

comp.security.firewalls: Re: Hacked? External address knocks on internal private address...

Re: Hacked? External address knocks on internal private address...

Source: <http://www.derkeiler.com/Newsgroups/comp.security.firewalls/2002-10/5615.html>

From: Whatever (the_duke@terra.es)

Date: 07/25/02

From: "Whatever" <the_duke@terra.es>

Date: Thu, 25 Jul 2002 05:13:16 GMT

Sorry for my poor English I'm Spanish... Specially now that I'm sleepy :)

I've peeked over your log, so let's see...

The important part of your message is that FTP is allowed out... since you can see that the public IP is using, infact, port 21, used to FTP.

- 1) You open a connection to an FTP Server and logon.
- 2) When you ask the server for a file the server issues a "PORT" command specifying a randomly choosen high port.
- 3) The client computer opens the port specified with the port command, and the FTP Server connects to it.

The client connection to the FTP server is called "control" connection.

The Server connection to the client is called "Data" connection.

Some Firewalls as Firewall-1 allows inspection at the application layer for FTP, so it can open a port on the firewall to allow the incoming Data connection... But there are still some firewalls that won't allow this, since they won't inspect the Application layer to find out if a "PORT" command has been issued.

I guess this is probably what is happening:

A user connects to an FTP server with IP 24.64.63.20 the FTP issues a PORT command and tries to connect to the client (192.168.168.21), but your firewall doesn't know it's not a hostile connection, but a normal FTP procedure, so it drops the packet.

So my guess is it's not really an attack but simply someone trying to connect to a FTP server and he/she would be going nuts trying to figure why he/she can't download files from the server.

I've reached this conclusion from your Log since you can see the external

Re: Hacked? External address knocks on internal private address...

comp.security.firewalls: Re: Hacked? External address knocks on internal private address...

(Public) IP is always using port 21 (FTP control), and the ports it is trying to access are high ports (Not service ports), and they are random or atleast pseudo-random. You have told us that FTP is allowed, therefore it must be a misconfiguration of the Firewall or the lack of support to FTP protocol from the firewall to open ports on the "PORT" command.

Hope I could help you a bit.

Best Wishes.

"Randell D." <randell@com.yahoo> escribió en el mensaje
news:FaB%8.40945\$Ag2.2056865@news2.calgary.shaw.ca...

> Folks,

>

> *I examine the log files daily and have more recently found the following
> messages*

>

> *22/07/2002 13:55:24.528Out-of-order command packet dropped24.64.63.20, 21,*

> *WAN192.168.168.21, 1945, LAN*

> *22/07/2002 13:57:42.624Out-of-order command packet dropped24.64.63.20, 21,*

> *WAN192.168.168.21, 1979, LAN*

> *22/07/2002 14:01:53.624Out-of-order command packet dropped24.64.63.20, 21,*

> *WAN192.168.168.21, 1988, LAN*

> *22/07/2002 14:03:16.336Out-of-order command packet dropped24.64.63.20, 21,*

> *WAN192.168.168.21, 2005, LAN*

>

> *We do not have any local services thus everything from HTTP, POP and
> whatever are blocked when requested from the world though employees within
> the building can mail, surf and FTP out. I have two networks – One that
sits*

> *behind the firewall which has two laptops being used by independant
(sales)*

> *staff. I have little/no control over these users machines. I also have a*

> *router configured behind the firewall creating a network purely for*

> *permanent employees who utilise PCs owned by the business with which I
have*

> *full control over – Each PC has an antivirus program running on it as well*

> *as a software firewall thus, correct me if I am wrong, but someone from
the*

> *Internet would have to climb two walls (firewall and router) before
getting*

> *in at the business owned and controlled network.*

>

> *My concern is the above log file tells me that a source IP of 24.64.63.20
is*

> *attempting to access 192.168.168.21 (the latter being my router) I am*

> *wondering if someone has managed to bypass the firewall and are now
working*

> *bypassing the router – Could I be right? If I am wrong, how do they know
my*

> *routers IP address since it is behind the firewall and hidden... There are*

Re: Hacked? External address knocks on internal private address...

comp.security.firewalls: Re: Hacked? External address knocks on internal private address...

> *only three devices*
> *on the 192.168.168 network and the fact they've come straight in at the*
> *router's*
> *address really has put the wind up me...*
>
> *All help would be hugely appreciated as I've taken great care with my*
> *network – before my time, someone had hijacked the servers and sent junk*
> *email to the world – and neither I nor the business want this to happen*
> *again...*
>
> *Regards*
> *Randell D.*
>
>
>

- ***Next message:*** Barry Strets: "Cisco VPN access thru Netscreen 10"
- ***Previous message:*** Cid Khan: "CheckPoint NG – Keygen"
- ***In reply to:*** Randell D.: "Hacked? External address knocks on internal private address..."
- ***Messages sorted by:*** [date] [thread] [subject] [author] [attachment]