

Next-hop scanning for open firewall ports

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/bugtraq/2002-09/0057.html>

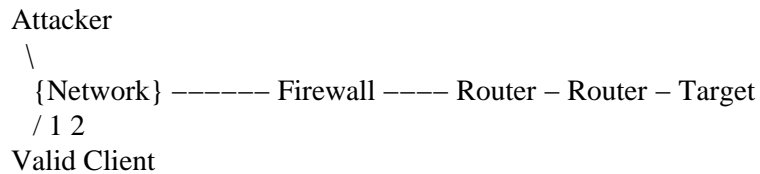
From: David G. Andersen (dga@lcs.mit.edu)

Date: 09/06/02

Date: Thu, 5 Sep 2002 19:31:15 -0400
From: "David G. Andersen" <dga@lcs.mit.edu>
To: bugtraq@securityfocus.com

Thinking about ways to figure out how to get through firewalls, the following attack occurred to me. The technique is similar to "firewalk"ing (Goldsmith) and to IP ID reverse scanning (Antirez). I call it next-hop scanning, because it operates by interrogating a router after the firewall, not the target.

Given a target computer (T) protected by a firewall (F), with some number of intervening routers:



The firewall has been configured to only permit a few valid clients access to the target machine. This kind of filtering is often performed to prevent or mitigate the effects of DoS attacks, where it's beneficial to push the filtering as far out into the network as possible. Now, assume that other traffic needs to traverse the network after the firewall, and can reach router 1.

The attack: Spoof traffic to the target, but set the TTL such that the packets expire at router 1. (Like firewalk) R1 will send back ICMP expired messages, but the attacker won't be able to observe them. Instead, the attacker will simultaneously send legitimate traffic to router 1, and will watch the IPID on the return (like idlescan). By this method, the attacker can determine which packets got through. If R1 is a busy router, it may be necessary to send a burst of a few packets to observe a significant jump in the IPID space. An example with a cisco router:

Start running an hping to watch the IPID at router1:

SecurityFocus Bugtraq: Next-hop scanning for open firewall ports

hping2 -r Router1

Then send a small burst of packets at the target, but cause them to expire at Router1:

```
hping2 -t 15 -i u10 -c 20 target
```

This results in a gratifying bump in IPID:

```
192.168.3.1 seq=91 id=+19 rtt=76.5 ms
192.168.3.1 seq=92 id=+16 rtt=233.4 ms
192.168.3.1 seq=93 id=+14 rtt=259.6 ms
192.168.3.1 seq=94 id=+41 rtt=76.2 ms <*** Note ID change
192.168.3.1 seq=95 id=+12 rtt=76.6 ms
192.168.3.1 seq=96 id=+10 rtt=75.5 ms
```

Nothing amazing, but it does point out another problem that can come from predictable IP IDs. Unlike idlescan, it's not anonymous, but in this case, the traffic never hits the target (so an IDS there won't register it), and it lets you use some random, forgotten router whose OS is less likely to do paranoid IP ID generation. Also has no dependence on TCP — you can use any protocol that gets through the filter.

To implement this attack, you need to know a router behind the filter. Hence, it's more useful in things like DoS filtering where the filtering is at the edge of a public network, and not at a private network. Interacts well with network discovery tactics.

References:

"Nmap stealth port scanner", Fyodor Vaskovich,
<http://www.insecure.org/nmap/index.html> 2002

"Posting About the {IP ID} Reverse Scan", Salvatore Sanfilippo (antirez),
<http://www.kyuzz.org/antirez/papers/dumbscan.html> 1998

"hping home page", Salvatore Sanfilippo (antirez),
<http://www.hping.org/>

"Firewalking: A traceroute-Like Analysis of IP Packet Responses to Determine Gateway Access Control Lists",
David Goldsmith and Michael Schiffman, 1998
<http://www.packetfactory.net/firewalk/>

I wasn't able to dig up evidence that this has been implemented before (though it's pretty close to idlescan). As always, feedback encouraged.

–Dave

Next-hop scanning for open firewall ports

SecurityFocus Bugtraq: Next-hop scanning for open firewall ports

--

work: dqa@lcs.mit.edu me: dqa@pobox.com
MIT Laboratory for Computer Science <http://www.angio.net/>
I do not accept unsolicited commercial email. Do not spam me.

- **Previous message:** Geoff Craig: "UPDATE: (Was Veritas Backup Exec opens networks for NetBIOS based attacks?)"
- **Next in thread:** Chris Brenton: "Re: Next-hop scanning for open firewall ports"
- **Reply:** Chris Brenton: "Re: Next-hop scanning for open firewall ports"
- **Reply:** Darren Reed: "Re: Next-hop scanning for open firewall ports"
- **Messages sorted by:** [date] [thread] [subject] [author] [attachment]