

RE: how to block connections running on non-default ports

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2005-08/0304.html>

From: James Scott-Brown (jamescottbrown_at_tiscali.co.uk)

Date: 08/19/05

To: <security-basics@securityfocus.com>

Date: Fri, 19 Aug 2005 20:28:41 +0100

As far as I am aware, telnet will not generally be detected as masqueraded connections because all the telnet protocol does is send any received data to the screen and anything typed to the remote computer. This is why you can use telnet to connect to a website on port 80 and send raw HTTP commands, or send an email from a mail-server via raw SMTP on port 25. A telnet connection on port 443 (normally used for SSL) is indistinguishable from an SSL connection coming from a browser. As far as the server is concerned, it is using the SSL protocol – not the telnet protocol. If you telnet to port 443 you will not receive a shell, you will connect to the SSL server (if one is running). If you wish to block port 443, you should do so at the firewall – after checking that it is not needed.

James Scott-Brown

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

From: Niranjan S Patil [<mailto:niranjan.patil@gmail.com>]

Sent: 15 August 2005 16:36

To: security-basics@securityfocus.com

Subject: how to block connections running on non-default ports

Hi list,

I recently noticed that our corporate IDS could not block some of connections that are seemingly unauthorised.

I launched a telnet connection to a remote server on Internet on port 23 and it was successfully blocked by our firewall. I change the listening port of the telnet server to 443 and launched another telnet connection on port 443. Neither our firewall or IDS was able to block this connection.

Aren't IDS supposed to block such masqueraded connections, i.e., protocols with non-default ports.

SecurityFocus BASICS: RE: how to block connections running on non–default ports

I have less knowledge on IDS, but isn't it simple for them to check packet headers and block/filter if they are not on right protocol/port?

Is this normal with all IDS?

Any help is appreciated.

--

Regards,
Niranjan S Patil