Montevideo deTodos

Metodologías y herramientas para el análisis de vulnerabilidades

María Eugenia Corti
Luis Garcimartin
Carlos García

Montevideo deTodos

¿Para qué?

Para garantizar la seguridad de nuestros sistemas.

Para analizar la exposición de nuestros servicios y sistemas en configuración de producción

Montevideo deTodos

Nuestro camino

- Estudio de estándares y técnicas
- Ensayos
- Adaptación a nuestra organización de los estándares existentes
- Aprobación por parte de la División TI
- Selección de herramientas
- Planificación y coordinación de pruebas
- Ejecución

Nuestro camino

- Estudio de estándares y técnicas
- Ensayos

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ISSAF
Information Systems Security Assessment Framework
www.oissg.org

OSSTMM v 2.2

- **Versión disponible al público hasta Diciembre 2010, publicada en 2006**
- **En proceso de incorporación de cambios a la 3.0**

ISSAF (2006)

Este framework es una buena guía práctica pero no provee un enfoque metodológico general para un entorno empresarial.

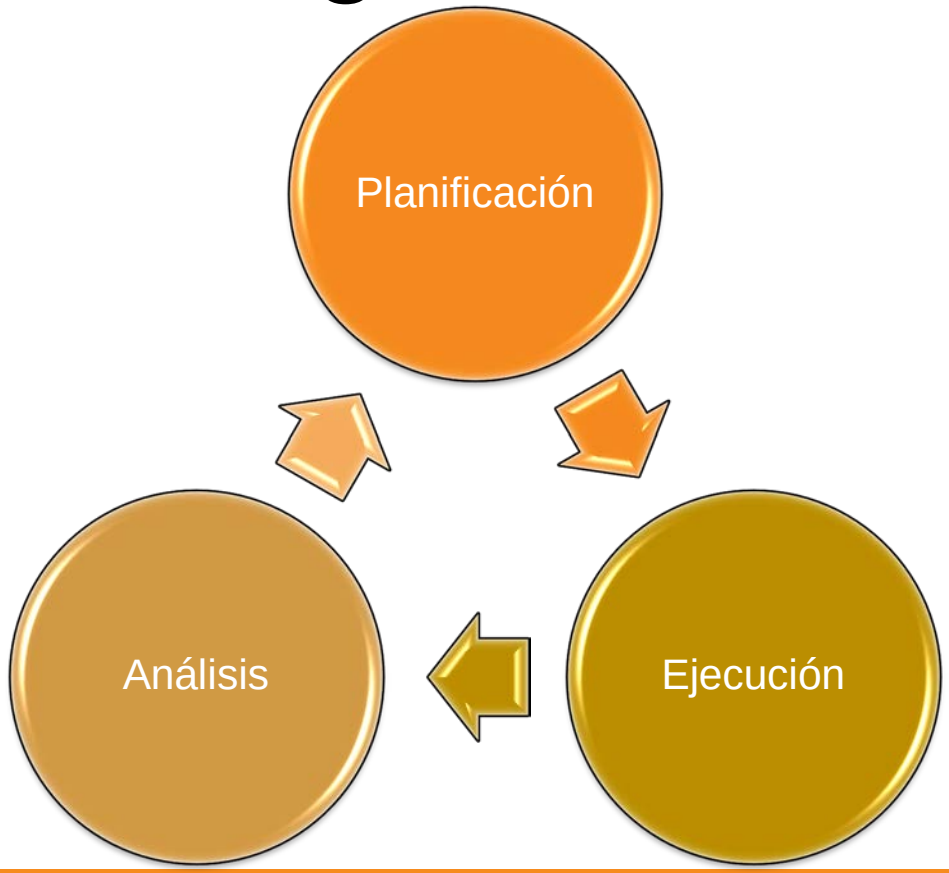
Montevideo deTodos

NIST SP 800-115

NIST National Institute of Standards and Technology U.S. Department of Commerce

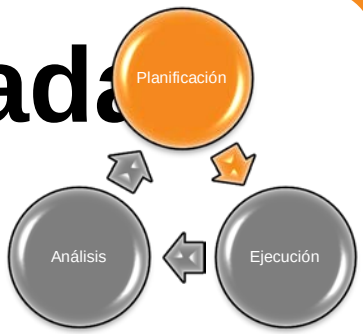
- Publicada e
- Por su orig ones medianas a
- Alto nivel d
- Tiene en cu os
- Presta espe garantizan la continuida es inesperadas ruebas

Metodología desarrollada



Montevideo deTodos

Metodología desarrollada



- Planificación
  - Condiciones previas
    - Acuerdos de confidencialidad
    - Objetivos y alcance
    - Niveles de riesgo aceptables
  - Prioridad y planificación de los Análisis
    - Que sistemas analizar y en que orden
    - Requerimientos legales, periodicidad, criticidad

Montevideo deTodos

Metodología desarrollada

- Planificación
  - Selección y adaptación de Técnicas
    - Auditoria interna o externa, a ciegas o no
    - Riesgos asociados a las técnicas versus el nivel de riesgo aceptable
    - Tiempo disponible
    - Posibles impactos
  - Logística
    - Obtener con los recursos para la prueba
    - Disponibilidad del apoyo de otros técnicos
    - Selección del equipo humano

Montevideo deTodos

Metodología desarrollada

- Planificación
  - Plan de trabajo
    - Se generan formularios detallados
    - Se elevan al CGC
    - Se recaba la autorización

Auditores

Nombre	Funcionario	Acuerdo de Confidencialidad

Análisis

Objetivo	Descripción:
	Analizar la exposición a Internet de la orga… …mara como insumo la informa…
Prioridad	Alta
Escenario	Tipo
Externo	Test de penetración

Requerimientos de la organización

Días autorizados	todos
Horario	0-11 hs 16-24 hs
Otros	

Logística

Hardware	disponibilidad
CPU con herramientas instaladas	
Modem 3g	
ADSL dedicado	

Ubicación Física
Oficinas Área Seguridad de la Información

Plan de trabajo

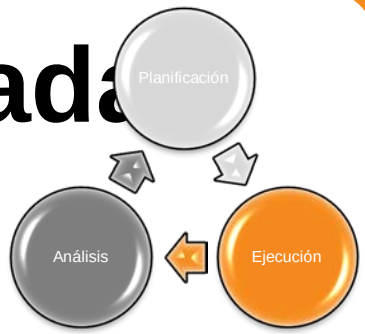
Paso	Técnica	Herramienta	Descripción
1	Planificación		En base a la información recopilara se ajustara el pr…
2	DNS	metaexploit	Se intentara explotar los servicios DNS
3	WWW	metaexploit	Se intentara explotar los servicios de publicación web
4	WWW	Pharos Proxy	Se intentara explotar los servicios de publicación web
5	Servidor de aplicaciones	metaexploit	Se intentara explotar los servidores de aplicaciones
6	Ataque a servicios específicos	Varias	Se intentan explotar servicios específicos descubiert…
7	Explotación manual	Varias	Verificación manual de las posibles vulnerabilidades
8			Análisis de las posibles vulnerabilidades detectadas
9			Informes

Riesgo

El riesgo de provocar una perdida de disponibilidad en los sistemas segun el plan presentado es alto.

Montevideo deTodos

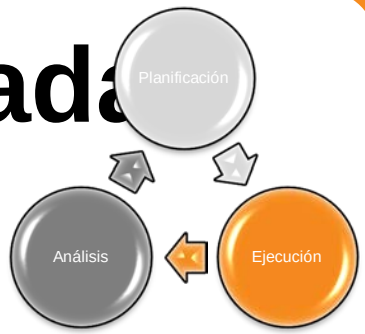
Metodología desarrollada



- Ejecución
  - Coordinación y ejecución
    - Se establece la oportunidad de la prueba
    - Se establecen reglas para la ejecución, como por ejemplo el registro detallado de las pruebas, la rigidez del plan
    - Se tienen en cuenta también, los desafíos que puede implicar la falta de realismo, la resistencia de los actores y el impacto operacional.
    - Nuestro enfoque fue lograr que los actores percibieran el valor de estas pruebas e integrarlos al proceso

Montevideo deTodos

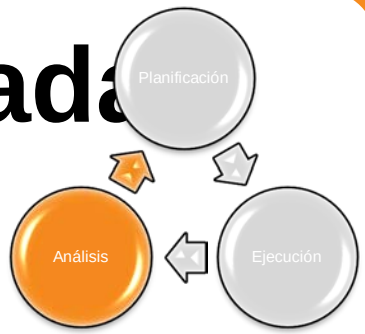
Metodología desarrollada



- Ejecución
  - Manejo de la información
    - Almacenamiento, transmisión de la información
  - Identificación de falsos positivos

Montevideo deTodos

Metodología desarrollada



- **Análisis**
  - **Categorización de vulnerabilidades**
  - **Análisis de las causas subyacentes por las que se generaron estas vulnerabilidades**
  - **Reportes**
    - **Registro escrito detallado**
    - **Presentación**
    - **Informe escrito ejecutivo**

[redacted]				[redacted]
	Puerto	Prot	Desc	Observación
	123	UDP	NTP	Network Time Protocol (NTP) Server Detection
			ICMP	ICMP Timestamp Request Remote Date Disclosure
	500	UDP	IKE	IPSEC Internet Key Exchange (IKE) Detection

Montevideo deTodos

Herramientas para el análisis de vulnerabilidades

Recolección de Información

Identificación de red, puertos y servicios

Análisis de Vulnerabilidades

Análisis de información pública

Montevideo deTodos

Recolección de Información

Obtener información acerca de : IPs públicas, propiedad del dominio, DNSs, hosts, reversos, forwards.

- http://www.robtex.com/
- http://www.ip-adress.com/whois/

Recolección de Información

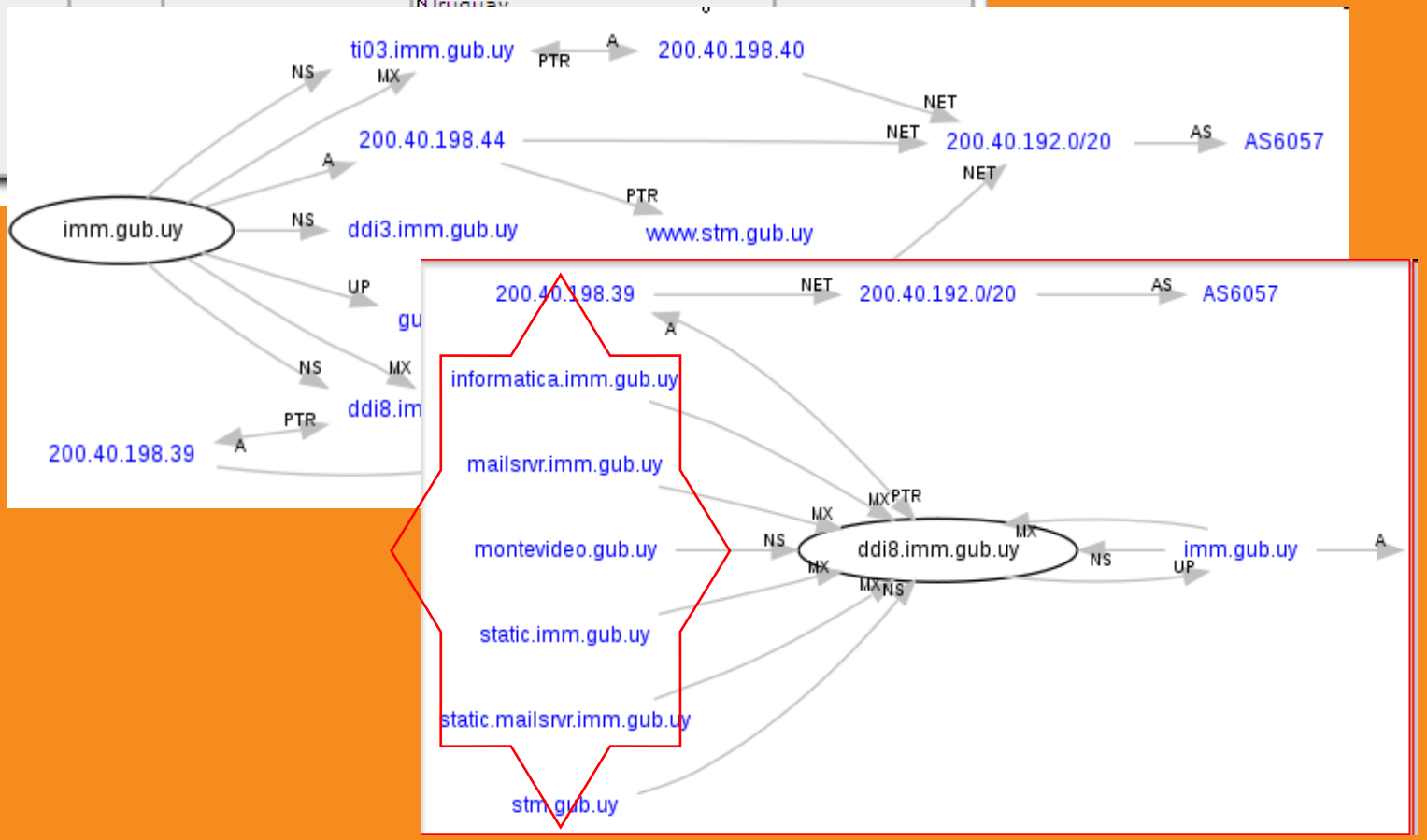
Identificación de red, puertos y servicios

Análisis de Vulnerabilidades

Análisis de información pública

robtex

Base	Record	Name	IP	Reverse	Route
www.imm.gub.uy	a		200.40.198.44 Uruguay	www.imm.gub.uy	200.40.192.0/20
imm.gub.uy	a		200.40.198.44 Uruguay	www.imm.gub.uy	
	ns-soa	ddi3.imm.gub.uy		(none)	
	ns	ddi3.imm.gub.uy		(none)	
		ddi8.imm.gub.uy	200.40.198.39		200.40.192.0/20



Recolección de Información

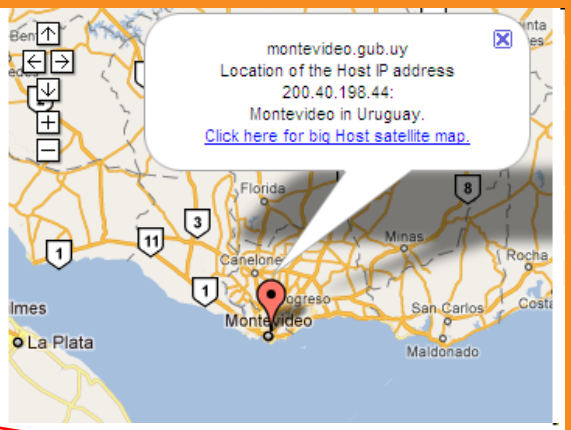
Identificación de red, puertos y servicios

Análisis de Vulnerabilidades

Análisis de información pública

ip-adress

montevideo.gub.uy IP address location & more:	
Host of the IP:	montevideo.gub.uy[Whois] [Reverse IP]
Host IP [?]:	200.40.198.44 [Whois] [Reverse IP]
IP country code:	UY
IP address country:	Uruguay
IP address state:	Montevideo
IP address city:	Montevideo
IP address latitude:	-34.8581
IP address longitude:	-56.1708
ISP of this IP [?]:	Administracion Nacional de Telecomunicaciones
Organization:	Servicio Internet Class
Local time in Uruguay:	2011-08-12 15:47



8 Hosts on this IP

Number	Domain / Host	Functions
1.	www.montevideo.gub.uy	[Whois]
2.	www.contribucion.montevideo.gub.uy:8081	[Whois]
3.	www.mecopa.montevideo.gub.uy	[Whois]
4.	cultura.montevideo.gub.uy	[Whois]
5.	agenda.montevideo.gub.uy	[Whois]
6.	sig.montevideo.gub.uy	[Whois]
7.	www.imm.gub.uy	[Whois]
8.	fotograma.montevideo.gub.uy	[Whois]

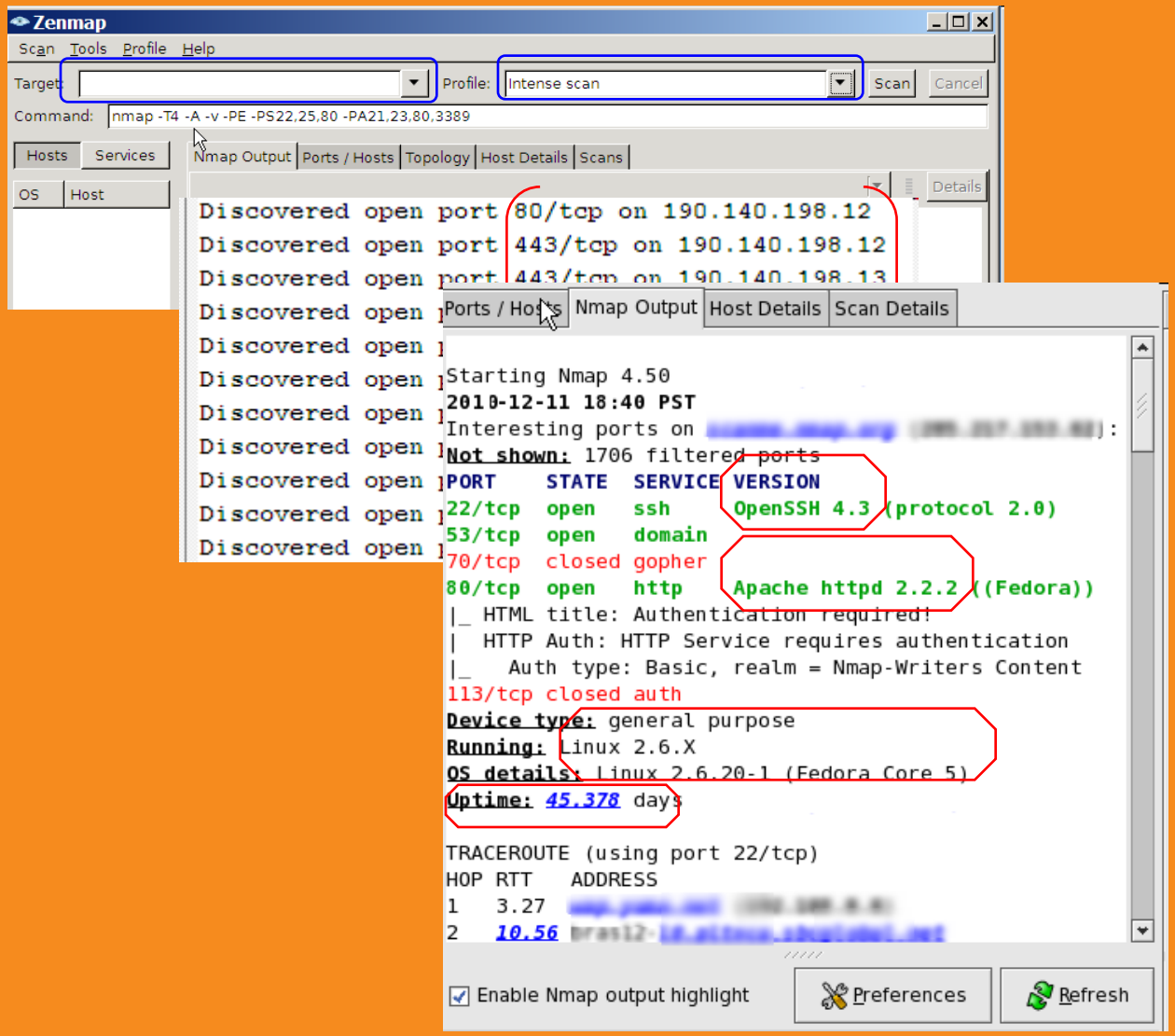
Montevideo deTodos

Identificación de red, puertos y servicios

"Scaneo" de puertos/servicios a los efectos de obtener información de sistemas operativos, servicios, versiones.

- Zenmap : official Nmap Security Scanner GUI

Zenmap

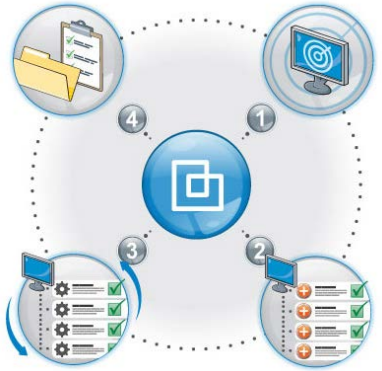

Zenmap
Scan Tools Profile Help
Target:
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389
Hosts
Services
OS
Host
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Details
Discovered open port 80/tcp on 190.140.198.12
Discovered open port 443/tcp on 190.140.198.12
Discovered open port 443/tcp on 190.140.198.13
Ports / Hosts
Nmap Output
Host Details
Scan Details
Starting Nmap 4.50
2010-12-11 18:40 PST
Interesting ports on
Not shown: 1706 filtered ports
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 4.3 (protocol 2.0)
53/tcp open domain
70/tcp closed gopher
80/tcp open http Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Authentication required!
| HTTP Auth: HTTP Service requires authentication
|_ Auth type: Basic, realm = Nmap-Writers Content
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 45.378 days
TRACEROUTE (using port 22/tcp)
HOP RTT ADDRESS
1 3.27
2 10.56
Enable Nmap output highlight
Preferences
Refresh

Montevideo deTodos

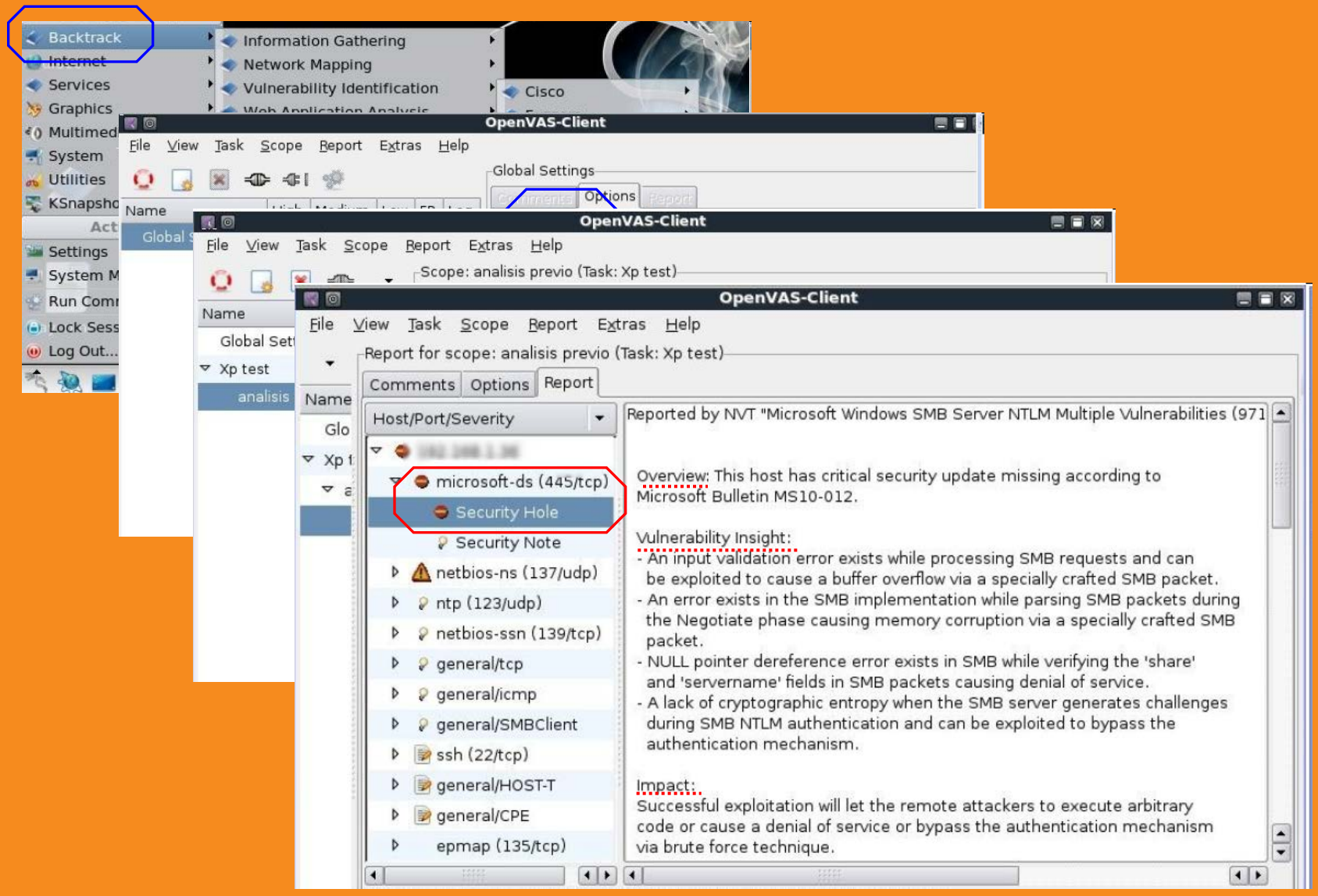
Análisis de vulnerabilidad

Búsqueda de servicios/aplicaciones expuestas a vulnerabilidades conocidas.

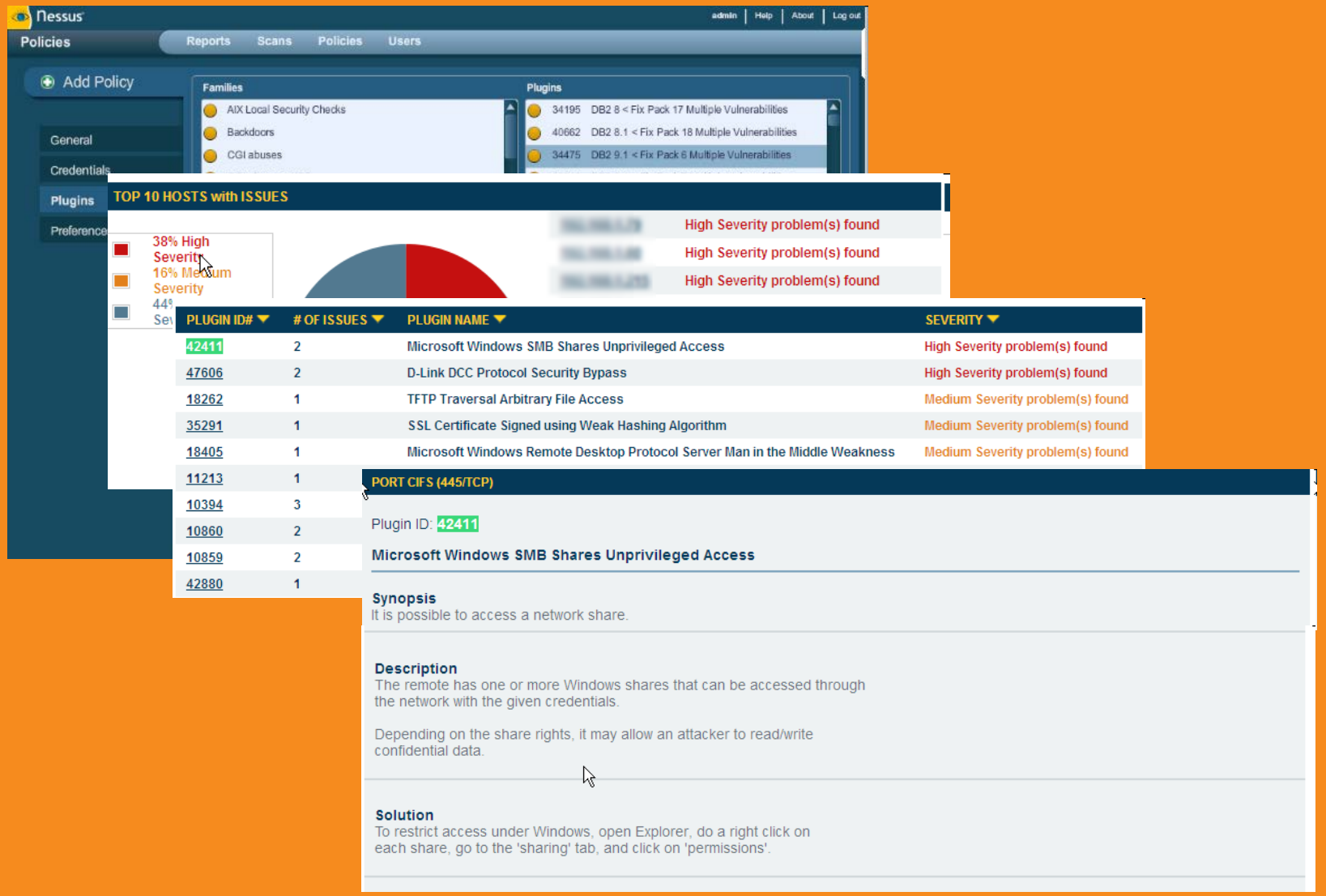
- OpenVas
- Nessus



OpenVas


Backtrack
Information Gathering
Network Mapping
Vulnerability Identification
Cisco
Services
Graphics
System
Utilities
Settings
Run Comm
Lock Sess
Log Out...
OpenVAS-Client
File View Task Scope Report Extras Help
Global Settings
Options
Scope: analisis previo (Task: Xp test)
Xp test
analisis
Report for scope: analisis previo (Task: Xp test)
Comments Options Report
Host/Port/Severity
microsoft-ds (445/tcp)
Security Hole
Security Note
netbios-ns (137/udp)
ntp (123/udp)
netbios-ssn (139/tcp)
general/tcp
general/icmp
general/SMBClient
ssh (22/tcp)
general/HOST-T
general/CPE
epmap (135/tcp)
Reported by NVT "Microsoft Windows SMB Server NTLM Multiple Vulnerabilities (971
Overview: This host has critical security update missing according to Microsoft Bulletin MS10-012.
Vulnerability Insight:
- An input validation error exists while processing SMB requests and can be exploited to cause a buffer overflow via a specially crafted SMB packet.
- An error exists in the SMB implementation while parsing SMB packets during the Negotiate phase causing memory corruption via a specially crafted SMB packet.
- NULL pointer dereference error exists in SMB while verifying the 'share' and 'servername' fields in SMB packets causing denial of service.
- A lack of cryptographic entropy when the SMB server generates challenges during SMB NTLM authentication and can be exploited to bypass the authentication mechanism.
Impact:
Successful exploitation will let the remote attackers to execute arbitrary code or cause a denial of service or bypass the authentication mechanism via brute force technique.

Nessus


Nessus
admin | Help | About | Log out
Policies
Reports Scans Policies Users
Add Policy
General
Credentials
Plugins
Preferences
Families
AIX Local Security Checks
Backdoors
CGI abuses
Plugins
34195 DB2 8 < Fix Pack 17 Multiple Vulnerabilities
40662 DB2 8.1 < Fix Pack 18 Multiple Vulnerabilities
34475 DB2 9.1 < Fix Pack 6 Multiple Vulnerabilities
TOP 10 HOSTS with ISSUES
38% High Severity
16% Medium Severity
High Severity problem(s) found
High Severity problem(s) found
High Severity problem(s) found
PLUGIN ID# | # OF ISSUES | PLUGIN NAME | SEVERITY
42411 | 2 | Microsoft Windows SMB Shares Unprivileged Access | High Severity problem(s) found
47606 | 2 | D-Link DCC Protocol Security Bypass | High Severity problem(s) found
18262 | 1 | TFTP Traversal Arbitrary File Access | Medium Severity problem(s) found
35291 | 1 | SSL Certificate Signed using Weak Hashing Algorithm | Medium Severity problem(s) found
18405 | 1 | Microsoft Windows Remote Desktop Protocol Server Man in the Middle Weakness | Medium Severity problem(s) found
11213 | 1
10394 | 3
10860 | 2
10859 | 2
42880 | 1
PORT CIFS (445/TCP)
Plugin ID: 42411
Microsoft Windows SMB Shares Unprivileged Access
Synopsis
It is possible to access a network share.
Description
The remote has one or more Windows shares that can be accessed through the network with the given credentials.
Depending on the share rights, it may allow an attacker to read/write confidential data.
Solution
To restrict access under Windows, open Explorer, do a right click on each share, go to the 'sharing' tab, and click on 'permissions'.

Pruebas Manuales

XSS (Cross-site scripting).
Inserción de comandos.
Alteración de parámetros de entrada.
SQLi (Inyección SQL).
Suplantación de identidad

- Validación de vulnerabilidades identificadas en pruebas automáticas (falsos-positivos).
- Pruebas específicas sobre aplicaciones propias.

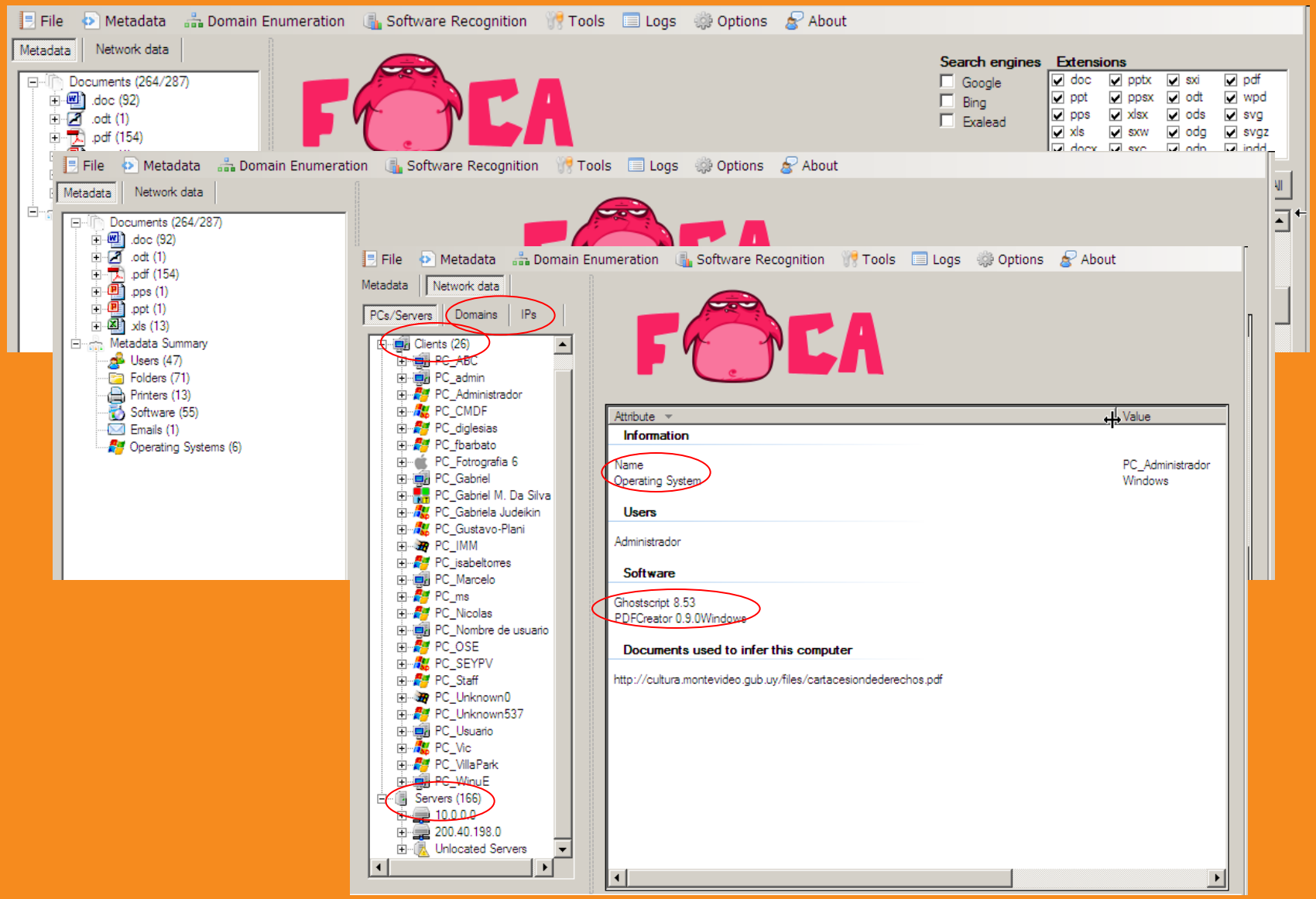
Montevideo deTodos

Análisis de información pública

- Foca : búsqueda de Metadatos e información oculta en documentos de Office, OpenOffice, PDF

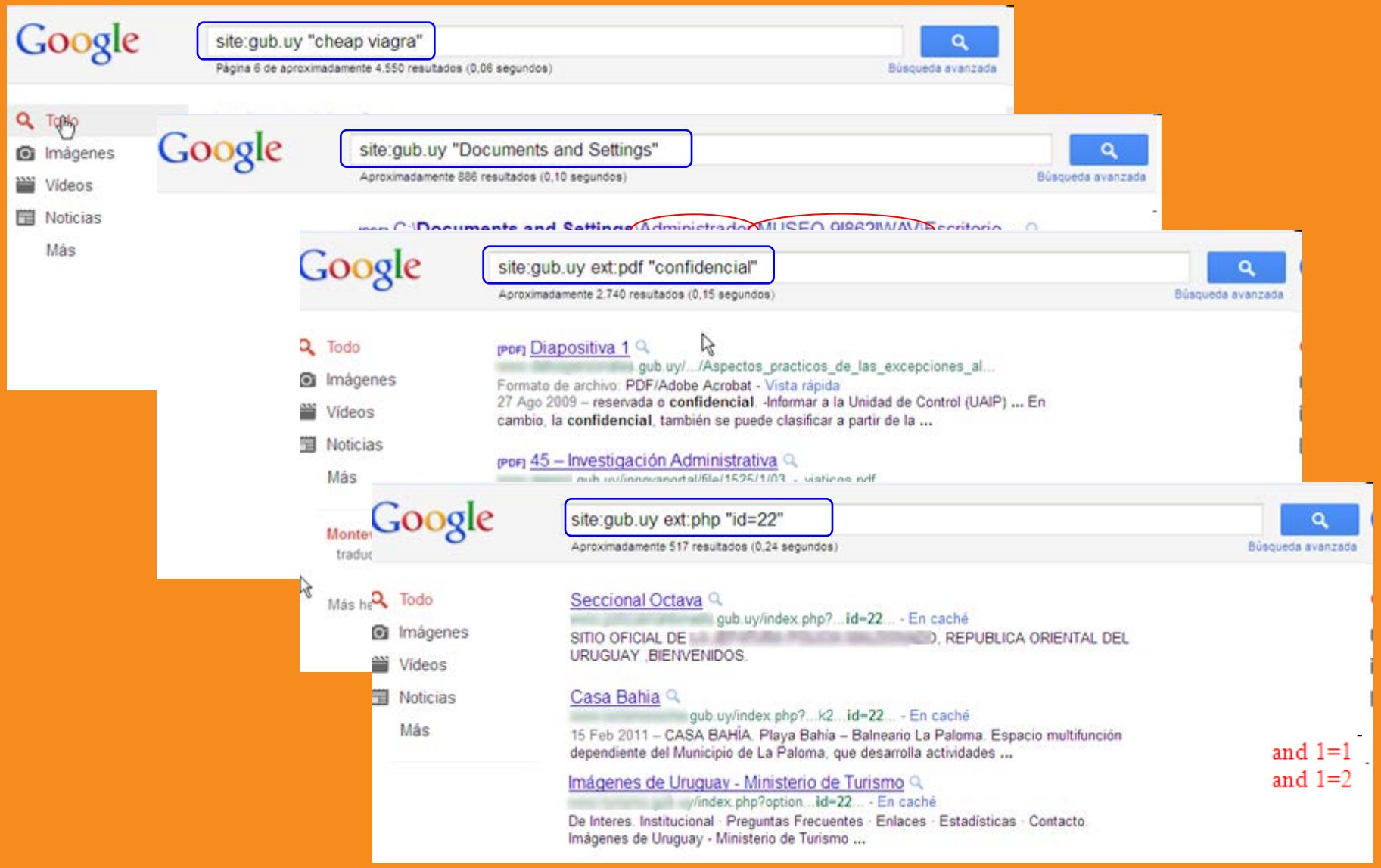
- Google hacking

Foca


File
Metadata
Domain Enumeration
Software Recognition
Tools
Logs
Options
About
Metadata
Network data
Documents (264/287)
.doc (92)
.odt (1)
.pdf (154)
.pps (1)
.ppt (1)
.xls (13)
Metadata Summary
Users (47)
Folders (71)
Printers (13)
Software (55)
Emails (1)
Operating Systems (6)
PCs/Servers
Domains
IPs
Clients (26)
PC_ABC
PC_admin
PC_Administrador
PC_CMDF
PC_diglesias
PC_fbarbato
PC_Fotrografia 6
PC_Gabriel
PC_Gabriel M. Da Silva
PC_Gabriela Judeikin
PC_Gustavo-Plani
PC_IMM
PC_isabeltorres
PC_Marcelo
PC_ms
PC_Nicolas
PC_Nombre de usuario
PC_OSE
PC_SEYPV
PC_Staff
PC_Unknown0
PC_Unknown537
PC_Usuario
PC_Vic
PC_VillaPark
PC_WinuE
Servers (166)
10.0.0.0
200.40.198.0
Unlocated Servers
Search engines
Google
Bing
Exalead
Extensions
doc
pptx
sxi
pdf
ppt
ppsx
odt
wpd
pps
xlsx
ods
svg
xls
sxw
odg
svgz
Attribute
Value
Information
Name
PC_Administrador
Operating System
Windows
Users
Administrador
Software
Ghostscript 8.53
PDFCreator 0.9.0Windows
Documents used to infer this computer
http://cultura.montevideo.gub.uy/files/cartacesiondederechos.pdf

Google hacking

Técnica de reconocimiento pasivo que utiliza los servicios de filtrado de búsqueda.



Montevideo deTodos

Seguridad en Aplicaciones

Test de seguridad en Aplicaciones

Auditoría de Aplicaciones

Revisión de Código

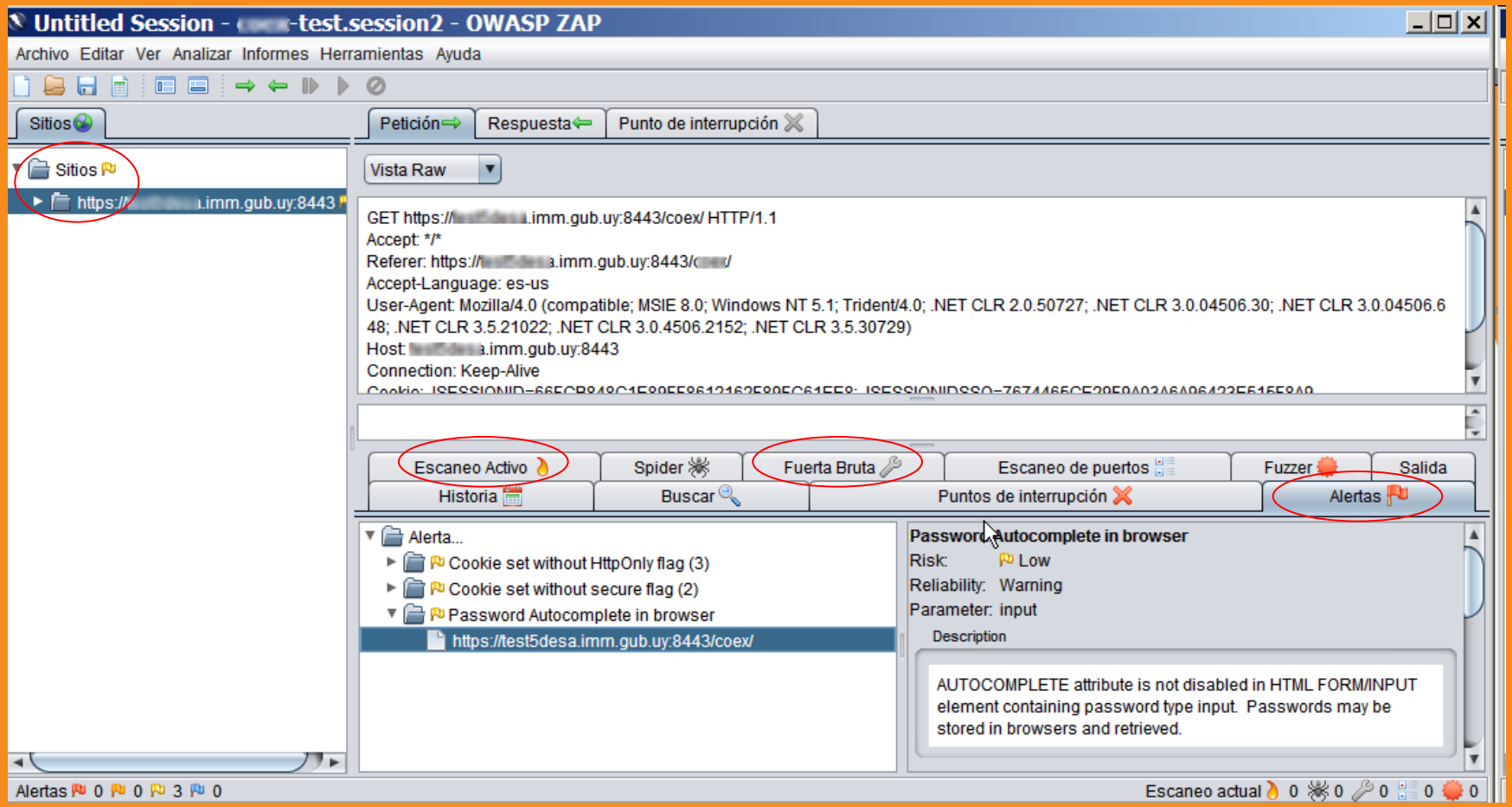
Montevideo deTodos

Test de seguridad en Aplicaciones

- OWASP ZAP : herramienta para búsqueda de vulnerabilidades en aplicaciones web.

OWASP ZAP
Version 1.3.1

OWASP ZAP

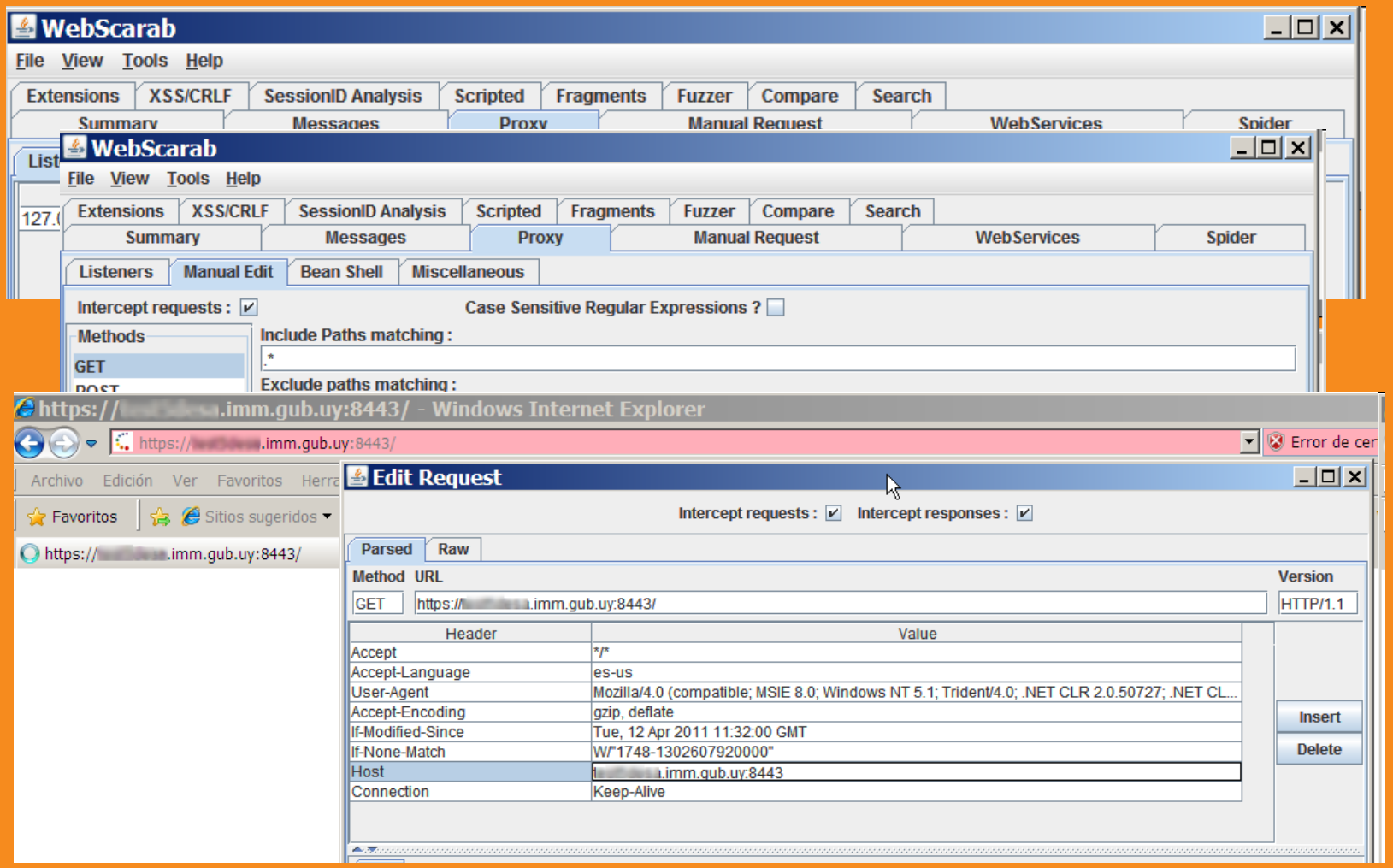

Untitled Session - -test.session2 - OWASP ZAP
Archivo Editar Ver Analizar Informes Herramientas Ayuda
Sitios
Petición
Respuesta
Punto de interrupción
Sitios
https:// .imm.gub.uy:8443
Vista Raw
GET https:// .imm.gub.uy:8443/coex/ HTTP/1.1
Accept: */*
Referer: https:// .imm.gub.uy:8443/ /
Accept-Language: es-us
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: .imm.gub.uy:8443
Connection: Keep-Alive
Escaneo Activo
Spider
Fuerta Bruta
Escaneo de puertos
Fuzzer
Salida
Historia
Buscar
Puntos de interrupción
Alertas
Alerta...
Cookie set without HttpOnly flag (3)
Cookie set without secure flag (2)
Password Autocomplete in browser
https://test5desa.imm.gub.uy:8443/coex/
Password Autocomplete in browser
Risk: Low
Reliability: Warning
Parameter: input
Description
AUTOCOMPLETE attribute is not disabled in HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.
Alertas 0 0 3 0
Escaneo actual 0 0 0 0 0

Montevideo deTodos

Auditoría de Aplicaciones

- OWASP Webscarab - Framework para análisis de aplicaciones bajo protocolos HTTP y HTTPS

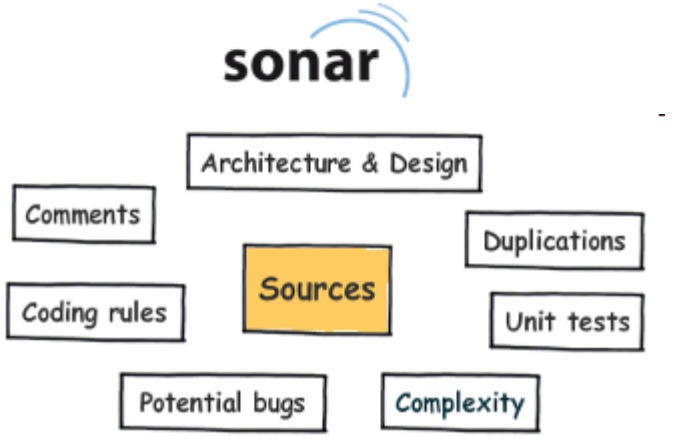
OWASP Webscarab



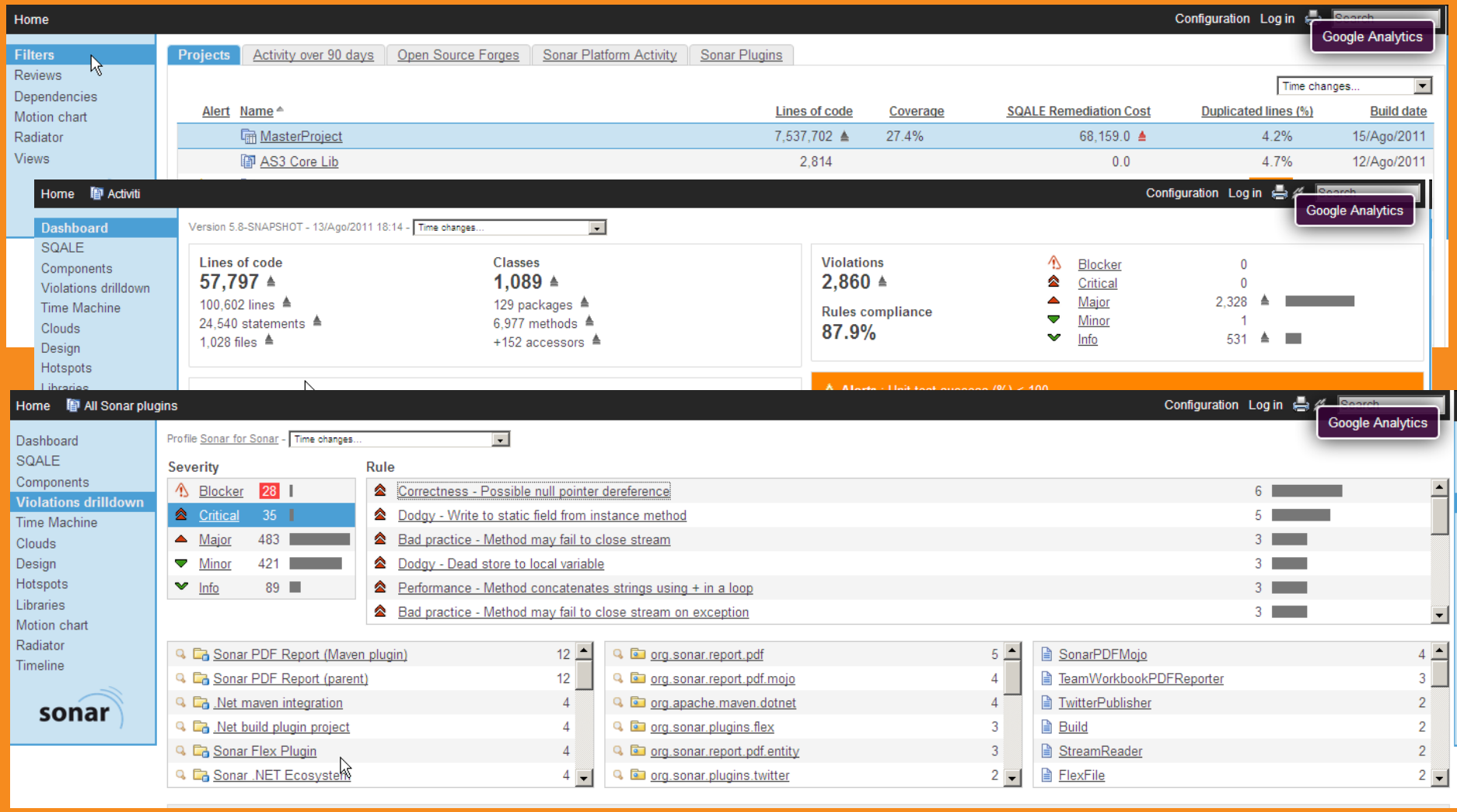
Montevideo deTodos

Revisión de Código

- Sonar : permite gestionar la calidad del código
  (Arquitectura, Diseño, Duplicaciones, Errores potenciales, etc)



Sonar


Home
Configuration
Log in
Google Analytics
Filters
Reviews
Dependencies
Motion chart
Radiator
Views
Projects
Activity over 90 days
Open Source Forges
Sonar Platform Activity
Sonar Plugins
Time changes...
Alert
Name
Lines of code
Coverage
SQALE Remediation Cost
Duplicated lines (%)
Build date
MasterProject
7,537,702
27.4%
68,159.0
4.2%
15/Ago/2011
AS3 Core Lib
2,814
0.0
4.7%
12/Ago/2011
Home
Activiti
Configuration
Log in
Google Analytics
Dashboard
SQALE
Components
Violations drilldown
Time Machine
Clouds
Design
Hotspots
Version 5.8-SNAPSHOT - 13/Ago/2011 18:14 -
Time changes...
Lines of code
57,797
100,602 lines
24,540 statements
1,028 files
Classes
1,089
129 packages
6,977 methods
+152 accessors
Violations
2,860
Rules compliance
87.9%
Blocker 0
Critical 0
Major 2,328
Minor 1
Info 531
Home
All Sonar plugins
Configuration
Log in
Google Analytics
Dashboard
SQALE
Components
Violations drilldown
Time Machine
Clouds
Design
Hotspots
Libraries
Motion chart
Radiator
Timeline
sonar
Profile Sonar for Sonar -
Time changes...
Severity
Blocker 28
Critical 35
Major 483
Minor 421
Info 89
Rule
Correctness - Possible null pointer dereference 6
Dodgy - Write to static field from instance method 5
Bad practice - Method may fail to close stream 3
Dodgy - Dead store to local variable 3
Performance - Method concatenates strings using + in a loop 3
Bad practice - Method may fail to close stream on exception 3
Sonar PDF Report (Maven plugin) 12
Sonar PDF Report (parent) 12
.Net maven integration 4
.Net build plugin project 4
Sonar Flex Plugin 4
Sonar .NET Ecosystem 4
org.sonar.report.pdf 5
org.sonar.report.pdf.mojo 4
org.apache.maven.dotnet 4
org.sonar.plugins.flex 3
org.sonar.report.pdf.entity 3
org.sonar.plugins.twitter 2
SonarPDFMojo 4
TeamWorkbookPDFReporter 3
TwitterPublisher 2
Build 2
StreamReader 2
FlexFile 2

Montevideo deTodos

Conclusiones

- Efectivo. Cumplidos los resultados esperados.
- Implementación sencilla, en tiempos esperados.
- Colaboración de otras áreas en la ejecución.
- Buena recepción y contribución para realizar correcciones.
- Revisión, actualización y corrección de la metodología.

Montevideo deTodos

Gracias !

seguridad.informatica@imm.gub.uy

Montevideo deTodos

Gracias !

seguridad.informatica@imm.gub.uy