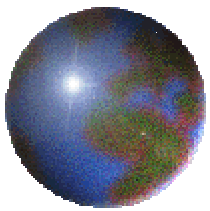
CENTRE NATIONAL
DE LA RECHERCHE
SCIENTIFIQUE

« JRES 2003 »

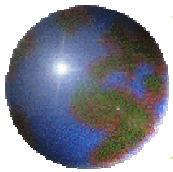


Detescan
Un outil de génération de rapports de scan depuis les logs issus d'un routeur ou d'un pare-feu

Denis Pugnère

Institut de Génétique Humaine

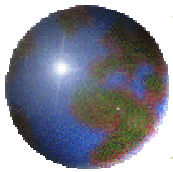
CNRS Montpellier



Présentation

- Outil de détection de scans et de rapport.
- Écrit en PERL, auteurs :

  Gabrielle Feltin, Bertrand Wallrich, Marwan Burelle, Jean-Claude Barbet, Joel Marchand, Philippe Weill, Bruno Kriner, Denis Pugnère
- Extrait les événements depuis les *logs* d'un routeur :
  - construction d ’un rapport, envoi par mail
  - le rapport contient :
    - résumé des *scans*
    - extrait des *logs* des *scans*
- 2 utilisations principales
  - pour l'administrateur réseau
  - pour le CERT Renater : consolidation, veille sécurité



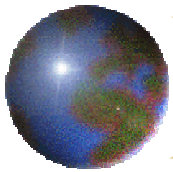
Pré-requis

- Routeur ou pare-feu ayant la capacité d ’enregistrer les évènements (traces) dans un journal de bord (log),
- un serveur *SYSLOG* (serveur Unix avec le *daemon SYSLOG* activé) qui va recevoir et stocker les évènements dans un fichier,
- configurer votre routeur pour qu'il envoie les traces sur le serveur *SYSLOG*,
- Mettre en place une politique de filtrage du type : TOUT INTERDIT SAUF : c ’est à dire configurer des filtres du routeur avec une politique : "filtrage de tout sauf",
- configurer le routeur pour enregistrer les traces des tentatives de violation des filtres.

Configuration IOS Cisco pour les traces

- Exemple pour Cisco

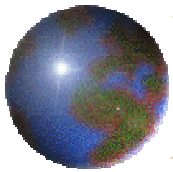
```
! Cisco IOS
! enregistrement des logs des access-list sur le serveur syslog (service local5)
logging trap debugging
logging facility local5
logging x.y.z.t
…
! configuration de l ’interface
interface Ethernet0
…
   ! on active l ’access-list 101 sur les paquets qui entrent sur l ’interface
   ip access-group 101 in
…

! acces au serveur web
access-list 101 permit tcp any a.b.c.d eq 80
…
! connexions ouvertes depuis l ’intérieur
access-list 101 permit tcp any any established

! en entree : TOUT LE RESTE EST BLOQUE
! a la place de : access-list 101 deny ip any any log
! remplacer par tcp + udp (pour avoir les numeros de ports TCP et UDP dans les logs)
access-list 101 deny tcp any any range 1 65535 log
access-list 101 deny udp any any range 1 65535 log
```



Configuration Extreme pour les traces

- Exemple pour Extreme Networks

```
# ExtremeWare 6.x
# pour enregistrer les logs des access-list sur le serveur syslog (service local5) :
conf syslog add x.y.z.t local5 debug
enable syslog
...
# acces au serveur web
create access-list serveur-www tcp destination a.b.c.d/32 ip-port 80 source any ip-port any permit ports any precedence 808
...
# en entree : on filtre les paquets TCP avec flag SYN
create access-list tcp-establ1 tcp destination any ip-port range 1 65535 source any ip-port any permit-established ports any  \
                                                                                                                precedence 1000
# on garde une trace de ces evenements
enable access-list tcp-establ1 log
# on laisse passer les autres paquets (flags SYN+ACK et ACK)
create access-list tcp-establ2 tcp destination any ip-port range 1 65535 source any ip-port any permit ports p precedence 1010
...
# en entree : TOUT LE RESTE EST BLOQUE
# a la place de: create access-list deny-global ip destination any source any deny ports p precedence 1020
# remplacer par tcp + udp (pour avoir les numeros de ports TCP et UDP dans les logs)
create access-list deny-global-tcp1 tcp destination any ip-port any source any ip-port any deny ports p precedence 1030
enable access-list deny-global-tcp1 log
create access-list deny-global-udp1 udp destination any ip-port any source any ip-port any deny ports p precedence 1035
enable access-list deny-global-udp1 log
```



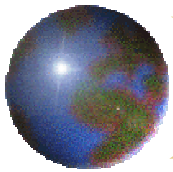
Configuration du serveur SYSLOG

- Exemple SYSLOG Linux

```
# fichier /etc/syslog.conf
# trace du routeur
local5.*                        -/var/log/routeur
```

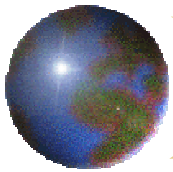
- Exemple SYSLOG SGI

```
# fichier /etc/syslog.conf
# trace du routeur
local5.debug                    /var/log/routeur
```



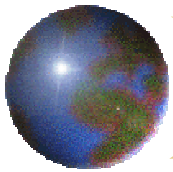
Fonctionnalités (1)

- Lecture de logs centralisés sur un serveur SYSLOG (Unix/NT?)
- Reconnaissance des formats de logs provenant de routeurs de différentes marques :
  - routeurs/commutateurs Cisco IOS v10.x, 11.x et 12.x ,
  - routeurs/commutateurs Foundry Networks,
  - routeurs/commutateurs Cabletron,
  - routeurs logiciels Tru64Unix screend,
  - routeurs/pare-feu logiciels Linux IPCHAINS,
  - routeurs/pare-feu logiciels Linux IPTABLES,
  - plugin portscan de la sonde logicielle SNORT,
  - routeurs/commutateurs Allied Telesyn,
  - routeurs/commutateurs Extreme Networks,
  - pare-feu Cisco PIX.



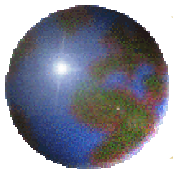
Fonctionnalités (2)

- Sélection d'une date d'événements parmi tous ceux contenus dans le(s) fichier(s) de logs :
  - les paquets *loggués* et refusés sur un port destination
  - les paquets *loggués* et refusés sur une machine destination
- Application d'un seuil (modifiable) de détection d'évènements :
  - ne sont rapportés les *scans* sur plus de 5 ports par machine
  - ne sont rapportés les *scans* sur plus de 3 machines



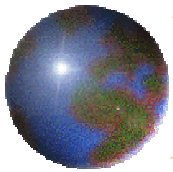
Fonctionnalités (3)

- Possibilité d'exclusion du rapport :
  - les adresses IP de certains réseaux ou de certaines machines
  - les *scans* à destination de certains ports (*TCP* ou *UDP*).
- Création, d'un seul rapport de synthèse en 2 parties :
  - un résumé des *scans* par port et par machine
  - un extrait des *logs* des *scans* par port et par machine (nombre de lignes de l'extrait modifiable)
- Envoi de ce rapport à une ou plusieurs personnes



Exemples d ’utilisation

- Utilisation des rapports de Detescan pour :
  - La détection de *scan* réseaux (*IP*, *ICMP*, *TCP*, *UDP*)
  - détection d ’erreurs de filtrage,
  - détection de problèmes de configuration des postes des utilisateurs (adressage *IP* incorrect, configuration *DNS*, configuration *NTP*...),
  - détection de l ’installation de services réseaux non déclarés,
  - détection d ’utilisation d ’applications non conformes à la charte informatique du laboratoire, du campus ou de celle de RENATER.



Exemple : scans sur 80/TCP

```
Subject: [detescan] Resume 23/09/2001

Parametres pour detection scans : nb machines minimum > 1, nb ports minimum > 1
Detescan.pl a détecté les scans suivants à partir des logs Cisco :

 Sep 23 00:56:22 : scan tcp de  vnd.xxxx.ru             sur le port 80 (www) ( 15 machines )
 Sep 23 18:28:10 : scan tcp de  cxxxxxx-a.pinol1.sfba.xxxx.com sur le port 80 (www) ( 2 machines )
 Sep 23 04:27:54 : scan tcp de  dhcp-019-098.cns.xxxx.edu      sur le port 80 (www) ( 2 machines )

Logs de chacun des scans :

 Sep 23 00:56:22 : scan tcp de  vnd.xxxx.ru             sur le port 80 (www) ( 15 machines )
Sep 23 00:56:22 gate 5d10h: IPACL: list 101 denied tcp 195.9.xxxx.37(2705) -> x.y.z.177(80), 2 packets
Sep 23 02:47:35 gate 5d12h: IPACL: list 101 denied tcp 195.9.xxxx.37(4641) -> x.y.z.89(80), 2 packets
Sep 23 05:05:59 gate 5d14h: IPACL: list 101 denied tcp 195.9.xxxx.37(3151) -> x.y.z.48(80), 2 packets
Sep 23 06:10:56 gate 5d15h: IPACL: list 101 denied tcp 195.9.xxxx.37(2547) -> x.y.z.147(80), 2 packets
Sep 23 06:46:29 gate 5d16h: IPACL: list 101 denied tcp 195.9.xxxx.37(3591) -> x.y.z.108(80), 2 packets

 Sep 23 18:28:10 : scan tcp de  c1xxxxxx-a.pinol1.sfba.xxxx.com sur le port 80 (www) ( 2 machines )
Sep 23 18:28:10 gate 6d03h: IPACL: list 101 denied tcp 65.5.xxxx.242(2658) -> x.y.z.179(80), 1 packet
Sep 23 19:17:27 gate 6d04h: IPACL: list 101 denied tcp 65.5.xxxx.242(4526) -> x.y.z.52(80), 2 packets

 Sep 23 04:27:54 : scan tcp de  dhcp-019-098.cns.xxxx.edu      sur le port 80 (www) ( 2 machines )
Sep 23 04:27:54 gate 5d13h: IPACL: list 101 denied tcp xxxx.xxxx.19.98(4395) -> x.y.z.207(80), 1 packet
Sep 23 04:35:17 gate 5d14h: IPACL: list 101 denied tcp xxxx.xxxx.19.98(2128) -> x.y.z.69(80), 1 packet
```

Ver nimba, code red...

La quantité de scans était de plus en plus importante et inhabituelle :

- Pas des scans linéaires ou pseudo-aléatoires de toutes les adresses d'un réseau IP durant une courte durée (comme le ferait *nmap*).
- Scans "lents" (quelques paquets par heure seulement) provenant d'un grand nombre d'adresses IP sources externes, durant plusieurs jours sur seulement un sous-ensemble des adresses IP de nos réseaux.

Ce type de scans ressemble au fonctionnement des vers *Code-Red* ou *Nimda* :

Exemple : Ver MS-SQL

```
Subject: [detescan] Resume 2003/01/25

parametres pour detection scans : nb machines minimum >= 5, nb ports minimum >= 5
Detescan v20021025 a détecté les scans suivants à partir des logs du routeur extreme

Jan 25 06:34:05 : scan udp de 24.217.xxx.8 sur le port 1434 () ( 335 machines )
Jan 25 06:34:05 : scan udp de 200.181.xxx.214 sur le port 1434 () ( 347 machines )

Logs de chacun des scans :

 Jan 25 06:34:05 : scan udp de 24.217.xxx.8 sur le port 1434 () ( 335 machines )
Jan 25 06:34:05 gate KERN: UDP Drop: 1-4093 24.217.xxx.8:4851->xxx.xxx.xxx.200:1434
Jan 25 06:34:14 gate KERN: UDP Drop: 1-4093 24.217.xxx.8:4851->xxx.xxx.yyy.244:1434
Jan 25 06:35:30 gate KERN: UDP Drop: 1-4093 24.217.xxx.8:4851->xxx.xxx.xxx.246:1434
Jan 25 06:39:35 gate KERN: UDP Drop: 1-4093 24.217.xxx.8:4851->xxx.xxx.zzz.225:1434
Jan 25 06:39:45 gate KERN: UDP Drop: 1-4093 24.217.xxx.8:4851->xxx.xxx.xxx.1:1434

 Jan 25 06:34:05 : scan udp de 200.181.xxx.214 sur le port 1434 () ( 347 machines )
Jan 25 06:34:05 gate KERN: UDP Drop: 1-4093 200.181.xxx.214:3163->xxx.xxx.xxx.183:1434
Jan 25 06:34:17 gate KERN: UDP Drop: 1-4093 200.181.xxx.214:3163->xxx.xxx.yyy.143:1434
Jan 25 06:35:48 gate KERN: UDP Drop: 1-4093 200.181.xxx.214:3163->xxx.xxx.zzz.145:1434
Jan 25 06:40:43 gate KERN: UDP Drop: 1-4093 200.181.xxx.214:3163->xxx.xxx.zzz.208:1434
Jan 25 06:40:55 gate KERN: UDP Drop: 1-4093 200.181.xxx.214:3163->xxx.xxx.xxx.156:1434
```

Scan massif sur port 1434/UDP

Très grand nombre de paquets reçus, sur toutes les adresses destination, départ depuis de multiples sources simultanément

Références :

http://www.nextgenss.com/advisories/mssql-udp.txt
http://www.microsoft.com/technet/security/bulletin/MS02-039.asp
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2002-0650

Exemple : causes multiples

```
Subject: [detescan] Resume 06/11/2001

parametres pour detection scans : nb machines minimum > 1, nb ports minim
detescan.pl a détecté les scans suivants à partir des logs Cisco :

 Nov 6 112959  scan udp de   time1.euro.apple.com    sur le port 123 (ntp) ( 2 machines )
 Nov 6 100352  scan udp de   time2.euro.apple.com    sur xxxx.igh.cnrs.fr ( 3 ports )
 Nov 6 120213  scan icmp de  165.21.xxxx.39          de type icmp (8/0) ( 3 machines )
 Nov 6 003654  scan tcp de   216.167.xxxx.211        sur le port 53 (domain) ( 3 machines )
 Nov 6 113252  scan udp de   ns1.club-internet.fr    sur xxxx.igh.cnrs.fr ( 6 ports )
 Nov 6 130229  scan tcp de   lns3-148.xxxx.w.club-internet.fr   sur le port 21 (ftp) ( 2 machines )

Logs de chacun des scans :

 Nov 6 112959  scan udp de   time1.euro.apple.com    sur le port 123 (ntp) ( 2 machines )
Nov  6 112959 gate 4w1d IPACL list 101 denied udp 194.151.19.93(123) -> x.y.z.34(123), 1 packet
Nov  6 145433 gate w1d IPACL list 101 denied udp 194.151.19.93(123) -> x.y.z.51(123), 1 packet

 Nov 6 100352  scan udp de   time2.euro.apple.com    sur xxxx.igh.cnrs.fr ( 3 ports )
Nov  6 100352 gate w1d IPACL list 101 denied udp 194.151.19.94(123) -> x.y.z.31(49158), 1 packet
Nov  6 220407 gate w1d IPACL list 101 denied udp 194.151.19.94(123) -> x.y.z.31(49207), 1 packet

 Nov 6 120213  scan icmp de  165.21.xxxx.39          de type icmp (8/0) ( 3 machines )
Nov  6 120213 gate w1d IPACL list 101 denied icmp 165.21.xxxx.39 -> x.y.z.255 (8/0), 1 packet
Nov  6 164048 gate w1d IPACL list 101 denied icmp 165.21.xxxx.39 -> x.y.z.255 (8/0), 1 packet

 Nov 6 003654  scan tcp de   216.167.xxxx.211        sur le port 53 (domain) ( 3 machines )
Nov  6 003654 gate w0d IPACL list 101 denied tcp 216.167.xxxx.211(1307) -> x.y.z.237(53), 1 packet
Nov  6 003657 gate w0d IPACL list 101 denied tcp 216.167.xxxx.211(1308) -> x.y.z.238(53), 1 packet

 Nov 6 113252  scan udp de   ns1.club-internet.fr    sur xxxx.igh.cnrs.fr ( 6 ports )
Nov  6 113252 gate w1d IPACL list 101 denied udp 194.117.200.10(53) -> x.y.z.216(1768), 1 packet
Nov  6 113839 gate w1d IPACL list 101 denied udp 194.117.200.10(53) -> x.y.z.216(1770), 1 packet

 Nov 6 130229  scan tcp de   lns3-148.xxxx.w.club-internet.fr    sur le port 21 (ftp) ( 2 machines )
Nov  6 130229 gate w1d IPACL list 101 denied tcp 213.44.xxxx.148(4046) -> x.y.z.34(21), 1 packet
Nov  6 130238 gate w1d IPACL list 101 denied tcp 213.44.xxxx.148(4063) -> x.y.z.65(21), 1 packet
```

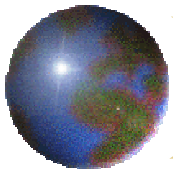
Problèmes de configuration de postes clients : ne pas reporter

Scans réels, reporter

Exemple : traceroute ou scan distribué ?

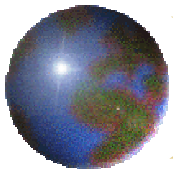
```
Subject: [detescan] Resume 31/05/2001

parametres pour detection scans : nb machines minimum > 1, nb ports minimum > 1
detescan.pl a détecté les scans suivants à partir des logs Cisco :


 May 31 : scan udp de        smtp.xxx.co.uk     sur xxx.igh.cnrs.fr ( 4 ports )
 May 31 : scan udp de        www.xxx.com        sur yyy.igh.cnrs.fr ( 6 ports )
 May 31 : scan udp de        www.xxx.net        sur xxx.igh.cnrs.fr ( 16 ports )

Logs de chacun des scans :

 May 31 : scan udp de smtp.xxx.co.uk sur xxx.igh.cnrs.fr ( 4 ports )
May 31 15:47:41 gate : list 101 denied udp 194.129.xxx.14(54374) -> xxx.xxx.xxx.1(33520), 1 packet
May 31 15:47:46 gate : list 101 denied udp 194.129.xxx.14(54374) -> xxx.xxx.xxx.1(33521), 1 packet
May 31 15:47:51 gate : list 101 denied udp 194.129.xxx.14(54374) -> xxx.xxx.xxx.1(33522), 1 packet
May 31 15:48:01 gate : list 101 denied udp 194.129.xxx.14(54374) -> xxx.xxx.xxx.1(33524), 1 packet

 May 31 : scan udp de        www.xxx.com        sur yyy.igh.cnrs.fr ( 6 ports )
May 31 15:48:03 gate : list 101 denied udp 216.129.xxx.4(59762) -> xxx.xxx.yyy.1(33505), 1 packet
May 31 15:48:40 gate : list 101 denied udp 216.129.xxx.4(59762) -> xxx.xxx.yyy.1(33512), 1 packet
May 31 15:48:45 gate : list 101 denied udp 216.129.xxx.4(59762) -> xxx.xxx.yyy.1(33513), 1 packet
May 31 15:49:01 gate : list 101 denied udp 216.129.xxx.4(59762) -> xxx.xxx.yyy.1(33516), 1 packet
May 31 15:49:06 gate : list 101 denied udp 216.129.xxx.4(59762) -> xxx.xxx.yyy.1(33517), 1 packet
May 31 15:49:32 gate : list 101 denied udp 216.129.xxx.4(59762) -> xxx.xxx.yyy.1(33522), 1 packet


 May 31 : scan udp de        www.xxx.net        sur xxx.igh.cnrs.fr ( 16 ports )
May 31 15:47:27 gate : list 101 denied udp 207.126.xxx.163(64256) -> xxx.xxx.xxx.1(33486), 1 packet
May 31 15:48:07 gate : list 101 denied udp 207.126.xxx.163(64256) -> xxx.xxx.xxx.1(33494), 1 packet
May 31 15:48:17 gate : list 101 denied udp 207.126.xxx.163(64256) -> xxx.xxx.xxx.1(33496), 1 packet
May 31 15:48:22 gate : list 101 denied udp 207.126.xxx.163(64256) -> xxx.xxx.xxx.1(33497), 1 packet
May 31 15:48:37 gate : list 101 denied udp 207.126.xxx.163(64256) -> xxx.xxx.xxx.1(33500), 1 packet
May 31 15:48:47 gate : list 101 denied udp 207.126.xxx.163(64256) -> xxx.xxx.xxx.1(33502), 1 packet
```

Signature de traceroute (ports UDP 33434 à 33523) ou scan distribué (même heure…) ?



Exemple : Deni de service distribué ?

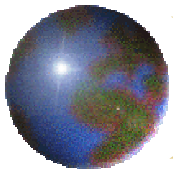
```
Subject: [detescan] Resume 2002/07/29

parametres pour detection scans : nb machines minimum >= 5, nb ports minimum >= 5
Detescan v20020319 a détecté les scans suivants à partir des logs du routeur extreme

 Jul 29 12:44:23 : scan udp de        194.251.xxx.103               sur xxx.xxx.xxx.20( 15 ports )
 Jul 29 12:47:40 : scan udp de        213.221.xxx.5               sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        chewbacca.xxx.co.uk        sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        ntserver.xxx.de        sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        198.246.xxx.11               sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        62-80-xxx-30.xxx.net        sur xxx.xxx.xxx.20 ( 48 ports )
 Jul 29 12:47:40 : scan udp de        194.177.xxx.120               sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        ghost.xxx.co.nz        sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        SMC-WEB2.xxx.DE        sur xxx.xxx.xxx.20 ( 54 ports )
 Jul 29 12:47:40 : scan udp de        station-202.101.xxx.com        sur xxx.xxx.xxx.20 ( 25 ports )
 Jul 29 12:47:40 : scan udp de        CHIMAERA.gaming.xxx.co.uk        sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        serv065.games.inet.xxx.dk        sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        80.78.xxx.25               sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        208.210.xxx.163               sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        212-246-xxx-29.xxx.net        sur xxx.xxx.xxx.20 ( 56 ports )
 Jul 29 12:47:40 : scan udp de        4.23.xxx.235               sur xxx.xxx.xxx.20 ( 56 ports )

Logs de chacun des scans :

 Jul 29 12:44:23 : scan udp de        194.251.xxx.103               sur xxx.xxx.xxx.20 ( 15 ports )
Jul 29 12:44:23 gate KERN: UDP Drop: 1-4093 194.251.xxx.103:33333->xxx.xxx.xxx.20:1305
Jul 29 12:44:55 gate KERN: UDP Drop: 1-4093 194.251.xxx.103:33333->xxx.xxx.xxx.20:1308

 Jul 29 12:47:40 : scan udp de        213.221.165.5               sur xxx.xxx.xxx.20 ( 56 ports )
Jul 29 12:47:40 gate KERN: UDP Drop: 1-4093 213.221.xxx.5:4849->xxx.xxx.xxx.20:1311
Jul 29 12:47:41 gate KERN: UDP Drop: 1-4093 213.221.xxx.5:4849->xxx.xxx.xxx.20:1312

 Jul 29 12:47:40 : scan udp de        chewbacca.xxx.co.uk        sur xxx.xxx.xxx.20 ( 56 ports )
Jul 29 12:47:40 gate KERN: UDP Drop: 1-4093 194.117.xxx.72:25300->xxx.xxx.xxx.20:1311
Jul 29 12:47:41 gate KERN: UDP Drop: 1-4093 194.117.xxx.72:25300->xxx.xxx.xxx.20:1312
```



Exemple : détection de trafic P2P

```
Subject: [detescan] Resume 2003/09/27

parametres pour detection scans : nb machines minimum >= 2, nb ports minimum >= 2
Detescan v20030207 a détecté les scans suivants à partir des logs du routeur extreme


 Sep 27 16:40:29 : scan udp/tcp de        207.44.xxx.40    sur xxx.igh.cnrs.fr ( 2 ports )
 Sep 27 16:40:32 : scan udp/tcp de        211.227.xxx.116   sur xxx.igh.cnrs.fr ( 2 ports )
 Sep 27 16:40:32 : scan udp/tcp de        207.44.xxx.27    sur xxx.igh.cnrs.fr ( 2 ports )
 Sep 27 16:40:35 : scan udp/tcp de        211.233.xxx.235   sur xxx.igh.cnrs.fr ( 2 ports )

Logs de chacun des scans :

 Sep 27 16:40:29 : scan udp/tcp de        207.44.xxx.40    sur xxx.igh.cnrs.fr ( 2 ports )
Sep 27 16:40:29 6W:gate KERN: UDP Drop: 1-4093 207.44.xxx.40:4246->xxx.xxx.xxx.54:4666
Sep 27 19:21:17 6W:gate KERN: TCP Not-Estb: 1-4093 207.44.xxx.40:57500->xxx.xxx.xxx.54:4662

 Sep 27 16:40:32 : scan udp/tcp de        211.227.xxx.116   sur xxx.igh.cnrs.fr ( 2 ports )
Sep 27 16:40:32 6W:gate KERN: UDP Drop: 1-4093 211.227.xxx.116:4246->xxx.xxx.xxx.54:4666
Sep 27 19:21:58 6W:gate KERN: TCP Not-Estb: 1-4093 211.227.xxx.116:53291->xxx.xxx.xxx.54:4662

 Sep 27 16:40:32 : scan udp/tcp de        207.44.xxx.27    sur xxx.igh.cnrs.fr ( 2 ports )
Sep 27 16:40:32 6W:gate KERN: UDP Drop: 1-4093 207.44.xxx.27:4246->xxx.xxx.xxx.54:4666
Sep 27 19:23:37 6W:gate KERN: TCP Not-Estb: 1-4093 207.44.xxx.27:35386->xxx.xxx.xxx.54:4662

 Sep 27 16:40:35 : scan udp/tcp de        211.233.xxx.235   sur xxx.igh.cnrs.fr ( 2 ports )
Sep 27 16:40:35 6W:gate KERN: UDP Drop: 1-4093 211.233.xxx.235:4665->xxx.xxx.xxx.54:4666
Sep 27 23:08:55 6W:gate KERN: TCP Not-Estb: 1-4093 211.233.xxx.235:39536->xxx.xxx.xxx.54:4662
```

signature du logiciel eDonkey : 4662/TCP et 4666/UDP



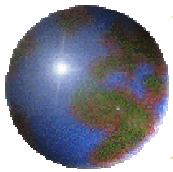
Exemples d'exécution

- En ligne de commande :

```
$ ./detescan.pl -routeur=ios -date "yesterday" /var/log/cisco*

$ ./detescan.pl -routeur=extreme -date "2003/11/19" -nbmach=2 -nbport=2 -nblig=5 \
                -ignoreports=113,137 -ignorehosts=192.168,10.2.3.4 \
                -dest=personne@email.fr /var/log/extreme.gz

$ ./detescan.pl -routeur=foundry -date "2 weeks ago" /home/archives/routeur*.gz

$ ./detescan.pl -routeur=ios -date "24 jun" /var/log/cisco.Z

$ ./detescan.pl -routeur=ios -date "1 month 3 days" /var/log/cisco
```

- Exécution automatique par crontab :

```
#tous les jours a 7h00 du matin: detescan sur logs cisco
0 7 * * *      $HOME/sources/detescan.pl -routeur=ios -date yesterday /var/log/cisco*
```



Références

- Présentation des différentes versions de detescan
  - http://www.urec.cnrs.fr/securite/outils/detescan.html
- Version présentée ici :
  - version v20030207
  - http://www.igh.cnrs.fr/perso/denis.pugnere/detescan
- FAQ: Firewall Forensics :
  - http://www.robertgraham.com/pubs/firewall-seen.html
- TCP & UDP Port Numbers :
  - http://www.wittys.com/files/all-ip-numbers.txt
- Liste de diffusion (nouvelles versions...)
  - detescan [AT] igh.cnrs.fr
  - inscription : envoyer un message a sympa [AT] igh.cnrs.fr avec dans le corps du message : sub detescan