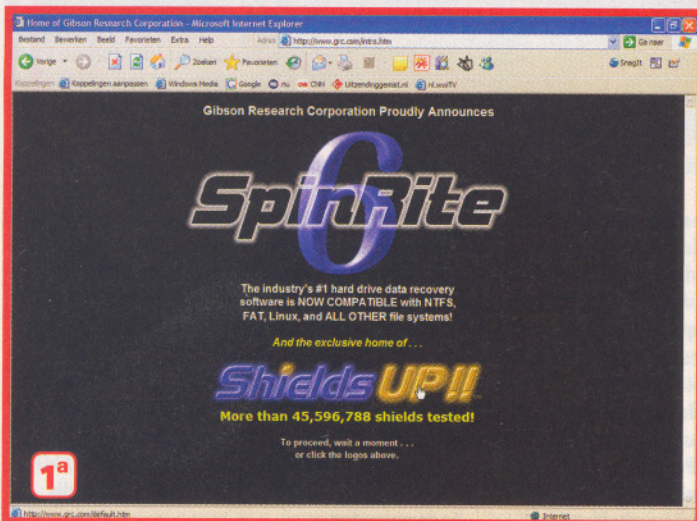


# Stap voor stap workshop

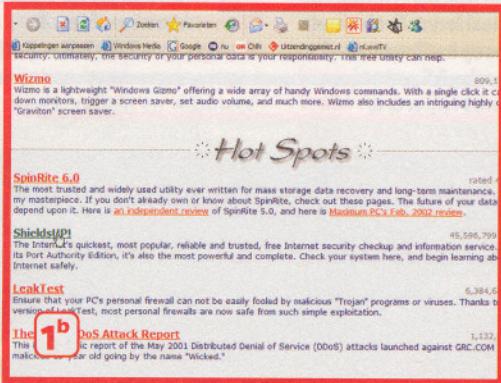
# Zijn mijn pc-poorten echt

De kans is groot dat u op uw pc een veiligheidspakket hebt geïnstalleerd, bestaande uit in ieder geval een virusscanner en een firewall. Of dat er in uw internetmodem/router een firewall zit. Maar hoe weet u nou of deze naar behoren werkt?

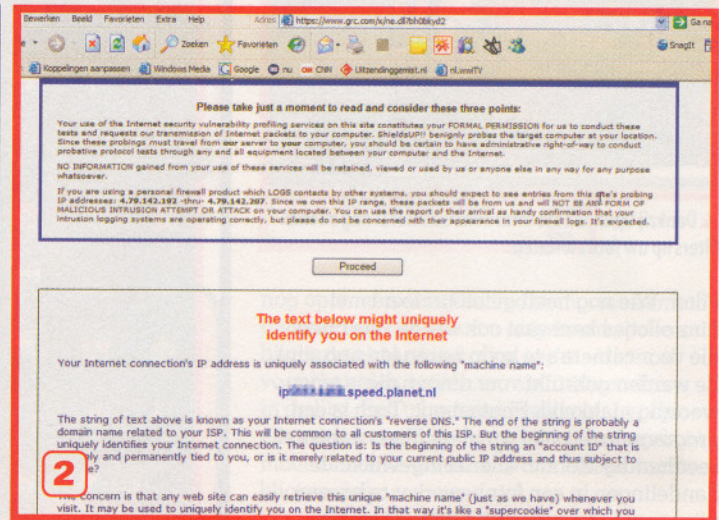
Er bestaan verschillende websites die op uw verzoek uw pc aanvallen en controleren of er wellicht onverhoopt deuren openstaan. In vaktaal heten deze pc-deuren 'poorten'. De ideale firewall zorgt ervoor dat al deze poorten hermetisch gesloten zijn. Pas dan kunt u met een gerust gevoel uw pc op het internet loslaten. Een van de bekendste sites waar u geheel gratis uw firewall kunt testen is die van Gibson Research.



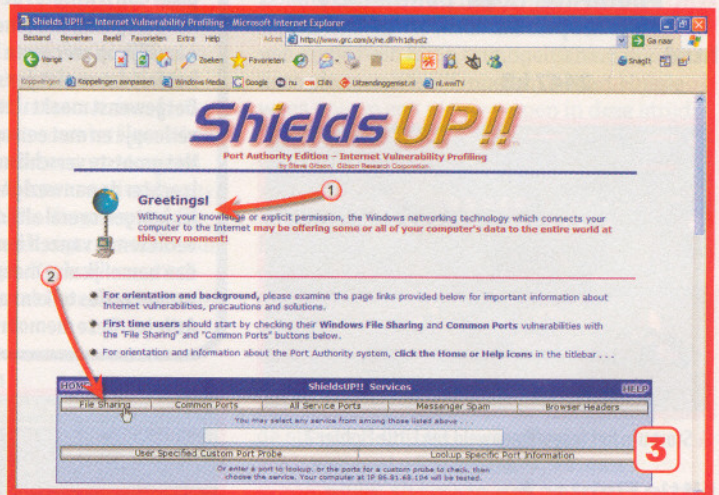
**1 START** uw browser en ga naar [www.grc.com](http://www.grc.com). Klik aldaar op het logo ShieldsUP!! In de nieuw geopende pagina scrollt u dan een flink eind naar beneden tot u de link ShieldsUP!! tegenkomt. Klik hierop om naar de testpagina's te gaan.



**2 IN HET VENSTER** waarin u gemeld wordt dat u pagina's via een beveiligde verbinding gaat weergeven klikt u op OK. Doe dat bij alle soortgelijke vensters die in het verloop van deze workshop verschijnen. Scroll weer wat naar beneden in de pagina. Daar vindt u ten eerste een knop Proceed (= doorgaan), maar ook daar vlak onder een link. Meestal bestaat deze uit een nummer en de naam van uw provider of simpelweg een rijtje getallen gescheiden door een punt. Hebt u een breedband internetverbinding, dan is dit het unieke adres van uw pc. Helaas betekent dit ook dat websites ongevraagd kunnen zien hoe vaak u hen bezoekt en eventueel uw hele surfgedrag in kaart brengen. Daar kan een firewall niets aan veranderen. Wat dat betreft bent u beter af als u nog over een antieke inbelverbinding beschikt: telkens als u inbelt krijgt uw pc een vers

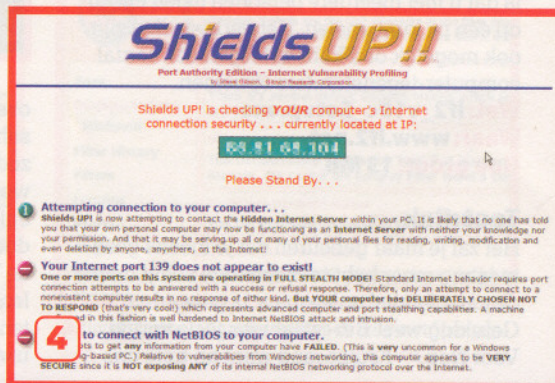


adres toegewezen. Inbelverbindingen zijn dus veel moeilijker te traceren dan breedbandverbindingen. Een reden te meer om te controleren of uw firewall naar behoren werkt.



**3 KLIK OP** Proceed, waarna u eigenlijk meteen al een beetje kunt aanvoelen in welke richting de test zal uitvallen. Als er helemaal bovenaan de pagina onder Greetings (groeten) gegevens staan die zo van uw pc afkomstig zijn, werkt uw firewall niet of niet goed. In ons geval (1) wordt er niets getoond en dat is precies wat we willen. De eerste vuurdoop vindt plaats na een klik op de knop File Sharing (2). Klik op deze knop om de test te starten.

**4 U BEHOORT** na de kortdurende test twee mintekens in een rood balletje te zien staan. Alleen dan is de aanval niet gelukt en bleek het niet



**4** to connect with NetBIOS to your computer. ShieldsUP!! is now attempting to connect to the Hidden Internet Server within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an Internet Server with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!

**4** Your Internet port 139 does not appear to exist! One or more parts on this system are operating in FULL STEALTH MODE! Standard Internet behavior requires port connection attempts to be answered with a success or refusal response. Therefore, only an attempt to connect to a non-existent computer results in no response of either kind. But YOUR computer has DELIBERATELY CHOSEN NOT TO RESPOND (that's very cool) which represents advanced computer and port stealth capabilities. A machine in this fashion is well hardened to Internet NetBIOS attack and intrusion.

**4** to connect with NetBIOS to your computer. ShieldsUP!! is now attempting to connect to the Hidden Internet Server within your PC. It is likely that no one has told you that your own personal computer may now be functioning as an Internet Server with neither your knowledge nor your permission. And that it may be serving up all or many of your personal files for reading, writing, modification and even deletion by anyone, anywhere, on the Internet!

# ht dicht?

mogelijk om informatie aan uw pc te ontfutselen. Blijkt er wél informatie gelekt te zijn, dan staat uw firewall hoogstwaarschijnlijk niet ingeschakeld (zie ook kader). Controleer in dat geval het firewall-onderdeel van uw beveiligingssoftware en kijk of het beveiligingsniveau op het hoogst mogelijke niveau is ingesteld. Deze instellingen werken per programma anders, maar de handleiding zal altijd uitkomst bieden.

Is being profiled. Please stand by. . .

Total elapsed testing time: 5.303 seconde

**PASSED** **TruStealth Analysis** **PASSED**

Your system has achieved a perfect "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

Port	Service	Status	Security Implications
0	<nul>	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
21	FTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
22	SSH	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
23	Telnet	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
25	SMTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
29	Finger	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
80	HTTP	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
110	POP3	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!
113	IDENT	Stealth	There is NO EVIDENCE WHATSOEVER that a port (or even any computer) exists at this IP address!

**5<sup>a</sup>**

**5** **SCROLL** weer wat naar beneden op de pagina en klik op de knop Common Ports. Als het goed is, krijgt u na even wachten een rijtje te zien met alleen maar groen gekleurde blokjes en – eveneens in het groen – de tekst PASSED. Dat betekent dat uw firewall uw pc volledig heeft afgeschermd van internet. Precies wat we willen, want het betekent dat niemand uw pc zelfs maar kan detecteren! Om de ultieme test uit te voeren, scrollt u weer even naar onderaan de pagina en klikt u op All Service Ports. Deze test duurt wat langer, maar uw pc wordt dan ook werkelijk op alle fronten aangevallen. Uw firewall werkt alleen dan goed wanneer alle tests geen enkel blokje informatie ongemerkt de buitenwereld insturen. ■

Is being carefully examined:

The port number of any location on the grid above may be determined by floating your mouse over the square. Most web browsers will display a pop-up window to identify the port. Otherwise, see the URL display at the bottom of your browser.

Legend:  Down  Closed  Stealth

Your elapsed testing time: 45.154 seconde

**PASSED** **TruStealth Analysis** **PASSED**

has achieved a perfect "TruStealth" rating. **Not a single packet** — solicited or otherwise — was received from your system as a result of our security probing tests. Your system ignored and refused to reply to repeated Pings (ICMP Echo Requests). From the standpoint of the passing probes of any hacker, this machine does not exist on the Internet. Some questionable personal security systems expose their users by "counter-probe the prober", thus revealing themselves. But your system wisely remained silent in every way. Very nice.

## Firewalls en firewalls

Wanneer u géén firewall in uw internetmodem- of router hebt geactiveerd moet u altijd een firewall op uw pc installeren. Dat kan desnoods de standaard in Windows ingebouwde firewall zijn, deze activeert u door in het Configuratiescherm in Klassieke weergave op het pictogram Windows Firewall te dubbelklikken. Kies in het daarop geopende venster de optie Ingeschakeld en klik op OK. Schakel de Windows Firewall echter niet in als u al andere firewallsoftware op uw pc hebt geïnstalleerd, dit om conflicten te voorkomen.

Ook als u wél over een in uw modem of router ingebouwde (hardware) firewall beschikt, is het toch zeer verstandig ook een exemplaar op uw pc te installeren. De softwarematige firewall controleert namelijk ook uitgaande verbindingen zodat u precies kunt aangeven welke programma's toegang krijgen tot internet en welke niet.