

RE: VoIP

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-02/0056.html>

From: Brewis, Mark (mark.brewis_at_eds.com)

Date: 02/10/05

To: "'Stelios Tigkas'" <kuffya@gmail.com>, pen-test@securityfocus.com

Date: Thu, 10 Feb 2005 12:15:12 -0000

Stelios,

From previous discussions on the lists:

sil [jesus@resurrected.us] on VULN-DEV 01/03/04

SIP

White Paper: Security in SIP-Based Networks

http://www.cisco.com/en/US/tech/tk652/tk701/technologies_white_paper09186a00800ae41c.shtml

http://www.ins.com/downloads/datasheets/sec_solution_voip_security_ds.pdf

<http://www.tml.hut.fi/Opinnot/Tik-110.501/2000/intro/voip.html>

<http://www.icete.org/Docs/workshop4.pdf>

Also,

Try Sivus – a VoIP Vulnerability Scanner: www.vopsecurity.org. You do need to understand SIP to get the most out of this though.

Pasquiet Loic (M.) [Loic.Pasquiet@Polytechnique.fr]
problem in voip environment on bugtraq 11/09/2004

short thread

Frederic Charpentier [fcharpen@xmcopartners.com]
VoIP pentest ? on pen-test, 27/10/04

and the thread that followed it.

Also, the new Voipsec@voipsa.org mailing list, www.voipsa.org.

More generally, the SJ Labs SJphone softphone from softjoys.com offers a really good means of testing VOIP environments/connections. Try making peer to peer calls within an environment, then configuring gateways within the phone to utilise the VoIP architecture to make calls.

VoIP can introduce more traditional holes within security architecture, in routers and firewalls, which is

RE: VoIP

SecurityFocus Penetration: RE: VoIP

always worth an explore.

Ethereal does a really good job of capturing and converting streamed UDP plaintext to .wav, allowing for the meaningful playback of unencrypted phone calls on a local LAN segment. Use a recent Ethereal for this. We've had mixed results sniffing VOIP on switched networks.

Hope this is of some use,

Mark

Mark Brewis

Security Consultant
EDS
UK Information Assurance Group
Wavendon Tower
Milton Keynes
Buckinghamshire
MK17 8LX.

Tel: +44 (0)1908 28 4013
Mbl: +44 (0)7989 291 648
Fax: +44 (0)1908 28 4393
E@: mark.brewis@eds.com

This email is confidential and intended solely for the use of the individual(s) to whom it is addressed. Any views or opinions presented are solely those of the author. If you are not the intended recipient, be advised that you have received this email in error and that any use, dissemination, forwarding, printing, or copying of this mail is strictly prohibited.

Precautions have been taken to minimise the risk of transmitting software viruses, but you must carry out your own virus checks on any attachment to this message. No liability can be accepted for any loss or damage caused by software viruses.

>>-----Original Message-----
>>From: Stelios Tigkas [mailto:kuffya@gmail.com]
>>Sent: 08 February 2005 11:01
>>To: pen-test@securityfocus.com
>>Subject: VoIP
>>
>>
>>
>>
>>Hello there comrades,
>>
>>I'm interested to familiarise with techniques, ideas and
>>tools related to VoIP testing. This is a brand new area for
>>me, and my short research yielded only a couple of tools such
>>as VOMIT and VoIPong.
>>As a matter of fact, I'm not sure which should be the 'scope'

RE: VoIP

SecurityFocus Penetration: RE: VoIP

>>*of a comprehensive VoIP test, and have not come across any*
>>*methodologies of this type.*
>>*Assume that an ISDN / VoIP router is configured to deny*
>>*incoming connections form arbitrary telephone numbers. I*
>>*would be particularly interested to see if there is a*
>>*possibility of bypassing such defence mechanisms, perhaps by*
>>*disguising into a 'trusted' telephone number, or by other means.*
>>*I'd be very glad to receive feedback/ideas on these issues*
>>
>>*Thanks,*
>>*Stelios.*
>>
>>
>>
>>