

Antwort: Sniffing Encrypted Traffic (w/ keys)

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-06/0269.html>

c.ehlen_at_bull.de

Date: 06/23/05

To: Brad DeShong <brad@deshong.net>
Date: Thu, 23 Jun 2005 17:29:35 +0200

Hi Brad,

try ssldump ...

<http://www.rtfm.com/ssldump/>

ssldump is an SSLv3/TLS network protocol analyzer. It identifies TCP connections on the chosen network interface and attempts to interpret them as SSLv3/TLS traffic. When it identifies SSLv3/TLS traffic, it decodes the records and displays them in a textual form to stdout. If provided with the appropriate keying material, it will also decrypt the connections and display the application data traffic.

Brad DeShong
<brad@deshong.net> An: pen-test@securityfocus.com
t> Kopie:
Thema: Sniffing Encrypted Traffic (w/ keys)
23.06.2005 04:42

During a recent assesment we compromised SSL keys for a webserver and wanted to sniff the "encrypted" traffic. In theory this works, but what tools exist to do this in practice? I've seen Covelight's Clearwatch on a Windows system, but we're working with a Linux system on the inside. Is a MITM necessary or can it be done by just looking at the traffic after the fact (at least for the half of the connection we have keys for?).

Thanks,
Brad DeShong
WestAnnex Security