



Software libre para proteger los activos de información.

Ing. Ricardo Naranjo Faccini, M.Sc.
2024-04-26

Descargue la presentación aquí



Software libre para proteger los activos de información por Ricardo Naranjo Faccini se distribuye bajo una Licencia Creative Commons Atribución 4.0 Internacional.

<https://www.skinait.com/software-libre-para-proteger-los-activos-de-informacion-Escritos-84/>



Qué es el software libre

Software protegido con
una licencia que
garantiza su libertad a
perpetuidad.



La General Public Licence - GPL

- **Licencia (copyleft)**

- Usar.
- Distribuir / Compartir.
- Estudiar.
- Modificar.
- Acompañar con código fuente.
- No cambiar las condiciones al distribuir.

- **OpenSource Initiative**

- <https://skinait.blogspot.com/2016/01/software-libre-o-software-abierto.html>



¿Es suficiente la libertad para garantizar la seguridad?

- Al igual que en SW privado, hay software libre malo.
- No, la licencia sólo protege las libertades.
- Hay 2 formas de verificar la calidad / seguridad
 - Descargar el código fuente, verificarlo y compilar.
 - Analizar a la comunidad alrededor del software.
 - Software ampliamente utilizado.
 - Foros de discusión con actividad reciente.
 - Actualizaciones y nuevas versiones recientes.
 - Más ojos → errores saltan a la vista.
 - Documentación generosa y actualizada:
 - Manuales.
 - Videotutoriales.
 - Traducciones.



Actividades de la seguridad de la información

Preparativas

- Planificar.
- Diseñar estrategias, políticas y métodos.
- Reservar recursos.
- Identificar incidentes potenciales.
- Diseñar posibles respuestas

Preventivas

- Evitar incidentes
- Priorizar riesgos
- Seleccionar controles
- Sensibilizar y capacitar

Detectivas

- Monitoreo 24x7
- Alertas oportunas
- Conocer síntomas

Reactivas

- Contener
- Erradicar
- Remediar
- Restaurar

Retrospectivas

- Medir desempeño
- Analizar causas y consc.
- Aprender
- Revisar incidentes
- Retroalimentar
- Afinar
- Mejorar
- Reportar

Actividades

Preparativas

- Planificar.
- Diseñar estrategias, políticas y métodos.
- Reservar recursos.
- Identificar incidentes potenciales.
- Diseñar posibles respuestas



- Inventario de activos
- Valorar los riesgos
- Documentar el SGSI con las políticas
- Conformación de un equipo de trabajo
 - Competente
 - Disponible
 - Completo
- Sistema de comunicación seguro
- Autoprotección
- Establecer una línea base

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- Inventario de activos
 - TIC
 - No TIC - críticos
 - Personal
- Gestión de mesa de ayuda (Tickets)
- Base de datos de conocimientos.
 - Alimentada desde diferentes fuentes.
 - Acceso abierto para todos.
 - Construcción colaborativa/moderada.
 - Interacción con pares.
- GLPI <https://glpi-project.org/>

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preparativas

Glpi

Glpi

ParcAssistance

AccueilParc**Ordinateurs**+ 🔍 ☰

Ordinateur

Entité racine

Sous-entités

Non

Nom	My-ThinkPad-Edge-E320	Statut	Production
Lieu	paris.rivoli	Type	Notebook
Responsable technique	-----	Fabricant	LENOVO
Groupe technique	Helpdesk	Modèle	1298A8G
Usager numéro	104	Numéro de série	LR9NKZ7
Usager	glpi	Numéro d'inventaire	331-14
Utilisateur	glpi	Réseau	-----
Groupe	Devs		
Domaine	local		
UUID	725BA801-507B-11CB-95E6-C6605	Commentaires	
Source de mise à jour	FusionInventory		

Créé le

Dernière mise à jour le 16-03-2018 16:55

Sauvegarder

Mettre à la corbeille

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preparativas

Glpi

Rechercher

Français ? ☆ 🐛 ⚙️ glpi ➡️

Outils Administration Configuration

Entité racine (Arborescence) super-admin

Systèmes d'exploitation 1 Composants 24 Volumes 3 Logiciels 2919 Connexions 11 Ports réseau 3 Gestion 1

Composants

Type de composant	Caractéristiques					Inventaire automatique	Actions	
Processeur	Fabricant		Fréquence (MHz)	Numéro de série	Lieu			
Intel(R) Core(TM) i5-2450M CPU @ 2.50GHz +	Intel	Mettre à jour	2500	Not Supported by CPU	paris.rivoli	Oui		
Mémoire	Type	Fréquence	Taille (Mio)	Numéro de série	Lieu			
DDR3 - SODIMM +	DDR3	1333 MHz	Mettre à jour	4096	947C2F3B	paris.rivoli	Oui	
			Mettre à jour	4096	B52A5D9F	paris.rivoli	Oui	
Disque dur	Fabricant		Capacité (Mio)	Numéro de série	Lieu			
ST320LT020-9YG142 +	Seagate	Mettre à jour	312571	W0430SS2	paris.rivoli	Oui		
M4-CT032M4SSD3 +	M4-CT032M4SSD3	Mettre à jour	31266	00000000130109246B3F	paris.rivoli	Oui		
Carte graphique				Lieu				
Intel(R) HD Graphics 3000 +		Mettre à jour		paris.rivoli	Oui			

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preparativas

Glpi

The screenshot displays the GLPI web interface. The top navigation bar includes 'Assets', 'Assistance', 'Management', 'Tools', 'Administration', and 'Setup'. The 'Assistance' section is active, and the 'Tickets' sub-section is selected. The main content area shows the ticket history for 'Network is unreachable (Root entity)'. The history includes several actions: a user post 'Great, that works, thank you!', an admin post 'Indeed, you should have 2.2.3.6 and 2.2.3.7. This should be fixed now!', a user post 'DNS have changed to 1.2.3.6 and 1.2.3.7 but this does not work either :(', an admin post 'This was wrong. We have changed configuration to fix that.', a user post 'I have 1.2.3.4 on primary and 1.2.3.5 on secondary.', an admin post 'Could you please tell us which DNS are configured?', and a final user post 'Network is unreachable' with the description 'Network is unreachable on my computer.' The interface also shows a sidebar with various menu items like 'Ticket', 'Processing ticket', 'Statistics', 'Approvals', 'Knowledge base', 'Items', 'Costs', 'Project tasks', 'Problems', 'Changes', 'Historical', and 'All'.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Installed Discover

All Filter plugin list Alpha ASC

Airwatch connector  Connector to gather inventory information from Airwatch ★★★★★ GPL v2+ Teclib, Walid Nouh 1.5.0-rc1	Barcode  This plugin allow you to generate bars code ★★★★★ AGPL v3+ David Durieux 2.5.0-rc2	Branding  ★ Network Basic Branding GLPI plugin. ★★★★★ GPL V3+ TECLIB' 1.1.0-rc1	Collaborative tools  ★ Network Basic Collaborative tools connectors ★★★★★ TECLIB' 1.1.0-rc1
Credit  This plugin allows you to declare and follow (by entity) the consumptions of different credit vouchers directly from the Ticket form. ★★★★★ GPLv3 TECLIB' 1.8.0-rc1	Escalade  This plugin simplifies the ticket escalation to different groups ★★★★★ GPL v2+ TECLIB', Alexandre Delaunay 2.5.0-rc1	Fields  The fields plugin allows you to add custom fields on glpi types : tickets, computers, users... ★★★★★ GPL v2+ Walid Nouh, François Legastelois... 1.11.0-rc1	Generic Objects Management  Do the inventory of new, non-native object types ★★★★★ GPL v2+ Walid Nouh 2.9.0-rc1
Inventory Number Generation  Inventory numbers generation ★★★★★ GPL v2+ Walid Nouh 2.5.0-rc1	ItilCategory Groups  This plugins aims to filter assignable groups in ticket by selected category ★★★★★ GPL v2+ Walid Nouh, François Legastelois... 2.4.0-rc1	MantisBT synchronization  This plugin allows to synchronize tickets, problems and changes with the MantisBT tool. ★★★★★ GPLv3 TECLIB' 4.4.0-rc1	Metabase  This plugin eases integration of GLPI with Metabase ★★★★★ AGPLv3 TECLIB' 1.1.0-rc1

< 1 2 3 > 25 plugins

Your plugin here ? [Contact us.](#) ✉️

- Automatización de procesos
- Acceso remoto
 - Xorg / wayland
 - Procesos en grupo

```
[localhost ~]$ crontab
```

- Criptografía

- Generación de huellas digitales
- Criptografía simétrica
- C

```
[localhost ~]$ ssh  
[localhost ~]$ gsh
```

```
[localhost ~]$ openssl  
[localhost ~]$ gnupg  
[localhost ~]$ cksum  
[localhost ~]$ sha256sum  
[localhost ~]$ sha512sum
```

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Conocer el equipo x línea de comandos

```
[localhost ~]$ acct  
[localhost ~]$ who  
[localhost ~]$ which  
[localhost ~]$ inxi  
[localhost ~]$ lsblk  
[localhost ~]$ lspci  
[localhost ~]$ hdparm  
[localhost ~]$ cat /proc/cpuinfo  
[localhost ~]$ cat /proc/meminfo
```

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- Sistema de gestión de seguridad de la información.
 - Políticas de seguridad de la información.
 - Controles establecidos.
 - Política de tratamiento de datos personales.
- Documentarlo.
- Hacerlo aprobar por la junta directiva.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



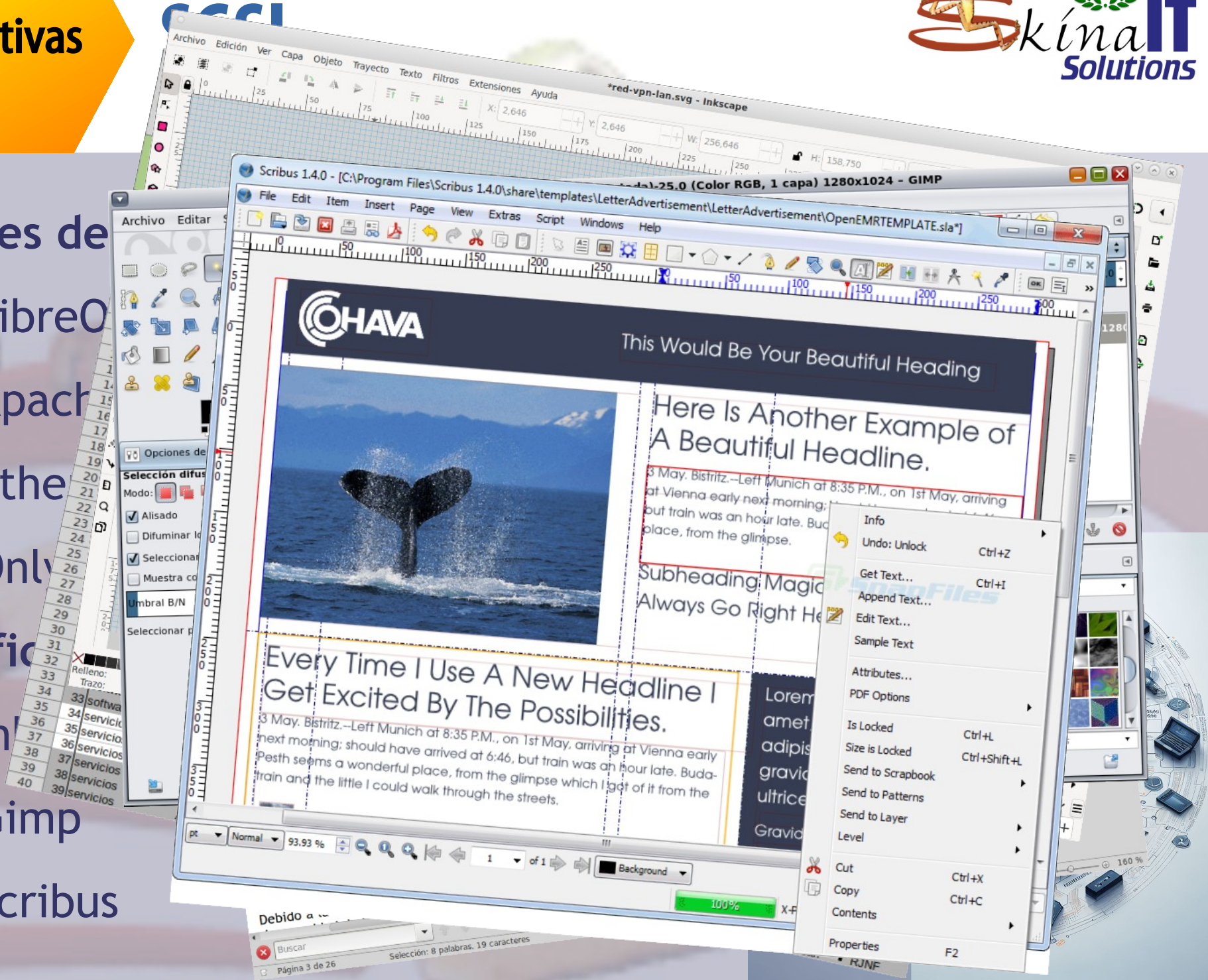
Preparativas

- Suites de

- LibreOffice
- Apache
- Ethernet
- Only

- Gráficos

- Inkscape
- Gimp
- Scribus



Preparativas

Comunicaciones



jitsi.org

1 Reunión Grupo Internacional Territoriosen Conflicto Fase 2

48:12

20

REC

1995 Conformación de comunidades

OFFICIAL linux slackware 2 DISC SET VERSION 3.0

ELF BINARIES!

The Internet's favorite 32-bit multiuser Operating System

READY-TO-RUN INCLUDES KERNEL 1.2.13 & 1.3.18

UNIX

Software Freedom Day

Homenaje a:
Luis Eduardo
Cano Oliveira
#HastaSiempreLuis

CC BY ND

Prezi

Ing. Ricardo Naranjo Faccini, M.Sc.

Jitsi meet

- OBS (transmisión de video)

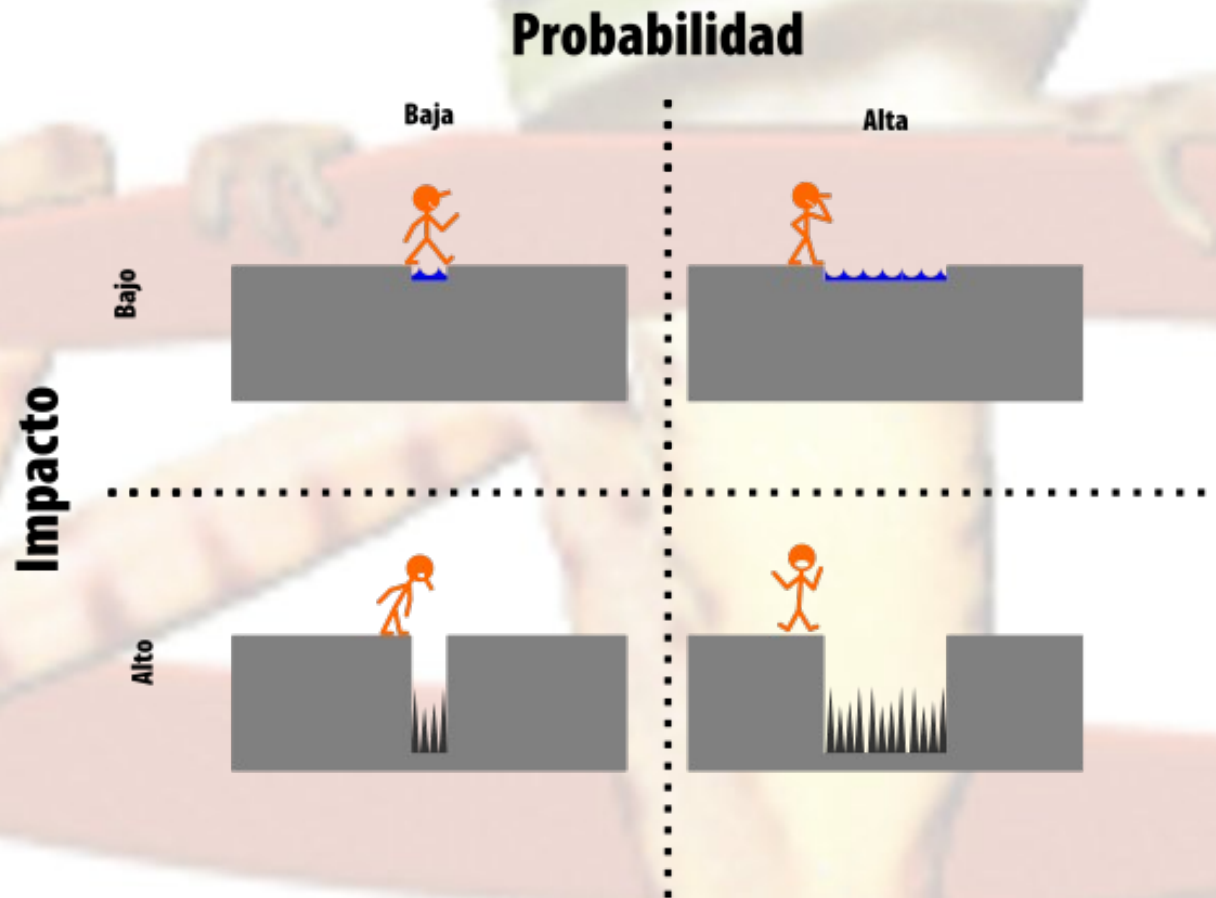
Preparativas

Preventivas

Detectivas

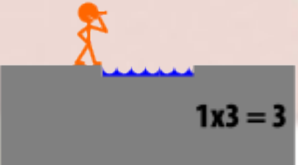
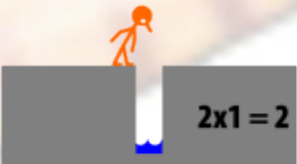
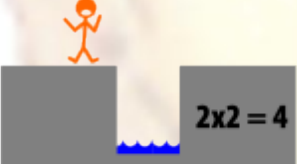
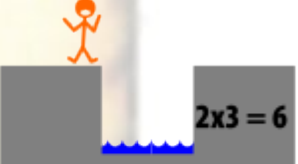
Reactivas

Retrospectivas



Nivel de Impacto de pérdida o daño

Probabilidad de ocurrencia de incidentes

	Baja (1)	Media (2)	Alta (3)
Bajo (1)	 $1 \times 1 = 1$	 $1 \times 2 = 2$	 $1 \times 3 = 3$
Medio (2)	 $2 \times 1 = 2$	 $2 \times 2 = 4$	 $2 \times 3 = 6$
Alto (3)	 $3 \times 1 = 3$	 $3 \times 2 = 6$	 $3 \times 3 = 9$

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- **Inteligencia de amenazas:**
 - Indagar cuales amenazas existen en el entorno.
 - Valorar la probabilidad de que ocurra la amenaza.
- **Análisis de vulnerabilidades:**
 - Basado en el inventario de activos.
 - Que exponen al activo a alguna amenaza.
- **Dar una valoración a cada riesgo**
 - Multiplicando la probabilidad de ocurrencia de una amenaza por el impacto de pérdida o daño del activo.
- **Planear la implementación de los controles**
 - De acuerdo con los recursos disponibles (económicos, temporales, personal y tecnología).
 - Utilizando una matriz de Eisenhower.
 - Calcular cuánto mitiga el riesgo como un valor porcentual.

Preparativas

Preventivas

Detectivas

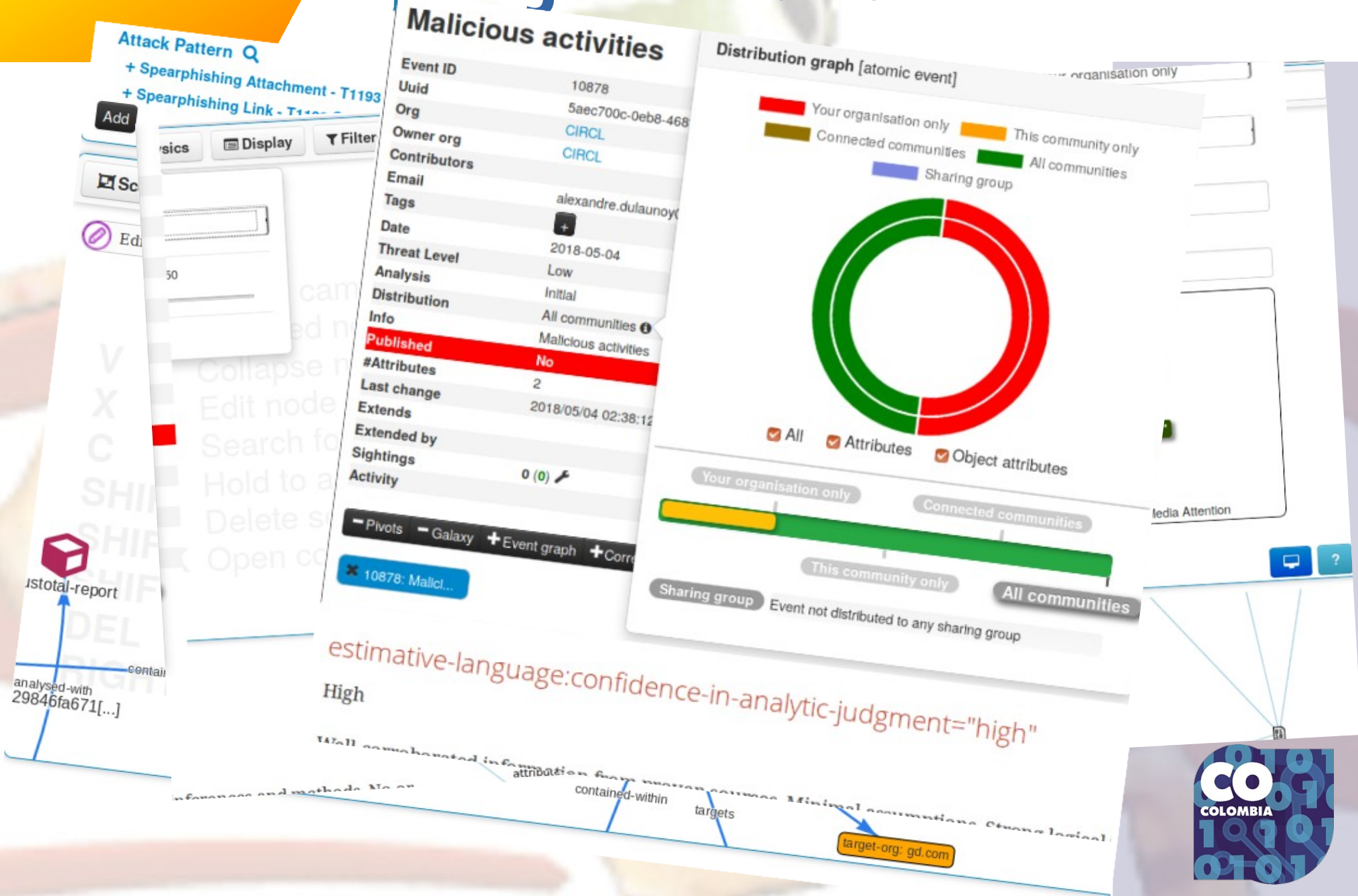
Reactivas

Retrospectivas



Preparativas

MISP: Threat Intelligence Platform

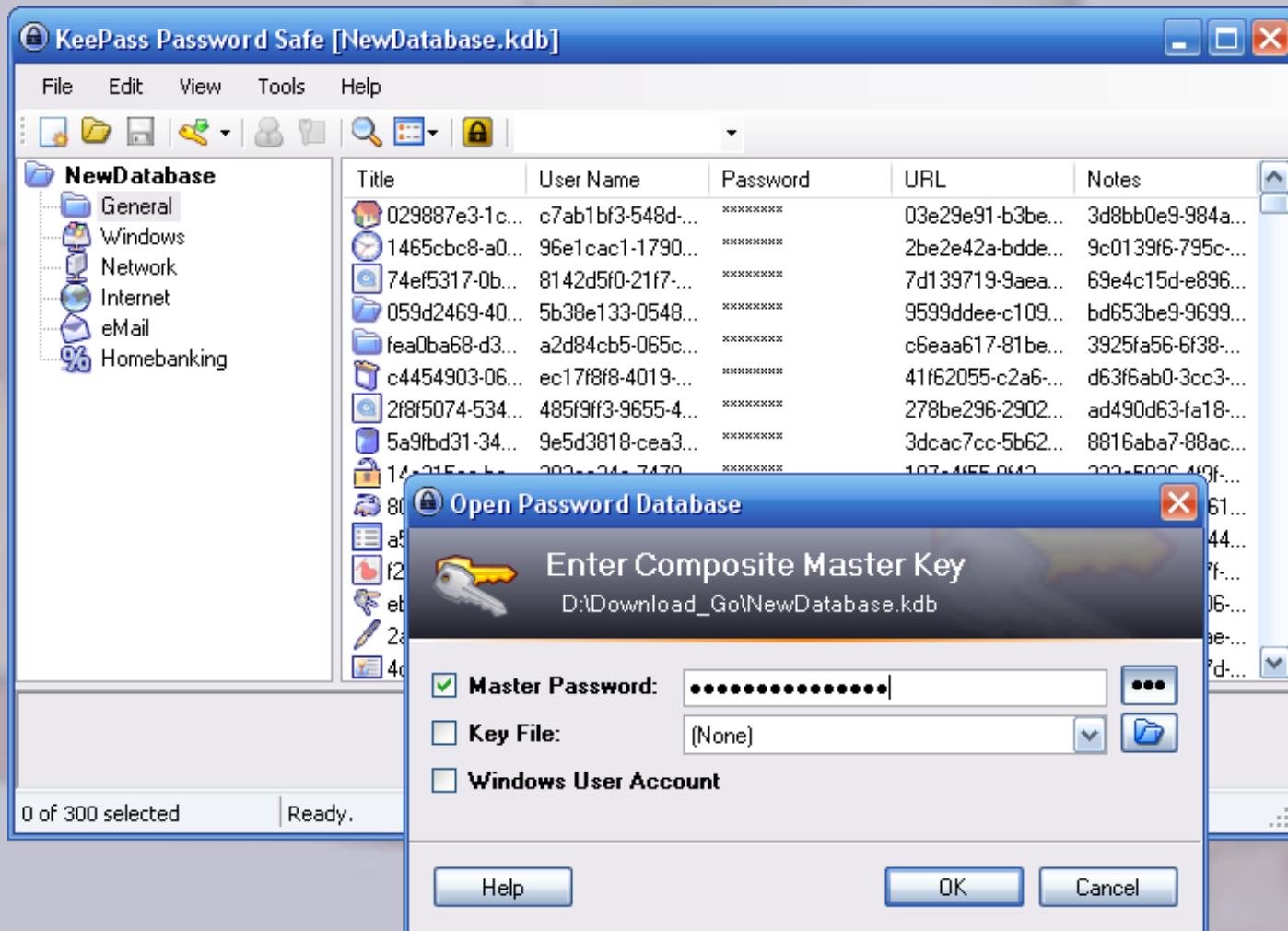


Preparativas

Maltego



• Keepass



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

A large green frog is perched on a red ledge, looking towards the camera. The frog's body is green with lighter green spots, and its eyes are large and white with black pupils. The background is a plain, light-colored wall.

Actividades

A photograph showing a crowd of people at a bullfight. In the foreground, a man in a black t-shirt and white shorts stands with his back to the camera, talking on a mobile phone. To his right, a brown bull is running. In the background, many people are sitting on bleachers, watching the event.

Preventivas

- Evitar incidentes
- Priorizar riesgos
- Seleccionar controles
- Sensibilizar y capacitar

- Dimensiones de la seguridad
- Defensa en profundidad
- Verificación de eventos sospechosos
- Actualización del inventario y las vulnerabilidades
- Realizar pruebas de penetración
- Capacitación / Sensibilización al personal
- Backups / Continuidad del negocio
- Implementar controles y auditar

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Organizar una arquitectura de SI

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Vulnerabilidades

Capas de seguridad

de las aplicaciones

de los servicios

de la infraestructura

8 dimensiones de la seguridad

Control de acceso

Autenticación

No repudio

Confidencialidad

Comunicaciones

Integridad

Disponibilidad

Privacidad

Amenazas

Ataques

Preventivas

Defensa en profundidad



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Defensa en profundidad



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- Seguridad física (Instalaciones)
 - Puertas, muros, ventanas, cercas, cubículos de acceso, perros, cámaras, campos minados, artillería antiaérea.
- Seg. de perímetro y red y de puntos finales.
 - Firewalls perimetrales
 - Configuración de enrutadores, protección del cableado
 - Monitoreo espectro electromagnético
 - Monitoreo / Firewalls perimetrales / Enrutadores / Proxys / IDS / IPS / aud. Logs.
 - OSSIM (alienvault) / SOAR.
 - Honeypots

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Defensa en profundidad



Preparativas

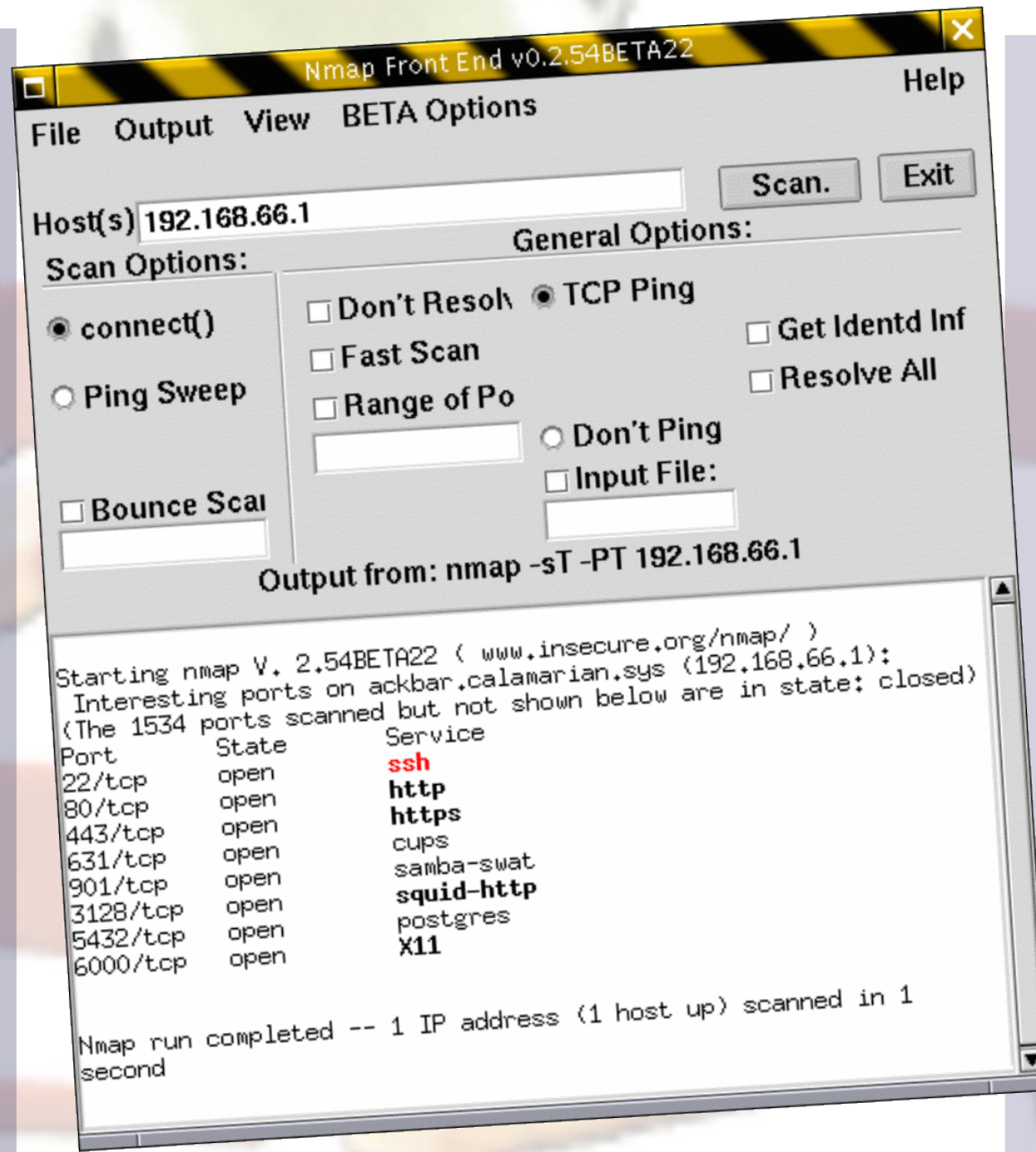
Preventivas

Detectivas

Reactivas

Retrospectivas

- Revisar puertos
- Previene troyanos
- Genera huellas digitales



Preparativas

Preventivas

Detectivas

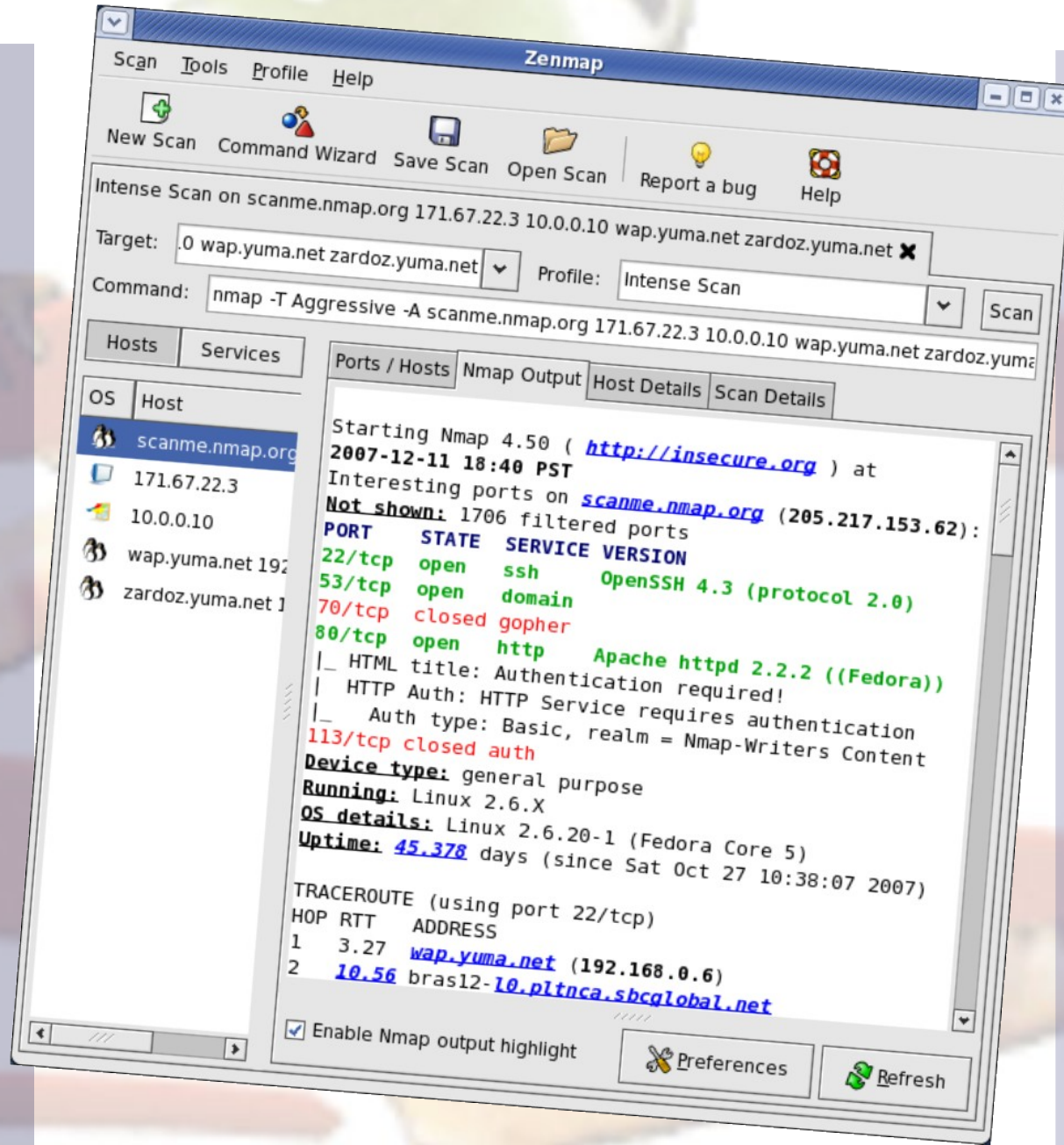
Reactivas

Retrospectivas

Preventivas



- Revisar puertos
- Previene troyanos
- Genera huellas digitales



Preparativas

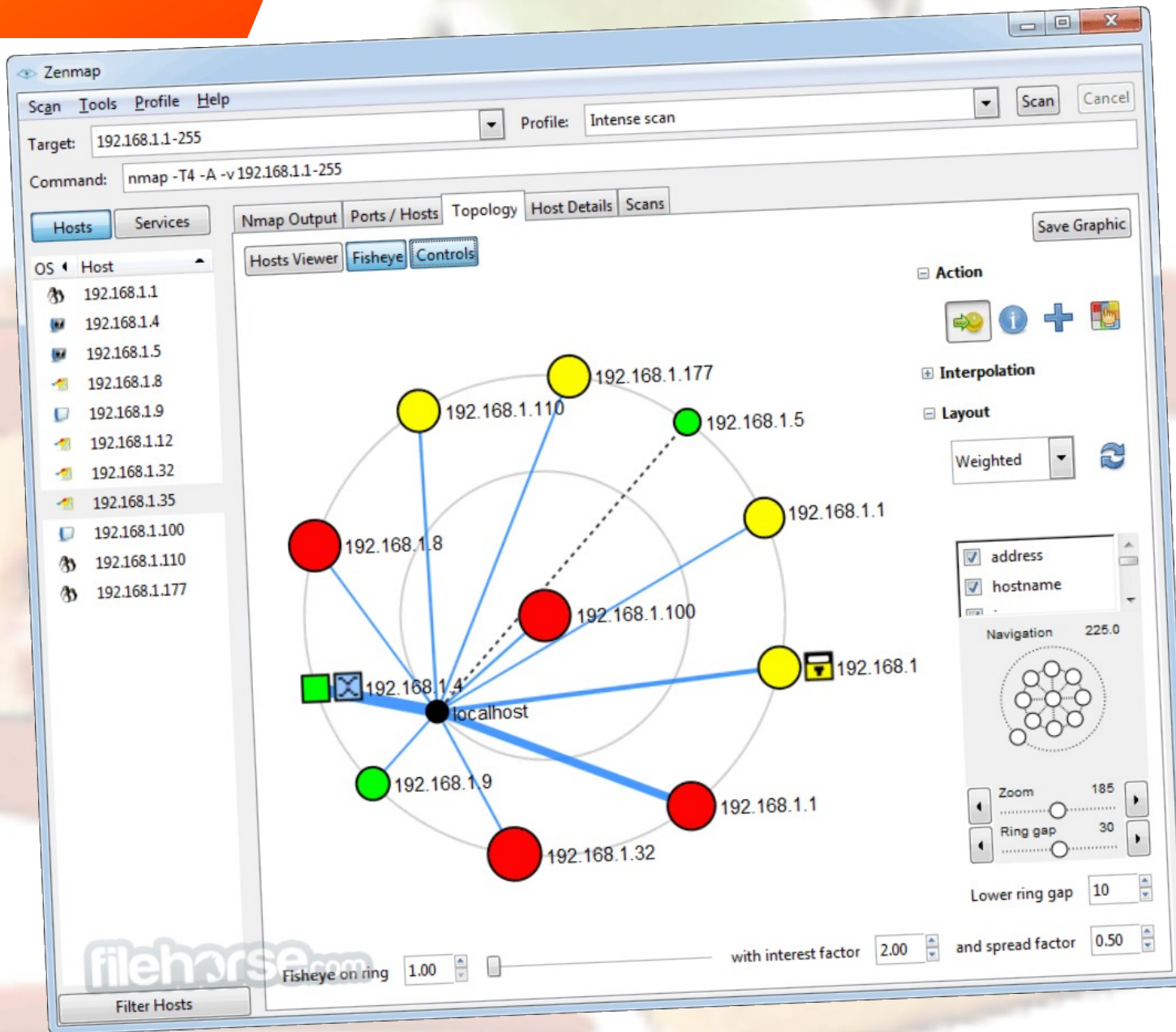
Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas



test.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: tcp

No.	Time	Source	Destination	Protocol	Info
11	1.226156	192.168.0.2	192.168.0.1	TCP	3196 > http [SYN] Seq=0 Len=0 MSS
12	1.227282	192.168.0.1	192.168.0.2	TCP	http > 3196 [SYN, ACK] Seq=0 Ack=
13	1.227325	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=1 Ack=1 Win
14	1.227451	192.168.0.2	192.168.0.1	HTTP	SUBSCRIBE /upnp/service/Layer3For
15	1.229309	192.168.0.1	192.168.0.2	TCP	http > 3196 [ACK] Seq=1 Ack=256 W
16	1.232421	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3196 [
17	1.248355	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [SYN] Seq=0 Len=0 MSS
18	1.248391	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [SYN, ACK] Seq=0 Ack=
19	1.250171	192.168.0.1	192.168.0.2	HTTP	HTTP/1.0 200 OK
20	1.250285	192.168.0.2	192.168.0.1	TCP	3196 > http [FIN, ACK] Seq=256 Ac
21	1.250810	192.168.0.1	192.168.0.2	TCP	http > 3196 [FIN, ACK] Seq=114 Ac
22	1.250842	192.168.0.2	192.168.0.1	TCP	3196 > http [ACK] Seq=257 Ack=115
23	1.251868	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [ACK] Seq=1 Ack=1 Win
24	1.252826	192.168.0.1	192.168.0.2	TCP	http > 3196 [FIN, ACK] Seq=26611
25	1.253323	192.168.0.2	192.168.0.1	TCP	3197 > http [SYN] Seq=0 Len=0 MSS
26	1.254502	192.168.0.1	192.168.0.2	TCP	http > 3197 [SYN, ACK] Seq=0 Ack=
27	1.254532	192.168.0.2	192.168.0.1	TCP	3197 > http [ACK] Seq=1 Ack=1 Win

Frame 11 (62 bytes on wire, 62 bytes captured)

Ethernet II, Src: 192.168.0.2 (00:0b:5d:20:cd:02), Dst: Netgear_2d:75:9a (00:09:5b:2d:75:9a)

Internet Protocol, Src: 192.168.0.2 (192.168.0.2), Dst: 192.168.0.1 (192.168.0.1)

Transmission Control Protocol, Src Port: 3196 (3196), Dst Port: http (80), Seq: 0, Len: 0

0000 00 09 5b 2d 75 9a 00 0b 5d 20 cd 02 08 00 45 00 ..[-u...]E.
0010 00 30 18 48 40 00 80 06 61 2c c0 a8 00 02 c0 a8 ...O.H@... a,.....
0020 00 01 0c 7c 00 50 3c 36 95 f8 00 00 00 00 70 02 ...|.P<6p.
0030 fa f0 27 e0 00 00 02 04 05 b4 01 01 04 02
P: 120 D: 103 M: 0 [Expert: Error]

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

*Wi-Fi

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
42	43.774186	38:37:82:7f:b1:63	IntelCor_43:b1:01	ARP	42	192.168.1.1 is at 38:37:82:7f:b1:63
43	44.443928	192.168.1.12	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
44	44.445996	192.168.1.12	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
45	44.448048	192.168.1.12	192.168.1.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
46	44.450067	192.168.1.12	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
47	44.451904	192.168.1.12	255.255.255.255	DB-LSP...	176	Dropbox LAN sync Discovery Protocol
48	45.653923	fe80::ffff:ffff:fffe	ff02::2	ICMPv6	103	Router Solicitation
49	45.746010	fe80::8000:5337:10	fe80::ffff:ffff:fff	ICMPv6	153	Router Advertisement

Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: LiteonTe_53:f1:ad (a4:db:30:53:f1:ad)
Sender IP address: 192.168.1.12
Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.1.1

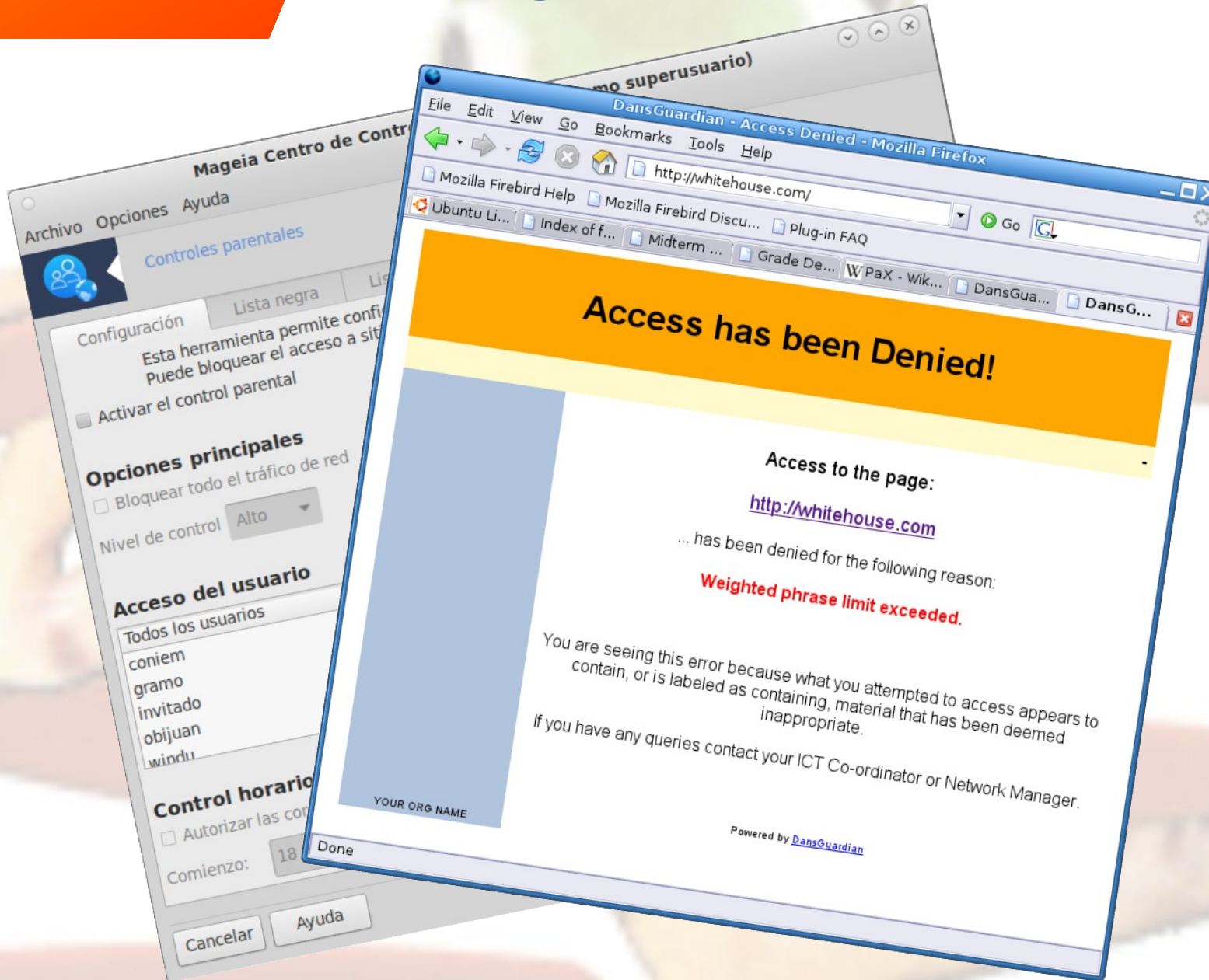
0000 ff ff ff ff ff ff a4 db 30 53 f1 ad 08 06 00 01 0S.....
0010 08 00 06 04 00 01 a4 db 30 53 f1 ad c0 a8 01 0c 0S..
0020 00 00 00 00 00 00 c0 a8 01 01

Sender MAC address (arp.src.hw_mac), 6 bytes

Packets: 50 · Displayed: 50 (100.0%) Profile: Default

Preventivas

e2guardian Dansguardian



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

AIDE - advanced intrusion detection system

- Saca huellas digitales de archivos
- Identifica modificaciones

```
AIDE 0.15.1 found differences between database and filesystem!!
Start timestamp: 2014-10-03 14:55:18

Summary:
Total number of files:      34002
Added files:                0
Removed files:              0
Changed files:              1

-----
Changed files:
-----
changed: /etc/aide.conf      Values stored in the aide DB

-----
Detailed information about changes:
-----

File: /etc/aide.conf
Size      : 4848
Perm      : -rw-----
Mtime     : 2014-10-03 14:46:09
Ctime     : 2014-10-03 14:52:09
SHA256    : j5k2ZaCE/NoRtFB4Q/itSS2TBRJdaUvk
SHA512    : D90rBEXYENjL9Btg9W0XZx9qgWe+E0kk
ACL       : old = A:

, 4873
, -rw-r--r--
, 2014-10-03 14:55:08
, 2014-10-03 14:55:08
, zAW7uQB1QqWe0oGQ0H1pwC90PkQUTGgP
, UXFv5t0YTji85i9f65ECQ5LVokqG9k/y
```

Preparativas

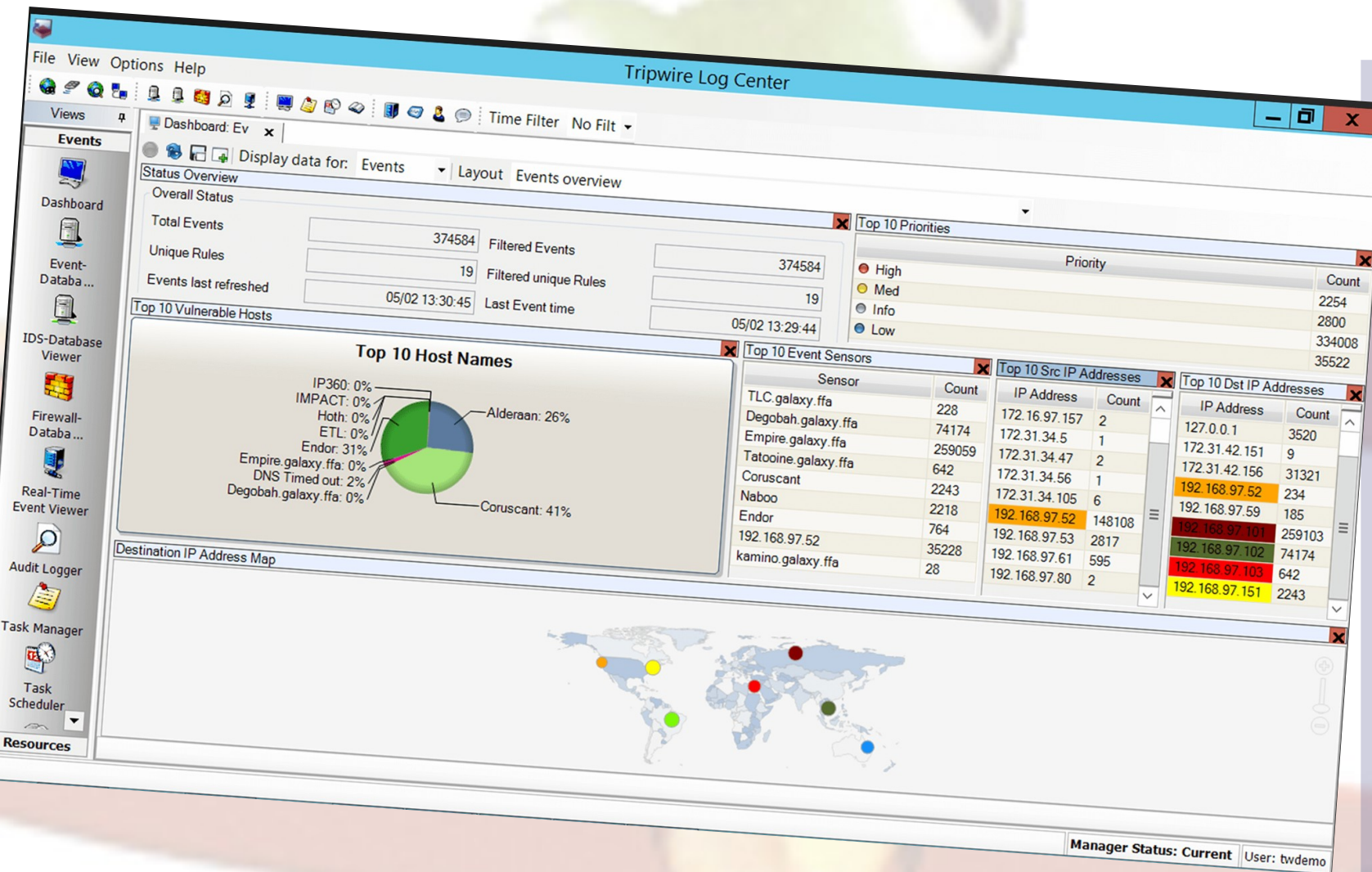
Preventivas

Detectivas

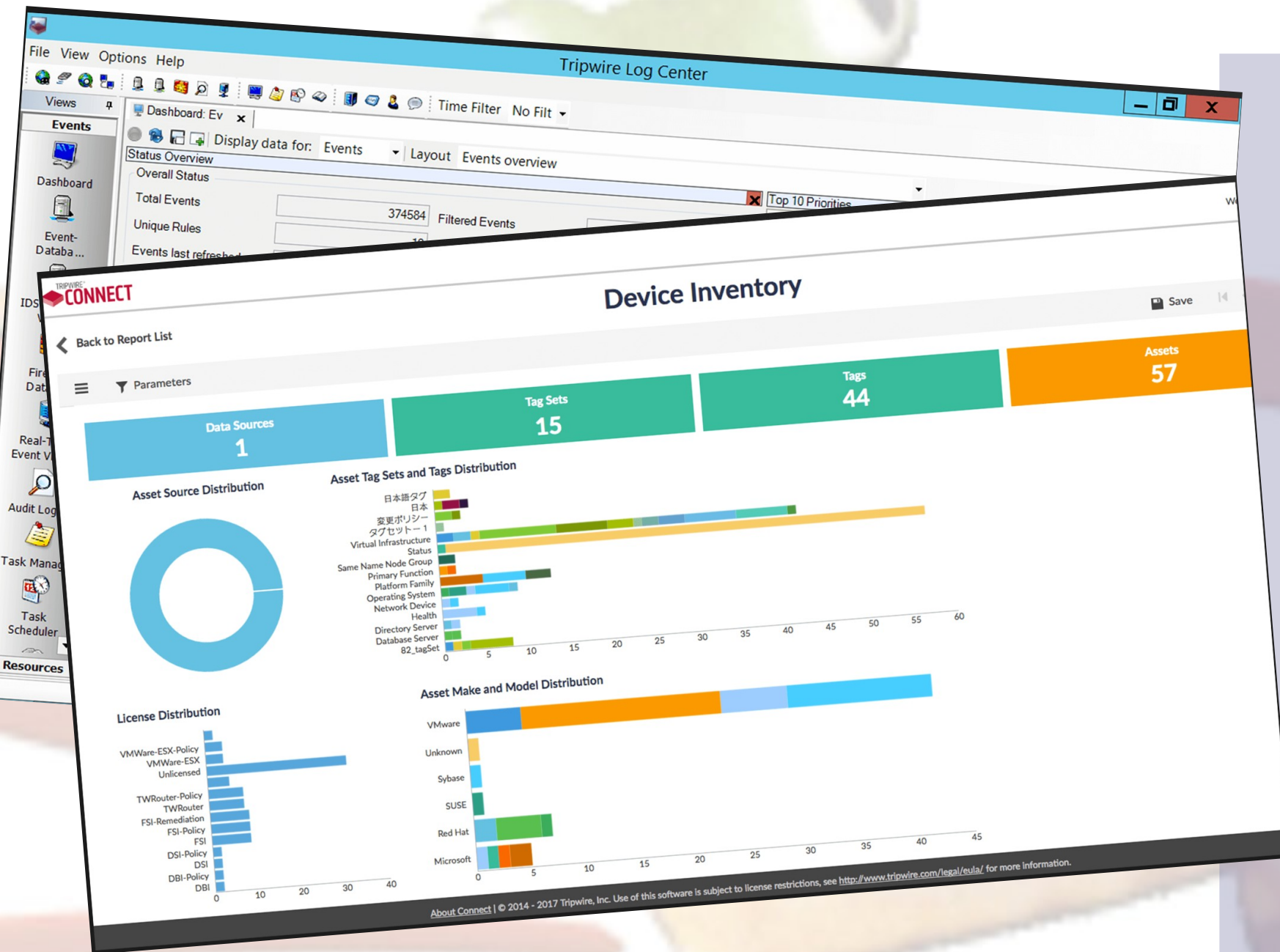
Reactivas

Retrospectivas

Tripwire



Tripwire

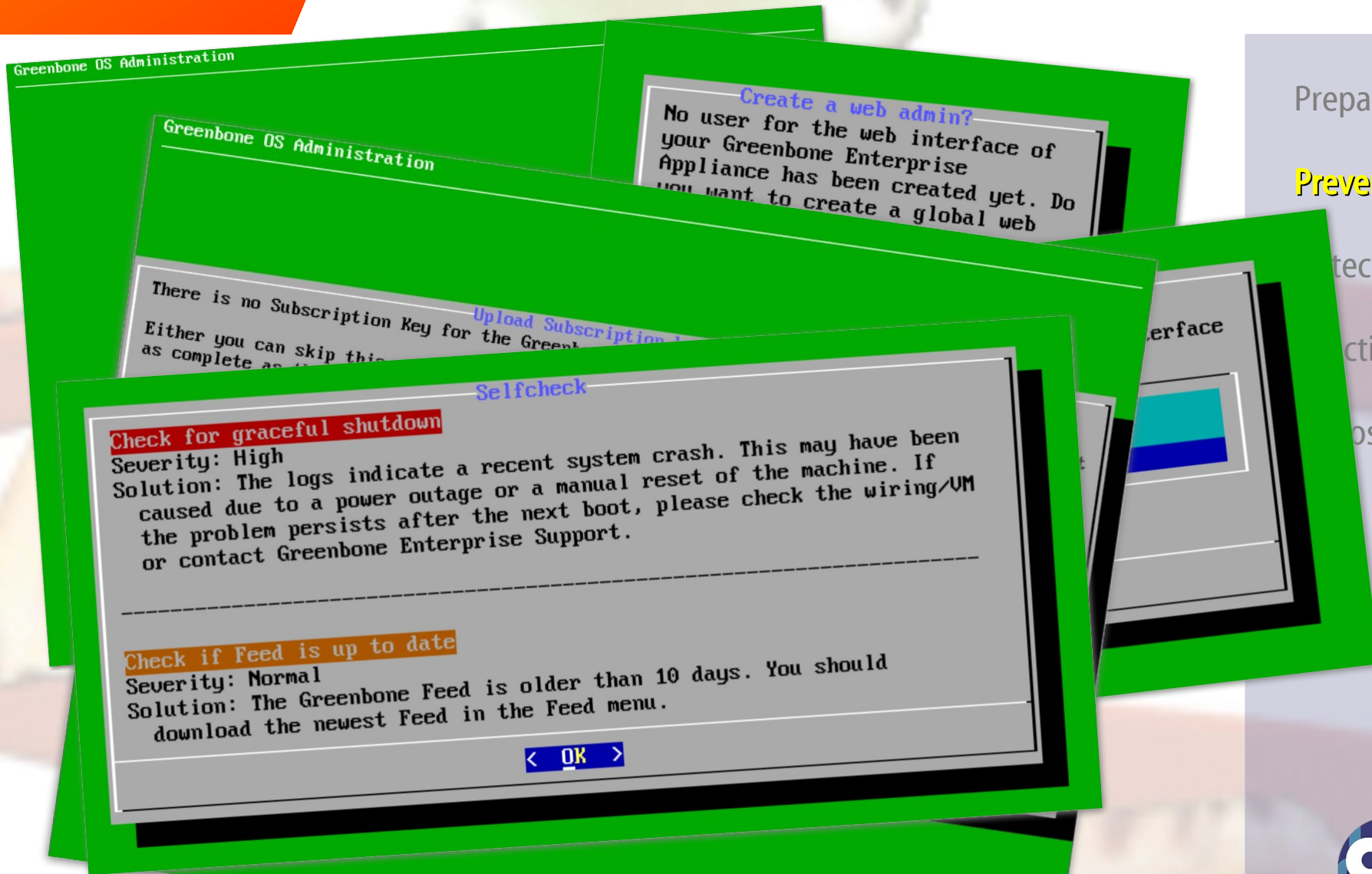


Preventivas



Greenbone OpenVAS

Open Vulnerability Assessment Scanner



Preparativas

Preventivas

Detectivas

Proactivas

Prospectivas

greenbone.org/
[Target.com](https://www.target.com/)
[vulners.com](https://www.vulners.com/)



Preventivas



Greenbone OpenVAS

Open Vulnerability Assessment Scanner



Greenbone

Sign in to your account

Username

admin

Password



Sign In

Greenbone
Enterprise

TRIAL

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

<https://www.openvas.org/>
<https://HacketTarget.com>
<https://Hostedscan.com>



Preventivas



Greenbone OpenVAS

Open Vulnerability Assessment Scanner



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

<https://www.openvas.org/>
<https://HacketTarget.com>
<https://Hostedscan.com>



Preventivas



Greenbone OpenVAS

Open Vulnerability Assessment Scanner



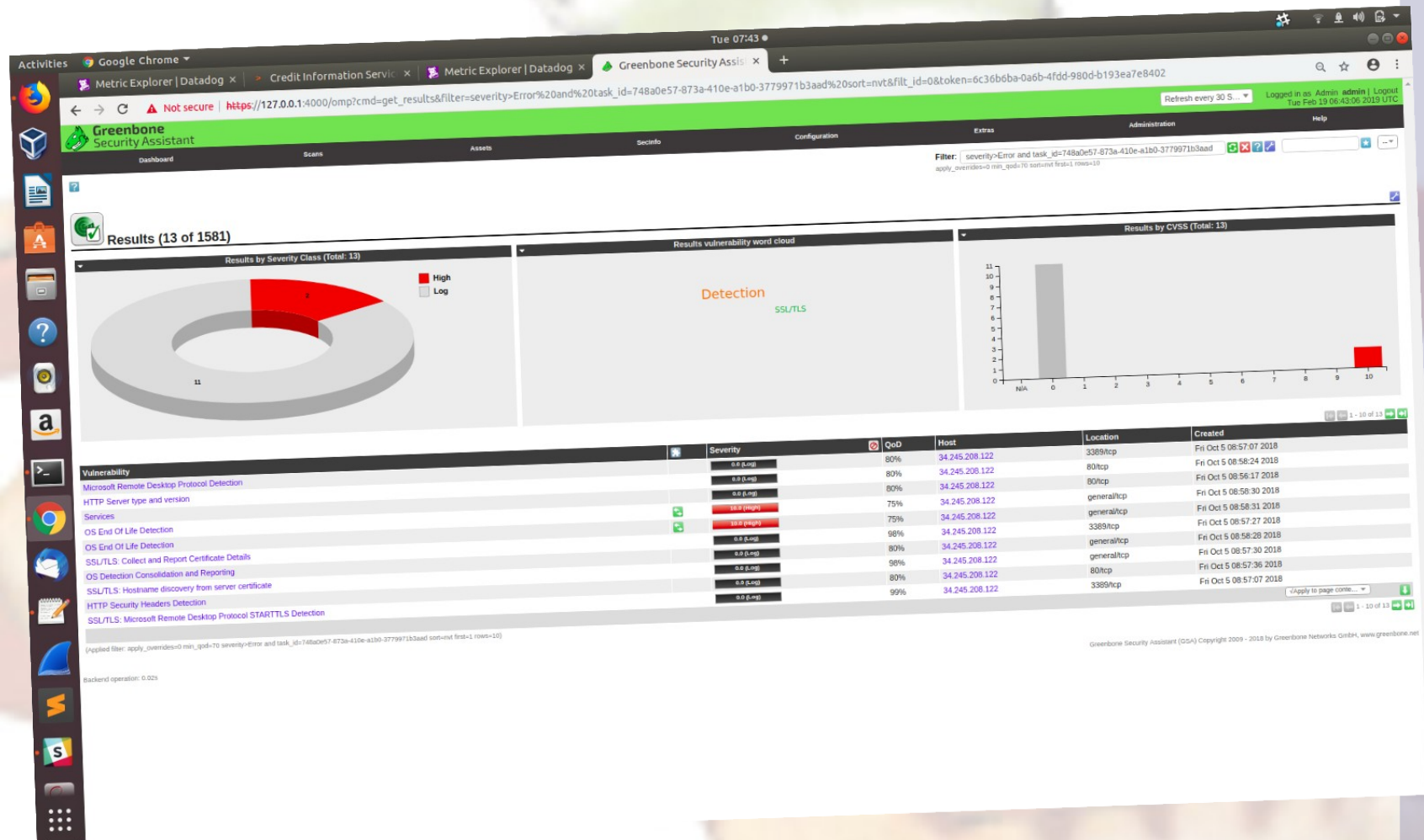
Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



<https://www.openvas.org/>
<https://HacketTarget.com>
<https://Hostedscan.com>

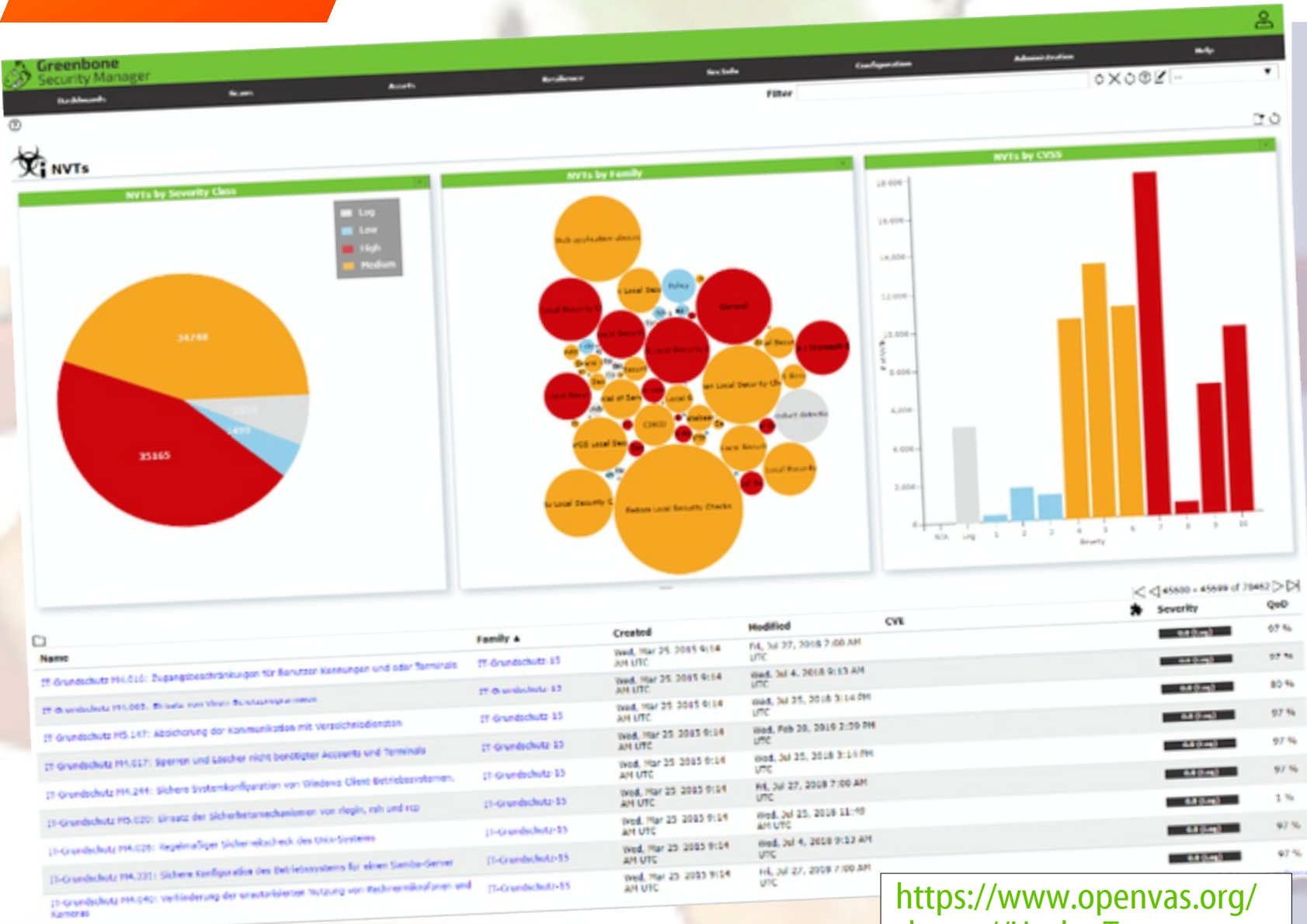


Preventivas



Greenbone OpenVAS

Open Vulnerability Assessment Scanner



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

<https://www.openvas.org/>
<https://HacketTarget.com>
<https://Hostedscan.com>



Preventivas



Greenbone OpenVAS

Open Vulnerability Assessment Scanner



HackerTarget.com

OpenVas Vulnerability Report

Summary

Scan started: **Tue Feb 12 11:08:49 2019 UTC**
Scan ended: **Tue Feb 12 11:18:44 2019 UTC**

1
HIGH

6
MEDIUM

1
LOW

Any **HIGH** and **MEDIUM** severity vulnerabilities should be investigated and confirmed so that remediation can take place. **LOW** risk items should not be ignored as they can be chained with other vulnerabilities to enable further attacks.

Host Summary

Host	Start	End	High	Medium	Low	Log
192.168.1.56 (WIDGETServer)	Feb 12, 11:09	Feb 12, 11:18	1	6	1	0
Total: 1			1	6	1	0

Vulnerability Summary

Severity	Description	CVSS	Count
High	Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (40		
Medium	DCE/RPC and MSRPC Services Enumeration Reporting		

<https://www.openvas.org/>
<https://HacketTarget.com>
<https://Hostedscan.com>

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas



Greenbone OpenVAS

Open Vulnerability Assessment Scanner



OpenVas Vulnerability Report

HackerTarget.com

Results by Host

Host 192.168.1.56

Host scan started: Tue Feb 12 11:09:04 2019 UTC

Port Summary for Host 192.168.1.56

Service (Port)	Severity
general/tcp	
3389/tcp	Low
636/tcp	Medium
445/tcp	Medium
443/tcp	High
135/tcp	Medium
3269/tcp	Medium
	Medium

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

<https://www.openvas.org/>
<https://HacketTarget.com>
<https://Hostedscan.com>



Preventivas



Greenbone OpenVAS

Open Vulnerability Assessment Scanner



Security Issues for Host 192.168.1.56

445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389) (OID:
1.3.6.1.4.1.25623.1.0.810676)

Summary

This host is missing a critical security update according to Microsoft Bulletin MS17-010.

Vulnerability Detection Result

Vulnerability was detected according to the Vulnerability Detection Method.

Impact

Successful exploitation will allow remote attackers to gain the ability to execute code on the target server, also could lead to information disclosure from the server.

Solution

Solution type: VendorFix

Run Windows Update and update the listed hotfixes or download and update mentioned hotfixes in the advisory

Affected Software/OS

Microsoft Windows 10 x32/x64 Edition Microsoft Windows Server 2012 Edition Microsoft Windows Server 2016
Microsoft Windows 8.1 x32/x64 Edition Microsoft Windows Server 2012 R2 Edition Microsoft Windows 7 x32/x64
Edition Service Pack 1 Microsoft Windows Vista x32/x64 Edition Service Pack 2 Microsoft Windows Server 2008
R2 x64 Edition Service Pack 1 Microsoft Windows Server 2008 x32/x64 Edition Service Pack 2

Vulnerability Insight

Multiple flaws exist due to the way that the Microsoft Server Message Block 1.0 (SMBv1) server handles certain requests.

Vulnerability Detection Method

Send the crafted SMB transaction request with fid = 0 and check the response to

Details: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)
1.3.6.1.4.1.25623.1.0.810676)

<https://www.openvas.org/>
<https://HacketTarget.com>
<https://Hostedscan.com>

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas

Detectar vulnerabilidades

<https://hostedscan.com/>

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

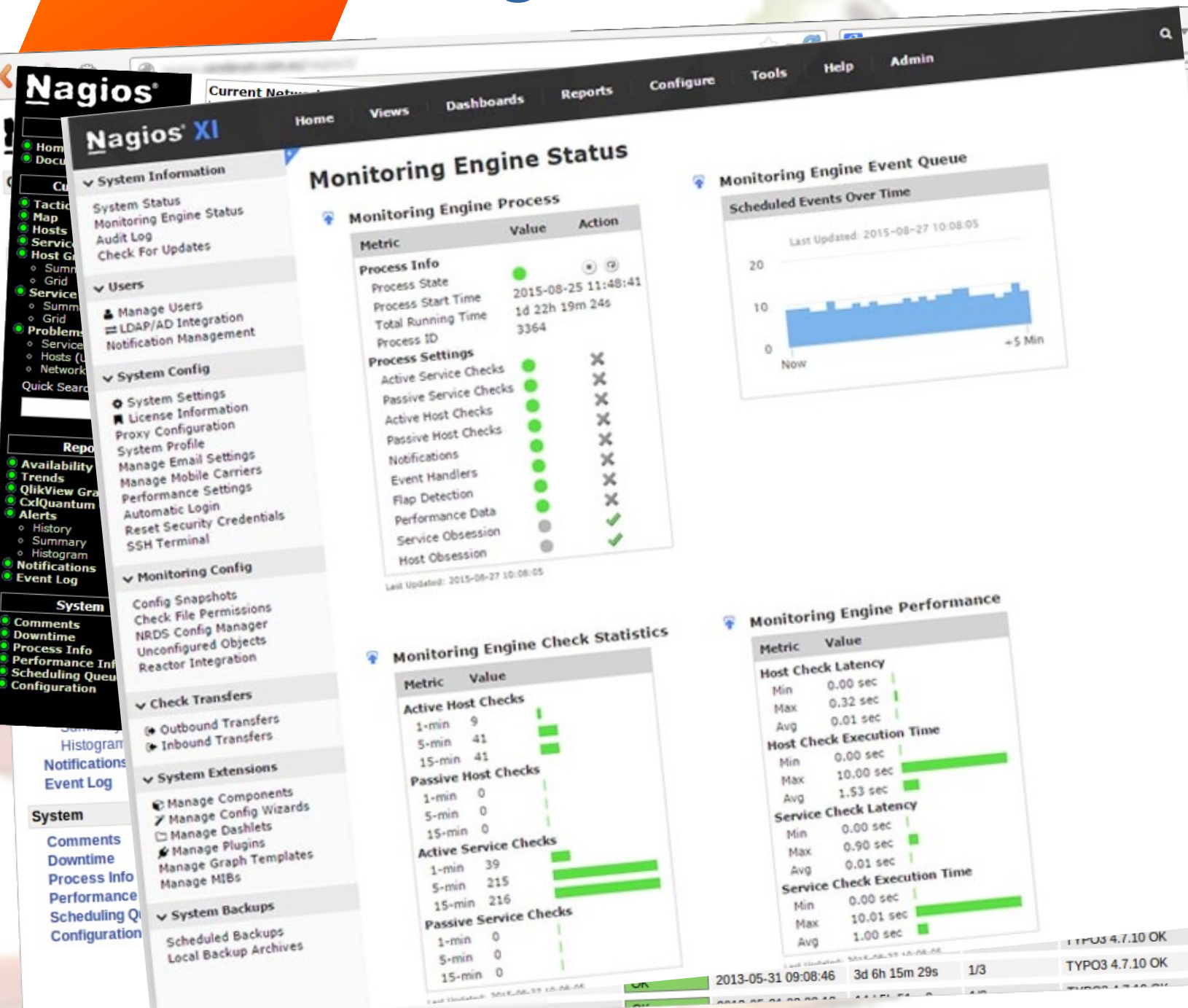
Scans

Request exceeded the free scan credits limit.

Scan	Target(s)
> Nmap	skinait.com
> Nmap UDP	skinait.com
> OpenVAS	skinait.com
> OWASP ZAP Active	skinait.com
> Sslyze	skinait.com

Preventivas

Nagios



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



- Distrib. de Gnu/Linux.
 - Basada en Debian.
 - Monitoreo.
 - Identificación de activos.
 - Detección de vulnerabilidades.
- Interfaz mediante navegador web.
- Une múltiples herramientas.
- Interfaz única y homogénea.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



- Monitoreo
 - Coordinado.
 - Unificado.
- Gestión de eventos de seguridad.
- Genera informes.
 - PDF.
 - Muy amigables.
 - Discriminados por IP
 - Descripción de las vulnerabilidades.
 - Brinda recomendaciones y pasos a seguir.
- Marca falsos positivos
- Comparte a otros Alienvaults.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



- Combina servicios y cruza información de: **ALIEN VAULT LABS**

- Arpwatch: detecta anomalías MAC.
- P0f: Identificación pasiva de OS.
- Pads: detecta anomalías en servicios.
- OpenVAS: Evaluación y correlación cruzada (IDS vs Escaner de Vuln.)
- **Snort: IDS + correlación cruzada Nessus.**
- Spade: detecta anomalías en paquetes.
 - Conocimiento de ataques sin firma.
- Tcptrack: información de sesiones.
- Ntop: base de datos de la red.
- **Nagios: monitorear la disponibilidad de los hosts y servicios.**
- nfSen: visor de flujos de red
- Osiris: IDS basado en host (HIDS).
- Snare: agrupa logs de sistemas Windows.
- OSSEC: IDS basado en hosts.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Alienvault



Preparativas

Preventivas

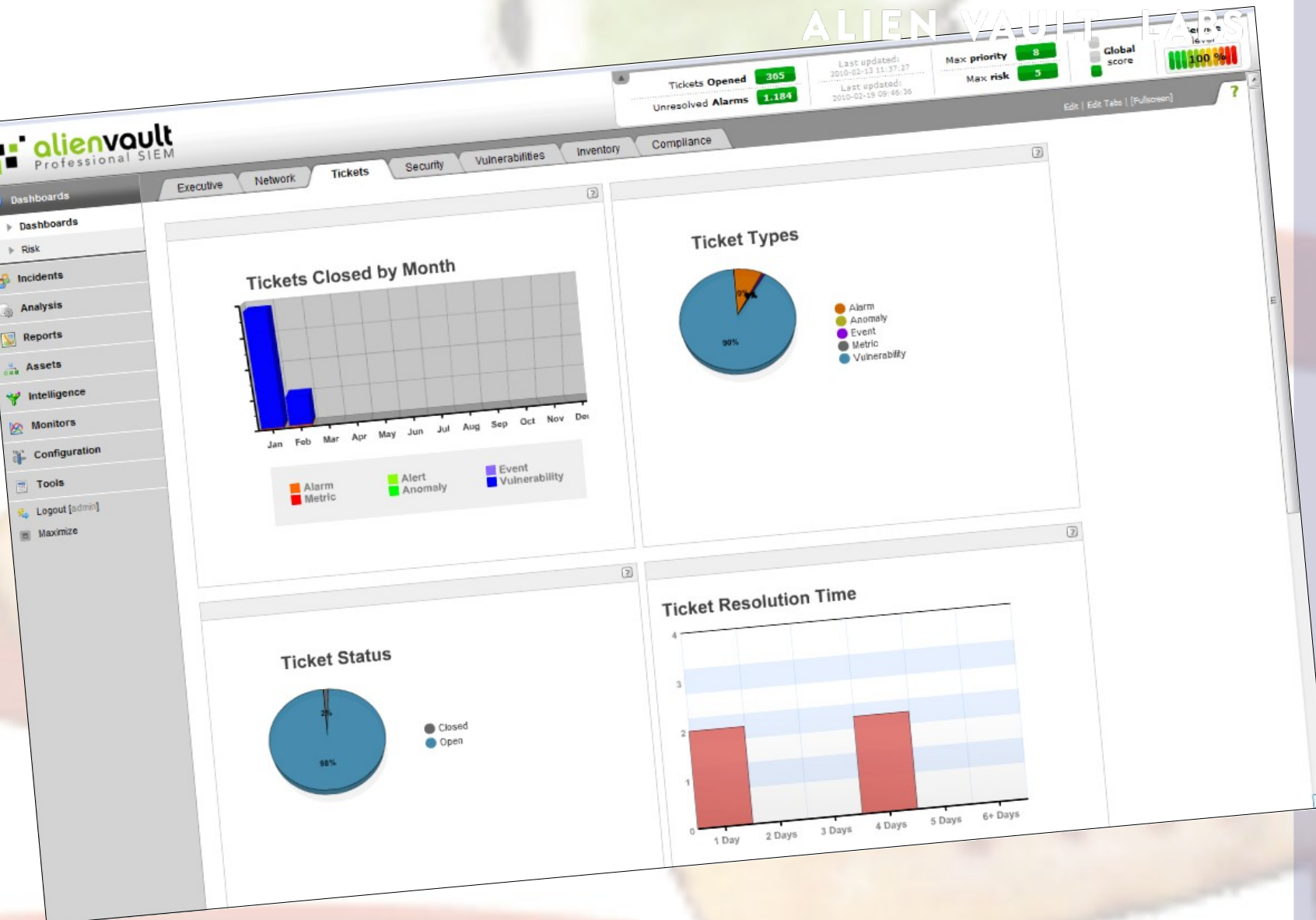
Detectivas

Reactivas

Retrospectivas

Preventivas

Alienvault



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas

Alienvault



ALIEN VAULT LABS

: I.T Security Vulnerability Report



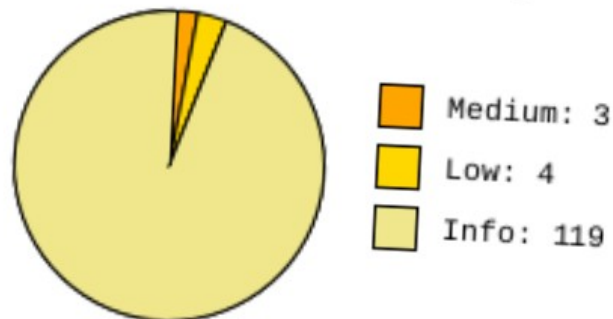
Scan time:

-

Generated:

2021-03-26 01:33:33

Total number of vulnerabilities identified on 6 system(s)



Total number of vulnerabilities identified per system

HostIP	HostName	Critical	High	Med	Low	Info
192.168.1.1	Host-192-168-1-1	--	--	3	2	52
192.168.1.66	Host-192-168-1-66	--	--	--	1	18
192.168.1.99	Host-192-168-1-99	--	--	--	1	20
192.168.1.2	Host-192-168-1-2	--	--	--	--	4
192.168.1.200	Host-192-168-1-200	--	--	--	--	4
192.168.1.88	Host-192-168-1-88	--	--	--	--	21
192.168.1.1		Host-192-168-1-1				

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Alienvault



ALIEN VAULT LABS



Medium:

Apache UserDir Sensitive Information Disclosure

Risk: Medium

Application: https

Port: 443

Protocol: tcp

ScriptID: 10766

Summary:

An information leak occurs on Apache based web servers whenever the UserDir module is enabled. The vulnerability allows an external attacker to enumerate existing accounts by requesting access to their home directory and monitoring the response.

CVSS Base Vector:

AV:N/AC:L/Au:N/C:P/I:N/A:N

Solution:

1) Disable this feature by changing 'UserDir public_html' (or whatever) to 'UserDir disabled'.

Or

2) Use a RedirectMatch rewrite rule under Apache -- this works even if there is no such entry in the password file, e.g.:

RedirectMatch ^/~(.*)\$ http://example.com/\$1

Or

3) Add into httpd.conf:

ErrorDocument 404 http://example.com/sample.html

ErrorDocument 403 http://example.com/sample.html

(NOTE: You need to use a FQDN inside the URL for it to work properly).

References:

<http://www.securiteam.com/unixfocus/5WP0C1F5FI.html>

CVSS Base Score: 5.0

Family name: Web Servers

Category: unknown

Copyright: Copyright (C) 2001 SecuriTeam

Version: 2020-08-24T15:18:35+0000

CVEs: CVE-2001-1013

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Pruebas de penetración (hacking ético, pen-testing)

- Kali Linux / Cyborg Hawk

- Distribuciones de Linux
- Todas las maldades juntas, unidas y listas para usar.
- Porque para defenderse hay que saber qué hacen los ciberdelincuentes.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Pruebas de penetración

- Todo listo, unido y fácil
 - Tutoriales hasta en Youtube.
 - Pero hay que saber qué se está haciendo.
 - Puede meterse en problemas penales.
 - El entorno Latinoamericano hace muy fácil.
 - Armitage: Metasploit preconfigurado y con GUI.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Cyborg Hawk



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Cyborg Hawk

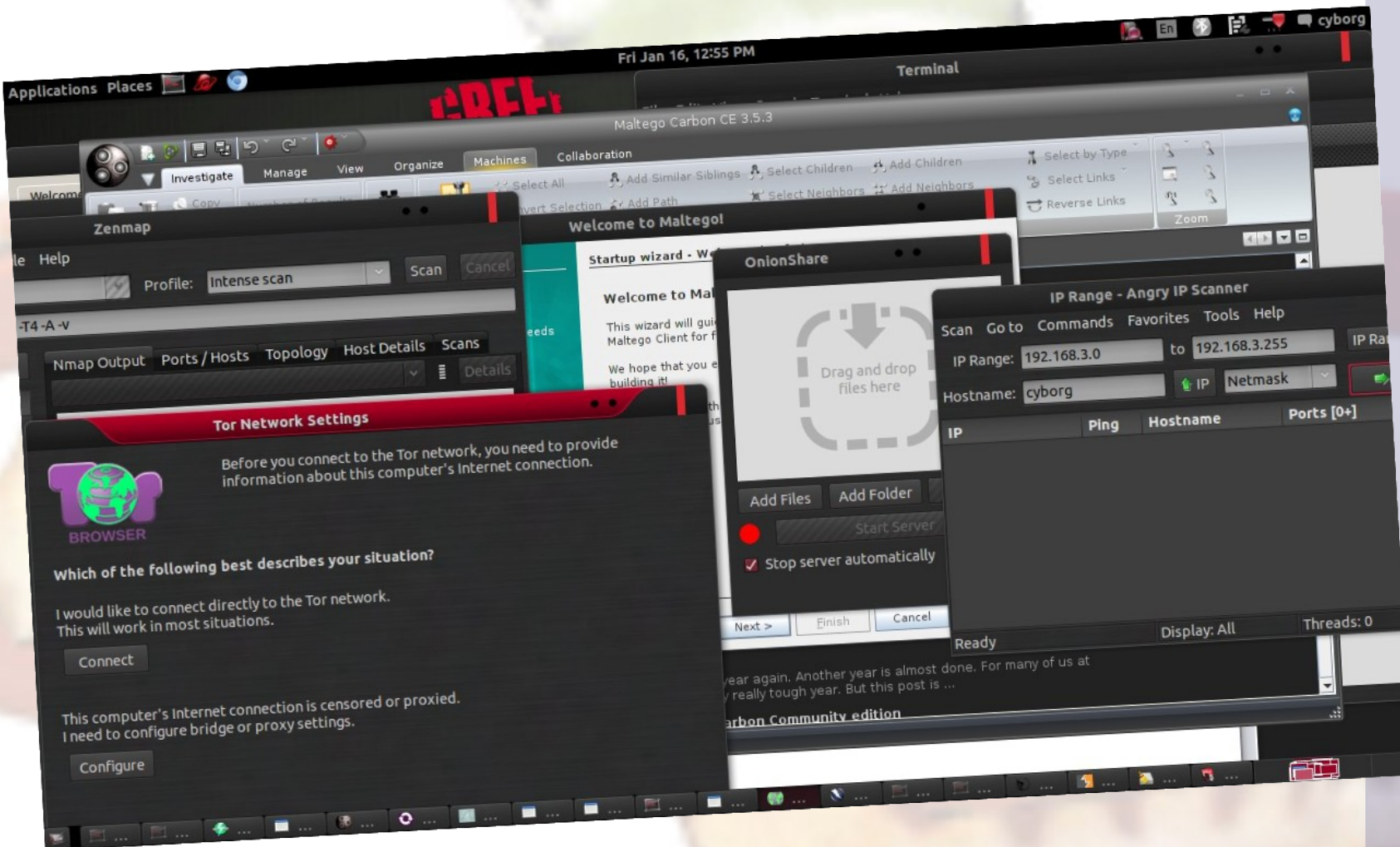
Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas

Metasploit / Armitage

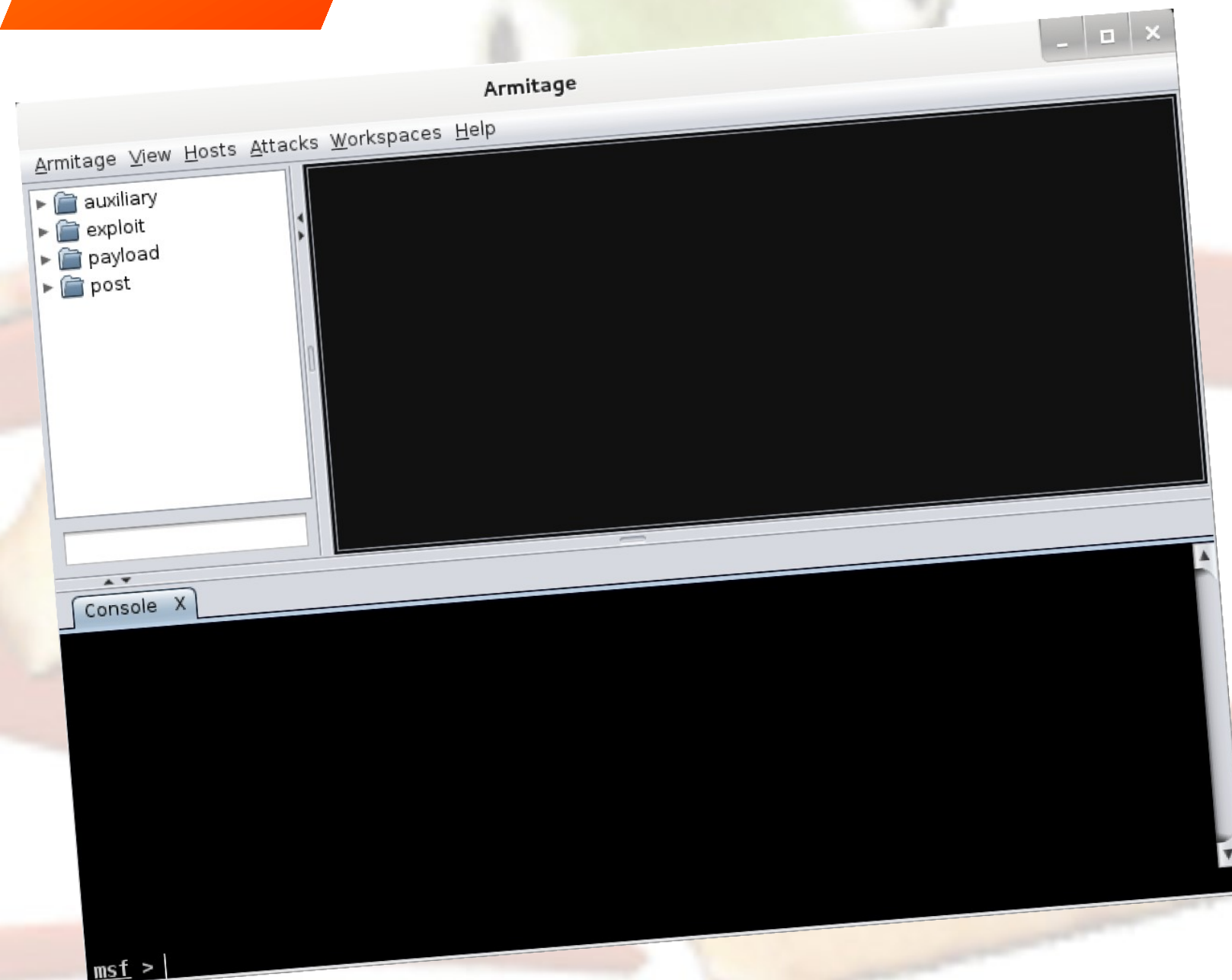
Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas

Metasploit / Armitage

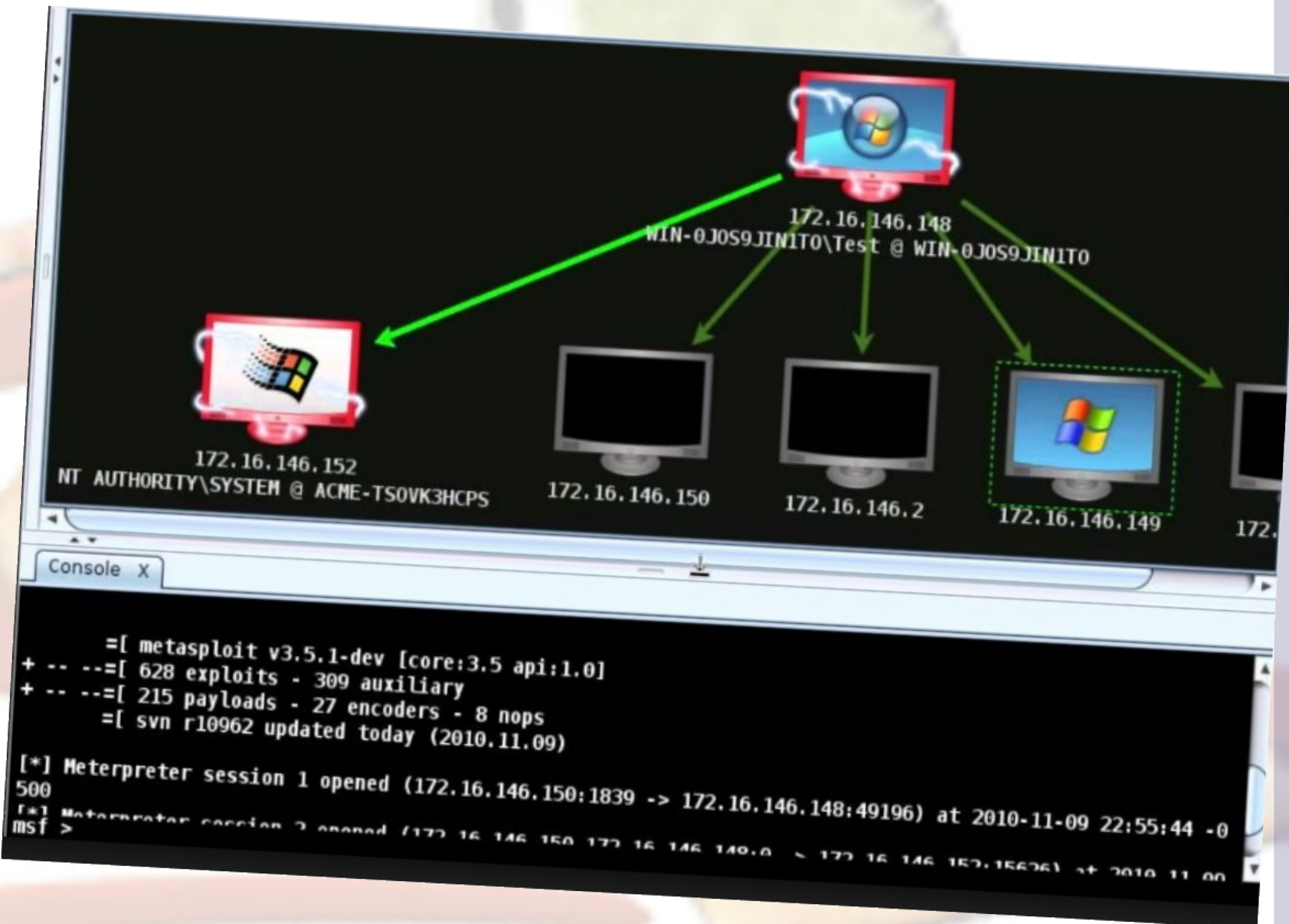
Preparativas

Preventivas

Detectivas

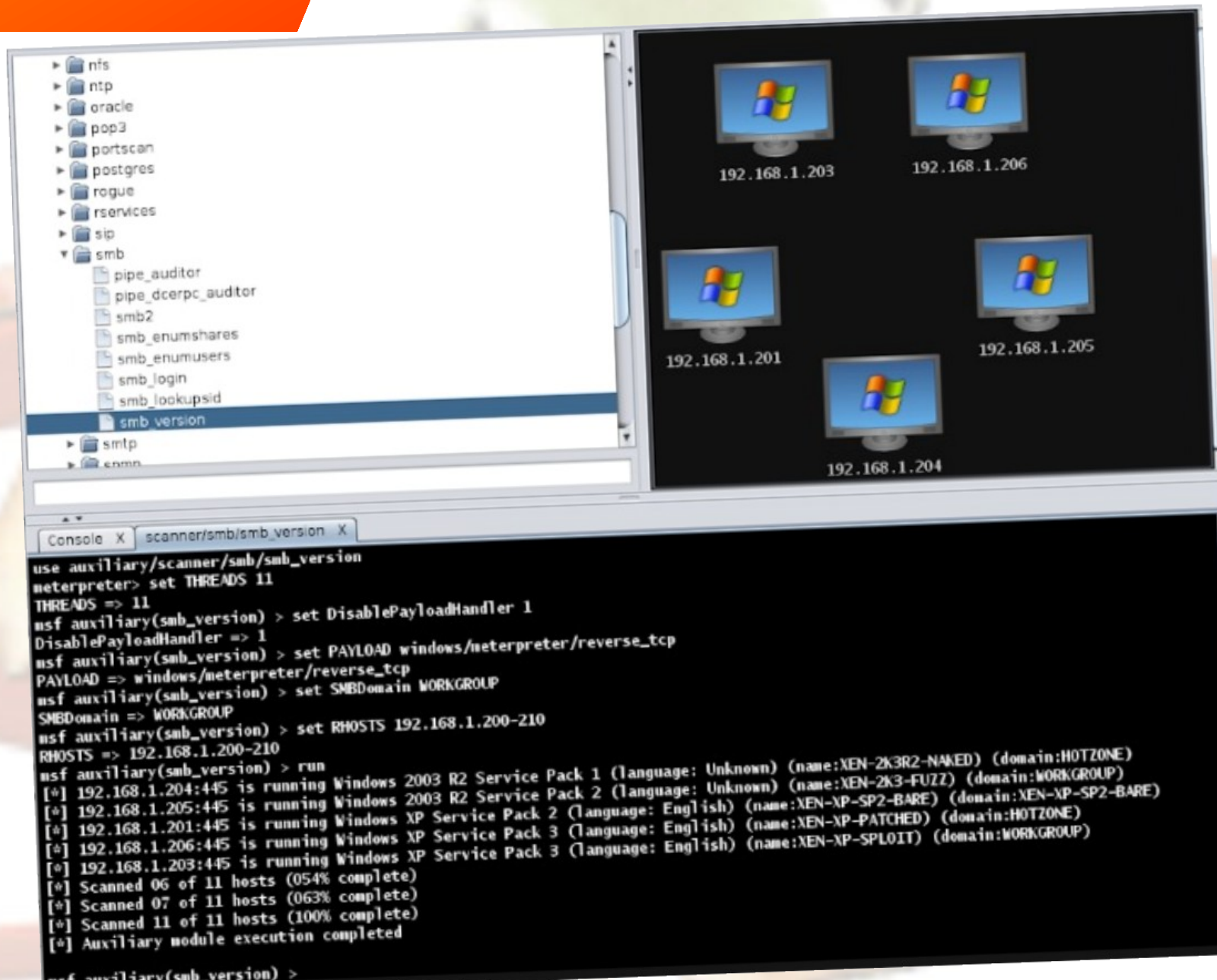
Reactivas

Retrospectivas



Preventivas

Metasploit / Armitage



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Metasploit / Armitage

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas

Defensa en profundidad



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- Seguridad en los puntos finales
 - Hardening de:
 - Servidores.
 - Estaciones de trabajo / Portátiles / Dispositivos móviles.
 - Revisión de conectores eléctricos / red / periféricos.
 - Antivirus y firewall de host.
 - Actualizado.
 - Ejecutado periódicamente.
 - Sandboxes

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Cuckoo: Sandbox

<https://cc-csirt.policia.gov.co/Sandbox>

<https://caivirtual.policia.gov.co>

The screenshot shows the official website of the Policía Nacional de Colombia. The header includes the police logo, the text 'POLICÍA NACIONAL DE COLOMBIA' and 'REPÚBLICA DE COLOMBIA LIBERTAD Y ORDEN', and the date 'Jueves 20 de Octubre de 2022 17:49:52'. A navigation bar contains links: Inicio, Servicios, Ciberseguridad, APPS, Mural Ciberdelito, Observatorio Ciberdelito, Multimedia, Ciberincidentes, and Contáctenos. The main content area is titled 'Servicios' and features several service tiles. The 'ANÁLISIS DE MALWARE' tile is highlighted with a purple oval. Other tiles include 'NO MORE RANSOM', 'Reporte', 'Ciberseguridad', 'CAI Virtual', and 'APPS'. A 'zendesk chat' widget is visible in the bottom right corner.

Servicios

- NO MORE RANSOM**
Busque su llave para desbloquear archivos cifrados (RANSOMWARE)
Ingresar
- Reporte**
Reporte los incidentes informáticos - Ley 1273 de 2009.
Ingresar
- Ciberseguridad**
Encuentre las recomendaciones, boletines, guías, informes e infografías de ciberseguridad.
Ingresar
- ANÁLISIS DE MALWARE**
Plataforma para el análisis de código malicioso
Ingresar
- CAI Virtual**
Primera iniciativa en Iberoamérica en atención en línea policial.
Ingresar
- APPS**
Aplicaciones móviles para el fortalecimiento de la ciberseguridad.
Ingresar

Reportar Incidente Informático

zendesk chat
Chatee con nosotros
Escribir mensaje aquí

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Cuckoo: Sandbox



La seguridad es de todos

Mindefensa

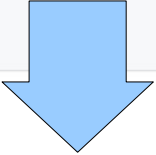
 Suscríbete  Iniciar sesión 

SANDBOX

Inicio / Servicios / Sandbox

Recent Pending Submit

Cuckoo



SUBMIT A FILE FOR ANALYSIS



SUBMIT URLS

Submit URLs

Submit

 Drag your file into the left field or click the icon to select a file.

Back to the top

©2010-2018 Cuckoo Sandbox

 El futuro es de todos

Presidencia de la República

 La seguridad es de todos

Mindefensa

 Colombia Compra Eficiente



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas

Cuckoo: Sandbox



La seguridad
es de todos
Mindefensa



Suscríbete



Iniciar sesión



SANDBOX

Inicio / Servicios / Sandbox

Recent Pending

Submit

submit-file » configure » analyze » Summary

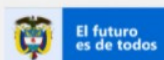
✓ Your submission has been received and the tasks are being processed!

Next: [View pending tasks](#) [Submit again](#)

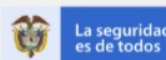
Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	Package
4565	20/10/2022 15:16	2020.02.05-PropuestaBuscador-Requerimientos.pdf	pdf
Done			

©2010-2018 Cuckoo Sandbox



El futuro
es de todos
Presidencia
de la República



La seguridad
es de todos
Mindefensa



Colombia Compra Eficiente

GOV.CO

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas

Cuckoo: Sandbox

gov.co/Sandbox

Recent Pending

Submit

Summary

2020.02.05-PropuestaBuscador-Requerimientos.pdf

File 2020.02.05-PropuestaBuscador-Requerimientos.pdf

Summary		Download Resubmit sample
Size	328.6KB	
Type	PDF document, version 1.5	
MD5	c943da2b088721bed4362e45b3c837a1	
SHA1	e0b6f0a77f0ce54c2297d69e41e44a0aaf634a08	
SHA256	482134fca763e668d6fe3575fe60d35eb46f9f784ec4f6f15ff0275ea51d284a	
SHA512	Show SHA512	
CRC32	A88B4C5A	
ssdeep	6144:Qcg5Le05F0IruTEtaNdb5hEHBmbVWE1Y+IkHmZXrgPow1kWeE6zpuKCKwZxDT+EL:QcGQCuTETcdB52FE1YimTR01r12psbDB	
Yara	None matched	

Score

This file shows numerous signs of malicious behavior.

The score of this file is **3.2 out of 10**.

Please notice: The scoring system is currently still in development and should be considered an **alpha** feature.

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Analysis					
Category	Started	Completed	Duration	Routing	Logs
FILE	Oct. 20, 2022, 3:16 p.m.	Oct. 20, 2022, 3:19 p.m.	203 seconds	none	Show Analyzer Log Show Cuckoo Log

Signatures

Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Cuckoo: Sandbox

Recent

Pending

Submit

Home

Menu

Lock

Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available (1 event)

Time & API

Arguments

Status

Return

Repeated

GlobalMemoryStatusEx

Oct. 20, 2022, 3:16 p.m.

1

1

0

One or more potentially interesting buffers were extracted, these generally contain injected code, configuration data, etc.

Performs some HTTP requests (2 events)

request

GET http://swupmf.adobe.com/manifest/60/win/reader9rdr-en_US.upd

request

GET http://swupmf.adobe.com/manifest/60/win/AdobeUpdater.upd

Checks adapter addresses which can be used to detect virtual network interfaces (1 event)

Time & API

Arguments

Status

Return

Repeated

GetAdaptersAddresses

Oct. 20, 2022, 3:16 p.m.

flags: 46
family: 0

1

0

0

Communicates with host for which no DNS query was performed (1 event)

host

104.91.164.139

Sets or modifies WPAD proxy autoconfiguration file for traffic interception (10 events)

Time & API

Arguments

Status

Return

Repeated

RegSetValueExW

Oct. 20, 2022, 3:16 p.m.

key_handle: 0x00000394
regkey_r: WpadDecisionReason
reg_type: 4 (REG_DWORD)
value: 1
regkey: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\{557A9EFC-64BC-4C71-99D6-F910304509AD}\WpadDecisionReason

1

0

0

key_handle: 0x00000394

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

De: support@skinait.com
Para: ventas@skinait.com
Asunto: E-mail Security Update™
Fecha: 16 Apr 2024 15:22:40 +0200 (16/04/24 08:22:40)

Server Requesting Authentication!

Server provider for skinait.com is conducting a security check to safeguard your email (ventas@skinait.com).
Hereby requesting authentication, failure to execute on or before 4/16/2024 3:22:39 p.m.
a new password will be generated by the server and you will be automatically logged out.

You are advised to continue using your current details.
To continue using your current details please use the button below.

Authenticate Now

Disclaimer

This email is intended solely for ventas@skinait.com only. It contains confidential and/or privileged information. If you are not the intended recipient or have received this message in error, you must not copy, distribute, disclose or take any action in reliance on any part of it. In such a case, you should inform us immediately and delete the message.

[https://cloudflare-ipfs.com/ipfs/
bafybeiexzyipcwkykb6zzlefeq336r72pvg3r3wekuxckguu
osbqohpdy/keswroker.html/#ventas@skinait.com](https://cloudflare-ipfs.com/ipfs/bafybeiexzyipcwkykb6zzlefeq336r72pvg3r3wekuxckguuosbqohpdy/keswroker.html/#ventas@skinait.com)



Preventivas

Cuckoo: Sandbox



MINISTERIO DE DEFENSA
NACIONAL



Suscríbete



Iniciar sesión



SANDBOX

Inicio / Servicios / Sandbox

Recent Pending

Submit

Cuckoo

SUBMIT A FILE FOR ANALYSIS

SUBMIT URLS

https://cloudflare-
ipfs.com/ipfs/bafybeiexzjyipcwykvb6zzlefeq336r72pvg3r3wekuxckguuo
sbqohpdy/keswroker.html/#ventas@skinait.com

SUBMIT URLS

https://cloudflare-
ipfs.com/ipfs/bafybeiexzjyipcwykvb6zzlefeq336r72pvg3r3wekuxckguuo
sbqohpdy/keswroker.html/#ventas@skinait.com

Drag your file into the left field

Submit

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Preventivas

Cuckoo: Sandbox



MINISTERIO DE DEFENSA
NACIONAL



Suscríbete



Iniciar sesión



SANDBOX

Inicio / Servicios / Sandbox

Recent Pending

Submit

submit file >> configure >> analyze

Configure your Analysis

Analyze

Selection: 1/1

https://cloudflare-ipfs.com/ipfs/bafybeioxzyipcwkyvb6zzlefeq336r72pvg3r3wekuxckguuosbqohpdy/keswroker.html/#ventas@skinait.com

Selection



Search selection



EXTENSION



HTTPS://CLOUDFLARE...

These files you selected will be included in your analysis. When ready, click 'analyze' next to the page title.

©2010-2018

Cuckoo Sandbox



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Cuckoo: Sandbox



MINISTERIO DE DEFENSA
NACIONAL



Suscríbete



Iniciar sesión



SANDBOX

Inicio / Servicios / Sandbox

Recent Pending

Submit

submit file >> configure >> analyze >> Summary

✓ Your submission has been received and the tasks are being processed!

Next: [View pending tasks](#) [Submit again](#)

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	
3946	17/04/2024 10:45	hxxps://cloudflare- ipfs.com/ipfs/bafybeiexzjyipcwykvb6zzlefeq336r72pvg3r3wekuxckguuosbqohpdy/kesv	 running
		Done	

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Cuckoo: Sandbox



MINISTERIO DE DEFENSA
NACIONAL



Suscríbete



Iniciar sesión



SANDBOX

Inicio / Servicios / Sandbox

Recent Pending

Submit

[submit file](#) >> [configure](#) >> [analyze](#) >> [Summary](#)

✓ Your submission has been received and the tasks are being processed!

Next: [View pending tasks](#) [Submit again](#)

Tasks: Refreshes every 2.5 seconds

Task ID	Date	Filename / URL	
3946	17/04/2024 10:45	hxxps://cloudflare- ipfs.com/ipfs/bafybeiexzjyipcwykvb6zzlefeq336r72pvg3r3wekuxckguuosbqohpdy/keswro	 reported
Done			

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Summary

URL Details

URL

https://cloudflare-ipfs.com/ipfs/bafybeieuxzjyipcwykvb6zzlefeq336r72pvg3r3wekuxckguosbqohpdy/keswroker.ntml/#ventas@skinait.com

Score

This url is **very suspicious**, with a score of **5.6 out of 10!**

Please notice: The scoring system is currently still in development and should be considered an *alpha* feature.

Expecting different results? Send us this analysis and we will inspect it. [Click here](#)

Information on Execution

Analysis

Category	Started	Completed	Duration	Routing	Logs
URL	April 17, 2024, 10:45 a.m.	April 17, 2024, 10:48 a.m.	196 seconds	none	Show Analyzer Log Show Cuckoo Log

Signatures

- ❗ Performs some HTTP requests (31 events) >
- ❗ Allocates read-write-execute memory (usually to unpack itself) (50 out of 656 events) >
- ❗ Creates executable files on the filesystem (18 events) >
- ❗ Changes read-write memory protection to read-execute (probably to avoid detection when setting all RWX flags at the same time) (1 event) >

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

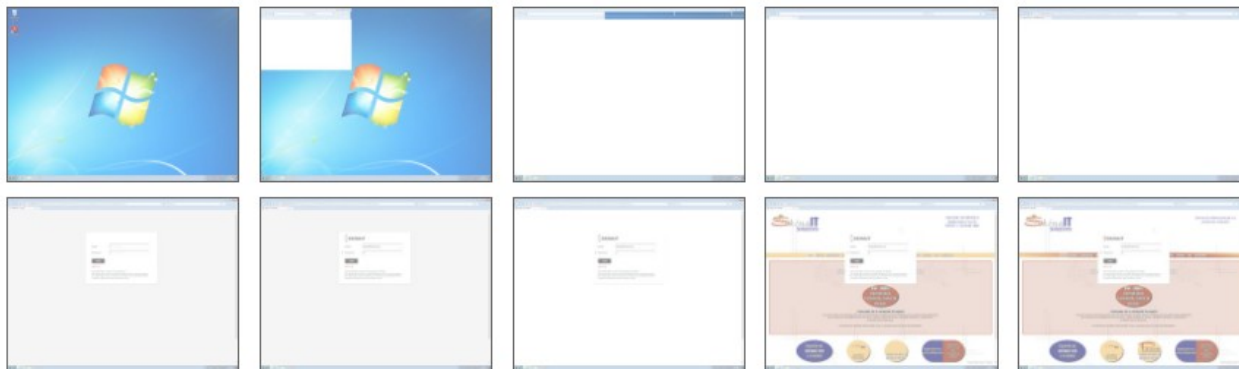
Recent Pending

Submit

✖ Connects to an IP address that is no longer responding to requests (legitimate services will remain up-and-running usually) (1 event) >

✖ A potential heapspray has been detected. 577 megabytes was sprayed onto the heap of the iexplore.exe process (3 events) >

Screenshots



Name	Response	Post	IP Address	Status	Action
assets.prezicdn.net	CNAME → d3aeorqw7ononu.cloudfront.net	2.19.34.40	104.17.64.14	Active	Moloch
	A → 18.155.252.22		104.18.38.233	Active	Moloch
	A → 18.155.252.87		142.250.218.99	Active	Moloch
	A → 18.155.252.18		142.250.78.42	Active	Moloch
	A → 18.155.252.111		142.250.78.46	Active	Moloch
x1.c.lencr.org	CNAME → crt.root-x1.letsencrypt.org.edgekey.net	2.19.34.40	142.250.78.68	Active	Moloch
	CNAME → e8652.dscx.akamaiedge.net		142.250.78.8	Active	Moloch
	A → 2.19.34.40		142.251.135.163	Active	Moloch
www.google.com	A → 142.250.78.8		142.251.135.163	Active	Moloch

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Cuckoo: Sandbox

The screenshot shows a web browser window displaying the SkinaIT Solutions website. The URL in the address bar is <https://cloudflare-ipfs.com/ipfs/bafybeisxjipcwylkvb6zzlfeq336r72pvg3r3wekuxckguasbqohpdy/keswoker.html/#ventas@skinait.com>. The page features a navigation bar with links: Inicio, Software, Capacitación, and GR. The main content area includes a login form with fields for Email (ventas@skinait.com) and Password, and a Login button. A NOTICE box states: "This information system is the property of SkinaIT. We advise all users to verify their email account for security reasons. By continuing to use the system you indicate your awareness of and consent to these terms and conditions of use." Below the login form, there is a section titled "BPM - GROUPS" with the text "Gobernabilidad, Trazabilidad y Control de procesos". A central message asks "¿Preocupado por la continuidad del negocio?" and describes the system's benefits for business continuity. At the bottom, there are four circular icons representing services: "Desarrollo de SOFTWARE WEB a la medida", "Ley Datos Personales", "Sistema web para la gestión de contratos", and "Capacitación en el uso de software libre" (which also lists OpenOffice, GNU/Linux, Php, PostgreSQL, and Python). The footer indicates the website was developed by Skina IT Solutions.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Defensa en profundidad

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Defensa en profundidad

- Seguridad de las aplicaciones
 - Software / Apps / WebApps / Cloud
 - Mantener actualizado
 - OSs / software / leng. de prog / motores de BD.
- Seguridad de los datos
 - Autenticación y autorización
 - Validar que cada persona es quien dice ser.
 - Saber qué permisos tiene cada persona.
 - Acceso / ejecución / modificación.
 - Cifrado
 - Plan de backups: datos, software, parámetros

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Antimalware: ClamAV

```
(venv) → tools git:(master) X cincan run cincan/clamav samples/clamav_sample.exe
cincan/clamav: pulling image ...
cincan/clamav: ≤ samples/clamav_sample.exe
LibClamAV Warning: *****
LibClamAV Warning: ** The virus database is older than 7 days! **
LibClamAV Warning: ** Please update it as soon as possible. **
LibClamAV Warning: *****
samples/clamav_sample.exe: OK

----- SCAN SUMMARY -----
Known viruses: 6562715
Engine version: 0.102.0
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.01 MB
Data read: 0.01 MB (ratio 1.00:1)
Time: 63.743 sec (1 m 3 s)
(venv) → tools git:(master) X
```

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Antimalware: pdf-parser.py y pdf-tools



```
lgramo@localhost pdfparser]$ ./pdf-parser.py --stats ../Respuesta_Mariano_Pedroza_No_de_radicado_20222200406721.pdf
Comment: 3
XREF: 0
Trailer: 0
StartXref: 1
Indirect object: 924
 151: 23, 27, 37, 38, 39, 40, 41, 42, 43, 44, 78, 108, 148, 149, 150, 152, 153, 154, 156, 157, 158, 160, 161, 162, 164, 165, 166, 168, 169, 17
0, 172, 173, 174, 176, 177, 178, 180, 181, 182, 184, 185, 186, 188, 189, 190, 192, 193, 194, 196, 197, 198, 200, 201, 202, 204, 205, 206, 208,
209, 210, 146, 215, 218, 219, 220, 222, 223, 224, 226, 227, 228, 230, 231, 232, 216, 237, 240, 241, 242, 244, 245, 246, 238, 249, 250, 252, 253
, 254, 260, 263, 266, 269, 270, 276, 279, 282, 285, 286, 287, 293, 296, 299, 302, 303, 306, 307, 308, 310, 311, 312, 314, 315, 316, 318, 319, 3
20, 304, 322, 323, 329, 330, 334, 335, 339, 340, 397, 533, 534, 544, 618, 741, 811, 892, 893, 894, 978, 1001, 1002, 1003, 1005, 1006, 1007, 100
9, 1010, 1011, 1013, 1014, 1015, 999, 1017, 1020
/Annot 62: 341, 352, 354, 356, 358, 360, 362, 364, 366, 368, 370, 372, 374, 376, 378, 380, 382, 384, 386, 388, 390, 392, 394, 535, 538, 541, 5
85, 588, 591, 593, 595, 597, 599, 601, 603, 605, 607, 610, 614, 616, 729, 732, 735, 738, 791, 794, 796, 799, 801, 803, 805, 807, 809, 951, 953,
958, 961, 966, 969, 971, 973, 975
/Catalog 1: 1
/Font 37: 147, 155, 163, 171, 179, 187, 195, 203, 217, 225, 239, 258, 261, 264, 267, 274, 277, 280, 283, 291, 294, 297, 300, 305, 313, 327, 32
6, 332, 331, 337, 336, 531, 530, 890, 889, 1000, 1008
/FontDescriptor 17: 259, 262, 265, 268, 275, 278, 281, 284, 292, 295, 298, 301, 328, 333, 338, 532, 891
/ObjStm 2: 10, 956
/Page 21: 6, 7, 8, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145
/Pages 3: 2, 1019, 1018
/Stream 15: 151, 159, 167, 175, 183, 191, 199, 207, 221, 229, 243, 309, 317, 1004, 1012
/StructElem 563: 525, 526, 398, 399, 400, 401, 402, 406, 403, 404, 405, 407, 410, 408, 411, 412, 409, 413, 414, 415, 416, 417, 418, 419, 420,
421, 422, 423, 342, 424, 425, 426, 427, 428, 429, 430, 431, 432, 353, 433, 434, 435, 436, 355, 437, 438, 357, 439, 440, 359, 441, 442, 443, 361
, 444, 445, 363, 446, 447, 365, 448, 449, 367, 450, 451, 369, 452, 453, 371, 454, 455, 373, 456, 457, 375, 458, 459, 377, 460, 461, 379, 462, 4
63, 381, 464, 465, 383, 466, 467, 468, 385, 469, 470, 471, 387, 472, 473, 474, 389, 475, 476, 477, 391, 478, 479, 393, 480, 481, 343, 482, 483,
484, 485, 486, 487, 488, 489, 490, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 396, 508, 509, 51
1, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559,
536, 537, 560, 561, 562, 563, 564, 539, 540, 565, 542, 543, 566, 567, 568, 569, 570, 571, 572, 574, 573, 575, 576, 577, 578, 579, 580, 581, 582
, 583, 584, 619, 620, 621, 586, 622, 587, 623, 624, 625, 626, 627, 589, 628, 629, 630, 631, 632, 633, 634, 635, 592, 636, 637, 638, 594, 639, 6
40, 641, 642, 643, 596, 644, 645, 598, 646, 647, 600, 648, 649, 602, 650, 651, 604, 652, 653, 606, 654, 655, 656, 590, 657, 658, 659, 660, 661,
662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 69
0, 608, 691, 609, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 611, 713, 714, 715,
716, 717, 615, 718, 719, 617, 720, 721, 722, 723, 612, 724, 725, 742, 743, 744, 745, 746, 748, 749, 747, 750, 751, 752, 753, 754, 755, 756, 757
, 758, 759, 760, 761, 762, 764, 763, 765, 730, 731, 766, 767, 768, 769, 770, 733, 734, 771, 736, 737, 772, 739, 740, 773, 774, 775, 776, 777, 7
78, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 812, 813, 814, 815, 816, 817, 818, 792, 819, 820, 795, 821, 793, 822, 823, 824,
825, 826, 827, 828, 829, 830, 797, 831, 832, 833, 834, 835, 836, 837, 838, 800, 839, 840, 841, 842, 802, 843, 844, 804, 845, 846, 806, 847, 84
8, 808, 849, 850, 810, 851, 852, 853, 798, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873,
874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909
, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 613, 510, 933, 934, 935, 9
36, 937, 944, 979, 980, 981, 952, 982, 983, 984, 985, 986, 987, 988, 954, 989, 990, 991, 992, 959, 960, 938, 939, 993, 962, 963, 994, 967, 995,
970, 996, 972, 997, 974, 968, 998, 976, 977, 964, 965, 940, 941, 942, 943, 344, 345, 346, 347, 348, 349, 350, 351
/XObject 51: 30, 29, 32, 31, 33, 34, 35, 36, 73, 107, 106, 105, 104, 103, 212, 211, 214, 213, 233, 235, 234, 236, 248, 247, 251, 255, 256, 257
, 271, 272, 273, 288, 289, 290, 321, 325, 324, 527, 529, 528, 726, 728, 727, 888, 945, 946, 947, 948, 949, 950, 1016
/XRef 1: 1021
Search keywords:
/URI 62: 341, 352, 354, 356, 358, 360, 362, 364, 366, 368, 370, 372, 374, 376, 378, 380, 382, 384, 386, 388, 390, 392, 394, 535, 538, 541, 585
```

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Antimalware: pdf-parser.py y pdf-tools

```
78, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 812, 813, 814, 815, 816, 817, 818, 792, 819, 820, 795, 821, 793, 822, 823, 824,
825, 826, 827, 828, 829, 830, 797, 831, 832, 833, 834, 835, 836, 837, 838, 800, 839, 840, 841, 842, 802, 843, 844, 804, 845, 846, 806, 847, 84
8, 808, 849, 850, 810, 851, 852, 853, 798, 854, 855, 856, 857, 858, 859, 860, 861, 862, 863, 864, 865, 866, 867, 868, 869, 870, 871, 872, 873,
874, 875, 876, 877, 878, 879, 880, 881, 882, 883, 884, 885, 886, 887, 895, 896, 897, 898, 899, 900, 901, 902, 903, 904, 905, 906, 907, 908, 909
, 910, 911, 912, 913, 914, 915, 916, 917, 918, 919, 920, 921, 922, 923, 924, 925, 926, 927, 928, 929, 930, 931, 932, 613, 510, 933, 934, 935, 9
36, 937, 944, 979, 980, 981, 952, 982, 983, 984, 985, 986, 987, 988, 954, 989, 990, 991, 992, 959, 960, 938, 939, 993, 962, 963, 994, 967, 995,
970, 996, 972, 997, 974, 968, 998, 976, 977, 964, 965, 940, 941, 942, 943, 344, 345, 346, 347, 348, 349, 350, 351
/XObject 51: 30, 29, 32, 31, 33, 34, 35, 36, 73, 107, 106, 105, 104, 103, 212, 211, 214, 213, 233, 235, 234, 236, 248, 247, 251, 255, 256, 257
, 271, 272, 273, 288, 289, 290, 321, 325, 324, 527, 529, 528, 726, 728, 727, 888, 945, 946, 947, 948, 949, 950, 1016
/XRef 1: 1021
Search keywords:
/URI 62: 341, 352, 354, 356, 358, 360, 362, 364, 366, 368, 370, 372, 374, 376, 378, 380, 382, 384, 386, 388, 390, 392, 394, 535, 538, 541, 585
, 588, 591, 593, 595, 597, 599, 601, 603, 605, 607, 610, 614, 616, 729, 732, 735, 738, 791, 794, 796, 799, 801, 803, 805, 807, 809, 951, 953, 9
58, 961, 966, 969, 971, 973, 975
[gramo@localhost pdfparser]$
[gramo@localhost pdfparser]$ ./pdf-parser.py --search javascript ../Respuesta_Mariano_Pedroza_No_de_radicado_20222200406721.pdf
[gramo@localhost pdfparser]$ ./pdf-parser.py --search javascript -raw ../Respuesta_Mariano_Pedroza_No_de_radicado_20222200406721.pdf
[gramo@localhost pdfparser]$
```

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- Busca código javascript embebido
- Pdf-tools
 - <https://blog.didierstevens.com/programs/pdf-tools/>
 - <https://youtu.be/tHVi2wKCkTc>
 - <https://drbeni.ch/malware-analysis-lab>

```
Terminal — bash — bash (tty1) — 96x50 — %1

Your system contains some unknown version numbers. Please run Rootkit Hunter
with the --update parameter or fill in the contact form (www.rootkit.nl)

Security advisories
* Check: Groups and Accounts
  Searching for /etc/passwd...           [ Found ]
  Checking users with UID '0' (root)...  [ OK ]

* Check: SSH
  Searching for sshd_config...
  Found /etc/sshd_config
  Checking for allowed root login... Watch out Root login possible. Possible risk!
  info:
  Hint: See logfile for more information about this issue
  Checking for allowed protocols...      [ Warning (SSH v1 allowed) ]

* Check: Events and Logging
  Search for syslog configuration...      [ OK ]
  Checking for running syslog slave...    [ OK ]
  Checking for logging to remote system... [ OK (remote logging) ]
  info: install.*                        @127.0.0.1:32376

[Press <ENTER> to continue]

----- Scan results -----

MD5
MD5 compared: 0
Incorrect MD5 checksums: 0

File scan
Scanned files: 342
Possible infected files: 0

Application scan
Vulnerable applications: 0

Scanning took 129 seconds

-----

Do you have some problems, undetected rootkits, false positives, ideas
or suggestions?
Please e-mail me by filling in the contact form (@http://www.rootkit.nl)
-----
```

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



- Inventarios de activos.
 - Adquisición/disposición de activos
 - Cambios en el personal (Contratación/Fin de contrato)
 - Disposición final / Retención de la información.
- Plan de mejora continua del SOC.
 - Adquisición y apropiación de nuevas herramientas. <https://opensoc.io/>
 - Capacitación permanente.
 - Actualizar buenas prácticas y procedimientos.
 - Uso de las nuevas herramienta adquiridas.
- Canales de comunicación con comunidad y pares para:
 - Identificar nuevas amenazas / vulnerabilidades emergentes.
 - Reportar incidentes (informes, alertas o denuncias).

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- Plan y operación de backups.
 - Parámetros de configuración de software
 - Información
 - Prioridad y orden
 - Cuantificar / valorar el tiempo de:
Generación / Recuperación.
- Simulacros.
 - Incidentes.
 - Recuperación.

Preparativas

Preventivas

Detectivas

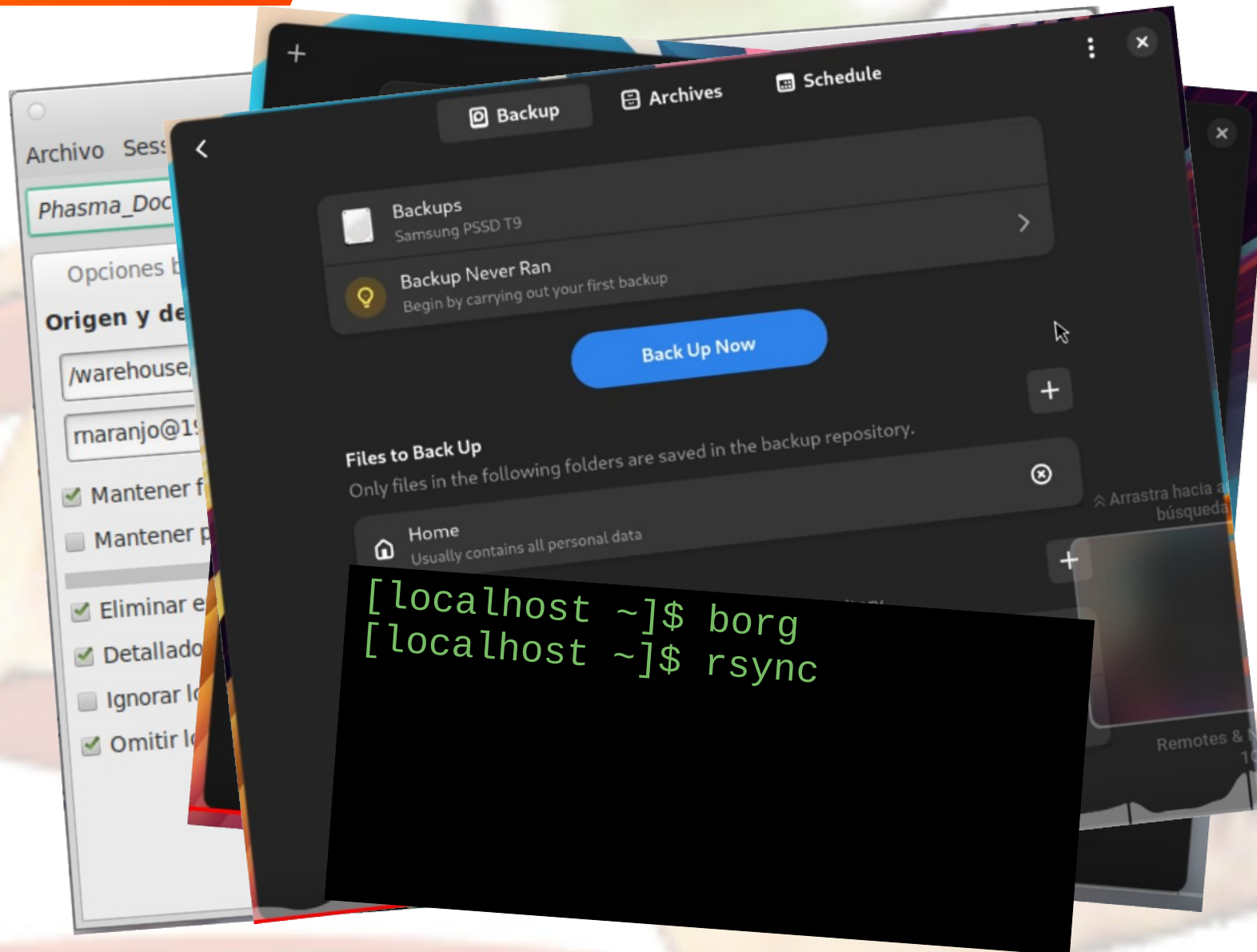
Reactivas

Retrospectivas



Preventivas

Planear la reacción



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

El computador más seguro del mundo es aquel que está desconectado ...

... pero siempre conseguirás que alguien lo conecte por ti.

- El recurso humano es la principal causa de problemas de seguridad.
- La compacencia es aliada del intruso.
- Auditar periódicamente para:
 - Aconsejar / Capacitar personal.
 - Detectar inconformidades.
 - Verificar el cumplimiento.
 - Aplicar procedimientos disciplinarios.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Preventivas

Capacitación y sensibilización

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



La matriz de Eisenhower ajustada

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Impacto en mitigación de riesgos

Alto

Costo de implementacion del control

Bajo

Alto

¡Hazlo ya!

Abordar riesgos críticos de manera eficiente, serán los primeros controles en ser implementados.

Planealo

Justificar la inversión con un análisis costo-beneficio o evaluar la posibilidad de asumir el riesgo o tercerizarlo mediante un seguro.

Bajo

Cuando se pueda

Pueden considerar ser implementados por su bajo costo, a pesar que mitigan riesgos de menor prioridad.

Usa mejor tus recursos

Evaluar cuidadosamente antes de implementar, en la mayoría de los casos se descartan para utilizar los recursos en otras áreas.

A green frog is perched on a red, curved ledge. The frog is looking towards the left. The background is a plain, light color.

Actividades

A person is sitting at a desk in a dimly lit room, working on a computer. There are several monitors displaying data and charts. The person is wearing a blue shirt and is looking at the screens.

Detectivas

- Monitoreo 24x7
- Alertas oportunas
- Conocer síntomas

- Monitoreo de funcionamiento de equipos y red:
 - Análisis de bitácoras.
 - Comparar con línea base.
 - Periódicamente.
 - Identificar cambios:
 - Detectar posibles ataques.
 - Identificar falsos positivos.
 - Ajustar línea base.
- Emisión de alertas oportunas.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- top / htop
- glances

Preparativas

Preventivas



```
[localhost ~]$ auditd
[localhost ~]$ lastcomm
[localhost ~]$ kill
[localhost ~]$ killall
[localhost ~]$ nice
[localhost ~]$ renice
```

```
command
mplescreenrecor
mplescreenrecor
ary
r/bin/X :0 -au
ry
plescreenrecor
plescreenrecor
plescreenrecor
plescreenrecor
plescreenrecor
plescreenrecor
/bin/pulseaud
plescreenrecor
e-terminal
F10
```

• kvsquard / monitor del sistema mate

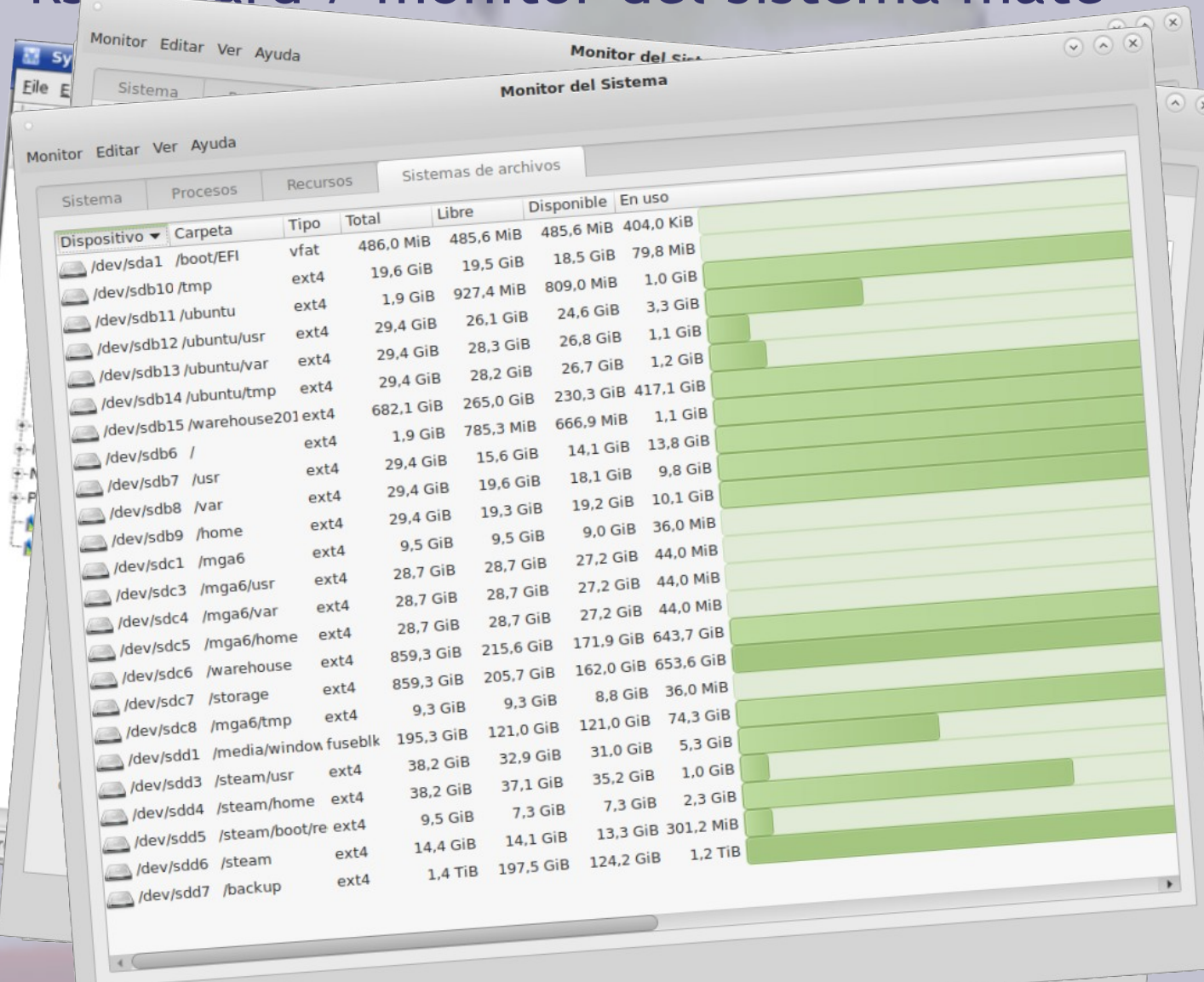
Preparativas

Preventivas

Detectivas

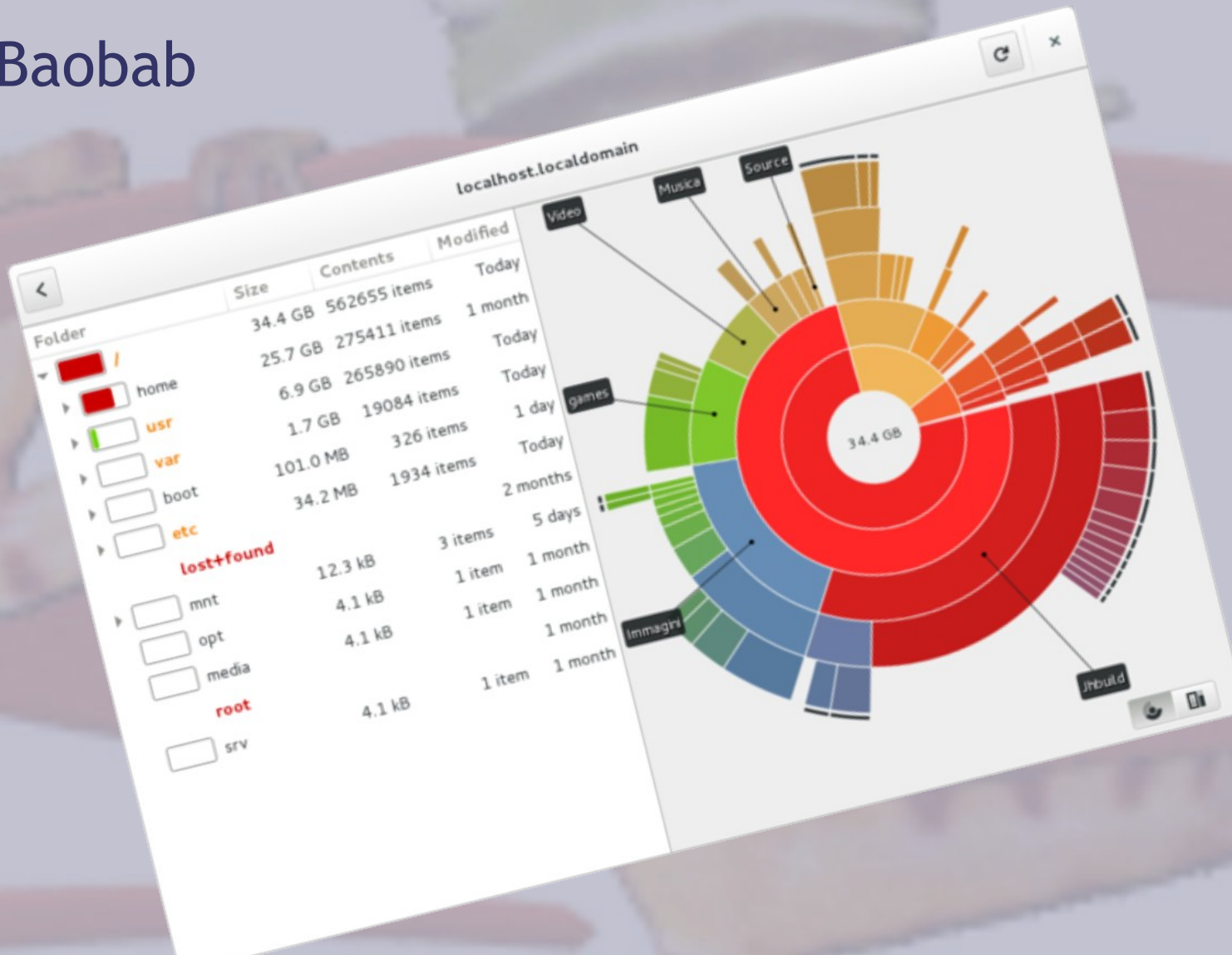
Reactivas

Retrospectivas



Sistema	Procesos	Recursos	Sistemas de archivos			
Dispositivo	Carpeta	Tipo	Total	Libre	Disponibile	En uso
/dev/sda1	/boot/EFI	vfat	486,0 MiB	485,6 MiB	485,6 MiB	404,0 KiB
/dev/sdb10	/tmp	ext4	19,6 GiB	19,5 GiB	18,5 GiB	79,8 MiB
/dev/sdb11	/ubuntu	ext4	1,9 GiB	927,4 MiB	809,0 MiB	1,0 GiB
/dev/sdb12	/ubuntu/usr	ext4	29,4 GiB	26,1 GiB	24,6 GiB	3,3 GiB
/dev/sdb13	/ubuntu/var	ext4	29,4 GiB	28,3 GiB	26,8 GiB	1,1 GiB
/dev/sdb14	/ubuntu/tmp	ext4	29,4 GiB	28,2 GiB	26,7 GiB	1,2 GiB
/dev/sdb15	/warehouse201	ext4	682,1 GiB	265,0 GiB	230,3 GiB	417,1 GiB
/dev/sdb6	/	ext4	1,9 GiB	785,3 MiB	666,9 MiB	1,1 GiB
/dev/sdb7	/usr	ext4	29,4 GiB	15,6 GiB	14,1 GiB	13,8 GiB
/dev/sdb8	/var	ext4	29,4 GiB	19,6 GiB	18,1 GiB	9,8 GiB
/dev/sdb9	/home	ext4	29,4 GiB	19,3 GiB	19,2 GiB	10,1 GiB
/dev/sdc1	/mga6	ext4	9,5 GiB	9,5 GiB	9,0 GiB	36,0 MiB
/dev/sdc3	/mga6/usr	ext4	28,7 GiB	28,7 GiB	27,2 GiB	44,0 MiB
/dev/sdc4	/mga6/var	ext4	28,7 GiB	28,7 GiB	27,2 GiB	44,0 MiB
/dev/sdc5	/mga6/home	ext4	28,7 GiB	28,7 GiB	27,2 GiB	44,0 MiB
/dev/sdc6	/warehouse	ext4	859,3 GiB	215,6 GiB	171,9 GiB	643,7 GiB
/dev/sdc7	/storage	ext4	859,3 GiB	205,7 GiB	162,0 GiB	653,6 GiB
/dev/sdc8	/mga6/tmp	ext4	9,3 GiB	9,3 GiB	8,8 GiB	36,0 MiB
/dev/sdd1	/media/window	fuseblk	195,3 GiB	121,0 GiB	121,0 GiB	74,3 GiB
/dev/sdd3	/steam/usr	ext4	38,2 GiB	32,9 GiB	31,0 GiB	5,3 GiB
/dev/sdd4	/steam/home	ext4	38,2 GiB	37,1 GiB	35,2 GiB	1,0 GiB
/dev/sdd5	/steam/boot/re	ext4	9,5 GiB	7,3 GiB	7,3 GiB	2,3 GiB
/dev/sdd6	/steam	ext4	14,4 GiB	14,1 GiB	13,3 GiB	301,2 MiB
/dev/sdd7	/backup	ext4	1,4 TiB	197,5 GiB	124,2 GiB	1,2 TiB

- ksysguard / monitor del sistema mate
- Baobab



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- John the ripper

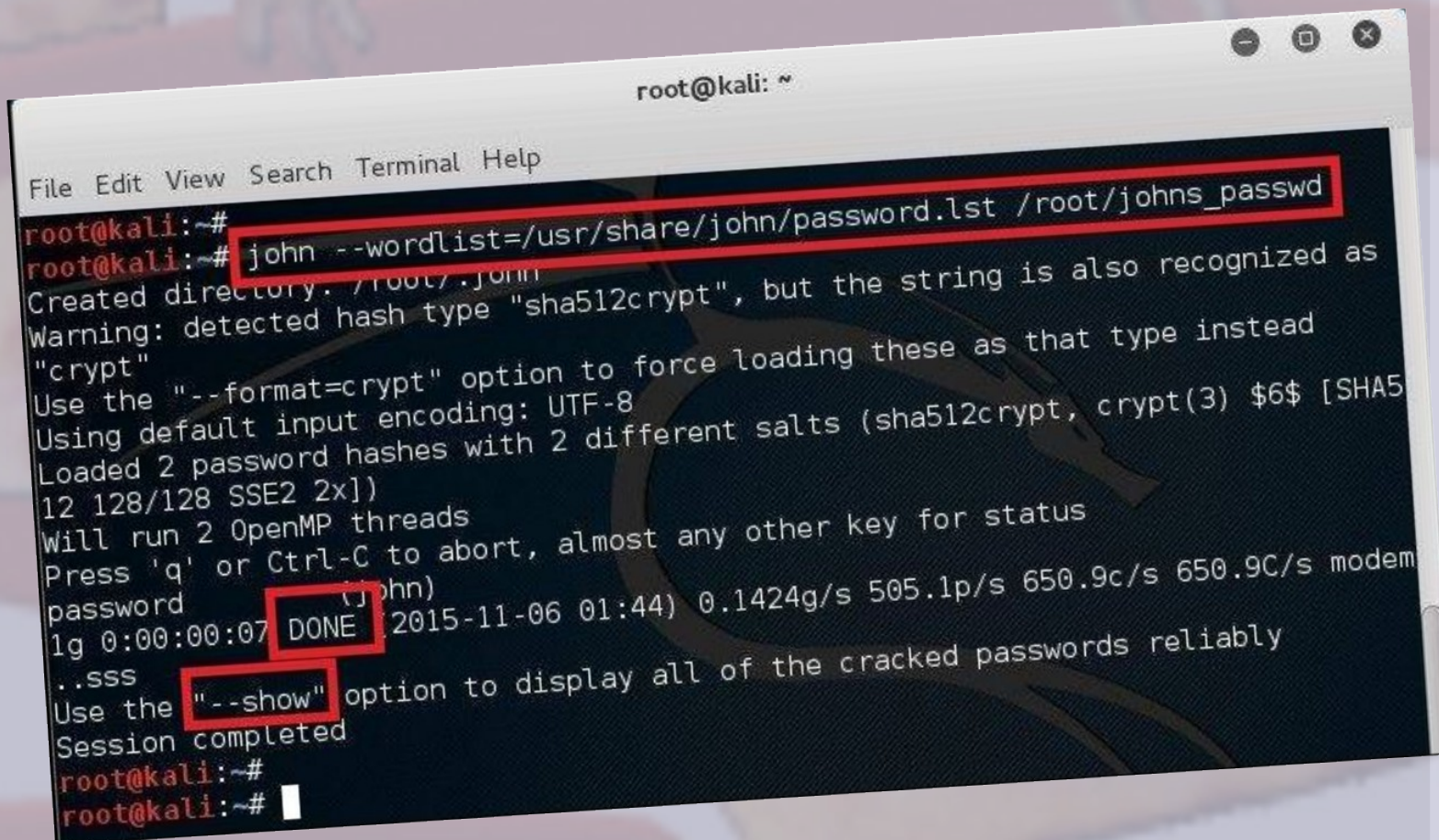
Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# john --wordlist=/usr/share/john/password.lst /root/johns_passwd
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as
"crypto"
Use the "--format=crypt" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 2 password hashes with 2 different salts (sha512crypt, crypt(3) $6$ [SHA5
12 128/128 SSE2 2x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
password (john)
lg 0:00:00:07 DONE (2015-11-06 01:44) 0.1424g/s 505.1p/s 650.9c/s 650.9C/s modem
..sss
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@kali:~#
root@kali:~#
```


- John the ripper
- Hydra

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

dawid@lab: ~

File Edit View Search Terminal Help

da ab:~\$ hydra -L list user -P list password 192.168.56.101 ftp -V
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2013-09-04 07:24:27
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking service ftp on port 21

[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_1" - 1 of 12 [child 0]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password" - 2 of 12 [child 1]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "msfadmin" - 3 of 12 [child 2]
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_2" - 4 of 12 [child 3]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_1" - 5 of 12 [child 4]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password" - 6 of 12 [child 5]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "msfadmin" - 7 of 12 [child 6]
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_2" - 8 of 12 [child 7]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_1" - 9 of 12 [child 8]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password" - 10 of 12 [child 9]
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10]
[21][ftp] host: 192.168.56.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-09-04 07:24:30

Detectivas

Monitorix
v3.8.1



Monitorix
v3.15.0

Hostname	Graph
localhost	All graphs
Local Host	
localhost	Weekly
Multihost	
All	Monthly
Producción	Yearly
Backups	
Laboratorio	

Ok

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Detectivas

Monitorear comportamiento

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Detectivas

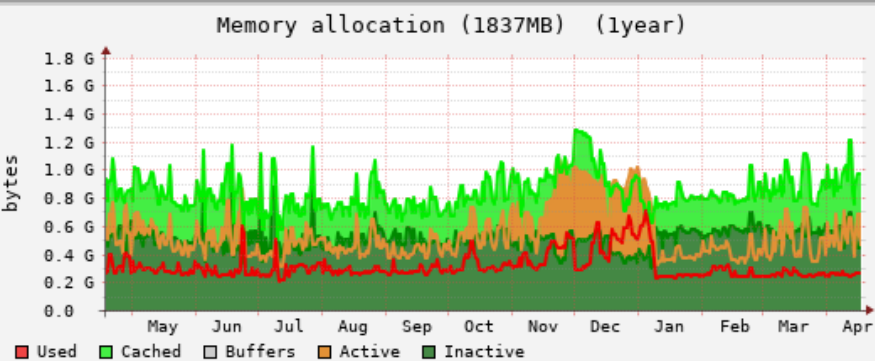
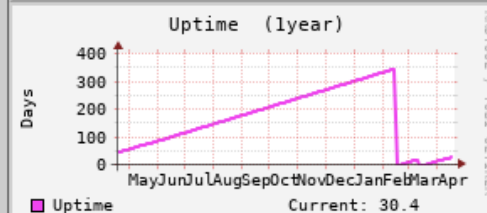
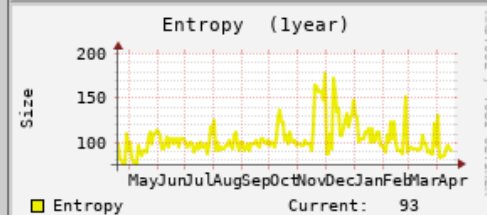
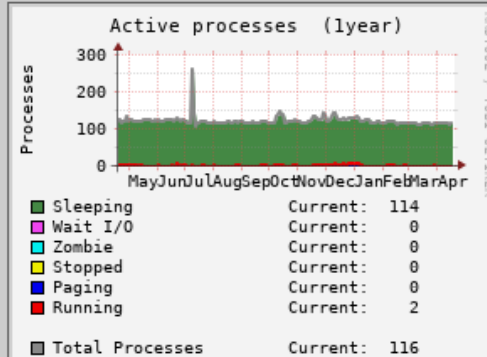
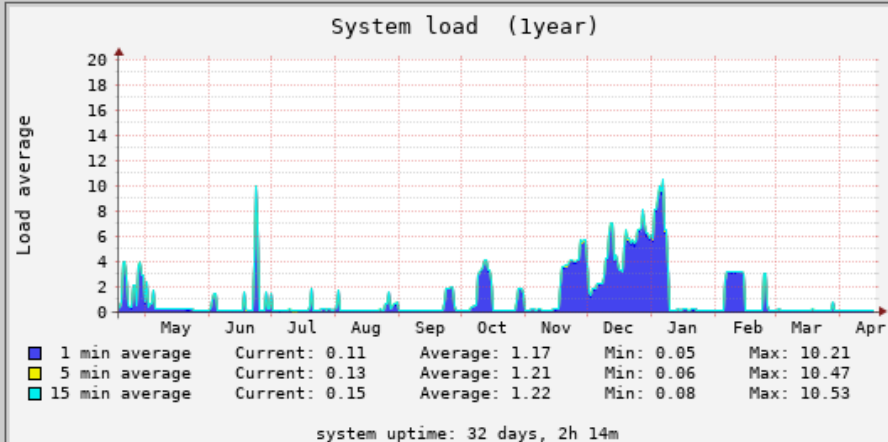
Monitorix

v3.8.1

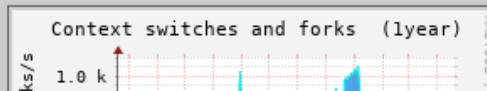
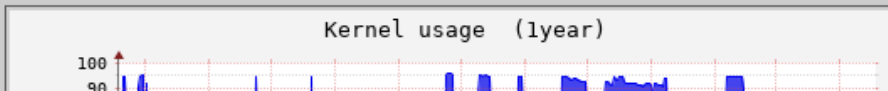
Host: **monitorix.skinait.com** last year

Wed Apr 17 17:21:10 UTC 2024

System load average and usage



Global kernel usage



Preparativas

Preventivas

Detectivas

Reactivas

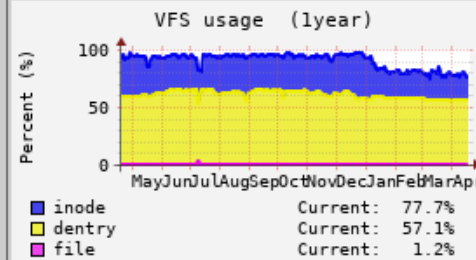
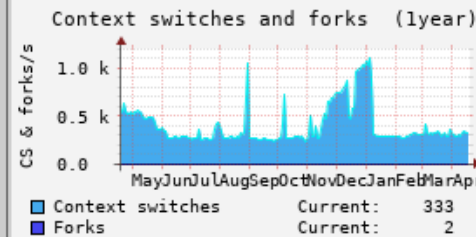
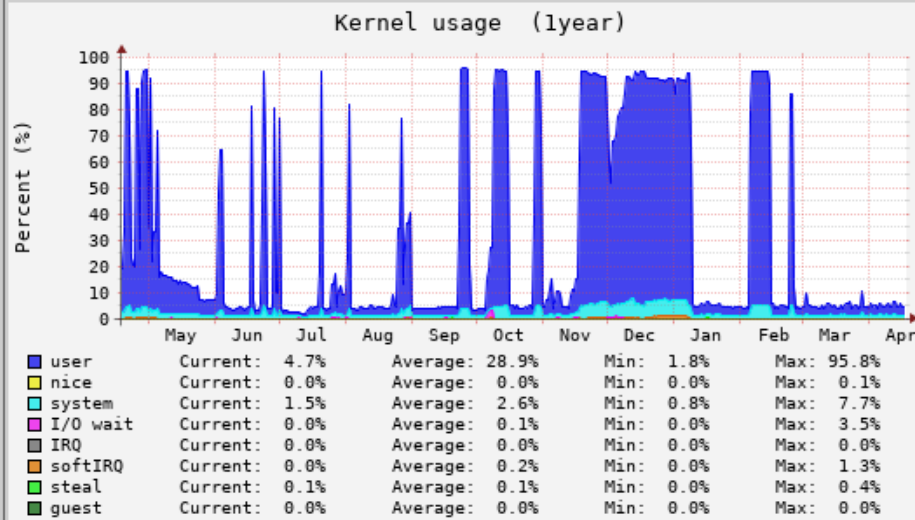
Retrospectivas

Detectivas

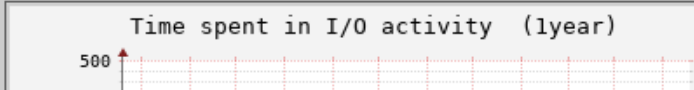
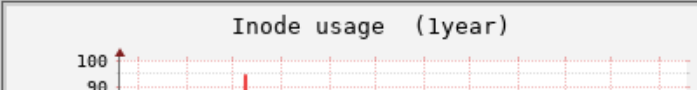
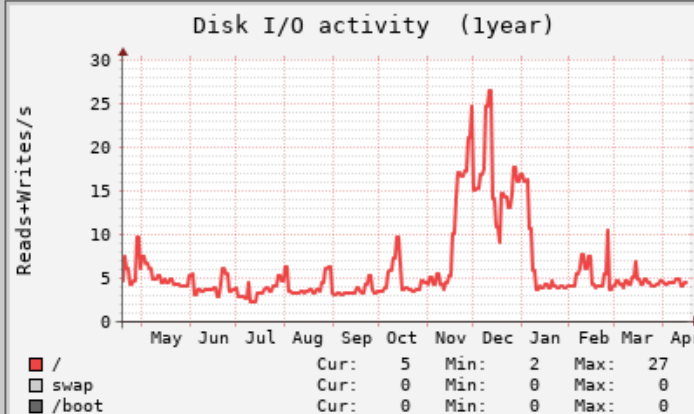
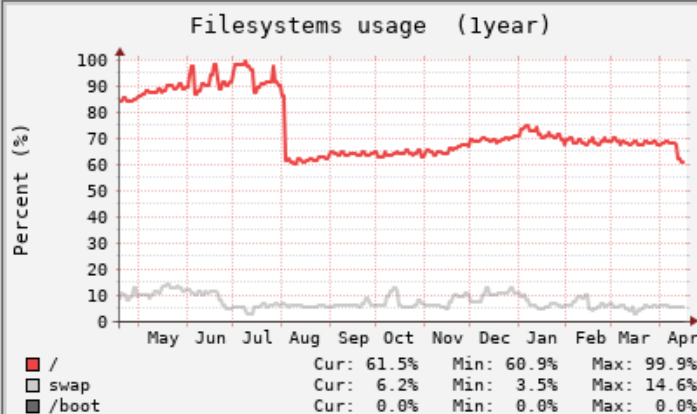
Monitorix v3.8.1



Global kernel usage



Filesystem usage and I/O activity



Preparativas

Preventivas

Detectivas

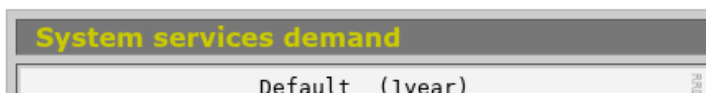
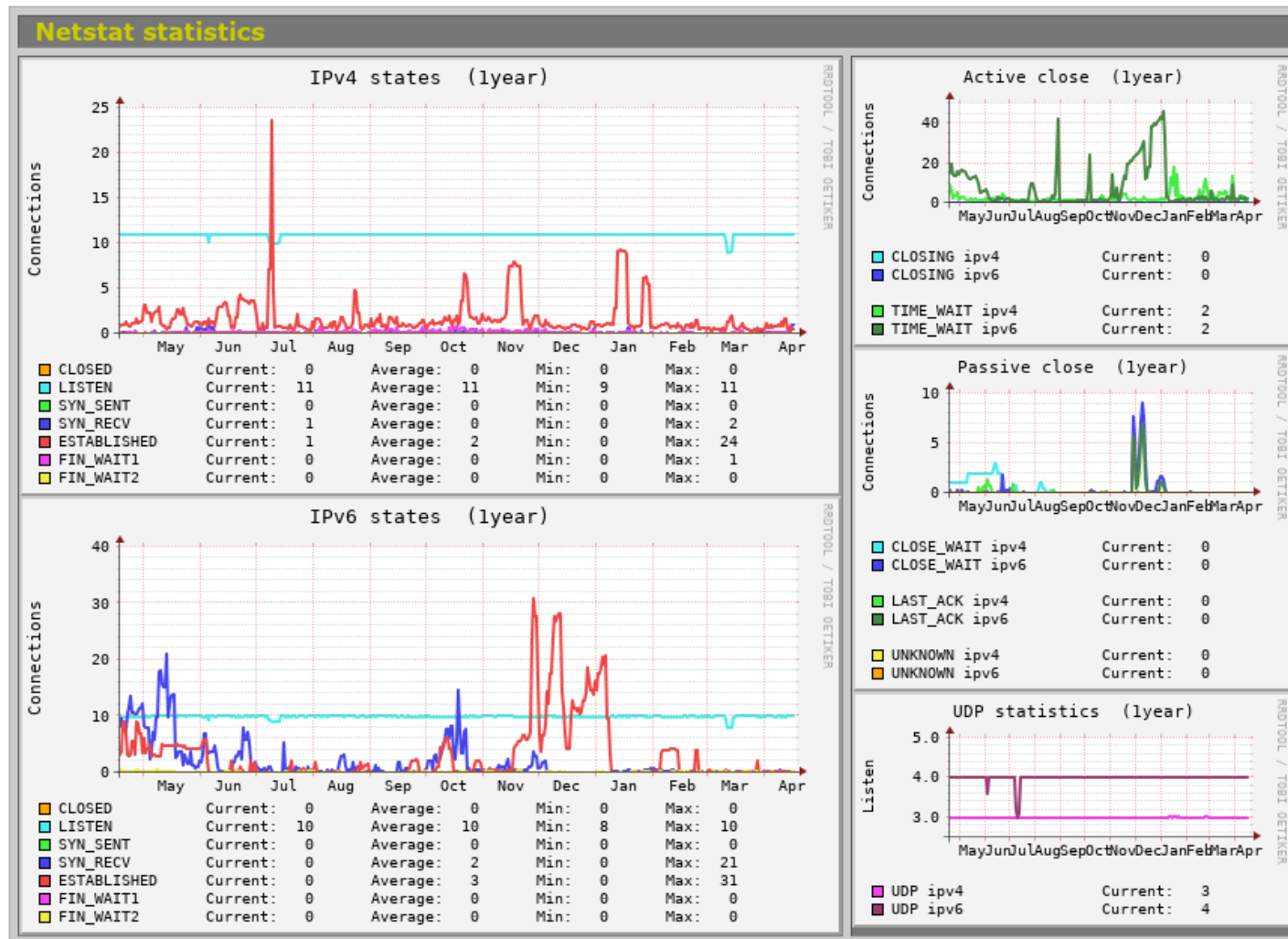
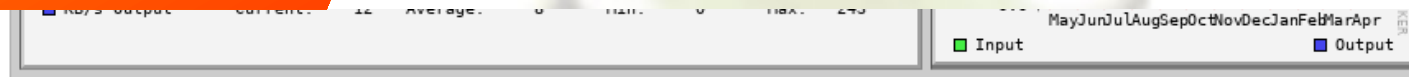
Reactivas

Retrospectivas



Detectivas

Monitorix v3.8.1



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

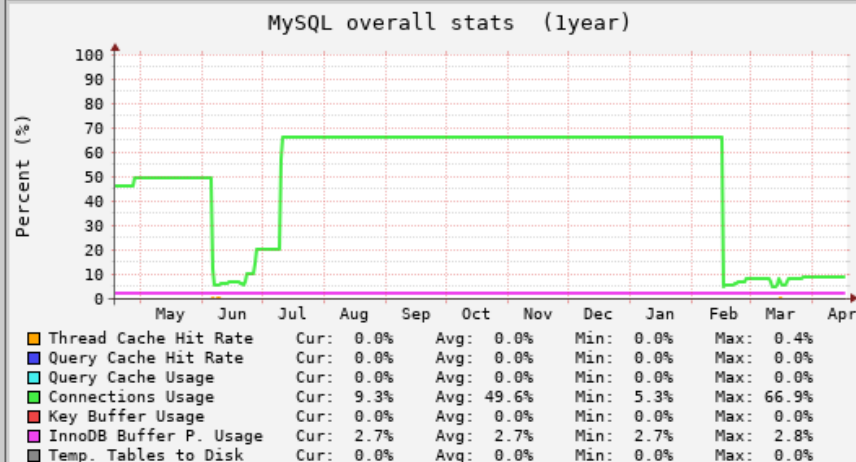
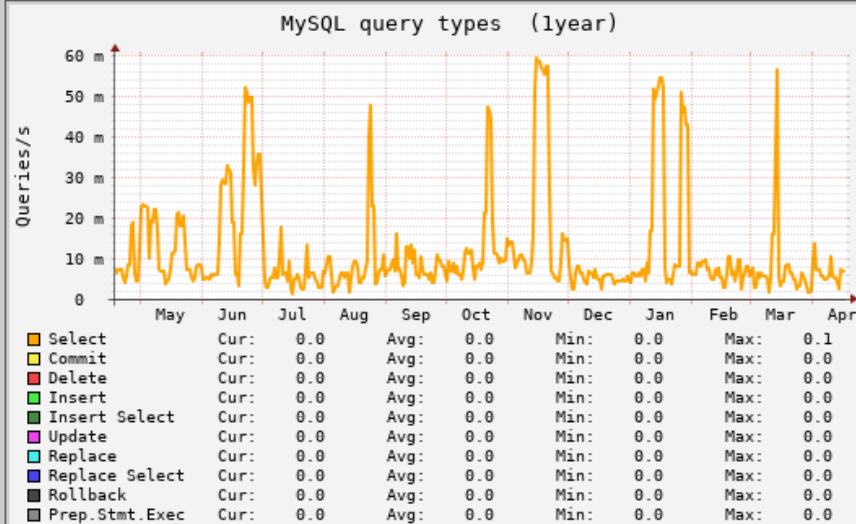


Detectivas

Monitorix v3.8.1

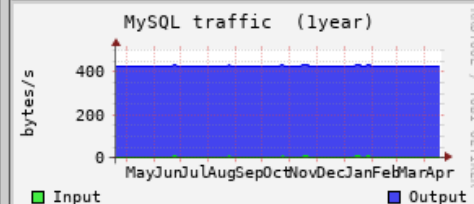
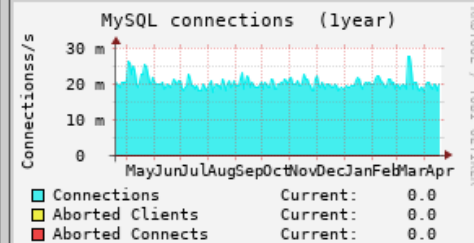
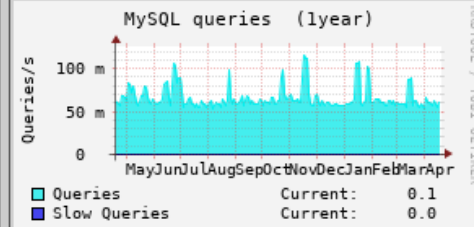
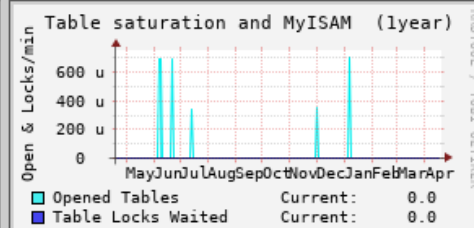
server-status?auto

MySQL statistics



localhost:3306

PostgreSQL statistics



Preparativas

Preventivas

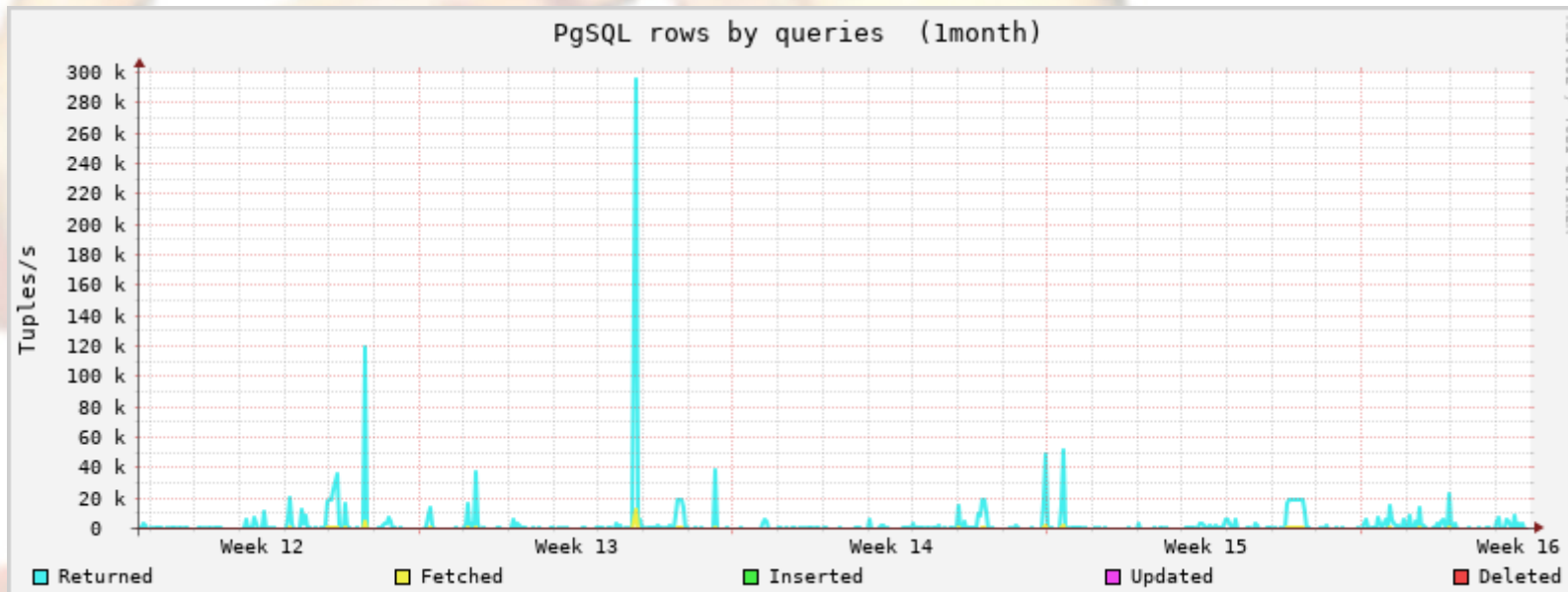
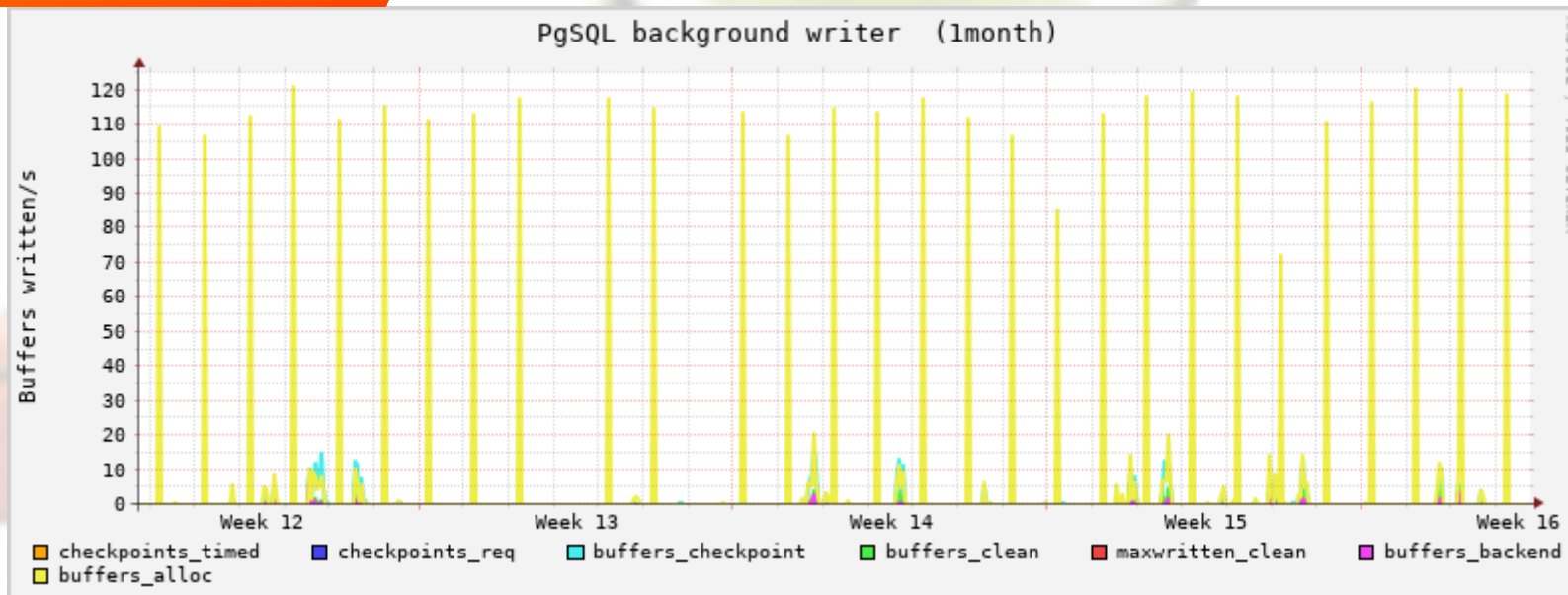
Detectivas

Reactivas

Retrospectivas

Detectivas

Monitorix v3.8.1



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

- Full Opensource
- Bajo consumo de procesamiento/RAM
- Voltaje memoria RAM → SPAM enviado por SMTP.
- MRTG: Carga de red.
- Reportes/estadísticas graficos.
- Almacena históricos para comparar.
- Alertas x email.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

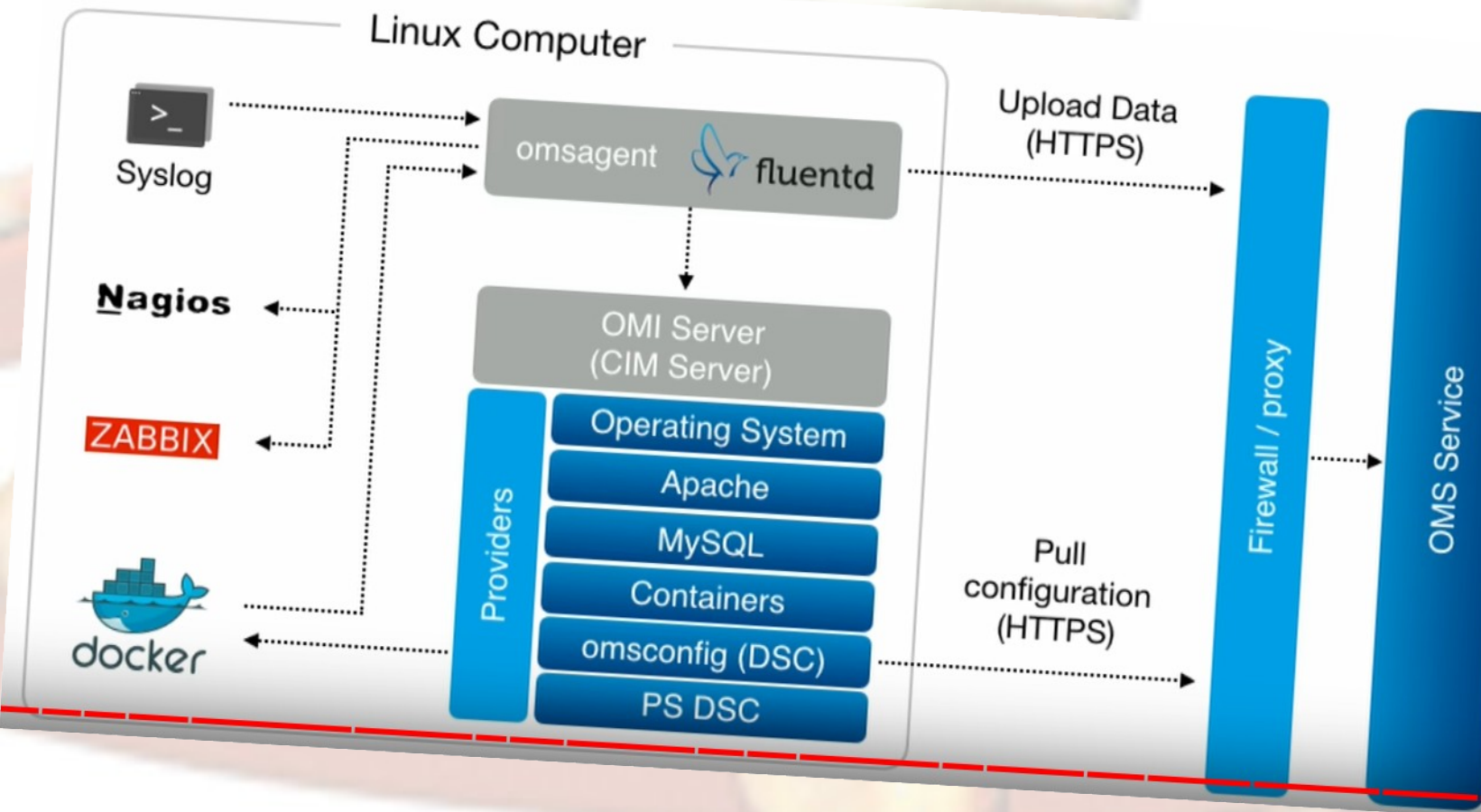
<https://youtu.be/ARRWV-rnHe4?t=304>

Activar Monitorix para varios equipos



Detectivas

Fluentd – Unificando información de bitácoras



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Detectivas

ZABBIX

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Detectivas



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Detectivas

Análisis de bitácoras: Elasticstack

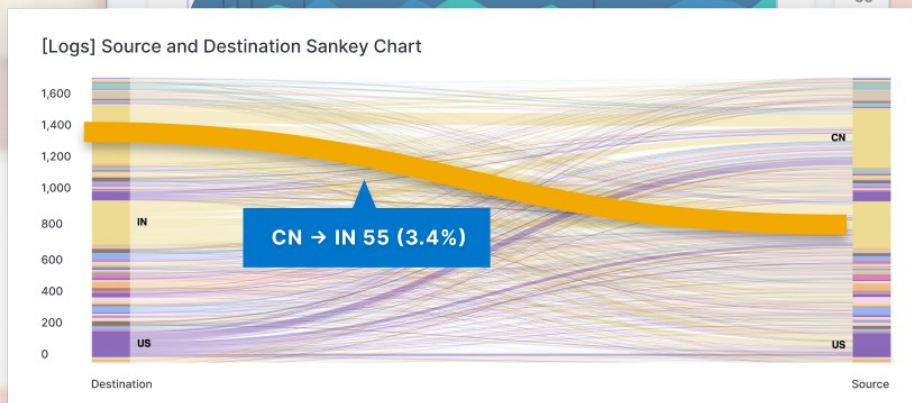
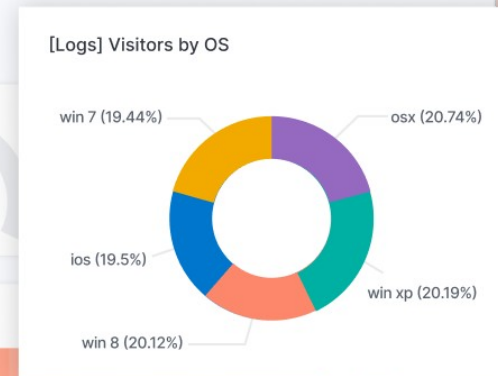
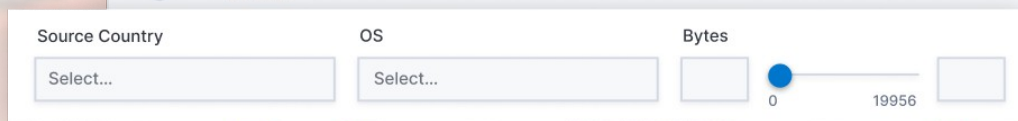
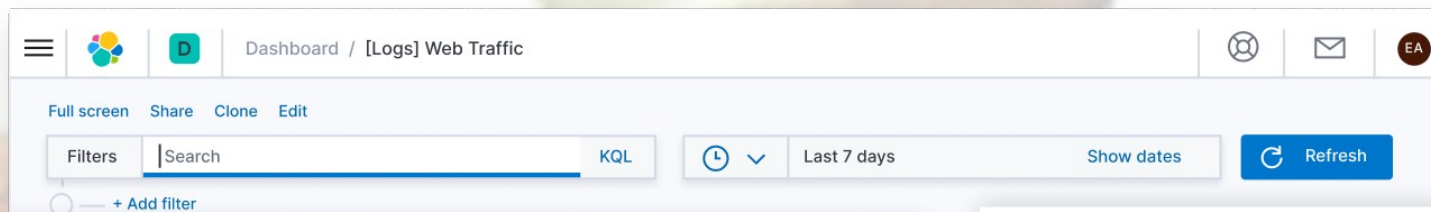
Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Detectivas

Análisis de bitácoras: graylog

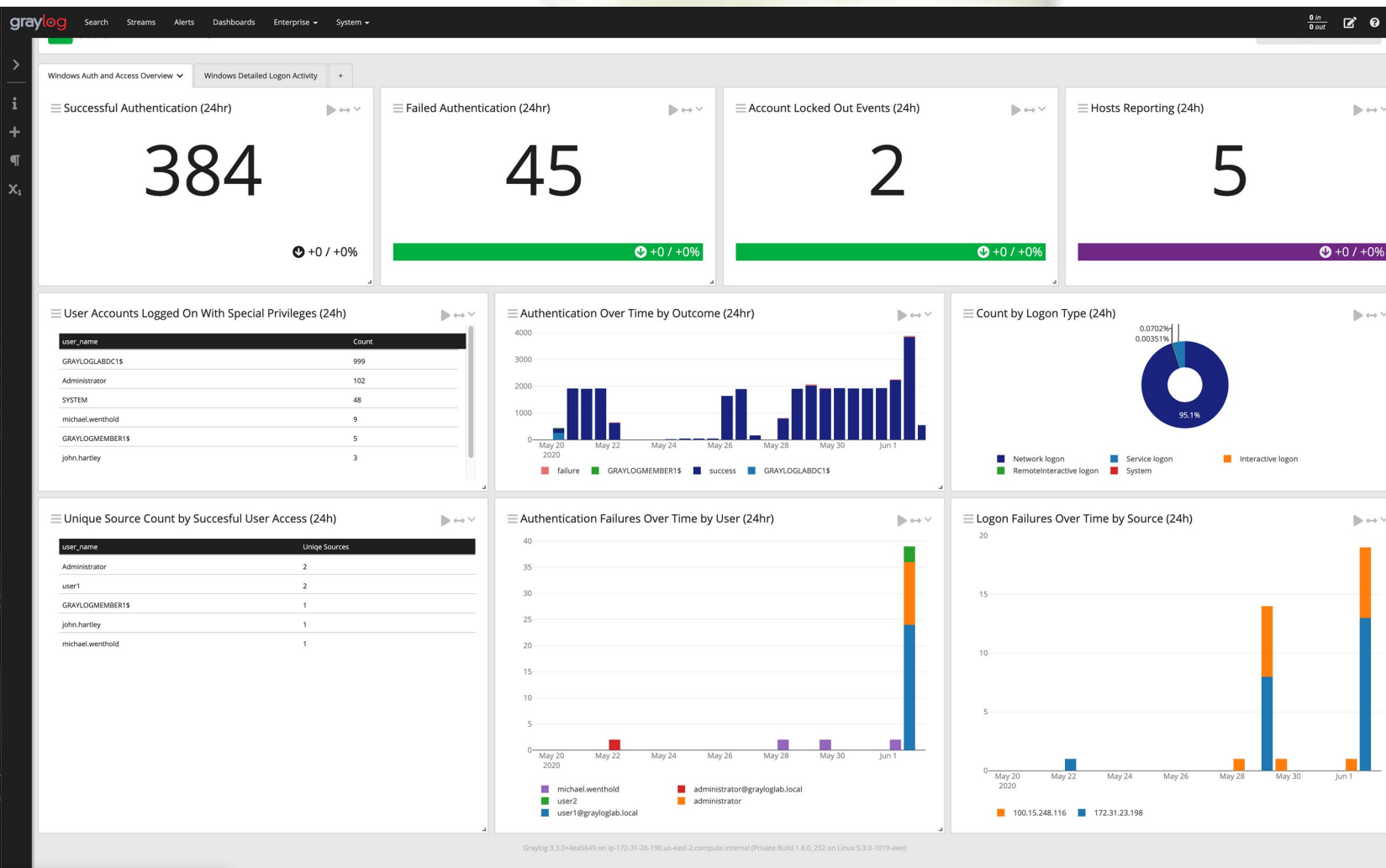
Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Detectivas

Verificar SSL

<https://www.ssllabs.com/ssltest/analyze.html>

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > javeriana.edu.co

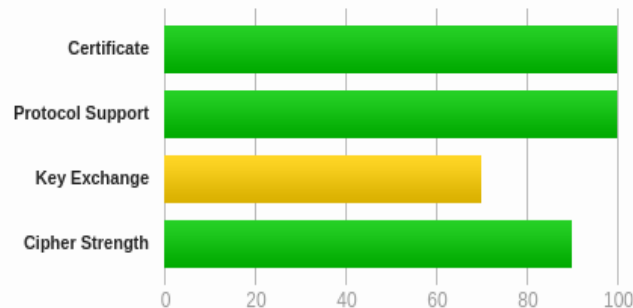
SSL Report: javeriana.edu.co (200.3.149.136)

Assessed on: Sun, 17 Mar 2024 23:45:04 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server does not support Forward Secrecy with the reference browsers. Grade capped to B. [MORE INFO »](#)

This site works only in browsers with SNI support.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO »](#)

Detectivas

¿Estás en listas negras?

- <https://ipcheck.proofpoint.com/>

proofpoint. Products Solutions Partners Resources Company

DYNAMIC REPUTATION IP LOOKUP

CHECK YOUR IP ADDRESS HERE

If your IP address is currently on our IP blocklist, or your IP is experiencing sending delays, this tool will help you determine if your IP is on our blocklist.

FOR PROOFPOINT CLIENTS

If you are a Proofpoint client, please click here for an expedited response.

IP Address *

159.65.88.88

✓ No soy un robot

reCAPTCHA
Privacidad - Términos

LOOKUP IP

Detectivas

mail-tester.com

Wow! Perfecto, puedes enviar

Puntuación:

10/10

Asunto : Prueba

Recibido hace 0 minutos

✓ Haz clic aquí para ver tu mensaje

✓ Le gustas a SpamAssassin

✓ No estás completamente autenticado

✓ Tu mensaje se podría mejorar

✓ No estás en ninguna lista negra

✓ No hay enlaces rotos

Tu adorable total: 10/10

- Comportamientos fuera de lo normal
 - Comparar con línea base
 - NIDS
- Triage de incidentes
 - Verificación inicial.
 - ¿Está sucediendo?
 - ¿que tan peligroso es?
 - Valor/identificación de los activos expuestos/afectados.
 - Nivel jerárquico del personal afectado.
 - Identificar falsos positivos.
 - Priorización ← Según el impacto y la reacción.

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Actividades



Reactivas

- Contener
- Erradicar
- Remediar
- Restaurar

- Contener el incidente para que no escale
- Investigar el incidente
 - Causas
 - Alcance
- Levantar evidencias
- Erradicar las fuentes del incidente
- Remediar
 - Activos expuestos o vulnerables.
 - Previendo que no se repita.
- Restaurar el funcionamiento a la normalidad
- Comunicar (Reportes / Alertas)

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Reactivas

Contención



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

```
[~]$ su -  
Contraseña:  
Último inicio de sesión:dom mar 21 16:17:52 UTC 2021 en pts/0  
Último inicio de sesión fallido:lun mar 29 15:52:20 UTC 2020 de  
159.65.11.115 en ssh:notty  
Hubo 79535 intentos de logueo fallidos desde el último logueo exitoso.
```

- Identifica intentos fallidos de acceso
- Si supera el máximo permitido → bloqueo
- Tras cierto tiempo vuelve a autorizar
- Si supera el máximo → bloqueo por más tiempo.

```
[~]$ su -  
Password:  
Last login: Tue Apr 30 01:03:57 UTC 2024 on pts/0  
Last failed login: Tue Apr 30 19:40:25 UTC 2024 from 43.157.80.160 on ssh:notty  
There were 628 failed login attempts since the last successful login.
```

Preparativas

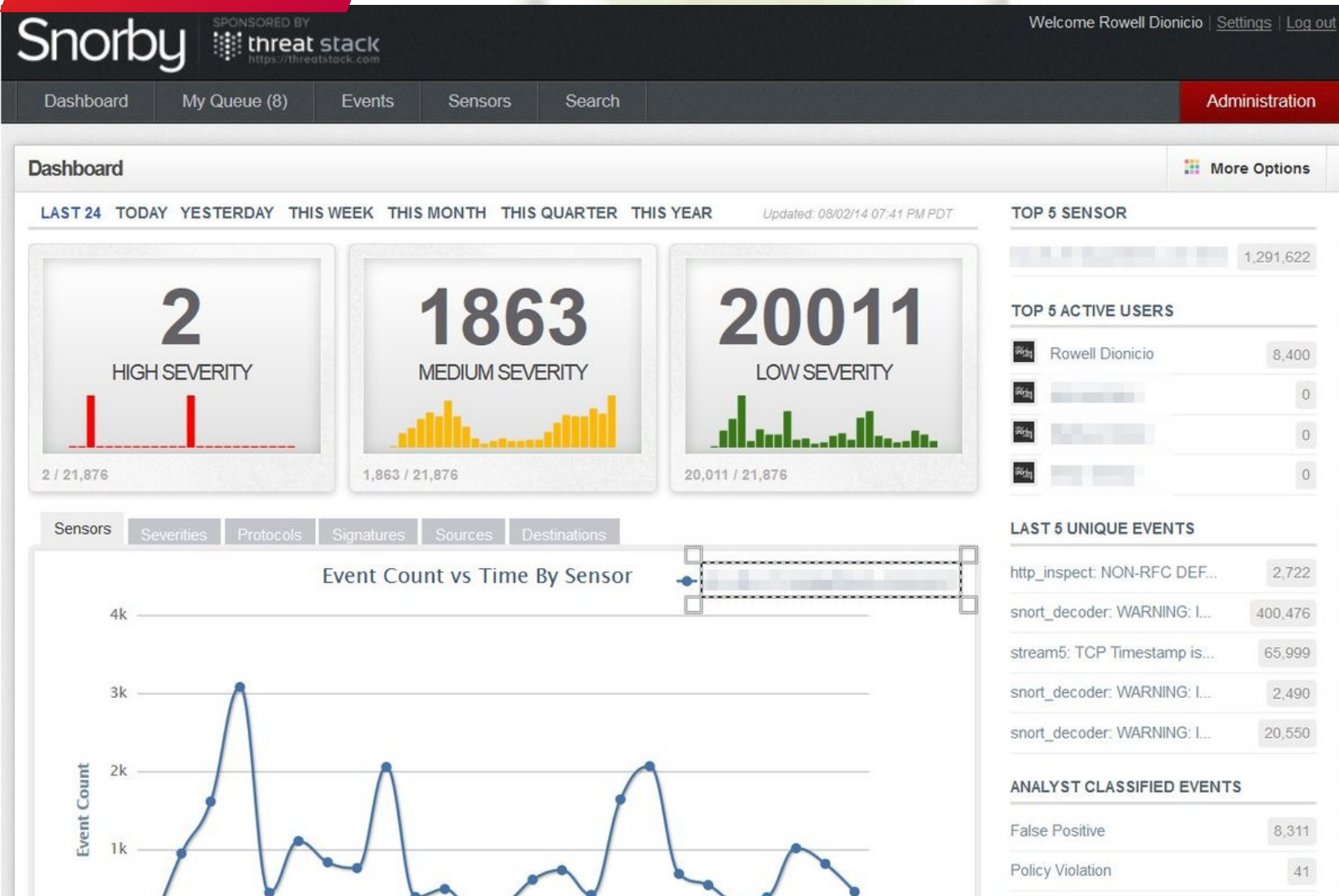
Preventivas

Detectivas

Reactivas

Retrospectivas

Reactivas



Preparativas

Preventivas

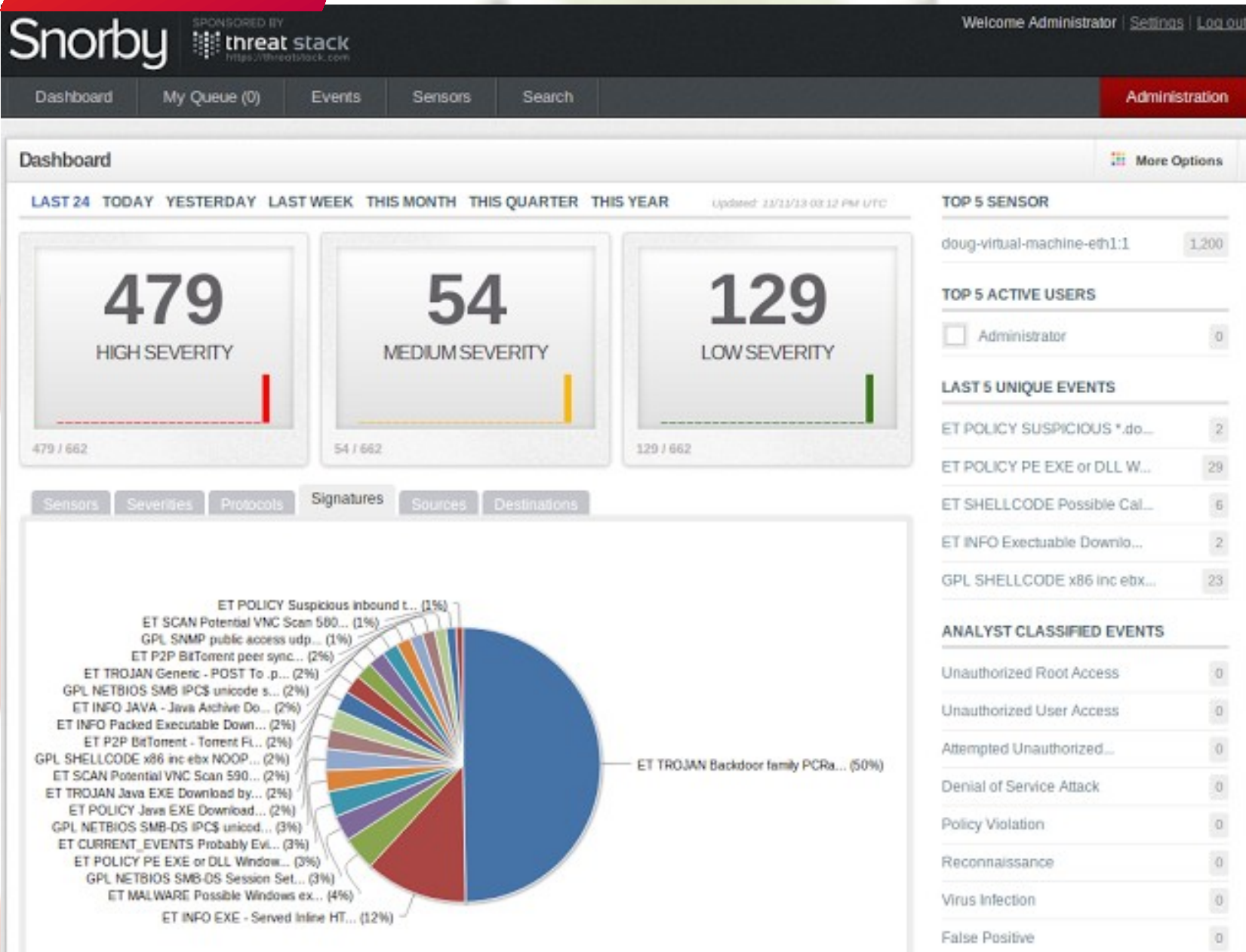
Detectivas

Reactivas

Retrospectivas



Reactivas



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas





Snort Interfaces Global Settings Updates Alerts Blocked Pass Lists Suppress IP Lists SID Mgmt Log Mgmt Sync

Snort Vulnerability Research Team (VRT) Rules

Enable Snort VRT ☒ Click to enable download of Snort VRT free Registered User or paid Subscriber rules

[Sign Up for a free Registered User Rule Account](#)
[Sign Up for paid Sourcefire VRT Certified Subscriber Rules](#)

Snort Oinkmaster Code

Obtain a snort.org Oinkmaster code and paste it here. (Paste the code only and not the URL!)

Snort GPLv2 Community Rules

Enable Snort GPLv2 ☐ Click to enable download of Snort GPLv2 Community rules

The Snort Community Ruleset is a GPLv2 VRT certified ruleset that is distributed free of charge without any VRT License restrictions. This ruleset is updated daily and is a subset of the subscriber ruleset.

Emerging Threats (ET) Rules

Enable ET Open ☒ Click to enable download of Emerging Threats Open rules

ETOpen is an open source set of Snort rules whose coverage is more limited than ETPro.

Enable ET Pro ☐ Click to enable download of Emerging Threats Pro rules

[Sign Up for an ETPro Account](#)
ETPro for Snort offers daily updates and extensive coverage of current malware threats.

Sourcefire OpenAppID Detectors

Enable OpenAppID ☐ Click to enable download of Sourcefire OpenAppID Detectors

The OpenAppID package contains the application signatures required by the AppID preprocessor.

OpenAppID Version

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Reactivas

Suricata

- Detección y gestión de intrusiones

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Reactivas

Suricata

• Detección y gestión de intrusiones

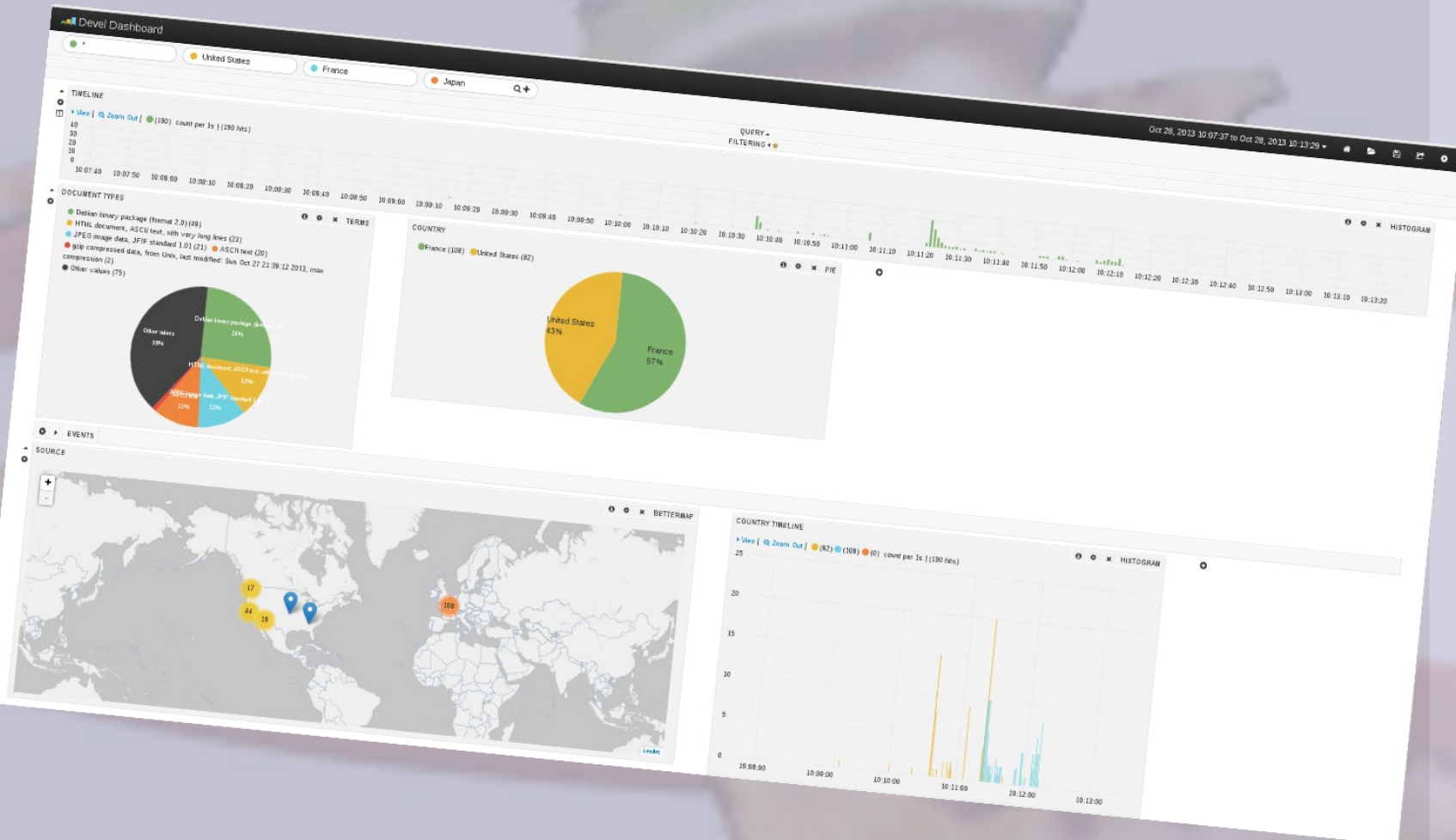
Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Reactivas

Wazuh

• Detección y gestión de intrusiones

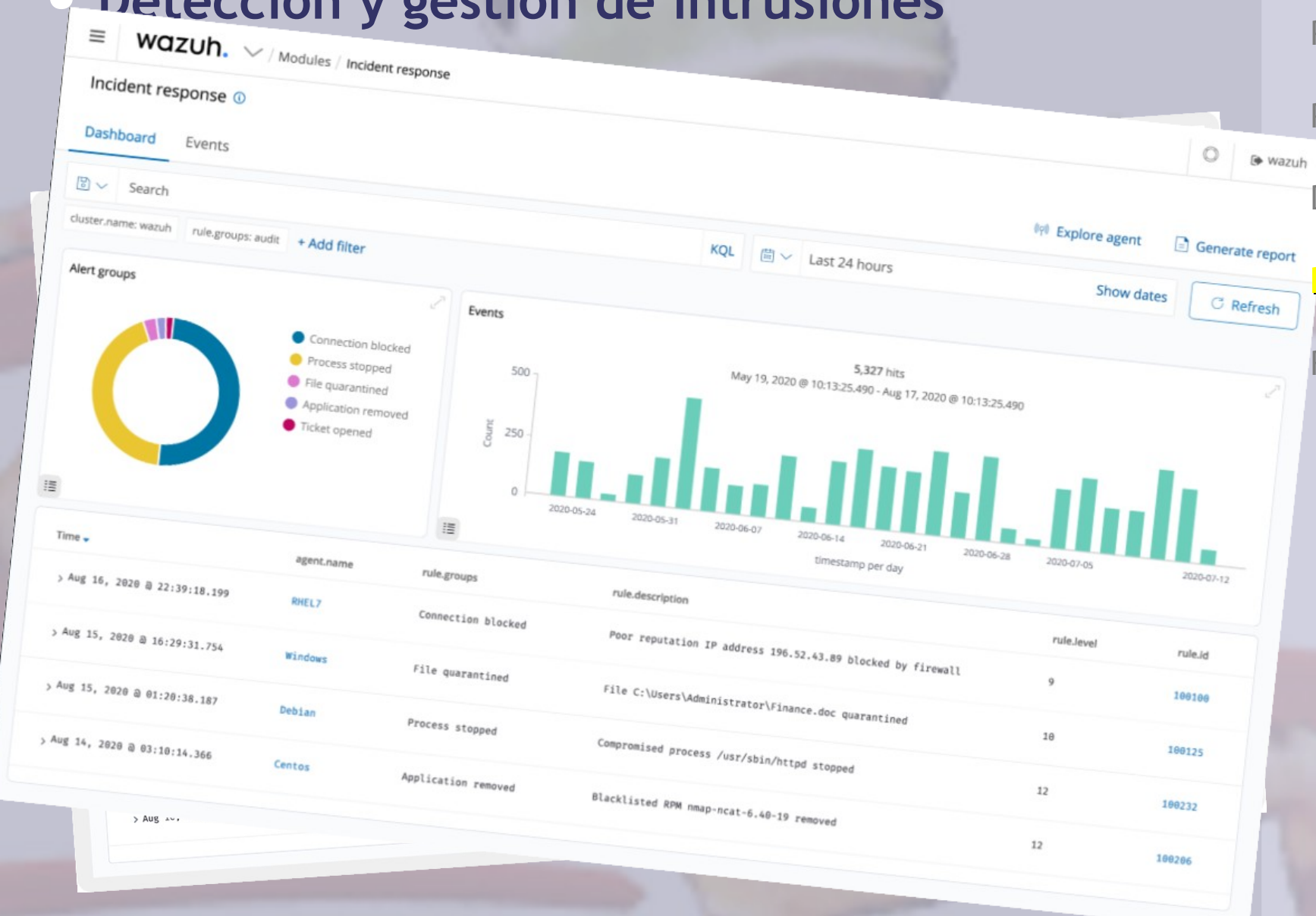
Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Reactivas

Security onion

- Distribución de linux

- Diseñada para

- caza de am

-

-

-

-

-

-

-

-

-

-

-

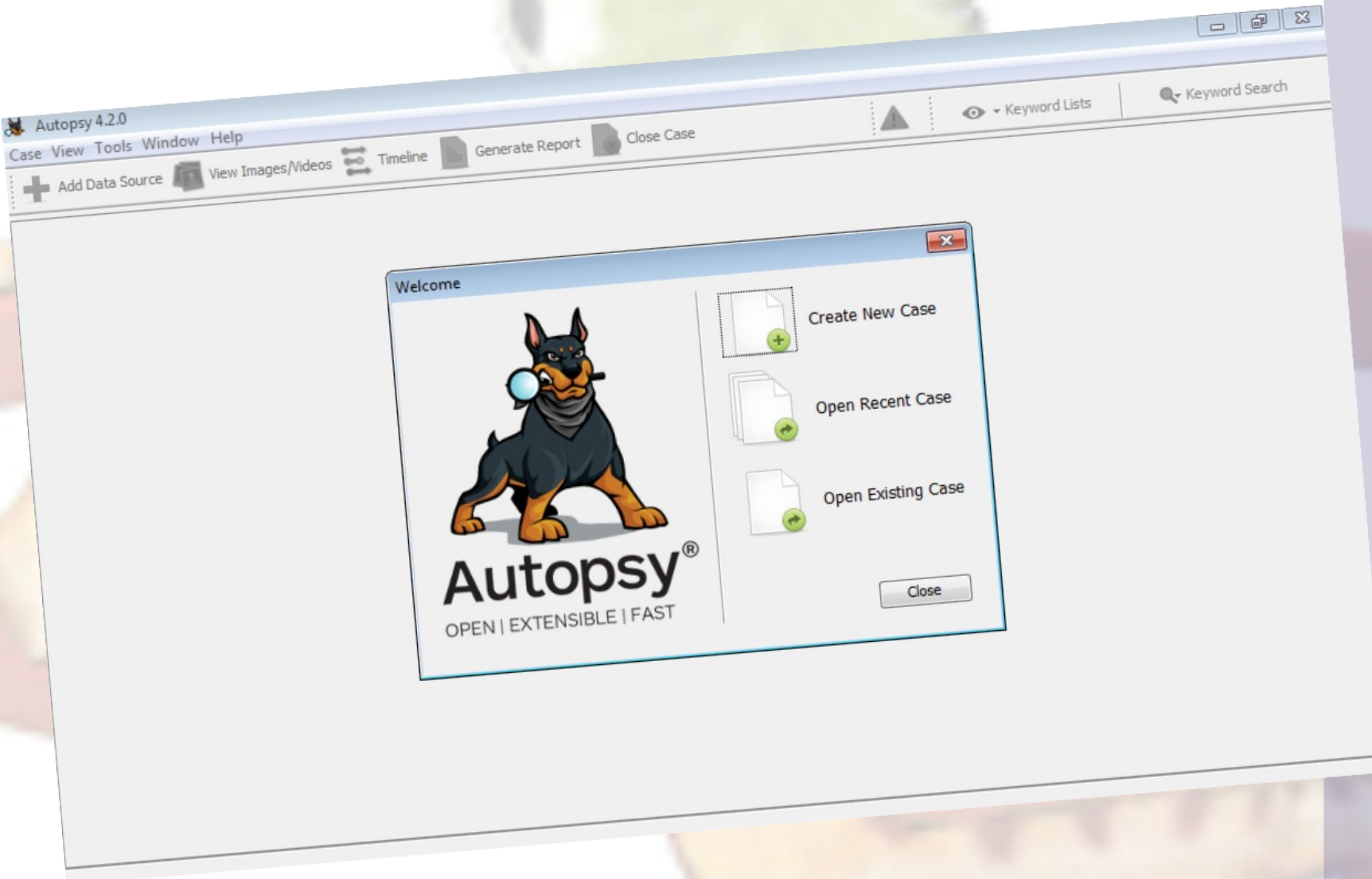


- Suricata...

Reactivas



AUTOPSY
DIGITAL FORENSICS



Preparativas

Preventivas

Detectivas

Reactivas

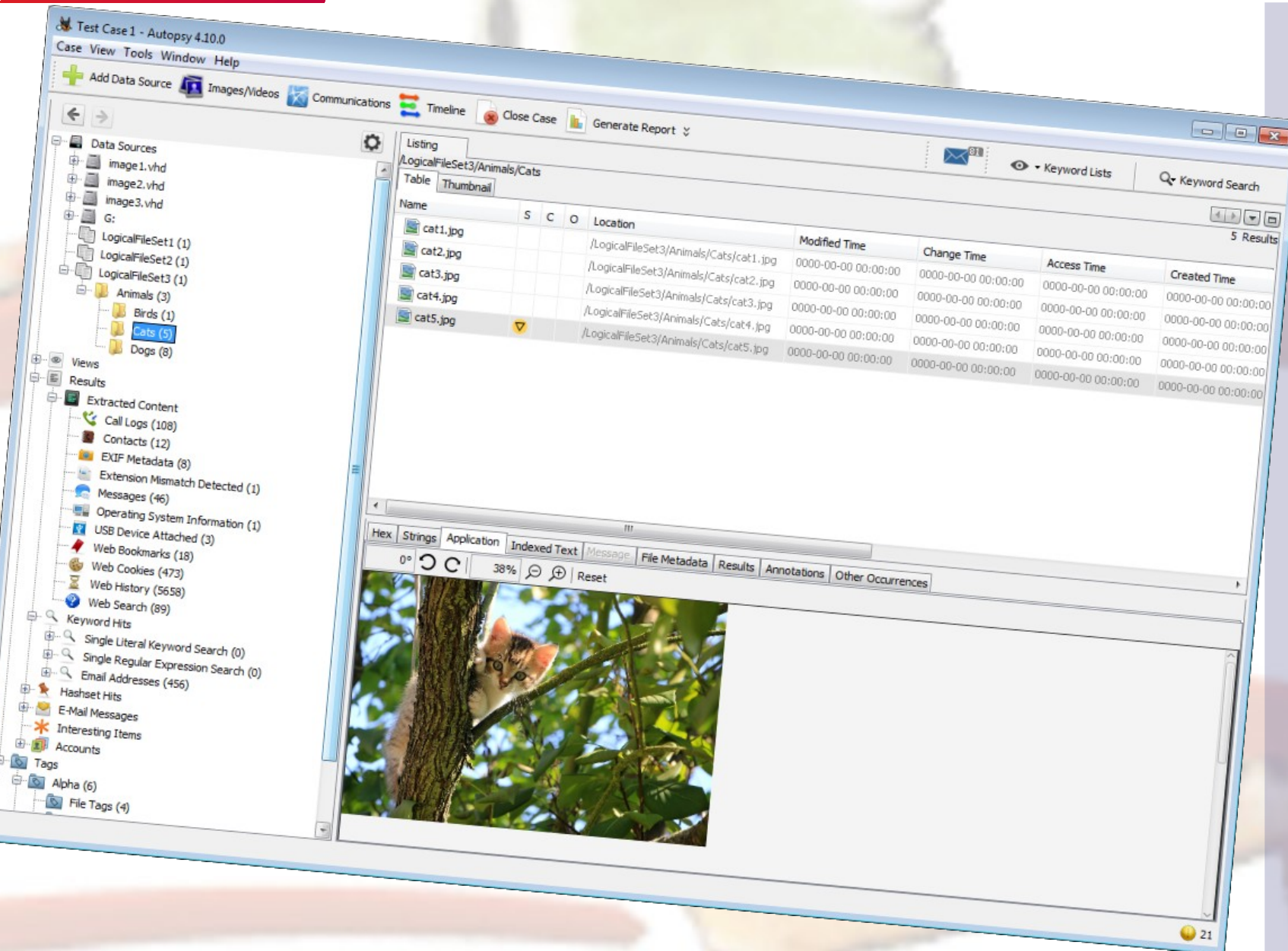
Retrospectivas



Reactivas



AUTOPSY
DIGITAL FORENSICS



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas





Image File Details

Local Name: images/recuperar.dd

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- ☐ Ignore the hash value for this image.
- ☒ Calculate the hash value for this image.
- ☐ Add the following MD5 hash value for this image:

☐ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: fat16)

Mount Point: C:

File System Type:

ADD

CANCEL

HELP

Preparativas

Preventivas

Detectivas

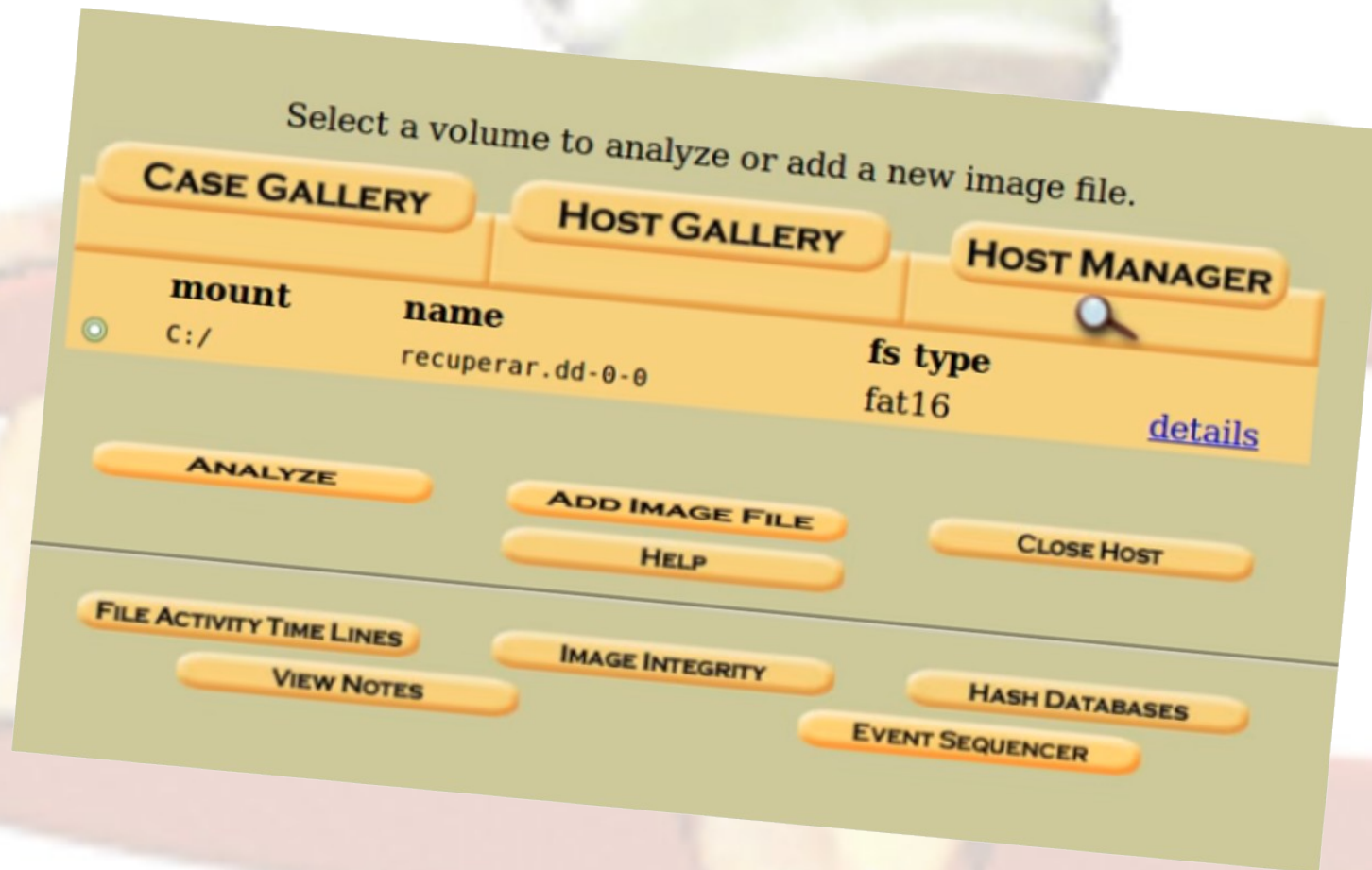
Reactivas

Retrospectivas

Reactivas



AUTOPSY
DIGITAL FORENSICS



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Reactivas



AUTOPSY

DIGITAL FORENSICS



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Directory Seek

Enter the name of a directory that you want to view.
C:/

VIEW

File Name Search

Enter a Perl regular expression for the file names you want to find.

SEARCH

File Analysis **Keyword Search** **File Type** **Image Details** **Meta Data** **Data Unit** **Help** **Close**

v / v	\$MBR	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	512	0	0	191619
d / d	\$OrphanFiles/	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0000-00-00 00:00:00 (UTC)	0	0	0	191622
✓ r / r	ing.dat	2004-02-14 12:52:11 (COT)	2004-02-14 00:00:00 (COT)	2004-02-14 12:52:09 (COT)	780	0	0	6
✓ d / d	irl/	2004-02-14 12:53:47 (COT)	2004-02-14 00:00:00 (COT)	2004-02-14 12:53:46 (COT)	1024	0	0	8
✓ r / r	rag1.dat	2004-02-14 12:51:21 (COT)	2004-02-14 00:00:00 (COT)	2004-02-14 12:50:53 (COT)	1584	0	0	4
✓ r / r	rag2.dat	2004-02-14	2004-02-14	2004-02-14	3873	0	0	5

File Browsing Mode

In this mode, you can view file and directory contents.

File contents will be shown in this window.

More file details can be found using the Metadata link at the end of the list (on the right).

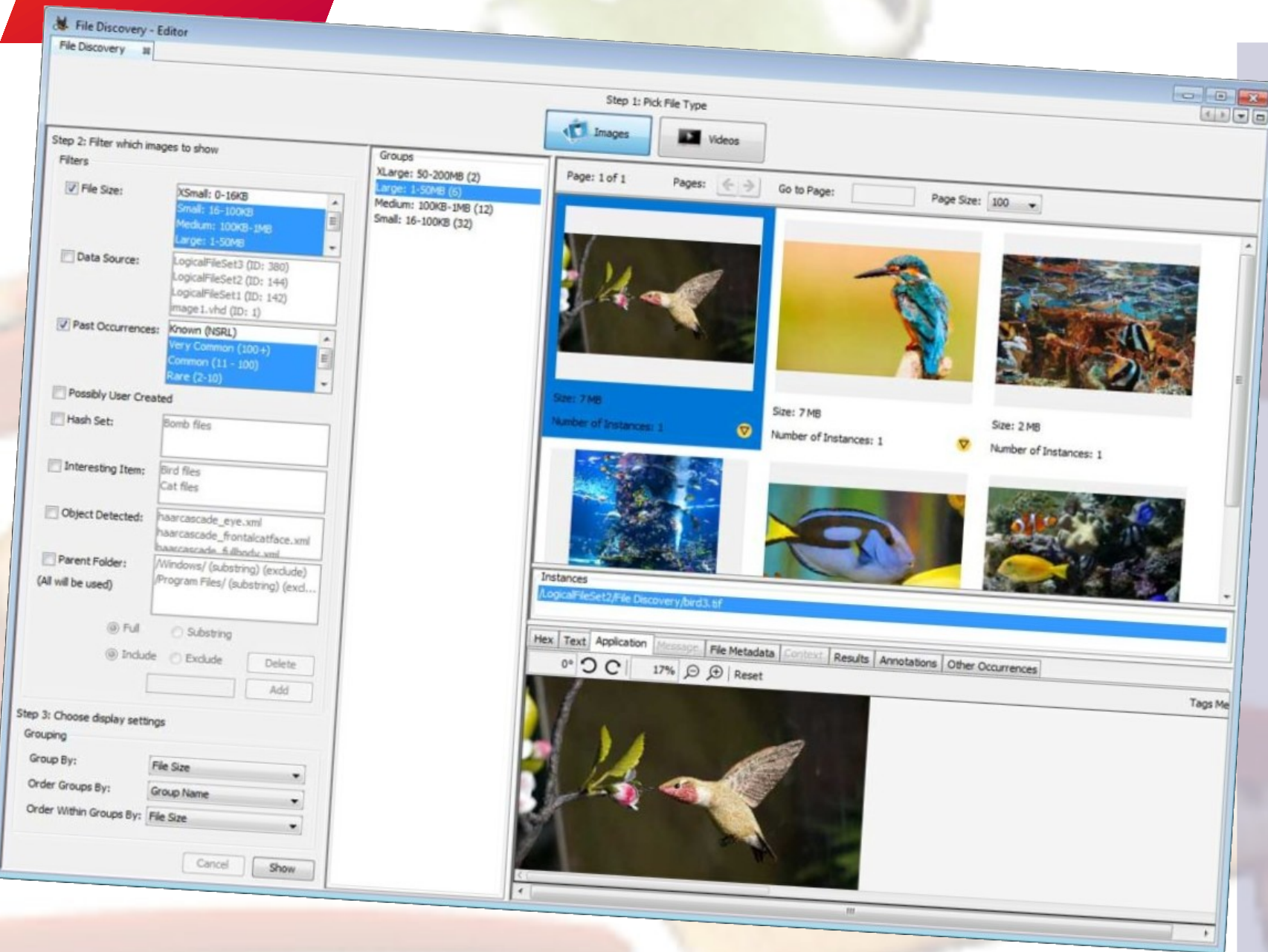
You can also sort the files using the column headers



Reactivas



AUTOPSY
DIGITAL FORENSICS



Preparativas

Preventivas

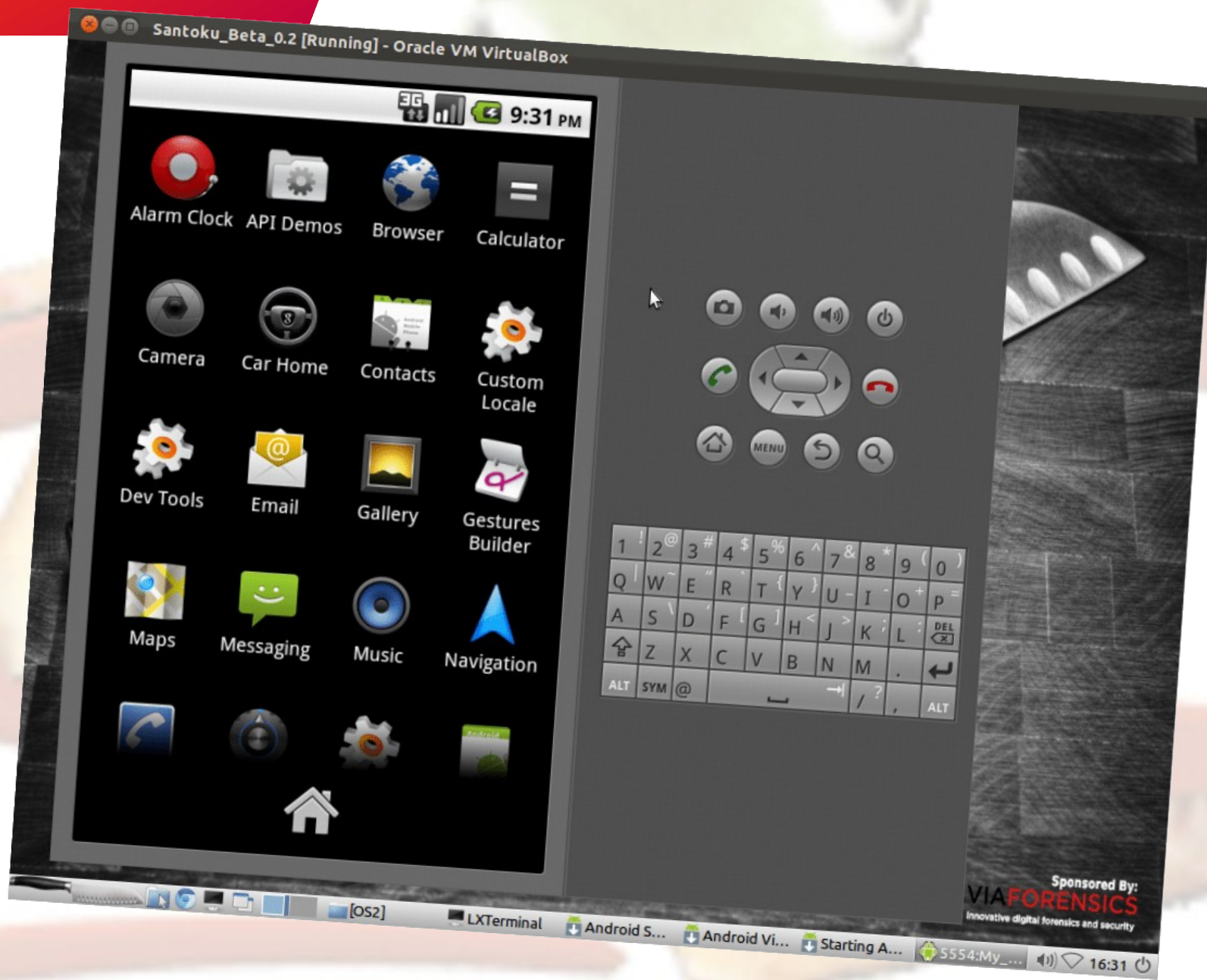
Detectivas

Reactivas

Retrospectivas

Reactivas

Santoku



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Reactivas

Santoku



Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas

Actividades



Retrospectivas

- Medir desempeño
- Analizar causas y consc.
- Aprender
- Revisar incidentes
- Retroalimentar
- Afinar
- Mejorar
- Reportar

- Evolucionar para incrementar la capacidad de:
 - Prevención
 - Detección
 - Reacción
- Reuniones post-incidente
- Informática forense para análisis de incidentes
- Medición de resultados
- Ajuste de políticas y controles
- Comunicación de informes y reportes y publicación de alertas

Preparativas

Preventivas

Detectivas

Reactivas

Retrospectivas



Descargue la presentación aquí

Muchas Gracias

¿Preguntas?

ventas@skinait.com

<http://www.skinait.com>

Software libre para proteger los activos de información por **Ricardo Naranjo Faccini** se distribuye bajo una Licencia Creative Commons Atribución 4.0 Internacional.

Basada en los artículos:

<https://www.skinait.com/como-proteger-los-activos-de-informacion-Escritos-71/> y

<https://www.skinait.com/software-libre-para-ciberseguridad-Escritos-53/>.

