Seguridad en Sistemas Informáticos (SSI)

VNIVERSITAT DE VALÈNCIA OpenCourseWare

Laboratorio: Snort

Carlos Pérez Conde

Departament d'Informàtica

Escola Técnica Superior d'Enginyeria

Universitat de València

Snort

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Objetivos:**
  - aprender a configurar una sonda basada en snort
  - aprender a interpretar las alertas generadas por snort
  - aprender a interpretar las reglas de snort
- **Configuración inicial (/etc/snort/snort.conf)**
  - configurar snort en “exta” para que considere como redes internas las redes 10.5.1.0/24 y 10.5.2.0/24, y como externa el resto
  - pedir que envíe las alertas a “syslog”
    - sugerencia: añadir “output alert_syslog: LOG_AUTH LOG_ALERT”
  - poner la sensibilidad del módulo “sfportscan” a alta (“high”)
  - ponerlo en marcha: snort -c /etc/snort/snort.conf

Snort

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Módulo “sfportscan”**
  - usar nmap en “extb” para hacer un barrido de puertos sobre “www.example.net” y sobre “ftp.example.net”
  - identificar las alertas de snort en /var/log/auth.log
  - comprobar que no se detecta el barrido si se realiza desde “extb” sobre “exta” (ambas pertenecen a la red externa)
  - modificar la configuración de “sfportscan” para que
    - se ignoren los barridos sobre sobre “ftp.example.net”
    - sugerencia: editar /etc/snort/snort.conf
  - comprobar que el cambio es efectivo
    - nótese que las alertas sobre ICMP no son generadas por este módulo, sino por las reglas del fichero /etc/snort/rules/icmp.rules
    - nótese que las alertas sobre SNMP no son generadas por este módulo, sino por las reglas del fichero /etc/snort/rules/snmp.rules

Snort

VNIVERSITAT DE VALÈNCIA OpenCourseWare

- **Reglas**
  - obtener un exploit para FTP
    - sugerencia: usar la dirección web http://exploits.elhacker.net/index.php?act=view&id=49
  - compilarlo y ejecutarlo en “extb”
    - sugerencia: usar la línea de órdenes
      ./openf -u ftp -p “” -l 0x0804d8b8 -r 0xbffff9d4 -h ftp -o 21 -a 2 -b18
  - identificar las alertas de snort en /var/log/auth.log
  - comprobar que también se detecta el ataque si se realiza desde “extf”
  - modificar las reglas para que **no** se activen cuando el ataque se lleve a cabo desde “extf”
    - sugerencia: editar /etc/snort/rules/ftp.rules
  - comprobar que el cambio es efectivo