

RE: Strange replies on closed port

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/pen-test/2006-02/msg00014.html>

- *From:* "Dario Ciccarone (dciccaro)" <dciccaro@xxxxxxxxxx>
 - *Date:* Wed, 1 Feb 2006 01:59:33 -0500
-

Thomas:

It would help immensely to those interested in answering your question to have a copy of the traffic as a PCAP file – while the test can easily be reproduced, would save time just to check your capture instead of doing it all again ;)

About your assumptions:

- a) hosts shouldn't by default just 'drop the packet and forget about it'. In TCP, the standard reply to a SYN segment sent to a closed port should be a RST – not dropping the packet. Dropping the packet w/o sending anything back smells of firewall in the middle, or some kernel tweaks
- b) that is the expected behaviour – but the ip field doesn't make any sense
- c) that message (AFAIR) should only be sent by the host when receiving an UDP datagram (not TCP) to a non 'listening' port.
- d) that message isn't generated by the end host, but by something in the path filtering packets – probably a router with ACLs

Packet filtering devices behaviour is all over the place. As an example, firewalls will probably drop the packet and send nothing back. Routers with an ACL blocking the packet in question will drop – and could, or could not, send an 'ICMP admin prohibited' back.

nmap does have a bunch of logic embedded to deal with all those variations – that's why when scanning a host it can print status like 'closed, open, firewalled, etc' for ports.

Thanks,
Dario

-----Original Message-----
From: thomas springer [<mailto:tuevsec@xxxxxxxx>]

RE: Strange replies on closed port

Sent: Sunday, January 29, 2006 2:53 PM
To: pen-test@xxxxxxxxxxxxxxxxxxxxx
Subject: Strange replies on closed port

Hi,

Nmap 3.999 is out! – with a "--badsum"-option like it is described in <http://www.phrack.org/phrack/60/p60-0x0c.txt> – have a look at the release notes.

As a brave pen-tester I took hping2 to fiddle around and check the basic statements of the ancient phrack-article.

What I expected to find was:

Connecting to a closed Port w/o Firewall: Target sends back an RST
Connecting to a closed Port with Firewall: Target drops packet, nothing happens.

But things seems that things are more complicated. I tried

hping -S -c 1 -p 1 www.hostname.com (a simple TCP-Syn on Port 1, which

I consider closed everywhere) shows that

- a) many hosts drop the packet as expected
- b) some hosts respond as expected "len=46 ip=000.67.41.130 ttl=48 id=29443 sport=1 flags=RA seq=0 win=512 rtt=25.0 ms"
- c) some hosts respond with ICMP: "ICMP Port Unreachable from ip=000.227.127.227 name=<name of target>"
- d) one hosts responds strange, like "ICMP Packet filtered from ip=000.94.95.253 name=<router 1 hop before the server>"

a and b seems to be clear:

a: firewalled host

b: non-firewalled host

c and d are a bit strange: Who is responding with the icmp-messages: the target-host or a packetfilter? Especially the hping-message in d confuses me a bit.

What should be the default behaviour for an ip-stack if it gets a SYN on a closed Port?

A bit confused,

tom

RE: Strange replies on closed port

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do!

Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831

Audit your website security with Acunetix Web Vulnerability Scanner:

Hackers are concentrating their efforts on attacking applications on your website. Up to 75% of cyber attacks are launched on shopping carts, forms, login pages, dynamic content etc. Firewalls, SSL and locked-down servers are futile against web application hacking. Check your website for vulnerabilities to SQL injection, Cross site scripting and other web attacks before hackers do!

Download Trial at:

http://www.securityfocus.com/sponsor/pen-test_050831
