

Re[2]: Why TCP is more secure than UDP?

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2007-07/msg00054.html>

- *From:* Adam Pal <pal_adam@xxxxxxx>
 - *Date:* Wed, 11 Jul 2007 22:13:09 +0200
-

Hello Buz,

Thank you for your details.

What you describe looks to me like some land or smurf-attack.

Let me go on...

- i) using the conf. you describe, if i understand you well, even 1 legitime ECHO will start some pending of packets.
- ii) as you describe it is for me a M-I-T-M attack where you basicaly spoof an IP

The point that you use TCP ur UDP doesnt really matter, because as i mentioned, the only thing which makes TCP harder to break is the pre-established connection with the seq-number.

Taking this in consideration, if Moe sniffs the traffic he can hijack the TCP-Session or try to guess the seq-nr.

But as i mentioned, we dont spoof here TCP or UDP, we basicaly spoof an IP and start an man in the middle (M-I-T-M) attack on the respective protocol.

--

Best regards,
Adam Pal

P.S.

Considering your scenario, if the router is configured not to accept inbound traffic with rfc-1918 source-addresses everything is ok. From that point of view it can be also a weakness of the router conf. more than a weakness of the protocol? :)

Wednesday, July 11, 2007, 9:18:42 PM, you wrote:

<=====Original message text=====

BD> I'll try and illustrate a security difference. Lets say I have a
BD> service called "Echo" that runs on both udp port 7 and tcp port 7 on
BD> two machines on my lan (192168.1.1 or "Larry" and 192.168.1.2 or
BD> "Curly".) Suppose this service just echoes back any packet I send it.
BD> Suppose my tricky friend "Moe" is across the internet at 10.0.0.1 (Oh

Re[2]: Why TCP is more secure than UDP?

BD> yeah – and let's also suppose these are not rfc 1918 addresses.) Moe's
BD> router and ISP are configured kinda loosely and don't really care
BD> about source addresses, just destination.

BD> If Moe uses a UDP packet with source 192.168.1.2 and destination
BD> 192.168.1.1, his first packet could (if My router configs are a
BD> little loose) get that packet to Larry, the content of that packet
BD> "SLAP" will get echoed to Curly who will then SLAP Larry who will
BD> then SLAP Curly ad infinitum. Burning network and CPU until noticed.
BD> (works well actually with port 19 and Chargen as one of the ports and
BD> 7 as the other.)

BD> If Moe uses a tcp packet with source 192.168.168.1.2 and a destination
BD> of 192.168.1.1. His packet will get to Larry and Larry will try and
BD> handshake with Curly who won't have any idea of what's going on and
BD> stop the transaction.

BD> It's easy for Moe to "spoof" either udp or tcp but the udp packet is
BD> more fun for Moe.

BD> Luck,
BD> Buz

BD> On 7/10/07, pal_adam@xxxxxxx <pal_adam@xxxxxxx> wrote:

Hi

I dont understand what you mean by spoofing, since wherever you
use UDP or TCP the underlying layer still remains IP so when you
spooof a source you spooof an IP source.

If you talk about a man-in-the-middle attack then taking a
closer look at both protocols will show that UDP doesnt establish
any connection before starting the communication.

Using TCP you`ll need to ACK incomming data using a
pre-established sequence number which makes the attack on TCP
harder but not impossible.

regards

Adam Pal

----- Original-Nachricht -----
Datum: 10 Jul 2007 02:11:12 -0000
Von: paavan.shah@xxxxxxxxxx
An: security-basics@xxxxxxxxxxxxxxxxxxxxxx
Betreff: Why TCP is more secure than UDP?

Re[2]: Why TCP is more secure than UDP?

It is said that UDP is considered more vulnerable to spoofing than TCP?

Can anyone point me to any document/link which describes TCP is more secure than UDP

--

Der GMX SmartSurfer hilft bis zu 70% Ihrer Onlinekosten zu sparen!
Ideal für Modem und ISDN: <http://www.gmx.net/de/go/smartsurfer>

<=====End of original message text=====

Attachment: smime.p7s

Description: S/MIME Cryptographic Signature