Как передать пример сообщения, чтобы гарантировать, что Антивирусный механизм просматривает на Cisco Email Security Appliance (ESA)

Содержание

Введение

Этот документ описывает, как передать пример сообщения для обеспечения или антивируса Sophos или механизма антивируса McAfee, просматривает на Cisco Email Security Appliance (ESA).

Как передать пример сообщения, чтобы гарантировать, что Антивирусный механизм просматривает на Cisco Email Security Appliance (ESA)

Путем передачи примера сообщения с тестом вирусное информационное наполнение через ESA мы можем инициировать механизм антивируса Sophos или McAfee. До выполнения шагов перечислил в этом документе, необходимо будет установить Политику Входящей или Исходящей почты и настроить почтовую политику для имения антивирусного отбрасывания, или карантинный вирус заразил сообщения. Этот документ использует код ASCII, предоставленный от EICAR (www.eicar.org), который моделирует тестовый вирус как прикрепление:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

> **Примечание:** На EICAR: *Этот тестовый файл был предоставлен EICAR для распределения как "Стандарт EICAR Антивирусный Тестовый файл", и это удовлетворяет все упомянутые выше критерии. Безопасно раздать, потому что это не вирус и не включает фрагментов зараженного вирусом кода. Большинство продуктов реагирует на него, как будто это был вирус (хотя они, как правило, сообщают о нем с очевидным названием, таким как "EICAR-AV-Test").*

Создайте текстовый файл

Использование Строки ASCII выше, создайте файл .txt и разместите строку, столь же записанную как тело файла. Вы будете в состоянии передать этот файл как прикрепление в вашем примере сообщения.

Передача примера сообщения

В зависимости от того, как вы работаете, можно передать пример сообщения через различные способы ESA. Два метода в качестве примера через CLI UNIX с помощью **почты** или от Outlook (или другое приложение для работы с электронной почтой).

CLI UNIX

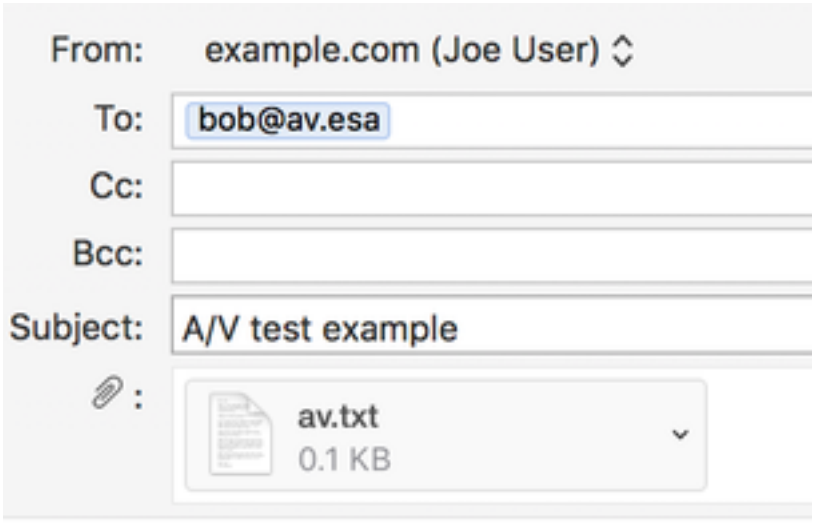
```
joe@unix.local:~$ echo "TEST MESSAGE w/ ATTACHMENT" | mail -s "A/V test example" -A av.txt
bob@av.esa
```

Ваша Среда UNIX должна будет быть должным образом настройкой, чтобы передать или передать почту через ваш ESA.

Outlook

Использование Outlook (или другое приложение для работы с электронной почтой), у вас есть два выбора в передаче кода ASCII через: 1) с помощью созданного файла .txt, 2) прямая вставка Строки ASCII в теле сообщения электронной почты.

С помощью. текстовый файл как прикрепление:



TEST MESSAGE w/ ATTACHMENT

Использование Строки ASCII в теле сообщения электронной почты:


```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Ваш Outlook (или другое приложение для работы с электронной почтой) должен будет быть должным образом настройкой, чтобы передать или передать почту через ваш ESA.

Проверка

На CLI ESA используйте **хвост** команды **mail_logs** до передачи примера сообщения. При наблюдении почтового журнала вы будете видеть, что сообщение просмотрено и поймано McAfee как "VIRAL":

```
Wed Sep 13 11:42:38 2017 Info: New SMTP ICID 306 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:42:38 2017 Info: ICID 306 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
Wed Sep 13 11:42:38 2017 Info: Start MID 405 ICID 306
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 From: <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 ICID 306 RID 0 To: <bob@av.esa>
Wed Sep 13 11:42:38 2017 Info: MID 405 Message-ID '<20170913153801.0EDA1A0121@example.com>'
Wed Sep 13 11:42:38 2017 Info: MID 405 Subject 'A/V test attachment'
Wed Sep 13 11:42:38 2017 Info: MID 405 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:42:38 2017 Info: MID 405 attachment 'av.txt'
Wed Sep 13 11:42:38 2017 Info: ICID 306 close
Wed Sep 13 11:42:38 2017 Info: MID 405 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:42:38 2017 Info: MID 405 interim AV verdict using McAfee VIRAL
Wed Sep 13 11:42:38 2017 Info: MID 405 antivirus positive 'EICAR test file'
Wed Sep 13 11:42:38 2017 Info: MID 405 enqueued for transfer to centralized quarantine "Virus"
(a/v verdict VIRAL)
Wed Sep 13 11:42:38 2017 Info: MID 405 queued for delivery
Wed Sep 13 11:42:38 2017 Info: New SMTP DCID 239 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:42:38 2017 Info: DCID 239 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:42:38 2017 Info: Delivery start DCID 239 MID 405 to RID [0] to Centralized Policy
Quarantine
Wed Sep 13 11:42:38 2017 Info: Message done DCID 239 MID 405 to RID [0] (centralized policy
quarantine)
Wed Sep 13 11:42:38 2017 Info: MID 405 RID [0] Response 'ok: Message 49 accepted'
Wed Sep 13 11:42:38 2017 Info: Message finished MID 405 done
Wed Sep 13 11:42:43 2017 Info: DCID 239 close
```

То же сообщение, передаваемое через и просмотренное Sophos:

```
Wed Sep 13 11:44:24 2017 Info: New SMTP ICID 307 interface Management (10.1.2.84) address
10.1.2.85 reverse dns host zane.local verified yes
Wed Sep 13 11:44:24 2017 Info: ICID 307 ACCEPT SG UNKNOWNLIST match sbrs[none] SBRS None country
Australia
```

```
Wed Sep 13 11:44:24 2017 Info: Start MID 406 ICID 307
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 From: <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 ICID 307 RID 0 To: <bob@av.esa>
Wed Sep 13 11:44:24 2017 Info: MID 406 Message-ID '<20170913153946.E20C7A0121@example.com>'
Wed Sep 13 11:44:24 2017 Info: MID 406 Subject 'A/V test attachment'
Wed Sep 13 11:44:24 2017 Info: MID 406 ready 1057 bytes from <joe@example.com>
Wed Sep 13 11:44:24 2017 Info: MID 406 attachment 'av.txt'
Wed Sep 13 11:44:24 2017 Info: ICID 307 close
Wed Sep 13 11:44:24 2017 Info: MID 406 matched all recipients for per-recipient policy my_av in
the inbound table
Wed Sep 13 11:44:24 2017 Info: MID 406 interim AV verdict using Sophos VIRAL
Wed Sep 13 11:44:24 2017 Info: MID 406 antivirus positive 'EICAR-AV-Test'
Wed Sep 13 11:44:24 2017 Info: MID 406 enqueued for transfer to centralized quarantine "Virus"
(a/v verdict VIRAL)
Wed Sep 13 11:44:24 2017 Info: MID 406 queued for delivery
Wed Sep 13 11:44:24 2017 Info: New SMTP DCID 240 interface 10.1.2.84 address 10.1.2.87 port 7025
Wed Sep 13 11:44:24 2017 Info: DCID 240 TLS success protocol TLSv1.2 cipher DHE-RSA-AES256-GCM-
SHA384 the.cpq.host
Wed Sep 13 11:44:24 2017 Info: Delivery start DCID 240 MID 406 to RID [0] to Centralized Policy
Quarantine
Wed Sep 13 11:44:24 2017 Info: Message done DCID 240 MID 406 to RID [0] (centralized policy
quarantine)
Wed Sep 13 11:44:24 2017 Info: MID 406 RID [0] Response 'ok: Message 50 accepted'
Wed Sep 13 11:44:24 2017 Info: Message finished MID 406 done
Wed Sep 13 11:44:29 2017 Info: DCID 240 close
```

На этом ESA лабораторной работы, 'Вирус Зараженные сообщения' настроен для Изоляции для "Действия, Прикладного для обмена сообщениями" на определенной почтовой политике. Действие с вашим ESA может варьироваться, на основе мер, принятых для зараженных сообщений вируса, обрабатываемых антивирусом на вашей почтовой политике.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация