RADIUS недопустимое руководство устранения неполадок средства проверки подлинности и средства проверки подлинности сообщения

Содержание

Введение

Этот документ описывает два механизма обеспечения безопасности RADIUS:

- Заголовок средства проверки подлинности
- Атрибут средства проверки подлинности сообщения

Этот документ покрывает, каковы эти механизмы обеспечения безопасности, как они используются, и когда необходимо ожидать сбой проверки.

Заголовок средства проверки подлинности

На RFC 2865 Заголовок Средства проверки подлинности 16 байтов длиной. Когда это используется в Access-Request, это называют Средством проверки подлинности Запроса. Когда это используется в любом виде ответа, это называют Средством проверки подлинности Ответа. Это используется для:

- Аутентификация ответа
- Сокрытие пароля

Аутентификация ответа

Если сервер отвечает корректным Средством проверки подлинности Ответа, клиент может вычислить, если тот ответ был отнесен к допустимому запросу.

Клиент отправляет запрос со случайным Заголовком Средства проверки подлинности. Затем сервер, который передает ответ, вычисляет Средство проверки подлинности Ответа с использованием пакета запроса наряду с общим секретным ключом:

```
ResponseAuth = MD5(Code + ID + Length + RequestAuth + Attributes + Secret)
```

Клиент, который получает ответ, выполняет ту же операцию. Если результатом является то же, пакет корректен.

> **Примечание:** Атакующий, который знает секретное значение, не в состоянии имитировать ответ, пока это не в состоянии осуществить сниффинг запроса.

Когда необходимо ожидать сбой проверки?

Если коммутатор больше не кэширует запрос (например, из-за таймаута), сбой проверки происходит. Вы могли бы также испытать его, когда общий секретный ключ недопустим (да - Access-Reject также включает этот заголовок). Таким образом, Устройство доступа к сети (NAD) может обнаружить несоответствие общего секретного ключа. Обычно об этом сообщают клиенты/серверы Аутентификации, авторизации и учета (AAA) как несоответствие общего ключа, но это не показывает подробные данные.

Сокрытие пароля

Заголовок Средства проверки подлинности также используется во избежание передачи атрибута User-Password в открытом тексте. Сначала Профиль сообщения 5 (MD5 - тайна, средство проверки подлинности) вычислен. Затем несколько операций XOR с блоками пароля выполняются. Этот метод восприимчив для офлайновых атак (таблицы радуги), потому что MD5 больше не воспринимается как сильный односторонний алгоритм.

Вот сценарий Python, который вычисляет User-Password:

```
def Encrypt_Pass(password, authenticator, secret):
       m = md5()
       m.update(secret+authenticator)
       return "".join(chr(ord(x) ^ ord(y)) for x, y in zip(password.ljust
(16,'\0')[:16], m.digest()[:16]))
```

Повторные передачи

Если какой-либо из атрибутов в Access-Request RADIUS изменился (как ID RADIUS, Имя пользователя, и так далее), новое поле Authenticator должно генерироваться и все другие поля, которые зависят от него, должен быть повторно вычислен. Если это - повторная передача, ничто не должно изменяться.

Учет

Значение Заголовка Средства проверки подлинности является другим для Access-Request и Бухгалтерского Запроса.

Для Access-Request Средство проверки подлинности генерируется случайным образом, и оно, как ожидают, получит ответ с ResponseAuthenticator, вычисленным правильно, который доказывает, что ответ был отнесен к тому конкретному запросу.

Для Бухгалтерского Запроса Средство проверки подлинности не случайно, но оно вычислено (согласно RFC 2866):

```
RequestAuth = MD5(Code + ID + Length + 16 zero octets + Attributes + Secret)
```

Если перерасчетное значение не совпадает со значением Средства проверки подлинности, Таким образом, сервер может сразу проверить бухгалтерское сообщение и отбросить пакет. Платформа Identity Services Engine (ISE) возвращается:

```
11038 RADIUS Accounting-Request header contains invalid Authenticator field
```

Типичная причина для этого является неправильным общим секретным ключом.

Атрибут средства проверки подлинности сообщения

Атрибут Средства проверки подлинности сообщения является атрибутом RADIUS, определенным в RFC 3579. Это используется для подобной цели: подписать и проверить. Но на этот раз, это не используется для проверки ответа, но запроса.

Клиент, который передает Access-Request (это может также быть сервер, который отвечает проблемой Доступа) вычисляет Hash-Based Message Authentication Code (HMAC) - MD5 от его собственного пакета, и затем добавляет атрибут Средства проверки подлинности сообщения как подпись. Затем сервер в состоянии проверить, что он выполняет ту же операцию.

Формула выглядит подобной Заголовку Средства проверки подлинности:

```
Message-Authenticator = HMAC-MD5 (Type, Identifier, Length, Request Authenticator,
Attributes)
```

Функция HMAC-MD5 берет в двух аргументах:

- Информационное наполнение пакета, который включает 16-байтовое поле Message-Authenticator, заполненное нулями
- Общий секрет

Когда должно использоваться Средство проверки подлинности сообщения?

MUST Средства проверки подлинности сообщения использоваться для каждого пакета, который включает сообщение Протокола EAP (RFC 3579). Это включает и клиента, который передает Access-Request и сервер, который отвечает проблемой Доступа. Если проверка отказывает, другая сторона должна тихо отбросить пакет.

Когда необходимо ожидать сбой проверки?

Когда общий секретный ключ будет недопустим, сбой проверки произойдет. Затем AAA-сервер не в состоянии проверить запрос.

Отчёты о ISE:

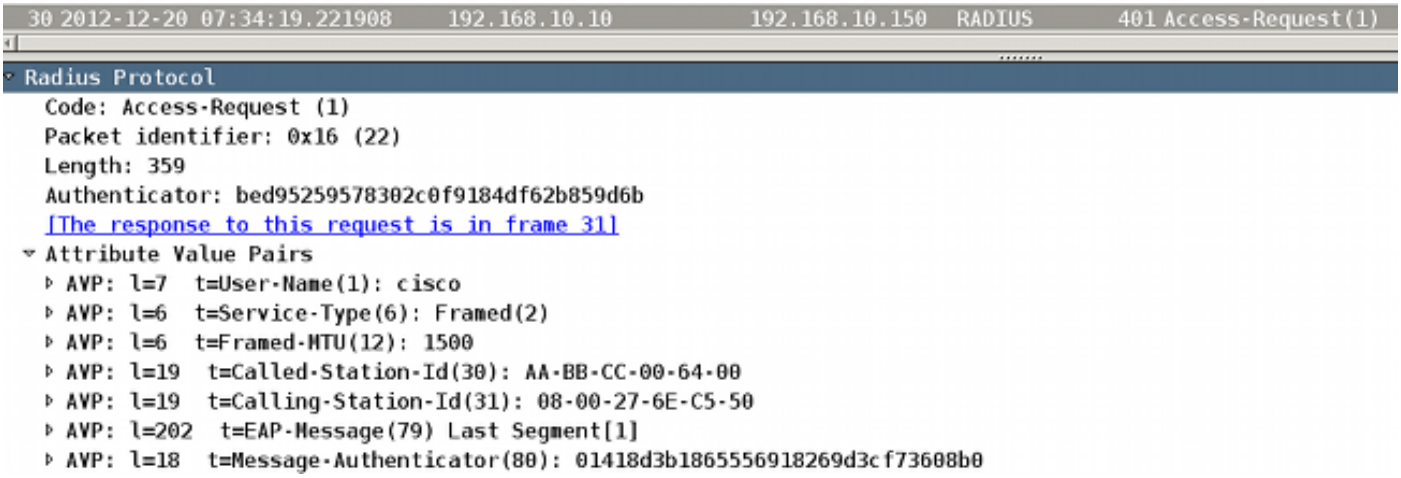
```
11036 The Message-Authenticator Radius Attribute is invalid.
```

Когда сообщение EAP подключено, это обычно происходит в последующем этапе. Первый Пакет RADIUS сеанса 802.1x не включает сообщение EAP; нет никакого поля Message-Authenticator, и не возможно проверить запрос, но на том этапе, клиент в состоянии проверить ответ с использованием поля Authenticator.

Проверьте атрибут средства проверки подлинности сообщения

Вот пример, чтобы проиллюстрировать, как вы вручную считаете значение, чтобы удостовериться, что это вычислено правильно.

Пакет номер 30 (Access-Request) был выбран. Это посреди сеанса EAP, и пакет включает поле Message-Authenticator. Цель состоит в том, чтобы проверить, что Средство проверки подлинности сообщения корректно:

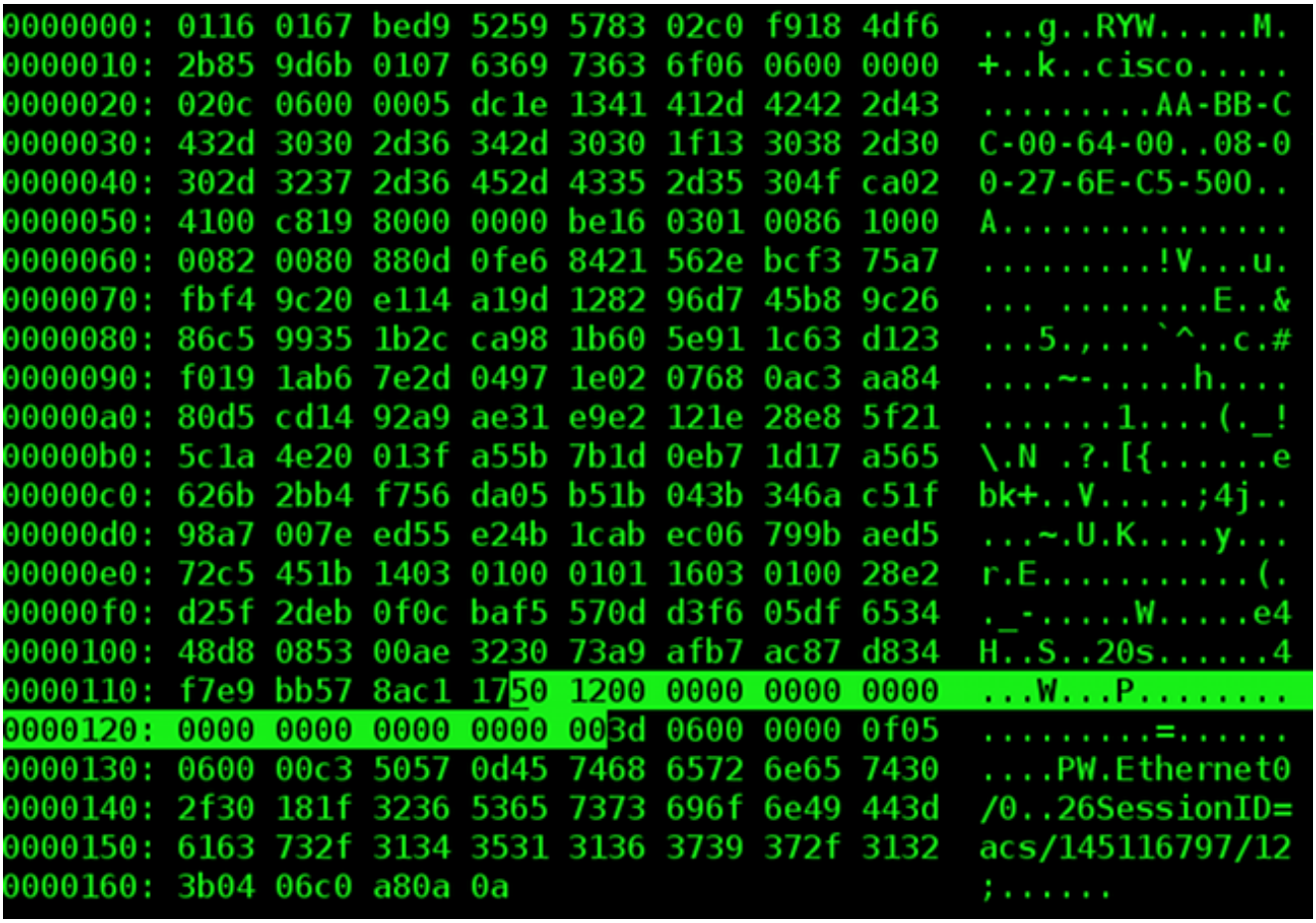


1. Щелкните правой кнопкой мыши **Протокол RADIUS** и выберите**, Export выбрал байты пакета**.

2. Запишите то информационное наполнение RADIUS в файл (двоичные данные).

3. Для вычислений поля Message-Authenticator необходимо поместить нули там и вычислить HMAC-MD5.

   Например, при использовании hex/Бинарного редактора, такого как энергия после ввода ": %! xxd", который переключается для преобразовывания режима в шестнадцатеричную систему и обнуляет 16 байтов, запускающихся после "5012" (50hex 80 в декабре, который является типом Средства проверки подлинности сообщения, и 12, является размером, который является 18 включая заголовок Пар значений атрибутов (AVP)):



После той модификации информационное наполнение готово. Необходимо возвратиться назад к hex/бинарному режиму (тип: ": %! xxd-r"), и сохранили файл (": wq").

4. Используйте OpenSSL для вычислений HMAC-MD5:

```
pluton # cat packet30-clear-msgauth.bin | openssl dgst -md5 -hmac 'cisco'
(stdin)= 01418d3b1865556918269d3cf73608b0
```

Функция HMAD-MD5 берет два аргумента: первый от стандартного ввода (stdin) является самим сообщением, и второй является общим секретным ключом (Cisco в данном примере). Результатом является точно то же значение как Средство проверки подлинности сообщения, подключенное к Пакету запроса доступа RADIUS.

То же может быть вычислено с использованием сценария Python:

```
pluton # cat hmac.py
#!/usr/bin/env python

import base64
import hmac
import hashlib

f = open('packet30-clear-msgauth.bin', 'rb')
try:
   body = f.read()
finally:
   f.close()

digest = hmac.new('cisco', body, hashlib.md5)
d=digest.hexdigest()
print d
```

```
pluton # python hmac.py
01418d3b1865556918269d3cf73608b0
```

Предыдущий пример представляет, как вычислить поле Message-Authenticator от Access-Request. Для проблемы Доступа, Access-Accept и Access-Reject, логика является точно тем же, но важно помнить, что Средство проверки подлинности Запроса должно использоваться, который предоставлен в предыдущем Пакете запроса доступа.

Дополнительные сведения

- RFC 2865
- RFC 2866
- RFC 3579
- Cisco Systems – техническая поддержка и документация