Herramienta para la generación de escenarios de apoyo a la docencia de la seguridad en redes

Enrique de la Hoz, Iván Marsá-Maestre, Miguel A. López-Carmona y María Teresa López-Merayo

(Universidad de Alcalá)

Grupos de Trabajo de RedIRIS, Córdoba, Noviembre 2010

Universidad de Alcalá

Departamento de Automática

Área de Ingeniería Telemática

Un poco de contexto
Docencia de Seguridad

- Importancia de la seguridad de redes y sistemas
- Necesidad de fortalizar esta materia en los currículos
- Dos bloques fundamentales
  - Seguridad de la Información
  - Seguridad de Sistemas
- La docencia de seguridad de sistemas requiere de una infraestructura adecuada

Un poco de contexto

Seguridad de Sistemas

- Necesidad de disponer de un entorno adecuado
- Las prácticas deben ser cercanas a los entornos reales
- Similares al ejercicio de la profesión
- Problemas en el despliegue de los mismos

Docencia basada en Escenarios

Desafíos

- Necesidad de proteger las redes del campus
  - Aislamiento de los laboratorios
- Dificultad para simular entornos de red de nivel empresarial
  - VPN, Radius, WiFi..
- Dificultad para la asignación de recursos para las distintas prácticas
  - Soporte para más de un proyecto simultáneamente
  - Soporte para distintas topologías de red

Docencia basada en escenarios

Desafíos

- Recursos necesarios para las diferentes prácticas
  - Que sean reproducibles por los alumnos
- Empleo de tecnologías acordes al estado del arte
  - Escalabilidad y extensibilidad
- Sobrecarga debida a la configuración y mantenimiento del laboratorio para distintas prácticas o proyectos
  - Agilizar las tareas de despliegue y mantenimiento

Alternativas Existentes

Laboratorios Hardware

- Utilización de hardware real
  - Incluyendo componentes de red reales
- Mayor grado de realismo
- Problemas
  - Coste
  - Tiempo de instalación despliegue y configuración
  - Reproducibilidad por el estudiante

Alternativas Existentes

Virtualización Descentralizada

- Empleo de máquinas virtuales para el despliegue del escenario
- Mayor grado de robustez y estabilidad
- Empleando uno o varios equipos para recrear el escenario
- Cierta flexibilidad en el despliegue de topología de red
  - VDE: Virtual Distributed Ethernet

Alternativas Existentes

Virtualización Centralizada

- Un servidor central alberga las máquinas virtuales
- Las redes se simulan en el mismo servidor
- Posibilidad de emplear un cluster en lugar del servidor
- Posibilidad de acceso remoto
- Inconvenientes:
  - Único punto de fallo
  - Necesidad de conectividad

NEMESIS

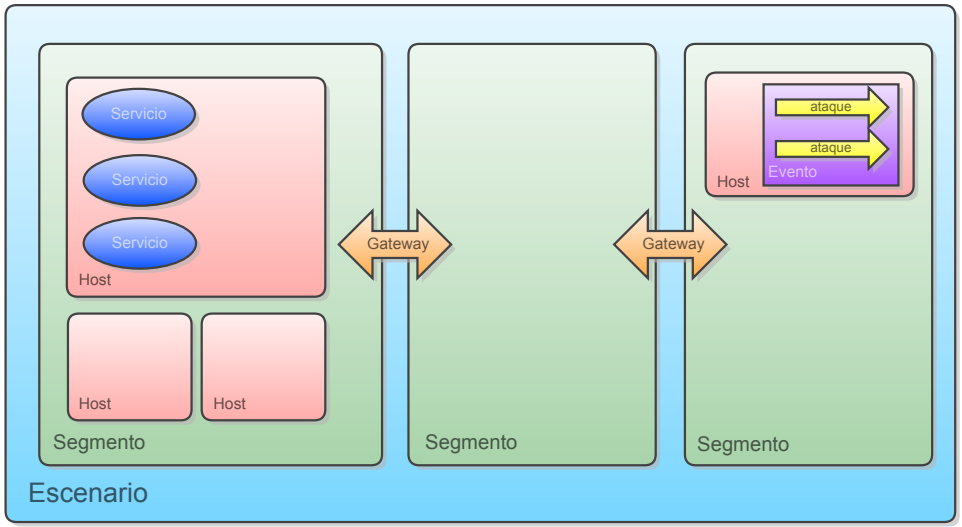
Requisitos de Diseño

- Herramienta para la generación de escenarios de apoyo a la docencia de la seguridad
- Orientada al trabajo en asignaturas de Gradoo
  - Tanto en clases magistrales como laboratorios
- Que permita reproducir todas las prácticas anteriores

NEMESIS

Elementos fundamentales

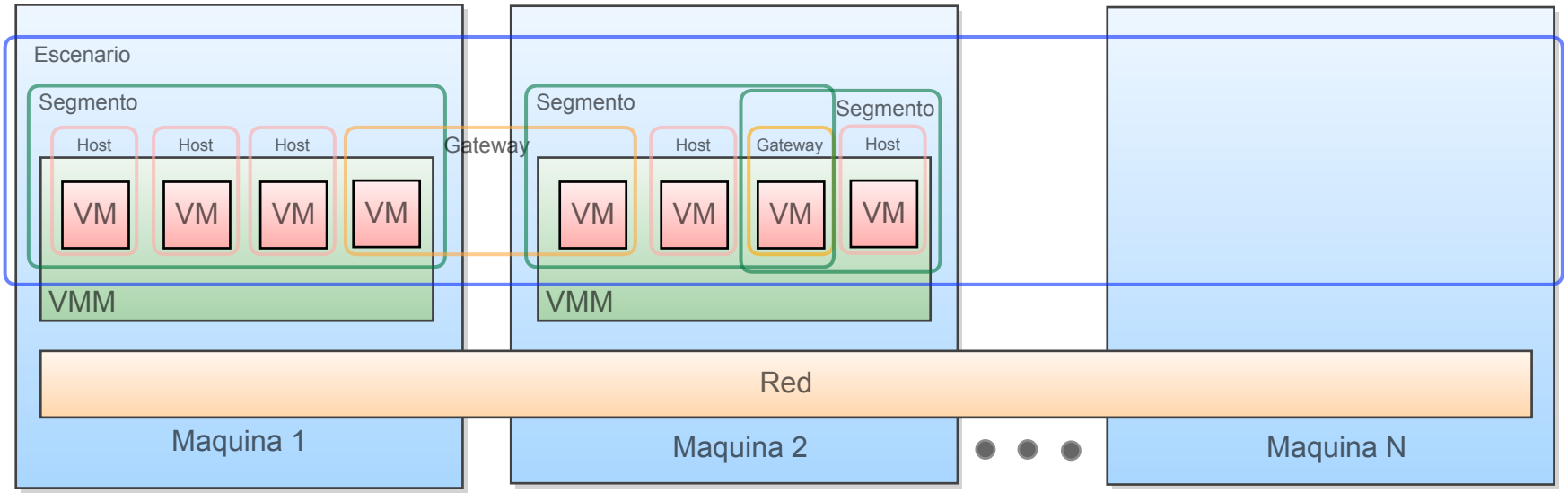
- Host:
  - Utilización de plantillas
- Segmento de red
- Gateway
- Servicio
- Evento
- Ataque



NEMESIS

Arquitectura Distribuida de Máquina Virtuales

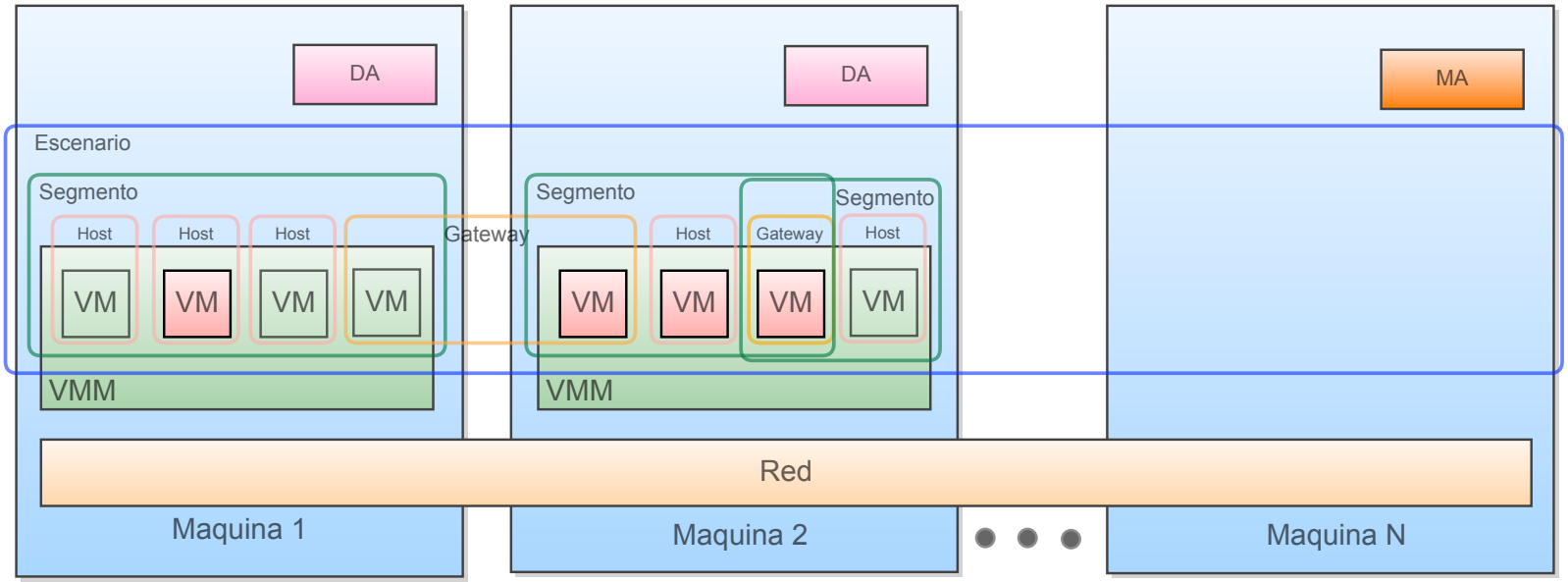
- Uso de máquinas virtuales
  - Versatilidad
- Cada máquina física albergará uno o varios segmentos de red



NEMESIS

Arquitectura Distribuida de Máquina Virtuales

- Los segmentos de red se conectarán entre sí por medio de gateways también virtuales
  - Para la plataforma la distribución es transparente
- Agentes de gestión y despliegue



NEMESIS

Descripción de los Escenarios

- Empleando XML
- Parseado por el MA que contacta con los DA de las máquina involucradas:
  - El DA arranca las VMs y prepara las topologías de red

```
<segment label=interna, host=172.29.16.21>
    <host ip=10.0.10.5, template=windows/>
    <host ip=10.0.10.6, template=windows/>
     <host ip=10.0.10.7, template=windows>
            <conf file=sysadmin.xml/>
           <display host=172.29.16.22/>
                    </host>
  <gateway template=firewall ipin=10.0.10.1
                  ipout=10.0.11.2 linkto=dmz>
    <ipchains rule="allow tcp 80 outbound"/>
    <ipchains rule="allow tcp 25 outbound"/>
    <ipchains rule="allow tcp 22 outbound"/>
                  </gateway>
                </segment>
```

NEMESIS

Descripción de los Escenarios

- Empleando XML
- Parseado por el MA que contacta con los DA de las máquina involucradas:
  - El DA arranca las VMs y prepara las topologías de red

```
<segment label=interna, host=172.29.16.21>
    <host ip=10.0.10.5, template=windows/>
    <host ip=10.0.10.6, template=windows/>
    <host ip=10.0.10.7, template=windows>
        <conf file=sysadmin.xml/>
        <display host=172.29.16.22/>
        </host>
```

NEMESIS

Descripción de los Escenarios (II)

- Host
  - ip, template
- Segment
  - Host
- Gateway
  - firewall

```
<segment label=internet, host=172.29.16.19>
  <host ip=213.18.21.7, template=windows/>
    <host ip=213.18.21.70, template=dvl>
                </host>
 <gateway template=firewall ipin=10.0.10.1
                ipout=10.0.11.2 linkto=dmz>
   <ipchains rule="allow tcp 80 outbound"/>
   <ipchains rule="allow tcp 25 outbound"/>
   <ipchains rule="allow tcp 22 outbound"/>
              </gateway>
            </segment>
```

NEMESIS

Descripción de los Escenarios. Interactividad

- Event
- Attack
- Display

```
<segment label=internet, host=172.29.16.19>
    <host ip=213.18.21.7, template=windows
        <display host="172.29.16.22"/>
            <host/>
    <host ip=213.18.21.70, template=dvl>
            <event at=5m16s>
        <attack template=portscan>
            <param name="ip"
             value="213.18.21.77"/>
        <param name="range"
              value="1..1024"/>
          </attack>
        </event>
      </host>
<gateway template=plain linkto=dmz/>
</segment>
```

NEMESIS

Creación de prácticas con NEMESIS

- Desde el punto de vista del atacante:
- Desde el punto de vista del defensor:

NEMESIS
Demo

- NEMESIS:
  - http://www.youtube.com/watch?v=Kh0HF2Nw-2w
- Ataques en NEMESIS:
  - http://www.youtube.com/watch?v=7s55WIYbLKE
  - http://www.youtube.com/watch?v=yewLtV0gnyE

Conclusiones

- NEMESIS es una herramienta modular, distribuida y extensible para la creación de escenarios
  - El empleo de virtualización dota a la herramienta de flexibilidad y escalabilidad
  - El empleo de XML y plantillas favorece la extensibilidad
- Trabajos futuros:
  - Empleo de xen como herramienta subyacente
  - Utilización de NEMESIS en entornos virtuales como un servicio en la nube