Содержание

Введение

В этом документе даются указания по защите протокола SNMP. Защита SNMP особенно важна в случае многократной атаки, эксплуатирующей уязвимости SNMP для провоцирования отказа в обслуживании (DoS).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Средство просмотра протокола SNMP? Релиз 10.3 или более поздний Программное обеспечение Cisco IOS.
- Протокол SNMP версии 3? Представленный в программном обеспечении Cisco IOS версии 12.0(3)T.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Стратегии защиты SNMP

Выберите строку хорошего сообщества SNMP

Это не полезный прием для использования **общественности**, столь же только для чтения и **частной** как строки имени и пароля для чтения и записи.

Настройка просмотра SNMP

Команда Setup SNMP view может заблокировать пользователя с только доступом к ограниченной Информационной базе управления (MIB). По умолчанию нет никакой **записи представления SNMP, существует**. Эта команда настроена в режиме глобальной конфигурации и сначала представлена в версии программного обеспечения Cisco IOS 10.3. Это работает подобное **access-list** в том, что, если у вас есть какое-либо **Представление SNMP** об определенных деревьях MIB, любое дерево запрещено необъяснимо. Однако последовательность не важна, и она проходит весь список для соответствия, прежде чем она остановится.

Чтобы создать или обновить обзорную запись, используйте **команду snmp-server view global configuration**. Для удаления указанной записи представления сервера SNMP используйте **эту команду с параметром no**.

Синтаксис:

```
snmp-server view view-name oid-tree {included | excluded} no snmp-server view view-name
```

Описание синтаксиса:

- **имя для просмотра**? Метка для обзорной записи, которую вы обновляете или создаете. Название используется для ссылки на запись.
- **дерево oid**? Идентификатор объекта Abstract Syntax Notation One (ASN.1) поддерево, которое будет включено или исключено из представления. Для определения поддерева задайте текстовую строку, состоящую из номеров, такой как 1.3.6.2.4, или слово, таких как **система**. Замените одиночный подыдентификатор звездочкой (*) подстановочный знак для определения семейства подчиненных деревьев; например, 1.3. *.4.
- **включенный | исключенный**? Тип представления. Необходимо задать или включенный или исключенный.

Когда представление требуется, вместо того, чтобы определить представление, могут использоваться два стандартных предварительных просмотра. Каждый - все, которое указывает, что пользователь видит все объекты. Другой *ограничен*, который указывает, что пользователь видит три группы: **система**, **snmpStats**, и **snmpParties**. Предварительно определенные представления описаны в RFC 1447.

Примечание: Первая **команда snmp-server**, которую вы вводите, включает обе версии SNMP.

Данный пример создает представление, которое включает все объекты в Группу системы MIB-II за исключением **sysServices** (Система 7) и все объекты для интерфейса 1 в группе интерфейсов MIB-II:

```
snmp-server view agon system includedsnmp-server view agon system.7 excluded snmp-server view agon ifEntry.*.1 included
```

Это - завершенный пример для того, как применить MIB со строкой имени и пароля и выходными данными **snmpwalk** с **представлением** на месте. Эта конфигурация определяет представление, которое запрещает доступ SNMP для таблицы протокола разрешения адресов (ARP) **(atEntry)** и позволяет его для MIB-II и Cisco частный MIB:

```
snmp-server view myview mib-2 includedsnmp-server view myview atEntry excludedsnmp-server view myview cisco includedsnmp-server community public view myview RO 11snmp-server community private view myview RW 11snmp-server contact pvanderv@cisco.com
```

Это - команда и выходные данные для Группы системы MIB-II:

```
NMSPrompt 82 % snmpwalk cough system system.sysDescr.0 : DISPLAY STRING- (ascii):Cisco Internetwork Operating System Software IOS (tm) 2500 Software (C2500-JS-L), Version 12.0(1)T,RELEASE SOFTWARE (fc2) Copyright (c) 1986-1998 by cisco Systems, Inc. Compiled Wed 04-Nov-98 20:37 by dschwart system.sysObjectID.0 : OBJECT IDENTIFIER: .iso.org.dod.internet.private.enterprises.cisco.ciscoProducts.cisco2520 system.sysUpTime.0 : Timeticks: (306588588) 35 days, 11:38:05.88 system.sysContact.0 : DISPLAY STRING- (ASCII):pvanderv@cisco.com system.sysName.0 : DISPLAY STRING- (ASCII):cough system.sysLocation.0 : DISPLAY STRING- (ASCII): system.sysServices.0 : INTEGER: 78 system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00 NMSPrompt 83 %
```

Это - команда и выходные данные для локальной группы системы Cisco:

```
NMSPrompt 83 % snmpwalk cough lsystem cisco.local.lsystem.romId.0 : DISPLAY STRING- (ASCII): System Bootstrap, Version 11.0(10c), SOFTWARE Copyright (c) 1986-1996 by cisco Systems cisco.local.lsystem.whyReload.0 : DISPLAY STRING- (ASCII):power-on cisco.local.lsystem.hostName.0 : DISPLAY STRING- (ASCII):cough
```

Это - команда и выходные данные для таблицы ARP MIB-II:

```
NMSPrompt 84 % snmpwalk cough atTable no MIB objects contained under subtree. NMSPrompt 85 %
```

Настройка SNMP Community с помощью списка доступа

Лучшая существующая практика рекомендует применить Списки контроля доступа (ACL) к строкам имени и пароля и гарантировать, что строки имени и пароля запросов не идентичны строкам имени и пароля уведомлений. Списки доступа обеспечивают дальнейшую защиту, когда используется в сочетании с другими защитными мерами.

Данный пример устанавливает ACL к строке имени и пароля:

```
access-list 1 permit 1.1.1.1 snmp-server community string1 ro 1
```

Если строка имени и пароля обнаружена атакующим, ли путем заключения компромисса удаленного устройства или путем сниффинга сообщения прерывания от сети без авторизации, Использование других строк имени и пароля для запросов и сообщений прерывания уменьшает вероятность дополнительных атак или компромиссов.

Как только вы включаете trap-сообщение со строкой имени и пароля, строка может быть включена для доступа SNMP в некотором программном обеспечении Cisco IOS. Необходимо явно отключить это сообщество.

Пример:

```
access-list 10 deny any snmp-server host 1.1.1.1 mystring1 snmp-server community mystring1 RO 10
```

Настройка SNMP версии 3

Версия SNMP 3 была сначала представлена в версии программного обеспечения Cisco IOS 12.0, но еще обычно не используется в управлении сетью. Для настройки версии SNMP 3 выполните эти шаги:

1. Назначьте идентификатор ядра для объекта SNMP (Необязательно).
2. Определите пользователя, **userone**, принадлежа группе **groupone** и примените **noAuthentication** (никакой пароль) и **noPrivacy** (никакое шифрование) этому пользователю.
3. Определите пользователя, **usertwo**, принадлежа группе **grouptwo** и примените **noAuthentication** (никакой пароль) и **noPrivacy** (никакое шифрование) этому пользователю.
4. Определите пользователя, **userthree**, принадлежа группе **groupthree** и примените **Аутентификацию** (пароль является user3passwd), и **noPrivacy** (никакое шифрование) этому пользователю.
5. Определите пользователя, **userfour**, принадлежа группе **groupfour** и примените **Аутентификацию** (пароль является user4passwd), и **Конфиденциальность** (des56 шифрование) этому пользователю.
6. Определите группу, **groupone**, с помощью V3 User Security Model (USM) и имея доступ для чтения на представлении **v1default** (по умолчанию).
7. Определите группу, **grouptwo**, с помощью V3 USM и имея доступ для чтения на представлении **myview**.
8. Определите группу, **groupthree**, с помощью V3 USM, имея доступ для чтения на представлении **v1default** (по умолчанию), и с помощью **аутентификации**.
9. Определите группу, **groupfour**, с помощью V3 USM, имея доступ для чтения на представлении **v1default** (по умолчанию), и с помощью **Аутентификации** и **Конфиденциальности**.
10. Определите представление, **myview**, который предоставляет доступ для чтения на MIB-II и запрещает доступ для чтения на частном MIB Cisco.**Выходные данные show running** дают дополнительные линии для **общественности** группы, вследствие того, что существует строка имени и пароля **общественность** Только для чтения, которая была определена.**Выходные данные show running** не показывают **userthree**.Пример:**snmp-server engineID local 1111000000000000000000snmp-server user userone groupone v3 snmp-server user usertwo grouptwo v3 snmp-server user userthree groupthree v3 auth md5 user3passwd snmp-server user userfour groupfour v3 auth md5 user4passwd priv des56 user4priv snmp-server group groupone v3 noauth snmp-server group grouptwo v3 noauth read myview snmp-server group groupthree v3 auth snmp-server group groupfour v3 priv snmp-server view myview mib-2 included snmp-server view myview cisco excluded snmp-server community public RO**

Это - команда и выходные данные для Группы системы MIB-II с помощью **пользователя userone**:

```
NMSPrompt 94 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy system Module SNMPV2-TC not
found system.sysDescr.0 = Cisco Internetwork Operating System Software IOS (TM) 4500 Software
(C4500-IS-M), Version 12.0(3)T,RELEASE SOFTWARE (fc1) Copyright (c) 1986-1999 by cisco Systems,
Inc. Compiled Tue 23-Feb-99 03:59 by ccai system.sysObjectID.0 = OID: enterprises.9.1.14
system.sysUpTime.0 = Timeticks: (28208096) 3 days, 6:21:20.96 system.sysContact.0 =
system.sysName.0 = clumsy.cisco.com system.sysLocation.0 = system.sysServices.0 = 78
system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00NMSPrompt 95 %
```

Это - команда и выходные данные для Группы системы MIB-II с помощью пользовательского **usertwo**:

```
NMSPrompt 95 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy system  Module SNMPV2-TC not found system.sysDescr.0 = Cisco Internetwork Operating System Software IOS (TM) 4500 Software (C4500-IS-M), Version 12.0(3)T,RELEASE SOFTWARE (fc1) Copyright (c) 1986-1999 by cisco Systems, Inc. Compiled Tue 23-Feb-99 03:59 by ccai system.sysObjectID.0 = OID: enterprises.9.1.14 system.sysUpTime.0 = Timeticks: (28214761) 3 days, 6:22:27.61 system.sysContact.0 = system.sysName.0 = clumsy.cisco.com system.sysLocation.0 = system.sysServices.0 = 78 system.sysORLastChange.0 = Timeticks: (0) 0:00:00.00
```

Это - команда и выходные данные для Локальной системной группы Cisco с помощью **пользователя userone**:

```
NMSPrompt 98 % snmpwalk -v3 -n "" -u userone -l noAuthNoPriv clumsy .1.3.6.1.4.1.9.2.1  Module SNMPV2-TC not found enterprises.9.2.1.1.0 = "..System Bootstrap, Version 5.2(7b) [mkamson 7b], RELEASE SOFTWARE (fc1)..Copyright (c) 1995 by cisco Systems,Inc..." enterprises.9.2.1.2.0 = "reload"enterprises.9.2.1.3.0 = "clumsy"enterprises.9.2.1.4.0 = "cisco.com"
```

Это - команда и выходные данные, показывая, что вы не можете получить Локальную системную группу Cisco с помощью пользовательского **usertwo**:

```
NMSPrompt 99 % snmpwalk -v3 -n "" -u usertwo -l noAuthNoPriv clumsy .1.3.6.1.4.1.9.2.1  Module SNMPV2-TC not found enterprises.9.2.1 = No more variables left in this MIB View NMSPrompt 100 %
```

Эта команда и результат для специализированного **tcpdump** (исправление для поддержки версии SNMP 3 и приложение printf):

```
NMSPrompt 102 % snmpget -v3 -n "" -u userone -l noAuthNoPriv clumsy system.sysName.0 Module SNMPV2-TC not found system.sysName.0 = clumsy.cisco.com
```

ACL настройки на интерфейсах

ACL является одной из мер безопасности и позволяет предотвратить имитацию IP-адресов (спуфинг). ACL можно применять к входящим или исходящим интерфейсам маршрутизаторов.

На платформах, которые не имеют опции для использования, получают ACL (rACL), возможно разрешить трафик Протокола UDP к маршрутизатору от IP-адресов, которым доверяют, с интерфейсными ACL.

Следующий расширенный список доступа может быть адаптирован к вашей сети. Данный пример предполагает, что маршрутизатор имеет IP-адреса 192.168.10.1 и 172.16.1.1 настроенных на его интерфейсах, что весь доступ SNMP должен быть ограничен станцией управления с IP-адресом 10.1.1.1, и что станция управления должна только связаться с IP-адресом 192.168.10.1:

```
access-list 101 permit udp host 10.1.1.1 host 192.168.10.1
```

Access-list должен тогда быть применен ко всем интерфейсам с помощью этих команд настройки:

```
interface ethernet 0/0ip access-group 101 in
```

Все устройства, которые связываются непосредственно с маршрутизатором на портах UDP, должны будут быть в частности перечислены в вышеупомянутом списке доступа. Программное обеспечение Cisco IOS использует порты в диапазоне 49152 - 65535 как исходный порт для сеансов исходящего соединения, таких как запросы Системы доменных имен (DNS).

Для устройств, которые имеют много IP-адресов, настроенных или много хостов, которые

должны связаться с маршрутизатором, это может не быть масштабируемым решением.

rACL

Для распределенных платформ rACL могут быть опцией, запускающейся в программном обеспечении Cisco IOS версии 12.0(21)S2 для Коммутируемого маршрутизатора Серии Gigabit Cisco 12000 (GSR) и релиз 12.0 (24) S для Cisco серии 7500. Получить списки доступа защищают устройство от вредного трафика, прежде чем трафик сможет повлиять на процессор маршрута. ACL тракта приема также считают оптимальным методом сетевой безопасности и нужно рассмотреть как долгосрочное добавление к хорошей сетевой безопасности, а также обходной путь для этой определенной уязвимости. Загрузка ЦПУ распределена процессорам линейной карты и помогает смягчать загрузку на процессоре основного маршрута. Статья под названием "GSR: Получите Списки контроля доступа, поможет определять и позволять легальный трафик вашему устройству и запрещать все нежелательные пакеты..

Инфраструктурные списки ACL

Несмотря на то, что часто трудно заблокировать трафик, передающий транзитом вашу сеть, возможно определить трафик, которому никогда нельзя позволять предназначаться для ваших устройств, относящихся к инфраструктуре и блока что трафик на границе вашей сети. ACL инфраструктуры (iACLs) считают оптимальным методом сетевой безопасности и нужно рассмотреть как долгосрочное добавление к хорошей сетевой безопасности, а также обходной путь для этой определенной уязвимости. Статья под названием "Защита ядра: Списки контроля доступа Защиты инфраструктуры представляют рекомендации и рекомендуемые методы развертывания для iACLs..

Характеристика безопасности коммутатора локальной сети (LAN) Cisco Catalyst

Функция IP Permit List ограничивает входящий доступ Telnet и SNMP к коммутатору с несанкционированных исходных IP-адресов. Поддерживаются сообщения Syslog и ловушки SNMP, чтобы уведомлять систему управления о нарушениях или о несанкционированном доступе.

Комбинация характеристик безопасности программного обеспечения Cisco IOS может использоваться для управления маршрутизаторами и коммутаторами Cisco Catalyst. Необходимо установить политику безопасности, которая ограничивает количество управляющих станций с возможностью доступа к коммутаторам и маршрутизаторам.

Для получения дополнительной информации о том, как увеличить безопасность на IP - сетях, обратитесь к Повышению безопасности на IP - сетях.

Проверка ошибок SNMP

Настройте ACL сообщества SNMP с **регистрационным** ключевым словом. **Системный журнал** монитора для неудачных попыток, как показывают ниже.

```
access-list 10 deny any log snmp-server community public RO 10
```

Когда кто-то пытается обратиться к маршрутизатору со строкой сообщества public, вы

видите **системный журнал**, подобный придерживающемуся:

```
access-list 10 deny any log snmp-server community public RO 10
```

Эти выходные данные означают, что access-list 10 запретил пять Пакетов snmp от хоста 172.16.1.1.

Периодически проверяйте SNMP путем выполнения **команды show snmp**, как показано здесь:

```
router#show snmp Chassis: 21350479 17005 SNMP packets input 37 Bad SNMP version errors**15420
Unknown community name**0 Illegal operation for community name supplied 1548 Encoding errors**0
Number of requested variables 0 Number of altered variables 0 Get-request PDUs 0 Get-next PDUs 0
Set-request PDUs 0 SNMP packets output 0 Too big errors (Maximum packet size 1500) 0 No such
name errors 0 Bad values errors 0 General errors 0 Response PDUs 0 Trap PDUs
```

Наблюдайте счетчики, отмеченные ** для неожиданных увеличений в частотах ошибок, которые могут указать на попытку разведки этих уязвимостей. Для создания отчетов о любой проблеме безопасности обратитесь к расследованию инцидента, связанного с безопасностью продукта Cisco.

Дополнительные сведения

- Уязвимость SNMP информационных сообщений Cisco Security
- V3 SNMP настройки с IOS 12.0
- Упрощенный протокол управления сетью (SNMP)
- Настройке функции SNMP
- Техническая поддержка - Cisco Systems