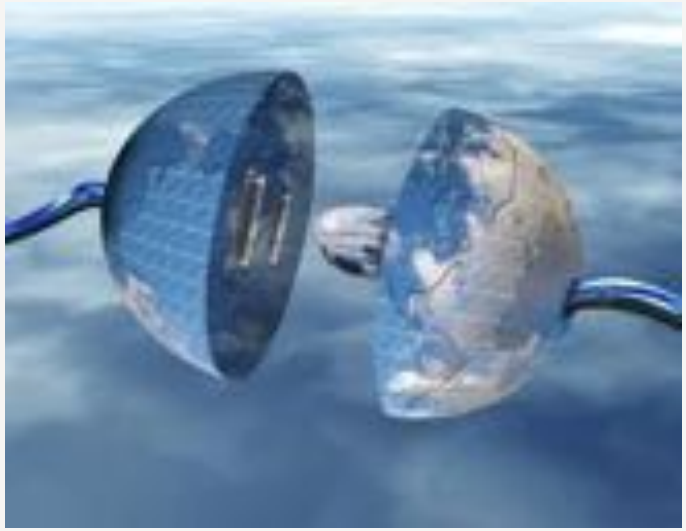

UNAM
CERT
Congreso Seguridad en Cómputo 2010
TELESCOPIO DE SEGURIDAD
DE LA UNAM
http://congreso.seguridad.unam.mx

TELESCOPIOS DE RED

Mecanismos de **detección y monitoreo** de tendencias de tráfico de red malicioso basado en:

- ✓ El despliegue de sensores distribuidos a lo largo de un entorno de red.
- ✓ Análisis de datos de varios dispositivos de conectividad



OBJETIVO DE UN TELESCOPIO DE RED

Detectar tráfico malicioso y **monitorear la actividad** general de la red combinando diversas tecnologías como:

- IDS
- Honeypots
- Darknets
- Flow server

Sin embargo, pueden ir más allá que los sistemas convencionales de monitoreo.

CARACTERÍSTICAS

- ✓ Modelo de detección distribuido
- ✓ Entornos de gran escala
- ✓ **Gran cantidad de información** recopilada, procesada y almacenada
- ✓ Altamente demandante en recursos de hardware
- ✓ Monitores de las tendencias de tráfico en espacios grandes de Internet: Identificación de anomalías a nivel global

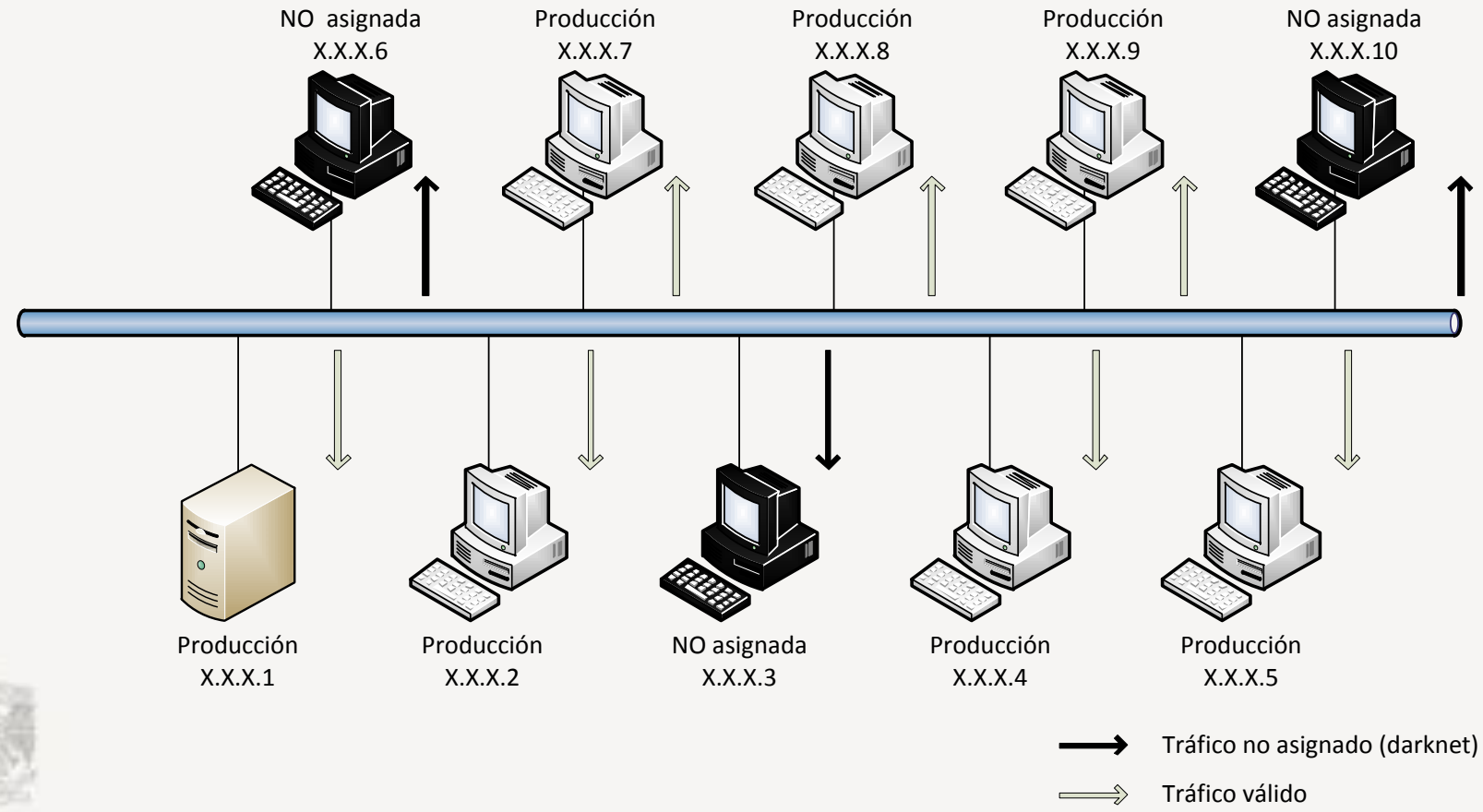
FUENTES DE INFORMACIÓN

- ✓ Darknet-UNAM (sobre 2 segmentos clase B)
- ✓ Sensores de SPAM
- ✓ PSTM
- ✓ Core UNAM*

UNAM CERT

DARKNETS

Equipos que utilizan direcciones IP o segmentos de red que **no están asignados** dentro de un entorno de red.



TRÁFICO DE RED "NO ASIGNADO"

En un entorno ideal este tráfico **no debería existir**, por lo tanto todo el tráfico en una darknet es **potencialmente anómalo**.

CARACTERÍSTICAS DE UNA DARKNET

- Utiliza direcciones IP no asignadas.
- Todo el tráfico en la darknet es **potencialmente sospechoso.**
- Baja probabilidad de falsos positivos.
- Puede detectar tráfico malicioso o anomalías en la configuración de dispositivos.

CARACTERÍSTICAS DE UNA DARKNET

- Ad-hoc a tecnologías honeypot:
  - Muestras de tráfico malicioso
  - **Muestras de malware**

- Generación de información estadística importante sobre el tráfico de red.

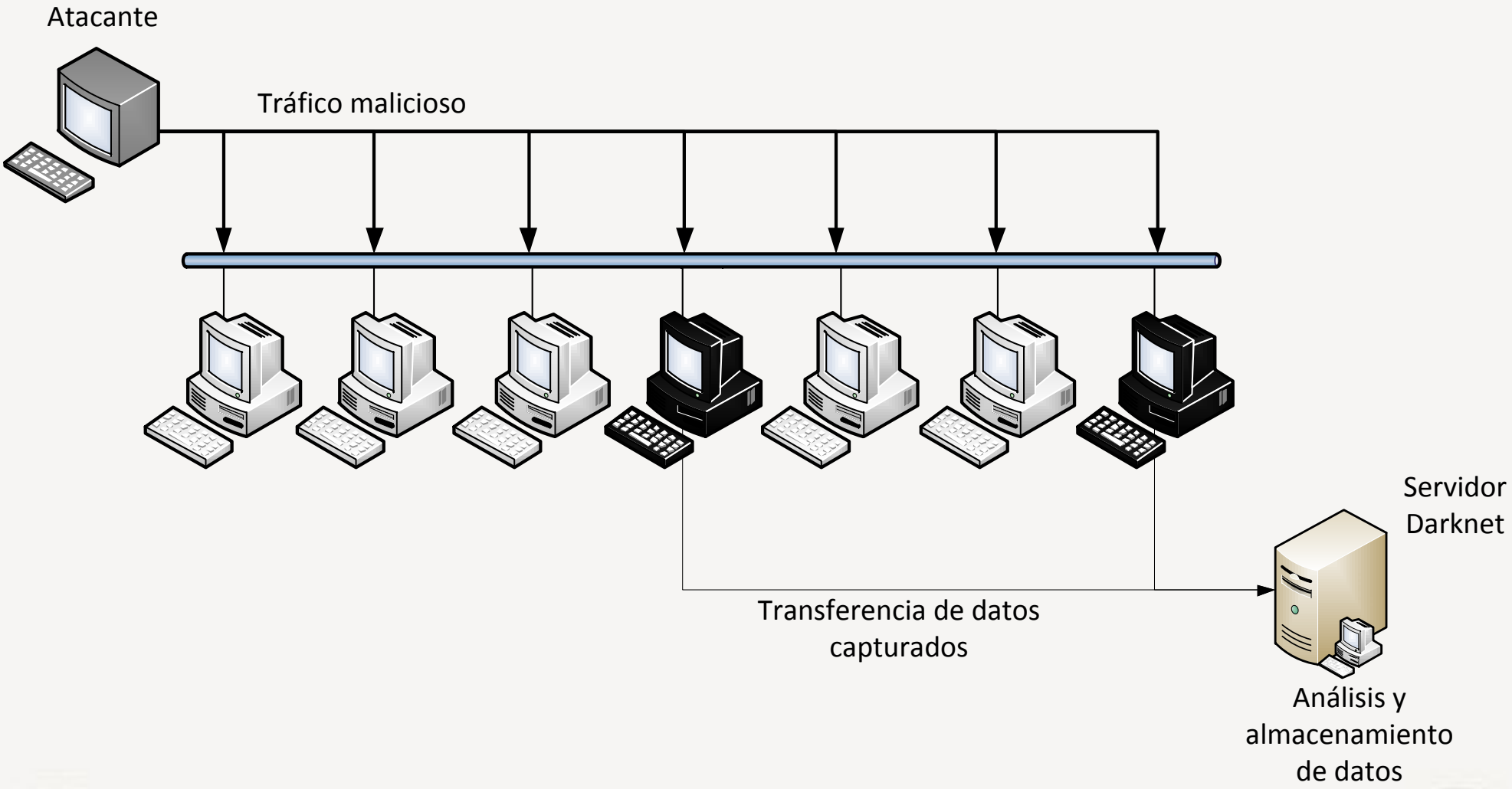
- **Inversión de direcciones IP** de la red para su funcionamiento.

ESQUEMA DE FUNCIONAMIENTO

Depende de sus objetivos, pero el concepto general toma en cuenta aspectos como:

- Tecnologías implementadas
  - **Honeypots, IDS, análisis de flujos**, etc.
- Capacidad y complejidad de interacción
  - **Simulación de servicios, equipos reales, etc.**
- Capacidad y complejidad de análisis
- Campo de acción

ESQUEMA DE FUNCIONAMIENTO



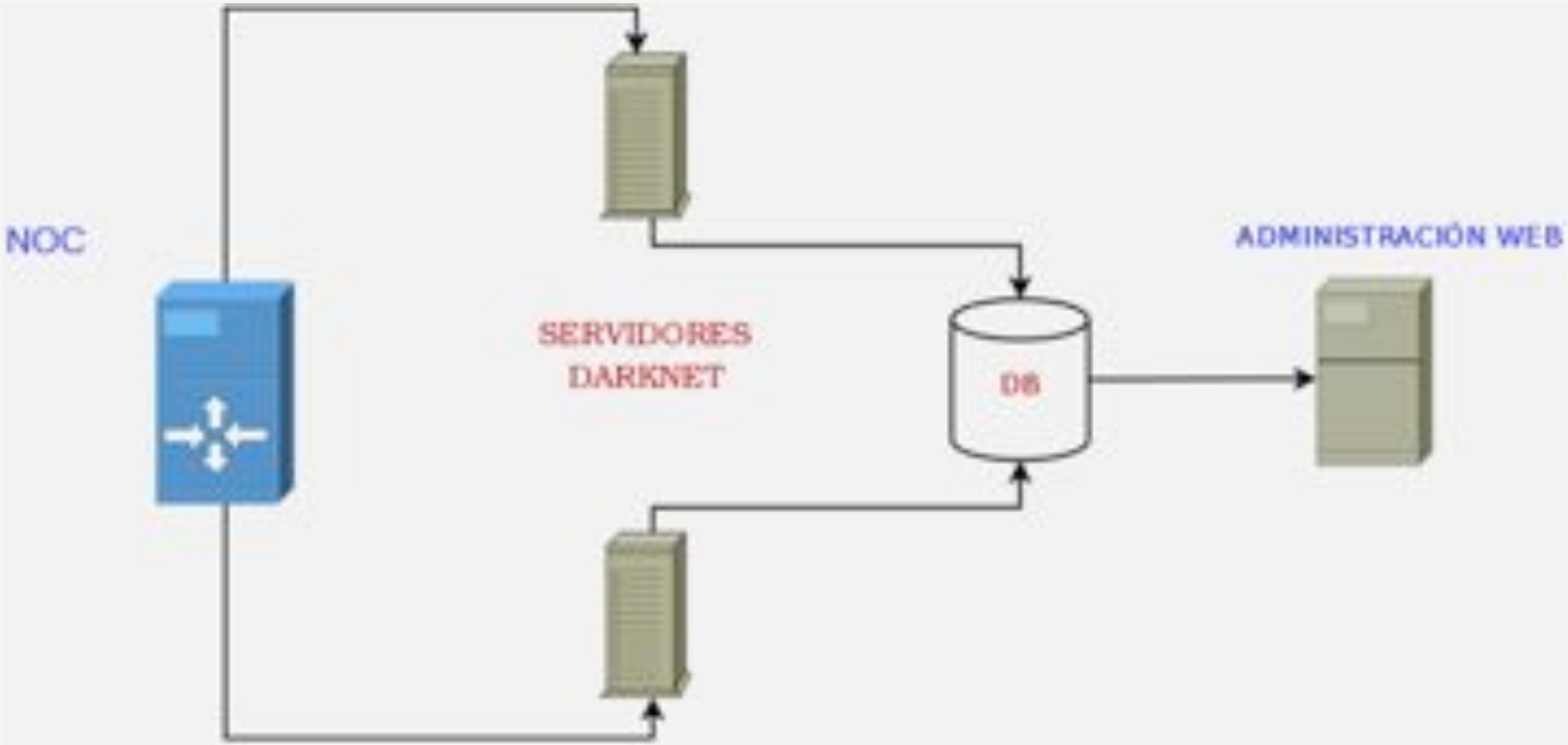
TECNOLOGÍAS UTILIZADAS

TECNOLOGÍA	OBJETIVOS	EJEMPLOS
Honeypot	Simulación de servicios, captura de malware y control de tráfico	Dionaea, honeytrap, honeyd, kojoney, kippo, argos, honeybot, glastopf, google hack honeypot, honeywall, etc.
IDS	Detección de tráfico malicioso mediante firmas	Snort, Sguil, BASE, Suricata, Ossec HIDS, Prelude Hybrid IDS, Aide,
Análisis de flujos	Análisis de flujos y generación de estadísticas de tráfico	Argus, Netflow
Análisis de tráfico y protocolos	Análisis del tráfico de red: paquetes, protocolos, aplicaciones, etc.	Tcpdump, Wireshark, Tshark, Snort, Windump, ntop, etc.
Análisis de log	Análisis de logs de aplicaciones y sistema	Scripts en perl, python, shell, utilerías Unix, Splunk, etc.


ESQUEMA DE MONITOREO

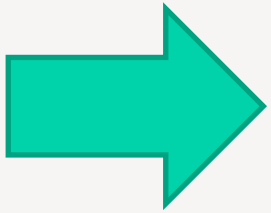
Departamendo de redes UNAM
Redireccionamiento de tráfico cuyo destino son IP's "no asignadas"

SERVIDORES DARKNET


NOC
SERVIDORES
DARKNET
DB
ADMINISTRACIÓN WEB

¿Cómo trabaja?

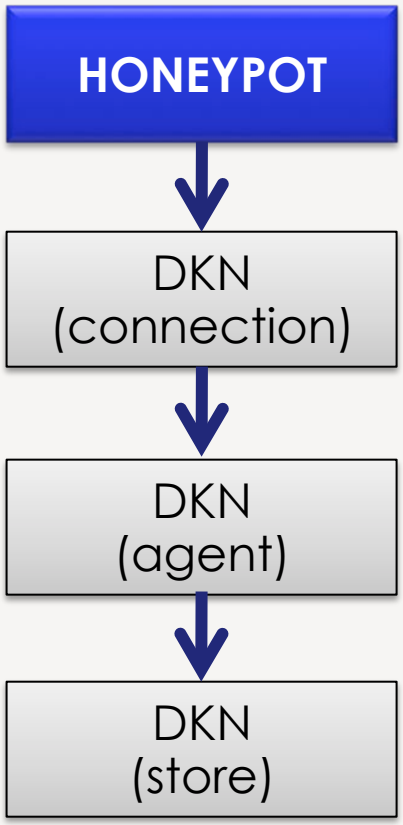
- **4 MÓDULOS**
  - *Honeypot*
  - *Flujos (STA submod)*
  - *IDS(STA submod)*
  - *LOGS**



- Herramientas de análisis
  - *Perl scripts*
  - *Shell scripts*
  - *Postgresql DB*
  - *Web-based management system (under construction)*

FUNCIONAMIENTO

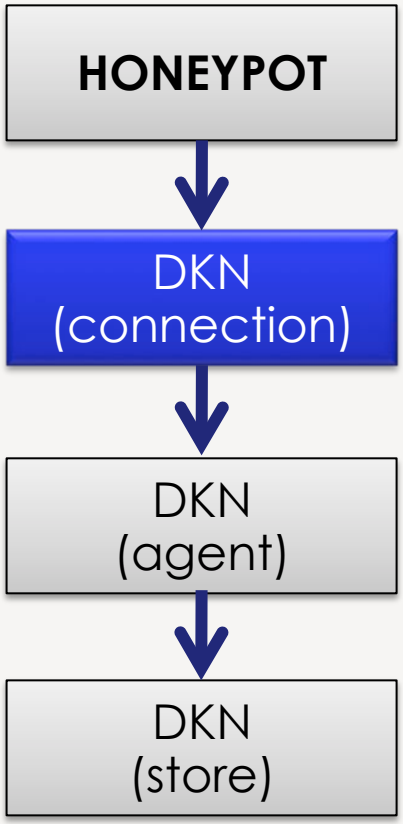
MODULO HONEYPOT



Ajuste al sofware de emulación de servicios para un procesamiento en tiempo real. El software honeypot maneja las conexiones y envía información de la conexión al módulo DKN…

FUNCIONAMIENTO

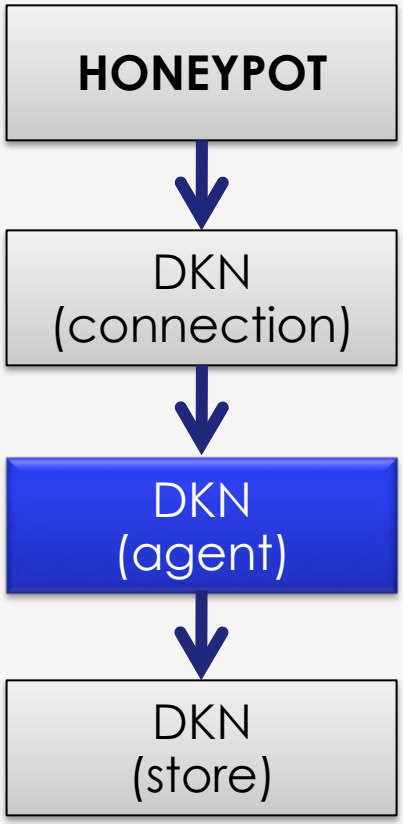
MODULO HONEYPOT



A partir de la información de la conexión, se clasifica el evento según reglas predefinidas. Además detecta si es una simple conexión y algún tipo de escaneo o barrido de puertos.

FUNCIONAMIENTO

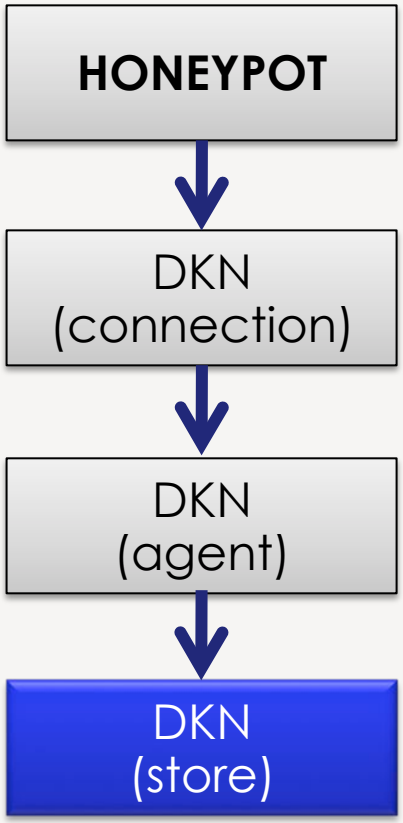
MODULO HONEYPOT



Analiza el payload capturado y genera un incidente conjuntando información del reporte de análisis y el propio payload.

FUNCIONAMIENTO

MODULO HONEYPOT



Almacena la información en la base de datos del Telescopio de Seguridad

Un vistazo…

Ejemplo de un incidente

dkn|**163**|tcp|**X.Y.Z.W**||||||**1271362670|1271362370|SQL WORM 1433|/data/dkn/events_connections/tcp-X.Y.Z.W-1433-1271362370.det|/dkn/events_connections/tcp-X.Y.Z.W-1433-1271362370.tgz|**

Un vistazo…

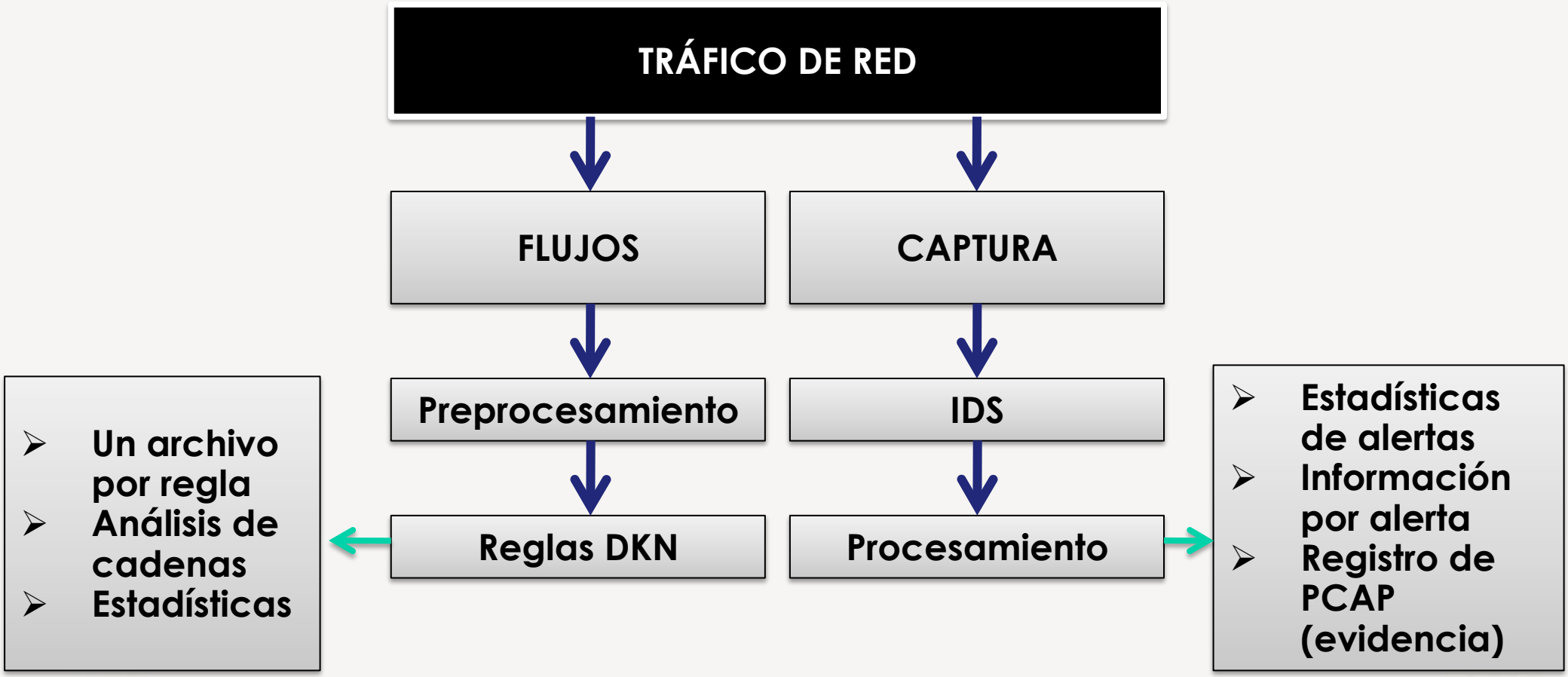
Ejemplo de un .det file:
/dkn/events_connections/udp-A.B.C.D-1434-1271361727.det

TS SRCIP&SPORT SRCIP&DPORT MD5 PAYLOAD STRINGS(Rules)

```
1271362370|192.168.1.14|3518|192.168.0.32|1433||||||
1271362378|192.168.1.14|4368|192.168.0.32|1433|285850d4aff8df0e2839ecd6bca68011|||||-(0)|
1271362378|192.168.1.14|4374|192.168.0.39|1433|36dc32801e14fbcdd23436759389f4d4|||||-(0)|
1271362378|192.168.1.14|4394|192.168.0.142|1433|cfd5cff90daae596afab961957826d3c|||||-(0)|
1271362378|192.168.1.14|4432|192.168.0.212|1433|b27e34b029eafa04e44fa4af416ed8cd|||||-(0)|
1271362378|192.168.1.14|4442|192.168.0.250|1433|910729ad1d2de99522b537b05ffd00a2|||||-(0)|
1271362378|192.168.1.14|4446|192.168.0.251|1433|ab1336d70e64574b411b6a133129c557|||||-(0)|
…
…
```

FUNCIONAMIENTO

MODULO STA (Análisis de tráfico estructurado)



PROCESANDO LA INFORMACIÓN

Los objetivos del procesamiento son:

- ✓ Clasificación de la información
- ✓ Formato de la información
- ✓ Detección de falsos positivos

PROCESANDO LA INFORMACIÓN

Durante la fase de pruebas se utilizaron servidores:

- ✓ **Dual-Xeon 3.2Ghz 2GB RAM**

Con aproximadamente 70,000 direcciones IP

- ✓**Utilizando 90% de recursos**

UNAM CERT

¿QUÉ PODEMOS DETECTAR?

- ✓ Escaneos
- ✓ Propagación de gusanos, bots, virus
- ✓ Ataques de fuerza bruta
- ✓ Ataques específicos que utilicen técnicas de spoofing
- ✓ Fallas en la configuración de dispositivos
- ✓ Identificación de patrones de botnets o redes P2P
- ✓ Patrones anormales de tráfico
- ✓ Nuevas tendencias de ataques
- ✓ Entre otros

GENERANDO ESTADÍSTICAS

Durante la fase de pruebas:

- Se reciben, manejan, procesan y registran aproximadamente **2.5 millones de conexiones diariamente.**

- Alrededor de **5Gb** de bitácoras diariamente.

- Miles de direcciones IP **internas y externas** a RedUNAM generando tráfico malicioso.

TRABAJO FUTURO

- Mejorar la eficiencia
- Capacidades adicionales de detección
- Incorporación de otras herramientas

✓ Conjuntarlo con la información del CORE-UNAM

✓ Posible implementación con ISP's del país y en otras Universidades

PROYECTOS SIMILARES

- Internet Motion Sensor (Arbor & UMICH)
- CAIDA (UCSD Network Telescope)
- Team Cymru: The Darknet Project
- Internet Background Noise (IBN)
- The IUCC/IDC Internet Telescope
- Isink (Internet sink)

OTROS PROYECTOS UNAM-CERT

- Sensores de tráfico malicioso (PSTM).
- Sensores de Correo Spam.
- Proyecto Malware-UNAM.
- Sandnet.
- Intercambio de información con otros organismos internacionales.

¿Preguntas?

Congreso Seguridad en Cómputo 2010

http://congreso.seguridad.unam.mx

José Roberto Sánchez Soledad
rsanchez@seguridad.unam.mx

Javier Ulises Santillán Arenas
jsantillan@seguridad.unam.mx

Dirección de contacto
Ciudad Universitaria
UNAM