Utilizando Inteligencia Artificial para la Detección de Escaneos de Puertos

Andrés Felipe Arboleda
Charles Edward Bedón

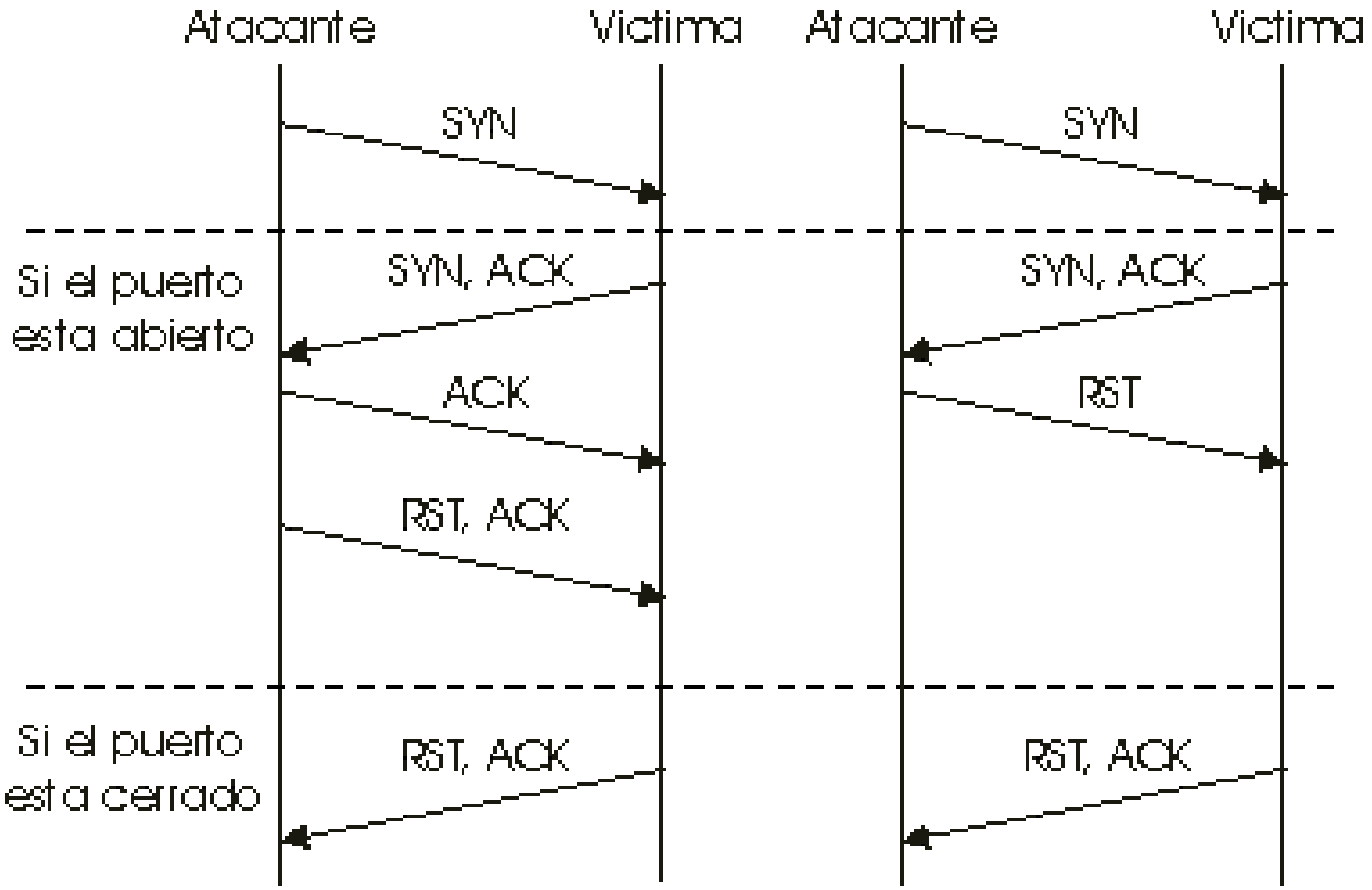
Director:
Siler Amador Donado

Universidad del Cauca

Anatomía de una Intrusión

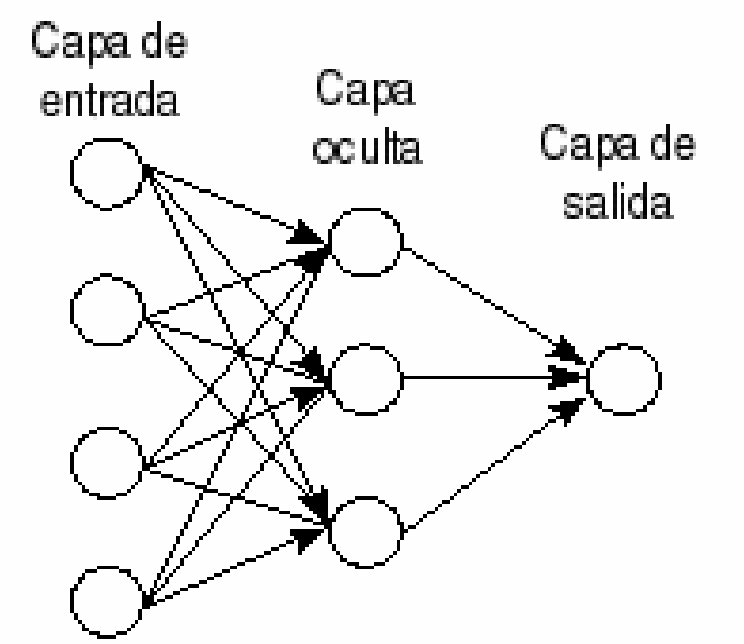
- Exploración del Contexto.
- Exploración de Red (Escaneo de puertos).
- Análisis de vulnerabilidades y planeamiento de estrategias.
- Explotación de vulnerabilidades.
- Implantación de puertas traseras.

Escaneo de puertos



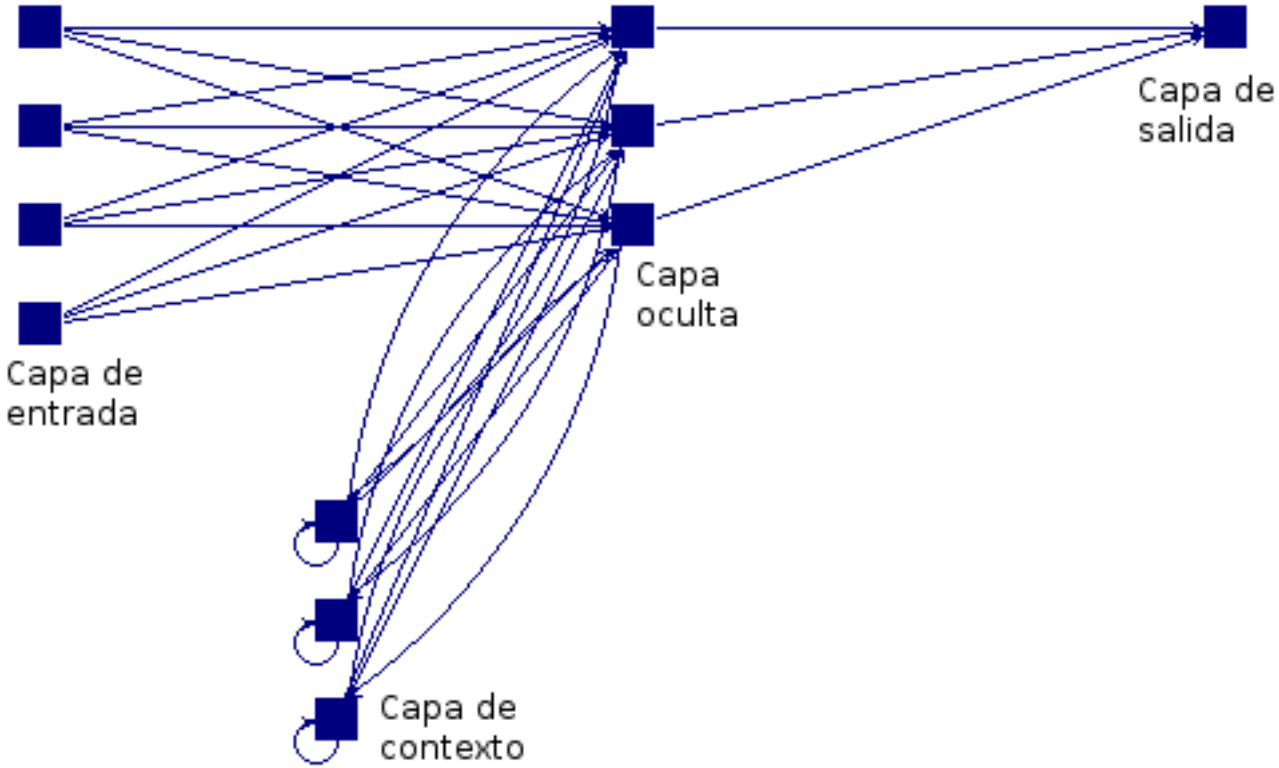
Redes Neuronales

- El Perceptrón Multicapa o MLP (*Multi-Layer Perceptron*)

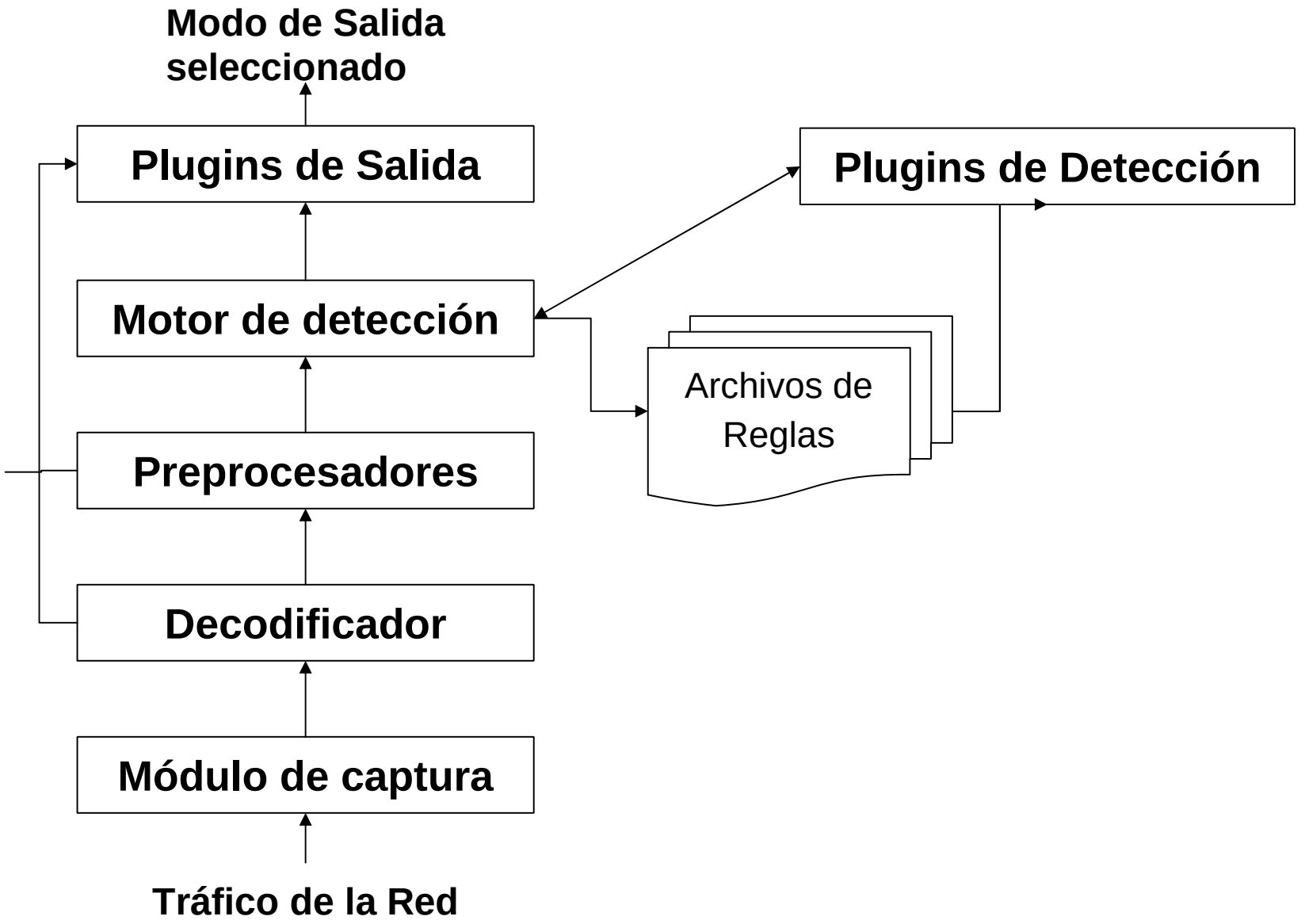


Redes Neuronales

- Red Neuronal Elman
  - Tiene en cuenta el **tiempo**



Módulos de Snort



Snort Frente a portscans

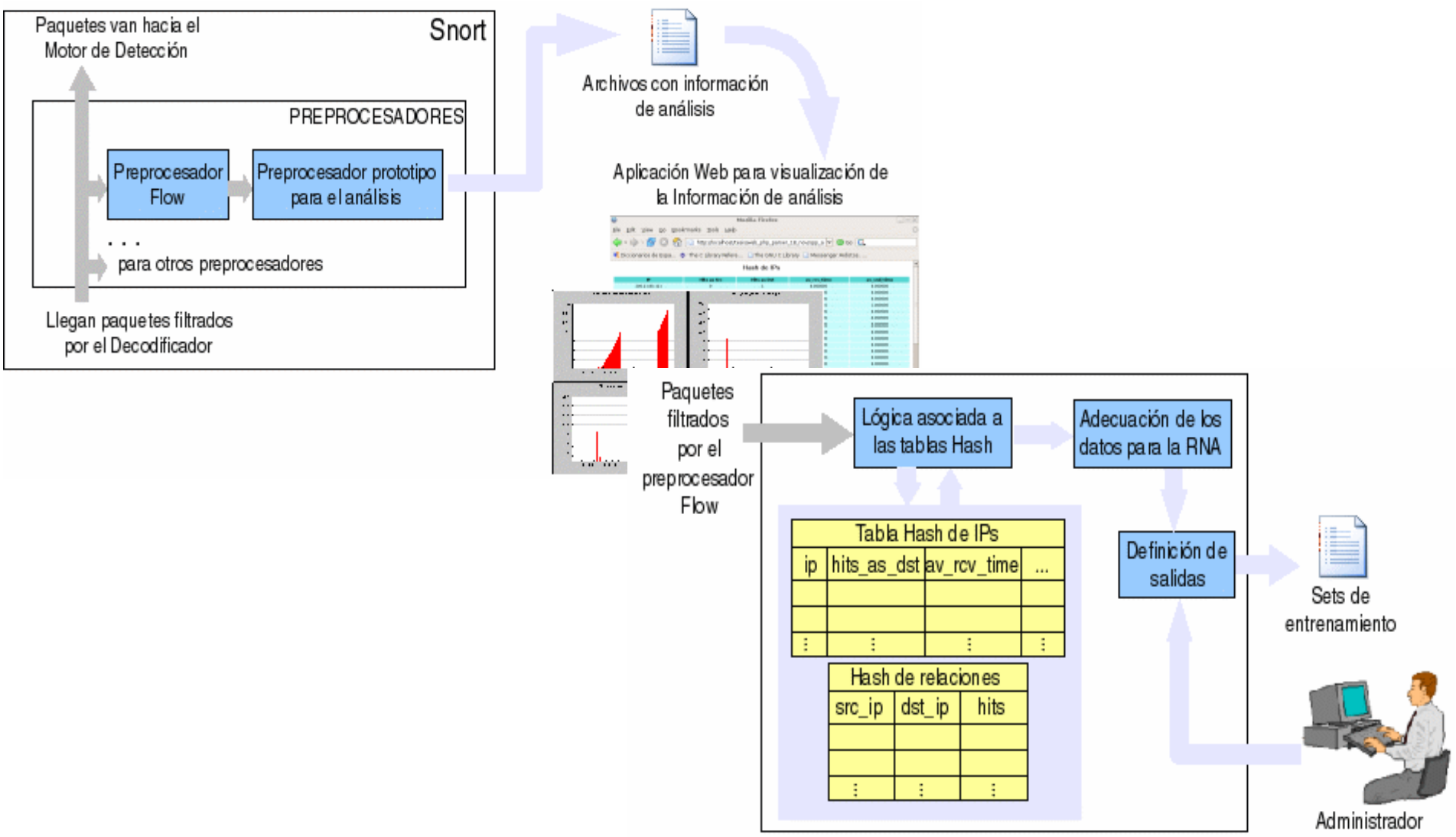
- Preprocesadores sfPortscan y portscan2 (basados en respuestas negativas y peticiones de conexión respectivamente).

- Reglas en scan.rules

SPP Portscan AI

- Se apoya en el preprocesador spp_flow, nativo en Snort.
- Uno de los conceptos principales es el de *flow*, que consiste en una combinación singular de IP de origen, puerto de origen, IP de destino y puerto de destino.
- Para el caso del portscanAI sirve para determinar los intentos de conexión de un host a otro.

Flujo de Datos



Parámetros Analizados

- **hits_as_dst** (*hits as destination* – *hits* como destino): número de paquetes de inicio de conexión (*flows*) como destino.
- **hits_as_src** (*hits as source* – *hits* como origen): número de paquetes de inicio de conexión (*flows*) como origen
- **av_rcv_time** (*average receive time* – tiempo promedio de recepción)
- **av_snd_time** (*average send time* – tiempo promedio de envío):
- **negative_resp** (*negative responses* – respuestas negativas)
- **rel_hits** (*relation hits* – *hits* de relación): es el número de peticiones de inicio de conexión que se realizan entre dos host dados.

Resultados 1/2

	sfPortscan	**PortscanAI**
Condiciones iniciales	0.3 MB	0.1 MB
Con tráfico (luego de 1676 paquetes)	0.2 MB	< 0.1 MB

	sfPortscan	**PortscanAI**	
		MLP	**Elman**
Escaneos detectados	2	5	1
Falsas alarmas	0	4	1
% de paquetes perdidos		0.057 %	0.045 %

Resultados 2/2

No. DE FALSOS POSITIVOS (FALSAS ALARMAS)			
	sfPortscan	PortscanAI	
		MLP	Elman
1. Uno a uno (TCP SYN)	0	0	0
2. Uno a muchos (TCP SYN)	0	0	0
3. Uno a uno (decoy)	0	0	0
4. Uno a uno (TCP Connect)	0	0	0
5. Uno a muchos (TCP Connect)	0	0	0

No. DE FALSOS NEGATIVOS (ATAQUES SIN DETECTAR)			
	sfPortscan	PortscanAI	
		MLP	Elman
1. Uno a uno (TCP SYN)	0	0	0
2. Uno a muchos (TCP SYN)	1	0	0
3. Uno a uno (decoy)	7	0	0
4. Uno a uno (TCP Connect)	0	0	0
5. Uno a muchos (TCP Connect)	1	0	0

Gracias

- Pagina del proyecto:
- http://afrodita.unicauca.edu.co/~aarboleda/snort_ai.htm

Andrés Felipe Arboleda
Ingeniero en Electrónica y Telecomunicaciones
Universidad del Cauca