ACRI
Almacén Colaborativo de Reglas de Intrusión

Víctor Barahona

Tecnologías de la Información

Universidad Autónoma de Madrid

Grupos de Trabajo RedIRIS 2005, Málaga

Antecedentes

- IDS en la UAM (Sep-2000)
- Problemática en el pasado
  - Ataques a Linux.
  - Gusanos.
  - Escaneos.
- Infierno en el presente
  - FXP
  - BootNets
  - SPAM

Pre-ACRI

- Las reglas oficiales no son suficientes.
- Generamos reglas propias.
- Otras instituciones hacen igual.
- Mismo problema, misma solución.
- Nace ACRI.

ACRI

- Almacén Colaborativo de Reglas de Intrusión.

  http://www.rediris.es/cert/proyectos/acri.es.html
- Reglas de intrusión de IDS.
- De momento solo Snort.
- Otros IDS bajo demanda.
- Apartado especial para Nmap.

Como contribuir

- Opción 1: BSCW (será Wiki)

  http://cvu.rediris.es/pub/bscw.cgi/0/588044

- Opción 2: Formulario web

  http://www.rediris.es/cgi-bin/sugerencias.pl?contact=acriadmin

- Opción 3: Correo personal (mejor no)

  victor.barahona@uam.es

Formato reglas Snort

- Origen, destino y puerto:

```
alert tcp any any -> $HOME_NET !21
```

- Mensaje de alerta:

```
msg: "ACRI: Posible FXP-STOR_ -
  maquina comprometida";
```

- Patrón:

```
flow: established; content:"STOR ";
  depth:5; classtype:successful-
  admin; sid:10031; rev:2;
```

Reglas Actuales

- Snort:
  - Detección FTPs Warez (FXP)
  - Detección Radmin (Control remoto)
- Nmap:
  - Detección de Radmin.
- Proximamente:
  - Detección Hacker Defender (Snort & Nmap)

Enlaces

- ACRI: http://www.rediris.es/cert/proyectos/acri.es.html
- BSCW ACRI: http://cvu.rediris.es/pub/bscw.cgi/0/588044
- Snort: http://www.snort.org/
- Como hacer reglas en Snort y sin perder el juicio: http://www.snort.org/docs/snort_htmanuals/htmanual_233/node16.html
- Nmap: http://www.insecure.org/nmap/
- Nmap version scan: http://www.insecure.org/nmap/versionscan.html

¿PREGUNTAS?