Attacker-centric risk assessment and metrics

Ezequiel Gutesman - Fernando Miranda

Corelabs
Core Security Technologies

November 3, 2009

Agenda

1. Evolución en las organizaciones
2. La visión del atacante
3. Penetration test como práctica de seguridad
4. Simulaciones
5. Definiendo riesgo: Centrados en el atacante
6. Midiendo
7. Conclusiones

Investigación en curso

- Attack Planning - últimos años
- Simulaciones de ataque
- Métricas para análisis de riesgo
- Todo lo anterior, para redes de gran escala

Nos olvidaremos por un momento de la definición usual de riesgo ($p_{evento} * impacto$) para concentrarnos en **priorizar** y **analizar** amenazas, utilizando esta definición para calcular métricas que nos permitan **actuar**.

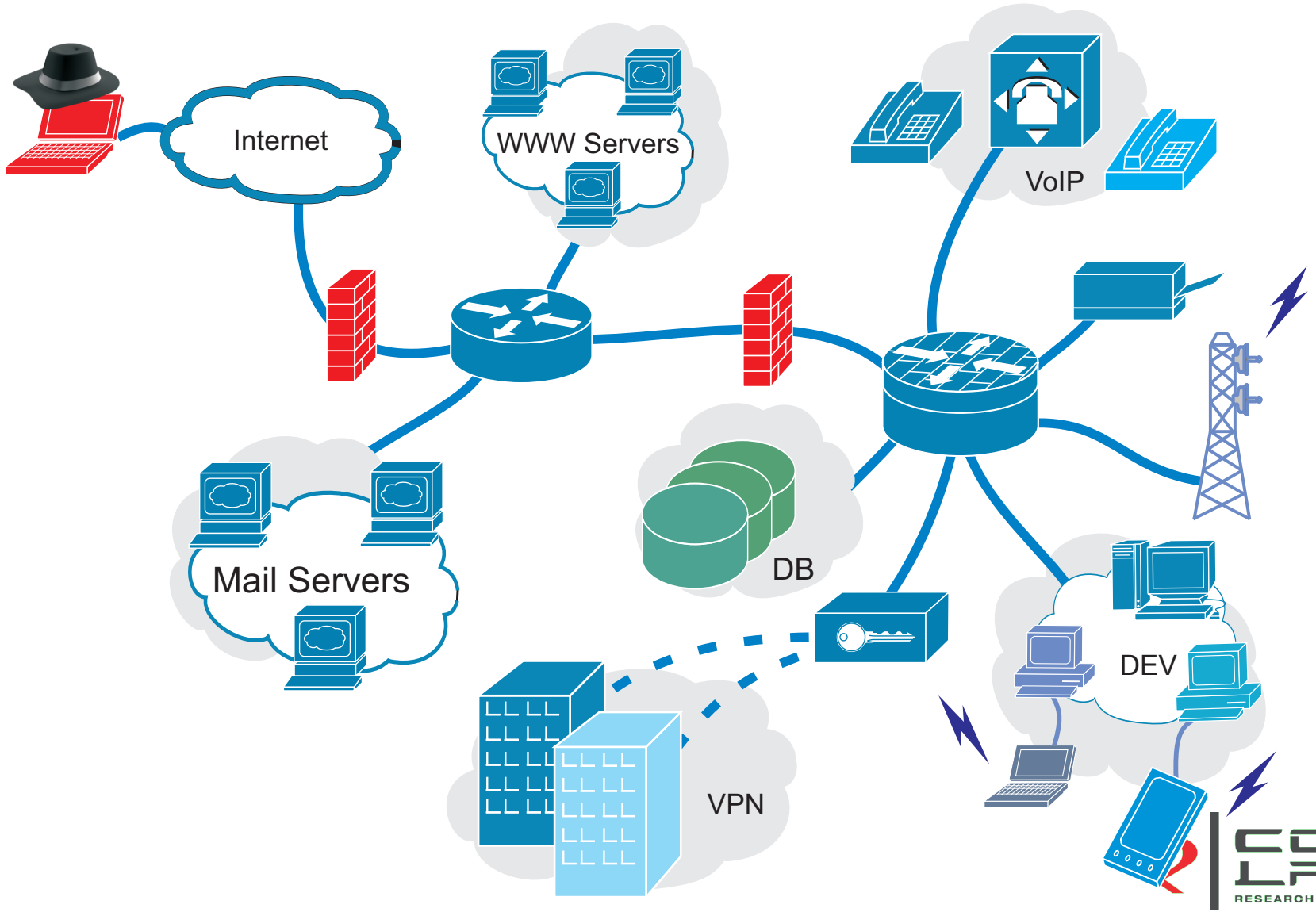
Objetivo: **Definir métricas de seguridad** aplicables a redes de gran escala, centrados en el punto de vista del atacante.

Estas métricas deben ser **útiles** para **tomar decisiones** en pos de la mejora del estado de la seguridad de una compañía.

Cambios en la complejidad tecnológica:

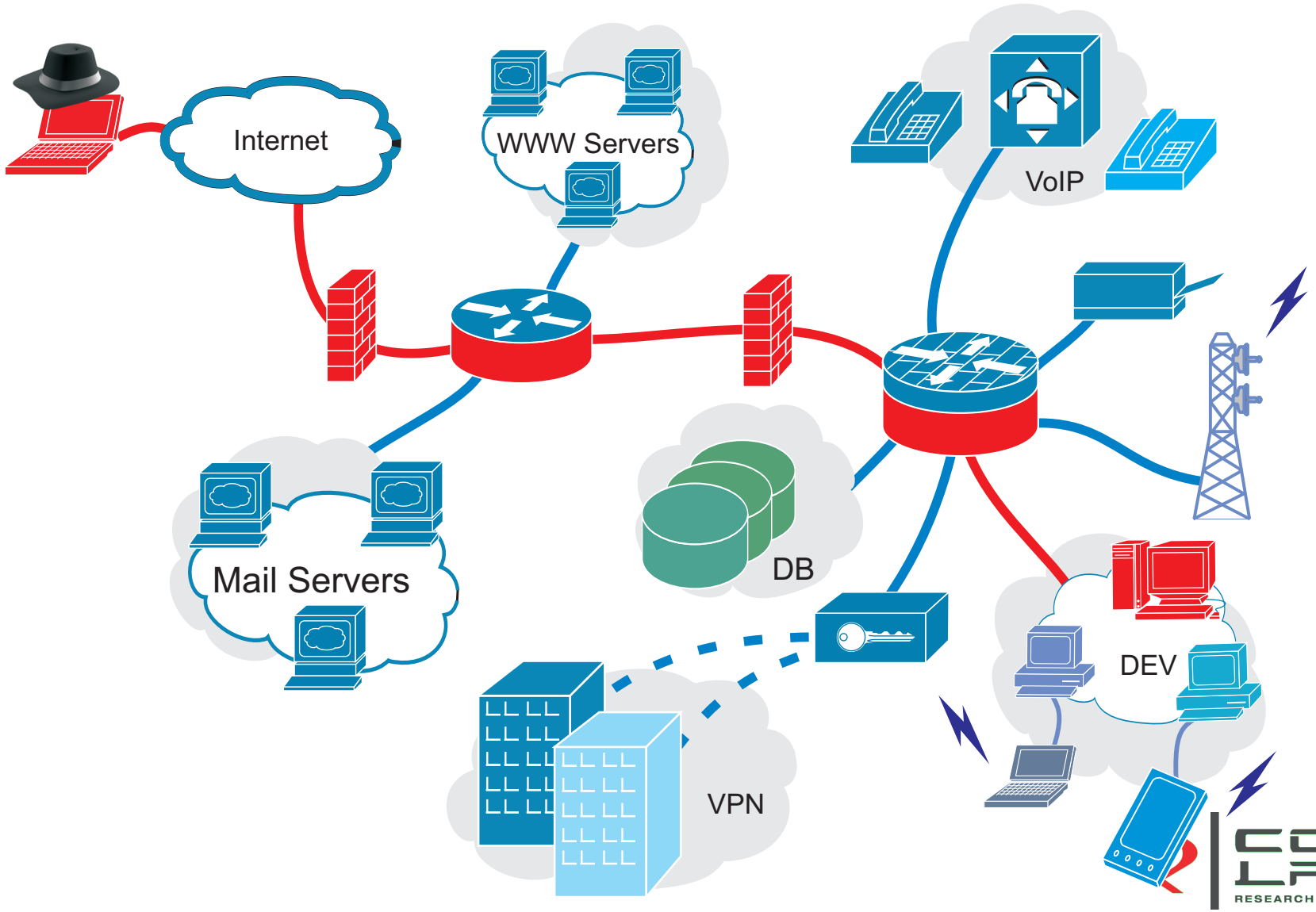
- Nuevas tecnologías:
  - Cómo saca ventaja un atacante de estas?
  - Qué objetivos persigue?
- En las interacciones entre tecnologías:
  - **Explotar relaciones de confianza**
  - Utilizar información pública
- Perímetro invertido

Perímetro, nueva concepción



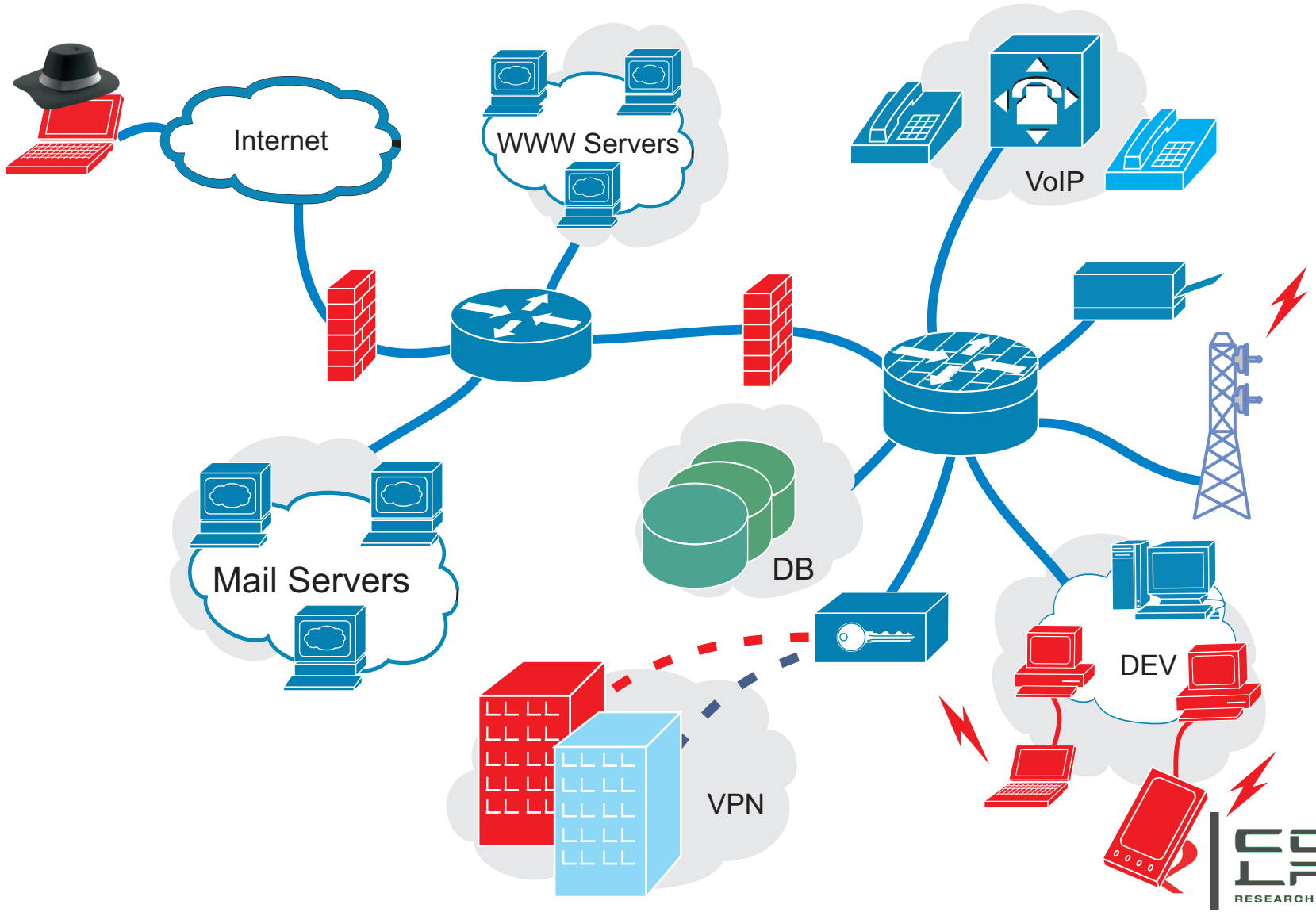
CORE LABS RESEARCH & DEVELOPMENT

Perímetro, nueva concepción



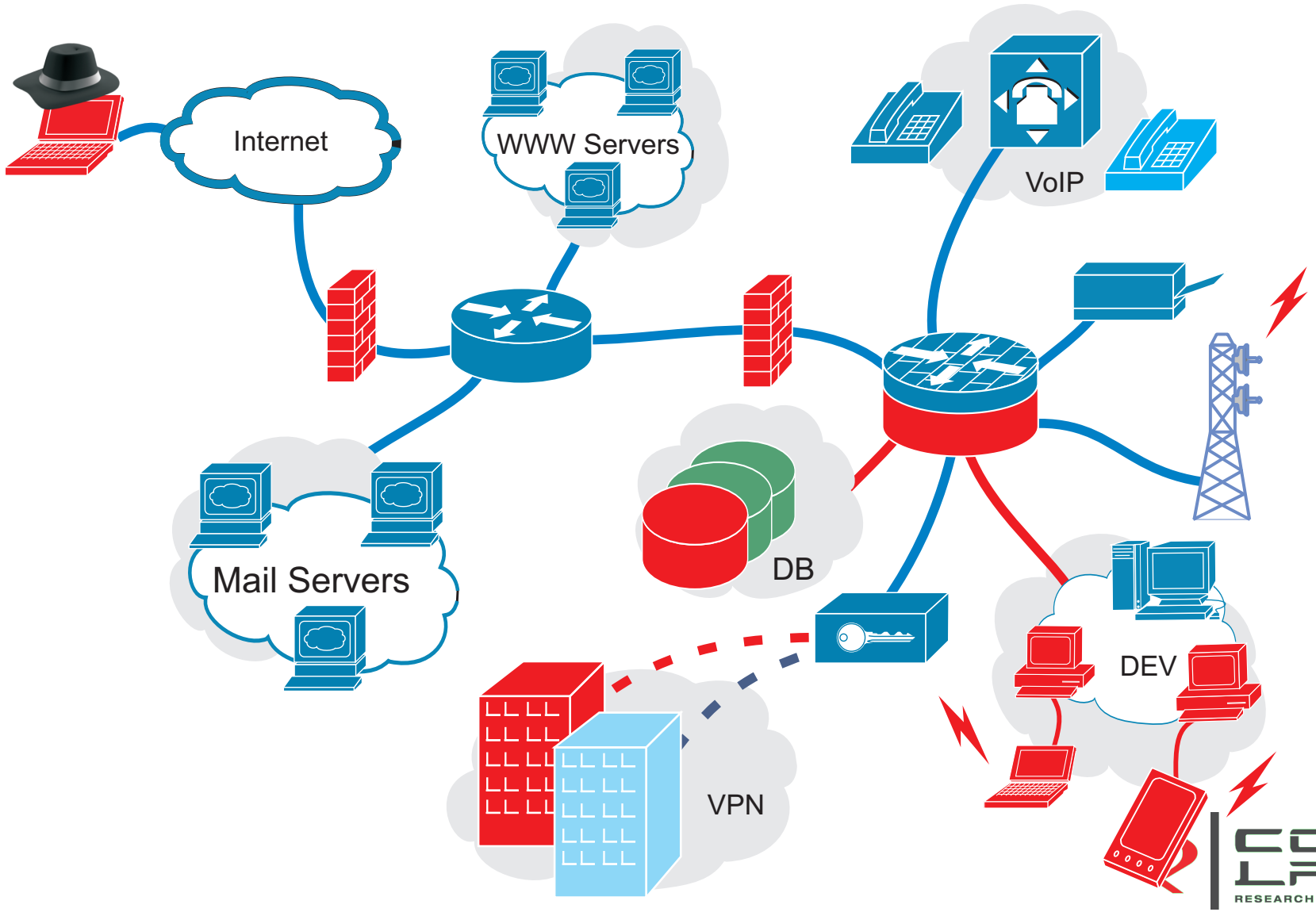
CORE LABS RESEARCH & DEVELOPMENT

Perímetro, nueva concepción



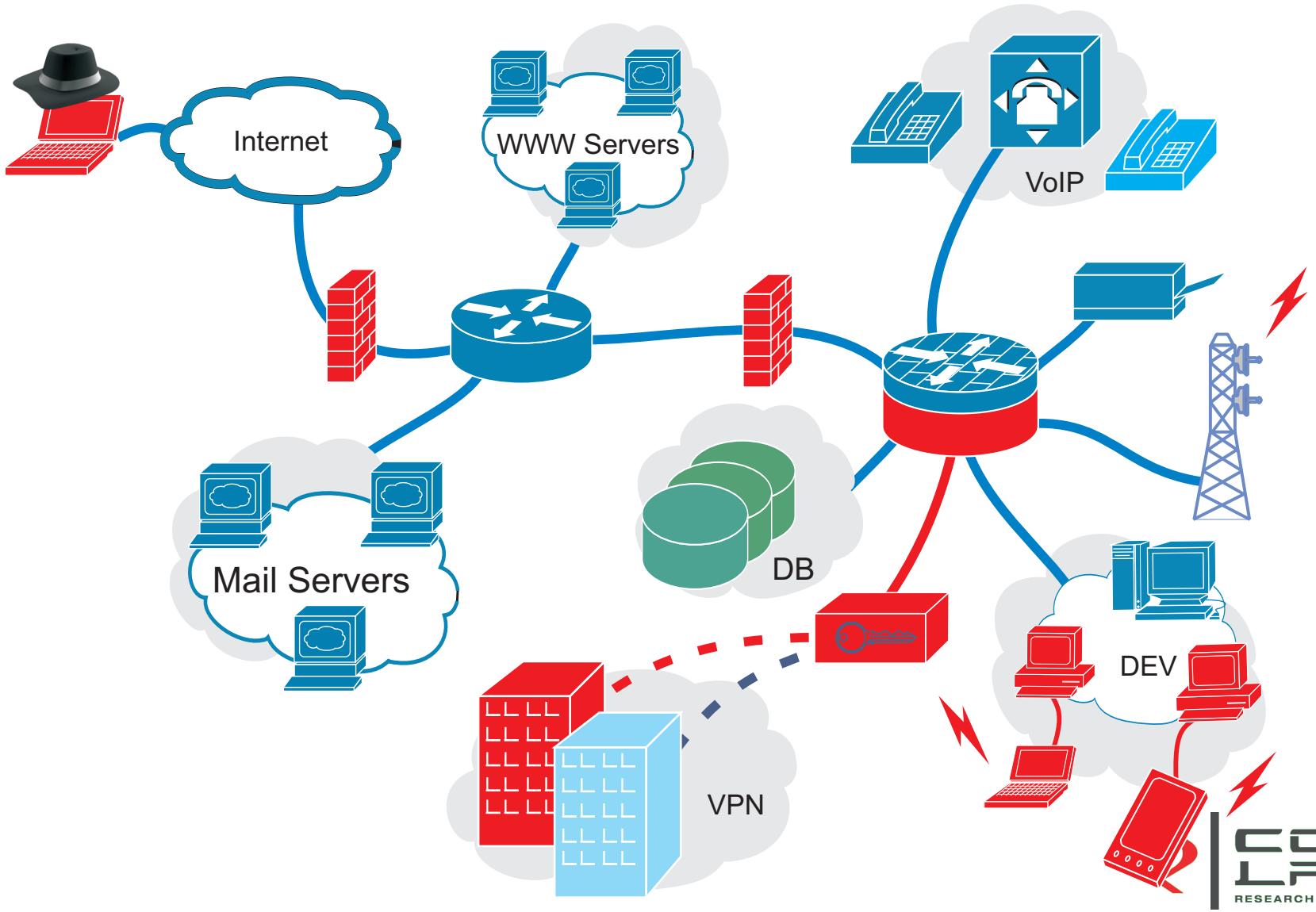
CORE LABS RESEARCH & DEVELOPMENT

Perímetro, nueva concepción



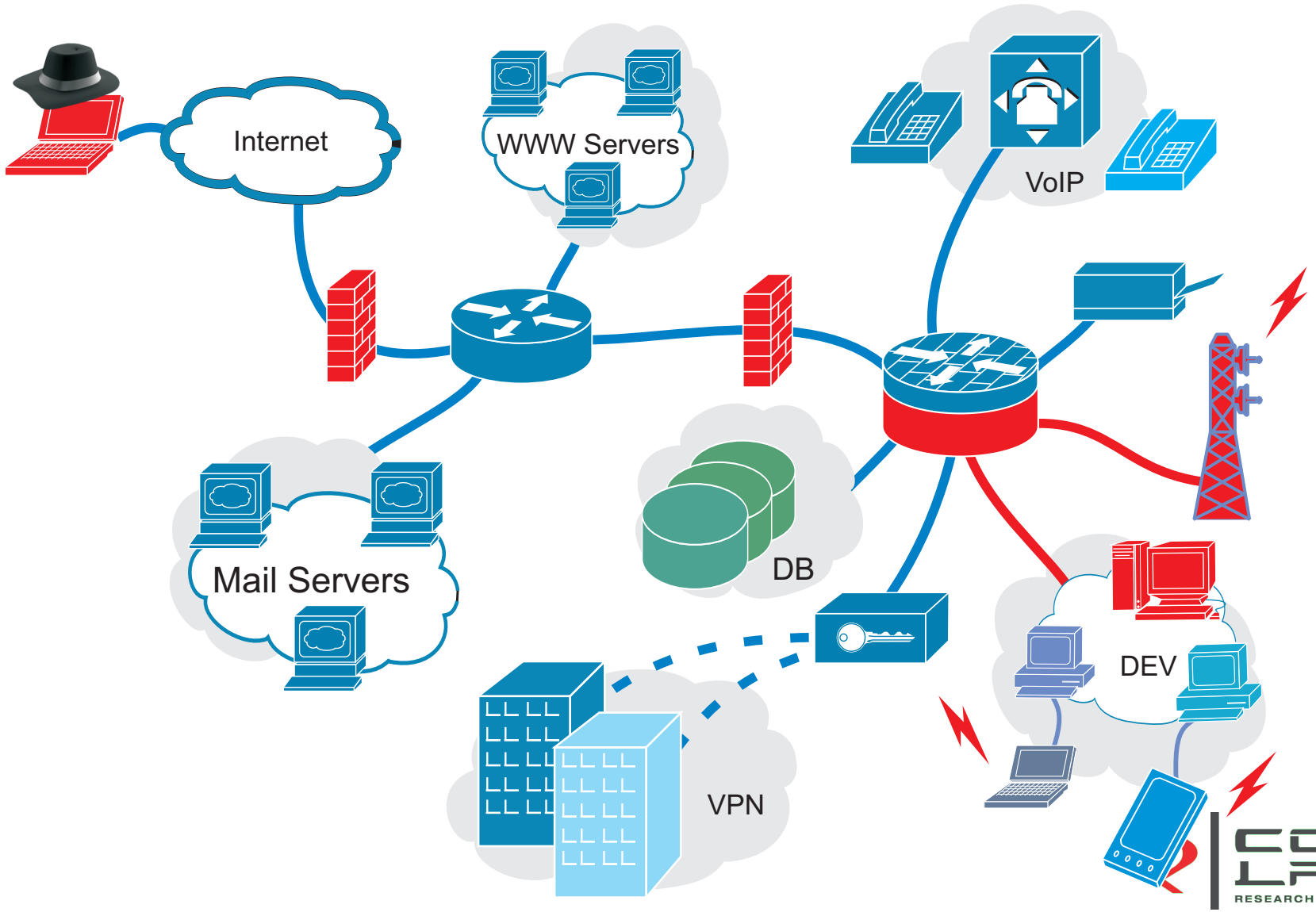
CORE LABS RESEARCH & DEVELOPMENT

Perímetro, nueva concepción



CORE LABS RESEARCH & DEVELOPMENT

Perímetro, nueva concepción



CORE LABS RESEARCH & DEVELOPMENT

Organizaciones

Cambios en la complejidad organizacional:

- Web services (desacoplamiento de tecnologías, consumo)
- Tercerización (Chile: 15vo.[1])
- Trabajo remoto (e.g. VPNs)
- Perímetros difusos, clowd computing, plataformas externas

[1] http://images.businessweek.com/ss/09/01/0114_top_outsourcers/16.htm

Organizaciones

Cambios en la lógica de negocios:

- Software as-a-service (e.g. CRM)
- Plataforma as-a-service (e.g. EC2)
- Proveedores de contenido

Métricas

- La tecnología ha evolucionado
- Las organizaciones han evolucionado
- Las formas de ataque han evolucionado y se han diversificado

¿Qué hay de las métricas para medir riesgos?
¿También han evolucionado?

Métricas

- La tecnología ha evolucionado
- Las organizaciones han evolucionado
- Las formas de ataque han evolucionado y se han diversificado

¿Qué hay de las métricas para medir riesgos? ¿También han evolucionado?

Métricas actuales (Jaquith, 2005)

Una buena métrica debe:

1. **Poder medirse de manera consistente.** El método de medición debe ser objetivo y repetible.
2. **Ser fácil de medir.** Usar herramientas automáticas (password crackers, software scanners) puede ser util.
3. **Tener una unidad de medida.** Tiempo, dinero o alguna escala numérica. Evitar códigos como “rojo”, “amarillo”, “verde”, “bajo riesgo”, “alta prioridad”, etc.

Fuente: *A Few Good Metrics*, 2005. Scott Berinato.

Andrew Jaquith: Cofundador de la consultora @stake (comprada por Symantec en 2004) y discípulo del infosecurity guru Dan Geer.

Métricas actuales (Jaquith, 2005)

Una buena métrica debe:

1. **Poder medirse de manera consistente.** El método de medición debe ser objetivo y repetible.
2. **Ser fácil de medir.** Usar herramientas automáticas (password crackers, software scanners) puede ser util.
3. **Tener una unidad de medida.** Tiempo, dinero o alguna escala numérica. Evitar códigos como “rojo”, “amarillo”, “verde”, “bajo riesgo”, “alta prioridad”, etc.

Fuente: *A Few Good Metrics*, 2005. Scott Berinato.

Andrew Jaquith: Cofundador de la consultora @stake (comprada por Symantec en 2004) y discípulo del infosecurity guru Dan Geer.

Métricas actuales (Jaquith, 2005)

Una buena métrica debe:

1. **Poder medirse de manera consistente.** El método de medición debe ser objetivo y repetible.
2. **Ser fácil de medir.** Usar herramientas automáticas (password crackers, software scanners) puede ser util.
3. **Tener una unidad de medida.** Tiempo, dinero o alguna escala numérica. Evitar códigos como “rojo”, “amarillo”, “verde”, “bajo riesgo”, “alta prioridad”, etc.

Fuente: *A Few Good Metrics*, 2005. Scott Berinato.

Andrew Jaquith: Cofundador de la consultora @stake (comprada por Symantec en 2004) y discípulo del infosecurity guru Dan Geer.

Métricas actuales (Jaquith, 2005)

1. **Baseline Defenses Coverage.** (Antivirus, Antispyware, Firewall, etc.) Determinar que tan bien protegida está una organización contra las amenzas más básicas de seguridad. La cobertura de dispositivos debería estar entre 94%-98%. Menos del 90% puede ser motivo de alarma.
2. **Patch Latency.**
3. **Password Strength.**
4. **Platform Compliance Scores.**
5. **Legitimate E-Mail Traffic Analysis.**

Fuente: *A Few Good Metrics*, 2005. Scott Berinato.

Andrew Jaquith: Cofundador de la consultora @stake (comprada por Symantec en 2004) y discípulo del infosecurity guru Dan Geer.

Métricas actuales (Jaquith, 2005)

1. **Baseline Defenses Coverage.**
2. **Patch Latency.** Medir el tiempo entre que se libera una actualización de seguridad y ésta finalmente se aplica. Es un indicador de la disciplina de actualizaciones de una organización y su habilidad para reaccionar ante nuevos exploits.
3. **Password Strength.**
4. **Platform Compliance Scores.**
5. **Legitimate E-Mail Traffic Analysis.**

Fuente: *A Few Good Metrics*, 2005. Scott Berinato.

Andrew Jaquith: Cofundador de la consultora @stake (comprada por Symantec en 2004) y discípulo del infosecurity guru Dan Geer.

Métricas actuales (Jaquith, 2005)

1. **Baseline Defenses Coverage.**
2. **Patch Latency.**
3. **Password Strength.** Esta métrica simplemente busca default passwords. La seguridad de una organización se ve "mejorada" porque se reemplazan passwords débiles por otros más fuertes o difíciles de romper.
4. **Platform Compliance Scores.**
5. **Legitimate E-Mail Traffic Analysis.**

Fuente: *A Few Good Metrics*, 2005. Scott Berinato.

Andrew Jaquith: Cofundador de la consultora @stake (comprada por Symantec en 2004) y discípulo del infosecurity guru Dan Geer.

Métricas actuales (Jaquith, 2005)

1. **Baseline Defenses Coverage.**
2. **Patch Latency.**
3. **Password Strength.**
4. **Platform Compliance Scores.** Herramientas de scoring como Center for Internet Security (CIS), pueden correr tests automáticos y detectar puertos innecesariamente abiertos, sistemas compartidos indiscriminadamente, permisos por default, etc.
5. **Legitimate E-Mail Traffic Analysis.**

Fuente: *A Few Good Metrics*, 2005. Scott Berinato.

Andrew Jaquith: Cofundador de la consultora @stake (comprada por Symantec en 2004) y discípulo del infosecurity guru Dan Geer.

Métricas actuales (Jaquith, 2005)

1. **Baseline Defenses Coverage.**
2. **Patch Latency.**
3. **Password Strength.**
4. **Platform Compliance Scores.**
5. **Legitimate E-Mail Traffic Analysis.** Estas métricas monitorean el tráfico entrante y saliente entre una organización y el exterior, incluyendo tamaño, cantidad y destinatario de los e-mails. Puede servir para detectar empleados desleales divulgando información o propiedad intelectual confidencial.

Fuente: *A Few Good Metrics*, 2005. Scott Berinato.

Andrew Jaquith: Cofundador de la consultora @stake (comprada por Symantec en 2004) y discípulo del infosecurity guru Dan Geer.

Dicho esto... Motivación

Toda métrica y todo proceso de risk assessment debería tener un **modelo** de atacante asociado. Muchas veces este modelo es implícito.

si el modelo de atacante está presente...

¿Cuán **real** es?

Estos **modelos implícitos** son muchas veces obsoletos.

Propuesta: Pensar **activa** y **explícitamente** en quién y cómo es el atacante del cual queremos protegernos.

Pensar **como** un atacante.

Penetration test: Imita los intentos y las técnicas de un perfil de atacante para comprometer una organización y acceder a información confidencial y estratégica de la misma.

¿Para qué podríamos utilizar un pen-test?

- Distinguir vulnerabilidades críticas de las insignificantes y los falsos positivos
- Preservar la imagen de una empresa y la lealtad de sus clientes
- Evitar costos de network downtime
- Justificar inversiones de seguridad
- Cumplir pre-requisitos de compañías aseguradoras
- Cumplir regulaciones (GLBA, PCI, HIPAA & Sarbanes-Oxley)

CORE LABS RESEARCH & DEVELOPMENT

Penetration testing

Penetration test: Imita los intentos y las técnicas de un perfil de atacante para comprometer una organización y acceder a información confidencial y estratégica de la misma.

¿Para qué podríamos utilizar un pen-test?

- Distinguir vulnerabilidades críticas de las insignificantes y los falsos positivos
- Preservar la imagen de una empresa y la lealtad de sus clientes
- Evitar costos de network downtime
- Justificar inversiones de seguridad
- Cumplir pre-requisitos de compañías aseguradoras
- Cumplir regulaciones (GLBA, PCI, HIPAA & Sarbanes-Oxley)

Limitaciones

- **Ventana de tiempo:** Definida y acotada.
- **Alcance (scope):** Normalmente se limita la cantidad de vectores de ataque y sistemas a testear.
- **Requiere de un experto:** Aunque existen herramientas automáticas, los mejores resultados se obtienen de equipos especializados.

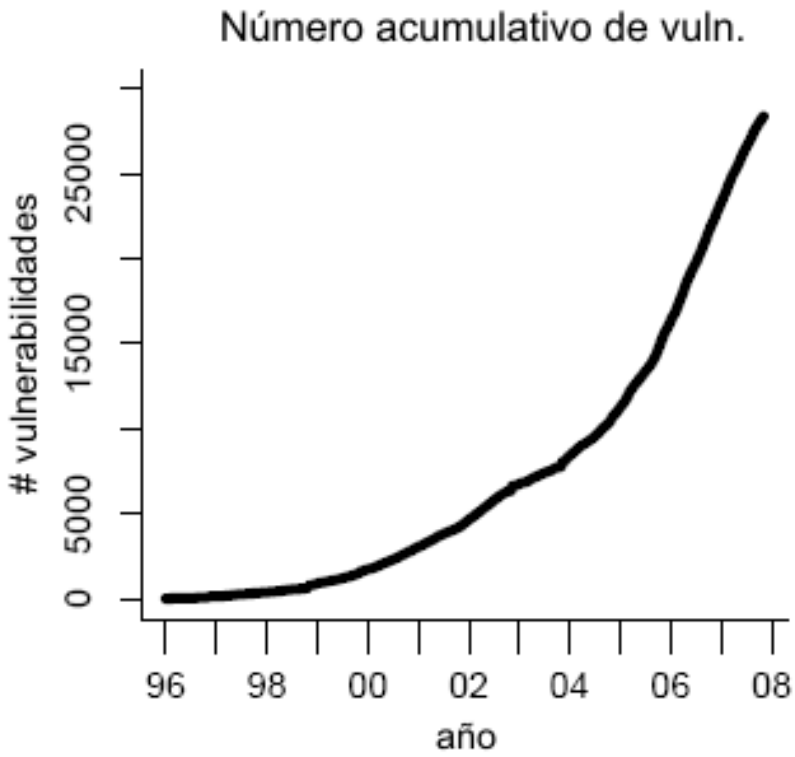
Las vulnerabilidades reportadas crecen año a año. Un experto, en el contexto de un pen-test, sólo puede atacar y analizar un porcentaje de todos los posibles caminos de ataque enfocado en el perfil de un tipo atacante.

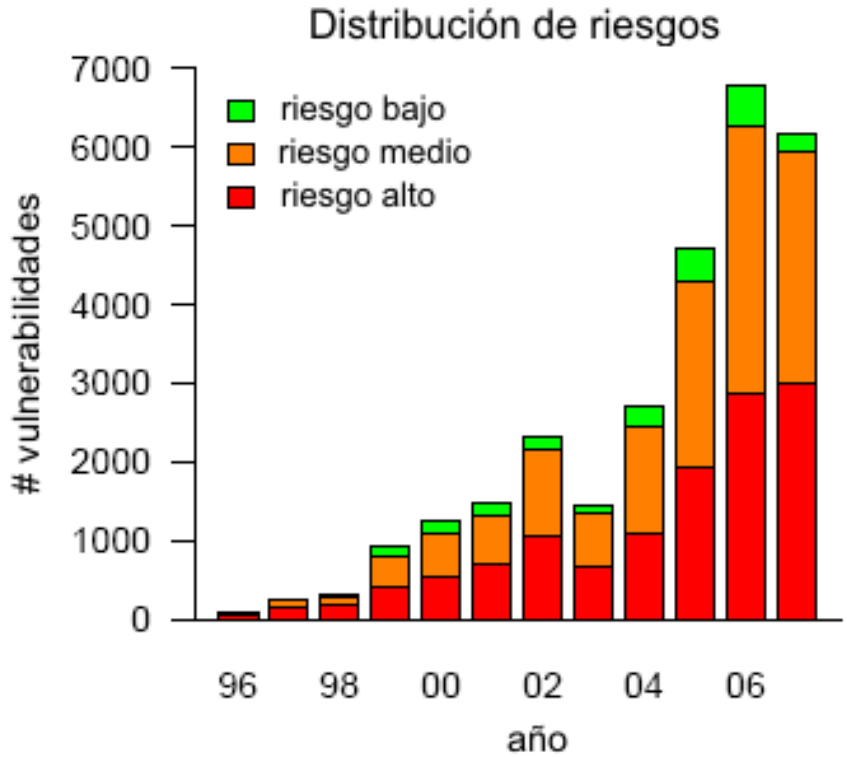
Limitaciones

- **Ventana de tiempo:** Definida y acotada.
- **Alcance (scope):** Normalmente se limita la cantidad de vectores de ataque y sistemas a testear.
- **Requiere de un experto:** Aunque existen herramientas automáticas, los mejores resultados se obtienen de equipos especializados.

Las vulnerabilidades reportadas crecen año a año. Un experto, en el contexto de un pen-test, sólo puede atacar y analizar un porcentaje de todos los posibles caminos de ataque enfocado en el perfil de un tipo atacante.

Vulnerabilidades reportadas 1996-2008



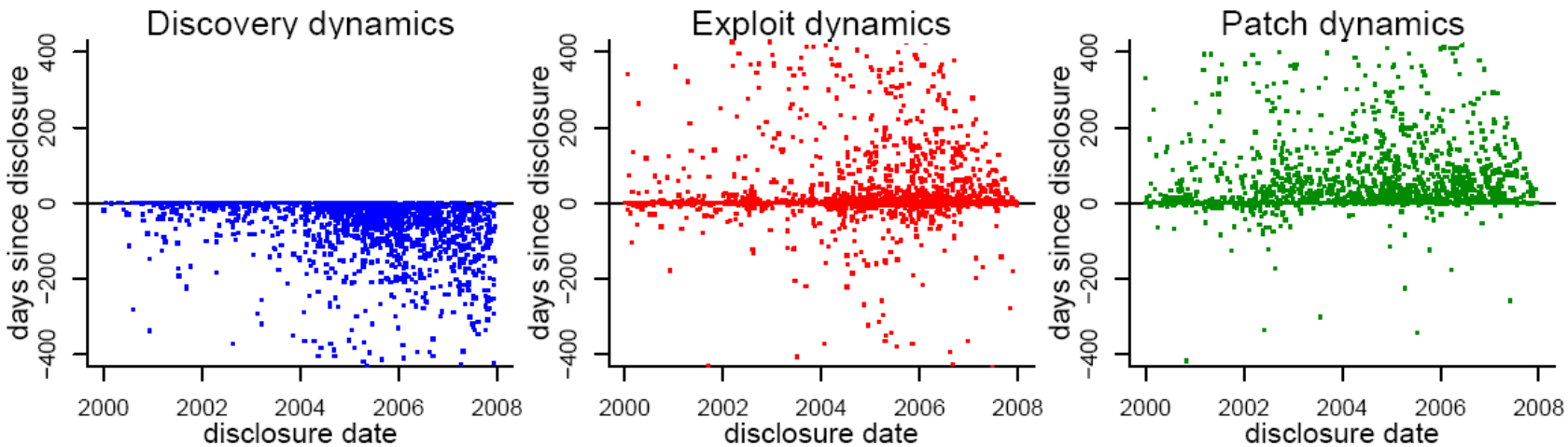


Recolección de datos: National Vulnerability Database (NVD), Open Source Vulnerability Database (OSVDB), CVE database.

Fuente: *Modelling the Security Ecosystem* - The Dynamics of (In)Security, 2009. Frei, Schatzmann, Plattner & Trammell.

CORE LABS RESEARCH & DEVELOPMENT

Vulnerabilidades reportadas 1996-2008



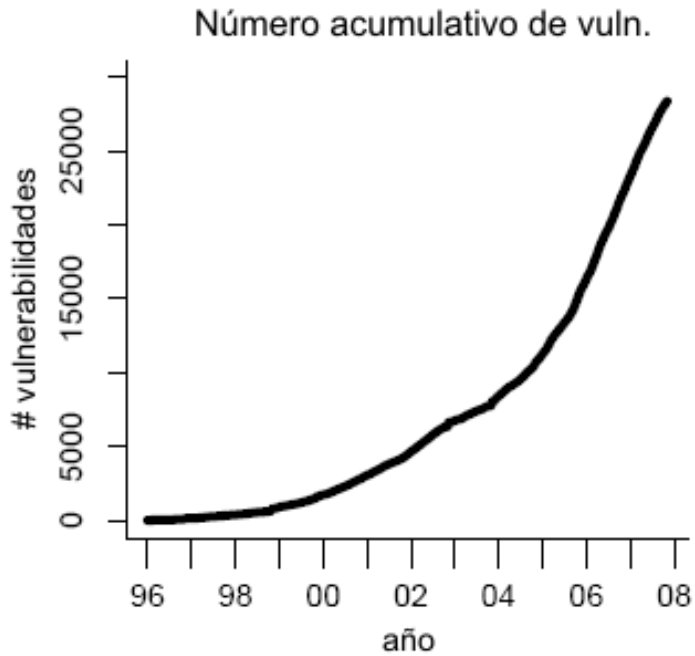
Recolección de datos: National Vulnerability Database (NVD), Open Source Vulnerability Database (OSVDB), CVE database.

Fuente: *Modelling the Security Ecosystem* - The Dynamics of (In)Security, 2009. Frei, Schatzmann, Plattner & Trammell.

CORE LABS RESEARCH & DEVELOPMENT

Tendencias y estadísticas

- En los últimos 15 años se reportaron cerca de 40000 vulnerabilidades.
- La mayoría de las vulnerabilidades reportadas provienen de productos y compañías bien conocidas.
- En 2007 el 20% de las vulnerabilidades reportadas provino del Top-10 (0.04%).
- Considerando las vulnerabilidades reportadas y el software existente (agregando sistemas hechos a medida, poco conocidos y 0-days) es difícil estimar la cantidad real de vulnerabilidades explotables.



CORE LABS RESEARCH & DEVELOPMENT

Tendencias y estadísticas

- En los últimos 15 años se reportaron cerca de 40000 vulnerabilidades.
- La mayoría de las vulnerabilidades reportadas provienen de productos y compañías bien conocidas.
- En 2007 el 20% de las vulnerabilidades reportadas provino del Top-10 (0.04%).
- Considerando las vulnerabilidades reportadas y el software existente (agregando sistemas hechos a medida, poco conocidos y 0-days) es difícil estimar la cantidad real de vulnerabilidades explotables.

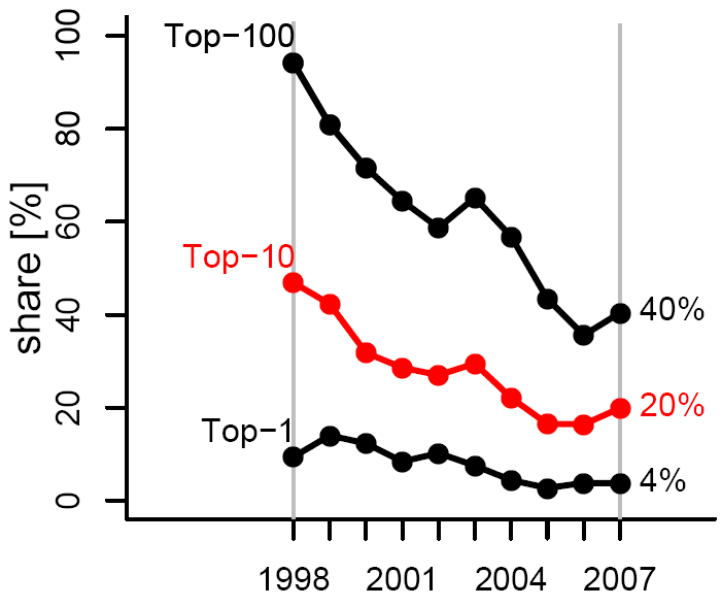
04	2005	2006	2007
osoft	Microsoft	Microsoft	Microsoft
too	Apple	Apple	Apple
lat	Linux	Oracle	IBM
ple	Mozilla	Mozilla	Oracle
nux	Sun	Linux	PHP
SE	IBM	IBM	Sun
GI	Oracle	Sun	Cisco
lla	Red Hat	Cisco	Mozilla
te	Ethereal	Joomla	HP
	SuSE	Novell	Linux

Fuente: National Vulnerability Database (NVD)

CORE LABS RESEARCH & DEVELOPMENT

Tendencias y estadísticas

- En los últimos 15 años se reportaron cerca de 40000 vulnerabilidades.
- La mayoría de las vulnerabilidades reportadas provienen de productos y compañías bien conocidas.
- En 2007 el 20% de las vulnerabilidades reportadas provino del Top-10 (0.04%).
- Considerando las vulnerabilidades reportadas y el software existente (agregando sistemas hechos a medida, poco conocidos y 0-days) es difícil estimar la cantidad real de vulnerabilidades explotables.

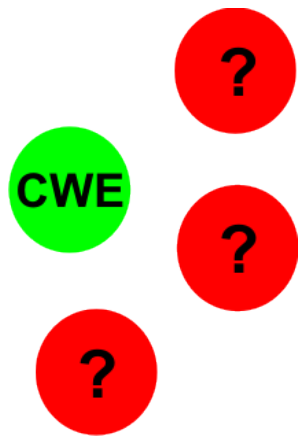


Fuente: National Vulnerability Database (NVD)

CORE LABS RESEARCH & DEVELOPMENT

Tendencias y estadísticas

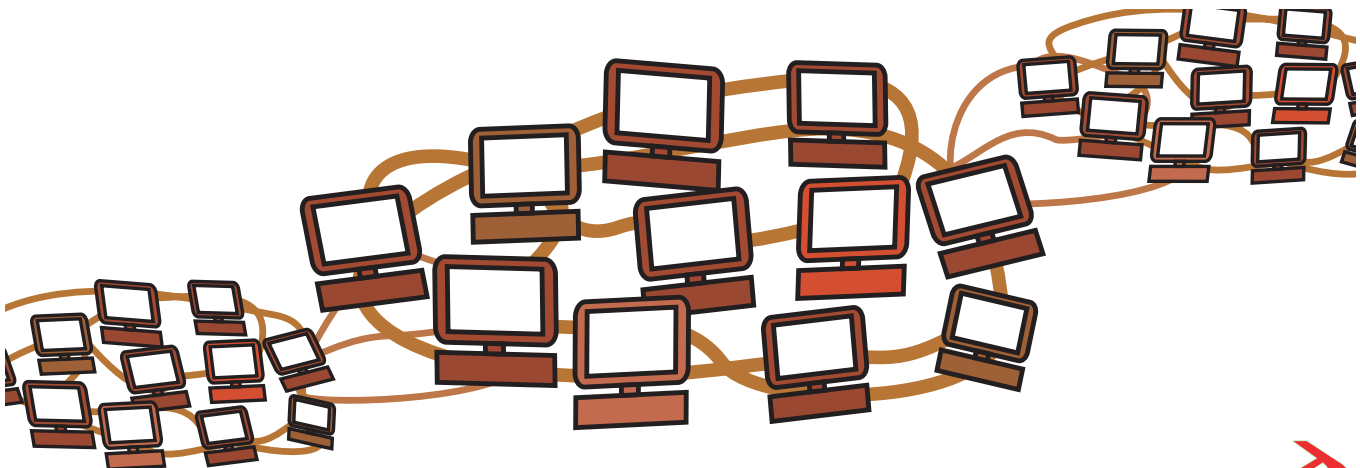
- En los últimos 15 años se reportaron cerca de 40000 vulnerabilidades.
- La mayoría de las vulnerabilidades reportadas provienen de productos y compañías bien conocidas.
- En 2007 el 20% de las vulnerabilidades reportadas provino del Top-10 (0.04%).
- Considerando las vulnerabilidades reportadas y el software existente (agregando sistemas hechos a medida, poco conocidos y 0-days) es difícil estimar la cantidad real de vulnerabilidades explotables.



El volúmen de datos y la imposibilidad de tener todos los exploits y vulnerabilidades disponibles hacen imposible analizar **todas** las posibles acciones de un atacante.

Una alternativa razonable podría consistir en el armado de **modelos** que mediante la utlización de **simuladores** nos ayuden a explorar las acciones de un atacante.

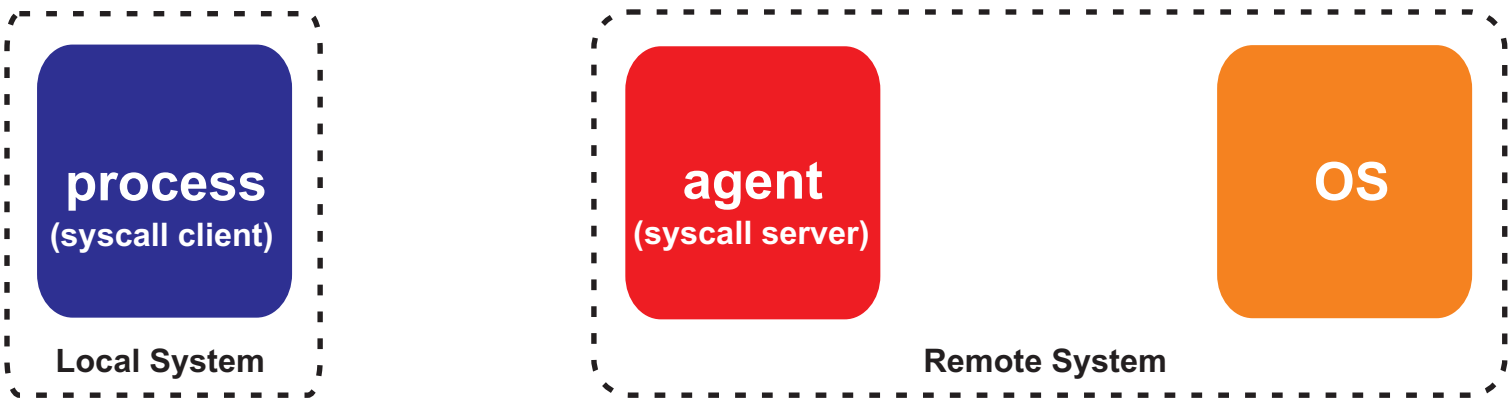
Insight permite simular redes de computadoras a gran escala, dispositivos de hardware, aplicaciones y sus vulnerabilidades, permitiendo la ejecución y el análisis de ataques cibernéticos.



CORE LABS RESEARCH & DEVELOPMENT

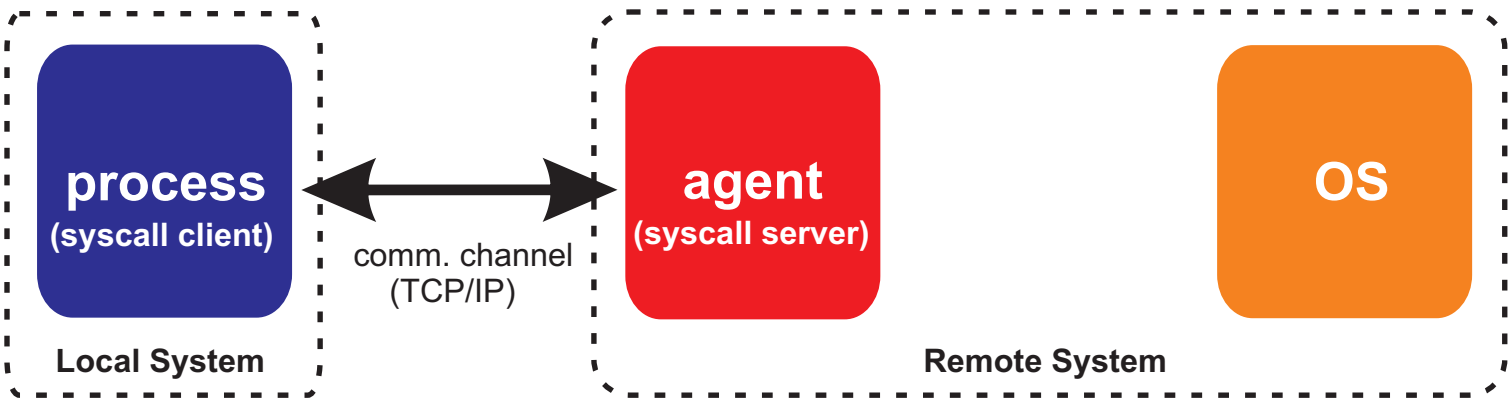
Algunas definiciones: Agentes

Un **agente** es un servidor de system-calls instalado en una computadora (remota) que es capaz de ejecutar cualquier system-call como un proceso local.



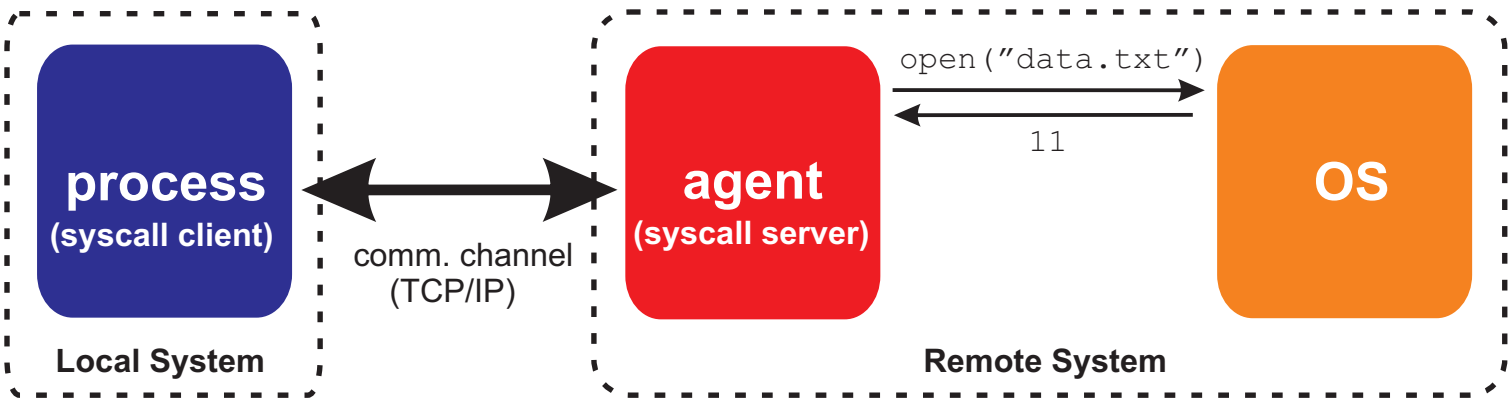
Algunas definiciones: Agentes

Un **agente** es un servidor de system-calls instalado en una computadora (remota) que es capaz de ejecutar cualquier system-call como un proceso local.



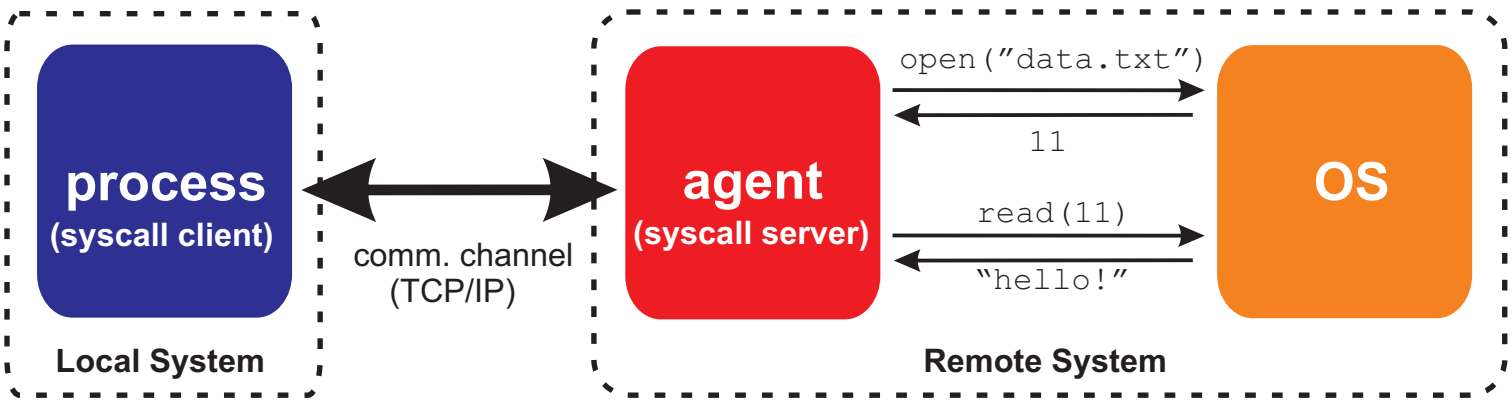
Algunas definiciones: Agentes

Un **agente** es un servidor de system-calls instalado en una computadora (remota) que es capaz de ejecutar cualquier system-call como un proceso local.



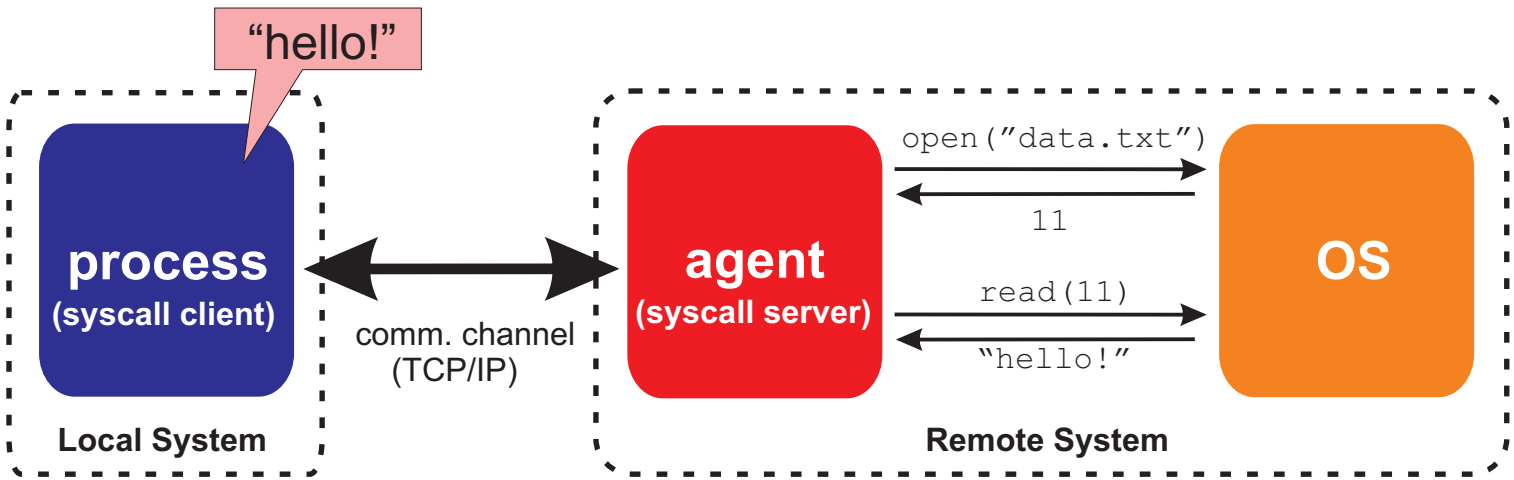
Algunas definiciones: Agentes

Un **agente** es un servidor de system-calls instalado en una computadora (remota) que es capaz de ejecutar cualquier system-call como un proceso local.



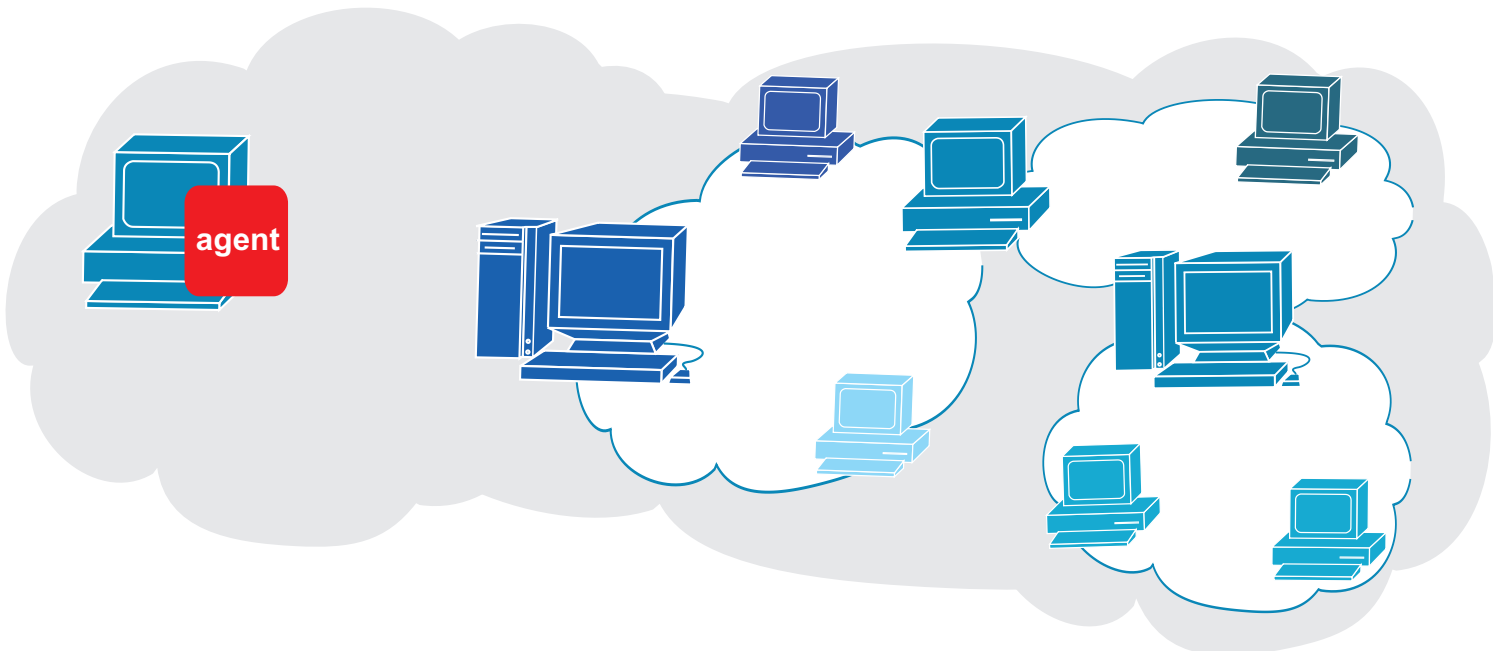
Algunas definiciones: Agentes

Un **agente** es un servidor de system-calls instalado en una computadora (remota) que es capaz de ejecutar cualquier system-call como un proceso local.



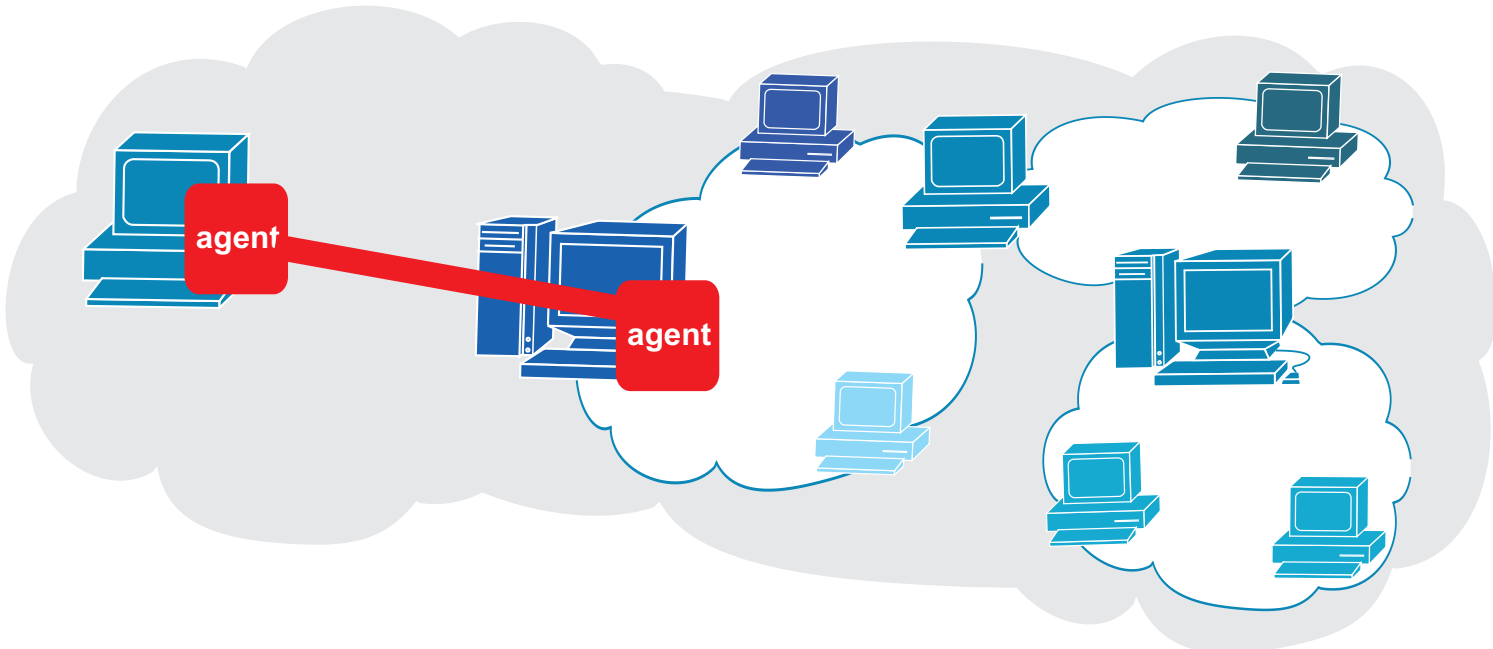
Algunas definiciones: Pivoting

Pivoting: Los agentes pueden encadenarse para construir ataques complejos.



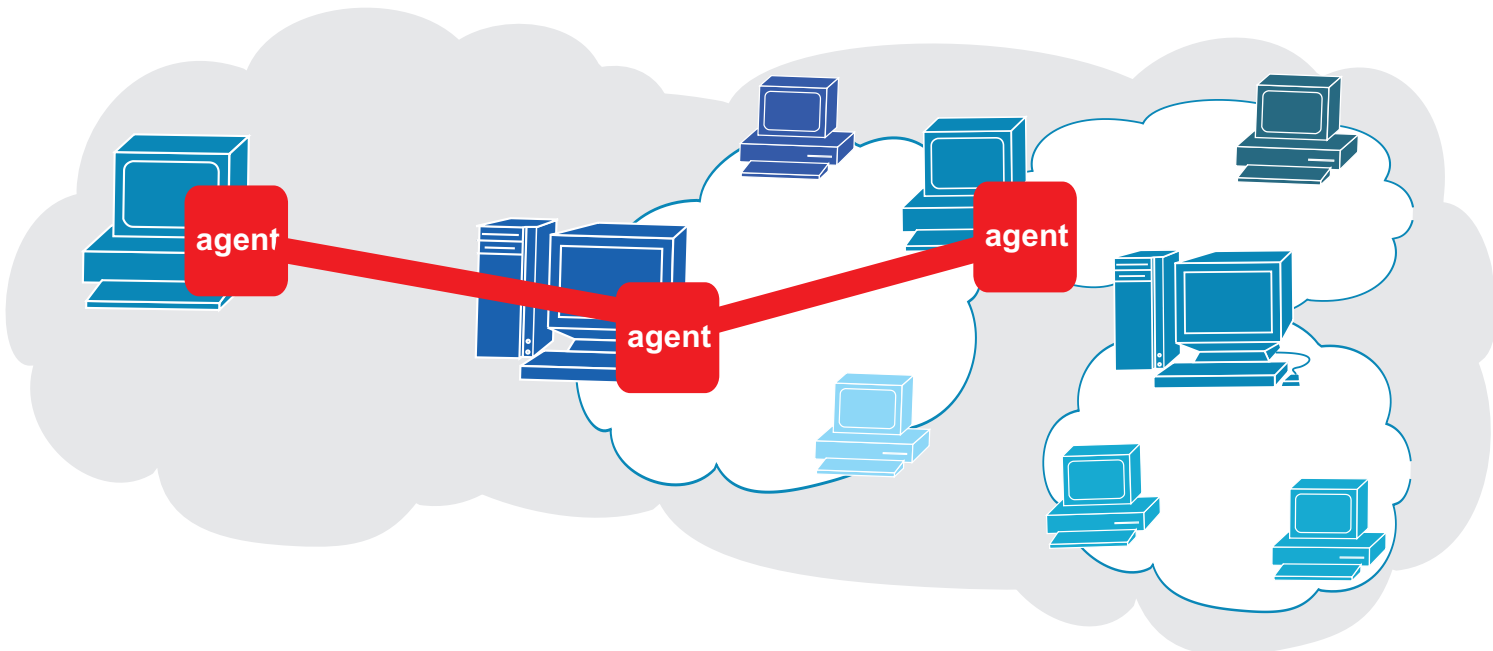
Algunas definiciones: Pivoting

Pivoting: Los agentes pueden encadenarse para construir ataques complejos.



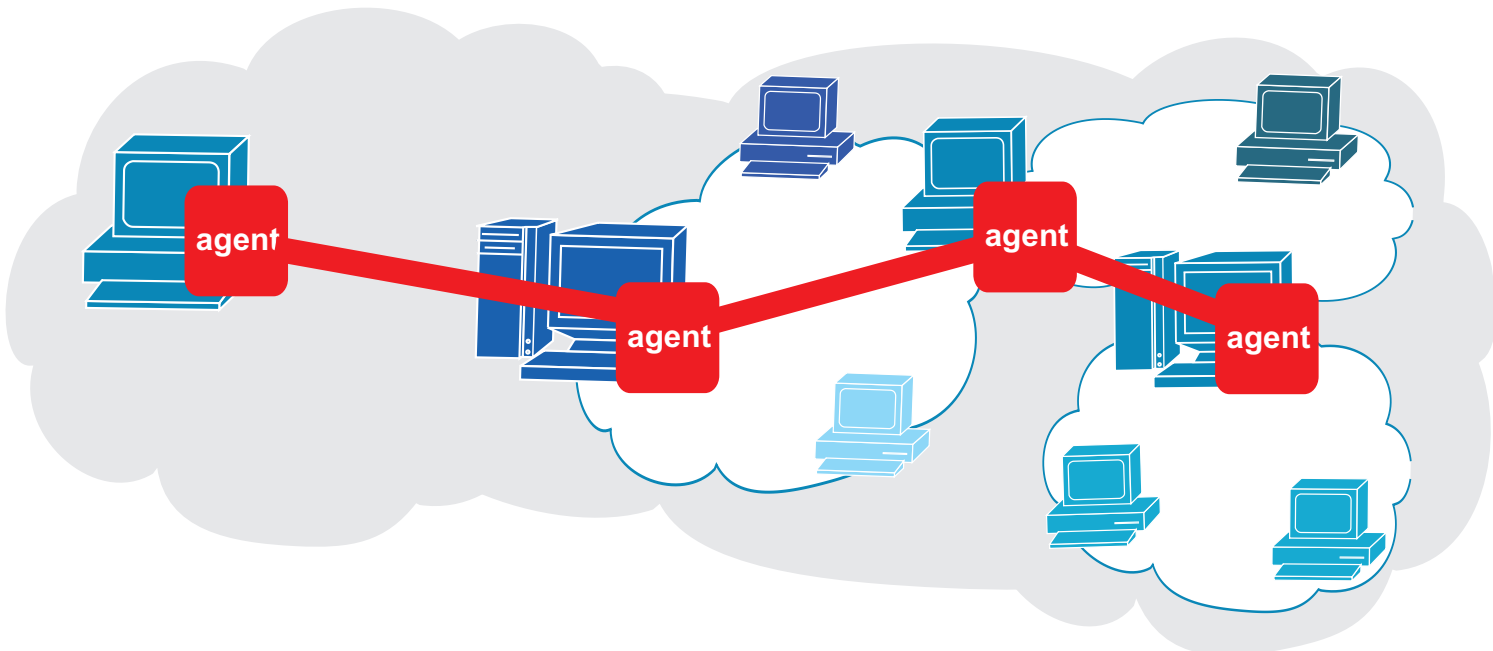
Algunas definiciones: Pivoting

Pivoting: Los agentes pueden encadenarse para construir ataques complejos.



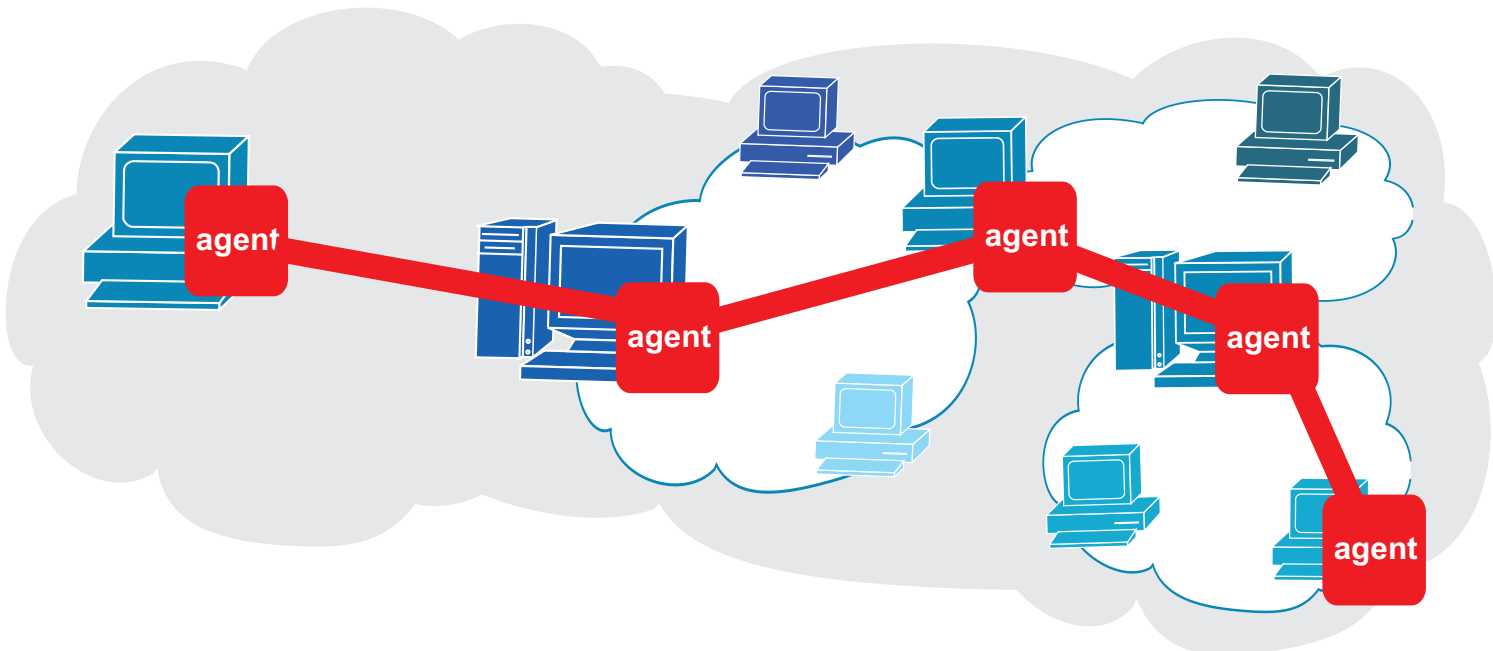
Algunas definiciones: Pivoting

Pivoting: Los agentes pueden encadenarse para construir ataques complejos.

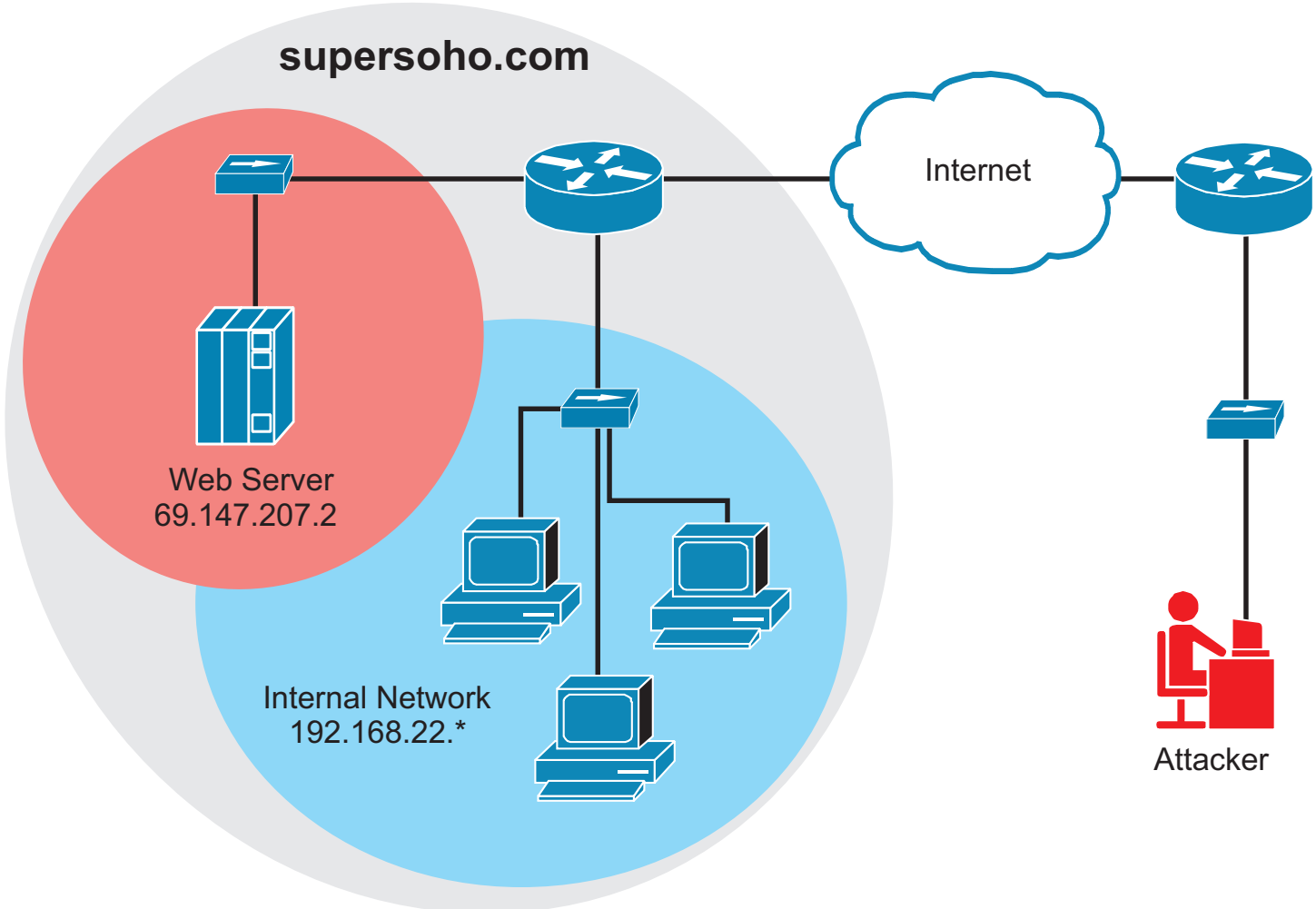


Algunas definiciones: Pivoting

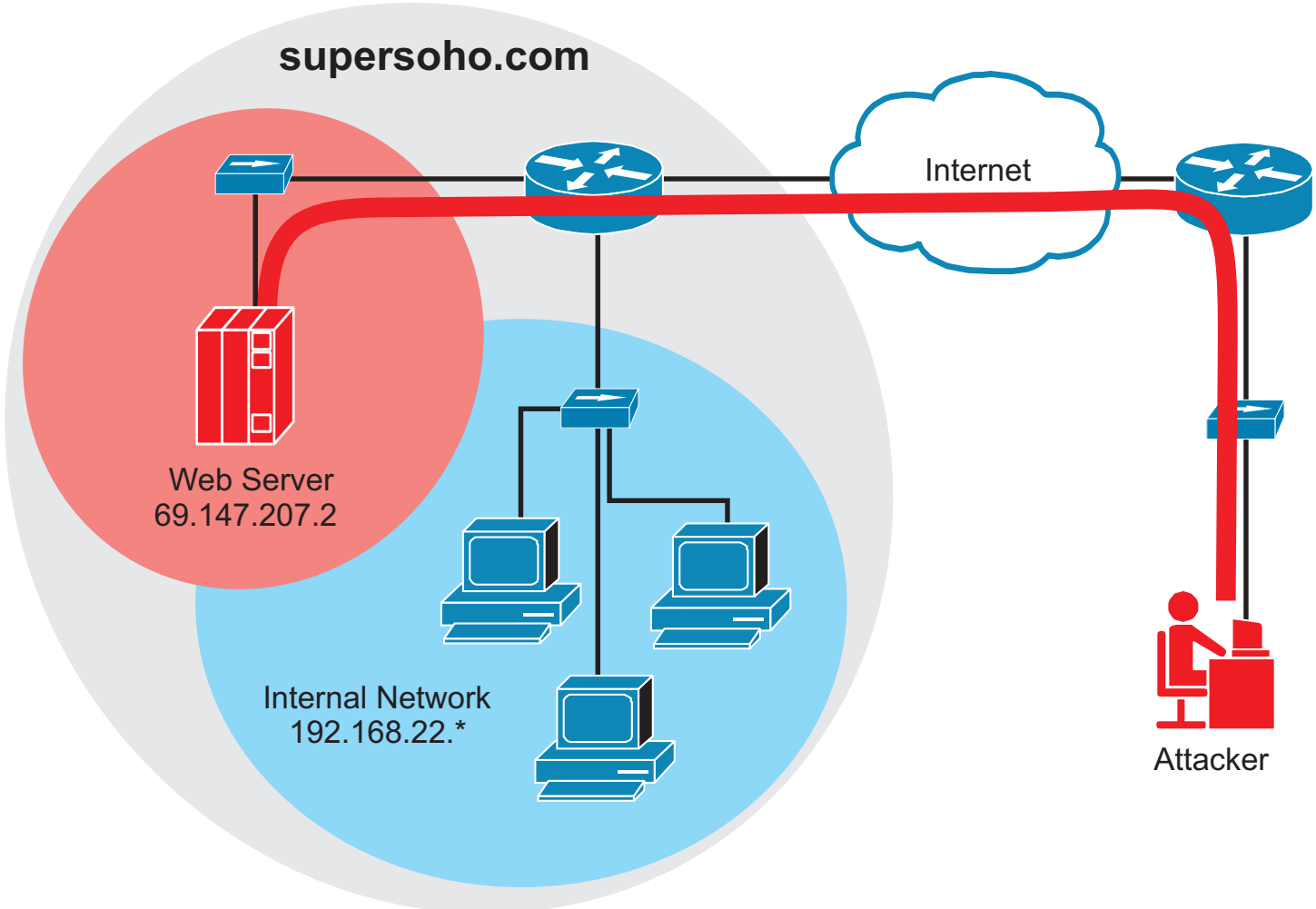
Pivoting: Los agentes pueden encadenarse para construir ataques complejos.



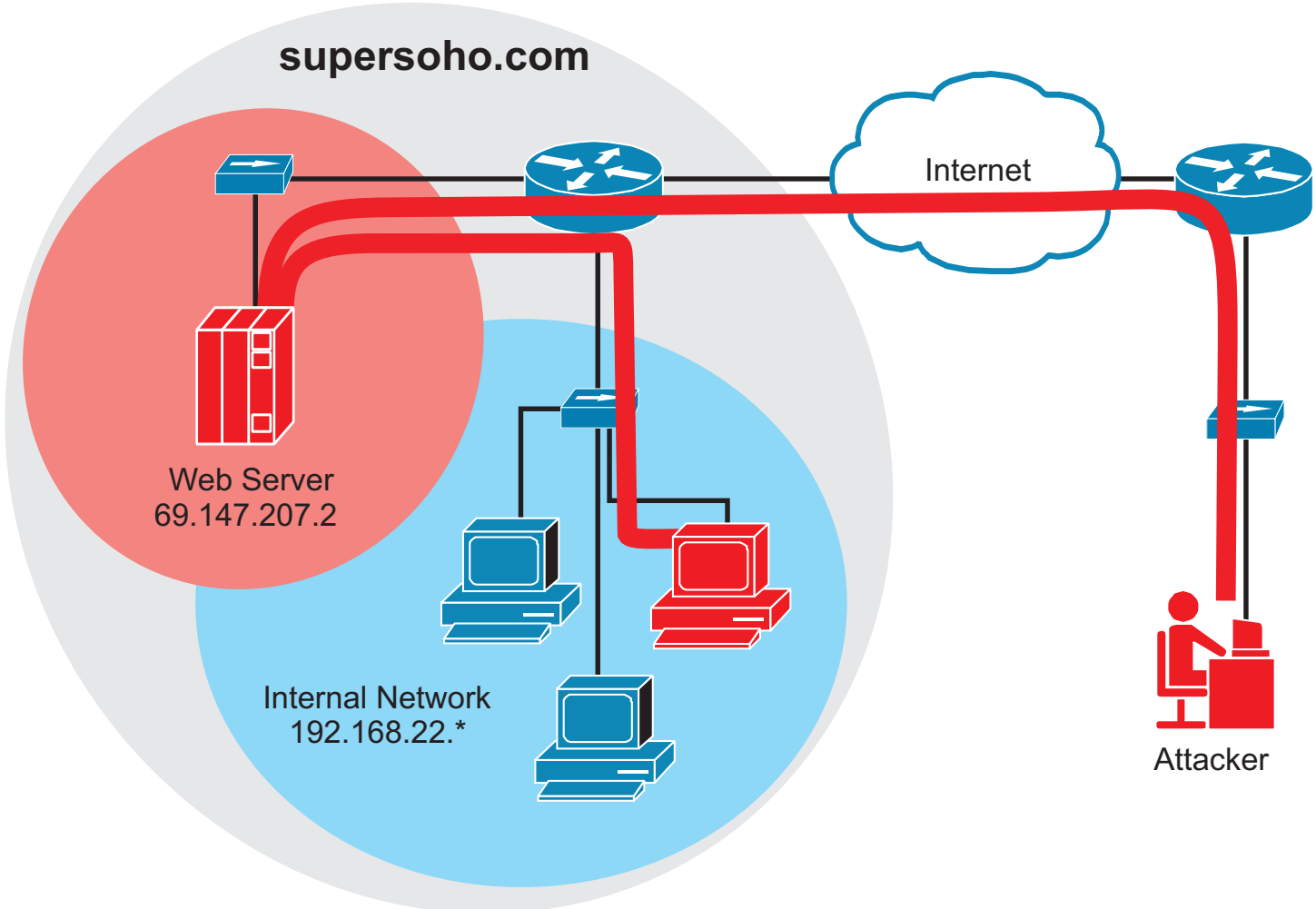
Demo: SuperSoho pentest



Demo: SuperSoho pentest



Demo: SuperSoho pentest

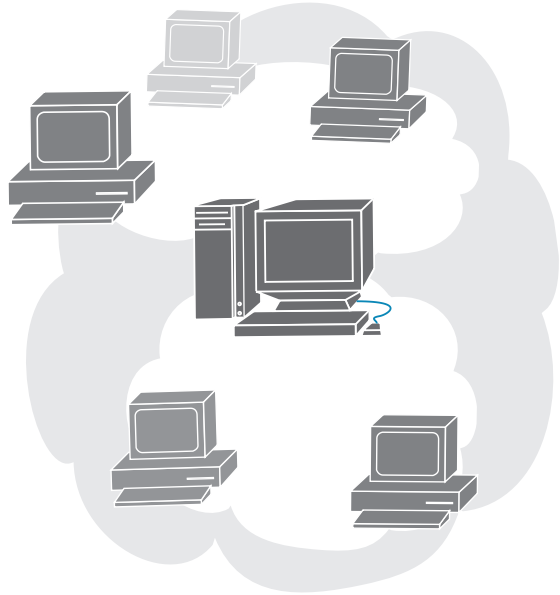


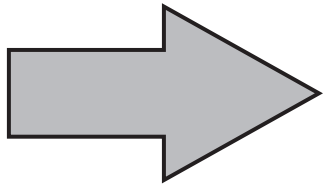
¿Por qué simular?

- Para experimentar sobre escenarios hipotéticos.
- Para analizar el impacto de ataques en un entorno controlado.
- Para realizar análisis post-ataque (forensics).
- Costo menor que un pen-test real.
- Podemos automatizar distintos aspectos de un pen-test, luego explorar más caminos de ataque y calcular métricas.

Métricas centradas en el atacante

Importar escenario

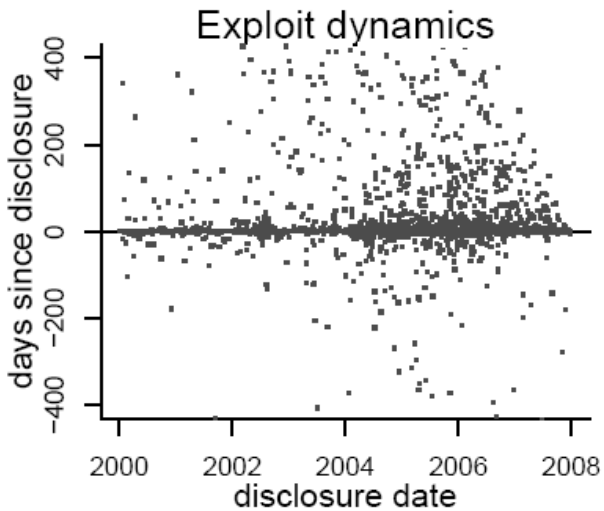




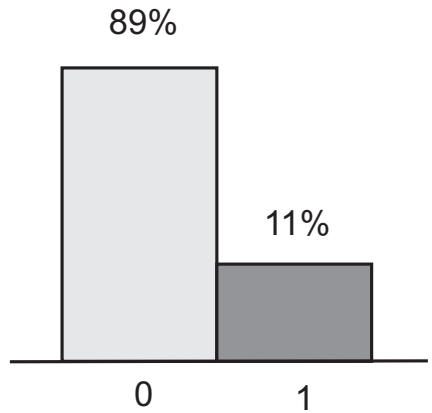
```
<machine>
  <os>windows</os>
  <version>XP</ver...
</machine>

<machine>
  <os>linux</os>
  <version>redhat</v...
</machine>
```

CORE LABS RESEARCH & DEVELOPMENT

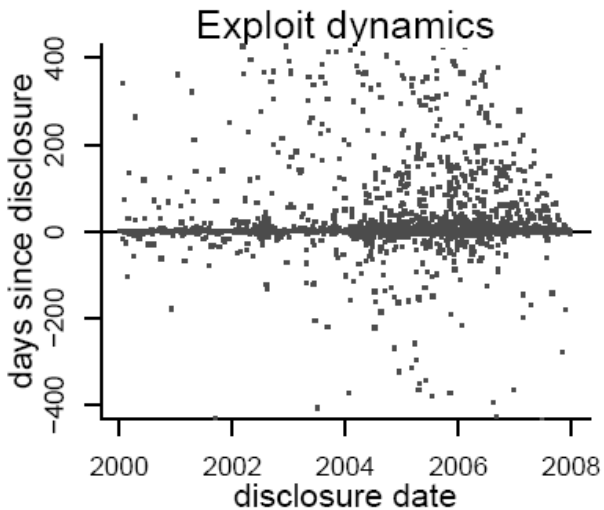
Métricas centradas en el atacante



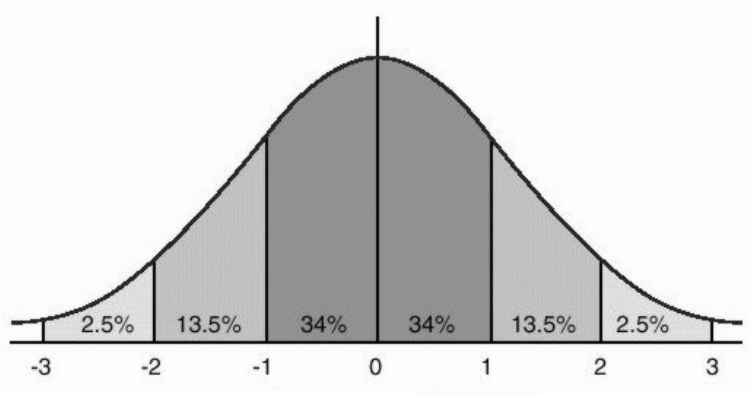
E1 : Prob. de explotar la aplicación X.



Distribución binaria (a.k.a. Bernoulli)



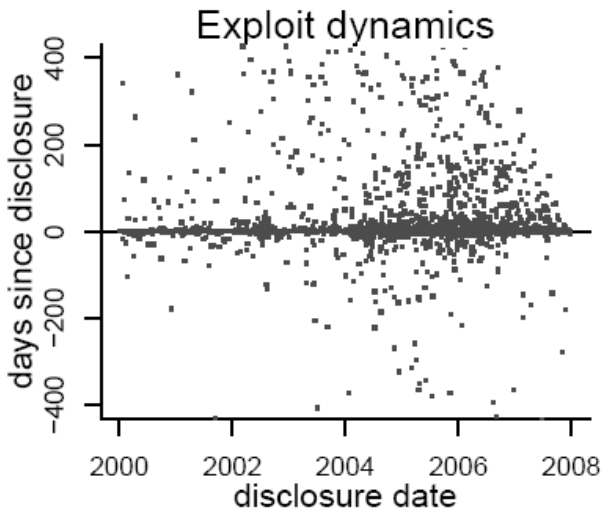
E2 : Cantidad de vulnerabilidades críticas en WinXP en los próximos 6 meses.



Distribución normal

CORE LABS RESEARCH & DEVELOPMENT

Métricas centradas en el atacante



E3 : Cantidad de correo electrónico fraudulento (phishing, client-side) recibido por semana.

E4 : Tiempo transcurrido en aplicar un patch a una máquina.

CORE LABS RESEARCH & DEVELOPMENT

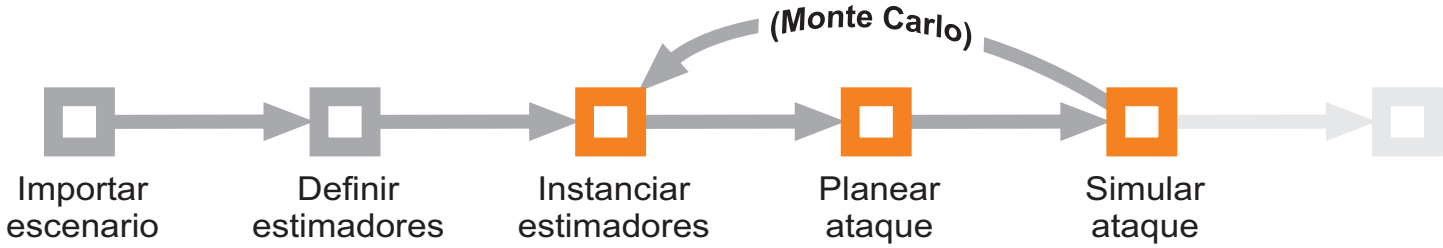
Métricas centradas en el atacante

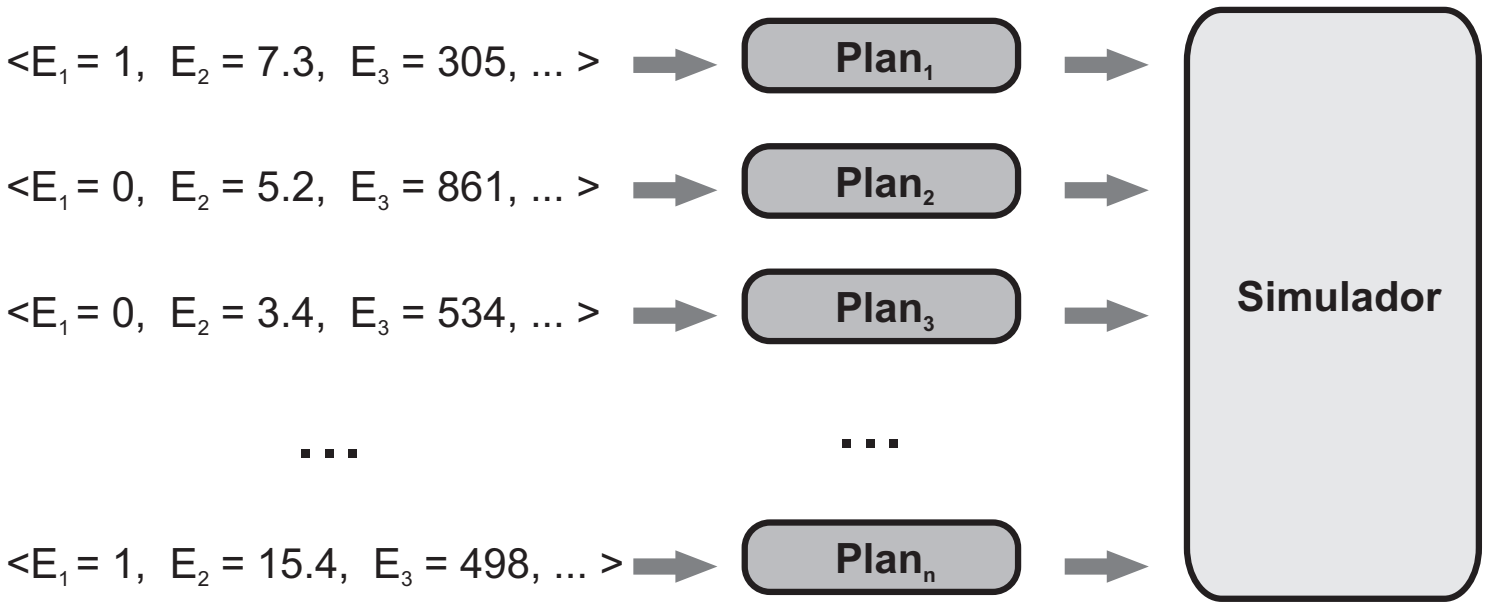
Métricas centradas en el atacante

$<E_1 = 1,\ E_2 = 7.3,\ E_3 = 305, \ldots >$ → **Plan$_1$** → Simulador

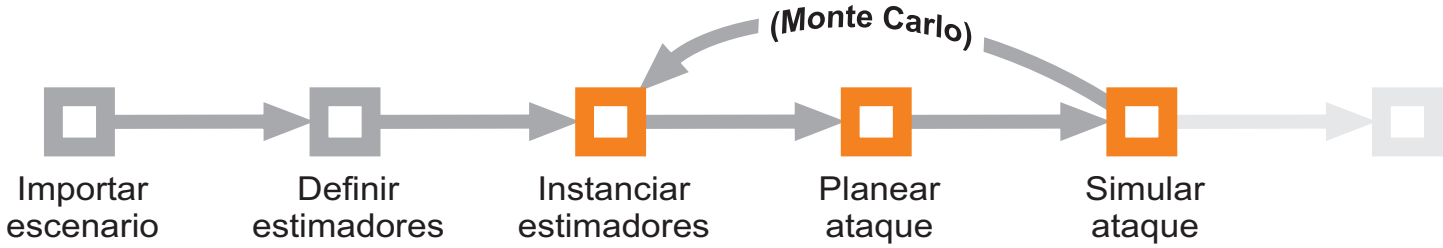
Métricas centradas en el atacante

Métricas centradas en el atacante





CORE LABS RESEARCH & DEVELOPMENT

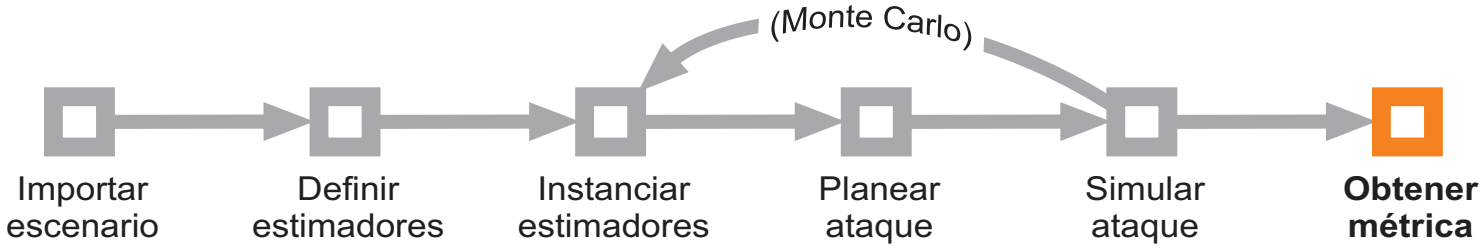


Simulaciones Monte Carlo:

1. Definir un dominio para los parámetros de entrada.
2. Generar parámetros de manera aleatoria, siguiendo distribuciones predefinidas.
3. Computar un resultado de manera determinística, usando los valores probabilísticos (o rangos).
4. Combinar los resultados en el resultado final.

CORE LABS RESEARCH & DEVELOPMENT

Métricas centradas en el atacante



Finalmente, queremos responder preguntas como:

- Dada una máquina, prob. de ser usada como pivot.
- Dada una red, prob. ser comprometida.
- Si incorporamos al modelo datos sobre el tiempo:
  - Media de tiempo necesario para comprometer un objetivo.
  - Tiempo mínimo para comprometer un asset.
  - Tiempo de respuesta ante la primer alarma.

Conclusiones

Métricas actuales

- Modelo implícito y obsoleto del atacante.
- Visión local.
- Resultados ambiguos: Riesgo alto, medio, bajo.

Métricas propuestas

- Modelo explícito del atacante (simulación de pen-tests)
- Visión global y realista.
- Resultados concretos: 1000 ataques $\rightarrow$ 5.1% exito.
- Los ataques pueden validarse con un pen-test real.

Las métricas presentadas **permiten tomar decisiones** sobre risk assesment.

CORE LABS RESEARCH & DEVELOPMENT

Conclusiones

Métricas actuales

- Modelo implícito y obsoleto del atacante.
- Visión local.
- Resultados ambiguos: Riesgo alto, medio, bajo.

Métricas propuestas

- Modelo explícito del atacante (simulación de pen-tests)
- Visión global y realista.
- Resultados concretos: 1000 ataques $\rightarrow$ 5.1% exito.
- Los ataques pueden validarse con un pen-test real.

Las métricas presentadas **permiten tomar decisiones** sobre risk assesment.

CORE LABS RESEARCH & DEVELOPMENT

Problemas a resolver

- **Simulación:** Diseño e implementación de simuladores.
  - Migrar una red real a un escenario automáticamente.
  - Incluir el tiempo como variable en las simulaciones.
- **Planning:** Desarrollar algoritmos avanzados.
- **Estimadores:** Recolección de datos para generación de modelos y estimadores estadísticos.
- **Métricas:** Diseño de nuevas y mejores métricas.

¡Gracias!

¿Preguntas?

ezequiel.gutesman@coresecurity.com
fernando.miranda@coresecurity.com

CORE LABS RESEARCH & DEVELOPMENT