

RE: UDP port scan results

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2002-04/0042.html>

From: Dawes, Rogan (ZA – Johannesburg) (rdawes@deloitte.co.za)

Date: 04/22/02

From: "Dawes, Rogan (ZA – Johannesburg)" <rdawes@deloitte.co.za>

To: "'Noonan, Wesley '" <Wesley.Noonan@bmc.com>, "'pen-test@securityfocus.com' '" <pen-test@securityfocus.com>

Date: Mon, 22 Apr 2002 18:11:36 +0200

I think nmap has an explanation of how it determines whether a UDP port is listening or not.

Essentially, if a UDP port has a listener, the packet will be accepted, most times silently (i.e. if it is not the correct format that the listener would normally respond to). If there is no listener there, the machine will return an ICMP port unreachable message, containing the port number in question.

Hence, a port scanner can assume, if it gets no response, that there is something listening, i.e. the port is "open".

However, this behaviour is easily mimicked (?sp) with a firewall in front of the target server. If the firewall is configured to silently drop unauthorised packets, the scanner will receive no response to its packets, and assume that ALL ports are open.

If there is a screening router in front of the target, and it is configured to send ICMP unreachables (fairly standard Cisco filter result), the scanner can report that the port is filtered, since the unreachable is coming from a different IP address to that of the target.

So, to answer your question eventually, it would be possible to write a port scanner that interrogated EVERY port, and only highlighted those that responded, however, that would require the following conditions:

The scanner author knows every possible UDP protocol, enough to build a first handshake packet, that would cause a response packet. (I would think this is prohibitive to start with)

The scanner would have to try EVERY UDP protocol it knows about against every port, in order to discern between "not there", and "I'm ignoring invalid packets" on non-standard ports. An example might be a TFTP server running on the SNMP well-known port. It wouldn't answer to a SNMP handshake, but would likely respond to a TFTP handshake

To your [1], I recommend this, because otherwise, you are providing accurate

SecurityFocus Penetration: RE: UDP port scan results

info, rather than the 65535 "positive" results they'd get otherwise.

Hope this was useful.

Rogan

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

From: Noonan, Wesley

To: 'pen-test@securityfocus.com'

Sent: 02/04/20 02:10

Subject: UDP port scan results

After having my previous post blocked and being asked to "search the archives", I did just that but only found one post (using "UDP" as the search criteria) that kind of had an answer. I did some digging around on the net, and found a site that had a better answer. The question was why all UDP ports are show as opened using various port scanners. The answer seems to be, and it kind of makes sense, that UDP being connectionless, the scanner has no real method to differentiate between an opened port, and a port that was silently dropped (which most firewalls should[1] do). The only way to know for sure that a port is closed would be to get a response indicating a closed port (i.e. ICMP response). This has led me to some other questions.

Is there a port scanner on the market (free or \$\$\$) that does not generate the "false positive" result of a UDP scan against a stealth host? For example, rather than reporting the ports opened, it only reports those ports it gets some sort of response from as opened, and reports the rest as "may be opened", "state unknown" or something similar.

If a UDP scan is run against a host, and rather than showing all ports the results show only certain ports opened, should this be considered a bad security situation, and if so why? My thoughts are that yes, it should be, as the host is not functioning in a "stealth" mode, which I think is a more secure process[1]. Simply put, a scanner can know with certainty which ports are opened if only certain ports are listed, where as in the other situation, every port appears to be opened.

RE: UDP port scan results

SecurityFocus Penetration: RE: UDP port scan results

Any opinions/answers from the list? Thanks.

Wes Noonan, MCSE/MCT/CCNA/CCDA/NNCSS
Senior QA Rep.
BMC Software, Inc.
(713) 918-2412
wnoonan@bmc.com
<http://www.bmc.com>

[1] I say should because most references I have seen recommend a firewall operating in a stealth fashion as being more effective since it requires any scanning, etc. to time out before proceeding causing more time to pass and increasing the likelihood of catching it occurring.

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:** [Evrin ULU: "Source Route/Spoofed Source"](#)
- **Maybe in reply to:** [Noonan, Wesley: "UDP port scan results"](#)
- **Next in thread:** [Franck Veysset: "Re: UDP port scan results"](#)
- **Next in thread:** [Anders Thulin: "Re: UDP port scan results"](#)
- **Reply:** [Franck Veysset: "Re: UDP port scan results"](#)
- **Messages sorted by:** [\[date \] \[thread \] \[subject \] \[author \] \[attachment \]](#)