

## Re: VoIP pentest ?

**Source:** <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2004-11/0043.html>

---

**From:** Ghaith Nasrawi ([libero\\_at\\_aucegypt.edu](mailto:libero_at_aucegypt.edu))

**Date:** 11/13/04

To: Andre Ludwig <[andre.ludwig@gmail.com](mailto:andre.ludwig@gmail.com)>

Date: Fri, 12 Nov 2004 22:26:54 -0500

sorry for the late post, I just wanted to add that there are several proposals for encrypted VoIP like:

<http://www.faqs.org/rfcs/rfc3853.html> (AES with SIP)

and there is another one for using SIP with TLS.

also, this

<http://web.mit.edu/sip/sip.edu/security.shtml>

would give you some insight about what kind of threats people should expect with VoIP deployment.

On Thu, 2004-10-28 at 15:57 -0400, Andre Ludwig wrote:

> <http://www.voip-info.org/wiki-Open+Source+VOIP+Software>

>

> *Hope this helps you out as far as general tools, as for methodology*  
> *you would be on your own to develop that. Get creative with the tools*  
> *on that page and you can do allot if the moon and stars are aligned*  
> *properly. Feel free to post any and all results you come up with.*

>

>

> *Tools and links*

>

> *Sip bomber*

> <http://metalinkltd.com/eng/downloads/>

>

> *Features:*

> *Analyses server resposes for rfc compliance*  
> *- Incorporates CERT tests*  
> *- Supports UDP, TCP and broken TCP transports*  
> *- Automatic and manual testing modes*  
> *- Ability to create and run custom tests*  
> *- QT user interface*

>

> *Best of all it's free and full source code is available.*

>

>

> *Vomit (converts CISCO voip convo into a wav from tcpdump file)*

## SecurityFocus Penetration: Re: VoIP pentest ?

>  
> <http://vomit.xtdnet.nl/>  
> *The vomit utility converts a Cisco IP phone conversation into a wave  
> file that can be played with ordinary sound players. Vomit requires a  
> tcpdump output file. Vomit is not a VoIP sniffer also it could be but  
> the naming is probably related to H.323.*  
>  
>  
> *Download*  
>  
>  
> *vomit-0.2c.tar.gz* <<http://vomit.xtdnet.nl/vomit-0.2c.tar.gz>> -  
> *Released 2004-01-02 (requires libdnet*  
> *<<http://libdnet.sourceforge.net>>)*  
> *vomit-0.2.tar.gz* <<http://vomit.xtdnet.nl/vomit-0.2.tar.gz>> - *Released*  
> *2001-12-12 (requires libnet <<http://www.packetfactory.net/libnet/>>)*  
> *phone.dump.gz* <<http://vomit.xtdnet.nl/phone.dump.gz>> - *sample dump*  
> *from a telephone conversation that I had at CITI*  
> *<<http://www.citi.umich.edu/>>.*  
>  
> *The vomit utility is distributed under a BSD-license and completely*  
> *free for any use including commercial.*  
>  
> *In order to build vomit, you need libevent*  
> *<<http://www.monkey.org/%7Eprovos/libevent/>>, a library for*  
> *asynchronous event notification and libdnet*  
> *<<http://libdnet.sourceforge.net>> or libnet*  
> *<<http://www.packetfactory.net/libnet/>>.*  
>  
> *Example*  
> *\$ vomit -r phone.dump | waveplay -S8000 -B16 -C1*  
>  
> *Errors*  
>  
> *Vomit works only for G.711.*  
>  
> *Acknowledgements*  
>  
> *The program contains wave file interpreting code from waveplay by Y.*  
> *Sonoda, ulaw conversion code from Sun Microsystems, and some pcap code*  
> *from Dug Song. It also contains contributions by Marius A. Eriksen.*  
>  
>  
>  
>  
> *SipSak*  
> *<http://sipsak.berlios.de/>*  
> *Features*  
>  
> *sending OPTIONS request*  
> *sending text files (which should contain SIP requests)*

Re: VoIP pentest ?

SecurityFocus Penetration: Re: VoIP pentest ?

- > *traceroute (see section 11 in RFC3261*
- > *<<http://iptel.org/info/players/ietf/callsignalling/rfc3261.txt>>)*
- > *user location test*
- > *flooding test*
- > *random character trashed test*
- > *interpret and react on response*
- > *authentication with qop supported*
- > *short notation supported for receiving (not for sending)*
- > *string replacement in files*
- > *can simulate calls in usrloc mode*
- > *uses symmetric signaling and thus should work behind NAT*
- > *can upload any given contact to a registrar*
- > *send messages to any SIP destination*
- > *Nagios compliant return codes*
- > *search for strings in reply with regular expression*
- > *use multiple processes to create more server load*
- > *read SIP message from STDIN (e.g. from a pipe '|')*
- >
- >
- >
- > *Andre Ludwig CISSP*
- >
- > *On Wed, 27 Oct 2004 11:28:51 +0200, Frederic Charpentier*
- > *<[fcharpen@xmcopartners.com](mailto:fcharpen@xmcopartners.com)> wrote:*
- > *> Hi all,*
- > *> does anyone have experiences or papers on VoIP pentest/assessment ?*
- > *> Expecting classic OS/Network audits and H323/ASN.1 flaws, I can't find*
- > *> any documentations or papers about flaws in VoIP architecture.*
- > *>*
- > *> Fred.*
- > *>*
- > *>*

---

> *> Internet Security Systems. – Keeping You Ahead of the Threat*

> *>*

> *> When business losses are measured in seconds, Internet threats must be stopped before they impact your network. To learn how Internet Security Systems keeps organizations ahead of the threat with preemptive intrusion prevention, download the new whitepaper, Defining the Rules of Preemptive Protection, and end your reliance on reactive security technology.*

> *>*

> *> [http://www.securityfocus.com/sponsor/ISS\\_pen-test\\_041001](http://www.securityfocus.com/sponsor/ISS_pen-test_041001)*

> *>*

---

> *>*

> *>*

--

(o\_

/\ Ghaith Nasrawi

v\_/\_

"Evil thrives when good men do nothing"