Deteccio d'un escaneig de ports

Sistemes: Ubuntu GNU/Linux (bast en Debian)

Instal·lació del servidor web:

```
# aptitude install webfs
```

He escollit webfs per la seva simplicitat ja que per fer el laboratori no cal res més avançat. He configurat el port per que sigui el 80:

```
# vi /etc/webfsd.conf
...
web_port=80
...
```

He instal·lat snort:

```
# aptitude install snort
```

Sel·leccionant la interfície eth1 i el rang 192.168.6.0/24 com a xarxa local. A continuació he hagut de modificar el fitxer de configuració /etc/snort/snort.conf i canviar la configuració de detecció d'scanneig:

```
preprocessor flow-portscan: \
    talker-sliding-scale-factor 0.50 \
    talker-fixed-threshold 30 \
    talker-sliding-threshold 30 \
    talker-sliding-window 20 \
    talker-fixed-window 30 \
    scoreboard-rows-talker 30000 \
    server-watchnet $HOME_NET \
    server-ignore-limit 200 \
    server-rows 65535 \
    server-learning-time 14400 \
    server-scanner-limit 4 \
    scanner-sliding-window 20 \
    scanner-sliding-scale-factor 0.50 \
    scanner-fixed-threshold 15 \
    scanner-sliding-threshold 40 \
    scanner-fixed-window 15 \
    src-ignore-net $HOME_NET \
    dst-ignore-net [10.0.0.0/30] \
    scoreboard-rows-scanner 30000 \
    alert-mode once \
    output-mode msg \
    tcp-penalties on
```

He eliminat les línies en negreta per tal de poder detectar scans dintre de la meva pròpia xarxa. La resta de la configuració ja estava bé per defecte.

He ficat en marxa l'snort:

```
/etc/init.d/snort start
```

Això fa que s'arrenqui snort amb els següents paràmetres:

```
/usr/sbin/snort -m 027 -D -c /etc/snort/snort.conf -l /var/log/snort -d -u snort -g snort -S
HOME_NET=[192.168.6.0/24] -i eth1
```

Significat:

-m 027	Umask amb els permisos que es creen els arxius, en aquest cas 777 – 027 = 750 per directoris (drwxr-x---) i 640 per fitxers (rw-r-----).
-D	Que s'executi en background com a dimoni.
-c /etc/...	Ubicació del fitxer de configuració.
-l /var/log/...	Ubicació del directori a on generar els logs
-d	Mostrar les dades de la capa aplicació en el cas que estiguem executant

	snort en mode verbose o packet logging (no es el nostre cas).
-u snort	Usuari amb el que s'executarà snort.
-g snort	Grup amb el que s'executarà snort.
-S HOME...	Definició de variables, establim el rang d'IP de la nostra xarxa local.
-i eth1	Interface de xarxa del sistema per on s'ha d'escoltar.

I des d'una altra màquina he utilitzat nmap per fer un scanneig:

```
# nmap  -O -sS -v 192.168.6.234

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2005-01-22 00:32 CET
Host 192.168.6.234 appears to be up ... good.
Initiating SYN Stealth Scan against 192.168.6.234 at 00:32
Adding open port 80/tcp
Adding open port 22/tcp
The SYN Stealth Scan took 1 second to scan 1659 ports.
For OSScan assuming that port 22 is open and port 1 is closed and neither are firewalled
Interesting ports on 192.168.6.234:
(The 1657 ports scanned but not shown below are in state: closed)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
Device type: general purpose
Running: Linux 2.4.X
OS details: Linux 2.4.7 (X86)
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=1611089 (Good luck!)
IPID Sequence Generation: All zeros

Nmap run completed -- 1 IP address (1 host up) scanned in 6.567 seconds
```

Significat dels paràmetres de l'nmap:

-sS	Scan utilitzant només paquets SYN, no s'acaba de establir la connexió. Només es fa un pas del three-hand shaking, d'aquesta forma fem menys “soroll”.
-O	Detectar el sistema operatiu en base a les respostes rebudes.
-v	Verbose.

Snort ha detectat correctament l'scan, si mirem /var/log/snort/alert:

```
[**] [121:4:1] Portscan detected from 192.168.6.75 Talker(fixed: 30 sliding: 30) Scanner(fixed: 0
sliding: 0) [**]
01/22-00:18:45.698790
```

Nmap suporta més tipus d'scans per tal d'aconseguir no ser detectats però no he aconseguit enganyar a Snort.

Alumne: Sergio Blanco Cuaresma