

## RE: sniffer in redhat 9

---

*Source:* <http://linux.derkeiler.com/Mailing-Lists/RedHat/2006-10/msg00186.html>

---

- *From:* "Gould, Aaron" <aaron.gould@xxxxxxx>
  - *Date:* Wed, 25 Oct 2006 15:08:56 -0500
- 

oops. thanks steve for the gracious reminder :)

sometimes i forget to do the basic reading first

Aaron

---

From: redhat-list-bounces@xxxxxxxxxxx on behalf of Serge Dubrouski  
Sent: Wed 10/25/2006 7:05 AM  
To: General Red Hat Linux discussion list  
Subject: Re: sniffer in redhat 9

There is one really good command in Linux/UNIX called man :-)

man tcpdump

.....

Under Linux:

You must be root or tcpdump must be installed setuid to root (unless your distribution has a kernel that supports capability bits such as CAP\_NET\_RAW and code to allow those capability bits to be given to particular accounts and to cause those bits to be set on a user's initial processes when they log in, in which case you must have CAP\_NET\_RAW in order to capture and CAP\_NET\_ADMIN to enumerate network devices with, for example, the -D flag).

.....

On 10/25/06, Gould, Aaron <aaron.gould@xxxxxxx> wrote:

i was doing it as "aaron", after su'ing to root, tcpdump works "tcpdump: listening on eth0". i added /usr/sbin/ to my "aaron" path, and now when i run tcpdump it says "tcpdump: no suitable device found" any ideas?

also, is there a nicer graphical sniffer built-into redhat? if not perhaps someone can suggest

RE: sniffer in redhat 9

the best and newest one to download with the most possible decodes for protocols such as h.323 and sip for VoIP

thanks  
Aaron

---

From: redhat-list-bounces@xxxxxxxxxx on behalf of mark  
Sent: Tue 10/24/2006 5:46 PM  
To: General Red Hat Linux discussion list  
Subject: Re: sniffer in redhat 9

Serge Dubrouski wrote:

yum install tcpdump

Or he can install it from the CD.... Though there is one question:  
Aaron, are you doing it as root, or as a user? I ask that, because users  
are frequently set up without /sbin and /usr/sbin in their path.

mark

Of course if you have yum configured.

On 10/24/06, Gould, Aaron <aaron.gould@xxxxxxxx> wrote:

i type tcpdump and it says "bash: tcpdump: command not  
found" where  
would i go to execute it? also where should i go to check if  
ethereal  
is on my redhat box?

Aaron

---

From: redhat-list-bounces@xxxxxxxxxx on behalf of alan  
Sent: Tue 10/24/2006 3:08 PM  
To: General Red Hat Linux discussion list  
Subject: Re: sniffer in redhat 9

On Tue, 24 Oct 2006, Serge Dubrouski wrote:

RE: sniffer in redhat 9

tcpdump

Ethereal might have been in that version as well. I would have to look.

On 10/24/06, Gould, Aaron  
<aaron.gould@xxxxxxx> wrote:

is there a built-in packet  
sniffer in redhat 9?

Aaron

--  
redhat-list mailing list  
unsubscribe  
<mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

--  
Gorgon minion: "Is the Source dangerous?"  
Gorgon Commander: "Only if it is on your side."  
- Quark Episode 2

--  
redhat-list mailing list  
unsubscribe  
<mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

--  
redhat-list mailing list  
unsubscribe  
<mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

--  
RE: sniffer in redhat 9

RE: sniffer in redhat 9

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

--

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

--

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

--

redhat-list mailing list

unsubscribe <mailto:redhat-list-request@xxxxxxxxxx?subject=unsubscribe>  
<https://www.redhat.com/mailman/listinfo/redhat-list>

RE: sniffer in redhat 9