

VIII JORNADAS

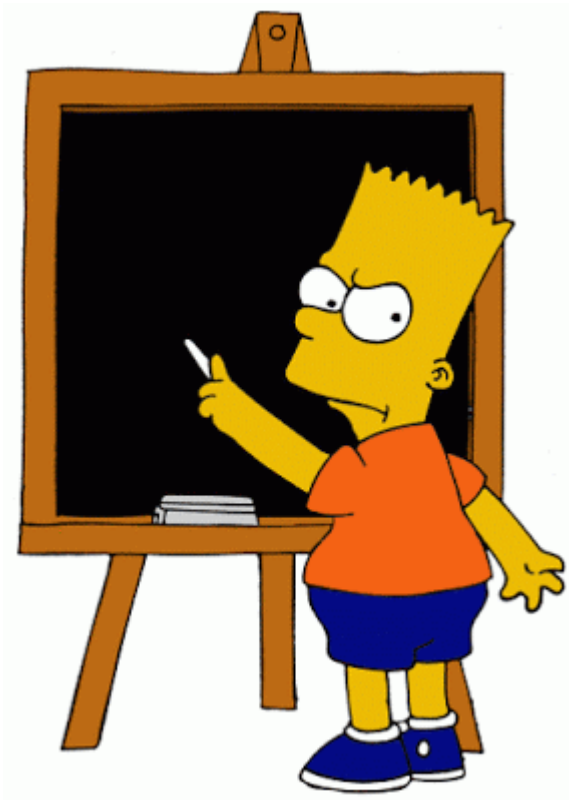
STIC CCN-CERT

La defensa del patrimonio tecnológico
frente a los ciberataques

10 y 11 de diciembre de 2014

Sendas de ataque





José A. Mañas

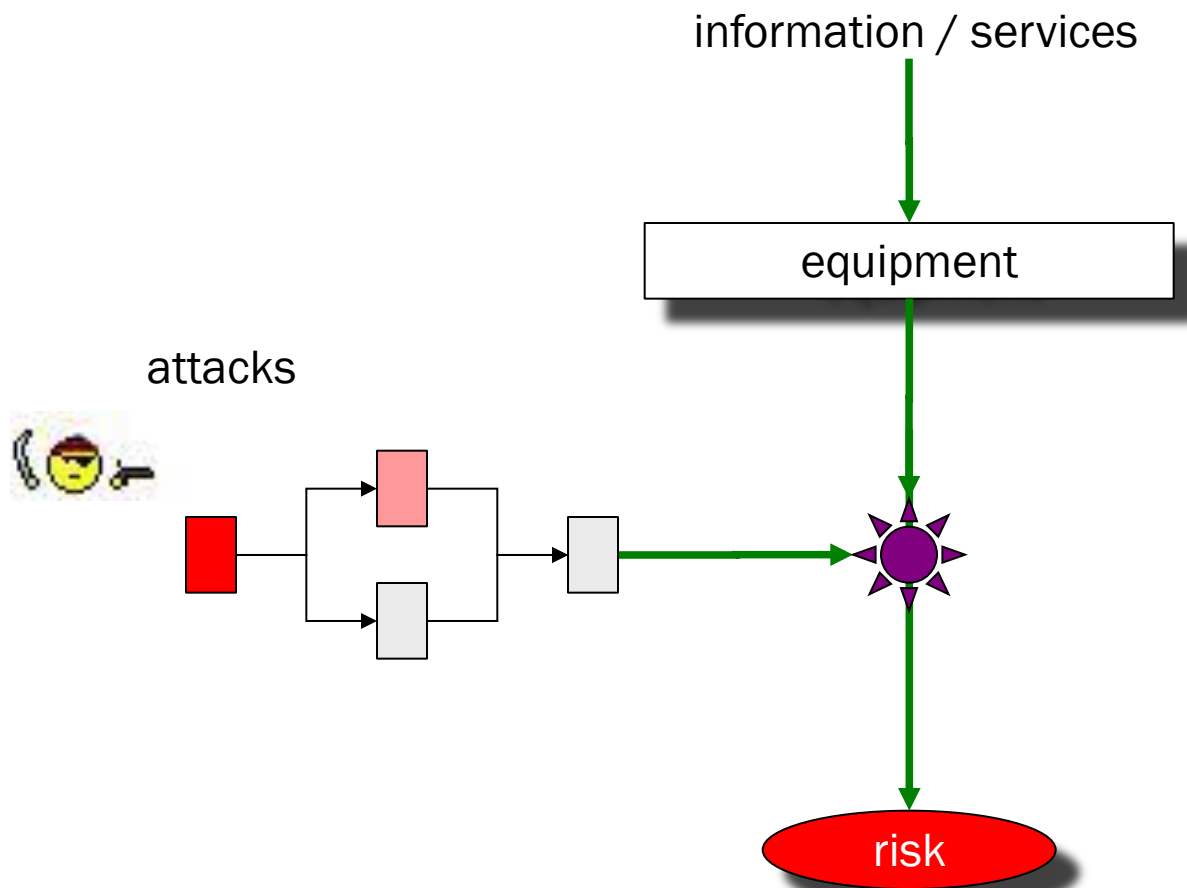
Universidad Politécnica de Madrid

jmanas@dit.upm.es

Índice

- 1 Seguridad física
 - protección del perímetro
- 2 Ciberataques
 - protección de los puntos de interconexión

Attacks



attacks



ataques

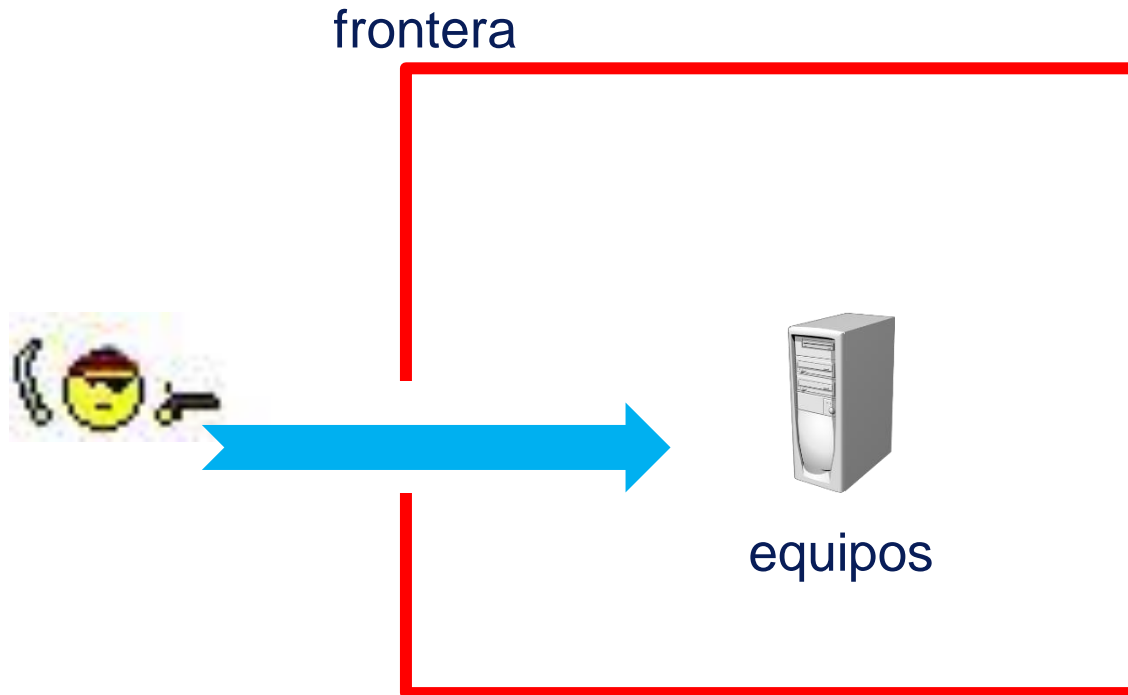
en PILAR

- A. Análisis de riesgos
 - A.1. Activos
 - A.2. Dominios lógicos
 - A.2.1. Activos
 - A.2.2. Arquitectura
 - A.2.3. Rutas de ataque
 - **A.3. Dominios físicos**
 - A.3.1. Activos
 - A.3.2. Arquitectura
 - A.3.3. Tiempos
 - A.3.4. Rutas de ataque
 - A.4. Amenazas
 - A.5. Salvaguardas
 - A.6. Impacto y riesgo

ataques

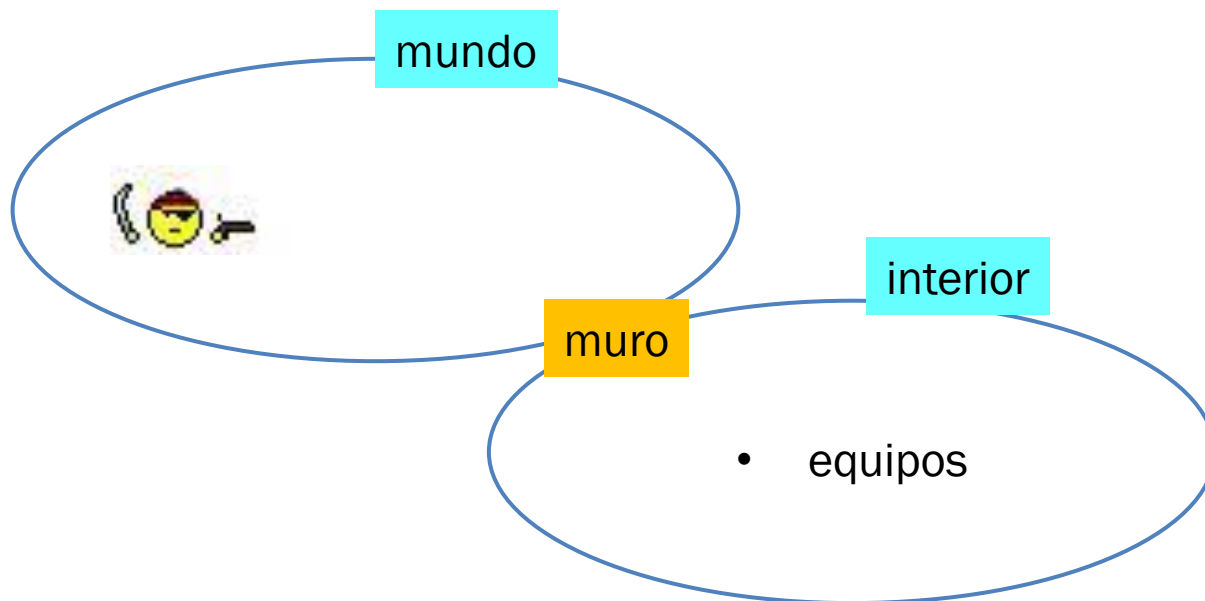
dominios físicos

- zonas físicas separadas por fronteras
- el atacante necesita atravesar el perímetro para acceder al interior



ataques

dominios físicos



activos (lo de siempre)

activo: [wall] perímetro físico - José A. Mañas (full)

código
wall

nombre
perímetro físico

Fuentes de información

dominio
[pps] seguridad física

descripción

CLASES DE ACTIVOS

- [arch] Arquitectura del sistema
 - [arch.pps] sistema de protección

☺ ⚠ ☹

ataques

dominios físicos

- este mundo se divide entre ...

The screenshot shows a network management interface with two main windows. The top window, titled 'ejemplo: dominios físicos - José A. Mañas (full)', displays a tree view of physical domains. The bottom window, titled 'dominio físico - José A. Mañas (full)', shows the configuration for a specific physical domain.

dominio físico - José A. Mañas (full) configuration:

- código: world
- nombre: el mundo exterior
- clase: EXT
- Fuentes de información: (empty field)
- descripción: (empty field)

ejemplo: dominios físicos - José A. Mañas (full) tree view:

- Domínios físicos
 - [core]
 - [D_files] Expedientes en curso
 - conexión presencial
 - conexión remota
 - usuarios
 - electrónica
 - servicio central
 - usuarios en red
 - acceso a Internet
 - [SW.SW_app] Tramitación de expedientes
 - [HW.PC] Puestos de trabajo
 - [HW.SRV] Servidor
 - [COM.LAN] Red local
 - [COM.firewall] Cortafuegos
 - [ADSL] Conexión a Internet
 - [offices] Oficinas
 - [dc] Sala de equipos
 - [wall] perímetro físico
 - [world] el mundo exterior
 - [wall] perímetro físico

- lo que está fuera
- lo que está dentro
- y cosas que están en medio

ataques

frontera

- la frontera puede estar formada por varios activos
- es necesario que haya algo de tipo PPS que es lo que detiene los ataques
- además pueden haber elementos que contribuyen a que el PPS sea eficaz
 - cámaras
 - servidores
 - personas
 - sistemas de alarma
 - ...

valoración de eficacia

1. se valora el elemento PPS que es la base de la eficacia
2. se corrige la eficacia protectora con la valoración de lo demás
 - se usan las salvaguardas de PILAR para valorar cada activo

ataques

fronteras

The screenshot shows a window titled "ejemplo: dominios físicos - José A. Mañas (full)". The interface is divided into several sections:

- Left Panel:** A tree view showing a folder named "fronteras" containing a sub-item "core / world". A yellow callout labeled "frontera" points to this folder.
- Top Right Panel:** Titled "Dominios físicos", it contains two checked items: "[core]" and "[world] el mundo exterior". A yellow callout labeled "entre zonas" points to the top of this panel.
- Middle Panel:** A horizontal separator line with a double-headed arrow. A yellow callout labeled "activos" points to this line.
- Bottom Panel:** Titled "ACTIVOS", it lists several categories with checkboxes:
 - [B] Activos esenciales: información & servicios
 - [IS] Servicios internos
 - [E] Equipamiento
 - [SS] Servicios subcontratados
 - [L] Instalaciones
 - [offices] Oficinas
 - [dc] Sala de equipos
 - [wall] perímetro físico
 - [P] Personal

At the bottom left of the "ACTIVOS" section, there is a checked checkbox labeled "PPS". A yellow callout labeled "chequeo" points to this checkbox. At the bottom right, there are three status icons: a smiley face, a question mark, and a sad face.

ataques

tiempos

ataque posible

ataque conjurado

The screenshot shows a security tool interface with a table of attack paths and a configuration dialog for a specific attack.

Table of Attack Paths:

Path	Attack Delay	Reaction Time
core [A.5] Suplantación de la identidad	-/-	-/-
core [A.11] Acceso no autorizado	-/-	-/-
core [A.25] Robo de equipos	-/-	-/-
core [A.26] Ataque destructivo	10 / 20	-15

Configuration Dialog: [world] [A.26, core]

- attack_delay: 10
- reaction_time: 20

Annotations:

- A yellow callout bubble points to the '10 / 20' value in the table, labeled "tiempo requerido para el ataque".
- A yellow callout bubble points to the '-15' value in the table, labeled "tiempo de reacción".

ataques

sendas de ataque

1. El atacante (EXT) está en su dominio (world)
 - podría entrar superando el perímetro
2. El atacante entra en la zona interna
 - puede atacar a los equipos

rutas de ataque	poten...	actual	objetivo	PILAR
EXT @ world				
core [A.5] Suplantación de la identidad	1	0,93	0,48	0,2
core [A.11] Acceso no autorizado	1	0,93	0,48	0,2
core [A.25] Robo de equipos	1	0,93	0,48	0,2
core [A.26] Ataque destructivo	1	0,93	0	0,2

sendas de ataque

1. El atacante (EXT) está en su dominio (world)
 - podría entrar superando el perímetro
2. El atacante entra en la zona interna
 - puede atacar a los equipos

ejemplo: protección de rutas - José A. Mañas (full)

Editar Exportar

probabilidad riesgo

rutas de ataque	potenc...	actual	objetivo	PILAR
rutas de ataque				
EXT @ world				
core [A.5] Suplantación de la identidad	{5,0}	{3,7}	{0,96}	{5,0}
core [A.11] Acceso no autorizado	{5,0}	{3,7}	{0,96}	{5,0}
core [A.25] Robo de equipos	{4,6}	{2,6}	{0,62}	{4,6}
core [A.26] Ataque destructivo	{5,0}	{3,7}	{0}	{5,0}

Save ? ? ?

protección de los activos → protección ruta

ejemplo: Eficacia de las salvaguardas - José A. Mañas (full)

Editar Expandir Exportar Importar Estadísticas

[base] red corporativa Fuentes de información

as...	tdp	salvaguarda	←→	judas	fuelle	com...	reco...	actual	obje...	PILAR
G	PR	[H] Protecciones Generales					8	L0-L5	L0-L5	L2-L5

ejemplo: Eficacia de las salvaguardas - José A. Mañas (full)

Editar Expandir Exportar Importar Estadísticas

[pps] seguridad física Fuentes de información

as...	tdp	salvaguarda	du...	fue...	co...	re...	act...	obj...	PIL...
F		[PPS] Protección del perímetro físico				7	L0...	L2...	L2...
F		[PPS.1] Diseño				5	L0...	L3	L3
F	PR	[L.depth] Defensa en profundidad					L1	L3	n.a.
T	EL	[L.IA] {xor} Mecanismo de autenticación				5	L1	L3	L2...
F	EL	[L.AC] Control de los accesos físicos				7	L1...	L3...	L2...
F	EL	[PPS.5] Barreras exteriores				4	L1	L3	L3
F	DC	[PPS.6] Se dispone de un sistema de detección de intrusión perimetral					L1	L3	n.a.
F	DC	[PPS.7] Se dispone de cámaras de vídeo de vigilancia					L1	L3	n.a.
F	AW	[PPS.8] El personal está concienciado y recibe formación en lo relativo a detección y reacción frente actividades sospechosas en las cercanías del recinto				2	L1	L3	L2
F	PR	[PPS.9] Iluminación de seguridad				5	L1	L3	L3
F	PR	[PPS.a] Vigilancia				5	L1	L3	L2...
F	IM	[PPS.b] La seguridad de la instalación no es responsabilidad de un único guarda				7	L0	L2	L4
F		[PPS.c] Registros de eventos:					L0	L2	n.a.

ataques

mitigación del riesgo

ejemplo: riesgo acumulado - José A. Mañas (full)

potencial actual objetivo PILAR

activo		[D]	[I]	[C]	[A]	[T]
<input type="checkbox"/>	♂ A [SRV] Servidor	{3,7}	{6,3}	{5,2}	{5,6}	
<input type="checkbox"/>	▲ [A.3] Manipulación de los registros de actividad (log)		{6,3}			
<input type="checkbox"/>	▲ [A.4] Manipulación de los ficheros de configuración	{2,4}	{4,2}	{4,2}		
<input type="checkbox"/>	▲ [A.5] Suplantación de la identidad		{4,6}	{4,6}	{5,2}	
<input type="checkbox"/>	○ [A.6] Abuso de privilegios de acceso					
<input type="checkbox"/>	○ [A.7] Uso no previsto					
<input type="checkbox"/>	▲ [A.8] Difusión de software dañino	{3,4}	{5,2}	{5,2}		
<input type="checkbox"/>	○ [A.11] Acceso no autorizado					
<input type="checkbox"/>	▲ [A.13] Repudio (negación de actuaciones)		{5,6}		{5,6}	
<input type="checkbox"/>	○ [A.15] Modificación de la información					
<input type="checkbox"/>	♂ [A.18] Destrucción de la información					
<input type="checkbox"/>	▲ [A.18] Destrucción de la información	{3,4}				
<input type="checkbox"/>	😬 EXT@world > [A.5, core]	{2,9}				
<input type="checkbox"/>	😬 EXT@world > [A.11, core]	{2,9}				
<input type="checkbox"/>	😬 EXT@world > [A.26, core]	{2,9}				
<input type="checkbox"/>	○ [A.19] Revelación de información					
<input type="checkbox"/>	▲ [A.22] Manipulación de programas	{2,9}	{5,2}	{5,2}		
<input type="checkbox"/>	○ [A.23] Manipulación del hardware					

- 1 + +1 dominio fuente gestionar leyenda html csv xml db 😊 ?

ataques

mitigación del riesgo

ejemplo: riesgo acumulado - José A. Mañas (full)

potencial	actual	objetivo	PILAR	resumen (impacto)	resumen (riesgo)	
activo	amenaza	dimensi...	riesgo	actual	objetivo	PILAR
<input type="checkbox"/> [HW.SRV] Servidor	[A.3] Manipulación de los registros de activida...	[I]	{6,3}	{4,5}	{1,0}	{1,9}
<input type="checkbox"/> [HW.SRV] Servidor	[A.15] Modificación de la información	[I]	{5,8}	{4,1}	{0,89}	{1,4}
<input type="checkbox"/> [HW.SRV] Servidor	[A.13] Repudio (negación de actuaciones)	[I]	{5,6}	{4,1}	{0,70}	{1,1}
<input type="checkbox"/> [HW.SRV] Servidor	[A.13] Repudio (negación de actuaciones)	[A]	{5,6}	{4,1}	{0,70}	{1,1}
<input type="checkbox"/> [HW.SRV] Servidor	[A.22] Manipulación de programas	[C]	{5,2}	{3,8}	{0,74}	{0,95}
<input type="checkbox"/> [HW.SRV] Servidor	[A.5] Suplantación de la identidad	[A]	{5,2}	{3,4}	{1,6}	{0,87}
<input type="checkbox"/> [HW.SRV] Servidor	[A.22] Manipulación de programas	[I]	{5,2}	{3,5}	{0,79}	{0,96}
<input type="checkbox"/> [HW.SRV] Servidor	[A.8] Difusión de software dañino	[I]	{5,2}	{3,6}	{0,48}	{0,88}
<input type="checkbox"/> [HW.SRV] Servidor	[A.6] Abuso de privilegios de acceso	[I]	{5,2}	{3,2}	{0,79}	{0,99}
<input type="checkbox"/> [HW.SRV] Servidor	[A.6] Abuso de privilegios de acceso	[C]	{5,2}	{3,5}	{0,75}	{0,97}
<input type="checkbox"/> [HW.SRV] Servidor	[A.8] Difusión de software dañino	[C]	{5,2}	{3,7}	{0,45}	{0,87}
<input type="checkbox"/> [HW.SRV] Servidor	EXT@world > [A.5, core] > [A.15] Modificació...	[I]	{5,0}	{3,2}	{0,73}	{0,91}
<input type="checkbox"/> [HW.SRV] Servidor	EXT@world > [A.11, core] > [A.15] Modificació...	[I]	{5,0}	{3,2}	{0,73}	{0,91}
<input type="checkbox"/> [HW.SRV] Servidor	EXT@world > [A.26, core] > [A.15] Modificació...	[I]	{5,0}	{3,2}	{0,73}	{0,91}
<input type="checkbox"/> [HW.SRV] Servidor	[A.25] Robo de equipos	[C]	{5,0}	{3,0}	{0,70}	{0,97}
<input type="checkbox"/> [HW.SRV] Servidor	EXT@world > [A.5, core] > [A.6] Abuso de privi...	[I]	{4,8}	{2,7}	{0,69}	{0,89}
<input type="checkbox"/> [HW.SRV] Servidor	EXT@world > [A.11, core] > [A.6] Abuso de pri...	[I]	{4,8}	{2,7}	{0,69}	{0,89}
<input type="checkbox"/> [HW.SRV] Servidor	EXT@world > [A.26, core] > [A.6] Abuso de pri...	[I]	{4,8}	{2,7}	{0,69}	{0,89}

A on off off off off off off

ataques

perfil del atacante

- In CAR we may specify attacks for internal and external origins

```
STIC_ext_en.car - Notepad
File Edit Format View Help

tsv= 2014-08-27.tsv

physical-threats:EXT= 2014-08-27_physical.xml
```

PILAR: [ejemplo] Unidad administrati

Proyecto Fichero Db Editar Nivel

Análisis cualitativo

- D. Proyecto
- A. Análisis de riesgos
 - A.1. Activos
 - A.2. Dominios lógicos
 - **A.3. Dominios físicos**
 - A.3.1. Activos
 - A.3.2. Arquitectura
 - A.3.3. Tiempos
 - A.3.4. Rutas de ataque
 - A.4. Amenazas
 - A.5. Salvaguardas
 - A.6. Impacto y riesgo
- R. Informes
- E. Perfiles de seguridad

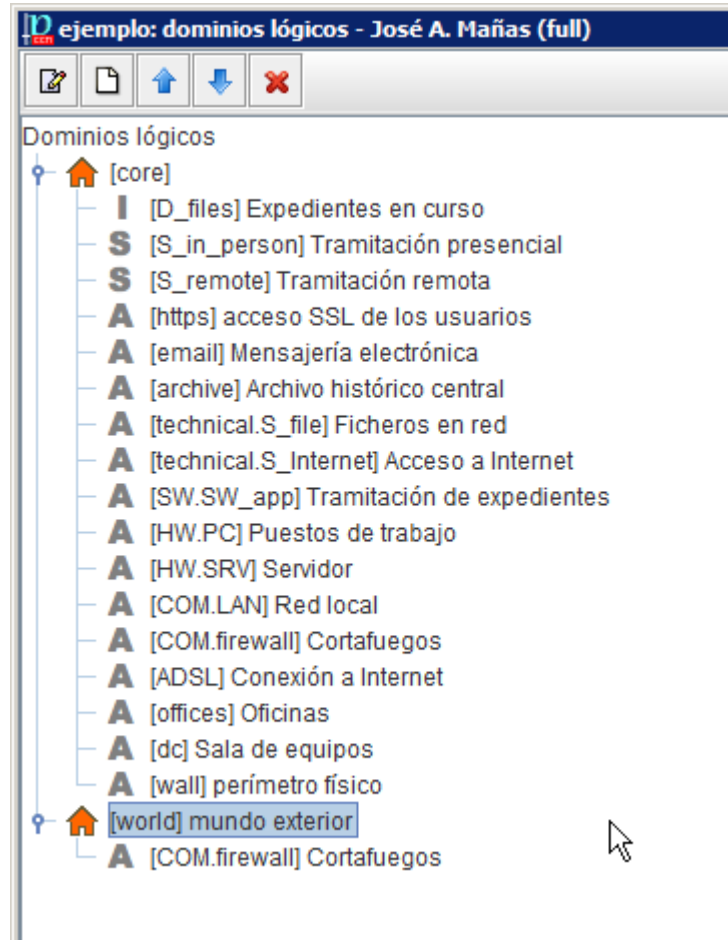
ataques

perfil del atacante

2014-08-27_physical.xml

- <threat-standard-values>
- <pps>
- <threat Z="A.5" f="1.0" follow="A" />
- <threat Z="A.11" f="1.0" follow="A" />
- <threat Z="A.25" f="1.0" follow="A.25" />
- <threat Z="A.26" f="1.0" follow="A" />
- </pps>
- <family F="HW">
- <threat f="1.0" s="1d" Z="A.6">
- <set D="D" deg="0.1"/>
- <set D="I" deg="0.1"/>
- <set D="C" deg="0.5"/>
- </threat>
- <threat f="1.0" s="1h" Z="A.7">
- <set D="D" deg="0.1"/>
- <set D="I" deg="0.01"/>
- <set D="C" deg="0.1"/>
- </threat>

ciberseguridad – interconexiones lógicas



ataques

cibe

activo: [COM.firewall] Cortafuegos - José A. Mañas (full)

código
firewall

nombre
Cortafuegos

dato	valor
descripción	equipo autónomo
administración	remota: gestionada
propietario	administrador de sistemas
cantidad	1

arriba abajo nueva eliminar estándar limpiar

Fuentes de información

dominio
[internet] conexión a internet

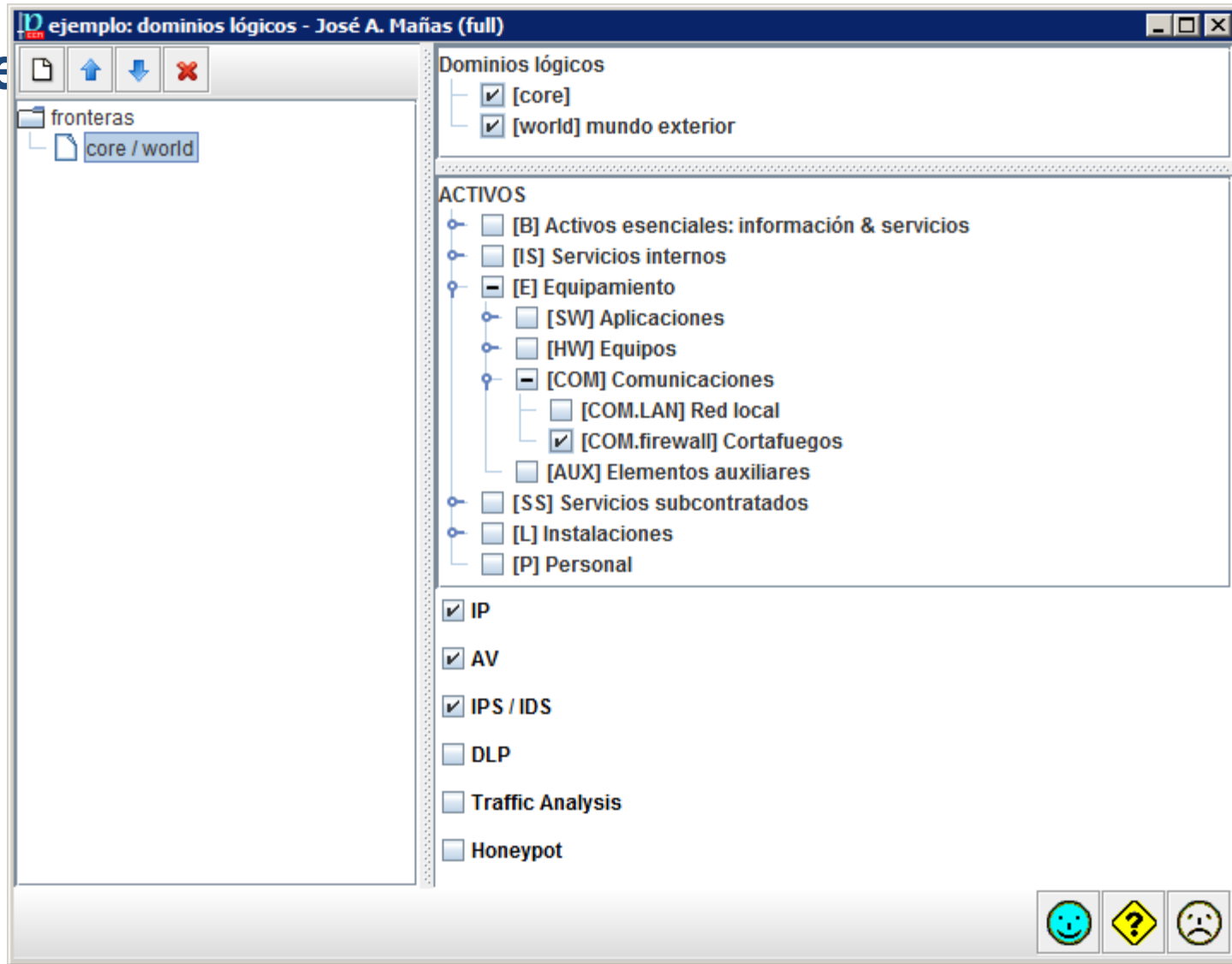
descripción

CLASES DE ACTIVOS

- [essential] Activos esencial...
- [arch] Arquitectura del siste...
 - [arch.sap] punto de [acceso al]
 - [arch.ip] punto de interconexión
 - [arch.ip.pkt] packet filter
 - [arch.ip.firewall] firewall (se
 - [arch.ip.proxy] application n
 - [arch.ip.r2p] router (2 ports)
 - [arch.ip.r3p] router (3 ports)
 - [arch.ip.dmz] 2 routers + dm
 - [arch.ip.gtwy] gateway (cha
 - [arch.ip.diode] one-way devi
 - [arch.ip.gap] air gap (air wal
 - [arch.pps] sistema de protecció
 - [or] alternativ...
- [availability] disponibilit...
- [evaluated] Productos o servicios e
- [D] Datos / Informaci...
 - [D.files] ficheros de dat...
 - [D.e-files] ficheros cifrad...
 - [D.backup] copias de respal...
 - [D.conf] datos de configuraci...
 - [D.int] datos de gestión inter...
 - [D.password] credenciales (ei

ataques

cibe



ataques

dónde estamos

- alfa
- experimentando
 - rápido para escenarios estándar
 - equilibrio entre complejidad y utilidad práctica
(que el análisis te diga qué debes proteger y qué no puedes)
- ajustando
 - perfiles de atacantes
 - salvaguardas
 - recomendaciones
- pendiente
 - μ PILAR /pps

➤ E-Mails

- ccn-cert@cni.es
- info@ccn-cert.cni.es
- ccn@cni.es
- sondas@ccn-cert.cni.es
- redsara@ccn-cert.cni.es
- carmen@ccn-cert.cni.es
- organismo.certificacion@cni.es

➤ Websites

- www.ccn.cni.es
- www.ccn-cert.cni.es
- www.oc.ccn.cni.es



Síguenos en Linked in