Изучаем Adversarial Tactics, Techniques & Common Knowledge (ATT@CK). Enterprise Tactics. Часть 7

habr.com/ru/articles/436350

Андрей Макеев

Обнаружение (Discovery)

Ссылки на все части:

Получив, в результате первичной компрометации, доступ в систему противник должен «осмотреться», понять что он теперь контролирует, какие возможности у него появились и достаточно ли текущего доступа для достижения тактической или конечной цели. Этот этап атаки называется «Обнаружение» (англ. *Discovery* — «научной открытие», «раскрытие», «разоблачение»).

Автор не несет ответственности за возможные последствия применения изложенной в статье информации, а также просит прощения за возможные неточности, допущенные в некоторых формулировках и терминах. Публикуемая информация является свободным пересказом содержания MITRE ATT&CK.

Операционные системы имеют множество встроенных инструментов с помощью которых противник может осуществлять исследование внутреннего периметра атакуемой сети после её компрометации. В Windows для сбора информации могут использоваться инструменты прямого взаимодействия с Windows API, функционал WMI и PowerShell.

Злоумышленник применяет методы обнаружения во время изучения атакуемой среды, поэтому выявление подобной активности следует рассматривать как часть цепочки атаки, за которой последуют попытки продвижения противника по сети.

В качестве меры, направленной на выявление вышеописанной активности в защищаемых системах, рекомендован мониторинг процессов и аргументов командной строки, которые могут использоваться в ходе сбора информации о системе или сети. Общей рекомендацией по предотвращению возможности несанкционированного внутреннего исследования защищаемой системы и сети является проведение аудита наличия ненужных системных утилит и потенциально-опасного ПО, которые могут использоваться для изучения защищаемой среды, и применение инструментов блокирования их запуска, например AppLocker или политик ограничения программного обеспечения (Software Restriction Policies).

Обнаружение учетных записей (Account discovery)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Злоумышленники могут пытаться получить перечень учетных записей локальной системы или домена.

Windows
Для получения информации об учетных записях могут быть использованы утилиты *Net* или *Dsquery*:

```
net user
net group
net localgroup
dsquery user
dsquery group
```

Злоумышленник может применять техники обнаружения владельца/пользователя системы (*System Owner/User Discovery*) для поиска основного пользователя, текущего пользователя системы или группы пользователей, которые обычно используют систему.

Mac
В Mac, группы пользователей могут быть получены с помощью команд *groups* и *id*. Также группы пользователей и пользователи могут быть перечислены с помощью следующих команд:

```
dscl . list /Groups
dscacheutile -q group
```

Linux
В Linux, локальные пользователи могут быть получены из файла */etc/passwd*, который доступен для чтение всем пользователям. В Mac этот же файл используется только в однопользовательском режиме в дополнение к файлу */etc/master.passwd*. Кроме того, в Linux также доступны команды *groups* и *id*.

Рекомендации по защите: Предотвратите возможность перечисления учетных записей администраторов при повышении уровня прав через UAC, поскольку это приведёт к раскрытию имен учетных записей администраторов. Соответствующий раздел реестра можно отключить с помощью GPO:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\CredUI\
EnumerateAdministrators
```

```
GPO: Computer Configuration > [Policies] > Administrative Templates > Windows Components > Credential User Interface: Enumerate administrator accounts on elevation.
```

Обнаружение окон приложений (Application Window Discovery)

Система: Windows, macOS
Права: Пользователь
Описание: Злоумышленники могут пытаться получить списки окон, открытых приложениями. Такие списки могут свидетельствовать о там как используется система или обнаружить контекст собранной кейлоггером информации. В Mac это можно сделать с помощью небольшого скрипта на AppleScript.

Обнаружение закладок браузера (Browser Bookmark Discovery)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Чтобы узнать о скомпрометированной системе как можно больше информации злоумышленники могут изучать пользовательские закладки браузера. Закладки могут раскрывать личную информацию о пользователях (например, банковские сайты, личные интересы, социальные сети и т.п.), а также информацию о внутренних сетевых ресурсах сети — серверах, инструментах, дашбордах и других инфраструктурных элементах. Противник может использовать учетные данные, закэшированные в браузере, для получения доступа к сервисам пользователя, адреса которых сохранены в закладках браузера. Места хранения закладок зависят от платформы и специфики приложений и ОС. Закладки браузера, как правило, хранятся в виде локальных файлов или баз данных.

Рекомендации по защите: Учитывая, что хранение информации в файлах является штатной функцией ОС, попытки подавления этой активности будут неуместны. Например, ограничение доступа к файлам закладок браузера, скорее всего, приведет к непреднамеренным побочных эффектам и нарушит работу легитимного ПО. Усилия по защите необходимо направить на предотвращение запуска средств и инструментов злоумышленника на более ранних стадиях атаки.

Обнаружение файлов и каталогов (File and Directory Discovery)

Система: Windows, Linux, macOS
Права: Пользователь, администратор, System
Описание: Злоумышленники могут перечислять файлы и каталоги или искать определенную информацию в конкретных локациях на хосте или на общих сетевых ресурсах.

Windows
Примерами утилит для получения информации о файлах и каталогах служить *dir* и *tree*. Пользовательские инструменты посредством прямого взаимодействия с Windows API могут также использоваться для сбора информации о файлах и каталогах.

Linux и macOS
В Linux и macOS обзор файлов и каталогов осуществляется с помощью команд *ls, find* и *locate*.

Рекомендации по защите: Учитывая, что представление информации в виде файлов и каталогов является штатной функцией ОС, попытки подавления этой активности будут неуместны. Усилия по защите необходимо направить на предотвращение запуска средств и инструментов злоумышленника на более ранних стадиях атаки.

Сканирование сетевых сервисов (Network Service Scanning)

Система: Windows, Linux, macOS
Права: Администратор, System
Описание: Злоумышленники могут пытаться получить список служб, запущенных на удаленных хостах, включая те, которые могут быть уязвимы для средств удаленного доступа. Методы получения такой информации включают в себя сканирование портов и уязвимостей с помощью инструментов, которые загружаются в систему.

Рекомендации по защите: Применяйте IDS/IPS-системы для обнаружения и предотвращения удаленного сканирования. Убедитесь, что ненужные порты закрыты, неиспользуемые службы отключены, а правильная сегментация сети соблюдается для защиты критично-важных серверов и устройств.

Обнаружение общих сетевых ресурсов (Network Share Discovery)

Система: Windows, macOS
Права: Пользователь
Описание: В локальных сетях часто есть общие сетевые диски и папки, которые позволяют пользователям получать по сети доступ к файловым каталогам, размещенным в различных системах. Злоумышленники могут искать общие

сетевые папки и диски в удаленных системах в целях поиска целевых источников данных и выявления потенциальных систем для дальнейшего продвижения по сети.

Windows
Обмен файлами в Windows-сетях осуществляется с помощью протокола SMB. Утилита *Net* может быть использована для получения от удаленной системы информации о наличии в ней общих сетевых дисков: `net view \remotesystem` Или получения информации об общих сетевых дисках в локальной системе: `net share`.

Mac
В Mac, локально-примонтированные общие сетевые ресурсы можно просмотреть с помощью команды: `df -aH`.

Прослушивание сети (Network Sniffing)

Система: Windows, Linux, macOS
Описание: Злоумышленник может использовать сетевой интерфейс в режиме *promiscuos mode* («неразборчивый» режим), в котором сетевая плата будет принимать все пакеты независимо от того кому они адресованы или использовать span-порты (порты зеркалирования) для захвата большого объема данных, передаваемых по проводным или беспроводным сетям.

Захваченные в ходе сниффинга данные могут содержать учетные данные, отправленные через незащищенные соединения без использования протоколов шифрования. Различные атаки на сетевые службы имен типа отравления LLMNR/NBT-NS путем перенаправления трафика также могут использоваться для сбора учетных данных на веб-сайтах, прокси-серверах и внутренних системах. В ходе прослушивание сети противник так же может выявить различные сведения о конфигурации (запущенные службы, номера версий, IP-адреса, имена хостов, VLAN ID и т.п.) необходимые для дальнейшего продвижения по сети и/или обхода средств защиты.

Рекомендации по защите: Убедитесь, что беспроводной трафик соответствующим образом зашифрован. По возможности, используйте Kerberos, SSL и многофакторную аутентификацию. Проводите мониторинг сетевых коммутаторов на предмет использования span-портов, отравления ARP/DNS и несанкционированных изменений конфигурации маршрутизатора. Применяйте средства выявления и блокировки потенциально-опасного ПО, которое может быть использовано для перехвата и анализа сетевого трафика.

Раскрытие парольной политики (Password Policy Discovery)

Система: Windows, Linux, macOS
Права: Пользователь

Описание: Парольная политика в сети — это способ гарантированного применения пользователями сложных паролей, которые трудно угадать или взломать путем перебора. Злоумышленник может пытаться получить доступ к информации о параметрах парольной политики атакуемой сети в целях создания списка распространенных общеизвестных паролей, удовлетворяющих требованиям политики (например, если политикой установлена минимальная длина паролей в 8 символов, то не пытаться использовать пароли типа pass123 или не проверять более 3-4х паролей на учетную запись, если количество неудачных попыток равно 6) и последующего запуска подбора паролей по словарю. Парольные политики могут применяться и быть обнаруженными как в Windows, так и в Linux и macOS.

Windows

```
net accounts
net accounts /domain
```

Linux

```
chage -l
cat /etc/pam.d/comman-password
```

macOS

```
pwpolicy getaccountpolicies
```

Рекомендации по защите: Попытки прямого воспрепятствования выявлению парольной политики не рекомендуются, поскольку параметры парольной политики должны быть известны всем системам и пользователям сети. Убедитесь, что применяемая вами парольная политика затрудняет брутфорс паролей и не позволяет использовать слишком легкие пароли. Самый распространенный способ применения парольной политики в корпоративной сети — это внедрение Active Directory.

В случае наличия задачи по выявлению вредоносной активности отслеживайте процессы на наличие инструментов и аргументов командной строки, указывающих на попытки выявления парольной политики. Сопоставьте эту активность с другими подозрительными действиями исходной системы, чтобы уменьшить вероятность ложного события, связанного с действиями пользователя или администратора. Противник скорее всего попытается выявить параметры парольной политики на ранних стадиях атаки либо совместно с применением других техник стадии выявления и обзора.

Обнаружение периферийных устройств (Peripheral Device Discovery)

Система: Windows
Права: Пользователь, Администратор, System
Описание: Злоумышленники могут пытаться собрать информацию о подключенных к компьютерам в атакуемой сети периферийных устройствах. Эта информация

может быть использована для повышения осведомленности об атакуемой среде и в использована при планировании дальнейших вредоносных действий.

Обнаружение групп доступа (Permission Groups Discovery)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Злоумышленники могут пытаться найти локальные или доменные группы доступа и исследовать параметры их разрешений.

Windows
Перечислить группы доступа можно с помощью утилиты *Net*:
`net group /domain`
`ner localgroup`

Linux
В Linux локальные группы можно перечислять с помощью команды *groups*, доменные — с помощью команды *ldapsearch*.

macOS
В Mac тоже самое можно сделать с помощью следующих команд:
`dscacheutil -q` — для доменных групп;
`dscl . -list /Groups` — для локальных групп.

Обнаружение процессов (Process Discovery)

Система: Windows, Linux, macOS
Права: Пользователь, Администратор, System
Описание: Противники могут пытаться получить информацию о запущенных с системе процессах с целью получения сведений о программном обеспечении, работающем на системах атакуемой сети.

Windows
Примером способа получения сведений о процессах в Windows является системная утилита *Tasklist*.

Mac и Linux
В Mac и Linux это выполняется с помощью команды *ps*.

Запросы к реестру (Query Registry)

Система: Windows
Права: Пользователь, администратор, System
Описание: Злоумышленники могут взаимодействовать с реестром Windows для сбора информации о системе, конфигурации и установленном ПО. Реестр содержит

значительный объем информации об операционной системе, конфигурации, программном обеспечении и безопасности. Некоторая информация может помочь противнику в проведении дальнейших операций в атакуемой сети. Взаимодействие с реестром может происходить с использованием различных утилит, например, *Reg* или при помощи запуска сторонних инструментов, использующих Windows API.

Обнаружение удаленных систем (Remote System Discovery)

Система: Windows, Linux, macOS
Права: Пользователь, Администратор, System
Описание: Противник, вероятно, попытается получить список систем в атакуемой сети. Обнаружить удаленные системы можно по IP-адресу, имени хоста или другому идентификатору, который в дальнейшем может использоваться для продвижения злоумышленника по сети из текущей системы. Соответствующие функциональные возможности могут быть включены в инструменты удаленного доступа (RAT), также могут быть использованы и встроенные системные утилиты.

Windows
Команды *ping* или *net view*.

Mac
Для обнаружения Mac-систем в пределах широковещательного домена (broadcast domain) применяется протокол *Bonjour*. Такие утилиты как *ping* также могут использоваться для сбора информации об удаленных системах.

Linux
Такие утилиты как ping также могут использоваться для сбора информации об удаленных системах.

Обнаружение программных средств обеспечения безопасности (Security Software Discovery)

Система: Windows, macOS
Права: Пользователь, администратор, System
Описание: Злоумышленники могут попытаться получить списки программных средств обеспечения безопасности, конфигураций, датчиков, установленных в системе. Целью противника могут быть такие вещи как локальные правила брандмауэра, антивирус и средства виртуализации. Эти проверки могут быть встроены в инструменты удаленного доступа (RAT), используемые на ранних стадиях атаки.

Windows
Примерами команд, которые могут использоваться для получения сведений о средствах безопасности, являются утилиты *netsh, reg query, dir* и *tasklist*, однако

могут применятся и другие более специфичные инструменты, предназначенные на выявление определенных систем безопасности, которые ищет противник.

Mac
Распространенным способом проверки на вредоносные программы является использование программ *LittleSnitch* и *KnockKnock*.

Обнаружение информации о системе (System Information Discovery)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Противник может попытаться получить подробную информацию об операционной системе и оборудовании, включая архитектуру, версию, исправления и установленные пакеты обновлений.

Windows
Примерами утилит для получения сведений о системе являются *ver, systeminfo* и *dir* для идентификации сведений о системе на основе существующих файлов и каталогов.

Mac
Команда *systemsetup* выдаёт подробную информацию о системе, но она требует административных привилегий. Кроме того, подробную разбивку конфигураций, правил брандмауэра, подключенных томов, оборудования и многих других вещей без необходимости повышения привилегий выдаёт *system_profiler*.

Обнаружение параметров конфигурации сети (System Network Configuration Discovery)

Система: Windows, Linux, macOS
Права: Пользователь
Описание: Злоумышленник, вероятнее всего, будет искать подробные сведения о сетевой конфигурации и параметрах систем к которым он имеет доступ или через исследование удаленных систем. Некоторые утилиты, предназначенные для администрирования операционной системы, могут использоваться для сбора вышеуказанной информации. Примеры таких утилит: *arp, ipconfig/ifconfig, nbtstat, route, tracert/tracerout* и т.п.

Обнаружение сетевых подключений (System Network Connections Discovery)

Система: Windows, Linux, macOS
Права: Пользователь, администратор
Описание: Злоумышленники могут пытаться получить список входящих и исходящих

сетевых подключений компрометированной системы, к которой они имеют доступ, или удаленной системы, запрашивая информацию по сети.

Windows
Утилиты и команды для получения сведений о сетевых подключениях:

```
Netstat
net use
net session
```

Mac и Linux
Для отображения текущих соединений могут использоваться *netstat* и *lsof*. По аналогии с "*net session*", утилиты *who* и *w* могут отображать текущих пользователей, вошедших в систему.

Обнаружение владельца/пользователя системы (System Owner/User Discovery)

Система: Windows, Linux, macOS
Права: Пользователь, администратор
Описание: Злоумышленники могут пытаться идентифицировать основного пользователя системы, текущего пользователя, зарегистрированного в данный момент, группу пользователей, которые обычно используют систему или определить на сколько активно пользователь использует систему. Противник может получать вышеуказанные сведения путем методов выявления учетных записей (см. технику «Обнаружение учетных записей») или используя методы Дампинга учетных данных. Сведения о пользователе и его имени распространены во всей системе — включены в информацию о владельцах процессов, файлов и каталогов, в информацию о сеансах и системные журналы, поэтому противник может применять различные методы обнаружения.
В Mac, текущий пользователь может быть идентифицирован с помощь утилит *users, w* и *who*. В linux-системах — только с помощью *w* и *who*.

Обнаружение системных сервисов (System Service Discovery)

Система: Windows
Права: Пользователь, администратор, System
Описание: Злоумышленник может пытаться получить информацию о зарегистрированных службах. Для сбора данных противник может использовать различные инструменты, в том числе встроенные утилиты, которые могут получать сведения о службах:

```
sc
tasklist /svc
net start
```

Раскрытие системного времени (System Time Discovery)

Система: Windows
Права: Пользователь
Описание: Системное время устанавливается в домене и хранится Службой времени (Windows Times Service) для обеспечения синхронизации времени между системами и сервисами в сети предприятия. Злоумышленник может получить системное время и/или часовой пояс из локальной или удаленной системы. Эта информация может быть собрана несколькими способами:
`net time \\hostname` — получение системного времени хоста;
`w32tm /tz` — получение часового пояса.
Информация о системном времени может быть полезна для применения противником различных методов атак, таких как выполнения файла с запланированной задачей или, основываясь на сведениях о часовом поясе, для раскрытия местоположения жертвы. *Рекомендации по защите:* Доброкачественное ПО использует легитимные процессы для сбора системного времени. Усилия по защите необходимо направлять на предотвращение выполнения нежелательного или неизвестного кода в системе. В целях предотвращения несанкционированного получения сведений о времени с удаленной системы такие инструменты как утилита *Net* могут быть заблокированы политикой безопасности. Мониторинг командной строки может быть полезен для обнаружения экземпляров Net.exe или других утилит, используемых для сбора системного времени и часового пояса. Мониторинг вызовов API в данных целях менее полезен из-за того, что API часто используется законным программным обеспечением.