

RE: Netcat through Squid HTTP Proxy

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2005-04/0069.html>

From: Otero, Hernan (EDS) (hernan.otero_at_lan.com)

Date: 04/18/05

To: Todd Towles <toddtowles@brookshires.com>, Joachim Schipper <j.schipper@math.uu.nl>, pen-test@
Date: Mon, 18 Apr 2005 12:01:09 -0400

Using ssh and direct connect through https proxy is an (old and well know) alternative. You can forward any port, local or remote, inside an ssh tunnel and no one will know what are you doing.

-H

-----Original Message-----

From: Todd Towles [<mailto:toddtowles@brookshires.com>]

Sent: Monday, April 18, 2005 9:20 AM

To: Joachim Schipper; pen-test@securityfocus.com

Subject: RE: Netcat through Squid HTTP Proxy

There is a POC shell program that uses XML-RPC called Monkey shell (<http://www.securiteam.com/tools/6L00F0KBFE.html>). It looks like it might require a re-code to be fully used as a pen-test tool. But it something to look at. -

You can try HTTP Tunnel as well.

httptunnel creates a bidirectional virtual data connection tunnelled in HTTP requests. The HTTP requests can be sent via an HTTP proxy if so desired.

This can be useful for users behind restrictive firewalls. If WWW access is allowed through a HTTP proxy, it's possible to use httptunnel and, say, telnet or PPP to connect to a computer outside the firewall.

<http://www.nocrew.org/software/httptunnel.html>

-Todd

> -----Original Message-----

> From: Joachim Schipper [<mailto:j.schipper@math.uu.nl>]

> Sent: Sunday, April 17, 2005 10:13 AM

> To: pen-test@securityfocus.com

> Subject: Re: Netcat through Squid HTTP Proxy

>

SecurityFocus Penetration: RE: Netcat through Squid HTTP Proxy

> *On Fri, Apr 15, 2005 at 10:40:31AM -0400, Rod S wrote:*

> > *Hello,*

> >

> > *I have a squid proxy server running, caching and filtering*

> *web access.*

> > *User workstations on my network are only allowed http*

> *access through*

> > *this proxy server. The firewall (Cisco PIX) will not let*

> *them connect*

> > *outbound to any ports.*

> >

> > *I've done some testing and was successful in running netcat*

> *to connect*

> > *to a remote server listening with netcat on port 80 and get*

> *a command*

> > *prompt for an internal machine (which is allowed to connect to any*

> > *outgoing ports) on that remote server. I'm wondering if*

> *it's possible*

> > *for netcat to connect through our proxy server to a remote*

> *machine and*

> > *send a cmd.exe shell in the same way? Any tips on*

> *preventing this or*

> > *any other information you care to share is appreciated.*

> >

> > *Thanks!*

> > *Rod*

>

> *Dear Rod,*

>

> *if I understand correctly, you can get a shell on a remote*

> *machine and want to allow a remote machine to get a shell on*

> *a local host. This can be achieved quite easily – search for*

> *'reverse shell'. One example which looks nice is rrs (*nix*

> *only) – see freshmeat.net. This one cannot do HTTP proxying,*

> *though, so it should be augmented or wrapped in something that can.*

>

> *The Hacker's Choice (www.thc.org) has just run an article on*

> *this, including an example in Perl. If you desire something*

> *more Windows-specific, you may want to ask Google, or any*

> *shades-of-grey-hat site you can find. ;-)*

>

> *However, simply, yes, this is possible. Quite a few of these*

> *kinds of reverse shells rely on HTTP CONNECT, so limiting*

> *that may help – but there are some seriously scary things out*

> *there, including reverse shells that communicate over DNS or*

> *ICMP (pings etc).*

>

> *A good I(P/D)S may help a little. Locking down the network*

> *further may help. However, it is almost impossible to keep a*

> *smart attacker in – make sure to keep him out.*

>

SecurityFocus Penetration: RE: Netcat through Squid HTTP Proxy

> *Joachim*

>