OSSIM

Autor: Enrique Rodríguez Rodríguez

ossim,, monitorización

Instalación

- Descargar la ISO desde http://www.alienvault.com/opensourcesim.php?section=Downloads
- Instalar la ISO siguiendo los pasos.
- Cuando se termine la instalación actualizar el Ossim.

Mapa general de Ossim

Dashboards

- Dashboards. Información de todos las áreas y datos generales, separados en diferentes secciones.
- Risk. Visualización de riesgos de forma gráfica.

Incidents

- Alarms. Listado de alarmas con opciones para administrarlas y crear informes.
- Tickets. Los tickets son tipos de incidencias que pueden ser configuradas para detectar lo que se quiera, alarmas, anomalías u otras. Aquí también se mostrarán gráficas con datos de los tickets.
- Knowledge DB. Documentos creados por usuarios que pueden ser asociados a varios elementos como hosts, redes, incidentes, etc.

Analysis

• Gestión de la seguridad del sistema. Contiene análisis de eventos y anomalías y sus estadísticas.

Reports

• Reports. Da opciones de visualizar diferentes informes y datos sobre la red o el hosts que se quiera ver, sobre las anomalías detectadas y otros modos.

Assets

- Asset Search. Posibilidad de realizar búsquedas de hosts con múltiples filtros.
- Assets. Listado de hosts registrados con posibilidad de gestionarlos.
- SIEM Components. Sensores.

Intelligence

• Configuración de políticas, acciones y directivas.

Monitors

- Network. Tenemos muchas opciones para ver datos con diferentes gráficas de servicios o por host. Por ejemplo si entramos en la pestaña Profiles y luego en Summary -> Hosts podremos ver la lista de hosts monitorizados con sus datos, pudiendo entrar en cada uno de ellos para ver mas detalles y gráficas.
- Availability. Datos de la monitorización de los hosts dados por le nagios.
- System. Información sobre los plugins instalados y su estado y la posibilidad de activarlos o desactivarlos. Actividad de los usuarios.

Configuration

• Configuración de Ossim, sus usuarios, los plugins y las actualizaciones del software.

Tools

• Herramientas para hacer copias de seguridad, descarga de utilidades y escaneos de la red.

Monitorización

Lo primero que se debería realizar es una búsqueda en la red sencilla para ver que se puede encontrar. Para eso vamos a **Tools -> Net Discovery** y configuramos la búsqueda. La primera opción es la de seleccionar la red, podremos elegir una de las que viene por defecto, una que hayamos definido nosotros antes en otro apartado del Ossim o poner la red de forma manual. La forma manual se puede poner de la siguiente manera: **192.168.1.0/24**, **192.168.1.64-68** o **192.168.1.64** en el caso de que solo sea esa la dirección que se desee escanear y no un rango de direcciones. **Enable full scan** nos da la opción de escanear los servicios de las direcciones, por defecto esta **Disable**, pero se puede poner en **Fast Scan** o **Full Scan. Timing template** nos da a elegir entre los modos de escaneo, por defecto en **normal.**

Manual Manual input	xamples: 192.168.1.0/24, 192.168.1.64-68
	Net discover options
Enable Full mode will be much slower but will inclu Fast mode w	e full scan: Disabled 💽 ude OS, services, service versions and MAC address into the inventory vill scan fewer ports than the default scan
Timing ter Paranoid a	nplate: (T3) normal

Para empezar se recomienda hacer una búsqueda general de toda el rango de direcciones, con la opción **Enable full scan** en **Disable** y el modo **normal**, para identificar todas las direcciones que tenemos disponibles. Lo siguiente sería escanear una a una las direcciones que se deseen monitorizar, con la opción **Enable full scan** en **Full Scan** y **Timing template** en **normal**. No se recomienda hacer la búsqueda de un rango de direcciones con la opción **Enable full scan** en **Full Scan** porque puede caerse el apache y no se completaría la operación.

Cuando se completa una búsqueda saldrá un mensaje: Scan completed. Click here to show the

Host 10.141.117.130 Insert

×

results. Nos llevará de nuevo al apartado de búsqueda añadiendo al final el **Scan results.** Si interesara guardar los resultados de la búsqueda en la base de datos, marcaríamos la casilla **Insert** de los host que interesa guardar y le daríamos a **Update database values.** Nos llevara a un formulario donde se nos pedirá una serie de datos, ya unos configurados por defecto y los demás no son necesarios. La que hay que tener en cuenta es la opción **Scan options**, que por defecto está desmarcada y si no se marca este host no será monitorizado por **nagios**, cosa que interesa tener. Para terminar le daremos a **OK** y será insertado el host en la base de datos si no existía y si existía será actualizado.

C	Please, select the network you want to scan:
	Manual Manual input examples: 192.168.1.0/24, 192.168.1.64-68
C.	Net discover options
Full mode wil be much s	Enable full scan: Disabled ower but will include OS, services, service versions and MAC address into the inventory Fast mode, will scan fewer ports than the default scan
Polite mod Aggress	Timing template: (T3) normal Paranoid and Sneaky modes are for IDS eviation slows down the scan to use less bandwidth and target machine resources inve and Insame modes speed up the scan (fast and reliable networks)
	Discover Manage Remote Scans
	Scan results
Mac 05	Services
00:13:72:CF:A3:7E (Dell) Microsoft Windows XP	💐 echo discard? daytime qotd chargen msrpc netbios-ssn microsoft-ds microsoft-rdp vnc-http vnc
	Update database values
	Clear scan result

Please, fill these global properties about the hosts you've scaned:

Optional group name	
Asset Value (*)	2 💓
Threshold C (*)	30
Threshold A (*)	30
RRD Profile (*) Insert new profile ?	None 💌
NAT	
Sensors (*) Insert new sensor ?	🗹 10.141.117.178 (opensourcesim
Scan options	Enable nagios
Description	
Latitude	
Lanaibuda	

Values marked with (*) are mandatory

Para ver los datos de hosts, servicios y estados en los que se encuentran deberemos ir a **Monitors** -> **Availability** o a **Dashboards** -> **Dashboards** y picar sobre la imagen de la gráfica **Availability**.



Si hay un error en la monitorización de alguno de los hosts, puede dar error en el nagios y puede que no muestre nada, en ese caso mirar que hosts son los que fallan y eliminar los servicios o hosts que sean necesarios para seguir con el funcionamiento normal del nagios.

Visualizar datos de la red

Dashboards -> Dashboards -> Network. Aquí se nos muestra alguna de las gráficas sobre datos de red. En alguna podremos picar y entrar para ver mas detalles.



Reports -> Reports nos permite ver informes detallados. Si queremos ver el estado de la red, introducimos la red y le damos a **generate**. En **General Status** veremos la información general de la red. **Inventory** nos da el nombre de la red y la lista con todos los hosts. **Network Traffic** contiene una gráfica de la distribución de los servicios y los detalles del tráfico en la red, que incluye múltiples gráficas sobre servicios procesos. En **SIEM** tenemos los datos sobre los Tickets, las Alarmas, las Vulnerabilidades y los Eventos.





Si vamos por el apartado **Monitors -> Network**, en la pestaña **Traffic** veremos una gran cantidad de gráficas y en la pestaña **Profiles** tendremos gráficas con otros datos y opciones.

Traffic

Profiles

Details | Overview | Graphs Profile | Ilive 🔻 | Alerts | Stats | P

Profile: live





En **Assets -> Asset Search** podremos buscar los host pertenecientes a una red determinada, y si lo hacemos desde la pestaña **Advanced** tendremos mas opciones de búsqueda. En **Assets -> Assets**

-> **Networks** se pueden crear, modificar o borrar redes y también se le pueden dar nombres para identificarlas. Desde aquí se puede activar o desactivar el nagios para toda una red.

Visualizar datos de hosts

Reports -> Reports nos ayuda a buscar el host que queremos ver introduciendo su dirección ip y dándole a **generate**. En **General Status** veremos la información general del host. **Inventory** nos da toda su descripción como su nombre, el sistema operativo, los servicios que tiene y datos sobre ellos. En **SIEM** tenemos los datos sobre los Tickets, las Alarmas, las Vulnerabilidades y los Eventos sobre este host.

		Genera	al Status		1		Invento	ory		Network Usage
	Service level:	100 %		Global score:	lobal score: 🗑 🕥 🛑 Host Info			Host belongs to:		
					Name	10.141.1	17.174	Net	Pvt_10	Traffic Sent
					Ip os	10.141.1	17.174	Net	Red	
					MAC	00:00:29:	38:E4:BC	SCHOOL	opensou cesm	
Ticket	ts Opened	2010-06-21 1	4:32:38	Max priority: 10	-		0	Wh	e is?	
Innesol	lead Alarms	2010-06-16-1	4:15:51	Highestrick: 1	Ser	vice	Ver	sion	Origin	
Vuln	erabilities müller			Highest Rick: - (0 events)	ssh (.	22/ip)	OpenSSH 4.3	(protocol 2.0)	Active	
SIE	M Events	2010-06-22 1	1.12.00	Highest Risk: 0 (186 erents)	http (80/ip)	Apache httpd 2	.2.3 ((CentO5))	Active	
Logg	er Events	1.1		Last Week: 8 erests	rpcbind	rpcbind (111/p) unknown		nown	Passive	Traffic Royd
An	iomales			Last Week: 0 events	rachind	rpcbind (111)p) u		0.090	Active	
Availability Events		1 A A		High Prior - (0 events)	rpcbind	rpcbind (636/ip) unknow		nown	Active	
	Avdiculary Events				100 Contractor 170	mysql (3306/lp) MySQL ((unauthorized) Passive		
_					mysal (mysal (1306/lp) 3306/lp)	MySQL (un MySQL (un	authorized) authorized)	Passive Passive	
IEM					mysql (mysql (3306/lp) 3306/lp)	MySQL (un MySQL (un	authorized) authorized)	Passive Passive	
IEM	Tickata				mysd (mysd (Alarms	1306/ip) 3306/ip)	MySQL (un MySQL (un	authorized) authorized)	Passive Passive Vuln	er abilities
IEM Ticket	Tickets	Priority	Status	Alarm	Mysql (Mysql (Alarms Risk	1306/ip) 3306/ip) Source	MySQL (un MySQL (un Destina	authorized) authorized)	Passive Passive Vuln	ar abilities
IEM Ticket ANOII	Tickets Title New Service Anomaly Incident Pandora Values ability or common	Priority 10	Status Open	Alarm Vulnerability scanning against opensourcesim-alienvault	Alarms Risk 1	1306/lp) 1306/lp) Source 10.141.117.174	MySQL (un MySQL (un Destina openaourcesiv	authorized) authorized) ition	Passive Passive Vuln	er abilities
Ticket ANOII ALAD6	Tickets Title New Service Anomaly Incident Pandora Vulnerability scanning against opensourcesim.alienvault	Priority 10 1	Status Open Open	Alarm Yulnerability scanning against opensourcesim.alienvault Yulnerability scanning against opensourcesim.alienvault	mysd (mysd (Alarms Risk 1 1	Source 10.141.127.174 10.141.127.174	MySQL (un MySQL (un Destina operatourcesin	authorized) authorized) stion nalienvauk	Passive Passive Vuln	er abilities
Ticket ANOII ALAOS	Tickets Title New Service Anomaly Incident Pandora yuheerability scanning against opensourcestim.aftenvaolt Alarma prueba Yuheerability scanning	Priority 10 1	Status Open Open	Alarm Yulnerability scanning against opensourcesim-alienvault Yulnerability scanning against opensourcesim-alienvault Yulnerability scanning against opensourcesim-alienvault	mysd (mysd (Alarms Risk 1 1 1	1306/p) 3306/p) Source 10.145.117.174 10.145.117.174 10.145.117.174 10.145.117.174	MySQL (un MySQL (un Destina operaourcesin operaourcesin operaourcesin	authorized) authorized) authorized) authorized authorized authorized authorized	Passive Passive Vuln	erabilities ound for <i>10.141.117.17</i>
TICKEEL ANOIII ALADA ALADA	Tickets Title New Service Anomaly Incident Pandora Vulnerability scanning against opensourcesim.alienvault Alaema prueba Vulnerability scanning against opensourcesim.alienvault Vulnerability scanning	Priority 10 1 1	Status Open Open Open	Alarm Vulnerability scanning against opensourcesim, alienvault Vulnerability scanning against opensourcesim, alienvault Vulnerability scanning against opensourcesim, alienvault Vulnerability scanning against opensourcesim, alienvault	Alarms Risk 1 1 1	Source Source 10.141.117.174 10.141.117.174 10.141.117.174 10.141.117.174	MySQL (un MySQL (un Destina operaourcesin operaourcesin operaourcesin	authorized) authorized) authorized) ation nalienvauk nalienvauk nalienvauk	Passive Passive Vuln	erabilities ound for <i>30.141.117.17</i>
TICKet ANOII ALA06 ALA05 ALA03	Tickets Title New Service Anomaly Incident Pandors Uninerability scanning against opensourcesim.aflenvault Vulnerability scanning against opensourcesim.aflenvault	Priority 10 1 1 1 1 1	Status Open Open Open Open	Alarm Vulnerability scanning against opensourcesim-alienvault Vulnerability scanning against opensourcesim-alienvault Vulnerability scanning against opensourcesim-alienvault	mysd (mysd (Alarms Risk 1 1 1 1	1306/p) 3306/p) Source 10.141.117.174 10.141.117.174 10.141.117.174 10.141.117.174 10.141.117.174 ▲	MySQL (un MySQL (un Destina operaourcesir operaourcesir operaourcesir	authorized) authorized) ation stion salienvauk salienvauk	Passive Passive Vuln	erabilities ound for <i>10.141.117.17</i>
IIIM Ticket AHOII ALA06 ALA05 ALA05 ALA03	Tickets Table Table New Service Anomaly Incident Pandora Unkerability scanning against opensourcestim.alienvault Alarma prueba Vulnerability scanning against opensourcestim.alienvault	Priority 10 1 1 1 1 1 1	Status Open Open Open Open Open	Alarm Vulnerability scanning against opensourcesim.alienvault Vulnerability scanning against opensourcesim.alienvault Vulnerability scanning against opensourcesim.alienvault	nysd (nysd (Alarms Risk 1 1 1 1	1305/(p) 3305/(p) Source 10.145.117.174 10.145.117.174 ↓ 10.145.117.174 ↓ 10.145.117.174	MySQL (un MySQL (un Destina opersourcesin opersourcesin opersourcesin	authorized) authorized) authorized) ation nalienvauk nalienvauk	Passive Passive Vuln	er abilities ound for <i>10.141.117.17</i>

Assets -> Assets contiene la lista de hosts identificados. Si entramos en alguno de ellos nos llevará a sus detalles como en **Reports**.

En **Monitors -> Availability** tenemos la monitorización de los servicios hecha por nagios. Tiene varias opciones de agrupamiento y si hacemos click sobre un host podremos ver sus detalles. Desde aquí se puede hacer que deje de monitorizarlo. Dentro de la pestaña Reporting podemos crear informes sobre el host que se elija.

or Lopensi	Info	Scheduling Qui	eue]			
ront Natur	ork Statue			Host Statu	is Totals	Service Status Totals
Updated: Tue ted every 90 59@ 3.0.6 - y	Jun 22 11:57:32 WEST 20 seconds	010		p Down Unreac	hable Pendin 0	Ok Warning Unknown Critical Pending 5 1 0 1 0
ed in as 7	This Host		1	All Problem	All Typer	All Problems All Types
T Include 1 1 Sec.	the treat			0	1	2 7
Service Stat	For This Host us Detail For All Hosts			-		
Service Stat	For This Host us Detail For All Hosts			Service Status	s Details For	Host
Service Stat	For This Heat us Detail For All Hosts	Status 7	I ast Check	Service Status '10.14'	s Details For 1.117.194'	Host
Service Sta	Service Contraction	Statum 1	Last Check	Service Status '10.14' Duration 1 6d 3h 19e 57s	s Details For 1.117.194'	Host States Information TCP CK - 0.067 second response time on part 10000
Service Sta	Service 1 Service 1 Service 1 Service 10000 Seneric TCP 10000	Status 7	Last Check 7 2010-06-22 11:53:35 2010-06-22 11:56 27	Service Status '10.14' Duration 1 6d 3h 19e 57s 6d 3h 19e 14s	5 Details For 1.117.194'	Host Statue Information TCP CK - 0.067 second response time on port 10000 TCP CK - 0.009 second response time on port 111
Service Sta	Service 1 Service 1 Service 1 Service 10 Service 1000 Service 100 1000 Service 100 1000	Status T Ox Of: OX	Last Check 2010-06-22 11:53 35 2010-06-22 11:56 27 2010-06-22 11:57 10	Service Status '10.14' Duration 1 6d 3h 19m 57s 6d 3h 19m 14s 6d 3h 19m 30s	s Details For 1.117.194' Attempt 1 1/4 1/4	Host Statue Information TCP CK = 0.067 second response time on port 10000 TCP CK = 0.009 second response time on port 111 TCP CK = 0.048 second response time on port 143
enications Service Sta	Service 1 Service 1 Servic	Status OK OK OK OK	Linst Check 2010-06-22 11:53-35 2010-06-22 11:56 27 2010-06-22 11:57-10 2010-06-22 11:57-10	Service Status '10.14' Duration 1 6d 3h 19n 57s 6d 3h 19n 14s 6d 3h 18n 30s 6d 3h 17n 47s	5 Details For 1.117.194' Attempt 7 1/4 1/4 1/4	Host TCP CK = 0.067 second response time on port 10000 TCP CK = 0.067 second response time on port 111 TCP CK = 0.048 second response time on port 443 TCP CK = 0.023 second response time on port 443 TCP CK = 0.023 second response time on port 671
L117.194	Service 1 Service 1 SENERC TCP 10000 OENERC TCP 10000 OENERC TCP 111 OENERC TCP 442 SENERC TCP 671 HTTP	Status OK OK OK OK WARNING	Last Check. 2010-06-22 11:53:35 2010-06-22 11:56:27 2010-06-22 11:52:48 2010-06-22 11:53:31 2010-06-22 11:53:31	Service Status '10.14' Ed 3h 18m 57s Ed 3h 18m 14s Ed 3h 18m 30s Ed 3h 17m 39	5 Details For 1.117.194' 1/4 1/4 1/4 1/4 1/4 4/6	Host Statue Information TCP CK = 0.067 second response time on port 10000 TCP CK = 0.009 second response time on port 111 TCP CK = 0.028 second response time on port 443 TCP CK = 0.023 second response time on port 671 HTTP VARING: HTTP: 1 403 Forbidden
Service Sta	Service Ser	Status OK OK OK WARNING CRITCAL	Enst Check (2010-06-22 11:53:35 2010-06-22 11:56:27 2010-06-22 11:52:10 2010-06-22 11:52:48 2010-06-22 11:53:31 2010-06-22 11:53:14	Service Status '10.14' Ed 3h 19m 57s Ed 3h 19m 14s Ed 3h 19m 14s Ed 3h 19m 32s Ed 3h 17m 47s Ed 3h 17m 3s Ed 3h 21m 23s	5 Details For 1.117.194' 1/4 1/4 1/4 4/4 4/4	Host Status Information TCP CK - 0.067 second response time on part 10000 TCP CK - 0.067 second response time on part 111 TCP CK - 0.048 second response time on part 443 TCP CK - 0.023 second response time on part 671 HTTP WARNING: HTTP/1.1403 Fortikiden Access deried for user Yagios(%710.141.117.178" (using password NO)

Si vamos por **Monitors -> Network** en la pestaña **Profiles** nos saldrá otras opciones. Entrando en **Summary -> Hosts** obtendremos la lista de los hosts. Entrando en ellos podremos ver mas información y gráficas.

ensourcesim 💓 Interface: 🛛 - No inte	rfaces found - 📉 [By host: Total By host: Sent By host: Recy Service statistic By clent-server]					
	Info about ord1298.grecasa.gobiernodecanarias.org 🖗					
IP Address	10.141.117.135 [unicast] [Purge Asset 🙆					
Custom Host Name						
First/Last Seen	Tue Jun 22 08:02:41 2010 - Tue Jun 22 12:00:15 2010 [Inactive since 0 sec]					
Subnet	10.141.117.0/24					
MAC Address 🕸	00:1E:C9:78:C4:FC					
OS Name	[Windows 2000 Advanced Server					
NetBios Name	ORD1298 (Server					
Host Location	Local (inside specified/local subnet or known network list					
IP TTL (Time to Live)	128:128 [~0 hop(s)					
Total Data Sent	1.3 MBytes/2,793 Pkts/0 Retran. Pkts [09					
Broadcast Pkts Sent	26 Pkt					
Data Sent Stats	Local Rem 0					
IP vs. Non-IP Sent	P 100 % Non-IP 01					
Total Data Rcvd	6.8 MBytes/9,089 Pkts/0 Retran. Pkts [09					
Data Rovd Stats	Local Rem 01					
IP vs. Non-IP Rcvd	IP 100 % Non-IP 0					
Sent vs. Rcvd Pkts	Sent Rcv 23.5 % 76.5					
Sent vs. Rovd Data	Sent Rcvv 16.0%					

Tickets

Introducción

Los tickets son tipos de incidencias que pueden ser configuradas para detectar lo que se quiera, alarmas, anomalías u otras.

Configuración general

Si se quiere que un ticket se abra automáticamente cuando se genera una alarma tenemos que tener la opción **Automatic Ticket Generation** habilitada, se encuentra en **Configuration -> Main.**

×

Cada vez que se encuentre una vulnerabilidad en el escaneo de un host se abrirá automáticamente un ticket. Se puede configurar el riesgo mínimo que tiene que tener una vulnerabilidad antes de que el ticket se abra. Para configurarlo ir a **Configuration -> Main** en el apartado **Vulnerability Scanner.**

Vulnerability Scan	ner		
Vulnerability Scanner con	figuratio	n	
Vulnerability Ticket Threshold	3	~	0

Si el valor es demasiado bajo creará muchos tickets después de cada exploración de vulnerabilidad, con valor 3 o 4 sólo se abrirán tickets de vulnerabilidad reales, y no cuando sean identificados los servicios en la red.

Crear un ticket

Para crear un nuevo ticket vamos a **Incidents -> Tickets** y en la parte inferior se encuentra **Insert new Ticket** y los posibles tipos de ticket que se pueden crear.

			Filter Simpl	e [change to Advanc	ed]					
	Class	Type Search	Search text in all fields In cha		large	Status	Priority	Actions		
ALL		ALL				Open 💌	ALL M	Search	Close sele	cted
	Ticket	Title	Priority	Created	Life Time	In charge	Submitter	Туре	Status	Entra
	ANO11	New Service Anomaly Incident Pandora	10	2010-06-21 14:37:30	20:06	OSSIM admin	OSSIM admin	Generic	Open	
	ALA09	New Alarm incident	9	2010-06-17 11:24:17	4 Days 23:19	javier	OS5IM admin	Anomales	Open	
	ALA06	Vulnerability scanning against opensourcesim, alienvault	1	2010-06-16 13:14:49	5 Days 21:28	OSSIM admin	OSSIM admin	Generic	Open	
	ALAOS	Alarma prueba	1	2010-06-14 10:29:45	8 Days 00:13	OSSIM admin	OSSIM admin	Generic	Open	
	ALA04	Vulnerability scanning against opensourcesim.alienvault	1	2010-06-14 10:29:11	8 Days 00:14	OSSIM admin	OSSIM admin	Net Performance	Open	
	ALA03	Yulnerability scanning against opensourcesim, alienvault	1	2010-06-14 10:28:47	8 Days 00:14	OSSEM admin	OSSIM admin	Generic	Open	
	ALAO2	Vulnerability scanning against opensourcesim.alienvault	1	2010-06-14 10:27:21	8 Days 00:16	OSSIM admin	OSSIM admin	Net Performance	Open	
	ALA01	Alarma prueba	1	2010-06-14 10:22:12	8 Days 00:21	OSSIM admin	OSSIM admin	Net Performance	Open	
										Pag.

Modificar un ticket

Para modificar un ticket lo abrimos picando en su nombre o en su id en **Incidents -> Tickets.**

 Vincular documentos. En Incidents -> Knowledge DB podemos tener guardados documentos. Estos documentos pueden ser vinculados a tickets, por ejemplo un documento que explica como quitar un troyano conocido, un mapa de red o la lista de personas con las que hay que contactar cada vez que hay un determinado problema. Para vincular uno de estos documentos vamos a la opción Link existing document dentro del ticket al que se quiera vincular.

ficket ID	Ticket	Status	Priority	Knowledge DB	Action
Name: New Service Anomaly Incident Pandora			RELATIONSHIPS for : New Service Anomaly Incident		
	Class: Anomaly			Document	
Type: Generic Greated: 2010-06-21 14:37:30 (20:12) Last Update: 20:12			prueba 💉 🖬		
			prueba	Edit commen	
ANO11	ANO11 In cherge: OSSIM admin Submitter: OSSIM admin Extra: n/a	Open	10		Delete comme
				C 2	New commen
	Host: 10.141.117.174 Port: 21 Previous Protocol (Version): [] New Protocol (Version): []				

• **Transferir ticket.** Cuando un usuario crea un ticket puede transferírselo a otro usuario con la opción **Transfer to** dentro del ticket que se quiera transferir.



- Adjuntar archivo. A un ticket se le puede adjuntar algún archivo con la opción Attachment.
- Subscribirse. Con la opción Subscribe/Unsubscribe podremos recibir correos o dejar de recibirlos cada vez que cambia algo en el ticket. El formato del correo se puede modificar en la opción Email Template en la parte superior derecha.

Last update: 2023/01/18 14:20	seguridad:monitorizacion:ossim http://wiki.intrusos.info/doku.php?id=seguridad:monitorizacion:ossim&rev=1413366227

	00100000000	100000 AV	Colort a TAC In one for meaning	
			Seet a Ho to see is meaning	
Template Labels		Subject	[own-incident] PRIORITY_STR: TITLE	
INCIDENT_NO		Body	Incident details	
TICKET_AUTHOR_MAME			Title: INCIDENT_NO - TITLE Statu: STATUS Type: CLASS - TYPE Promity: PRIORITY_JUIN (PRIORITY_STR) In charge: IN_CHARGE_NAME -(IN_CHARGE_EMAIL> Created: CREATION_DATE (LIFE_TIME ago) Tage: TAGE Exits info EXTRA_INFO Tacket details Author: TICKET_AUTHOR_NAME -TICKET_AUTHOR_EMAIL> TICKET_DESCRIPTION Actions: TICKET_ACTION Part tickets:	

Preview Reset to Defaults Save Template

- Cerrar un ticket Para cerrar o reabrir un ticket, cambiaremos la opción Status al estado en que se quiera tener, y se rellenarán los campos para explicar el motivo, por ejemplo puede ser cerrado porque se creó por un falso positivo y de esta manera no se abrirá en el futuro por este motivo.
- Clasificarlos. Para clasificar los tickets se pueden usar los tipos, que ya vienen definidos por defecto o pueden ser creados o modificados. Para crear, modificar o borrar algún tipo está la opción Types en la parte superior derecha. Para cambiar el tipo de un ticket ya creado tendremos que darle a la opción Edit comment dentro del ticket.

Ticket type	Description	Actions
Generic		
Expansion Virus		[Modify] [Delete]
Corporative Nets Attack		[Modify] [Delete]
Policy Violation		[Modify] [Delete]
Security Weakness		[Modify] [Delete]
Net Performance		[Modify] [Delete]
Applications and Systems Failures		[Modify] [Delete]
Anomalies		[Modify] [Delete]
Nessus Vulnerability		
Add n	iew type	

Title	New Service Anomaly Incident Pandora
Submitter	OSSIM admin
Priority	10 💌
Туре	Generic
Anomaly type	Generic Expansion Virus Corporative Nets Attack
Host	
Sensor	Security Weakness
Port	Net Performance Applications and Systems Failures Anomalies Nessus Vulperability
Old Protocol	
Old Version	
New Protocol	
New Version	
When	ANY

 Etiquetas. Las etiquetas pueden agregar información al ticket de forma rápida. Para agregar nuevas etiquetas lo haremos en la opción Tags, en la parte superior derecha. Vienen dos etiquetas por defecto: OSSIM_INTERNAL_PENDING. Si esta etiqueta se fija, el escáner de vulnerabilidad no se abrirá de nuevo el mismo ticket. OSSIM_FALSE_POSITIVE. Si esta etiqueta está activa, la vulnerabilidad se marcará como un falso positivo y no se volverá a abrir en un futuro análisis.



Errores

No carga la página. Puede ser que el apache esté caído. Reiniciar el servidor apache:

/etc/init.d/apache2 start

Referencias

- http://www.openredes.com/category/alienvault-usm-ossim/manuales-ejemplos-alienvault-usm-ossim/
- http://ossim.net/dokuwiki/doku.php?id=user_manual:incidents:tickets
- página principal http://www.ossim.net/
- Descargar desde http://www.ossim.com/home.php?id=download
- foro http://www.ossim.net/forum/
- turoriales http://www.alienvault.com/blog/dk/ossim/tutorials/index
- http://windowsitpro.com/article/articleid/99992/analyze-network-events-with-ossim-toolset.html

From: http://wiki.intrusos.info/ - **LCWIKI**

Permanent link: http://wiki.intrusos.info/doku.php?id=seguridad:monitorizacion:ossim&rev=1413366227



Last update: 2023/01/18 14:20