Re: Modifying packets in userspace using libnetfilter_queue

[Date Prev][Date Next][Thread Prev][Thread Next][Date Index][Thread Index]

- *Subject*: Re: Modifying packets in userspace using libnetfilter_queue
- *From*: Bruno Moreira Guedes <thbmatrix@xxxxxxxxx>
- *Date*: Thu, 30 Jul 2009 13:54:55 -0300
- *Cc*: "netfilter-devel@xxxxxxxxxxxxxxx" <netfilter-devel@xxxxxxxxxxxxxxx>
- *In-reply-to*: <5BB67BF4A0D4544A918C2FD76487A1E13D8944D6@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx>

```
2009/7/30 Srinivasan, Suman (Suman)** CTR **
<suman.srinivasan@xxxxxxxxxxxxxxxxxx>:
> Hi all,
>
> Sorry for this elementary question, but I am new to the world of packet modification. I browsed the recent netfilter-devel archives and cou
>
> I am trying to modify TCP packets in userspace. I know it is inefficient to do it in userspace, but I just need a prototype to test for now
>
> I couldn't find much documentation on doing this, except for the documentation on the following URL, the nfqnl_test.c file and some modific
> http://www.nufw.org/doc/libnetfilter_queue/
>
> I have gotten this far:
> 1. Have set up iptables rules to send the TCP packets I want to intercept down a NFQUEUE queue.
> 2. Am able to use nfqnl_test.c to receive and print out packet info.
> 3. Used netinet/tcp.h and sample code to check TCP headers
> 4. Able to print out TCP payload using TCP and IP header information
> 5. Able to modify the TCP payload (or at least the copy)
>
> However, the modified packets are not really being transmitted! I assume this is because I am getting a copy of the packets or the packet c

When I've done it the problem was the checksum. Try to verify if this
is correct :)

>
> How do I actually modify the packet in userspace so that it is sent out over the network?

You send it by calling nfq_set_verdict and passing in the last two
arguments the packet length and the pointer to packet. Of course, you
must accept the packet.

>
> Also, if I modify the TCP packets and add more data to the payload, what would I change? I assume that I would only have to change the foll
>
> - TCP payload length
> - Checksum
> - IP length (?, would I have to touch this field)
>

The best problem I had with this in the past was the checksum. Check
if your checksum is being right calculated by recalculating the
checksum of a packet you already know the right sum, or running
tcpdump -v.

Remember: anywhere you change you need to recalculate the TCP
pseudo-header(TCP over IPV4 if it's the case) checksum, and if you
change the IP header you also need to recompute the IP checksum.

> Is there anything else that I am not thinking of?
>
> By the way, the documentation available out there is a little hard for a newcomer to the world of iptables/netfilter. I'm getting a little

http://www.netfilter.org/projects/index.html
I think you getting from there you'll using the active.

>
> Sorry for this long e-mail.
>
> Thank you,
> Suman
>
> --
> Falun Gong: www.falundafa.org | www.faluninfo.net
> Peaceful meditation faces persecution in mainland China
> --
> To unsubscribe from this list: send the line "unsubscribe netfilter-devel" in
> the body of a message to majordomo@xxxxxxxxxxxxxxx
> More majordomo info at  http://vger.kernel.org/majordomo-info.html
>
```

And also, if you change some headers you'll need to care about
connection tracking(my elbow hurts right now because of it).

I also thanks if you successfully do NAT at user-space and say me how!!

[]'s
--Bruno Moreira Guedes
A boring child
--
To unsubscribe from this list: send the line "unsubscribe netfilter-devel" in
the body of a message to majordomo@xxxxxxxxxxxxxxx
More majordomo info at http://vger.kernel.org/majordomo-info.html

- **References**:
  - **Modifying packets in userspace using libnetfilter_queue**
    - *From:* Srinivasan, Suman (Suman)** CTR **

- Prev by Date: **Re: Modifying packets in userspace using libnetfilter_queue**
- Next by Date: **RE: Modifying packets in userspace using libnetfilter_queue / got it working**
- Previous by thread: **RE: Modifying packets in userspace using libnetfilter_queue / got it working**
- Next by thread: **conntrack helper - expectations**
- Index(es):
  - **Date**
  - **Thread**

[Linux Resources] [LARTC] [Bugtraq] [Yosemite Forum] [Photo]