

RE: Using a Compromised Router to Capture Network Traffic

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-07/0074.html>

From: Axel Dunkel (ad@Dunkel.de)

Date: 07/15/02

Date: 15 Jul 2002 20:52:16 +0200
From: "Axel Dunkel" <ad@Dunkel.de>
To: Ryan_Moffett@stercomm.com

> *Is this hosted on an alternate site other than the geocities site which has
> exceeded the xfer limit?*

For a while, I have put it on
http://www.Dunkel.de/download/GRE_sniffing.doc
to help out.

Best regards,
Axel Dunkel

> -----Original Message-----
> *From: Penetration Testing [mailto:pentest@infosecure.com.au]*
> *Sent: Monday, July 15, 2002 2:44 PM*
> *To: pen-test@securityfocus.com*
> *Subject: Using a Compromised Router to Capture Network Traffic*
>
>
> *Hi all.*
>
> *I have recently completed some experimentation into using a captured router
> to sniff network traffic on a remote network. This is in the same vein as
> Gaus's article in Phrack 56 (Things to do in cisco land when you are dead).*
>
> *I have tried to build on Gaus's work in that I terminated the GRE tunnel on
> a Cisco router instead of a *nix machine. I explored a couple of possible
> scenarios for this, the net result being that it is possible to remotely
> capture (bi-directional) network traffic using NO customised tools; all that
> is required is one cisco router with vanilla IOS, and a machine that can run
> snoop or tcpdump.*
>
> *Anyway, if anyone is interested, the document describing the experiment and
> results is available at http://www.geocities.com/david_taylor_au/
> (Word 2000 format). Or, contact me.*

SecurityFocus Penetration: RE: Using a Compromised Router to Capture Network Traffic

>
> *Regards,*
> *Dave Taylor*
>
>
>

> *This list is provided by the SecurityFocus Security Intelligence Alert (SIA)*
> *Service. For more information on SecurityFocus' SIA service which*
> *automatically alerts you to the latest security vulnerabilities please see:*
> <https://alerts.securityfocus.com/>

> *This list is provided by the SecurityFocus Security Intelligence Alert (SIA)*
> *Service. For more information on SecurityFocus' SIA service which*
> *automatically alerts you to the latest security vulnerabilities please see:*
> <https://alerts.securityfocus.com/>

Systemberatung A. Dunkel GmbH, Gutenbergstr. 5, D-65830
Kriftel
Tel.: +49-6192-9988-0, Fax: +49-6192-9988-99, E-Mail:
ad@Dunkel.de

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- ***Previous message:*** [Erwin van der Zwan: "Re: Scanning for blank admin passwords on a windows box"](#)
- ***In reply to:*** [Moffett, Ryan: "RE: Using a Compromised Router to Capture Network Traffic"](#)
- ***Next in thread:*** [Jeremy Junginger: "RE: Using a Compromised Router to Capture Network Traffic"](#)
- ***Messages sorted by:*** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)