

RE: Questions about 192.168

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2003-07/0476.html>

From: D. Weiss (*David_at_cawdgw.net*)

Date: 07/09/03

To: "Jim" <jimhoward300@hotmail.com>, <SECURITY-BASICS@securityfocus.com>

Date: Tue, 8 Jul 2003 23:29:39 -0700

X.X.X.255 is a broadcast address normally. Ignore super netting, etc. Just think class C IPs for the moment, like your modem. Your cable modem is, for all intents and purposes, a router, whether or not you have it set as some can, to "Gateway". If yours is old, it may not be a router, but lets keep it simple.

Routers don't behave as normal network devices.

Routers ignore and drop broadcasts. By definition, routers will not process and pass a broadcast request. If they did pass them, the entire Internet would be one big broadcast storm.

When the broadcast ping hit your router interface, it dropped it, as a matter of course. Expected behavior.

When you pinged the router directly, it slipped into normal network device mode and answered (although a "real" router might be configured via access list to drop pings and other types of suspect traffic.) Because it answered, the PC's arp table caught the traffic and logged the response.

Now, the "Private address" ranges (10.x.x.x, 172.16-31.x.x, and 192.168.x.x) are not supposed to be configured to be passed by routers to the Internet, per the RFC 1918. However, manufacturers of routers can't make this impossible because if I have a large company, geographically dispersed or not, I will find it better to use private addresses for my intranet, and then only need a few "Public" addresses so my folks can email, VPN in from home, etc.

And then, some ISP's are just plain sloppy and don't "Not" route the private address spaces.

So, if I want to go around taking wacks at peoples networks and systems, I have to look at where I'll get the most "Bang for the Buck" or best return for time spent (or bandwidth used, and program scripted) I'm going the smack away at Microsoft product published vulnerabilities because there's lots of pretty little scripts out there already and there are by far more untrained persons running Microsoft products than untrained *nix products. I'm going

to go around looking like 192.168 networks because that's what lots of Network Address Translation (NAT) devices, like cable modem/routers use. True, the *nix systems can also be penetrated, but by far the number of untrained script-kiddies using pre-canned scripts outnumber the knowledgeable hackers, and the old adage that if you are hacking to look kewl, you hack Microsoft and if you are "in it for the money, you hack *nix" may not be always true, it is mostly true that *nix hacks want nothing more than to NOT be noticed (once caught on to being rooted because the hacker had cleaned up some system problems that caused the HP Unix load to barf, because he wanted that system to run really well, so he could reliably use it). Anyway, there are all sorts of silly things a person behind a dsl router or cable modem can do if they are untrained, such as run W2K and not block the Active Directory port 445, or running Win9X, ME, or NT and not blocking outgoing 137-139, thereby inviting anyone who can reach your system using a private address to join your subnet or private class C and bang away at your shared resources and userids/passwords. If the ISP routes the private range, why, then I have a greater range for my scans and attacks. And I'll be a couple hops away. And I won't stay out there for any length of time at any IP because one CAN triangulate on an IP, if it stays out there long enough and you have a couple of buds at different places willing to help.

As far as not getting responses, it is rather trivial to ignore pings, or even statefully packet inspect and ignore goobs of traffic that are not "interesting". This is sometimes incorrectly called "Stealth Mode". When in a true stealth mode, the interface will not answer to anything. The problem with achieving this is the same programming problem application and software engineers face: Accounting for every weird thing someone might try. A couple of years ago there were some sniffer programs that could sit in stealth mode, sucking up your intelligence on your network, that were advertised as being stealthed. They did not report home, someone had to come get the collected data from the machine. But a specially crafted corrupt arp reply message forced on the wire caused these promiscuously set "stealthed" interfaces to answer, giving away where they were and who they were. To the informed, few interface configurations are truly "stealthed". See replay attacks on the web for explanations on how to defeat SPI'd interfaces. If you aren't really up on the subject, or you just left your toolbox at home, even a access control list denying pings can look like stealth. You run a prepackaged port scanner. The person who wrote it knows how to hit ports and see if they are listening. But to scan someone with it, you HAVE to talk to them. You HAVE to check if the port is listening to get an answer. They don't normally (okay, MS and some MAC/*nix DO announce they are listening to the world) tell the world they are there till asked. So your firewall DOES get the IP and port they knocked on. Is it surprising that they are blocking the ICMP packets that are the guts of pings and trace routes? (Trace route is basically a set of pings with increasing TTLs (Times to live))

If you could immediately scan them, you'd likely find some ports listening (Hey, they have to hear their own scan victims replies, don't they?) but the newer ones are using stateful packet inspection on those, to insure they don't reply. So you replay attack. And the knowledge and speed envelope

spiral upward, ever increasing.

The old saw "the more you know, the more dangerous you can be" is true.

Very wordy for me and in some places, after proof reading, overly simplified, but those who want to take issue should be reminded they didn't ask these questions and I judged Jim's skill level on the basis of one short email. And Jim, same to you, please don't see insult in the level of the explanation. Answering an email is vastly different than sitting in my basement with my lab and sniffers/snort boxes and killing a case of beer while enumerating my mom's PC 6000 miles away (Only as practical examples mom, never in malice)

D. Weiss
CCNA/MCSE

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

From: Jim [mailto:jimhoward300@hotmail.com]
Sent: Monday, July 07, 2003 5:27 PM
To: security-basics@securityfocus.com
Subject: Questions about 192.168

Hi,

I've been following some of the conversations about 192.168 networks, and tried some experimentation, and came up with a few questions:

1. I've tried the technique mentioned to ping the broadcast address, and then check arp -a (on Windows 2000 machines). This didn't seem to work. For example, I pinged 192.168.100.255. This should add all 192.168.100.x IPs into my arp cache, right? But my cable modem didn't show up in my arp cache after doing this. However, when I pinged my cable modem directly (192.168.100.1), it did show up in my arp cache. I tried this on a computer on the Internet (which I telneted to), with similar results. (Is it because Microsoft recognizes 192.168.100.255 as a valid IP?). When I do a traceroute to my cable modem (192.168.100.1), it is a direct hop.
2. However, with the computer on the Internet I mentioned (which I am telneting to), there were the following IPs: 192.168.1.0, 192.168.1.1, 192.168.1.2, 192.168.1.3, and 192.168.1.255 – which I found through doing an nmap scan. (pinging 192.168.1.255 produced no results in the arp table) Three are apparently Cisco routers (192.168.1.0 and 192.168.1.255 are both ping-able). When doing nmap, it shows 192.168.1.255 as remote, the others as local. However, when I do a traceroute on these supposedly local ones, it shows a number of hops out over the Internet, implying that they are not connected locally. Does this make sense?
3. I recently checked my firewall (Network ICE), and noticed an attack from this IP: 192.168.1.113. I tried to ping the attacking IP, but no

SecurityFocus BASICS: RE: Questions about 192.168

response. The attack details were these:

TCP OS Fingerprint, and then FTP Port Probe. Does this make any sense?

How can someone use a supposedly local IP (192.168) to attack me?

(Cable modem with 2 computers hooked up).

So can someone clarify these things? IE, why does it look like the only way to really detect 192.168 devices on your network is to scan for them – in other words, the pinging of the broadcast address doesn't work (or am I pinging the wrong broadcast address?). Why do 192.168 devices, which are supposed to be local, have a number of (internet) hops between them when you ping them? And can anyone explain how someone could attack me via my cable modem, with a source address of 192.168.1.113 (which I was unable to ping or otherwise detect)? In general, why don't these 192.168 addresses show up in the routing table, netstat, etc.?

Thanks,

Jim

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!
The Gartner Group just put Neoteris in the top of its Magic Quadrant,
while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug–n–play secure remote access in
about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>

Evaluating SSL VPNs' Consider NEOTERIS, chosen as leader by top analysts!
The Gartner Group just put Neoteris in the top of its Magic Quadrant,
while InStat has confirmed Neoteris as the leader in marketshare.

Find out why, and see how you can get plug–n–play secure remote access in
about an hour, with no client, server changes, or ongoing maintenance.

Visit us at: <http://www.neoteris.com/promos/sf-6-9.htm>
