САИБ

КИБЕРУЧЕНИЯ

СИБИРСКАЯ АКАДЕМИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

SAIB.BIZ
INFO@SAIB.BIZ
+7 (383) 309 26 36

Киберучения

Проведение учебных кибератак и имитация действий злоумышленников – важнейший инструмент анализа и оценки эффективности систем обеспечения информационной безопасности Компании.

В рамках Киберучений осуществляется комплексная оценка систем управления и мониторинга информационной безопасности с целью модернизации систем защиты информации и улучшения навыков специалистов подразделений кибербезопасности.

Сибирская академия информационной безопасности предлагает услугу проведения **Киберучений**.

Киберучения позволят оценить не только настройку средств защиты информации, но и реакцию специалистов информационной системы на инциденты ИБ, действия службы информационной безопасности и подразделений ИТ.

Данная оценка позволяет скорректировать и усовершенствовать информационную безопасность на предприятии.

Поговорим об услугах, которые включают в себя Киберучения:

— Обход системы защиты почты;
— Безопасность учётных записей;
— Фишинговые рассылки;
— Поиск информации из открытых источников, в том числе в открытых репозиториях кода;
— Обход PAM;
— Разработка и использование псевдовирусных вложений;
— Имитация действий внутреннего нарушителя;
— Имитация и проверка L2-атак;
— Проверка настройки средств защиты и анализ реакции SOC.

SAIB.BIZ
INFO@SAIB.BIZ
+7 (383) 309 26 36

ОБХОД СИСТЕМЫ ЗАЩИТЫ ПОЧТЫ

Услуга заключается в таргетированой и творческой попытке обхода систем защиты Заказчика по Чек-листу (Таблица №1), но не ограничиваясь им. Задачей обхода является подтвержденное заражение рабочей станции заказчика с возможностью удаленного управления.

Таблица № 1 «Чек-лист обязательных проверок при обходе систем защиты»

Наименование средства защиты информации	Описание минимальных методов обхода системы защиты
AV/EDR	Обфускация кода, использование тактик "Living off the Land“.
Sandbox	Детектирование виртуализации, установленного ПО для мониторинга, анализ эмуляции работы пользователя .
Шлюз безопасности почты, Антиспам	Повышение доверия доменов, организация ссылок с помощью облачных хранилищ, проверка возможности подмены отправителя, использование не бинарных загрузчиков вредоносного кода, упаковщиков/архивов.
IDS/IPS	Использование легитимных протоколов для управления агентом, изменение поведения эксплойтов и агентов в сети.
DPI, Web-фильтрация	Инкапсуляция трафика с использованием ряда легитимных протоколов и служб/сервисов в сети Интернет.
AV/EDR	Обфускация кода, использование тактик "Living off the Land“.

БЕЗОПАСНОСТЬ УЧЁТНЫХ ЗАПИСЕЙ

Аудит паролей методом «Белого ящика»

В рамках реализации данного метода в корпоративную инфраструктуру организации развертывается программное решение, позволяющее проанализировать текущие настройки парольной политики и пароли пользователей службы каталогов Active Directory на предмет наличия потенциальных рисков, связанных с реализаций вредоносных действий, связанных с получением нелегитимных прав доступа в информационных системах посредством подбора паролей.

Список выполняемых проверок:

— Анализ текущих паролей пользователей на предмет идентичности с другими учётными записями;

— Анализ текущих паролей пользователей на предмет использования механизма авторизации в целевых системах или наличия установленных требований к минимальной длине пароля;

— Анализ текущих паролей пользователей организации на предмет возможной компрометации в сети Интернет, используя механизмы проверки «по чёрному списку».

— Анализ существующего списка административных учётных записей на предмет наличия возможных рисков использования;

— Поиск устаревших паролей пользователей;

— Анализ соответствия настроек корпоративной парольной политики с существующими российскими отраслевыми стандартами и мировым практикам.

Аудит паролей методом «Черного ящика»

В рамках реализации данного метода будут задействованы различные методики компрометации учётных данных пользователей на сервисах, доступных на сетевом периметре организации.

Список выполняемых проверок:

— Сканирование публичных сервисов внешнего периметра, требующих авторизации;

— Анализ и оценка полученного списка учётных записей на предмет наличия возможных рисков использования;

— Проведение взлома учетных записей путем подбора паролей к ним методом Brute force.

Перебор паролей по доменным учётным записям происходит методом Password Spraying.

```
┌─[root@axxtel-vmwarevirtualplatform]─[/home/axxtel]
└──╼ #crackmapexec smb 192.168.10.200 -u ad_users_axxteltestcorp.txt -p 'Ctynz,hm2021' --continue-on-success | grep '[+]'
SMB         192.168.10.200  445    SERV-AD-TEST     [+] axxtel.test.corp\bas:Ctynz,hm2021
SMB         192.168.10.200  445    SERV-AD-TEST     [+] axxtel.test.corp\pmd:Ctynz,hm2021
┌─[root@axxtel-vmwarevirtualplatform]─[/home/axxtel]
└──╼ #
```

```
┌─[root@axxtel-vmwarevirtualplatform]─[/home/axxtel]
└──╼ #patator smb_login host=192.168.10.200 domain=axxtel.test.corp user=FILE0 password=qwe123QWE 0=ad_users_axxteltestcorp.txt -x ignore:code=c000006d
11:09:15 patator    INFO - Starting Patator 0.9 (https://github.com/lanjelot/patator) with python-3.9.1 at 2021-09-13 11:09 +07
11:09:15 patator    INFO -
11:09:15 patator    INFO - code     size   time | candidate                          |   num | mesg
11:09:15 patator    INFO - -----------------------------------------------------------------------------
11:09:15 patator    INFO - 0        48    0.022 | Administrator                    |     1 | AXXTELTEST\SERV-AD-TEST (Windows 6.3 Build 9600)
11:09:15 patator    INFO - 0        48    0.154 | vasid                            |     9 | AXXTELTEST\SERV-AD-TEST (Windows 6.3 Build 9600)
11:09:15 patator    INFO - 0        48    0.013 | fudo3                            |    59 | AXXTELTEST\SERV-AD-TEST (Windows 6.3 Build 9600)
11:09:15 patator    INFO - 0        48    0.024 | t34                              |    60 | AXXTELTEST\SERV-AD-TEST (Windows 6.3 Build 9600)
11:09:15 patator    INFO - Hits/Done/Skip/Fail/Size: 4/74/0/0/74, Avg: 122 r/s, Time: 0h 0m 0s
```

При переборе хешей используются словари, и все операции происходят локально в режиме offline. Производительность такого перебора значительно выше.

```
Host memory required for this attack: 222 MB

Dictionary cache hit:
* Filename..: D:\DICTIONARIES\words_rine_rus_password_list_wds.txt
* Passwords.: 3400965990
* Bytes.....: 55899786118
* Keyspace..: 3400965990

Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password- and salt-length (typically down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

cd9d0955b78c332f077b664d81ca975a:fgtkmcby123

Session..........: hashcat
Status...........: Cracked
Hash.Name........: MD5
Hash.Target......: cd9d0955b78c332f077b664d81ca975a
Time.Started.....: Mon Sep 13 11:33:33 2021 (11 secs)
Time.Estimated...: Mon Sep 13 11:33:44 2021 (0 secs)
Guess.Base.......: File (D:\DICTIONARIES\words_rine_rus_password_list_wds.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  7933.9 kH/s (4.84ms) @ Accel:1024 Loops:1 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 84344832/3400965990 (2.48%)
Rejected.........: 0/84344832 (0.00%)
Restore.Point....: 83755008/3400965990 (2.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#1....: fgfnbxyjcnm55845 -> fgbkfr45674
Hardware.Mon.#1..: Temp: 51c Fan:  0% Util: 18% Core:1569MHz Mem:3802MHz Bus:16

Started: Mon Sep 13 11:33:32 2021
```

ФИШИНГОВЫЕ РАССЫЛКИ

Услуга преследует цель – проверка осведомленности пользователей Заказчика методом фишинговых рассылок. После рассылки, сценарии и технические особенности которой согласуются вместе с заказчиком, собирается подробная статистика и проводится анализ действий пользователей – их реакция на фишинговые письма.

Порядок предоставления услуги состоит из 9 этапов:

1. Получение списка почтовых адресов заказчика (предусматривается два способа получения информации):
   a. Заказчик предоставляет списки почтовых адресов самостоятельно.
   b. Получение списка почтовых адресов Заказчика с помощью проведения OSINT (описание работ и итоги включаются в отчет).
2. Проведение анализа полученных адресов.
3. Составление условных групп основанных на категориях пользователей (Кадровые отделы, Отделы службы информации, ИТ-отделы) по согласованию с заказчиком.
4. Выявление наименее защищенных субъектов инфраструктуры (наименее защищенными считаются лица, на которых обнаружено большее количество скомпрометированной информации).
5. Планирование рассылки, определение типа рассылки (таргетированная/групповая/массовая), разработка уникальных сценариев.
6. Разработка дизайна и создание фишинговых форм авторизации для получения данных пользователей. Формы по внешнему виду могут повторять оригинал, если они имитируют реально существующий ресурс. Для данных форм приобретаются похожие на оригинал доменные имена, которые «отстаиваются» в течении необходимого времени, для защиты от детектирования как недавно созданные ресурсы средствами защиты информации.
7. Согласование материалов фишинговой рассылки с ответственным лицом заказчика.
8. Проведение рассылки. Возможно проведение рассылок в несколько волн. Согласуется время проведения.
9. Составление отчета о проделанной работе и реагировании пользователей на рассылку.

ПОИСК ИНФОРМАЦИИ ИЗ ОТКРЫТЫХ ИСТОЧНИКОВ, В ТОМ ЧИСЛЕ В ОТКРЫТЫХ РЕПОЗИТОРИЯХ КОДА

Данная услуга позволяет осуществлять пассивный и активный сбор информации из общедоступных источников (поисковые системы, социальные сети, DNS-сервера компании, база данных WHOIS, анализ метаинформации из документов на сайтах компании и т.д.).

Существует два варианта предоставления данной услуги:

1) Ручной единоразовый поиск и сбор информации;
2) Поставляемое по годовой подписке SaaS-решение, позволяющее проводить сканирование постоянно.

Подробнее о ручном сборе информации. Осуществляется пассивный и активный сбор информации из общедоступных источников (поисковые системы, социальные сети, DNS-сервера компании, база данных WHOIS, анализ метаинформации из документов на сайтах компании и т.д.).

- определение пути прохождения трафика и структуры сети;
- сканирование всех портов для диапазона обозначенных IP-адресов;
- идентификация устройств, определение используемых ОС;
- сбор информации о работающих сервисах;
- сканирование на наличие уязвимостей автоматическими средствами.

На основе общедоступной информации, а также путем перебора составляется список ресурсов для тестирования. После согласования с заказчиком определяется область IP-подсетей. Происходит поиск и фиксирование соответствия между всеми доменными именами, принадлежащими заказчику, и IP-адресами.

На ресурсе, к примеру, таком как https://github.com/ проводится поиск критичных данных, предоставленных в общий доступ. Разведываются репозитории, которые связаны с компанией (ее сотрудниками) или с ПО компании. Репозитории могут содержать различную технологическую информацию, относящуюся к внутренней ИТ-инфраструктуре компании. В том числе, могут быть обнаружены пароли действующих учетных записей.

Подробнее о постоянном сканировании. Данная услуга основана на заведении заказчика в системе. Заказчик, как пользователь внутри системы может видеть актуальную информацию по активам (домены, IP-адреса и т.д.) своей компании, а также постоянно выявляемые проблемы (уязвимости, неправильные настройки и т.д.).

Функционально решаются следующие задачи:

- Находит и связывает активы компании, даже забытые, показывая в реальном времени актуальную инфраструктуру на основе сканирования всей сети интернет;

- Обнаруживает актуальные уязвимости по базе данных общеизвестных уязвимостей информационной безопасности (CVE), используя полученную информацию, к примеру, по разведанному ПО, которое использует компания;
- Находит ошибки в настройках, отсутствующие настройки в программном обеспечении компании;
- Проводит разведку по открытым и закрытым источникам о компании, её упоминаниях (к примеру, на хакерских форумах) и различных утечках информации;

Заказчик может работать с активами и проблемами своей компании на основе составленного цифрового отпечатка. Менеджмент проблем происходит автоматически – система сравнивает первоначальные цифровые отпечатки компании с текущими: к примеру, заказчик закрыл некую уязвимость, обновив ПО – система отметит ту уязвимость как решенную. Также есть и опция самостоятельного менеджмента проблем – заказчик отмечает проблемы как «решенные», «ложно-позитивные», «в работе» и т.д.

Существует и управление активами. В таком случае заказчик может отметить домены или IP-адреса как принадлежащие ему или как неактуальные.

Система строит граф по найденным активам, связывающиеся с основным доменом.

В рамках бесплатного пилота (1 месяц) проходят следующие этапы:

1) Заполнение заказчиком небольшого опросного листа с информации о его компании;
2) Регистрация компании заказчика в системе, после чего происходит первичное сканирование по всей поверхности инфраструктуры данного клиента;
3) Проведение конференции с заказчиком, во время которой проводится демонстрация функционала системы, найденной первичной информации по компании;
4) Регистрация пользователя от заказчика в системе, предоставление простого и краткого мануала по менеджменту активов;
5) Пользователь подтверждает или отмечает как неактуальные активы компании (только домены и IP-адреса, остальное по желанию);
6) Система проводит досканирование компании по согласованным в пункте 5 активам;
7) Готовится отчет по актуальным и наиболее значимым проблемам для компании заказчика, после чего он предоставляется вместе с выгруженными приложениями активов и проблем компании;
8) Принимается решение об использовании подписки заказчиком.

ОБХОД PAM

Данная услуга во время тестирования позволяет проверить функционирование использующейся у Заказчика PAM-системы для анализа возможности ее обхода.

В основном выбираются и реализуются 3 вектора атаки для проведения тестирования:

1) Атаки, направленные на уязвимости самого решения класса PAM. Производится поиск уязвимостей (к примеру, автоматизированное сканирование), анализ кода (к примеру, reverse engineering).
2) Атаки, направленные на повышение привилегий в системе с обходом средств защиты информации и регистрации действий привилегированных пользователей в системе PAM. Данные атаки зачастую используют некорректную конфигурацию прав доступа.
3) Атаки, направленные на уязвимости виртуализации серверов на которых размещена система PAM. В целях реализации данного вектора получают сетевой доступ к среде виртуализации путем эксплуатации уязвимости сервисов, находящихся в том же сетевом сегменте что и среда виртуализации. После чего производится эксплуатация уязвимости самой среды виртуализации. Реализация данного вектора атаки позволяет обойти любые ограничения системы PAM путем ее отключения в среде виртуализации.

РАЗРАБОТКА И ИСПОЛЬЗОВАНИЕ ПСЕВДОВИРУСНЫХ ВЛОЖЕНИЙ

Под нужды и требования с согласованием от Заказчика реализуются различные псевдовирусные вложения, имитирующие работу существующих известных типов вредоносного программного обеспечения.

Примером подобных типов будут являться следующие вирусы:

— Шифровальщики;
— Трояны удаленного доступа;
— Кейлоггеры и др.

По согласованию с заказчиком вирус может вести себя по-разному: обнаруживать себя или наоборот скрывать свое присутствие, использовать обфускацию кода, низкоуровневые хуки и т.д.

В рамках проведения проекта согласовывается способ доставки и точки фиксации действий пользователей и системы защиты.

Для данного тестирования готовится поэтапный план работ, включающий в себя разработку, схему предоставления и применение псевдовирусного вложения.

ИМИТАЦИЯ ДЕЙСТВИЙ ВНУТРЕННЕГО НАРУШИТЕЛЯ

Производится проверка реакции системы, СЗИ и другого ПО на совершение различных подозрительных действий пользователем внутри периметра.

Такими действиями, например, могут являться:

1. *«Хакерские» активности:*

- Запуск и использование Windows PowerShell;
- Запуск скриптов (примеры файлов с расширениями: .js, .ps, .php и другие);
- Использование средств администрирования учетных записей;
- Активация неразрешенных для обычных пользователей команд в консолях (сетевые команды, cipher, assoc и другие).

2. *Нарушение корпоративных политик:*

- Нарушение режима рабочего времени;
- Нецелевое использование рабочего времени;
- Имитация действий из «зоны риска».

3. Корпоративный шпионаж:

- Утечки данных;
- Раскрытие информации;
- Попытки нецелевого доступа;
- Вербовка сотрудников.

Перечень работ и используемые планы учение разрабатываются совместно с Заказчиком.

ИМИТАЦИЯ И ПРОВЕРКА L2-АТАК

В рамках данной услуги проводятся атаки на канальный уровень модели OSI. Атаки такого типа несут серьезную опасность, так как их успешное выполнение позволяет обходить защиту всех вышестоящих уровней. Примером таких атак могут являться: spoofing, атака типа человек посередине или relay-атаки.

Для тестирования настройки СЗИ, реакции системы производятся попытки манипуляции с траффиком сети – прослушивание, перенаправление (встраивание в качестве посредника), дублирование, подмена.

Проведение различных атак, а не только одной/конкретной не только согласуется с заказчиком, но и расширяет возможности тестирования, позволяя результаты одной атаки использовать для проведения другой.

Работы проводятся в соответствии с чек-листом работ.

ПРОВЕРКА НАСТРОЙКИ СРЕДСТВ ЗАЩИТЫ И АНАЛИЗ РЕАКЦИИ SOC

Оценка реагирования SOC проводится в соответствии с нижеприведенными разделами:

1. Оценка техник по матрице - ATT&CK Matrix for Enterprise

— Initial Access
— Execution
— Persistence
— Privilege Escalation
— Defense Evasion
— Credential Access
— Discovery
— Lateral Movement
— Collection
— Command and Control
— Exfiltration

2. Оценка потенциального ущерба

3. Оценка выявленных действий реагирования

4. Оценка сокрытия используемых средств и методов защиты

5. Оценка методов реагирования

6. Оценка действий пользователей (оценка уровня осведомленности)

7. Оценка скорости реакции SOC, основанная на собранной информации

8. Дополнительные проверки подсистем информационной безопасности:

Подсистема	Объект аудита	Состав работ
Подсистема Анализа защищённости	Регулярность поиска и устранения уязвимостей	Поиск машин с уязвимостями внутри периметра и снаружи, эксплуатация.
Подсистема мониторинга	Скорость выявления аномальной ситуации и реагирование персонала на нее	1. Генерация разрозненного подозрительного трафика на объекты мониторинга снаружи и внутри периметра. Регистрирация траффика у себя и по обратной связи от заказчика смотреть скорость

		реагирования, локализации и устранения. 2. Исходя из продуктов заказчика, которые находятся на мониторинге, можно сформировать одну комплексную атаку, которая отразится на всех мониторируемых объектах.
Подсистема защиты сетевого траффика	Проверка корректности конфигурации средств защиты	1. Сканирование различных портов и хостов, попытки подключения на эти порты. 2. При предоставлении машины внутри периметра, попытка настроить VPN-туннель с нашей машиной. 3. Попытки brute force формы авторизации по управлению СЗИ (в случае с web-формой, например)
Подсистема контроля сотрудников и утечек конфиденциальной информации	Оценка реагирования и вероятности выявления	

В рамках работ по внешнему периметру мы проводим проверки, сгруппированные по следующим направлениям:

— Разведка – поиск информации об организации по различным источникам;

— Получение первоначального доступа – доставка в атакуемую систему вредоносного кода или нагрузки и обеспечение его дальнейшего выполнения;

— Выполнение – исполнение и применение атакующим средств выполнения различных команд, сценариев и исполняемых файлов, доставленных на предыдущем этапе;

— Закрепление – обеспечение постоянства присутствия в атакуемой системе.

В рамках работ по внутреннему периметру мы проводим проверки, сгруппированные по следующим направлениям:

— Разведка – сбор информации о целевых системах: информации о сети; сервисах, имеющихся как во внутренней инфраструктуре, так и на периметре; информации о рабочих станциях и серверах: установленная ОС, подключенные устройства и т.д.;

— Интерпретатор команд и скриптов – проверка возможности исполнения кода скриптовых языков на интерпретаторах, установленных на узлах сети, в т.ч. удалённо;

— Эксплуатация распространённых уязвимостей;

— Планировщики задач;

— Извлечение учётных данных из хранилищ – попытка извлечения учётных данных из хранилищ операционной системы (LSASS, /etc/shadow и т.д.) и приложений: браузеров и т.д. Учётные данные могут быть извлечены как в открытом виде, так и в виде хэшей для дальнейшей передачи на перебор;

— Подслушивание сети – проверка возможности подслушивания сети с целью получения информации (учётных данных, информации о сервисах и т.д.). Данная проверка также может выявлять использование устаревших протоколов (SMBv1, LLMNR, NetBIOS), которые используют механизмы разрешения имен, основанные на широковещательной отправке запросов.;

— Горизонтальное продвижение – выявление возможности передвижения злоумышленника между узлами сети;

— Command&Control – выявление возможности каналов связи с серверами типа Command&Control (C2). При помощи C2-сервера злоумышленник может установить канал управления до зараженного узла сети и производить действия от его имени;

— Эксфильтрация данных.

Остались вопросы? Свяжитесь с нами!