Comparaison de scanners et prise d'empreintes d'un poste Win2k pro

1 Introduction

Dans un réseau informatique, divers utilisateurs (normal, *superuser*, administrateur, …) accèdent à des ressources (fichiers, imprimante, …) et services (*web*, ftp, …) partagés.
Chaque système informatique (poste client, serveur, routeur, …) exige une configuration spécifique qu'il convient de définir avec précision et de contrôler périodiquement ; surtout quand ces systèmes sont connectés à *internet*.

Le principe de sécurité "Tout interdire et accepter spécifiquement chaque cas" n'est malheureusement pas respecté lors d'une installation par défaut de Windows 2000 (facilité d'utilisation, compatibilité NetBIOS, …)

Le but de cette étude consiste à connaître les vulnérabilités potentielles de Windows 2000 et de les éliminer.
Divers tests de pénétration seront ainsi réalisés afin de disposer d'éléments de comparaison simulant l'action d'un *hacker* effectuant des balayages *(scanning)* avec prises d'empreintes.

Cette étude doit également démontrer le gain en sécurité obtenu dans un réseau composé exclusivement de systèmes Windows 2000 dépourvus des compatibilités NT Lan Manager, NetBIOS, …

2 Objectifs

- Etablir un comparatif entre différents scanners
- Effectuer des testes de *scanning* sur différentes configurations de Windows 2000

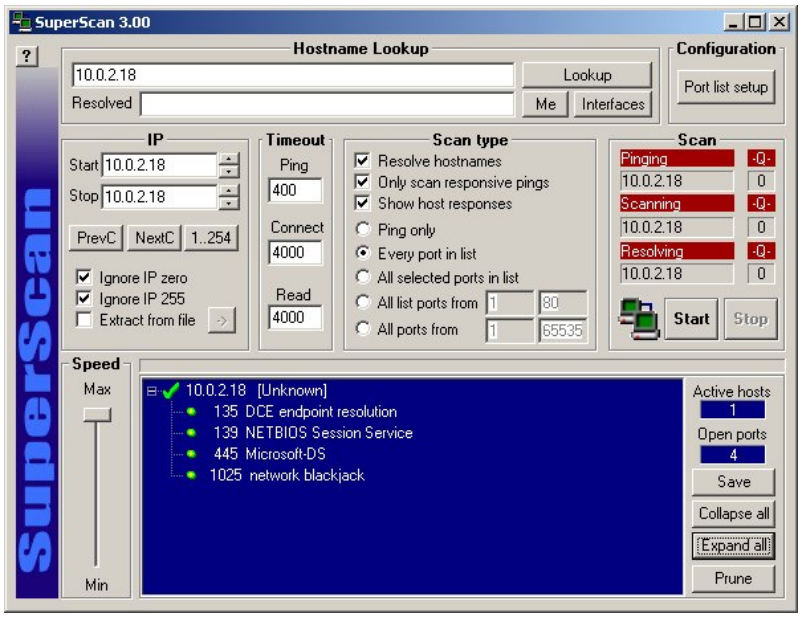
3 Logiciels utilisés

Plusieurs logiciels permettant de *scanner* des machines connectées à un réseau sont disponibles. Nous avons testé certain d'entre eux afin de choisir les mieux adaptés pour nos essais. Les logiciels testés sont les suivants :

- SuperScan
- Fscan
- NmapNT
- LANguard

3.1 **SuperScan** (v3.0)

SuperScan est un logiciel gratuit disponible sur le site http://www.webattack.com/get/superscan.shtml. Son utilisation est simple grâce à une interface graphique.



Il permet d'identifier les machines active dans une plage d'adresses IP définit par l'utilisateur et de détecter les ports ouverts sur ces machines. Pour cela, il utilise des requêtes ICMP (ping) afin d'identifier les machines présentes sur le réseau. Ensuite, il effectue des requêtes TCP sur les machines actives afin de détecter les ports ouverts. Sur certain réseau, les paquets ICMP ECHO req (ping) sont bloqués à l'aide d'un *firewall*. Pour cela, il est possible d'effectuer un *scan* des ports à des adresses ne répondant pas au *ping*.

Requête sur un port TCP ouvert	Requête sur un port TCP fermé
→ ICMP ECHO req	→ ICMP ECHO req
← ICMP ECHO reply	← ICMP ECHO reply
→ TCP SYN	→ TCP SYN
← TCP ACK,SYN	← TCP ACK,RST
→ TCP ACK	
→ TCP ACK,FIN	
← TCP ACK	
← TCP ACK,FIN	
→ TCP ACK	

La définition des ports à *scanner* se fait soit par une sélection dans une liste, soit par la définition d'une plage de ports.

Autres options :

- résolution d'adresse IP en *hostname* (129.194.184.80 → www.td.unige.ch)
- réglages des *timouts* (*ping, connect, read*)
- réglage de la vitesse de *scan* (nombre de requêtes envoyer en parallèle)

Les points forts de ce programme sont :

- la simplicité d'utilisation (interface graphique)
- la rapidité (envoie des requêtes à plusieurs ports en même temps)

Les points faibles sont :

- ne permet pas de *scanner* les ports UDP

3.2 **Fscan** (v1.12)

Fscan est un petit exécutable fonctionnant en ligne de commande. Il est disponible gratuitement sur le site http://www.crackinguniversity2000.it/Hack2/fscan112.zip. Ce programme, apparemment simple, offre beaucoup de possibilités.

```
FScan [-abefhqnv?] [-cditz <n>] [-flo <file>] [-pu <n>[,<n>-<n>]] IP[,IP-IP]

 -?/-h - shows this help text
 -a    - append to output file (used in conjunction with -o option)
 -b    - get port banners
 -c    - timeout for connection attempts (ms)
 -d    - delay between scans (ms)
 -e    - resolve IP addresses to hostnames
 -f    - read IPs from file (compatible with output from -o)
 -i    - bind to given local port
 -l    - port list file - enclose name in quotes if it contains spaces
 -n    - no port scanning - only pinging (unless you use -q)
 -o    - output file - enclose name in quotes if it contains spaces
 -p    - TCP port(s) to scan (a comma separated list of ports/ranges)
 -q    - quiet mode, do not ping host before scan
 -r    - randomize port order
 -t    - timeout for pings (ms)
 -u    - UDP port(s) to scan (a comma separated list of ports/ranges)
 -v    - verbose mode
 -z    - maximum simultaneous threads to use for scanning
```

En effet il permet de *scanner* les ports TCP et UDP sur une plage d'adresses définit par l'utilisateur. Les ports à *scanner* peuvent êtres définis soit directement dans la commande, soit dans un fichier créé par l'utilisateur.

Scan du port TCP 135 sur une machine se trouvant à l'adresse IP 10.0.2.18 : Fscan –p 135 10.0.2.18

Requête sur un port TCP ouvert	Requête sur un port TCP fermé
→ ICMP ECHO req	→ ICMP ECHO req
← ICMP ECHO reply	← ICMP ECHO reply
→ TCP SYN	→ TCP SYN
← TCP ACK,SYN	← TCP ACK,RST
→ TCP ACK	
→ TCP ACK,FIN	
← TCP ACK	
← TCP ACK,FIN	
→ TCP ACK	

Scan du port UDP 135 sur une machine se trouvant à l'adresse IP 10.0.2.18 : Fscan –u 135 10.0.2.18

Requête sur un port UDP ouvert	Requête sur un port UDP fermé
→ ICMP ECHO req	→ ICMP ECHO req
← ICMP ECHO reply	← ICMP ECHO reply
→ UDP	→ TCP UDP
	← TCP ICMP dest unreachable

Les paquets ICMP ECHO peuvent être supprimés grâce à l'option –q (*quiet mode*) afin de laisser moins de traces sur des machines (*sniffer*) à l'écoute des ping.

Autres options :
- résolution d'adresse IP en *hostname*
- réglages des *timouts*

Les points forts de ce programme sont :
- la rapidité (envoie des requêtes à plusieurs ports en même temps)
- permet de *scanner* les ports TCP et UDP

Les points faibles sont :
- Interface non graphique

3.3 **NmapNT** (v2.53)

Ce programme est un *scanner* s'exécutant en ligne de commande. Il est disponible gratuitement sur le site http://eeye.com/html/Research/Tools/nmapnt.html. L'installation de WinPcap est nécessaire au fonctionnement de NmapNT (http://netgroup-serv.polito.it/winpcap/install/default.htm).

```
nmap V. 2.53 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
  -sT TCP connect() port scan (default)
* -sS TCP SYN stealth port scan (best all-around TCP scan)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan.  Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended.  Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oM <logfile> Output normal/machine parsable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

NmapNT permet de *scanner* les ports TCP et UDP. Il offre un nombre impressionnant de méthode pour *scanner* les ports TCP afin de pouvoir pénétrer des réseaux protégés par d'éventuels *firewalls*. Les ports à *scanner* peuvent êtres définis soit directement dans la commande, soit dans un fichier créé par l'utilisateur ou encore, en utilisant une liste prédéfinit des ports les plus intéressant (option -F). Cette liste se trouve dans le fichier « nmap-services ».

Scan du port TCP 135 sur une machine à l'adresse IP 10.0.2.18 : nmapnt –sT –p 135 10.0.2.18

Requête sur un port TCP ouvert	Requête sur un port TCP fermé
→ ICMP ECHO req	→ ICMP ECHO req
→ TCP ACK	→ TCP ACK
← ICMP ECHO reply	← ICMP ECHO reply
← TCP RST	← TCP RST
→ TCP SYN	→ TCP SYN
← TCP ACK,SYN	← TCP ACK,RST
→ TCP ACK	
→ TCP RST	

On remarque deux différences par rapport aux *scanners* précédent :

- NmapNT utilise, en plus du ping, un paquet TCP ACK permettant de détecter la présence d'une machine, même si les paquets ICMP ECHO sont bloqués par un *firewall*. En effet, certains *firewalls* laissent passer des paquets TCP ACK afin de permettre aux utilisateurs (protégés par celui-ci) d'accéder à certains services (http, …). Si un paquet TCP RST est reçu par le *scanner*, il en déduit qu'une machine est présente à l'adresse testée.

- Lorsque NmapNT a détecté qu'un port est ouvert, il envoie TCP RST afin d'éviter la séquence TCP ACK,FIN … . Cela permet un gain en temps sur chaque port actif et laisse moins de traces dans les fichiers log de la cible.

L'option suivante permet de réaliser un *scan* « mi-ouvert » sur le port TCP 135, car la connexion TCP n'est pas établit complètement. L'avantage de cette méthode est de ne pas laisser de trace (la plupart du temps) sur la machine cible : nmapnt –sS –p 135 10.0.2.18

Requête sur un port TCP ouvert	Requête sur un port TCP fermé
→ ICMP ECHO req	→ ICMP ECHO req
→ TCP ACK	→ TCP ACK
← ICMP ECHO reply	← ICMP ECHO reply
← TCP RST	← TCP RST
→ TCP SYN	→ TCP SYN
← TCP ACK,SYN	← TCP ACK,RST
→ TCP RST	

Les 3 options ci-dessous permettent de traverser les *firewalls* bloquant les paquets TCP SYN. Normalement, les ports fermés doivent répondre par un paquet TCP RST et ceux qui sont ouverts ne doivent pas prendre en compte ces paquets. Malheureusement cela ne fonctionne pas sur les machines Microsoft, car un paquet TCP RST est systématiquement retourné, quel que soit l'état du port.

Option FIN : nmapnt –sF –p 135 10.0.2.18

Requête sur un port TCP ouvert	Requête sur un port TCP fermé
→ ICMP ECHO req	→ ICMP ECHO req
→ TCP ACK	→ TCP ACK
← ICMP ECHO reply	← ICMP ECHO reply
← TCP RST	← TCP RST
→ TCP FIN	→ TCP FIN
	← TCP ACK,RST

Option Xmas : nmapnt –sX –p 135 10.0.2.18

Requête sur un port TCP ouvert	Requête sur un port TCP fermé
→ ICMP ECHO req	→ ICMP ECHO req
→ TCP ACK	→ TCP ACK
← ICMP ECHO reply	← ICMP ECHO reply
← TCP RST	← TCP RST
→ TCP URG,PSH,FIN	→ TCP URG,PSH,URG
	← TCP ACK,RST

Option *Null Scan* : nmapnt –sN –p 135 10.0.2.18

Requête sur un port TCP ouvert	Requête sur un port TCP fermé
→ ICMP ECHO req	→ ICMP ECHO req
→ TCP ACK	→ TCP ACK
← ICMP ECHO reply	← ICMP ECHO reply
← TCP RST	← TCP RST
→ TCP -	→ TCP -
	← TCP ACK,RST

Scan du port UDP 135 sur une machine à l'adresse IP 10.0.2.18 : nmapnt –sU -p 135 10.0.2.18

Requête sur un port UDP ouvert	Requête sur un port UDP fermé
→ ICMP ECHO req	→ ICMP ECHO req
→ TCP ACK	→ TCP ACK
← ICMP ECHO reply	← ICMP ECHO reply
← TCP RST	← TCP RST
→ UDP	→ TCP UDP
	← TCP ICMP dest unreachable

NmapNT effectue le *scan* des ports UDP de la même manière que Fscan.

Les paquets ICMP ECHO req et TCP ACK peuvent être supprimer en utilisant l'option –P0.

Autres options :

- Possibilité de prendre une empreinte TCP/IP (*fingerprint*) permettant de déterminer le type de système d'exploitation (Windows, Linux, …).
- Permet d'envoyer des leurres (paquet avec adresses IP source modifiée) afin de rendre difficile la localisation de la source d'attaque.
- possibilité d'utiliser un serveur FTP *proxy* pour effectuer un *scan*

Les points forts de ce programme sont :

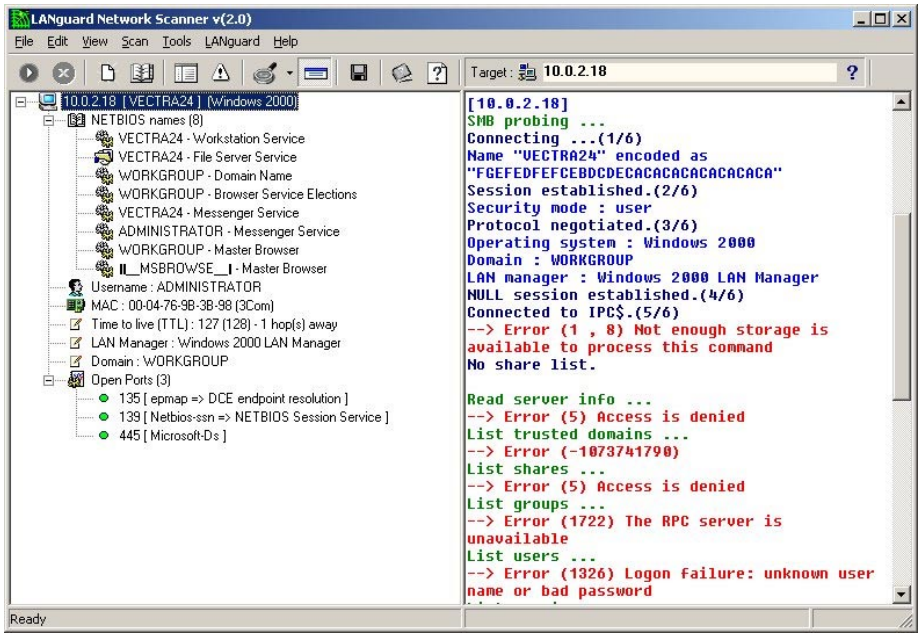
- la rapidité (envoie des requêtes à plusieurs ports en même temps)
- permet de *scanner* les ports TCP et UDP
- permet de passer à travers certain *firewall*
- permet de rendre plus difficile la localisation de la source du *scan*

Les points faibles sont :

- Lors du *scan* des ports UDP, NmapNT trouve des ports ouverts alors qu'ils sont fermés (option -sU) et inversement, il trouve des ports fermés alors qu'ils sont ouverts (option -F). Cela ne se produit pas avec Fscan.

3.4 **LANguard** (v2.0)

LANguard est un logiciel qui est bien plus qu'un simple *scanner* de ports. En effet, il permet d'obtenir des informations sur certain point pouvant mettre en danger la sécurité d'un système Windows. Il est disponible gratuitement pour un usage personnel sur le site http://www.gfi.com/languard/lanscan.htm.



Ce programme permet, comme les *scanners* précédents, d'effectuer un *scan* des ports TCP d'une machine active. Les ports à *scanners* sont définit dans une liste modifiable par l'utilisateur.

Requête sur un port TCP ouvert	Requête sur un port TCP fermé
→ ICMP ECHO req	→ ICMP ECHO req
← ICMP ECHO reply	← ICMP ECHO reply
→ TCP SYN	→ TCP SYN
← TCP ACK,SYN	← TCP ACK,RST
→ TCP ACK	
→ TCP ACK,FIN	
← TCP ACK	
← TCP ACK,FIN	
→ TCP ACK	

De plus, il se sert des ports NetBios Name Service (UDP/137), NetBios Session Service (TCP/139), SNMP (UDP/161) et Microsoft-DS (TCP/445), pour obtenir les informations suivante sur des systèmes Windows :

- Nom de la machine (Vectra23)
- Nom du domaine de la machine
- Version du système d'exploitation (Windows 2000 Service Pack 2)
- Username de l'utilisateur de la machine
- Adresse MAC de la machine
- …

Lors du scan, s'il y a une équivalence entre les *logins* (*username, password, domain*) du poste client et de la machine cible, LANguard possède suffisamment de droits pour obtenir des informations sur les groupes d'utilisateurs, les services, les partages, … de cette machine. Cela fonctionne aussi sur un serveur si le client possède un compte utilisateurs sur celui-ci. Ce programme est donc très utile pour récolter des informations sur une machine distante. Mais on peut aussi l'utiliser sur sont propre système (en « local ») pour évaluer les points vulnérables de sa machine.

Autres options :

- résolution d'adresse IP en *hostname*
- fonction *traceroute*
- recherche de mots de passe (pour partage Windows 9x/ME)

Les points forts de ce programme sont :

- exploite NetBios pour obtenir des informations
- indication des points vulnérable d'une machine
- présentation des résultats claire et lisible

Les points faibles sont :

- ne permet pas de *scanner* les ports UDP

Tableau récapitulatif

Le tableau ci-dessous résume les principales caractéristiques des programmes décrit précédemment.

	TCP	UDP	NetBios	Détection OS	Scan simultané des ports	Interface graphique	WinPcap
SuperScan	X	-	-	-	X	X	-
Fscan	X	X	-	-	X	-	-
NmapNT	X	X*	-	X	X	-	X
LANguard	X	-	X	X	-	X	-

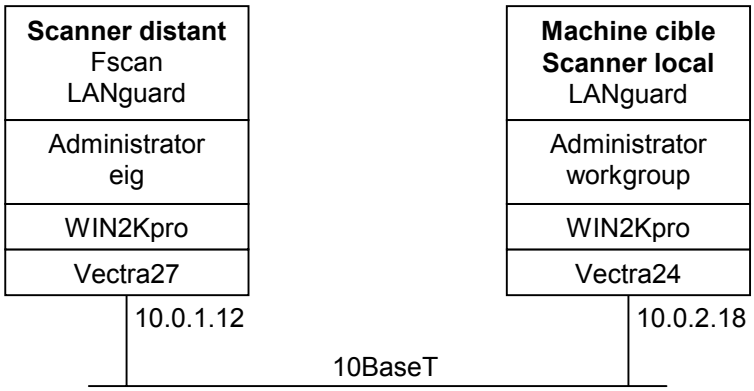
(* Des erreurs ont été constatées lors des scans UDP de NmapNT (voir ci-dessus))

Comme on le voit, chaque *scanner* à ses avantages et ses inconvénients. C'est pourquoi les tests qui vont suivre sont faits à l'aide de plusieurs de ces programmes. Fscan est utilisé pour déterminer tous les ports TCP et UDP ouverts et LANguard est utilisé pour détecter des vulnérabilités spécifiques à Windows 2000.

4 Windows 2000 professional (anglais)

Les tests suivants ont pour but de détecter les ports ouverts, sur Windows 2000 professional, afin de mettre en évidence certaines vulnérabilités. Cela est fait en trois phases :

- *Scan* de la machine, cible avec Fscan, depuis la machine distante. Cela permet de détecter tous les ports TCP et UDP ouverts.
- *Scan* de la machine cible, avec LANguard, depuis la machine distante. Cela permet de voir les informations qu'il est possible de récolter sans avoir de droits sur la machine cible.
- *Scan* de la machine, cible avec LANguard, en « local ». Cela permet de voir les informations qu'il est possible de récolter en ayant des droits sur la machine cible.



Les tests sont réalisés dans l'ordre suivant :

- Test 1 : Configuration par défaut après l'installation de Win2Kpro
- Test 2 : Installation du *Service Pack 2* (SP2)
- Test 3 : Désactivation du partage de fichiers et d'imprimantes
- Test 4 : Désactivation de NetBIOS sur TCP/IP
- Test 5 : Association à un domaine

4.1 Test 1 : Configuration par défaut après l'installation de Win2Kpro

Dans ce premier test, nous allons voir quels sont les ports ouverts par défaut lors de l'installation de Windows 2000 professional.

Configuration lors de l'installation de Windows 2000 professional (MSDN cd 12) :

- Format HD :
  C : 20 Gbytes (System – NTFS)
  D : 18 Gbytes (Unformatted)
- Regional Setting :
  French (Switzerland)
- Personalize Your Software :
  Name : Vectra24
  Organization :
- Computer Name and Administrator Password
  Computer name : VECTRA24
  Administrator password :
- Networking Settings
  Typical settings
- Workgroup or Computer Domain
  No, this computer is not on a network, or is on a network without a domain
- User of This Computer
  Windows always assumes the following user has logged on this computer
  Username : Administrator
  Password :
- Configuration des TCP/IP
  IP address : 10.0.2.18
  Subnet mask : 255.255.255.0
  Default gateway : 10.0.2.1
  DNS server : 10.0.2.10

Configuration lors du test :

- Windows 2000 professional
- Partage de fichiers et d'imprimantes, activé (par défaut)
- NetBIOS sur TCP/IP, activé (par défaut)
- User : Administrator
- Domaine : workgroup

Le premier *scan* est effectué avec Fscan afin d'établir une liste de tous les ports TCP et UDP ouvert par défaut sur la machine cible. Grâce à la commande suivante, les 65535 ports TCP et UDP sont testés (**attention, cette opération dure environ 20 min**) :

```
Fscan -v -p 1-65535 -u 1-65535 10.0.2.18

Adding TCP port range 1-65535
Adding UDP port range 1-65535
Adding IP 10.0.2.18
Using 64 threads.
Connect timeout set to 600 ms.
Ping timeout set to 500 ms.
Scan delay set to 0 ms.

Scan started at Wed Feb 27 08:28:29 2002

Scanning TCP ports on 10.0.2.18
10.0.2.18         135/tcp
10.0.2.18         139/tcp
10.0.2.18         445/tcp
10.0.2.18        1025/tcp
Scanning UDP ports on 10.0.2.18
10.0.2.18         135/udp
10.0.2.18         137/udp
10.0.2.18         138/udp
10.0.2.18         445/udp
10.0.2.18         500/udp
10.0.2.18        1026/udp

Scan finished at Wed Feb 27 08:49:45 2002
Time taken: 131070 ports in 1275.815 secs (102.73 ports/sec)
```

Description des ports actifs :

- 135/tcp : Ce port est utilisé pour le Remote Procedure Call (RPC) qui est un service permettant à un programme sur une machine Windows (l'ordinateur du client) d'appeler les services d'un autre programme fonctionnant sur une machine Windows séparé (le serveur) dans un réseau distribué.

- 139/tcp : Ce port est utilisé pour les services de session NetBIOS qui font partie des protocoles NetBIOS sur TCP/IP (NetBT) et sont utilisés pour SMB (*Server Message Block*), le partage de fichiers et le partage d'imprimantes.

- 445/tcp : Ce port est utilisé pour le protocole SMB permettant le partage de fichiers sous Windows NT et Windows 2000. Windows 2000 permet d'exécuter SMB directement sur TCP/IP, sans couche supplémentaire NetBT.

- 1025/tcp : Port dynamique utiliser par Windows ou d'autres applications.

- 135/udp : Ce port est utilisé pour RPC (Remote Procedure call) → IPC$

- 137/udp : Ce port est utilisé par le protocole NetBIOS pour faire le lien entre un *Hostname* et une addresse IP sur un réseau NetBIOS-aware.

- 138/udp : NetBIOS Datagram Service

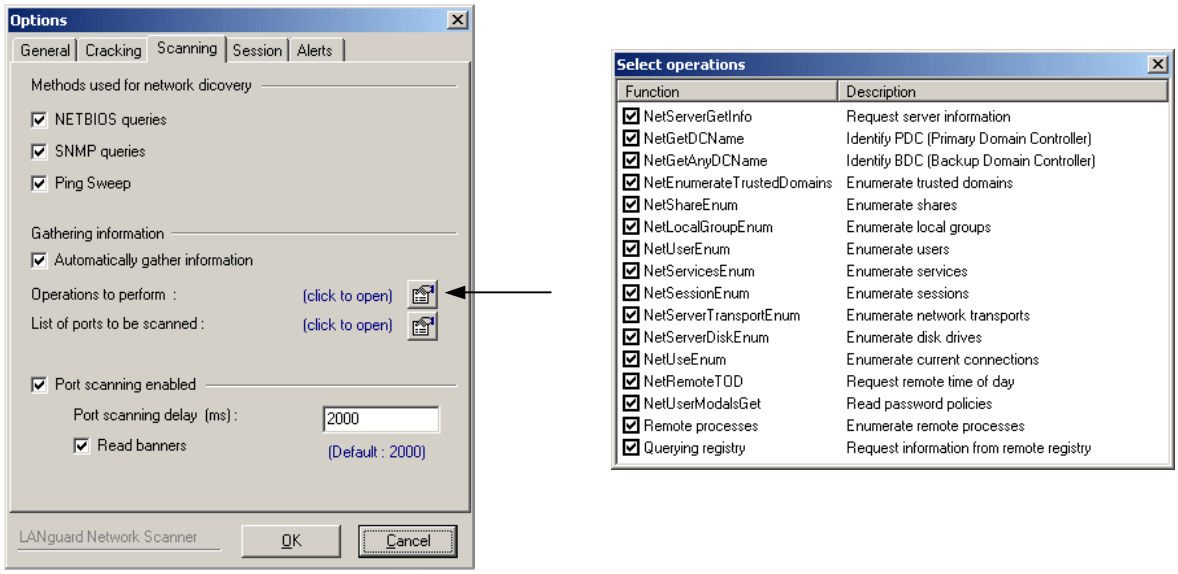
- 445/udp : Idem que 445/tcp

- 500/udp : ISAKMP ou IKE (for Windows 2000), IPSec

- 1026/udp : Port dynamique utiliser par Windows ou d'autres applications.

Remarques : Les ports plus grand que 1024 sont des ports dynamiques. Le port 1025 est le premier port dynamique utilisé par Windows, c'est pour cela qu'il est ouvert la plupart du temps.

Le deuxième *scan* est effectué avec LANguard, depuis la machine distante, sur la cible. Afin d'obtenir un maximum d'informations sur la machine cible, allez dans : ***Scan*** – ***Options*** - onglet ***Scanning*** - ***Operations to perform*** pour ouvrir la fenêtre ***Select operations*** (figure ci-dessous). Sélectionnez toutes les opérations.



Toujours dans l'onglet ***Scanning***, cliquez sur ***List of ports to be scanned*** et sélectionnez tous les ports.

En effectuant le *scan* de la machine cible, LANguard arrive à obtenir, grâce à NetBios, les informations suivantes :

- HostName : Vectra24
- MAC : 00-04-76-9B-3B-98
- UserName : ADMINISTRATOR
- LAN Manager : Windows 2000 LAN Manager
- Domain : WORKGROUP
- Operating Systeme : Windows 2000
- Information sur les services NetBios (voir Mesures\Empreintes\W2K PRO\tst\tst1LANgExt.html)
- Certains ports TCP ouverts (135,139,445)

En effectuant la même opération en « local », LANguard affiche, en plus des informations ci-dessus, des indications sur (voir Mesures\Empreintes\W2K PRO\tst\tst1LANgInt.html) :

- Les partages (Shares)
- Les Groupes (Administrators, Guests, Users,…)
- Les Utilisateurs (Alice, Bob)
- Les services exécutés
- Les processus actifs
- Les *Password policy*
- Les alertes (Informe sur des éléments pouvant compromettre la sécurité du système)
- …

Ce premier test nous a permis de constater des vulnérabilités très graves au niveau de la sécurité. Par défaut, WIN2Kpro utilise NetBios sur TCP/IP et partage ses fichiers et ses imprimantes. Cela permet à des logiciels comme LANguard, d'obtenir quantités d'informations sur une cible. De plus, Windows possède des partages administratifs comme C$ (partage du disque « C: » à la racine) ou encore IPC$, ADMIN$.

4.2 Test 2 : Installation du *Service Pack 2* (SP2)

Dans ce deuxième test, nous allons voir s'il y a une différence visible dans la configuration par défaut de Windows 2000 après l'installation du *Service Pack 2* (SP2 (MSDN cd 16.1)).

Configuration lors du test :

- Windows 2000 professional **SP2**
- Partage de fichiers et d'imprimantes, activé (par défaut)
- NetBIOS sur TCP/IP, activé (par défaut)
- User : Administrator
- Domaine : workgroup

Nous effectuons les mêmes *scan* que pour le test précédent. Voici ce que nous obtenons avec Fscan :

```
Fscan -v -p 1-65535 -u 1-65535 10.0.2.18

Adding TCP port range 1-65535
Adding UDP port range 1-65535
Adding IP 10.0.2.18
Using 64 threads.
Connect timeout set to 600 ms.
Ping timeout set to 500 ms.
Scan delay set to 0 ms.

Scan started at Wed Feb 27 10:09:38 2002

Scanning TCP ports on 10.0.2.18
10.0.2.18         135/tcp
10.0.2.18         139/tcp
10.0.2.18         445/tcp
10.0.2.18        1025/tcp
Scanning UDP ports on 10.0.2.18
10.0.2.18         135/udp
10.0.2.18         137/udp
10.0.2.18         138/udp
10.0.2.18         445/udp
10.0.2.18         500/udp
10.0.2.18        1026/udp

Scan finished at Wed Feb 27 10:30:53 2002
Time taken: 131070 ports in 1275.234 secs (102.78 ports/sec)
```

On constate que les ports ouverts par défaut sont identiques à ceux du test 1.

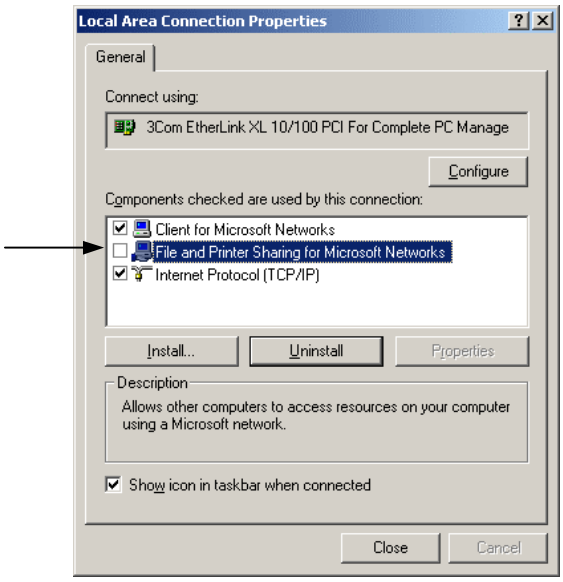
En effectuant un *scan* avec LANguard, depuis la machine distante, on constate, là aussi, qu'il n'y a pas de différence par rapport au test précédent (voir Mesures\Empreintes\W2K PRO\tst\tst2LANgExt.html).

Par contre, lors du *scan* « local » avec LANguard, on a constaté les différences suivantes (voir Mesures\Empreintes\W2K PRO\tst\tst2LANgInt.html) :

- Service Pack 2, détecté
- Service « TapiSrv » – Telephony, supprimé
- Processe « msiexec », ajouté
- Alerte « NetBIOS Name Server Protocol Spoofing (Win2k) », supprimé
- Alerte « Network Dynamic Data Exchange (DDE) vulnerability », supprimé
- Alerte « Windows 2000 Relative Shell Path », supprimé
- Alerte « Windows 2000 SNMP parameters », supprimé

4.3 Test 3 : Désactivation du partage de fichiers et d'imprimantes

A présent, nous allons désactiver le partage de fichiers et d'imprimantes sur la machine cible. Pour cela, allez dans : ***Control Panel*** - ***Network and Dial-up*** **Connections** - ***Local Area Connection*** - ***Properties***. Dans la fenêtre ***Local Area Connection Properties***, désactivé ***File and Printer Sharing for Microsoft Networks*** (voit figure ci-dessous).



Configuration lors du test :

- Windows 2000 professional SP2
- Partage de fichiers et d'imprimantes, **désactivé**
- NetBIOS sur TCP/IP activé, (par défaut)
- User : Administrator
- Domaine : workgroup

Résultat de Fscan :

```
Fscan -v -p 1-65535 -u 1-65535 10.0.2.18

Adding TCP port range 1-65535
Adding UDP port range 1-65535
Adding IP 10.0.2.18
Using 64 threads.
Connect timeout set to 600 ms.
Ping timeout set to 500 ms.
Scan delay set to 0 ms.

Scan started at Wed Feb 27 10:57:23 2002

Scanning TCP ports on 10.0.2.18
10.0.2.18          135/tcp
10.0.2.18          139/tcp
10.0.2.18         1025/tcp
Scanning UDP ports on 10.0.2.18
10.0.2.18          135/udp
10.0.2.18          137/udp
10.0.2.18          138/udp
10.0.2.18          500/udp
10.0.2.18         1026/udp

Scan finished at Wed Feb 27 11:18:37 2002
Time taken: 131070 ports in 1274.633 secs (102.83 ports/sec)
```

On constate que les ports 445 TCP et UDP sont à présent fermés.

Lors du *scan* « distant » avec LANguard, on voit les choses suivantes (voir Mesures\Empreintes\W2K PRO\tst\tst3LANgExt.html) :

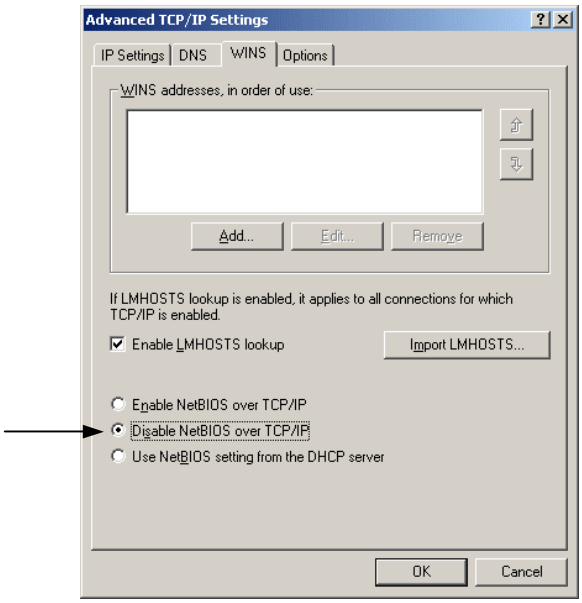
- Une mauvaise détection du système d'exploitation (Windows XP/ME au lieu de Windows 2000)
- LANguard n'obtient plus d'information sur le *Domain* et le *LAN Manager*.
- Le service NetBIOS « Files Server Service » n'est plus détecté

En effectuant le *scan* « local », on constate que LANguard obtient le même résultat que le *scan* « distant » (voir Mesures\Empreintes\W2K PRO\tst\tst3LANgInt.html)

Ce test nous a montré qu'en désactivant le partage de fichiers et d'imprimantes, les ports 445 TCP et UDP sont désactivés. Cela empêche l'obtention de nombreuses informations. Par exemple, lors du test local, LANguard n'obtient plus les informations sur les partages, les groupes, les services,… .

4.4 Test 4 : Désactivation de NetBIOS sur TCP/IP

Pour ce test, nous allons désactiver NetBIOS sur TCP/IP. En effet, Windows 2000 permet de travailler sans ce protocole propriétaire, mais il n'est plus possible de partager des fichiers avec des machines NT4. Pour cela, allez dans : ***Control Panel*** - ***Network and Dial-up Connections*** - ***Local Area Connection*** – ***Properties*** - ***Internet Protocol (TCP/IP)*** – ***Properties*** - ***Advanced…*** - onglet ***WINS*** - ***Disable NetBIOS over TCP/IP*** (voir figure ci-dessous).



Configuration lors du test :

- Windows 2000 professional SP2
- Partage de fichiers et d'imprimantes, désactivé
- NetBIOS sur TCP/IP, **désactivé**
- User : Administrator
- Domaine : workgroup

Résultat de Fscan :

```
Fscan -v -p 1-65535 -u 1-65535 10.0.2.18

Adding TCP port range 1-65535
Adding UDP port range 1-65535
Adding IP 10.0.2.18
Using 64 threads.
Connect timeout set to 600 ms.
Ping timeout set to 500 ms.
Scan delay set to 0 ms.

Scan started at Wed Feb 27 11:41:12 2002

Scanning TCP ports on 10.0.2.18
10.0.2.18         135/tcp
10.0.2.18        1025/tcp
Scanning UDP ports on 10.0.2.18
10.0.2.18         135/udp
10.0.2.18         500/udp
10.0.2.18        1026/udp

Scan finished at Wed Feb 27 12:02:26 2002
Time taken: 131070 ports in 1273.451 secs (102.93 ports/sec)
```

On constate que les ports TCP 139 et UDP 137,138 sont à présent fermés.

Lorsqu'on effectue le *scan* « distant » avec LANguard, on remarque qu'il n'obtient presque plus d'information (voir Mesures\Empreintes\W2K_PRO\tst\tst4LANgExt.html). En effet, les seuls éléments récoltés sont :

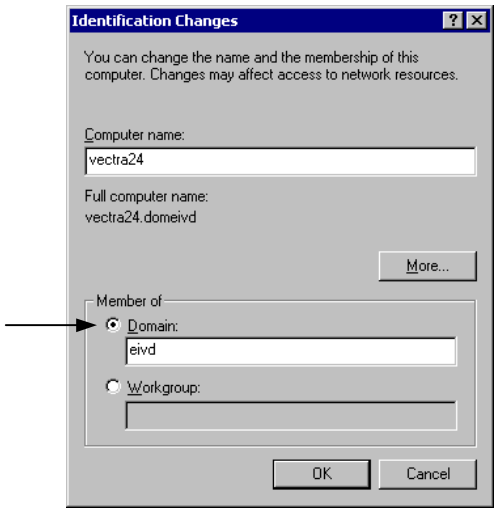
- Une mauvaise détection du système d'exploitation (Windows XP/ME au lieu de Windows 2000)
- Le nombre de *hop* jusqu'à la machine cible
- Le port TCP 135 ouvert

La situation est identique pour le *scan* « local » (voir Mesures\Empreintes\W2K PRO\tst\tst4LANgInt.html).

Ce test montre bien qu'en désactivant NetBIOS sur Windows 2000, il n'est pratiquement plus possible d'obtenir d'information sur la cible.

4.5 Test 5 : Association à un domaine

Jusqu'à présent, notre machine Windows 2000 n'appartenait pas à un domaine, mais faisait partie du *workgroup*. Pour ce test, nous allons l'associer à un domaine (EIVD). Allez sur l'icône ***Computer*** - ***Properties*** - onglet ***Network Identification*** - ***Properties***. Dans la fenêtre ***Identification Changes*** sélectionnez ***Domain*** et entrez le nom du domaine (EIVD), puis cliquer sur ***OK*** (voir figure ci-dessous). Afin que la machine soit associée au domaine, il faut entrer un ***Username*** et un ***Password*** correspondant à un compte du domaine.



Configuration lors du test :

- Windows 2000 professional SP2
- Partage de fichiers et d'imprimantes, désactivé
- NetBIOS sur TCP/IP, désactivé
- User : Administrator Password : dceivd
- Domaine : **eivd**

Résultat de Fscan :

```
Fscan -v -p 1-65535 -u 1-65535 10.0.2.18

Adding TCP port range 1-65535
Adding UDP port range 1-65535
Adding IP 10.0.2.18
Using 64 threads.
Connect timeout set to 600 ms.
Ping timeout set to 500 ms.
Scan delay set to 0 ms.

Scan started at Wed Feb 27 13:53:52 2002

Scanning TCP ports on 10.0.2.18
10.0.2.18         135/tcp
10.0.2.18        1030/tcp
Scanning UDP ports on 10.0.2.18
10.0.2.18         135/udp
10.0.2.18         500/udp
10.0.2.18        1026/udp
10.0.2.18        1047/udp
10.0.2.18        1054/udp

Scan finished at Wed Feb 27 14:15:07 2002
Time taken: 131070 ports in 1274.643 secs (102.83 ports/sec)
```

On constate que le port TCP 1025 est, cette fois, désactivé. Par contre, les ports ci-dessous sont apparus :

- 1030/tcp : port dynamique utiliser par Windows ou d'autres applications.
- 1047/udp : port dynamique utiliser par Windows ou d'autres applications.
- 1054/udp : port dynamique utiliser par Windows ou d'autres applications.

En ce qui concerne LANguard, les résultats sont identiques que ceux du test 4 (voir ci-dessus).

5 Conclusions

Ces différents testes montrent l'avantage offert par Windows 2000 de pour voir désactiver NetBIOS/TCPIP. On constate qu'il est beaucoup plus difficile d'obtenir des informations sur les postes connectés au réseau, sans ce protocole.

Les ports 135, 445 et >1024 sont nécessaire au fonctionnement de Windows 2000 en réseau. Ils doivent donc rester ouverts dans l'intranet, mais doivent être bloqués par le firewall protégeant l'intranet.

Il existe d'autre scanner permettant d'effectuer des testes plus perfectionnée (ISS, Nessus, …). C'est pourquoi ce travail a été poursuivit dans le cadre d'un projet de semestre intitulé « Test d'intrusion ». Différents tests ont été effectués sur Windows 2000 (Pro, Server, DC, …) avec différents types de scanners dont *ISS* et *Nessus*.

6 Références

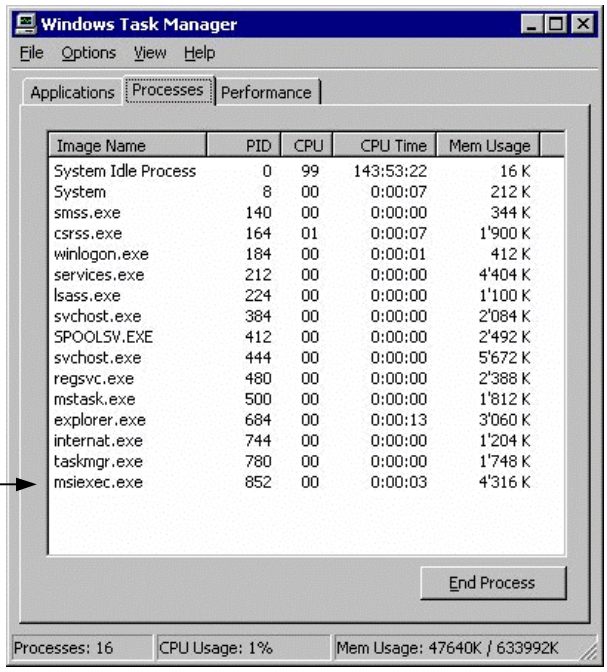
- **Halte aux Hacker**
  Scambray, McClure, Kurtz
  Editions OEM, ISBN 2-7464-0292-0
- **Test d'intrusion**
  Projet de semestre de Miguel Marfil
  Session 2002
- **A List of the Windows 2000 Domain Controller Default Ports (Q289241)**
  Documentations\Empreinte\A List of the Windows 2000 Domain Controller Default Ports.htm

Annexes

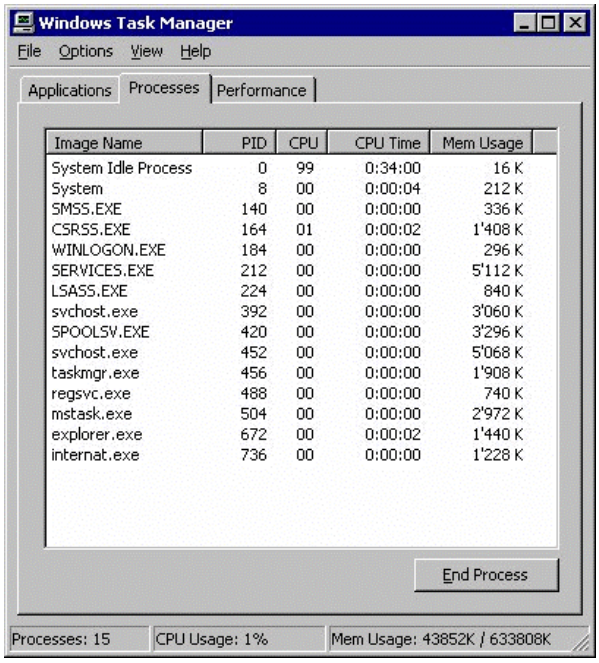
Task manager

Processus actif lors des tests :

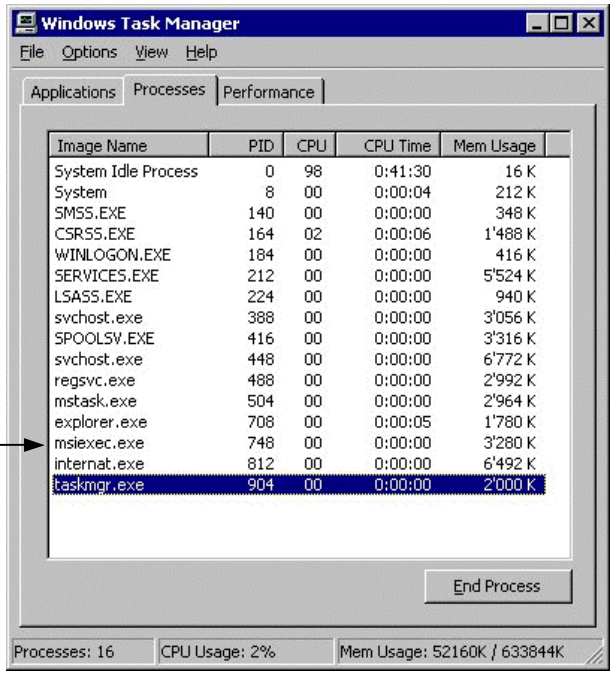
Test 1



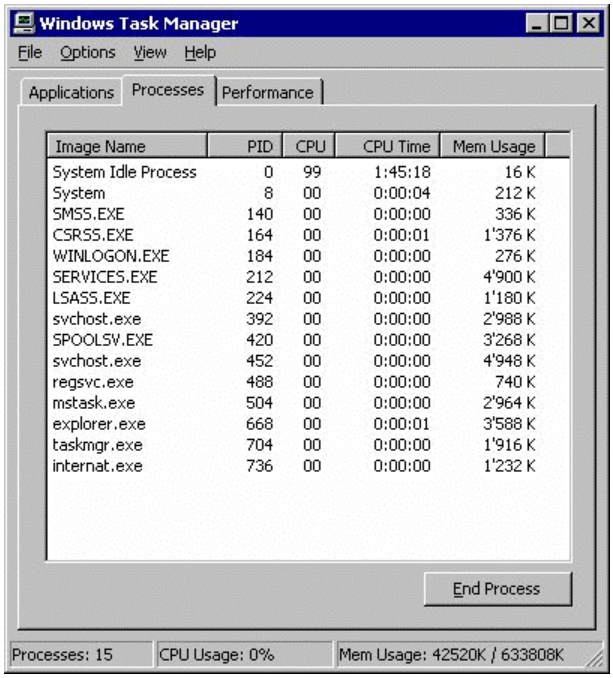
Test 2



Test 3



Test 4 – Test 5



Fport

Programme permettant de déterminer le processus à l'origine d'un port.
http://www.foundstone.com/knowledge/proddesc/fport.html

```
fport
C:\Fport>netstat -a

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    vectra24:epmap         vectra24.domeivd:0     LISTENING
  TCP    vectra24:microsoft-ds  vectra24.domeivd:0     LISTENING
  TCP    vectra24:1030          vectra24.domeivd:0     LISTENING
  UDP    vectra24:epmap         *:*
  UDP    vectra24:microsoft-ds  *:*
  UDP    vectra24:1026          *:*
  UDP    vectra24:1039          *:*
  UDP    vectra24:1048          *:*
  UDP    vectra24:isakmp        *:*

C:\Fport>fport -p
FPort v1.33 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid   Process            Port  Proto Path
400   svchost        ->  135   TCP   C:\WINNT\system32\svchost.exe
8     System         ->  445   TCP
536   MSTask         ->  1030  TCP   C:\WINNT\system32\MSTask.exe

400   svchost        ->  135   UDP   C:\WINNT\system32\svchost.exe
8     System         ->  445   UDP
224   lsass          ->  500   UDP   C:\WINNT\system32\lsass.exe
224   lsass          ->  1026  UDP   C:\WINNT\system32\lsass.exe
212   services       ->  1039  UDP   C:\WINNT\system32\services.exe
184   winlogon       ->  1048  UDP   \??\C:\WINNT\system32\winlogon.exe


C:\Fport>_
```

```
Command Prompt
C:\scanner\fscan>fscan -v -p 1-65535 -u 1-65535 10.0.2.18
FScan v1.12 - Command line port scanner.
Copyright 2000 (c) by Foundstone, Inc.
http://www.foundstone.com

 Adding TCP port range 1-65535
 Adding UDP port range 1-65535
 Adding IP 10.0.2.18
 Using 64 threads.
 Connect timeout set to 600 ms.
 Ping timeout set to 500 ms.
 Scan delay set to 0 ms.

 Scan started at Wed Mar 06 16:37:34 2002

 Scanning TCP ports on 10.0.2.18
10.0.2.18          135/tcp
10.0.2.18         1030/tcp
 Scanning UDP ports on 10.0.2.18
10.0.2.18          135/udp
10.0.2.18          500/udp
10.0.2.18         1026/udp
10.0.2.18         1039/udp
10.0.2.18         1048/udp

 Scan finished at Wed Mar 06 16:58:48 2002
 Time taken: 131070 ports in 1274.633 secs (102.83 ports/sec)

C:\scanner\fscan>_
```

Remarques:

Les ports trouvés par Fscan, correspondent aux ports qui sont ouvert par un processus autre que « systeme » dans Fport. Le nombre de port ouvert par ce dernier est variable.

Les numéros des ports pour les processus « services » et « winlogon » change à chaque *boot* de la machine, mais pas à la fermeture d'une session.