

Re: Dlink.com.sg intrusion with worm??

Source: <http://www.derkeiler.com/Newsgroups/comp.security.misc/2006-10/msg00062.html>

- *From:* ibuprofin@xxxxxxxxxxxxxxxxxxxxxxxxxxxx (Moe Trin)
 - *Date:* Wed, 11 Oct 2006 19:25:17 -0500
-

On 12 Oct 2006, in the Usenet newsgroup comp.security.misc, in article <452d164f\$1@xxxxxxxxxxxxxxxxxxxxxxxx>, Luther wrote:

I thought I could get some geeks to show how to counter this intrusion.

It's highly unlikely to be an intrusion. You are using a piece of easily confused or badly misconfigured software.

Questions

1. Packet filtering why and how? How much technical detail you have to know?

Concepts – addresses, protocols, port numbers and how they all tie together.
A couple of RFCs that might help:

1118 Hitchhikers guide to the Internet. E. Krol. September 1989.
(Format: TXT=62757 bytes) (Status: INFORMATIONAL)

1180 TCP/IP tutorial. T.J. Socolofsky, C.J. Kale. January 1991.
(Format: TXT=65494 bytes) (Status: INFORMATIONAL)

Use any search engine and look for RFC1118 and RFC1180.

2. www.dlink.com.sg will response from relatively fast to very slow as you request more pages (3~5). It required you to enable script for both the global and local site. Did it use some script code to attack port 21 and 1149?

```
[compton ~]$ grep 21 /etc/services
ftp 21/tcp # File Transfer [Control]
[compton ~]$
```

0959 File Transfer Protocol. J. Postel, J. Reynolds. October 1985.

Re: Dlink.com.sg intrusion with worm??

(Format: TXT=147316 bytes) (Obsoletes RFC0765) (Updated by RFC2228, RFC2640, RFC2773) (Also STD0009) (Status: STANDARD)

1635 How to Use Anonymous FTP. P. Deutsch, A. Emtage, A. Marine. May 1994. (Format: TXT=27258 bytes) (Also FYI0024) (Status: INFORMATIONAL)

A couple more RFCs for you to look at. It might be a surprise to you, but there is more than the World Wide Web on the Internet. That RFC0959 pre-dates hypertext and the web by five years, and the origins of FTP go back to April 1971 – a bit before Bill Gates heard about computers. Port 1149 on your system was one end of a conversation with port 21 on their end – you were trying to download something.

You should try it if you think you are better than them.

Why? I have no need to download anything from DLink, never mind their Singapore office.

3. Someone may want to suggest that disable all unused ports. But then some of the port may use from time to time eg ftp, smtp, NNTP, POP etc.

Are you running a _server_ on each one of those ports? I very much doubt it seeing as how you don't recognize an FTP transfer. Big clue: people connect to those ports to find a server. If you aren't serving, you DON'T want the ports open. Period.

So what would you suggest? Will it mean that I have to enable it everytime when use?

No, you are a _client_ not a server. Your end of the connections is those high port numbers above 1025 (such as the 1149 you thought was being "attacked"). Your system picks the next available port number to CALL OUT. But because there is no server listening on those ports, no one can CALL IN. Notice the difference in the words "out" and "in".

Old guy

.

Re: Dlink.com.sg intrusion with worm??