SAINT®

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

¿Cuan seguro es seguro?

-Cuales herramientas necesitas para proteger tu organización

IntegraTec
Integraciones Tecnológicas

Tenacious Information Security

Como manejo el riesgo?

¿Que Herramientas necesito?-

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

Como manejo el riesgo?

Tipos de pruebas

- **Escaneo de vulnerabilidades**

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

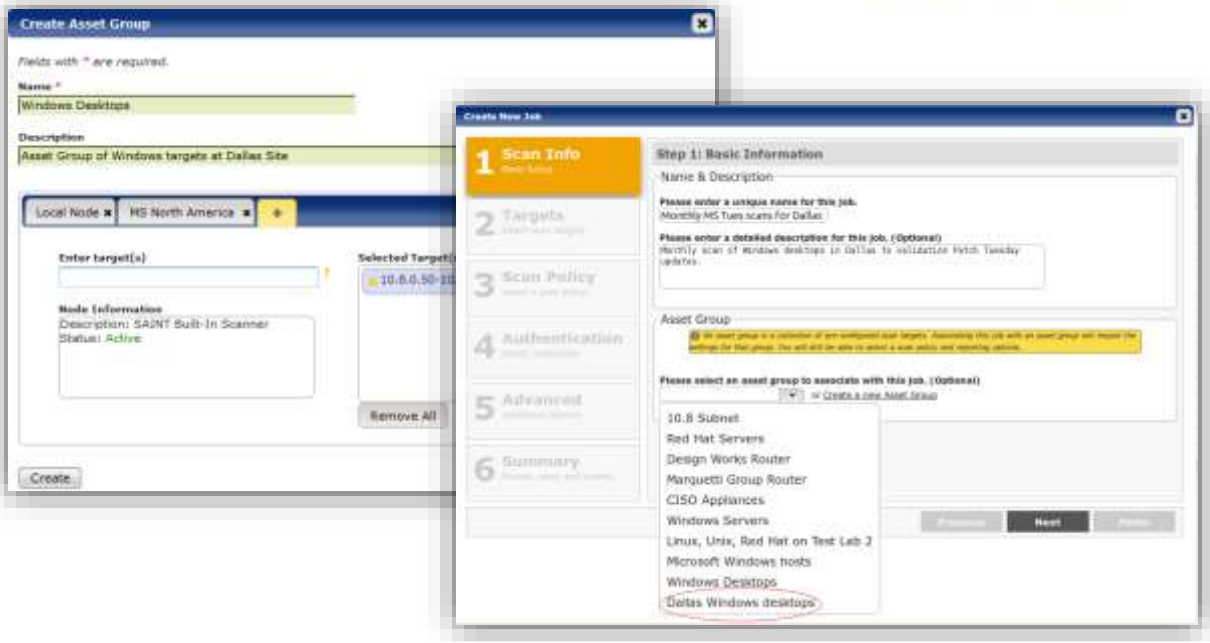
- **Pruebas de penetración ("PEN testing")**

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

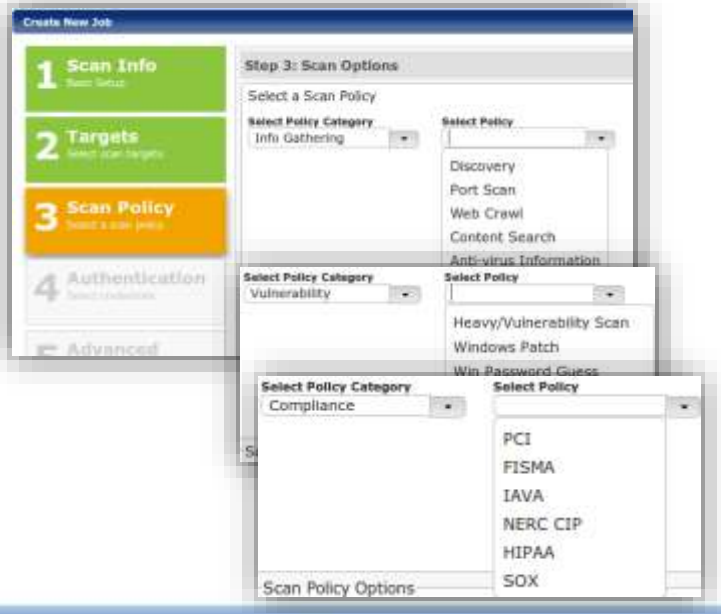
Vulnerabilidades

Maneja el escaneo por maquina individual o sistema completo…

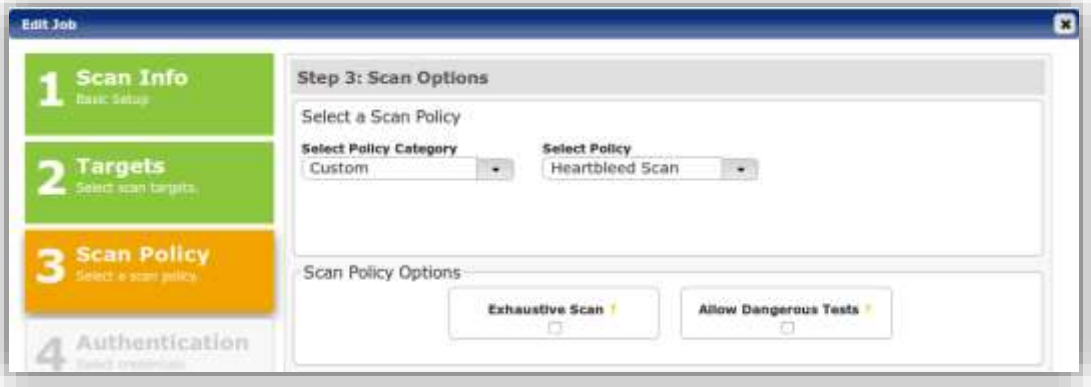
Define específicamente que parte del sistema debe ser escaneado.



Chequea los riesgos basado en tipos de vulnerabilidades

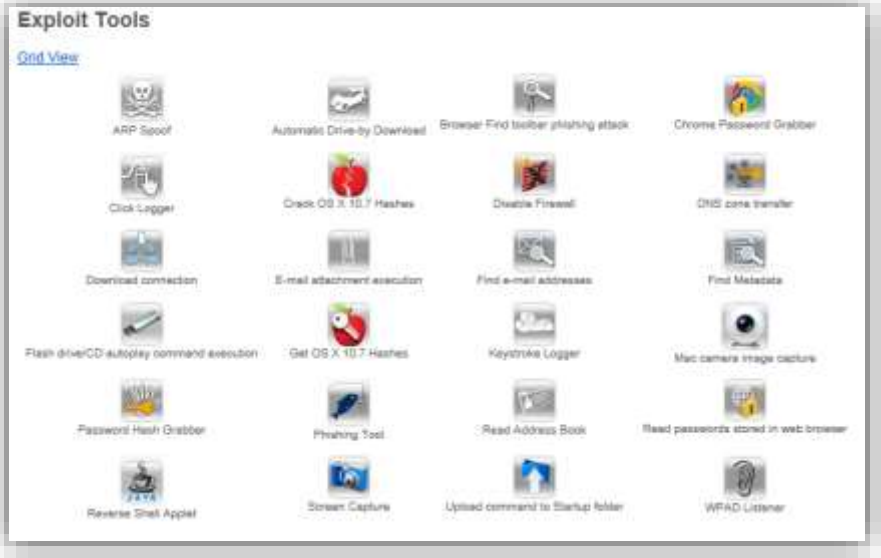


Crea tus propias políticas internas. Basadas en reglas de industria o Corporativas.



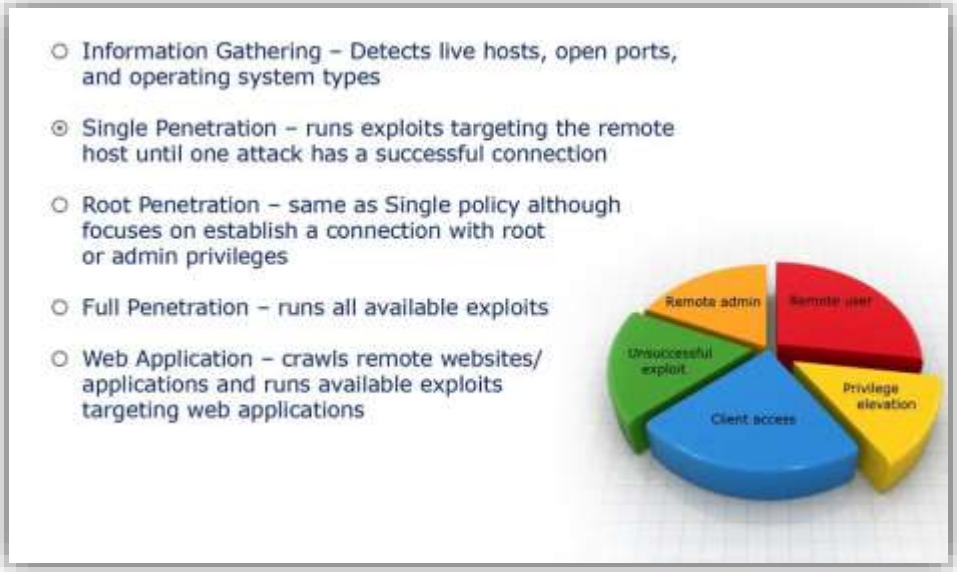
Pruebas de Penetración (PEN testing)

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



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

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

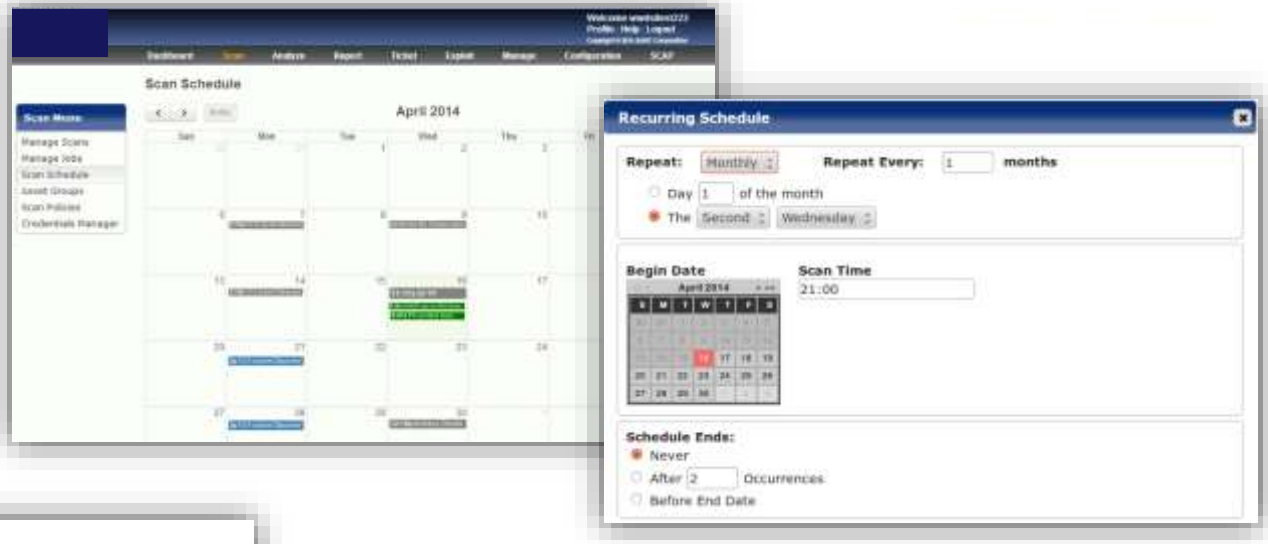


Escaneo de vulnerabilidades vs. Pruebas de penetración

	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.

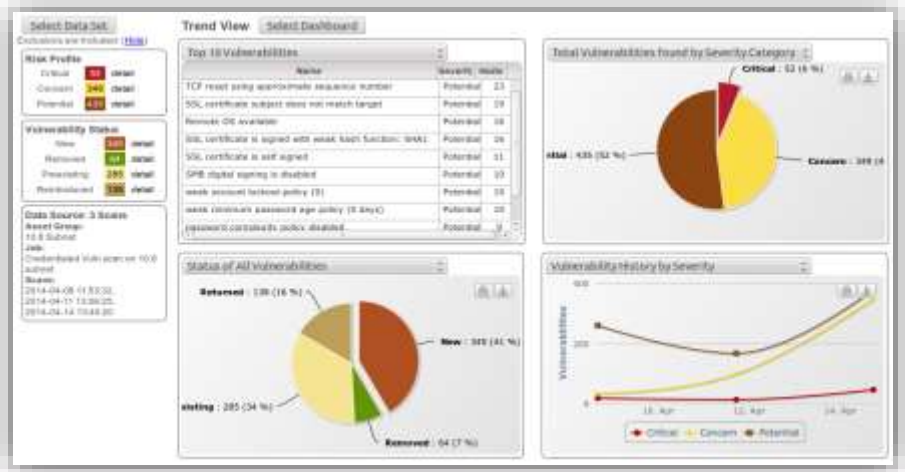
Monitoreo constante

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



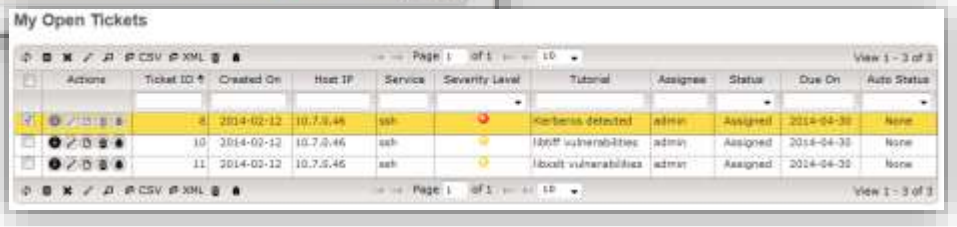
La herramienta debe tener un mecanismo de monitoreo de remediación de posibles riesgos.

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-

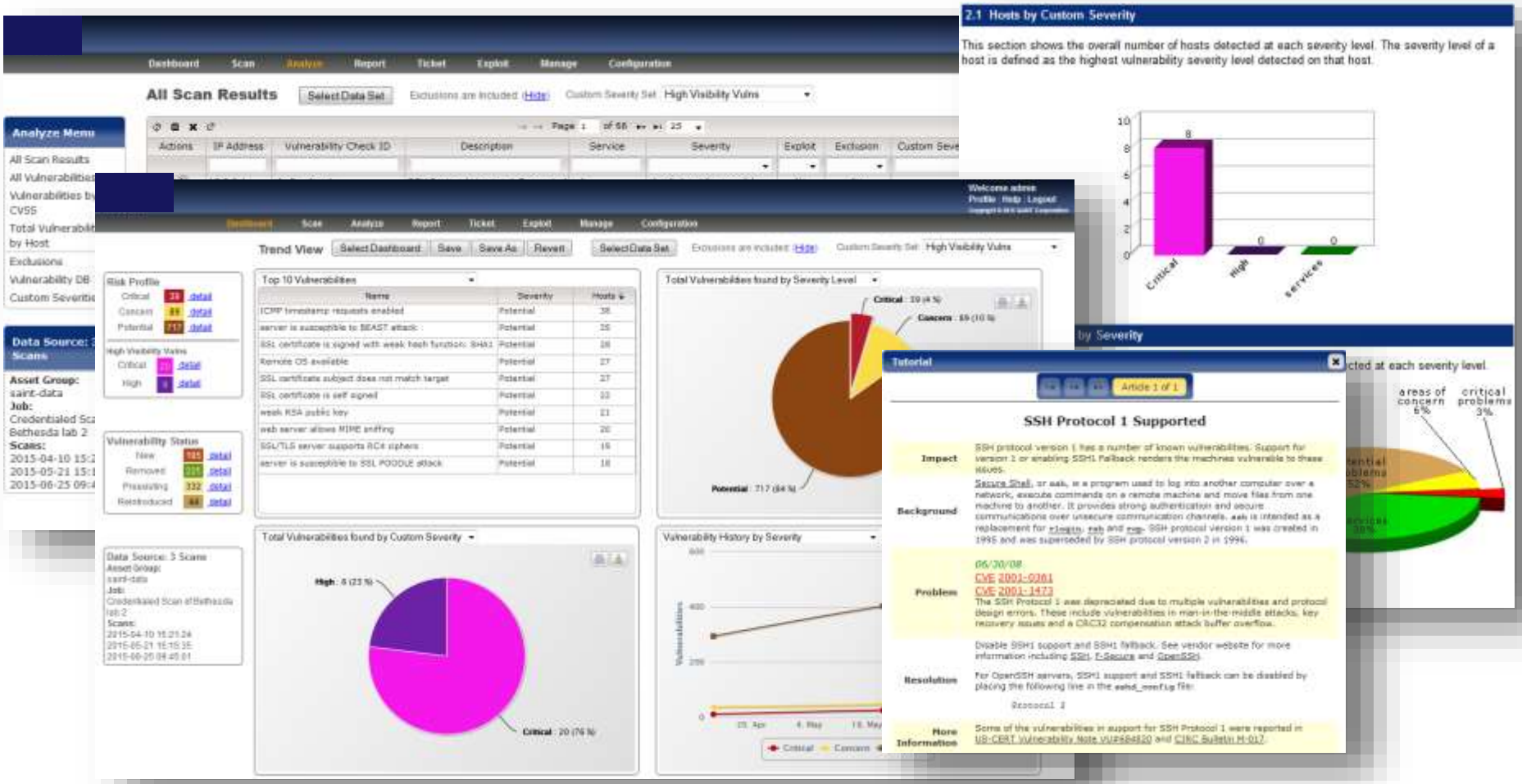
Tiquetes generados cuando vulnerabilidades sean descubiertas..

Asignan un fecha para completar remediación.

Chequea el sistema par asegurar la remediación efectivamente haya ocurrido.

Reportes Analíticos

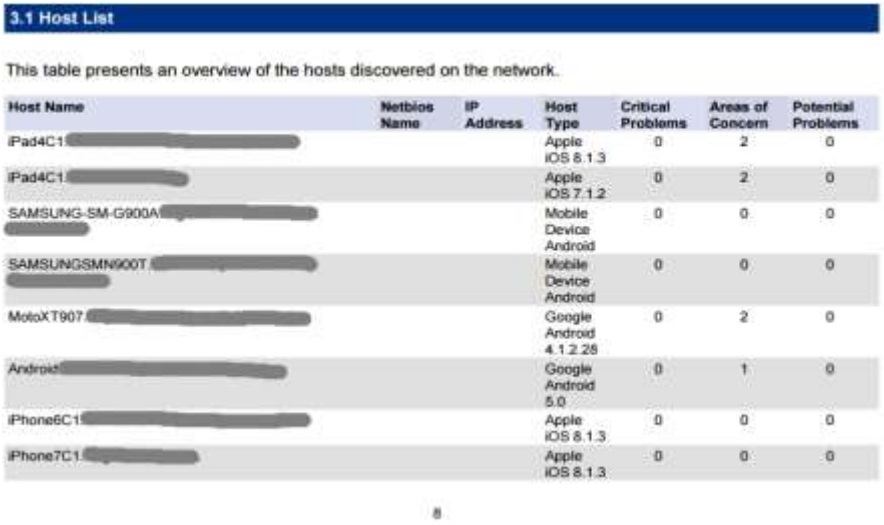
Importante tener reportes que sean informativos, detallados y fácil de descifrar.



Seguridad Móvil

- **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 rede 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.*

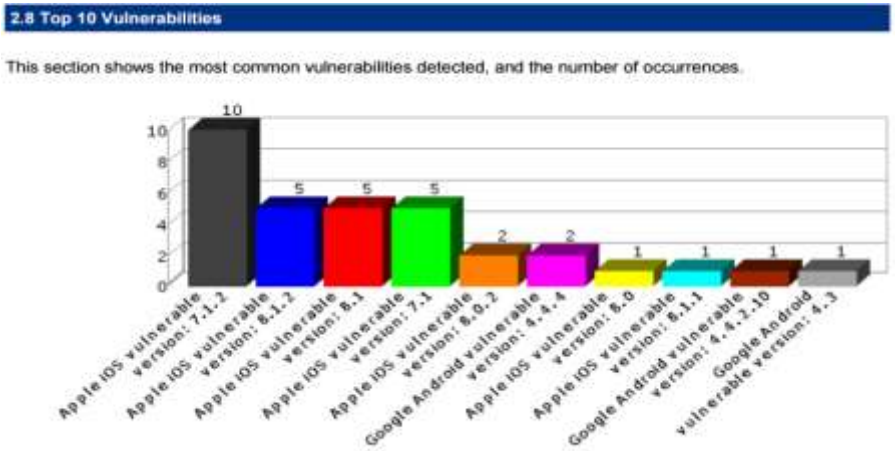


3.1 Host List

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

8



SAINT®

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

Gracias por su atención-

Alberto E. Aguilar-Sartori

aguilarae@saintcorporation.com

@SAINTscan

@Beartoe_Aguilar

IntegraTec
Integraciones Tecnológicas

Tenacious Information Security