

Re: OpenSSH, Telnet, Windows Authentication and double-hops

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2007-10/msg00059.html>

- *From:* "jmartzoo-google@xxxxxxxxx" <jmartzoo-google@xxxxxxxxx>
 - *Date:* Fri, 12 Oct 2007 08:22:57 -0700
-

On Oct 11, 10:03 pm, "Richard E. Silverman" <r...@xxxxxxxxx> wrote:

We're looking for a solution to create a secure single-signon deployment on a Windows network. The chain of connections looks like this:

Client: Telnets through SSH Tunnel to -->

Does this mean that you are setting SSH port forwarding (e.g. with ssh -L)

Exactly, yes. On the client I execute the two following commands in separate DOS console windows in this order:

- 1) ssh -v -N -L 2023:server1:23 server1
- 2) telnet localhost 2023

and using telnet through that (that's what "tunnel" usually means), or that you are actually logging into Server1 via SSH? Sometimes people use "telnet" as a generic word referring to any kind of remote login (which it isn't). I'm assuming the latter, because otherwise your description doesn't make sense to me.

No, I'm truly using a telnet client.

Re: OpenSSH, Telnet, Windows Authentication and double-hops

Server1: that runs our application locally and connects to ---->
Server2: that serves up the database using SQL Server

We're hitting an issue when we reach the SQL Server machine. Logging in to SQL Server, the network has deprecated our logon down to 'NT AUTHORITY\ANONYMOUS LOGON'. The database kicks us out.

We've learned that this is commonly referred to as the "double-hop" issue and is well known with web development. There are mechanisms in IIS to set up delegation and impersonation and caching etc, to get past this.

We want to continue using public/private key authentication for the SSH.

You will not be able to, at least not alone. SSH publickey authentication does not provide the other side with either a Kerberos ticket, or your password in order to acquire one. You need GSSAPI/Kerberos authentication with ticket forwarding ("delegation").

I'm going to look into this right away. I'm aware of Kerberos, but have never seen the term GSSAPI before. Is the 'delegation' a configuration that needs to be made on the Kerberos service? I expect that this will need to be done at the domain layer, is this correct? Will we have to rely on someone with the authority to make changes at the domain level to be able to do this? I've read the term "domain controller" in reference to the Kerberos service, does that fit into what you are describing to me?

We've tried the -A switch when starting up the SSH tunnel with no avail.

This has to do with forwarding the OpenSSH key agent, which has nothing to do with Kerberos tickets.

Ok. Sounds like there's no need for us to use this switch then.

Re: OpenSSH, Telnet, Windows Authentication and double-hops

Is there anything that SSH can offer us so that we can maintain the authentication ticket over the second hop?

You mean, maintain it over the first hop so it's available for the second.

Yes, that's what I'm hoping for.

You haven't said what SSH implementation you are using. Some provide

We're focusing on the OpenSSH for Windows distribution. Client side, we're going to need 2 flavors... one for Windows desktop machines, and another for Windows CE devices.

integration with Windows Kerberos (SSPI) and can do this for you, e.g. Tectia from ssh.com and VShell from VanDyke. You *might* get it to work with OpenSSH/Cygwin. I have compiled OpenSSH on Windows with Kerberos support and had it work; however, the ccache is an MIT one and has nothing to do with the Windows ccache. The MIT KfW system does integrate with SSPI; however, I don't know if there's a way to hook OpenSSH into it.

Did you make code changes to the OpenSSH sources to achieve this?

Is the MIT ccache (certificate cache?) available to all of us?

This brings up an interesting segue actually... we'd love to remove the dependency for the Telnet server/client and are thinking ahead to integrating an SSH server in our application. Essentially, we'd like to run our application as a service that opens a secure port with the SSH authentication and that limits user interaction to streaming data from our application to the client. I'm getting the impression that it would be possible to do this with the OpenSSH source code, am I thinking correctly? Ultimately, I'd like to have our service use core functionality from the OpenSSH libraries without changing any of the core code... maybe just make calls into the cygcrypto-0.9.7.dll (or

Re: OpenSSH, Telnet, Windows Authentication and double-hops

whichever one is truly pertinent)... does this seem possible?

We'd even be thrilled to just get rid of Telnet now without our own links into the SSH core, but we've run into a couple of behavioral differences that are blocking us from doing it. I've thrown one up to the group for help in this posting:

http://groups.google.ca/group/comp.security.ssh/browse_thread/thread/c3fb90fd3b747553/#

and the other has to do with killing orphaned sub-processes and I've just found this thread to examine:

http://groups.google.ca/group/comp.security.ssh/browse_thread/thread/51c4ad8e9494a35f/0b8854eb4a1b32a7?lnk=gs

Richard, many, many thanks for taking the time to help me out. Your feedback is helping me understand what's possible and driving out the shadows! :~)

Regards,
John

—
Richard Silverman
r...@xxxxxxxx