

NAME

radump – tcpdump processing of the user data buffers from an **argus(8)** data file/stream.

COPYRIGHT

Copyright (c) 2000-2012 QoSient. All rights reserved.

SYNOPSIS

radump -r argus-file [ra options]

DESCRIPTION

Radump reads **argus** data from an *argus* data stream or file, and prints out tcpdump style decoding of the user data buffers.

OPTIONS

Radump, like all ra based clients, supports a number of **ra options** including filtering of input argus records through a terminating filter expression. See **ra(1)** for a complete description of **ra options**.

EXAMPLE INVOCATION

This example dumps the user capture buffers of arp traffic seen in the file. When there is no user buffer, or if the decoder can't decode it, the length will 0.

```
% radump -r argus.file -s suser:64 duser:64 -N 5 - arp
          srcUdata                                dstUdata
s[38]="who-has 192.168.0.66 tell 192.168.0.68"    d[36]="192.168.0.68 is-at c8:2a:14:58:7a:55"
s[37]="who-has 192.168.0.1 tell 192.168.0.68"    d[36]="192.168.0.68 is-at 80:71:1f:3c:c3:88"
s[37]="who-has 192.168.0.1 tell 192.168.0.66"    d[0]=""
s[37]="who-has 192.168.0.1 tell 192.168.0.78"    d[0]=""
s[38]="who-has 192.168.0.34 tell 192.168.0.66"    d[0]=""
```

This example decodes the user capture buffers of DNS traffic seen in the file.

```
% radump -s stime pkts suser:64 duser:64 -r ~/argus/data/argus*00.out.gz - port domain
          StartTime TotPkts srcUdata                                dstUdata
17:48:36.589949      2 s[37]="48936+ [ ] A? www.cylab.cmu.edu. (35)"    d[32]="48936 1/3/0 A 128.2.129.188 (64)"
17:48:36.590557      2 s[30]="3018+ [ ] A? qosient.com. (29)"            d[31]="3018 1/2/0 A 216.92.14.146 (64)"
17:48:36.708172      2 s[39]="27243+ [ ] A? ajax.googleapis.com. (37)"    d[26]="27243 2/4/4 CNAME[|domain]"
17:48:36.776033      2 s[31]="45149+ [ ] A? nsmwiki.org. (29)"           d[33]="45149 1/3/0 A 69.163.152.168 (64)"
17:48:36.776501      2 s[40]="51781+ [ ] A? www.surveymonkey.com. (38)"    d[31]="51781 1/13/0 A 75.98.93.51 (64)"
17:48:36.776655      2 s[31]="38953+ [ ] A? www.cmu.edu. (29)"           d[51]="38953 3/2/1 CNAME WWW-CMU.ANDREW.cmu.edu.,[doma
17:48:36.777014      2 s[32]="64748+ [ ] A? www.cert.org. (30)"          d[33]="64748 1/2/0 A 192.88.209.244 (64)"
17:48:36.978293      2 s[44]="53009+ [ ] A? www.google-analytics.com. (42)" d[27]="53009 17/4/4 CNAME[|domain]"
```

This example decodes the user capture buffers of HTTP traffic seen in the file.

```
radump -s stime proto dport pkts suser:32 duser:32 -r ~/argus/data/argus*00.out.gz -L0 -N5 - port http
          StartTime Proto Dport TotPkts srcUdata                                dstUdata
17:48:36.592155      tcp http      27 s[32]="GET /research/cydat.html" d[32]="HTTP/1.1 200 OK..Date: M"
17:48:36.632662      tcp http      24 s[32]="GET /argus/ HTTP/1.1..Ho" d[32]="HTTP/1.1 200 OK..Date: M"
17:48:36.705481      tcp http      23 s[32]="GET /files/css/public.cs" d[32]="HTTP/1.1 200 OK..Date: M"
17:48:36.705669      tcp http      11 s[32]="GET /files/css/public_lc" d[32]="HTTP/1.1 200 OK..Date: M"
17:48:36.705987      tcp http      15 s[32]="GET /files/js/home.js HT" d[32]="HTTP/1.1 200 OK..Date: M"
```

AUTHORS

Carter Bullard (carter@qosient.com).

SEE ALSO

ra(1), **rarc(5)**, **argus(8)**