Содержание

Вопрос

- То, почему компьютерные имена машины или имена пользователей NULL, вошло в accesslog?
- Как вы определяете запросы с помощью рабочей станции или учетных данных NULL для более позднего опознавательного освобождения?

Среда

- Cisco Web Security Appliance (WSA) - все версии
- Схема проверки подлинности NTLMSSP с заместителями IP
- Windows Vista и более новая настольная и мобильная Microsoft Operation Systems

Признаки

WSA блокирует запросы от некоторых пользователей или неожиданно ведет себя. Accesslog показывают компьютерные имена машины или имя пользователя NULL и домен вместо идентификаторов пользователей.

Проблема решает себя после:

- Заместители испытывают таймаут (значение по умолчанию для Суррогатного Таймаута составляет 60 минут),
- Перезапуск процесса прокси (команда CLI> *диагностика*> *прокси*> *удар*)
- Сбрасывание опознавательного кэша (команда CLI> *authcache*> *flushall*)

Общие сведения

В последних версиях операционной системы Microsoft не требуется, что в реального пользователя больше входят для приложений для отправления запросов к Интернету больше. Когда те запросы получает WSA и запрашивают аутентифицироваться, никакие учетные данные пользователя не доступны для использования для аутентификации клиентской рабочей станцией, которая вместо этого может взять имя машины компьютера для замены.

WSA возьмет предоставленное имя машины и передаст его Active Directory (AD), который

проверяет его.

С проверенной аутентификацией WSA создает Заместителя IP привязка названия рабочей станции машины к IP-адресу рабочей станции. Дальнейшие запросы, прибывающие из того же IP, будут использовать заместителя и таким образом название рабочей станции.

С названием рабочей станции, не являющимся участником любой AD группы, запросы могут не инициировать ожидаемую Политику доступа и таким образом быть заблокированы. Проблема сохраняется, пока заместитель не испытал таймаут, и аутентификация должна быть возобновлена. На этот раз, с реальным пользователем, в которого входят и доступные учетные данные допустимого пользователя, новый Заместитель IP будет создан с этой информацией, и дальнейшие запросы будут совпадать с ожидаемой Политикой доступа.

Когда приложения передают недопустимые учетные данные (имя пользователя NULL и домен NULL) и НЕ допустимые учетные данные машины, другой замеченный сценарий. Это считают ошибкой проверки подлинности и заблокируют или если гостевая политика включена, отказавшую аутентификацию рассматривают как "гостя".

Название рабочей станции заканчивается **$**, придерживавшимся **@DOMAIN**, который делает названия рабочей станции легкими отследить при помощи команды CLI **grep** на accesslog за **$**. Посмотрите пример ниже для разъяснения.

```
> grep $@ accesslogs

1332164800.0000 9 10.20.30.40 TCP_DENIED/403 5608 GET http://www.someURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_WEBCAT_11-DefaultGroup-Internet-NONE-NONE-
NONE-NONE <-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

Линия выше показов пример Заместителя IP, уже созданного для IP-адреса 10.20.30.40 и имени машины **gb0000d01$.**

Для обнаружения запроса, который передал имя машины, первое возникновение названия рабочей станции для определенного IP-адреса должны быть определены. Следующая команда CLI выполняет это:

```
> grep 10.20.30.40 -p accesslogs
```

Ищите результат первое возникновение названия рабочей станции. Три первых запроса обычно распознаются как NTLM Single-Sin-On (NTLMSSP/NTLMSSP) квитирование, как описано здесь и показываются в примере ниже:

```
1335248044.836 0 10.20.30.40 TCP_DENIED/407 1733 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.839 0 10.20.30.40 TCP_DENIED/407 483 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.845 10 10.20.30.40 TCP_DENIED/403 2357 GET http://SomeOtherURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_ADMIN_PROTOCOL_11-DefaultGroup-DefaultGroup-
DefaultGroup-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

При устранении проблем гарантируйте, что они тебя запросы для того же URL и

зарегистрированы в очень кратковременном интервале indicatiting, что это - автоматизированное квитирование NTLMSSP.

В то время как прозрачные запросы были бы зарегистрированы с Кодом ответа HTTP 401 (Не прошедший поверку подлинности), в приведенном выше примере предыдущие запросы зарегистрированы с Кодом ответа HTTP 407 (Требуемая проверка подлинности прокси-сервера) для явных запросов.

Существует новая характеристика, доступная на AsyncOS 7.5.0 и выше где можно определить другой суррогатный таймаут для учетных данных машины. Это может быть настроено с помощью следующей команды:

```
1335248044.836 0 10.20.30.40 TCP_DENIED/407 1733 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.839 0 10.20.30.40 TCP_DENIED/407 483 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.845 10 10.20.30.40 TCP_DENIED/403 2357 GET http://SomeOtherURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_ADMIN_PROTOCOL_11-DefaultGroup-DefaultGroup-
DefaultGroup-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

Можно использовать те же шаги для обнаружения, который запросы передали учетные данные NULL и обнаруживают, какой URL или Клиент User Agent передают недопустимые учетные данные и освобождают их от аутентификации.

Освобождение URL от аутентификации

Для предотвращения этого запроса, заставляющего ложного заместителя быть созданным, URL должен быть освобожден от аутентификации. Или, вместо того, чтобы освободить URL от аутентификации, вы могли бы решить освободить приложение, отправляющее сам запрос от аутентификации, удостоверившись заставлять любые запросы о приложении быть освобожденными от аутентификации. Это возможно путем добавления Клиента User Agent, который будет зарегистрирован в accesslog путем добавления дополнительного параметра **%u** в дополнительных **Пользовательских Полях** в подписке accesslog WSA. После определения Клиента User Agent это должно быть освобождено от аутентификации.