

Re: firewall appliance help

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2001-11/0090.html>

From: Erlend J. Leiknes (nookie@online.no)

Date: 11/20/01

Message-ID: <002701c17186\$f7ef5c60\$0a01a8c0@supermaskin>
From: "Erlend J. Leiknes" <nookie@online.no>
To: "HA LO" <halo7@onebox.com>, <pen-test@securityfocus.com>
Subject: Re: firewall appliance help
Date: Tue, 20 Nov 2001 06:48:23 +0100

There is a method called "Dumb scan" which relies on a computer on the internet/outside the firewall that aren't firewalled (trusted host (If you know the ip of a trusted host, then you can portscan internal machines)).

Get the hping2 utility, and you will find the text in their readme file.

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

From: HA LO <halo7@onebox.com>

To: <pen-test@securityfocus.com>

Sent: Monday, November 19, 2001 9:59 PM

Subject: firewall appliance help

- > *I am pretty much a newbie to actual pentesting but not a newbie to networking.*
- > *I have been lurking on this list a while trying to learn as much as I can. So here is what I need a little help with.*
- >
- > *I am trying to communicate/scan with a computer behind one of those firewall/router appliances. When I've done an Ack scan it shows that all ports are unfiltered,*
- > *but all other scans show the ports as being filtered, so I think it is a packet filter and is not stateful. It probably is also performing NAT. How can I determine what hosts are live on the internal network and how would I be able to establish any communication with them.*
- >
- > *What kind of switches with nmap would I be able to use to determine live hosts behind such a router, and then once I can determine what hosts are up what kind of tools can I use to actually try and test/penetrate such a host through the firewall.*
- >
- > *Sorry to take up your time with such a newbie question but I've searched the archives and didn't really come up with a specific solution. Links or just a push in the right direction would be really appreciated, I'll do the research from there. Thanks.*

SecurityFocus Penetration: Re: firewall appliance help

>
>
> _____
> *FREE voicemail, email, and fax...all in one place.*
> *Sign Up Now! <http://www.onebox.com>*
>
>
>

--
> 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/>
>
>

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:** jjore@imation.com: "[Re: wanted: a script to try dictionary attacks against NOTES ID files](#)"
- **In reply to:** [HA LO: "firewall appliance help"](#)
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)