор данных о взаимодействии с сервисами со стороны пользователей или других сервисов:
    a. Анализ сетевых протоколов взаимодействия;
    b. Анализ конфигурации защищенного обмена информации.

11. Проверка возможности реализации MITM-атак (Man In the Middle):
    a. Спуфинг сетевых протоколов (ARP, DHCP, NetBIOS, mDNS, LLMNR и другие);
    b. Получение учетных данных, хэшей паролей или иной конфиденциальной информации.
12. Проверка стойкости аутентификационных данных пользователей сервисов:
    a. Анализ парольных политик;
    b. Проверка стандартных учетных данных и простых словарных паролей на сервисах;
    c. Проведение bruteforce-атак на полученные хэши паролей пользователей.
13. При компрометации сервисов производится попытка повышения привилегий в ОС с последующим получением дополнительных учетных данных;
14. Проверка возможности реализации атак на доменную инфраструктуру:
    a. Анализ настроек доменной конфигурации и взаимодействия между доменами;
    b. Получение всей доступной информации о пользователях, компьютерах и сессиях в домене
    c. посредствам протоколов LDAP и SMB;
    d. Анализ групповых политик;
    e. Поиск небезопасных конфигураций привилегий для разных групп и пользователей домена;
    f. Проверка возможности проведения специфичных атак: NTLM-Relay, Pass-the-hash, Kerberoasting и другие;
    g. Проверка возможности повышений привилегий при текущей конфигурации домена.
15. Выявление специфичных свойств внутренней инфраструктуры, негативно влияющих на безопасность;
16. Проверка возможности повышения привилегий в сети и дальнейшего развития атаки с целью получения максимальных логических привилегий путем:
    a. Получения административного доступа к контроллеру домена;
    b. Захвата контроля над максимальным количеством хостов;
    c. Получения доступа к серверам, используемым для централизованной аутентификации.
17. Анализ полученных результатов, оценка критичности выявленных уязвимостей;
18. Разработка рекомендаций по устранению выявленных недостатков безопасности системы;
19. Составление отчета о выполненной работе

Анализ защищенности беспроводных сетей

1. Анализ мощности вещания беспроводных точек доступа;
2. Построение карты покрытия беспроводной сети;
3. Выявление развернутых беспроводных сетей;
4. Выявление беспроводных сетей со скрытым ESSID;
5. Анализ использования механизмов защиты беспроводных сетей;
6. Анализ используемых средств, ограничивающих подключение к сети;
7. Проверка возможности обхода используемых ограничений;
8. Захват и анализ беспроводного трафика в пассивном режиме;
9. Проверка возможности подключения к беспроводной сети, представляясь другим устройством;
10. Проверка возможности восстановления пароля из захваченного трафика в пассивном режиме;
11. Проверка возможности реализации атаки CAFFE LATTE;
12. Проверка возможности реализации атаки CHOP-CHOP;
13. Анализ конфигурации беспроводных сетей WPA Enterprise;
14. Анализ используемых средств подтверждения подлинности точки доступа;
15. Создание ложной точки доступа;
16. Проверка возможности подключения клиентов к ложной точке доступа;
17. Проверка возможности захвата аутентификационных данных пользователей;
18. Проверка возможности реализации атаки типа «человек посередине»;
19. Выявление, перечисление подключенных к беспроводной сети устройств;
20. Проверка возможности принудительной деаутентификации;
21. Захват сессии аутентификации в пассивном режиме;
22. Захват сессии аутентификации с применением принудительной деаутентификации клиента;
23. Проверка стойкости пароля путем перебора захваченной сессии аутентификации с использованием
1. словаря;
24. Проверка стойкости пароля путем перебора захваченной сессии аутентификации (brutforce);
25. Выявление точек доступа, использующих механизм WiFi Protected Setup;
26. Проверка возможности подбора WPS PIN;
27. Проверка возможности обхода механизмов защиты от подбора WPS PIN;
28. Проверка возможности реализации атак Pixie Dust;
29. Проверка возможности реализации атаки KRACK;

30. Проверка возможности реализации атаки с использованием PMKID;
31. Проверка сегментации и изоляции «гостевых» беспроводных сетей;
32. Проверка возможности доступа в КИС через «гостевые» беспроводные сети;
33. Сбор и анализ полученных результатов;
34. Составление отчета о выполненной работе.

Оценка осведомленности сотрудников в вопросах информационной безопасности

1. Поиск информации о сотрудниках компании в общедоступных источниках, социальных сетях;
2. Разработка сценариев взаимодействия с пользователями через средства обмена сообщениями - мессенджеры (Skype, Telegram, WhatsApp и др.);
3. Разработка сценариев взаимодействия с пользователями посредством соцсетей (если они используются компанией официально);
4. Разработка сценариев для почтовых рассылок;
5. Разработка фишинговых ресурсов;
6. Проверка дополнительных возможностей для проведения атак (подделка адресов почты, выявление критичных внешних ресурсов, атаки на перебор учетных данных);
7. Выявление возможных векторов атак на инфраструктуру компании через сотрудников компании;
8. Проведение целенаправленной атаки на сотрудников (e-mail рассылка) с целью выполнения вложения на ПК сотрудников;
9. Проведение целенаправленной атаки на сотрудников (рассылка через мессенджер) с целью выполнения вложения на ПК сотрудников;
10. Проведение таргетированной атаки на сотрудников путем совершения звонков на телефоны с целью развития других атак;
11. Проведение нетаргетированной атаки путем распространения брендированных под Заказчика USB накопителей на территории заказчика с целью выполнения несанкционированных действий на ПК сотрудников Заказчика;
12. Проведение целенаправленной атаки на сотрудников (e-mail рассылка) для заманивания/привлечения сотрудников на фишинговый сайт с целью компрометации учетных записей;
13. Проведение целенаправленной атаки на сотрудников (рассылка через мессенджер) для заманивания сотрудников на фишинговый сайт с целью компрометации учетных записей;
14. Проведение целенаправленной атаки на сотрудников (рассылка через соцсети) для заманивания сотрудников на фишинговый сайт с целью компрометации учетных записей;

15. Анализ защищенности системы контроля и управления доступом (СКУД);
16. Проведение атак на сотрудников (личная беседа) с целью получения учетных записей, технических аккаунтов, паролей от Wi-Fi сетей;
17. Закрепление и дальнейшее проникновение в систему;
18. Анализ полученных данных;
19. Составление отчета, содержащего информацию о действиях каждого сотрудника (открытие письма, переход на фишинговый сайт, ввод учетных данных, запуск вредоносного вложения)

Отчетные материалы

по результатам тестирования на проникновение должна быть проведена оценка общего уровня защищенности ИТ-инфраструктуры Заказчика по различным направлениям информационной безопасности, позволяющая определить, насколько эффективны используемые меры защиты. Должны быть даны всесторонние оценки уровня защищенности как по выявленным векторам проникновения, так и с учетом применяемых механизмов защиты. В рамках отчетных материалов должны быть перечислены не только выявленные уязвимости и приведены описания проведенных работ, но и предоставлены аналитические выводы о существующих угрозах ИБ, выполнена оценка возможного влияния их реализации на ИТ-инфраструктуру Заказчика, проведено ранжирование выявленных недостатков по уровню риска (согласно метрикам CVSS v3), приведены графические отображения выявленных векторов атак на схемах, даны рекомендации по устранению всех выявленных недостатков.

По результатам проекта Заказчику должна быть предоставлена объективная и независимая оценка защищенности ИТ-инфраструктуры, позволяющая определить, насколько эффективны на практике применяемые меры защиты информации.

В состав отчетных материалов должны входить следующие документы:

1. Отчет о результатах комплексного тестирования на проникновение — подготавливается по окончании комплексного тестирования на проникновение и должен содержать:
    - общие сведения о проведенном тестировании на проникновение;
    - результаты проведенных проверок;
    - развернутые технические выводы;
    - оценку состояния защищенности ИТ-инфраструктуры Заказчика как с точки зрения потенциальных векторов проникновения, так и с точки зрения используемых механизмов защиты;
    - перечень и описание существующих угроз;

- графическое отображение всех выявленных векторов атак с оценкой сложности их реализации;
- выводы по анализу уязвимостей в веб-приложениях и методам их нейтрализации;
- описание хода работ, выявленных уязвимостей, ранжирование их по степени потенциальной опасности, вероятности их использования, описание последствий реализации выявленных уязвимостей;
- перечень скомпрометированных в рамках работ компонентов ИТ-Инфраструктуры Заказчика;
- рекомендации по устранению выявленных уязвимостей, в том числе 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;
- результаты эксплуатации нескольких критически опасных уязвимостей, включая информацию о полученном уровне привилегий в ИТ-инфраструктуре Заказчика на различных этапах тестирования.

2. Отчет о результатах оценки осведомленности сотрудников в вопросах информационной безопасности — подготавливается по окончании работ по оценке осведомленности сотрудников в вопросах информационной безопасности и должен содержать содержит:
   - оценку эффективности программы повышения осведомленности;
   - статистику по каждому из типов атаки и действиям пользователей;
   - перечень сотрудников, недостаточно осведомленных в вопросах информационной безопасности;
   - полученные в рамках работ учетные данные и информацию о версиях используемого ПО.
3. Краткий отчет для Руководства Заказчика — готовится на основе двух предыдущих отчетов и содержит краткое описание проведенных работ, суммаризованное описание достигнутых Исполнителем результатов, обобщённые выводы о состоянии защищенности ИТ-инфраструктуры Заказчика и осведомленности сотрудников в вопросах информационной безопасности.