

SAINT®

Integrated Vulnerability Management,
Penetration Testing, Compliance, and
Configuration Assessment.



*¿Cuan seguro es seguro?
-Cuales herramientas
necesitas para proteger tu
organización*



Tenacious
Information
Security

¿Que Herramientas necesito?-

- Escaneo de vulnerabilidades
- Pruebas de penetración
- Monitoreo constante
- Control de remediación
- Reportes Analíticos
- Seguridad Móvil

Tipos de pruebas

- **Escaneo de vulnerabilidades**

“Identifica el sistema y especificaciones, a la vez buscando vulnerabilidades conocidas y ofreciendo soluciones para eliminar dichos riesgos.”

- **Pruebas de penetración (“PEN testing”)**

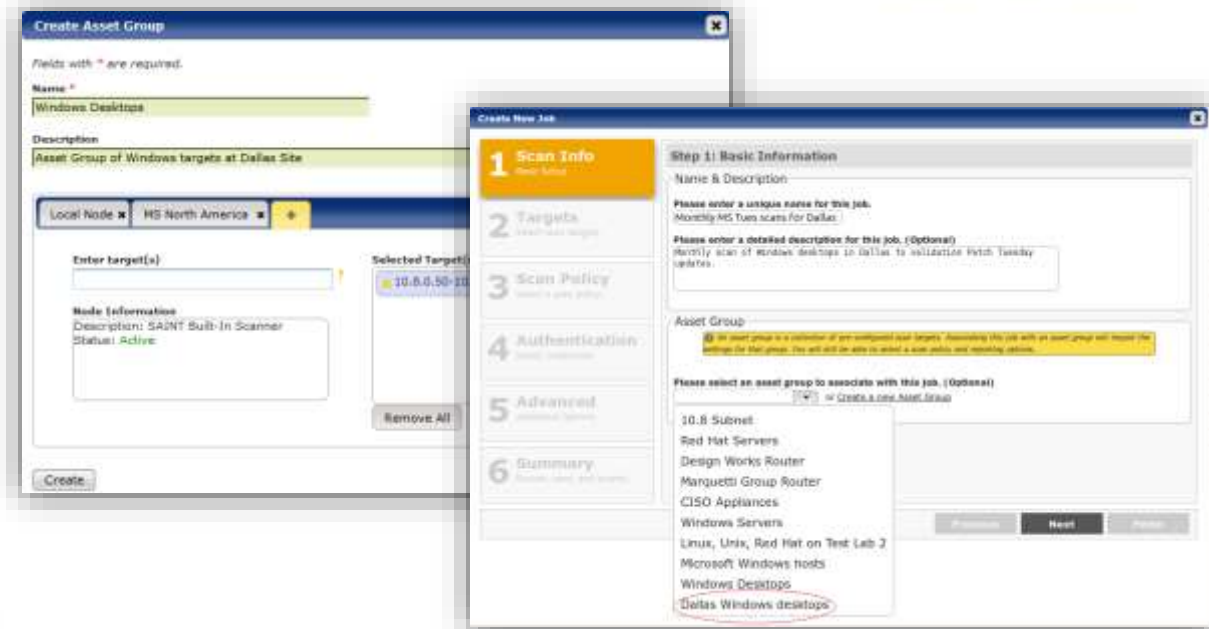
“Pruebas de seguridad en donde los asesores duplican situaciones reales de ataques y como circunvenjan el sistema en busca de vulnerabilidades, en aplicaciones o sistemas.”

Vulnerabilidades

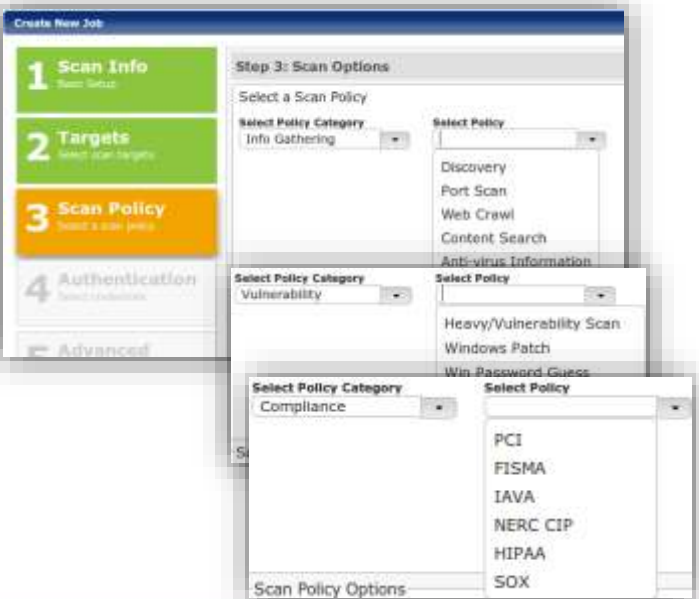
Maneja el escaneo por maquina individual o sistema completo...

Define específicamente que parte del sistema debe ser escaneado.

Chequea los riesgos basado en tipos de vulnerabilidades



Crea tus propias políticas internas. Basadas en reglas de industria o Corporativas.



El “PEN Testing” es una parte integral de la estrategia de manejo completo de riesgos a los sistemas

Exploit Tools

[Grid View](#)



La solución debe tener herramientas específicas de vulnerabilidades explotables e ingeniería social.....

Importante tener posibilidad de diferentes niveles de ataque dependiendo el resultado deseado.



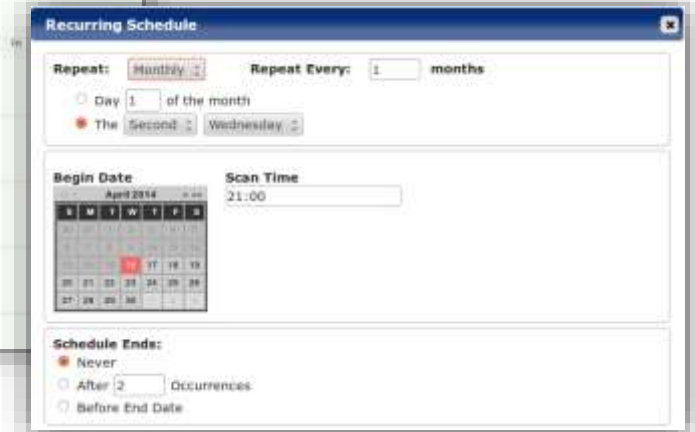
- Information Gathering – Detects live hosts, open ports, and operating system types
- Single Penetration – runs exploits targeting the remote host until one attack has a successful connection
- Root Penetration – same as Single policy although focuses on establish a connection with root or admin privileges
- Full Penetration – runs all available exploits
- Web Application – crawls remote websites/ applications and runs available exploits targeting web applications



	Escaneo de Vulnerabilidades	PEN Testing
Proposito	Identificar riesgos	Identificar riesgos usando métodos múltiples
Cuando	Por lo menos una vez por cuatrimestre, depende de volumen	Anualmente o cuando hayan cambios significativos
Como	Métodos automatizados y verificación manual	Algunas partes manualmente otras de forma automática.
Reportes	Lista de la vulnerabilidades conocidas con niveles de alarma- Critico, Alto, normal, etc.	Descripción de vulnerabilidades con información mas detallada.
Tiempo	Segundo, minutos, horas. Depende del volumen.	Días o semanas dependiendo de cuan complicado sea el proyecto.

Monitoreo constante

Define la frecuencia con la cual el sistema es monitoreado.-
Diariamente, Semanal, mensual? Depende de la política de seguridad de la empresa

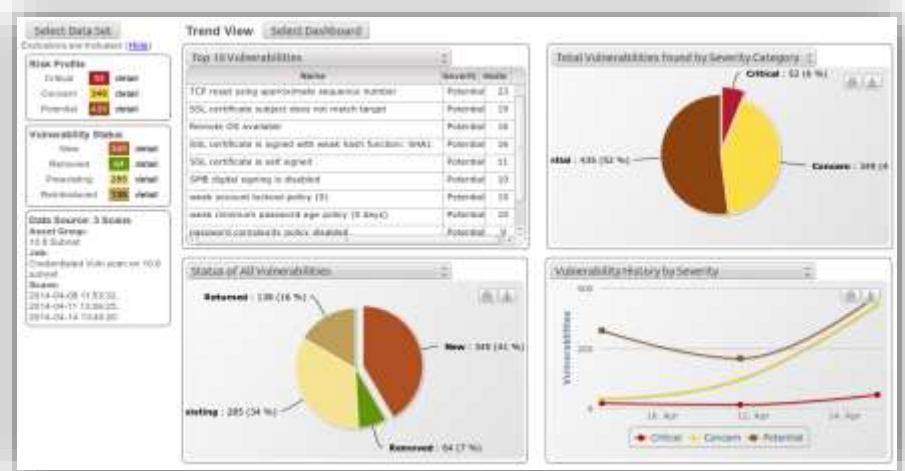


All Tickets

Actions	Ticket ID	Host IP	Service	Description	Status	Assignee	Due On	Last Occurred
	1	10.0.0.1	ftp	TCP reset using approximate sequence number	New		2014-05-07	2014-04-15
	2	10.0.0.2	http	web server uses cleartext HTTP Basic authentication (/)	Assigned	jalbrigt	2014-05-07	2014-04-15
	3	10.0.0.10	https	weak RSA public key	Assigned	idbrsr	2014-05-07	2014-04-14
	4	10.0.0.1	http	Remote OS available	New		2014-05-07	2014-04-15
	9	10.0.0.14	ftp	TCP reset using approximate sequence number	New		2014-05-07	2014-04-15
	10	10.0.0.11	https	Web server allows cross-site tracing	Assigned	jalbrigt	2014-05-07	2014-04-15

La herramienta debe tener un mecanismo de monitoreo de remediación de posibles riesgos.

A través del tiempo reportes comparativos informan el bienestar de l sistema y como han cambiado, o han sido remediados los riesgos.



Tiquetes de remediación

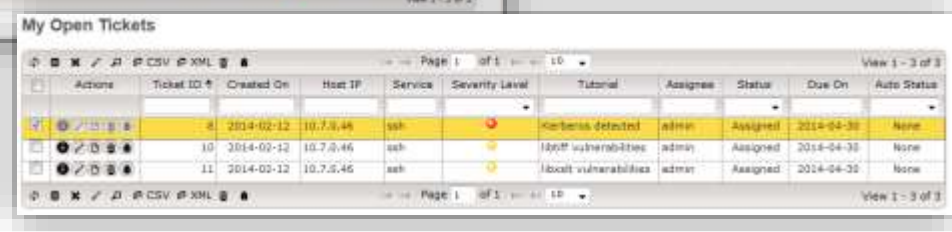
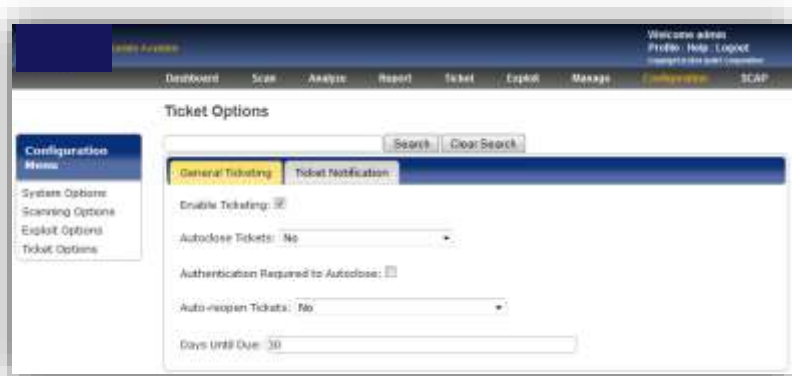
La herramienta debe tener capacidad de generar tiquetes de remediación

Pasos-

Tiquetes generados cuando vulnerabilidades sean descubiertas..

Asignan un fecha para completar remediación.

Chequea el sistema par asegurar la remediación efectivamente haya ocurrido.



Reportes Analíticos

Importante tener reportes que sean informativos, detallados y fácil de descifrar.

The screenshot displays a comprehensive security scanner interface with the following components:

- Navigation:** Dashboard, Scan, Analyze, Report, Ticket, Exploit, Manage, Configuration.
- All Scan Results:** A table with columns for Actions, IP Address, Vulnerability Check ID, Description, Service, Severity, Exploit, Exclusion, and Custom Severity. It includes a 'Select Data Set' dropdown and pagination (Page 1 of 55).
- Analyze Menu:** All Scan Results, All Vulnerabilities, Vulnerabilities by CVSS, Total Vulnerability by Host, Exclusions, Vulnerability DB, Custom Severity.
- Data Source:** 3 Scans, Asset Group: saint-data, Job: Credentialed Scan of Bethesda lab 2, Scores: 2015-04-10 15:2, 2015-05-21 15:1, 2015-06-25 09:4.
- Risk Profile:** Critical: 20, Concern: 19, Potential: 717.
- High Visibility Vults:** Critical: 20, High: 4.
- Vulnerability Status:** New: 105, Removed: 231, Pending: 332, Reintroduced: 144.
- Top 10 Vulnerabilities:**

Name	Severity	Hosts
ICMP timestamp requests enabled	Potential	38
server is susceptible to BEAST attack	Potential	35
SSL certificate is signed with weak hash function: SHA1	Potential	28
Remote OS available	Potential	27
SSL certificate subject does not match target	Potential	27
SSL certificate is self signed	Potential	23
weak RSA public key	Potential	21
web server allows MIME sniffing	Potential	20
SSL/TLS server supports RC4 ciphers	Potential	19
server is susceptible to SSL POODLE attack	Potential	18
- Total Vulnerabilities found by Severity Level:** Pie chart showing Critical: 20 (4%), Concern: 19 (3%), Potential: 717 (84%).
- Total Vulnerabilities found by Custom Severity:** Pie chart showing High: 4 (23%), Critical: 20 (76%).
- Vulnerability History by Severity:** Line chart showing vulnerability counts over time (21 Apr, 4 May, 18 May).
- 2.1 Hosts by Custom Severity:** Bar chart showing the number of hosts detected at each severity level. Text: "This section shows the overall number of hosts detected at each severity level. The severity level of a host is defined as the highest vulnerability severity level detected on that host." The chart shows 8 Critical hosts, 0 High, and 0 Effective.
- Tutorial: SSH Protocol 1 Supported:**
 - Impact:** SSH protocol version 1 has a number of known vulnerabilities. Support for version 1 or enabling SSH1 fallback renders the machines vulnerable to these issues.
 - Background:** `Secure Shell`, or `ssh`, is a program used to log into another computer over a network, execute commands on a remote machine and move files from one machine to another. It provides strong authentication and secure communications over insecure communication channels. `ssh` is intended as a replacement for `rlogin`, `rsh` and `rcp`. SSH protocol version 1 was created in 1995 and was superseded by SSH protocol version 2 in 1996.
 - Problem:** 06/30/08, CVE 2001-0201, CVE 2001-1473. The SSH Protocol 1 was deprecated due to vulnerabilities and protocol design errors. These include vulnerabilities in man-in-the-middle attacks, key recovery issues and a CAC32 compensation attack buffer overflow.
 - Resolution:** Disable SSH1 support and SSH1 fallback. See vendor website for more information including `SSH-E-Secure` and `OpenSSH`. For OpenSSH servers, SSH1 support and SSH1 fallback can be disabled by placing the following line in the `ssh_config` file:
`Protocol 2`
 - More Information:** Some of the vulnerabilities in support for SSH Protocol 1 were reported in US-CERT Vulnerability Note VU#28432 and CINC Sublet M-017.
- Additional Charts:** A 3D pie chart titled "areas of concern" showing Critical problems at 3%, areas of concern at 5%, and other categories at 92%.

- **Bring your own device (BOYD)** “Trae tu dispositivo personal.” Buena idea y real!. Usuarios usan sus propios dispositivos; los mantienen; pueden ser contactados a todas horas; se pueden conectar a la red interna en cualquier momento; teniendo los recursos necesarios en momento instante. Fantástico.... Pero existe un potencial peligro:
 - Los dispositivos no son parte de la configuración interna controlada
 - No hay manera de saber que sistema operacional usan;
 - Están conectados a la infraestructura critica interna usada por todos y
 - Raras veces los usuarios son entrenados en como usar información critica en estos dispositivos personales.
- *QUE TAL... si el ingeniero a cargo puede verificar el mismo nivel de seguridad de los sistemas internos pero para los sistemas móviles- Celulares inteligentes, Tablet, etc.*

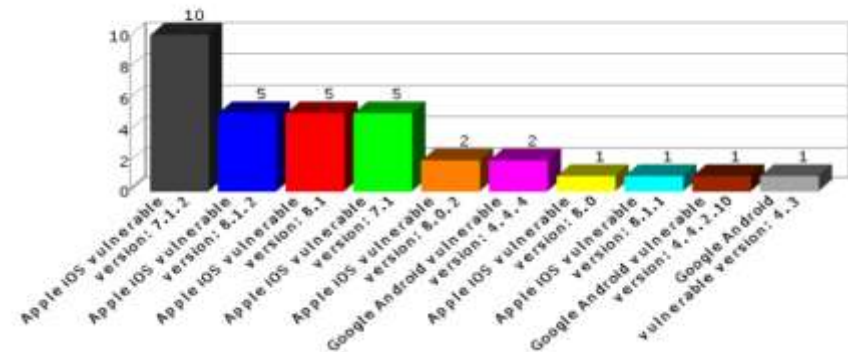
3.1 Host List

This table presents an overview of the hosts discovered on the network.

Host Name	Netbios Name	IP Address	Host Type	Critical Problems	Areas of Concern	Potential Problems
IPad4C1			Apple iOS 8.1.3	0	2	0
IPad4C1			Apple iOS 7.1.2	0	2	0
SAMSUNG-SM-G900A			Mobile Device Android	0	0	0
SAMSUNGSMN900T			Mobile Device Android	0	0	0
MotoXT907			Google Android 4.1.2.28	0	2	0
Android			Google Android 5.0	0	1	0
iPhone6C1			Apple iOS 8.1.3	0	0	0
iPhone7C1			Apple iOS 8.1.3	0	0	0

2.8 Top 10 Vulnerabilities

This section shows the most common vulnerabilities detected, and the number of occurrences.



SAINT®

Integrated Vulnerability Management,
Penetration Testing, Compliance, and
Configuration Assessment.



Gracias por su atención-
Alberto E. Aguilar-Sartori
aguilarae@saintcorporation.com
@SAINTscan
@Beartoe_Aguilar



Tenacious
Information
Security