

RE: [fw-wiz] False results to DMZ

Source: <http://www.derkeiler.com/Mailing-Lists/Firewall-Wizards/2006-01/msg00074.html>

- *From:* Ralf.Zessin@xxxxxxxxxxx
 - *Date:* Tue, 24 Jan 2006 14:04:00 +0100
-

Hello David,

with firewalls or other security devices between scanner and target you have always a Problem with malformed IP-Packets. The behaviour depends on firewall-settings.

Please check the behavior in your case with tcpdump. I assume that your pix first pretends that all ports are open and if the Ack-Flag is received (which never comes with the syn-scan), the real connection was established and if fails, the RST-Flag comes back. This behaviour was one kind of protection against SYN-Flood attacks .

Try the following:

Connection to an open port with telnet (telnet <target> <portnum>)
With tcpdump you should see the normal three-way handshake

Connection to a unavail port/host

If you see the three-way handshake with an additional RST Packet, you know, it works like described above.

Therefore you have to use the tcp-connect() scan to check your systems.

- Ralf

> -----Original Message-----

> From: firewall-wizards-admin@xxxxxxxxxxxxxxxxxxxxxx

> [<mailto:firewall-wizards-admin@xxxxxxxxxxxxxxxxxxxxxx>]On Behalf

> Of David U.

> Haltinner

> Sent: Friday, January 20, 2006 4:14 PM

> To: firewall-wizards@xxxxxxxxxxxxxxxxxxxxxx

> Subject: [fw-wiz] False results to DMZ

>

>

> First off, the DMZ is setup with virtual interfaces (PIX), and the

> scanning source is inside. The firewall allows anything IP from this

> scanner. If I scan most of the DMZ's, I get normal results,

RE: [fw-wiz] False results to DMZ

> with all of
> the scans.
> Using NMAP, If I scan one specific DMZ, I only get results
> with the SYN
> scan and TCP window scans, AND it says every port is open (what the
> firewall allows). Cisco support is not being helpful. Does anyone have
> any idea why this is? It's weird. Im trying to automate Nessus against
> the DMZ servers, and its giving too many false positives about open
> ports.
> I have taken packet traces, and the only thing weird is that I am
> getting an ACK back for every port, but they are Zero Window
> (TCP Window
> Scan brings back every port open).
> Any ideas?
> _____
> firewall-wizards mailing list
> firewall-wizards@xxxxxxxxxxxxxxxxxxxxx
> <http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>
>

firewall-wizards mailing list
firewall-wizards@xxxxxxxxxxxxxxxxxxxxx
<http://honor.icsalabs.com/mailman/listinfo/firewall-wizards>

• **Follow-Ups:**

- ◆ **[RE: \[fw-wiz\] False results to DMZ](#)**
 ◇ From: David U. Haltinner

- Prev by Date: **[RE: \[fw-wiz\] Questions about converting FW-1 ruleset to PIX - sort of...](#)**
- Next by Date: **[Re: \[fw-wiz\] Scanning host thru Check Point](#)**
- Previous by thread: **[RE: \[fw-wiz\] False results to DMZ](#)**
- Next by thread: **[RE: \[fw-wiz\] False results to DMZ](#)**
- Index(es):
 - ◆ **[Date](#)**
 - ◆ **[Thread](#)**

RE: [fw-wiz] False results to DMZ