

Shields UP!!tm

Port Authority Edition – Internet Vulnerability Profiling
by Steve Gibson, Gibson Research Corporation.

Lower Port

Goto Port 112

Probe THIS Port

Probe Port 113

Enter Port: 0-65535

Higher Port

Goto Port 114

Port Authority Database

Port 113

Name: **auth / ident**

Purpose: **Authentication Service / Identification Protocol**

Description: Auth/Ident servers — which are supposed to run on the local user's machine — open port 113 and listen for incoming connections and queries from remote machines. These querying machines provide a local and remote "port pair" describing some other already-existing connection between the machines. The user's "ident" server is tasked with looking up and returning the connection's "USER ID" and perhaps additional information, such as an eMail address, full name, or whatever.

Related Ports: -

Background and Additional Information:

The "Authentication Protocol" for port 113 was originally proposed back in September of 1984 in a short two and a half page [RFC 912](#). Four months later that RFC was superceded by [RFC 931](#). Then eight years later, the protocol was further refined and renamed to the "Identification Protocol" with [RFC 1413](#).

The idea behind this protocol was to provide an automated means for remote servers to automatically identify the users who were attempting to connect to them. This means that when a user attempts to connect to a remote machine offering some public service, that remote server would, in turn, attempt to connect back to the user to ask the user's computer to identify the user.

This was originally conceived as a convenient means for allowing things like automatic logon to FTP servers so that users would not need to manually

"authenticate" themselves with a username and password. While that might have been a nice idea, the protocol was so simple-minded that it was trivial to fool. It provided no real security, so no one ever took it seriously or trusted it. It was finally renamed from "Authentication Protocol" to "Identification Protocol" because it fell so far short of being able to usefully authenticate anything.

The problem with completely stealthing port 113

Despite the fact that IDENT it was never very useful, even today some crusty old UNIX servers — most commonly IRC Chat, but some eMail servers as well — still have this IDENT protocol built into them. Any time someone attempts to establish a connection with them, that connection attempt is completely put on hold while the remote server attempts to use IDENT to connect back to the user's port 113 for identification.

If the user had no NAT router or personal firewall — and no IDENT server running in their machine to accept the remote server's connection request on port 113 — the user's computer would receive the port 113 connection request and immediately, actively reject the connection. The remote server would quickly know that IDENT was not running on the remote user's machine, it probably wouldn't care, and it would proceed to grant the user's suspended connection request.

However, if either a NAT router or a personal firewall ARE blocking and dropping incoming IDENT requests — if IDENT is fully stealthed — the remote server's attempts to connect would go unanswered. After waiting a while to hear back from its first connection request packet, it would send a second request packet. Then, after waiting much longer, it would send a third, and a fourth after waiting even longer still. With port 113 stealthed by the user, each incoming request would simply be dropped and ignored by the user's local security defenses. But in the meantime the remote server — and the user's original connection request — are "hung" waiting for some reply.

Since stealthed TCP connection attempts usually take 45 seconds or more to be abandoned, the effect is that stealthing of port 113 can cause some connections to some remote servers to hang for nearly a minute. (And SOME remote servers will even go so far as to finally refuse the original connection request if nothing is ever heard back from the client's port 113.)

Is all this really a problem?

Probably . . . Not. Most people who arrange to fully stealth port 113 never have any trouble connecting to any remote servers they commonly use. If, after stealthing port 113, you do experience connection delays, such as when sending or retrieving eMail, you'll know it immediately since it's usually quite apparent, and you'll know that your ISP is using an IDENT-dependent eMail server. (But this is *not* common.)

The trouble experienced by most security conscious people, is that port 113 can sometimes be rather tricky to stealth . . .

Stealthing port 113 on NAT routers

NAT router manufacturers certainly don't want to get the reputation that their NAT router causes connection trouble. But NAT routers have the problem that incoming IDENT requests are inherently unsolicited. As we know, NAT routers double as terrific hardware firewalls due to their natural tendency to drop all incoming unsolicited packets, thus stealthing their owner's networks. But since stealthing port 113 can "theoretically" cause connection problems (but probably never does) NAT routers usually treat port 113 specially. They deliberately return a "closed" status, actively rejecting connection attempts . . . but blowing their otherwise full-stealth cover in the process.

New users of NAT routers, who use this site to check their security, are often disappointed to discover a single closed (blue) port floating in a calm sea of stealth green.

The good news is . . . it **is** possible to configure NAT routers to return them to full stealth. The trick is to use the router's own "port forwarding" configuration options to forward just port 113 into the wild blue yonder. Just tell the router to forward port 113 packets to a completely non-existent IP address, one way up at the end of your router's internal address range. The router will then NOT return a port closed status. It will simply forward the port 113 packet "nowhere" . . . and your network will be returned to full stealth status.

It is my hope that NAT routers may consider incorporating the sort of adaptive dynamic IDENT handling which has always been (uniquely) offered by the Zone Alarm personal firewall . . .

Stealthing port 113 on personal firewalls

One of the things that first caught my eye about the Zone Alarm personal firewall (aside from the fact that it was free) was that it has always been very clever about handling IDENT's port 113. I recall being impressed and thinking "these guys really know what they're doing". When Zone Alarm receives an inbound connection request for port 113, it checks to see whether the computer has recently initiated any outbound connections to the remote server sending the IDENT request. If not, the IDENT packet is simply dropped, stealthing the protected machine. But if the user does have an existing "relationship" with the sender of the IDENT request, the IDENT packet is allowed to pass through Zone Alarm's firewall protection so that the user's system can respond normally (which usually means immediately returning a closed status for the port). This means that Zone Alarm is a "stateful packet inspecting personal firewall", not

just a simpler static packet filter.

At the time of this writing, Zone Alarm is still the only personal firewall to offer this sort of adaptive dynamic IDENT port handling. I hope that other firewalls will follow suit once the benefits are better understood.

The good news is that since IDENT is almost never used, simple "hard stealthing" of port 113, which **is** available from all personal firewalls, is probably sufficient. It will allow your system to remain completely invisible on the Internet and will almost certainly never cause any connection trouble.

The final IDENT RFC 1413:

- <http://www.ietf.org/rfc/rfc1413.txt>
- <http://www.faqs.org/rfcs/rfc1413.html>

Trojan Sightings: Invisible Identd Deamon, Kazimas

The entire contents of this page is copyright © 2003 by Gibson Research Corporation.

Home

Purchasing

Tech Support

Mailing List

Projects

Free Stuff

Discussions



Gibson Research Corporation is owned and operated by Steve Gibson. The contents of this page are Copyright (c) 2003 Gibson Research Corporation. Spinrite, ShieldsUP, NanoProbe, and the slogan "It's MY Computer" are registered trademarks of Gibson Research Corporation, Laguna Hills, CA, USA. GRC's web and customer [privacy policy](#).