

RE: Netcat through Proxy

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-04/0256.html>

adisegna_at_sisocorp.com

Date: 04/15/05

Date: Fri, 15 Apr 2005 13:27:34 -0400
To: <securitybasics@gmail.com>

If there isn't a protocol filter on the proxy and the netcat server retransmits the data back from port 80 sure.

Arthur DiSegna
Information Technology Group
Security Identification Systems Corporation

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

From: Rod S [mailto:securitybasics@gmail.com]
Sent: Thursday, April 14, 2005 8:19 AM
To: security-basics@securityfocus.com
Subject: Re: Netcat through Proxy

So, it is possible to tunnel a netcat connection through a squid http proxy server?

On 4/13/05, adisegna@sisocorp.com <adisegna@sisocorp.com> wrote:

> *The pix won't provide the level of application layer filtering you would need to prevent this. I also use a PIX and have to deal with the same issue. The PIX is great for speed and preventing outside attacks but not inside out attacks (internal users) from open ports like http (80). I am now in the process testing an application layer firewall to stick behind the PIX to combat this problem. This will be a growing concern for corporations using level 3 and 4 type firewall appliances.*

>

> AD

> *Information Technology Group*

> *Security Identification Systems Corporation*

>

>

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

> *From: Rod S [mailto:securitybasics@gmail.com]*

SecurityFocus BASICS: RE: Netcat through Proxy

> *Sent: Wednesday, April 13, 2005 12:00 PM*
> *To: security-basics@securityfocus.com*
> *Subject: Netcat through Proxy*

>
> *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*
>
>

> ---
> *Earn your MS in Information Security ONLINE*
> *Organizations worldwide are in need of highly qualified information*
> *security*
> *professionals. Norwich University is fulfilling this demand with its*
> **MS**
> *in*
> *Information Security offered online. Recognized by the NSA as an*
> *academically excellent program, NU offers you the opportunity to earn*
> *your*
> *degree without disrupting your home or work life.*
>
> http://www.msia.norwich.edu/secfocus_en
>

> ----
>
>

Earn your MS in Information Security ONLINE
Organizations worldwide are in need of highly qualified information
security
professionals. Norwich University is fulfilling this demand with its MS
in
Information Security offered online. Recognized by the NSA as an

SecurityFocus BASICS: RE: Netcat through Proxy

academically excellent program, NU offers you the opportunity to earn your degree without disrupting your home or work life.
http://www.msia.norwich.edu/secfocus_en
