SCProgress

Cloud24x7

Vulnerability Assessment & Penetration Testing

Evaluación de Vulnerabilidades y Test de Penetración

SERVICIOS COMPUTACIONALES PROGRESS
La Pradera E7-21 y Mariana de Jesús, oficina 301, Quito – EC 170518
Telf: (+593) 2 2900865, mail: info@scprogress.com, www.scprogress.com

RESUMEN EJECUTIVO

En mutuo acuerdo con el cliente y el director del area de TI, se realiza la evaluación de vulnerabilidades y test de penetración en los equipos de seguridad perimetral del cliente.

El reporte es generado en base a las observaciones y resultados obtenidos durante el periodo de evaluación. En el informe se detallará la marca y serie del equipo al, posteriormente se hará referencia al mismo como DISPOSITIVO.

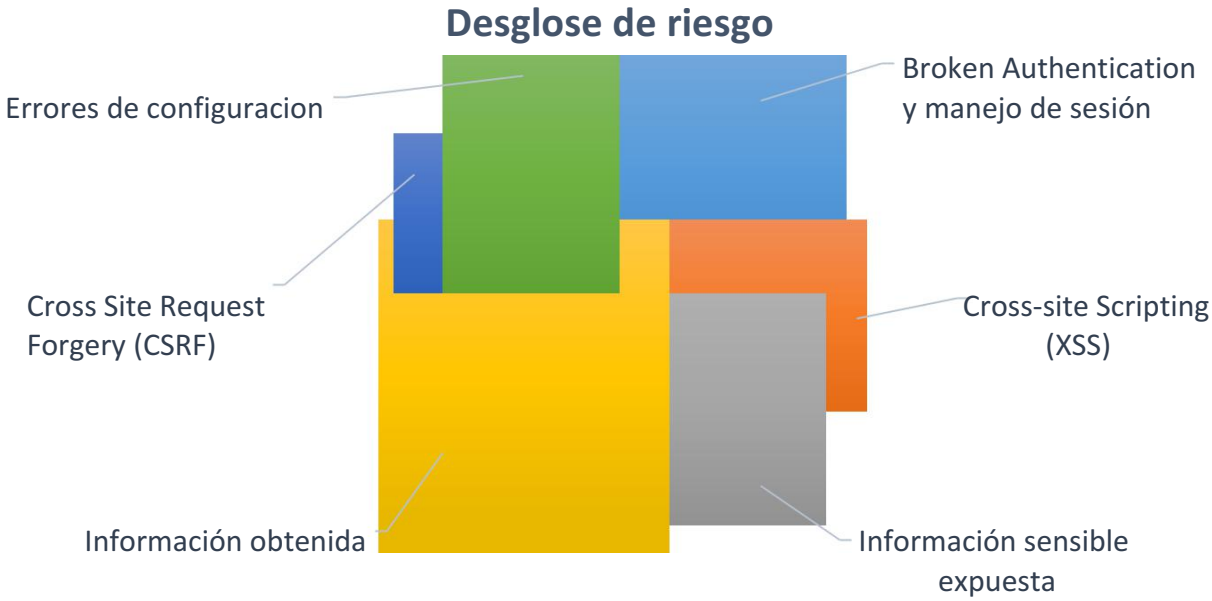
Datos del dispositivo

Localización	
Tipo de dispositivo	
Marca del dispositivo	
Modelo	
Número de serie	XXXXXXXXXXX-XXXXXX
Tipo de escaneo	Externo/Interno/mixto
Fecha y hora de inicio de la evaluación	
Fecha y hora de terminación de la evaluación	
Dirección IP	
Lugar de origen de la evaluación	

NIVEL DE SEGURIDAD

Mas de 100 tests de vulnerabilidades se realizan en los dispositivos con el fin de determinar el nivel de seguridad. Se determina el porcentaje de vulnerabilidades detectadas y las medidas que requieren tomar de manera urgente.

Estas vulnerabilidades se muestran en dos gráficas que son: el resumen de evaluación y el desglose de riesgo. Estos resultados dan una muestra del estado de seguridad actual.



NOTA: Las gráficas son unicamente con fines demostrativos, los porcentajes y valores cambian según los resultados obtenidos.

OBJETIVO Y ALCANCE

El propósito de la evaluación es el de determiner las vulnerabilidades de seguridad en los dispositivos analizados. El alcance de la evaluación está limitado a las IPs analizadas.

Metodología

El escaneo externo de vulnerabilidades es realizado apra evaluar la efectividad de los controles y configuraciones actuales en las configuraciones de seguridad en la red del cliente. Además, el información recabada durante la evaluación se la usará unicamente como evidencia de soporte de los hallazgos. La evaluación se lleva a cabo de una manera que simula a un agente malicioso involucrado en un ataque directo hacia los sistemas del cliente. Al mismo tiempo, se toman todas las medidas del caso, para no causar ningún daño a los dispositivos o red del cliente.

Tipos de vulnerabilidades

Los tests de vulnerabilidades realizados durante la evaluación pertenecen al siguiente tipo de amenazas.

Matriz de Riesgo

Los niveles de riesgo de seguridad pueden ser clasificados mediante una matriz de riesgo. Los niveles de criticidad de las vulnerabilidades dependen del impacto a la organización, si la vulnerabilidad fue explotada y su complejidad o el nivel de dificultad necesaria para explotar la vulnerabilidad. La explotación de la vulnerabilidad puede resultar en la fuga de información sensible, impacto en la continuidad del negocio, compromiso de la red o implantación en sistemas críticos o los usuarios de malware/ransomware.

Acontinuación la descripción de los niveles de criticidad basado en el impacto en los dispositivios analizados y en la organización.

ALTO	MEDIO	BAJO
Un atacante puede comprometer completamente la confidencialidad, integridad y disponibilidad del dispositivo; sin ningún tipo de condiciones especiales, privilegios o forma de autenticación alguna.	Un atacante puede comprometer parcialmente la confidencialidad, integridad y disponibilidad del dispositivo; sin ningún tipo de condiciones especiales, privilegios o forma de autenticación alguna.	Un atacante puede comprometer ligeramente la confidencialidad, integridad y disponibilidad del dispositivo; sin ningún tipo de condiciones especiales, privilegios o forma de autenticación alguna.

PRINCIPALES OBSERVACIONES

En esta secciónse detalla como el dispositivo respondió a los test de vulnerabilidad realizados durante el periodo de evaluación, que cubre la siguiente información.

- Fortalezas de seguridad del dispositivo.
- Debilidades encontradas en el dispositivo, asi como al severidad, impacto, recomendación de remediación y evidencia de soporte.

Fortalezas de seguridad del dispositivo

En esta sección, se detallan las fortalezas y las correctas configuraciones que presenta el dispositivo hacia determiandos tipos de vulnerabilidades y ataques.

NOTA: La siguiente tabla es únicamente con fines demostrativos.

Debilidades encontradas en el dispositivo

En esta sección, se detallan las debilidades y vulnerabilidades encontradas en el dispositivio durante la evaluación. Además de los tipos de ataques, se especificia la severidad de las vulnerabilidades, el impacto y la remediación a fin de mejorar la seguridad del sistema. Los resultados obtenidos de la evaluación se presentan como evidencia de soporte del proceso.

NOTA: L*a siguiente tabla es únicamente con fines demostrativos y de ejemplificación.*

- Ruptura de autentificación y Administración de sesión

Vulnerabilidad	Autenticación con credencial en texto plano
Severidad	ALTO
Observaciones	Se tiene acceso al dispositivo por medio de canales no cifrados, los cuales revelan la información de los adminsitradores.
Impacto	Esto puede resultar en la exposición de información sensible. El atacante puede tomar control total sobre el dispositivo, sobre toda la red y sobre la información reservada de la organización.
Remediación	El acceso al dispositivo de ser restringido unicamente a canales cifrados. El inicio de sesión debe ser siempre por HTTPS y no HTTP.

Evidencia