M11 SEGURETAT I ALTA DISPONIBILITAT

Administració de Sistemes Informàtics en Xarxa
IES de l'Ebre

UF2 – Seguretat Activa i Accés Remot

SNORT

SNORT IDS

Amb l'**augment dels atacs** cibernètics soferts durant els últims anys, les **tecnologies que poden mitigar** les pèrdues de les empreses afectades han guanyat importància.
Els **IDS son part d'aquestes tecnologies** de mitigació ja que la seva funció es detectar **comportaments anòmals dins de la nostra xarxa o intents d'accés** no desitjats.

Què és SNORT?

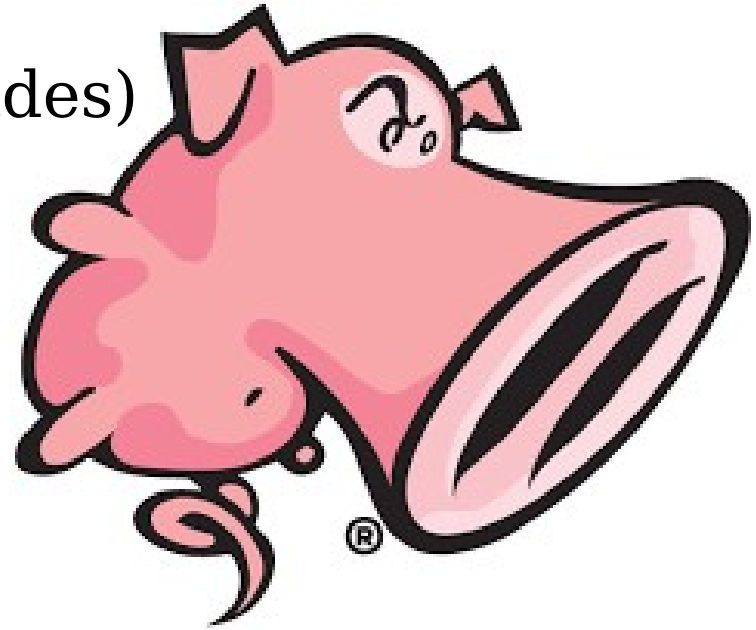
- Snort es un IDS que es capaç d'analitzar el tràfic de la nostra xarxa a temps real i reaccionar a patrons detectats.
- Això ens permet detectar connexions que no s'haurien de produir o atacs a la nostra xarxa.

Funcionament dels IDS

- Fan servir diferents eines:
  - Recollida de dades (packet **sniffing**)
  - Aplicació de **regles** per detectar riscos
  - Filtratge comparant els **patrons de tràfic** observats amb patrons d'atacs predefinits
  - Detecció **d'esdeveniments no esperats** a la xarxa
  - **Generació d'alarmes** per diferents mitjans
  - **Actuació sobre el tràfic** detectat

SNORT

- Modes de Funcionament:
  - Monitorització (sniffer)(-v capçaleres -d dades)
    - **`sudo snort -v -i eth0`**
    - **`sudo snort -vd -i eth0`**
  - Enregistrament de paquets de la Xarxa
    - **`sudo snort  -l ./log  -i eth0`**
  - HIDS (Host IDS) / NIDS (Network IDS)
    - **`sudo snort -A console -c /etc/snort/snort.conf -i eth0`**
    - Fa servir regles per monitorar



Ubicació dels IDS

- Cal situar-lo on **pugui capturar tot el tràfic** a monitorar
- La ubicació dependrà del seu us com a IDS/IPS
  - **IPS ha de situar-se inline** al mig de la comunicació
  - Cal anar amb compte que el processament de l'IPS no provoqui pèrdues de paquets
- De vegades es posa un **IDS abans** del *tallafocs* (monitora TOT el tràfic) i un altre **IDS/IPS després** (només gestiona tràfic que deixa passar el tallafocs)

SNORT Inline (IPS)

- Permet **blocar el tràfic entre 2 interfícies**
- El paràmetre -Q indica que ha de funcionar inline
- Diferents modes de funcionament
  - Alertes per consola
    - **`snort -d -A console -c snort.conf -i eth1:eth2 -Q`**
  - Enregistrar Alertes
    - **`snort -d -A full -c snort.conf -i eth1:eth2 -Q`**

Fitxers de configuració

- Arxiu de **configuració** es troba a
  - /etc/snort/snort.conf
- L'arxiu disposa d'un **índex**, ja que està dividit en **diferents seccions** per a que el seu us sigui més amigable.

```
#--------------------------------------------------
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
#--------------------------------------------------
```

Regles a Snort

- Amb la instal·lació **d'SNORT**, també s'instal·len un **conjunt de regles base**, que es poden utilitzar o modificar segons el nostre interès, i es poden trobar a:
  - **`/etc/snort/rules/`**
- Des de l'arxiu de configuració es poden **activar i desactivar** conjunts de regles.
  - Indica amb **`include`** els arxius de regles a carregar
    - **`include $RULE_PATH/local.rules`**
- **Regles**
  - **Arxius amb extensió .rules**
  - Situats a la carpeta **`/etc/snort/rules`**
- **Alertes**
  - **`/var/log/snort`**

Variables SNORT

Una de les parts més importants de la configuració d'SNORT, és configurar correctament les seves variables, per a que les regles es puguin aplicar correctament.

- Variables estàndard: var
  - **`var RULE_PATH /etc/snort/rules`**
- Variables de ports: portvar
  - **`portvar PORTS_A_MIRAR [22,80,1024:1050]`**
- Variables de xarxa: ipvar
  - **`ipvar HOME_NET 10.0.0.0/24`**
  - **`ipvar EXTERNAL_NET !$HOME_NET`**

Variables SNORT

Snort diposa d'una sèrie de variables globals amb les que podem configurar de forma senzilla l'estructura de la nostra xarxa.

- **HOME_NET**: Defineix el rang de la xarxa interna. Ajuda a decidir si el tràfic detectat ens afecta.
- **EXTERNAL_NET**: Defineix el rang fora de la xarxa interna.
  - Per a definir aquest rang se sol utilitzar !HOME_NET
- **SERVERS**: Es defineix on estan els servidors interns, i per defecte té el mateix valor que HOME_NET.
- **PORTS**: Ens ajuden a definir els ports de servei per als nostres servidors.
- **Llista Blanca**: Existeix una llista on indicar els dispositius exclosos de les regles.
- **Llista negra**: Es derfineixen els hosts que generen una alerta si son detectats a la xarxa.

Regles SNORT

Les regles d'Snort tenen un **format únic**, el que permet que qualsevol analista pugui revisar una regla, entendre què està buscant i el motiu de la seva creació.

Les regles es divideixen en dues parts: La **Capçalera**, amb els mateixos camps per a totes les regles i **els camps específics** que ens permeten ajustar més concretament què busquem.
A la Capçalera hi podem trobar:

- **Acció**: Indica que succeeix si la regla es dispara en analitzar un paquet, els seus valors possibles son:
  - **Alert**: s'envia una alerta i s'emmagatzema la informació a un arxiu de log.
  - **Log**: igual que l'anterior però no s'envia cap alerta.
  - **Pass**: S'ignora el paquet.
  - **Drop**: Es bloqueja el paquet i es guarda informació en l'arxiu de log.
  - **Reject**: Es bloqueja el pqeut i es força una errada en la comunicació.
  - **sdrop**: Es bloqueja el paquet, però no es deixa constaància al log.

Regles SNORT

- **Protocol:** tipus de protocol de comunicació.
- **Origen i destí:** Es pot utilitzar com a origen i destí una xarxa, una ip o una variable definida a l'arxiu de configuració. Si utilitzem el comodí ***any*** estem senyalant a qualsevol ip o xarxa.
- **Ports**: Podem utilitzar qualsevol port o utilitzar el compodí any.
- **Direcció**:
  - → la regla només actua en la direcció Origen cap a Destí
  - ↔ la regla actua en ambdues direccions.

Regles SNORT

Els **camps específics** ens permeten ajustar més concretament que busquem, es troben entre parèntesi i separats per ‘’;’’ . Hi podem trobar:

- **msg**: Missatge a mostrar en cas de que es dispari l’alerta
- **sid**: Dins dels paràmetres de la regla sempre hi ha d’existir almenys un identificador de regla (SID). Com a norma, les regles pròpies utilitzen un SID superior a 1000000.
- **rev**: Versió de la regla
- **classtype**: Permet donar info sobre el tipus d'atac
- **priority**: Permet indicar la importància de l'alerta
- **flow**: Permet indicar el flux de informació (connexions establertes TCP, connexions relacionades...)

Creant les nostres Regles SNORT

- **Objectiu**: Es necessari saber quin es l'objectiu de la regla:
  - Detectar un tipus de tràfic.
  - Bloquejar tràfic a llocs no permesos.
  - Crear perfiles de navegació
  - Buscar connexions de noves amenaces.
  - Detectar fugues d'informació.
- **Acció**: que volem que passi.
  - Informar al nostre SOC (Centre d'Operacions de Seguretat).
  - Escriure en un log amb informació.
  - Actuar sobre el Firewall.

Creant les nostres Regles SNORT

- **Abast**: Area d'actuaciñio de la regla.
  - Interna.
  - Externa.
  - Comunicació de fora a dins.
  - En Ambdós sentits.
  - Tota la xarxa o alguns equips.
- **Optimització**: Quina es la millor forma de buscar.
  - Valor Hexadecimals.
  - Cadenes de text.
  - Text en la URL.

Revisió d’alertes

- Els arxius de log de les alertes, així com la resta de logs generats per Snort, es troben per defecte a **`/var/log/snort`**

```
root@snortserver:~# ls /var/log/snort/
alert      snort.log.1583753168  snort.log.1583753802  snort.log.1583754293
snort.log  snort.log.1583753293  snort.log.1583753959
root@snortserver:~#
```

- Contingut d’un arxiu alert:

```
root@snortserver:~# cat /var/log/snort/alert
[**] [1:1917:6] SCAN UPnP service discover attempt [**]
[Classification: Detection of a Network Scan] [Priority: 3]
03/09-11:27:16.996030 00:50:56:C0:00:08 -> 01:00:5E:7F:FF:FA type:0x800 len:0xD8
192.168.134.1:65456 -> 239.255.255.250:1900 UDP TTL:1 TOS:0x0 ID:31325 IpLen:20 DgmLen:202
Len: 174
```

Exemples regles SNORT

```
alert tcp $HOME_NET 21 → any any (msg:"Error autenticació FTP"; content:"Login or password incorrect"; sid:1000003; rev:1;)
```

- Davant de qualsevol connexió des de la nostra xarxa, des del port 21 a qualsevol destí i qualsevol port.
- Aquestes connexions son les respostes que generen els servidors FTP de la nostra xarxa.
- Si dins d'aquestes connexions es troba el text "Login or password incorrect", genera l'alerta (acció).
- Aquesta regla doncs es dispara en cas de que es produeixi un error d'autenticació en algun dels nostres servidors FTP.

Exemples regles SNORT

```
Alert tcp $EXTERNAL_NET any → $HOME_NET 3306 (msg:"MYSQL show databases attempt"; flow: to_server, established; content:"|0F 00 00 00 03 | show databases"; sid:1000004; rev:1;)
```

- Alerta davant qualsevol connexió des de fora de la nostra xarxa, i que intenti connectar a un servidor MYSQL de la nostra xarxa.
- Aquesta connexió s'ha d'iniciar des de fora de la xarxa i ha d'haver rebut resposta del servidor (to_server, established).
- Si entre aquestes connexions es troba el text "show databases" després dels valors hexadecimals , és genera l'alerta.
- L'objectiu de la regla es detectar si des de l'exterior de la nostra xarxa s'està intentat mostrar una llista de les bases de dades d'un servidor intern.