Dekodieren einer Sniffer-Trace für RADIUS-Transaktionen

Inhalt

Inhalt

Einführung

Das Layout der RADIUS-Pakete (Remote Authentication Dial In User Service) für Authentifizierung und Abrechnung wird in den RFCs 2138 und 2139 beschrieben. Dieses Dokument enthält ein Beispiel für die Aufteilung der Pakete in einem Austausch zwischen einem RADIUS-Client und einem RADIUS-Server. Dazu gehört das Senden des anbieterspezifischen Attributs 26 und unseres Anbietercodes 9 (Cisco). Der RADIUS-Client ist "rtpkrb.rtp.cisco.com", und "rtp-pinecone.rtp.cisco.com" ist der RADIUS-Server. Im folgenden Austausch:

1. rtpkrb sendet eine Zugriffsanfrage an rtp-pinecone.
2. rtp-pinecone sendet eine access-accept to rtpkrb.
3. rtpkrb sendet eine Buchhaltungsanfrage (start) an rtp-pinecone.
4. rtp-pinecone sendet eine Accounting-Antwort an rtpkrb.
5. rtpkrb sendet eine Buchhaltungsanfrage (Stopp) an rtp-pinecone.
6. rtp-pinecone sendet eine Accounting-Antwort an rtpkrb.

-
-

```
PktID Timestamp     Size Source Node          Destination Node  Status Protocol
-------------------------------------------------------------------------------
    1 18:14:20.355  0119 rtpkrb.rtp.cisco.    rtp-pinecone.rtp.        DoD UDP

Frame 1 Size   119 Absolute Time Sep 21 18:14:20.355 ASCII MODE
-------------------------------------------------------------------------------
  00000: 08 00 20 1a 5f 3d 00 00 0c 5c 5b 38 08 00 45 00   .. ._=...\[8..E.
  00016: 00 65 04 e0 00 00 fd 11 8b da 0a 1f 01 05 ab 44   .e.............D
  00032: 76 65 06 6d 06 6d 00 51 af 1b 01 09 00 49 a4 74   ve.m.m.Q.....I.t
  00048: 24 e1 6f ce 77 79 88 6e e7 be 3c fe 0d a2 04 06   $.o.wy.n..<.....
  00064: 0a 1f 01 05 05 06 00 00 00 12 3d 06 00 00 00 05   ..........=.....
  00080: 01 06 62 69 6c 6c 1f 0b 31 30 2e 33 31 2e 31 2e   ..bill..10.31.1.
  00096: 35 02 12 fe 57 fc ec b1 88 e1 91 50 c2 fd de 8f   5...W......P....
  00112: 3f 69 20 cc 5c 19 97                              ?i .\..

X-byte  Value           Meaning
42      01              access request
43      09              identifier
```

```
44-45   0049            length (X49 = 73 = byte 42-114)
46-61                   Request Authenticator
62      04              Attribute 4 = NAS-IP-Address
63      06              length of attribute
64-67   0a 1f 01 05     10.31.1.5
68      05              Attribute 5 = NAS-Port
69      06              length of attribute
70-73   12              X12 = 18 (i.e. tty 18)
74      3d              Attribute 61 = NAS-Port-Type
75      06              length of attribute
76-79   00 00 00 05     5 = virtual
80      01              Attribute 1 = User-Name
81      06              length of attribute
82-85   62 69 6c 6c     'bill'
86      1f              Attribute 31 = Calling-Station-ID
87      0b              length of attribute
88-96   31 30 2e 33 31 2e 31 2e 35 = 10.31.1.5
97      02              Attribute 2 = User-Password
98      12              length of attribute
99-114  fe 57 fc ec b1 88 e1 91 50 c2 fd de 8f 3f 69 20 = encrypted password
```

-

Zugehörige Informationen

- RADIUS-Technologieunterstützung
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems