C'est quoi un port* ?

Le mot ***port*** est au fait l'abréviation de ***port de communication***. Au fait, le PC utilise **65535** de ces ***ports***. Ces ***ports*** (**portes**) seront utilisés selon les besoins (commandes) du processeur.
Exemple : Si vous utilisez la commande ***Imprimer***, le ***port 139*** servira pour cette action.

Chacun de ces ***65 535 ports*** a une signification exacte (**normalisé**) et ils sont pareils pour chaque PC !

Vous pouvez accéder à une liste complète de ces ports et de leur signification aux adresses URL suivantes :

http://www.iana.org/assignments/port-numbers

http://www.webwizardbiz.com/tutorials/firewalls/

L'assignation des ports est gérée par l'I.A.N.A. (Internet Assigned Numbers Authority) : http://www.iana.org/

Ces **65535 ports** peuvent être regroupés dans **trois catégories** :

1. Les ports bien connus **0 à 1023**.
2. Les ports registrés de **1024 à 49151**
3. Les ports dynamiques et ports privés de **49152 à 65535**

Essayez de visualiser ces *ports* (portes) comme faisant partie d'une maison, une maison avec 65535 portes.
Au fait, un immeuble administratif avec 65535 collaborateurs dont chaque bureau (porte) est assigné un numéro de 1 à 65535.

Ces portes (**ports**) doivent bien entendu être protégés, sinon un intrus peut avoir accès pour voler et ou détruire du matériel y stocké !

Dans un immeuble ou une maison nous prenons recours à un système anti-intrusion (**système d'alarme**).
Pour le PC nous utilisons un ***Firewall*** (**pare-feu**). Le ***Firewall*** (**pare-feu**) protège nos ***ports de communication***, il les surveille et nous avertit quand il y a une attente à notre sécurité ! Le ***Firewall*** peut être visualisé comme un portier contrôlant le **trafic non désiré entrant et sortant**.

*Veuillez noter que le ***Firewall*** intégré de ***WINDOWS XP*** ne contrôle que le trafic entrant et pas le trafic sortant ! (19.12.2004.)*

Il existe deux sortes de ***Firewall*** :

1. **Desktop Firewall** (logiciel / programme)
2. **Hardware Firewall** (Matériel physique ou intégré dans un **ROUTER**)

Pour les privés, les ***Desktop Firewall*** (logiciels / programmes) sont utilisés. Ces ***Desktop Firewall*** existent même en version gratuite (**Freeware**) dont notamment ***ZONEALARM*** du fabricant **ZONELABS** : **http://www.zonelabs.com**

Comment installer et configurer ZONEALARM ?

Vous trouverez à l'adresse URL suivante un très bon tutoriel :

http://www.cases.public.lu/publications/dossiers/firewall/Zonealarm/ZA3/index.html

Comment savoir maintenant si les ports de mon PC sont bien sécurisés ?

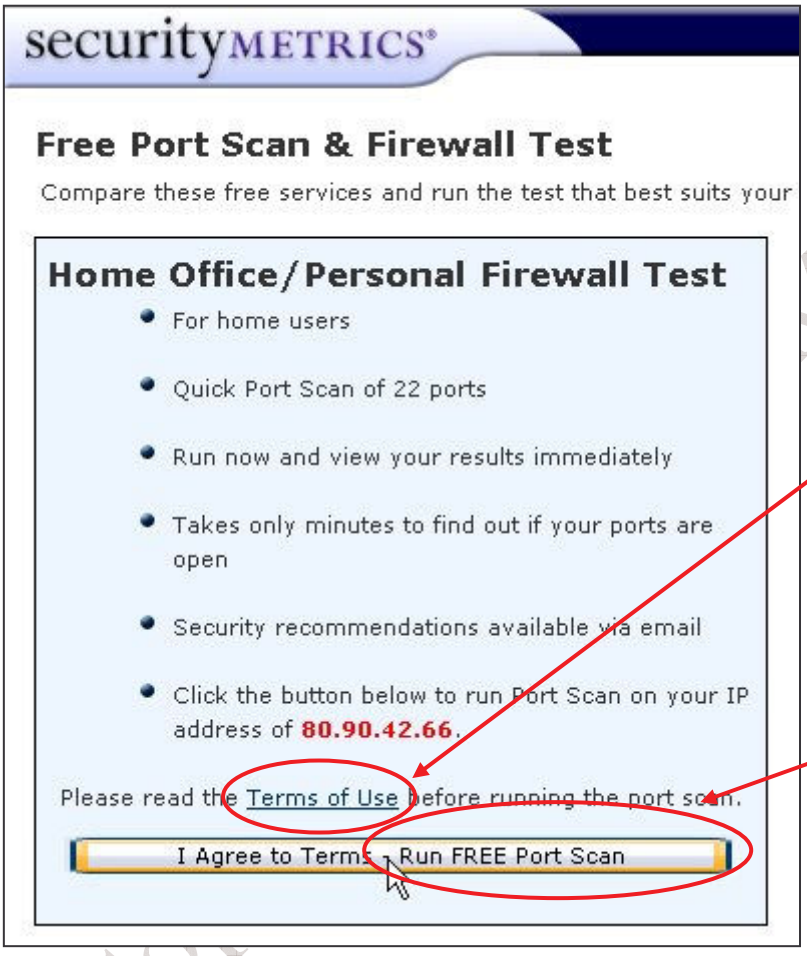
Il existe des ***services gratuits*** (pour usage non commercial) sur Internet ***où nous pouvons tester*** en ligne (online) la vulnérabilité des ****ports* de notre PC, sans avoir besoin de connaissances techniques, accessible à tout le monde !***

Un de ces services est ***SECURITYMETRICS*** http://www.securitymetrics.com
Ce service est en anglais.

Un autre bon service gratuit est *PORT-SCAN* http://www.port-scan.de
Ce service est en allemand.

Dans notre exemple (Case study) nous utiliserons le service gratuit de ***Securitimetrics***.

Pour ceci, ouvrez dans votre navigateur (**Browser**) notre *Internet Monitor*, http://www.internetmonitor.lu et cliquez sur le lien d'image ***Free Port Scan***.



Ceci nous ramène au site de ***Securitymetrics*** où nous pouvons maintenant tester gratuitement la vulnérabilité de nos ports.

Veuillez d'abord lire les termes d'utilisation du service en cliquant sur ***Terms of use***.

Après cette action vous acceptez les conditions d'utilisation en cliquant sur le bouton ***Run FREE Port Scan***

La page suivante s'ouvrira.

securityMETRICS®

Products | Test Results | Register | Security Info | Search

Port Scan Results

Please wait. A Port Scan requires from 5 seconds to 3 minutes to complete.Your screen will automatically scroll as your port scan results are displayed. This free port scan will test 22 of the 500 most commonly used communication ports on your computer/server.

Automatic Connection Analyzer

Internet **attackers** and worms **can directly probe** your computer for open ports and vulnerabilities, because your computer (**80.90.42.66**) is connected directly to the Internet.

There are thousands of ports on your computer that may pose serious security risks. Every program that accesses the Internet uses one of your open ports. New vulnerabilities are discovered in these programs every day. (See our security bulletin for more details)

We recommend running a Desktop Check to thoroughly examine the security of your computer. The Desktop Check will analyze your computer for thousands of open ports and over 600 security vulnerabilities. Your Desktop Check report (see sample report) will provide instructions or recommendations to help you immediately close any unneeded open ports and to repair security vulnerabilities.

Ceci nous montre que nous sommes protégés.

Vous recevrez maintenant **21 alarmes** de votre firewall (pare-feu), dans notre cas nous utilisons ***ZONEALARM***.

Ces alarmes, nous les acquittons en cliquant sur le bouton ***OK***.

N.B. : Ce TEST n'effectue l'analyse que de 22 PORTS du PC, mais les plus importants et les plus vulnérables !

Les tests étant terminés après 1,5 – 3 minutes, la figure suivante devrait être présente.

Port Scan Results for: 80.90.42.66

Program	Port	Status	Explanation
FTP	21	Stealth	File Transfer Protocol (FTP) allows users to transfer files to other computers over the Internet. A poorly configured FTP server allows hackers to copy your files, install trojan applications on your computer or obtain unauthorized remote command prompt access to your computer.
SSH	22	Stealth	Secure Shell (SSH) uses encryption to secure information sent over a network. While it typically improves security there are numerous problems with older versions of SSH which may allow brute force attacks.
Telnet	23	Stealth	Telnet allows a remote user to access your computer and perform commands. It is suspectible to brute force attacks and clear text password sniffing. A computer is misconfigured if this port is open. Use SSH instead.
SMTP	25	Stealth	SMTP is used to send email. There are numerous vulnerabilities with SMTP such as unauthorized hard disk file access, username verification or SPAM email redirection.
DNS	53	Stealth	Domain Name Services are used to tell other computers what your IP address is. There are several exploits associated with this service.
Finger	79	Stealth	Finger provides information such as usernames and usage information. Turn this service off or block this port to stop others from gaining valuable system information.
HTTP	80	Stealth	World Wide Web services allow you to publish web pages to the Internet. There are hundreds of severe security vulnerabilities associated with this service. Keep your WWW server software updated.
POP3	110	Stealth	Post Office Protocol(POP) software downloads email. Hackers may use weaknesses in POP to intercept your email, create fictitious mail accounts or gain remote access to your computer.
NetBIOS	139	Stealth	NetBIOS is used by Microsoft Windows and some UNIX/Linux programs to share files. If your hard disk is shared improperly (write access to everyone without authentication) you may be giving the world access to your hard disk. (Trojan files can be copied to your computer.) Make sure this port is closed and your hard drive shares are configured properly.
SNMP	161	Stealth	Simple Network Management Protocol (SNMP) port may allow a hacker to obtain information about your computer. There are also security vulnerabilities associated with this port. You should turn off this service if you don't need it.
SSL	443	Stealth	HTTP servers use Secure Sockets Layer (SSL) to encrypt data from web browsers. There are hundreds of severe security vulnerabilities associated with this service. Keep your WWW server software updated.
MS DS	445	Stealth	Microsoft Directory Services is used by Microsoft Networks for security authentication. Typically this port should not be exposed to the Internet.
Socks Proxy	1080	Stealth	An unsecured SOCKS Proxy may disqualify you from IRC server access. Make sure this port is closed.
KaZaA	1214	Stealth	KaZaA is a popular peer-to-peer file-sharing program with many known vulnerabilities and at least one known worm (Benjamin) targeting it.
UPnP	5000	Stealth	Universal Plug and Play allows your computer to automatically integrate with other network devices. There are known security vulnerabilities associated with this service.
HTTP Proxy	8080	Stealth	HTTP Proxy provides a way for a hacker to pretend to be your computer. Others who may have been hacked may see your computer address and want you to justify why you hacked them.

Trojan Port Scan Results for: 80.90.42.66

Program	Port	Status	Trojans Common to Port
Trojan	6776	Stealth	2000 Cracks, BackDoor-G, SubSeven, VP Killer
Trojan	7000	Stealth	Exploit Translation Server, Kazimas, Remote Grab, SubSeven, SubSeven 2.1 Gold
Trojan	12345	Stealth	Ashley, Cron/Crontab, Fat Bitch trojan, GabanBus, icmp_client.c, icmp_pipe.c, Mypic, NetBus, NetBus Toy, NetBus worm, Pie Bill Gates, Whack Job, X-bill
Trojan	20034	Stealth	NetBus 2.0 Pro, NetBus 2.0 Pro Hidden, NetRex, Whack Job
Trojan	27374	Stealth	Bad Blood, Ramen, Seeker, SubSeven, SubSeven 2.1 Gold, Subseven 2.1.4 DefCon 8, SubSeven Muie, Ttfloader
Trojan	31337	Stealth	Back Fire, Back Orifice 1.20 patches, Back Orifice (Lm), Back Orifice Russian, Baron Night, Beeone, BO client, BO Facil, BO spy, BO2, Cron/Crontab, Freak88, Freak2k, icmp_pipe.c, Sockdmini

Si vous recevez comme résultat l'indication *Stealth*, votre PC est invisible sur Internet et les chances que vous soyez attaqués sont minimes.

Si par contre le test vous montre les indications ***Open*** et ou ***Closed***, soit que vous n'ayez pas installé de ***Firewall*** (pare-feu) ou bien, que celui-ci est mal réglé !

Le cas où vous ne disposez pas de ***Firewall*** (pare-feu), je peux vous conseiller ***ZONEALARM*** de ZONELABS : http://www.zonelabs.com

Ce **pare-feu** (**Firewall**) est multi langues et existe aussi en **version gratuite**.
Un très bon tutoriel peut être trouvé à l'URL suivante :

http://www.cases.public.lu/publications/dossiers/firewall/Zonealarm/ZA3/index.html