Отчет по тестированию на проникновение

Bank

xx.xx.2023

Краткое содержание

Команда пентестеров компании SkillFactory провела внешнее и внутреннее тестирование на проникновение в рамках оказания услуг по поиску уязвимостей, оценки поверхности атак и проверки реализации рисков.

В ходе тестирования командой Skillfactory были применены реальные методы для проведения атак которые на текущий момент времени являются актуальными и используются известными APT (Advanced Persistent Threat). Последовательность действий в рамках этого подхода включает сбор данных из открытых источников (OSINT), энумерацию, эксплуатацию и проведение атаки на конкретные цели для достижения конкретных оперативных результатов.

Данное тестирование на проникновение включало в себя следующие цели:

* Произвести оценку степени защищенности исследуемых ресурсов;
* Составить план действий для минимизации ущерба и снижению или ликвидации рисков для заказчика;
* Подготовить список необходимых мер и средств защиты для снижения поверхности атаки на ресурсы заказчика

Конкретные замечания по этой оценке изложены в разделе "Замечания и рекомендации" настоящего отчета. Ниже приводится краткое резюме этих замечаний:

* Устаревшие версии сервисов, используемых на ресурсах компании
* Большое количество уязвимостей с оценкой “Критично” и “Высокий” уровнями угрозы
* Отсутствие контроля версий ПО и кода
* Отсутствие строгой сегментации IT инфраструктуры средствами межсетевого экранирования
* Недостаточный уровень базовых механизмов защиты инфраструктуры
* Отсутствие мониторинга безопасности ресурсов
* Как следствие отсутствия мониторинга, также отсутствие реагирования на инциденты безопасности

Ниже приводится краткая информация о целях и задачах, поставленных команде пентестеров, в частности:

* Получение доступа к конфиденциальной информации
* Выявление возможных каналов утечек со стороны внешнего атакующего
* Получение административных прав доступа к инфраструктуре
* Получение данных о поверхности атаки и рисках

Далее приводятся общие рекомендации по уменьшению рисков, выявленных в ходе исследования:

* Устаревшие версии сервисов, используемых на ресурсах компании и отсутствие контроля версий операционных систем несут риски компрометации данных компании.   
  Для ликвидации риска рекомендуется ввести систему, следящую за уязвимостями и обязать сотрудников являющихся администраторами систем, следить за актуальностью версий ОС и сервисов
* Отсутствие контроля за основными каналами утечки данных в рамках внешнего и внутреннего нарушителя. Для минимизации риска необходимо внедрить комплекс из ПО и процессов по детектированию данного типа угроз с основным аспектом на повышение “прозрачности” управления жизненным циклом данных
* В случае использования персонализированных девайсов (смартфоны, ноутбуки, рабочие станции и.т.д) рекомендуется внедрить модель управления Нулевого Доверия (Zero Trust), что позволит избежать неконтролируемых или “невидимых” атак как со стороны внешнего нарушителя, так и со стороны внутреннего нарушителя. Данная модель включает в себя комплекс процессов и ПО, которые рекомендуется для внедрения.
* Отсутствие защиты внешнего периметра в рамках текущий архитектуры может привести к атакам типа “конкурентная разведка” и атаки со стороны операторов шифровальщиков. Чтобы снизить риск данных атак необходимо разделить системы на несколько сегментов с применением подхода эшелонированной защиты. Один из быстрых и возможных шагов - использовать WAF (Web Application Firewall) для защиты веб-ресурсов
* Рассмотреть возможность пересмотра IT архитектуры, опираясь на полученные данные после анализа поверхности атаки для получения процесса BCDR - Business continuity (BC) and disaster recovery (DR)

В разделе "Замечания и рекомендации" настоящего доклада команда представила конкретные рекомендации по уменьшению рисков, связанных с этими вопросами.

SkillFactory ценит возможность поддержки Bank с его компьютерной безопасности. Мы будем рады помочь вам и ИТ-персоналу Bank в будущих начинаниях.

Оглавление

Раздел Страница

[**1 Методология и цели 6**](#_30j0zll)

[**2 Сценарий и скоуп 7**](#_1fob9te)

[2.1 Сценарий 7](#_3znysh7)

[2.2 Скоуп 7](#_2et92p0)

2.2.1 Прочее 7

[**3 Нарратив атаки 8**](#_tyjcwt)

[3.1 Общая схема атаки (внешний периметр) 8](#_3dy6vkm)

[3.2 Общая схема атаки (внутренний периметр) 8](#_1t3h5sf)

[3.3 Оценка уровня защищенности 8](#_4d34og8)

[3.4 Анализ внешнего периметра 9](#_2s8eyo1)

[3.4.1 Miss Configuration SSH 9](#_17dp8vu)

[3.5 Реализация вектора через почту скомпрометированного пользователя 10](#_35nkun2)

[3.5.1 Получение первичных данных необходимых для входа 10](#_1ksv4uv)

[3.5.2 Email адреса 11](#_3j2qqm3)

[3.5.3 Получение пароля в слитых данных сторонних сервисов 11](#_1ci93xb)

[3.5.4 Осуществление входа в доступные ресурсы скомпрометированного пользователя 12](#_3as4poj)

[3.5.5 Получение доступа к данным из электронной почты, Teams и календарей 13](#_147n2zr)

[3.5.6 Рассылка фишинговых писем 13](#_32hioqz)

[3.6 Реализация вектора через компрометацию учетных записей со слабыми паролями в домене bank.local.INT 14](#_1v1yuxt)

[3.6.1 Изначальный доступ 14](#_4f1mdlm)

[3.6.1.1 Получение изначального доступа с первичным обходом средств защиты 14](#_2u6wntf)

[3.6.2 Обход антивирусной защиты 16](#_nmf14n)

[3.6.3 Повышение привилегий 18](#_2lwamvv)

[3.6.3.1 Повышение привилегий через уязвимый сервис 18](#_111kx3o)

[3.6.3.2 Повышение привилегий через технику uac-schtasks 19](#_2zbgiuw)

[3.6.4 Активное сканирование 20](#_sqyw64)

[3.6.4.1 Сканирование сети 20](#_3cqmetx)

[3.6.4.2 Проксирование трафика 21](#_1664s55)

[3.6.5 Сбор данных о домене и приоритезация целей 22](#_1jlao46)

[3.3.8.1 Атака DcSync 28](#_1baon6m)

[3.3.8.2 Дамп паролей пользователей 29](#_39kk8xu)

[3.3.8.3 Brute Force атака на hash паролей 30](#_3mzq4wv)

[**4 Замечания и рекомендации 31**](#_1gf8i83)

[4.1 Замечание #1 Vulnerability Management 31](#_40ew0vw)

4.1.1 Рекомендация 31

[4.2 Замечание #2 Insufficient network access 31](#_2fk6b3p)

4.2.1 Рекомендация 31

[4.3 Замечание #3 Weak Password Policy 31](#_upglbi)

4.3.1 Рекомендация 31

[5 Замечание #3 2FA is not presented 31](#_3ep43zb)

[5.1 Рекомендация 31](#_1tuee74)

[5.2 Замечание #4 Active Directory bad configuration 32](#_4du1wux)

5.2.1 Рекомендация (Опционально) 32

[5.3 Замечание #5 Отсутствие адекватных мер реагирования и сдерживания атакующих 32](#_2szc72q)

5.3.1 Рекомендация (Опционально) 32

[**6 Заключение 33**](#_184mhaj)

# Методология и цели

Команда тестирования на проникновение использует методы реального атакующего для нацеливания на тестируемые системы. Так же команда тестирования на проникновение использует модель Red Team, имитирующую инструменты, техники тактики и процедуры реального противника (TTPs), основанные на сценариях и целях атаки. В отличие от традиционного теста на проникновение, модель Red Team позволяет тестировать всю сферу безопасности организации, включая людей, процессы и технологии.

Во время тестирования были использованы три основные фазы Red Team, чтобы в полном объеме имитировать реальную угрозу. Инфльтрация, закрепление и достижение цели. Последовательность действий при таком подходе включает сбор данных с открытым исходным кодом (OSINT), проведение энумерации, эксплуатацию и непосредственно атаку на необходимую цель. Информация, собранная во время сбора данных OSINT, используется в сочетании с пассивным и активным методами энумерации. Информация о энумерации обычно содержит подробные сведения о конкретном оборудовании, службах и программном обеспечении, запущенных на удаленных компьютерах. Следующий этап включает анализ всей накопленной информации для выявления потенциальных векторов атак. Если уязвимость может быть использована, операторы пытаются получить дополнительный доступ к сети или системе и собрать конфиденциальную системную информацию, чтобы создать эффект и продемонстрировать воздействие на клиента. Были использованы проверенные инструменты, методологии и опыт оператора, чтобы предотвратить непреднамеренные сбои в работе, ухудшение качества или отказ в обслуживании клиента.

Поставленные цели:

* Анализ поверхности атаки
* Выявление наиболее быстрых и эффективных возможностей для атаки
* Определение точек роста и снижение количества уязвимостей с применением лучших практик

# Сценарий и скоуп

## Сценарий

Основной сценарий подразумевал, что операторы команды пентестеров основываются на предполагаемой модели взлома с использованием сервера управления для сокрытия своего присутствия в периметре клиента. Для основной части тестирования была использована фишинговая атака внутри периметра (Internal Spear Phishing) от лица одного из скомпрометированных сотрудников. Подход, основанный на модели предполагаемого взлома, позволяет быстро начать проверку и позже использовать доступ, полученный в результате фишинговой атаки, для проверки правильности действий.

## Скоуп

Скоуп исследования Bank включал в себя следующие данные:

**Внешний скоуп**

Пул IP Адресов:

| xxx.xxx.xxx.xxx/xx |
| --- |

**Внутренний скоуп**

Пул IP Адресов:

| xxx.xxx.xxx.xxx/xx  xxx.xxx.xxx.xxx/xx |
| --- |

### Прочее

Далее будут перечислены интересные находки которые так или иначе могут быть использованы для развития новых векторов атак. Cписок таких находок:

Интересные находки

# Нарратив атаки

В следующем разделе описывается последовательность событий и выделяются ключевые моменты в ходе реализации векторов атак.

## Общая схема атаки (внешний периметр)

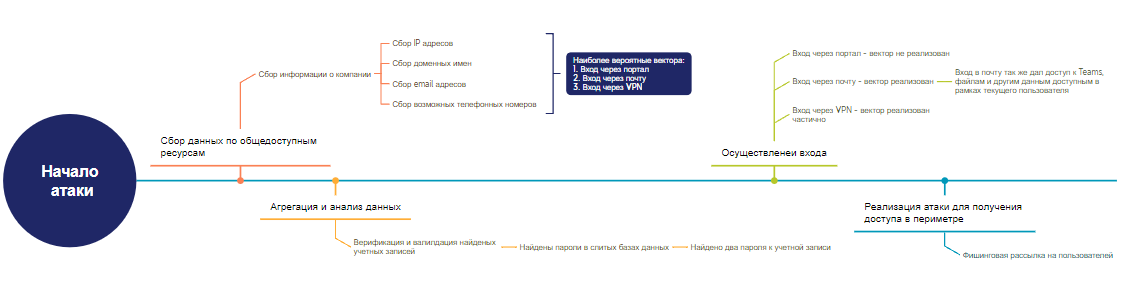
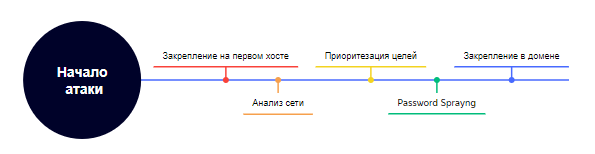


Рисунок 1: Общий ход атаки (внешний периметр)

## Общая схема атаки (внутренний периметр)



## Оценка уровня защищенности

На основе полученных данных и реализованных векторов атак команда SkillFactory оценивает следующим образом:

**Внешний периметр** - средний уровень защищенности

**Внутренний периметр** - низкий уровень защищенности

## Анализ внешнего периметра

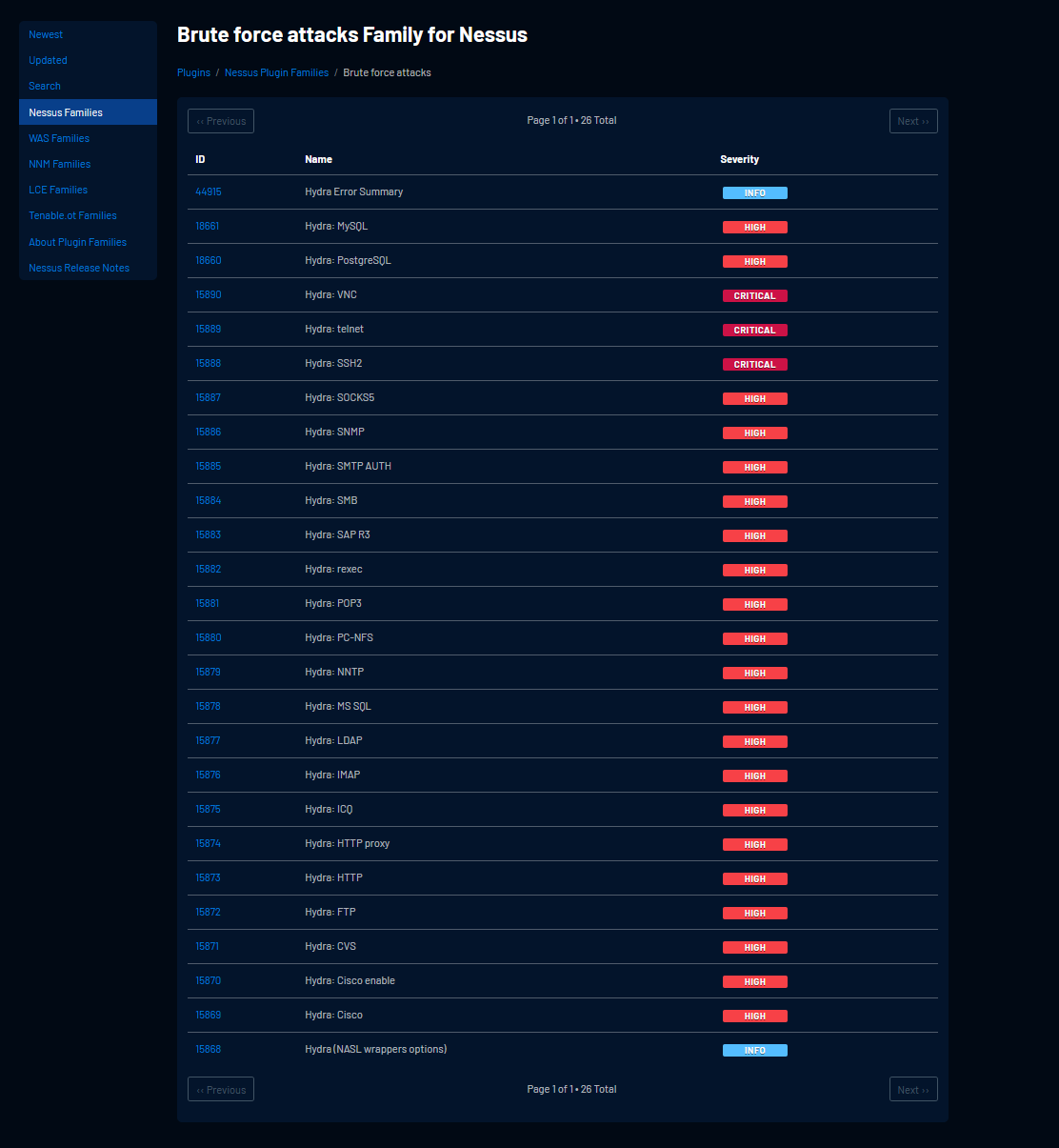
### Miss Configuration SSH

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Средняя

В ходе анализа внешнего периметра операторам удалось обнаружить большое количество хостов с неверно настроенным SSH сервером. В данном случае можно осуществлять атаку перебора паролей, так как отсутствует авторизация по ключам.



## Реализация вектора через почту скомпрометированного пользователя

### Получение первичных данных необходимых для входа

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Низкая

В ходе проведения разведки методами OSINT были обнаружены следующие данные:

1. email адреса
2. социальные сети
3. чувствительные данные в общем доступе

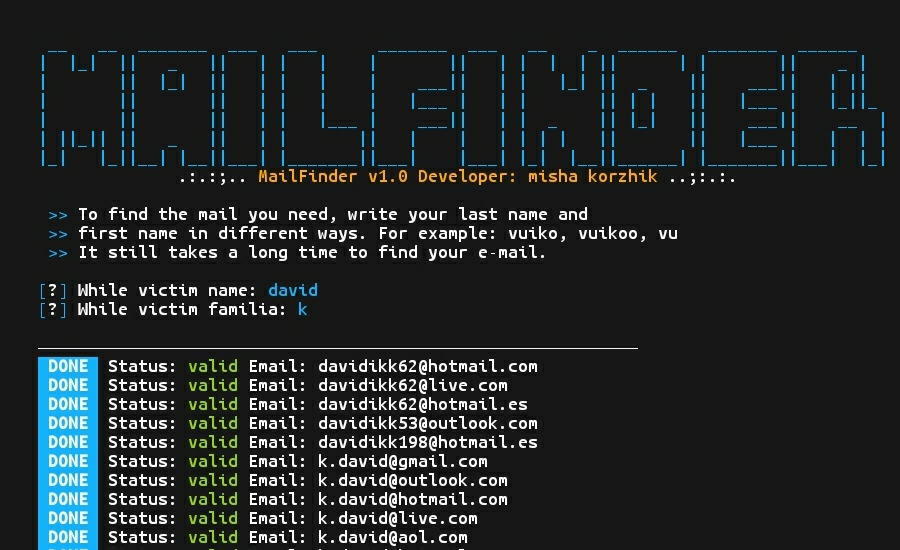


Рисунок 2: <DESCRIPTION>

### Email адреса

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Низкая

Исходя из полученных данных, операторы смогли составить список email адресов

тут список email ^^

### Получение пароля в слитых данных сторонних сервисов

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Высокая

В доступных источника для пользователя user@user.user было обнаружено 2 пароля:

1. Pass123
2. QWerty1234

Исходя из полученных данных, операторы пришли к выводу что это один из представителей топ менеджмента компании.

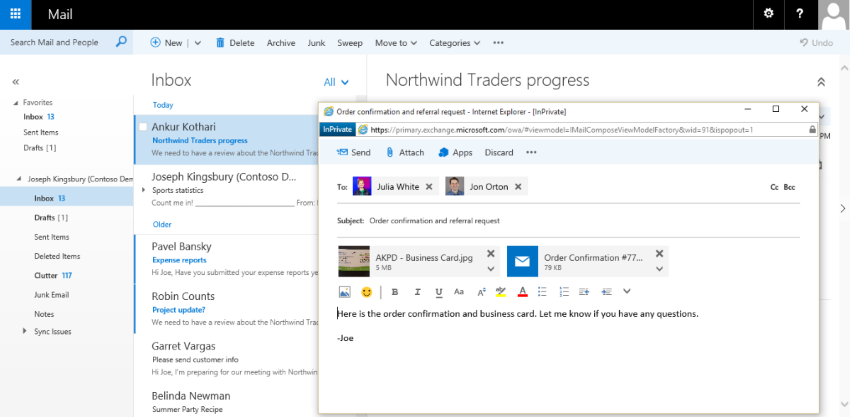
### Осуществление входа в доступные ресурсы скомпрометированного пользователя

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Высокая

В конечном итоге актуальным был второй пароль, который открыл доступ к корпоративным системам. Первый оказался невалидным и в дальнейшем никак не использовался для проведения развития атаки. Первый вход был осуществлен через сайт После этого операторы при помощи методики GAL смогли узнать нейминги и доменное имя для входа в owa



### Получение доступа к данным из электронной почты, Teams и календарей

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Высокая

Изучив наличие команд и групп в переписках, операторы приняли решение провести атаку Internal Spear Phishing, что в свою очередь позволяло в дальнейшем скомпрометировать другие учетные записи и закрепиться на компьютере одного из пользователей.

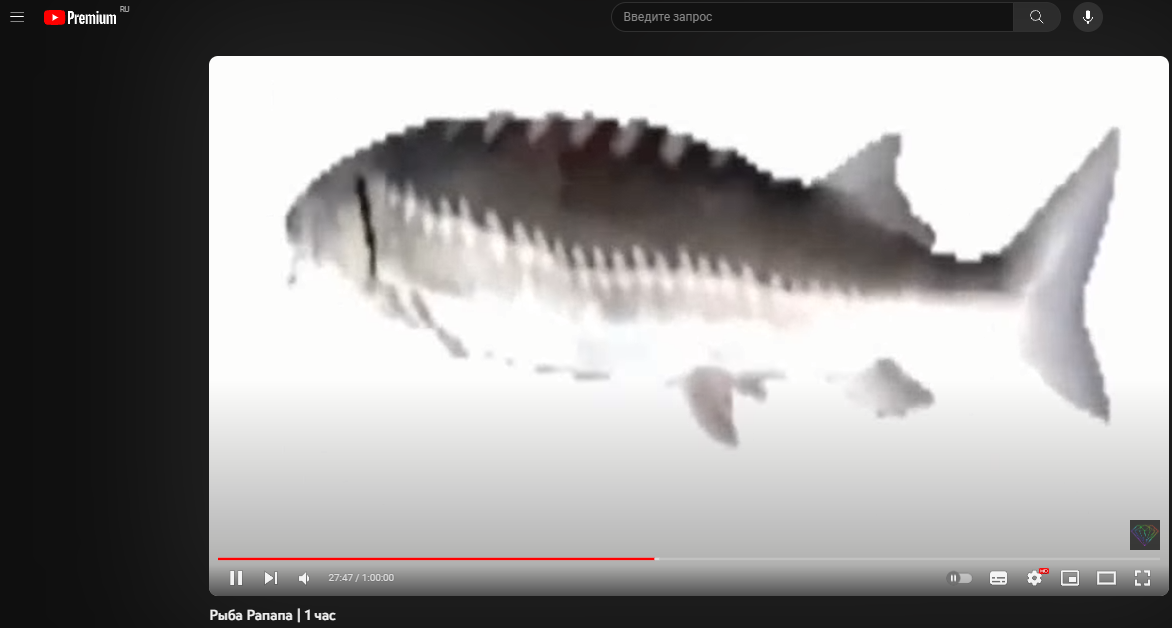
### Рассылка фишинговых писем

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Высокая

Для проведения атаки Internal Spear Phishing операторами был выбран безвредный payload - видео с рыбкой на youtube.



Далее операторы подготовили письмо на всех пользователей в компании с маскированием оригинальной ссылки которая указывала на address

После отправки были получены множественные переходы по ссылке.

| Figure 1: <DESCRIPTION> |
| --- |
|  |

## Реализация вектора через компрометацию учетных записей со слабыми паролями в домене bank.local.INT

### Изначальный доступ

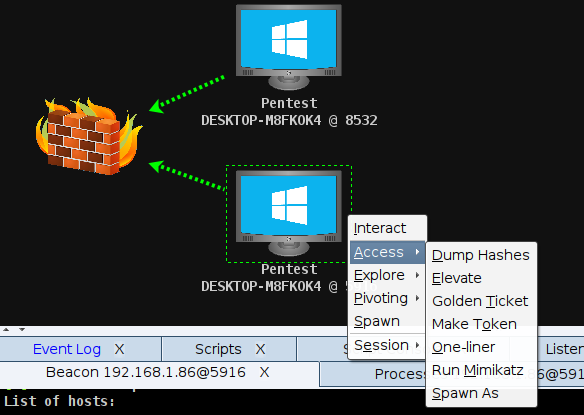
#### Получение изначального доступа с первичным обходом средств защиты

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Низкая

Для закрепления в первой итерации был запущен fileless агент для первичного сбора данных с обходом текущих средств антивирусной защиты.



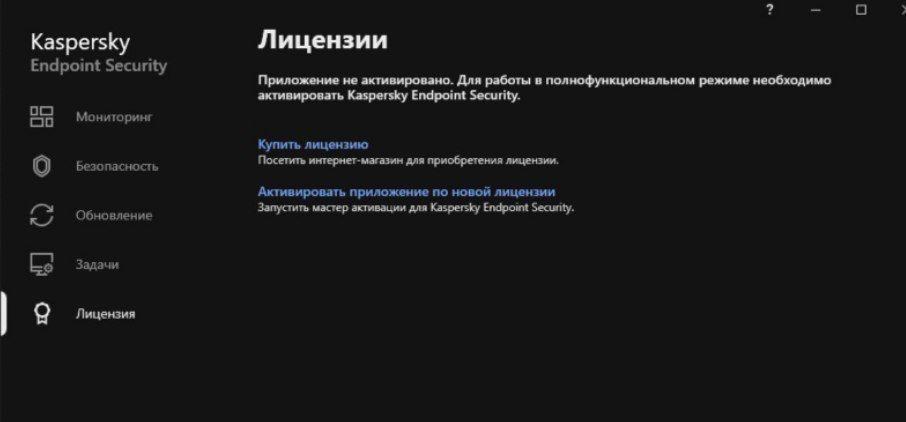
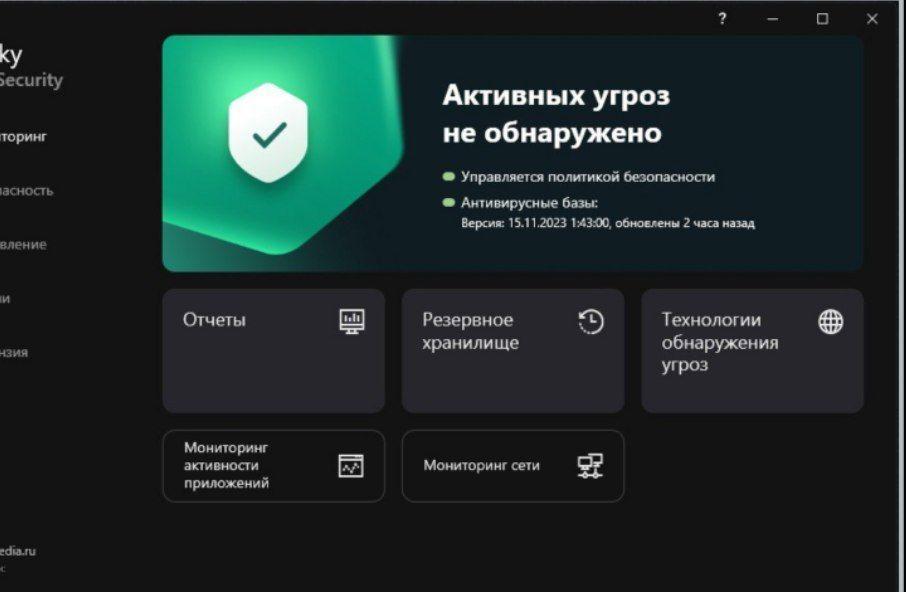
### Обход антивирусной защиты

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Высокая

Для обхода антивирусной защиты применялась техника эксплуатирования miss configuration. В данном случае операторам удалось выявить что в решении KES используются неверно настроенные политики управления лицензиями. Это позволило операторам удалить текущую лицензию для антивируса, что в свою очередь отключает механизмы самозащиты антивируса.

****

После этого операторы исполнителя произвели удаление KES штатными средствами Kavremover что позволило в дальнейшем не использовать сложные техники обхода средств защиты.

### Повышение привилегий

#### Повышение привилегий через уязвимый сервис

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Средняя

Для повышения привилегий операторы заказчика использовали уязвимость **Unquoted Service Paths** которая была обнаружена в одном из агентов заказчика. Данный агент был изучен на подтверждение наличия уязвимости при помощи процесса декомпиляции.

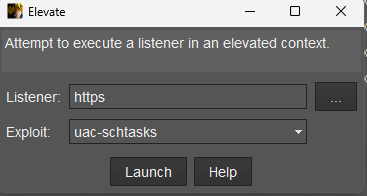
#### Повышение привилегий через технику uac-schtasks

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Средняя

Также для поднятия привилегий на конечном хосте, операторами была реализована атака uac-schtasks которая позволила повысить свои привилегии в системе до уровня NT AUTHORITY\SYSTEM

****

****

### Активное сканирование

#### Сканирование сети

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Низкая

Для понимания и приоритизации целей, операторами было проведено сканирование нескольких подсетей.

****

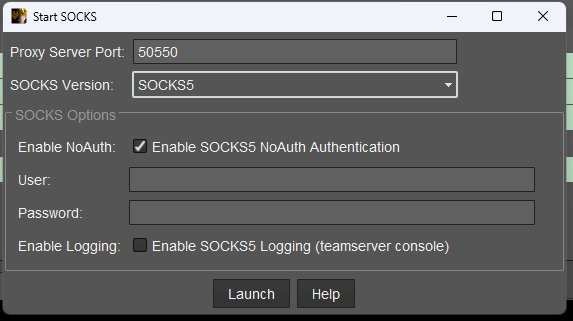
#### Проксирование трафика

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Средняя

Для получения доступа в недоступные сегменты операторы использовали проксирование трафика на скомпрометированных машинах. Каждый скомпрометированный хост выступал прокси-сервером, что позволило в дальнейшем сохранить доступ даже в условиях потери контроля над изначальным устройством.



##### 

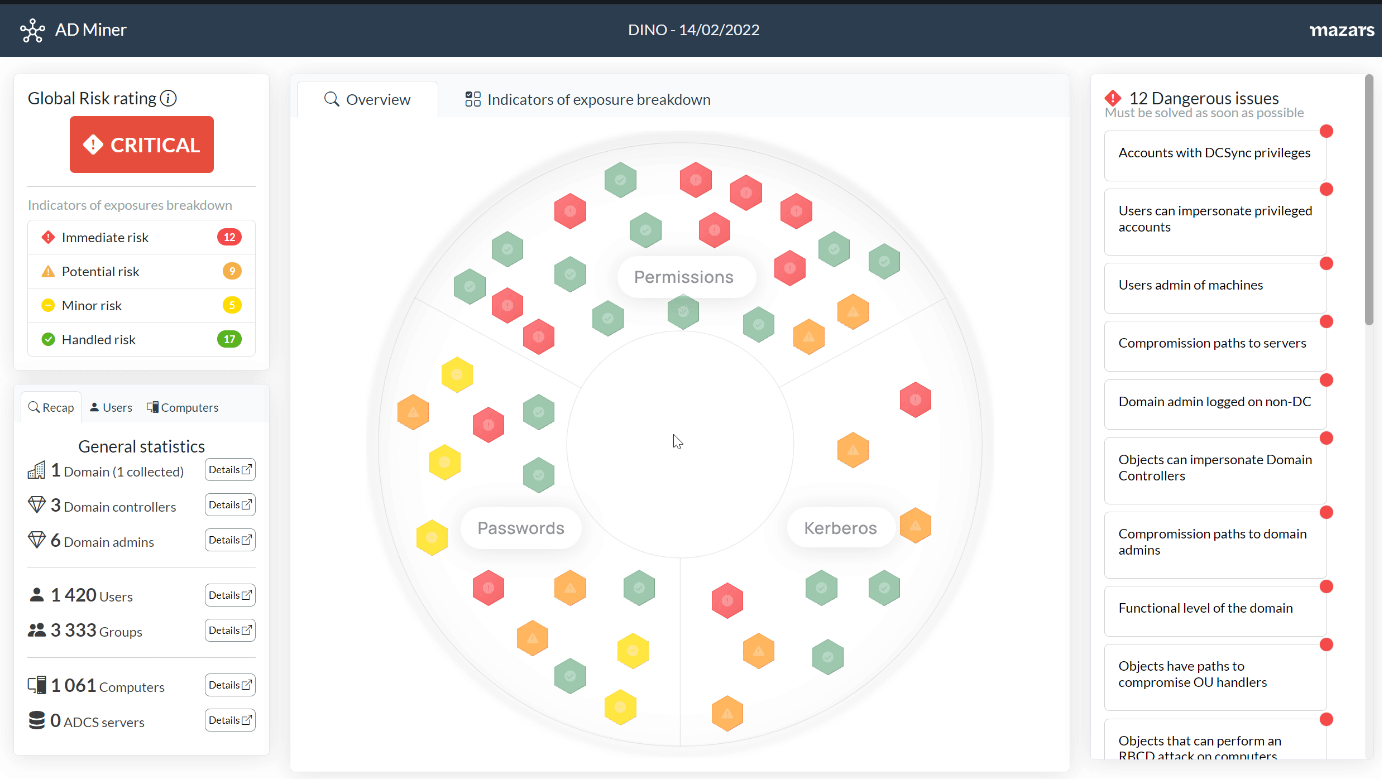
## Сбор данных о домене и приоритезация целей

После повышения привилегий на конечном хосте при помощи утилиты SharpHound была собрана детальная информация о домене, что в дальнейшем позволило выявить наиболее незащищенные места для реализации векторов атаки.

Исходя из полученных данных операторы приоритизировали вектора в цель получения прав администратора домена при помощи эксплуатирования уязвимостей или поиска miss configuration.

Вектора которые находились в приоритете:

1. Password Spraying
2. NTLM Relay (KrbRelayUP)
3. Exchange RCE

****

**3.3.1 Реализация атаки Password Spraying**

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Средняя

На основе ранее полученных данных из домена, операторы выбрали первый вектор, так как парольная политика была известна и было известно несколько паролей, включая предоставленный заказчиком. Атака проводилась по эксклюзивным словарям с применением дополнительных масок для повышения шанса на успешный подбор пароля.

Были получены доступа к следующим аккаунтам:

*bank.local\Administrator LoveLove1234!*

*USER001 Xx123456!*

*USER002 GoldGold123!*

*USER003 Aa123456!*

**3.3.8 Компрометация и закрепление в домене**

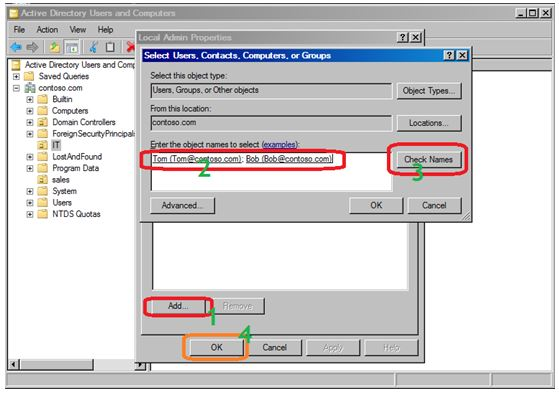
##### 3.3.8.1 Добавление нового пользователя в группу администраторов домена

##### CVE-ID: N/A

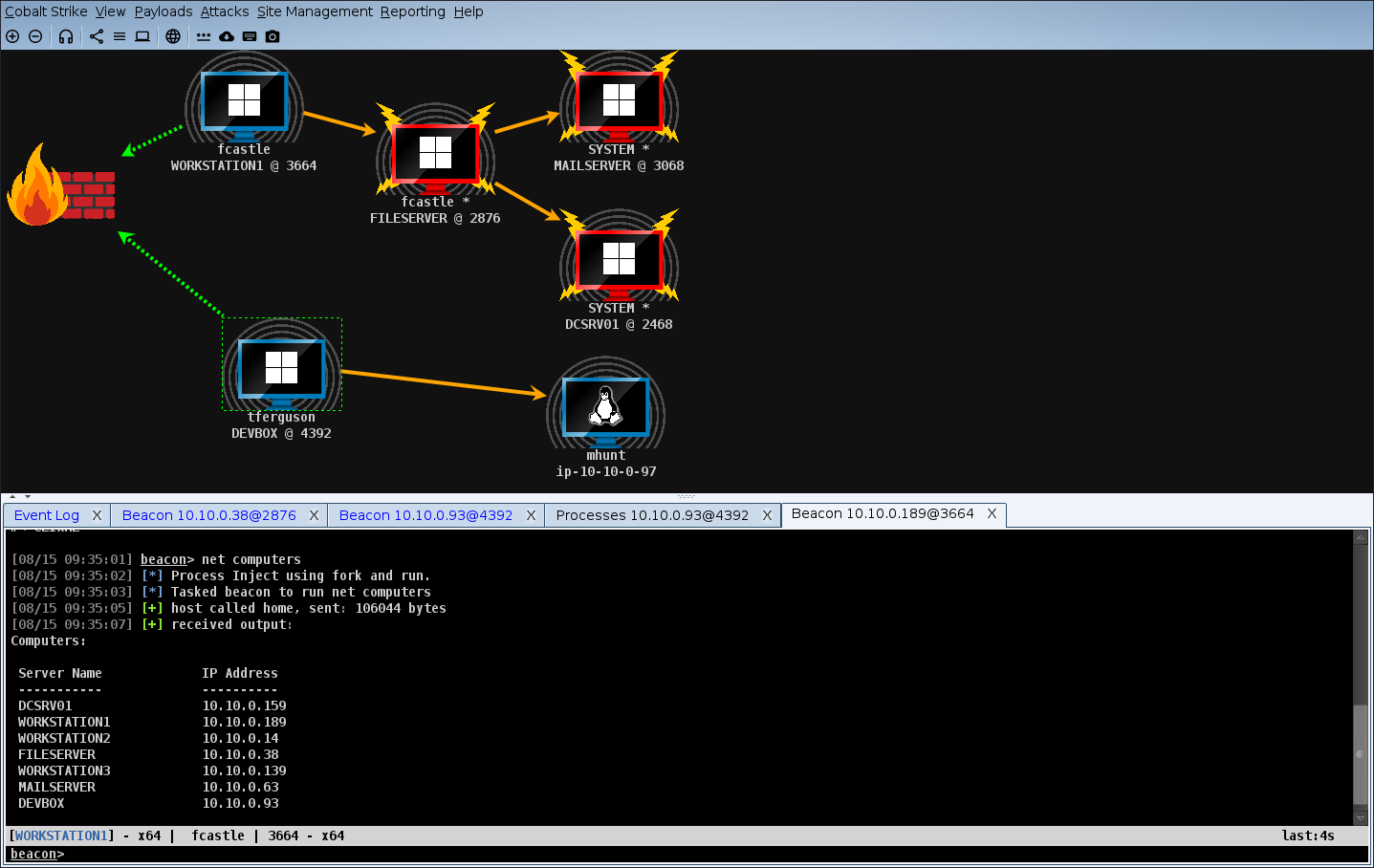
##### CVSS: N/A

##### Критичность: Высокая

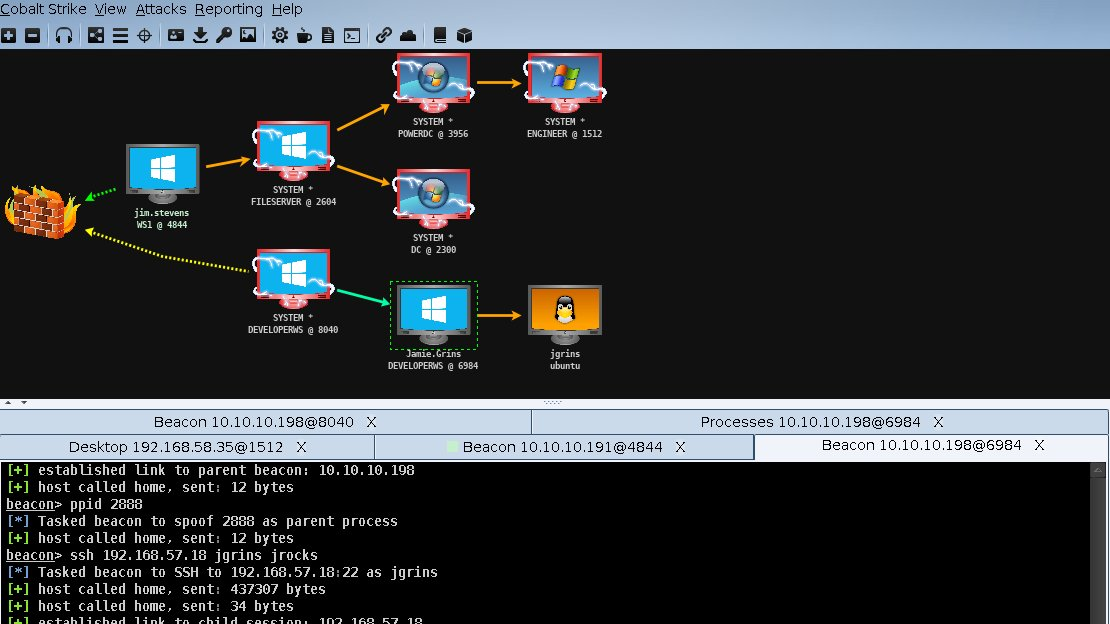
Для компрометации и закреплении в домене, операторы использовали технику добавления нового пользователя с последующим добавлением в группу доменных администраторов.



После этого для получения канала управления на домен контроллере был запущен beacon (маяк) взаимодействия с системами.



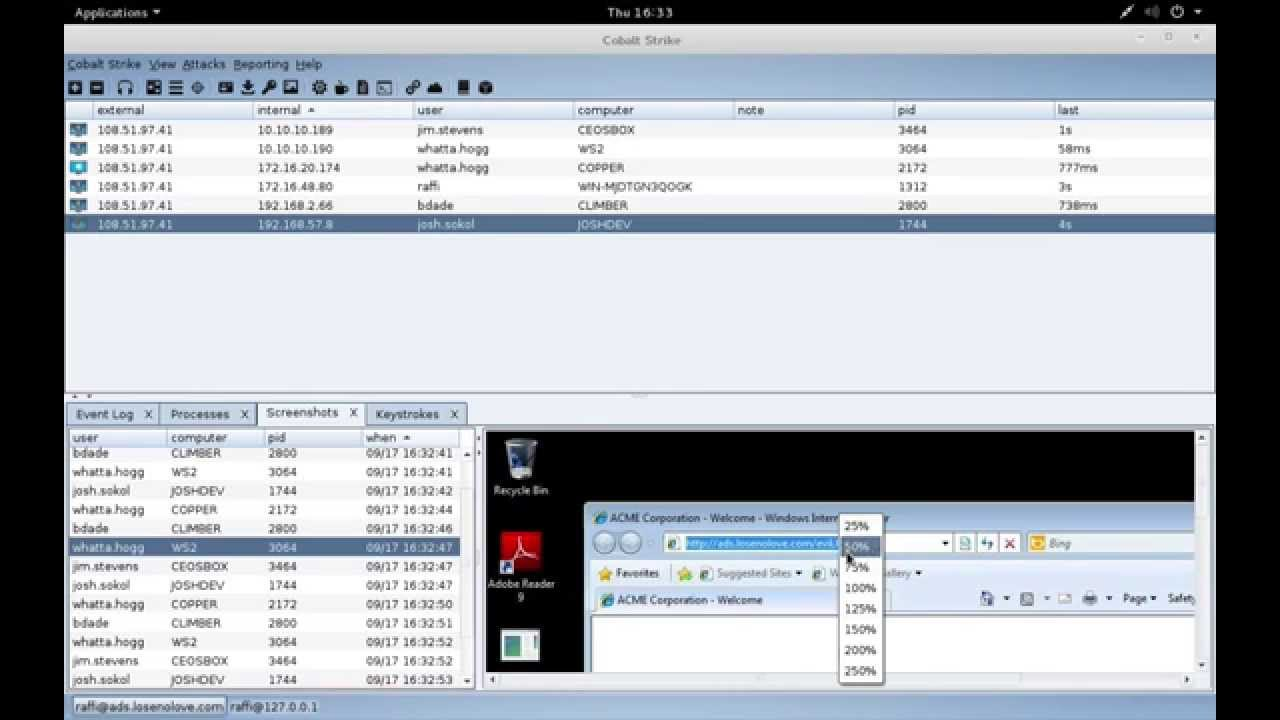
Так же было обнаружено что домен контроллер имеет прямой выход в интернет, что позволило обойтись без построения дополнительных каналов связи с C2 сервером.



Далее операторы исходя из целей выше осуществили горизонтальное перемещение на сервер terminal-srv который является терминальным сервером. Данный сервер был выбран в качестве точки данных которые должны быть эксфильтрированы.

В качестве данных были выбраны произвольные файлы из папок пользователей.

Файлы были успешно эксфильтрированы



#### 3.3.8.1 Атака DcSync

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Высокая

Для дальнейшего продвижения и достижения целей, операторы провели атаку dcsync, что позволило получить krbtgt hash и все доступные hash для всех пользователей в домене. При наличии krbtgt hash операторы смогли проводить атаку Golden Ticket и обеспечить себе закрепление в домене в любых условиях.

| 3.3.8.2 Дамп паролей пользователейCVE-ID: N/ACVSS: N/AКритичность: Высокая Для получения дополнительных учетных данных в открытом виде, операторы сделали дамп lsass и смогли получить дополнительные учетные данные в открытом виде. |
| --- |

#### 

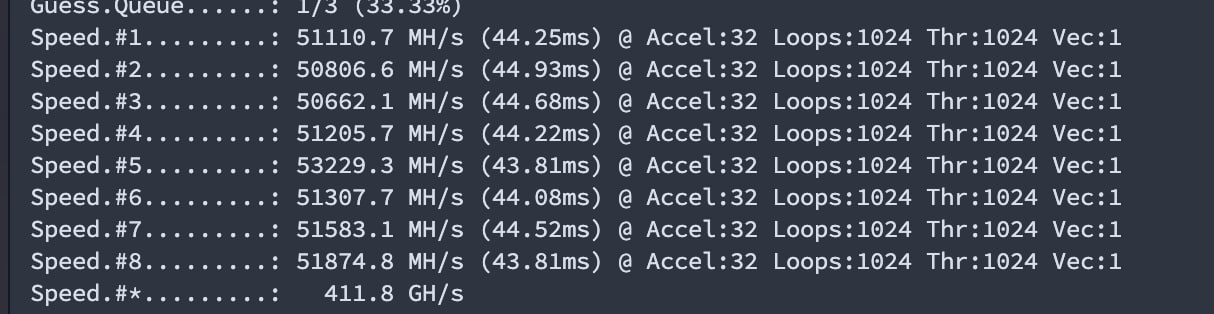
#### 3.3.8.3 Brute Force атака на hash паролей

##### CVE-ID: N/A

##### CVSS: N/A

##### Критичность: Высокая

После проведения DcSync операторами была реализована brute force атака на полученные hash от паролей. В течении 19 часов из 1154 хешей были восстановлены 556.



# Замечания и рекомендации

Данный раздел описывает обнаруженные уязвимости, неверные настройки или отсутствие тех или иных мер защиты или сдерживания атакующих

## Замечание #1 Vulnerability Management

Отсутствие процесса управления уязвимостями позволило выявить множественное отсутствие патчей, отсутствие Security and Administration Baselines что существенно расширяет поверхность атаки.

### Рекомендация

Изменить подход к администрированию текущих систем, использовать Baselines для снижения поверхности атаки, внедрить процесс Vulnerability Management с использованием любых доступных систем для поиска и управления уязвимостями.

## Замечание #2 Insufficient network access

Множество критичных сервисов имеет прямой доступ в сеть Интернет без каких либо ограничений. Например Active Directory, ADCS, PrintServer. Данная ошибка является критической так как при закреплении на сервере атакующие имеют неограниченный доступ в любой момент времени ко всей сети.

### Рекомендация

Отключить критичные сервисы от прямого доступа к сети интернет, ограничить сетевое взаимодействие в рамках HBF или других имеющихся решений для межсетевого экранирования. Интеграция NGFW/IPS/IDS систем.

## Замечание #3 Weak Password Policy

Текущая парольная политика включает в себя не истекающие пароли, низкие требования к сложности пароля. Все это позволило провести одну из наиболее шумной и наименее эффективной атаки - brute force.

### Рекомендация

Внедрить более сложную парольную политику, сделать пароли истекающими каждые 30-90 дней. Проверять новые пароли на переиспользование или незначительные изменения.

## Замечание #3 2FA is not presented

Отсутствие 2FA позволило операторам получить внешний изначальный доступ, что заметно ускорило реализацию дальнейшей атаки.

### Рекомендация

Внедрить 2FA решение

## Замечание #4 Active Directory bad configuration

Текущий анализ Active Directory показал наличие 5 или более критических замечаний. Данные замечания ставят под угрозу всю сеть компании и реализация данных угроз может иметь очень серьезные последствия для бизнес процессов компании.

### Рекомендация (Опционально)

Пересмотреть текущее состояние Active Directory и использовать Active Directory Security Baselines для митигация текущих угроз.

## Замечание #5 Отсутствие адекватных мер реагирования и сдерживания атакующих

В ходе проведения атаки удалось выявить что у команды IT отсутствует план реагирования на случай возможных инцидентов в которых они могут потерять контроль над системами и ситуацией в целом.

### Рекомендация (Опционально)

В рамках IT процессов рекомендуется создать новый процесс который будет описывать Disaster Recovery план по сдерживанию атаки и экстренной изоляции бизнес критичных систем.

Так же рекомендуется внедрение Security экспертизы для внедрения процессов Security Operations которые возьмут на себя роль группы реагирования на инциденты, мониторинга и снижения ущерба от атак в союзе с IT.

# Заключение

Команда Skill Factory выполнила тестирование на проникновение по запросу Bank, чтобы оценить вероятность проведения реальной кибератаки и масштаб потенциального ущерба от неё. Несмотря на препятствующие проведению тестирования на проникновение со стороны системных администраторов Bank действия, такие как:

* блокирование и последующее удаление учетной записи предоставленной специально для проведения теста на проникновение;
* [сброс пароля для учетной записи krbtgt](https://adsecurity.org/?tag=krbtgt) для митигации атаки golden ticket;
* сброс всех скомпрометированных паролей пользователей;

наша команда успешно выявила ряд уязвимостей, которые можно было использовать для закрепления, повышения привилегий, расширения доступа по всему домену и эксфильтрации конфиденциальной информации из сети. Мы считаем, что атака со стороны потенциальных киберпреступников представляет реальную угрозу и может успешно скомпрометировать системы Bank, основываясь на тактике, которая была продемонстрирована в ходе теста на проникновение.

Для выполнения каких-либо действий, описанных в этом отчете не использовались узкоспециализированные эксплойты или инструменты. Команда Skill Factory использовала общедоступный фреймворк для атак, практически всех видов эксплуатации. Требования к уровню технических навыков, необходимых для выполнения отдельных действий выполненных в ходе проведения тестирования, варьировался от низкого до среднего. Требуемые технические возможности и уровень доступа, которые были достигнуты путем объединения этих уязвимостей, должны являться причиной для беспокойства руководства компании поскольку успешный тест на проникновение свидетельствует, что в сетевой инфраструктуре Bank были уязвимости, которые могут быть использованы злоумышленниками низкой квалификации.

Также Специалисты команды Skill Factory продемонстрировали, что злоумышленники с организованной фишинговой кампанией потенциально могут скомпрометировать домен Bank и удаленно собирать конфиденциальные данные, наблюдать, нарушать или блокировать бизнес-операции.

Выявленные проблемы по итогам проведенного тестирования, демонстрируют потенциальные риски, как для бизнеса, так и для репутации компании.

Утечка конфиденциальной и финансовой информации, нарушение операций и потеря доверия клиентов, могут повлечь за собой серьезные последствия, устранение которых повлечет за собой многомиллионные издержки.

Реструктуризация сетевой инфраструктуры, а также выполнение вышепредставленных рекомендаций для Bank позволит улучшить безопасность, снизить риски и сберечь репутацию.

В дополнение к вышеуказанным рекомендациям, можем отметить также базовые, которым необходимо следовать в первую очередь:

* провести харденинг ОС и приложений, продолжая следить за актуальностью внесенных изменений в ходе этого процесса;
* пересмотр политик active directory;
* пересмотр политик для антивирусного решения;
* интеграция IDS/IPS системы;
* внедрение honeypot сети;
* провести обновление всех текущих KB на критичных системах под управлением Windows;
* пересмотреть или внедрить планы BC DRP для сохранения работоспособности критичных бизнес систем.

Команда Skill Factory смогла выполнить все поставленные перед ней задачи по выявлению угроз, и мы надеемся, что в результате выявления этих уязвимостей и последующего их устранения уровень безопасности систем Bank будет улучшен.