

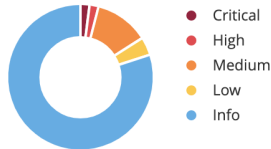
Tarea de Auditoría de Seguridad

1.- Debe llevar a cabo un estudio de vulnerabilidades en dos portales, para ello se requiere utilizar las herramientas aprendidas en el curso, en especial Tenable Nessus Essentials (<https://www.tenable.com/downloads/nessus?loginAttempted=true>). Se debe seleccionar uno de los portales del listado proporcionado más adelante y otro debe ser identificado a través de la transferencia de zona del DNS interno, priorizando aquel que presente vulnerabilidades críticas y altas. Posteriormente, se debe realizar un análisis detallado de las brechas de seguridad encontradas en las auditorías, con el objetivo de evaluar los riesgos y su impacto potencial en la integridad, confidencialidad y disponibilidad de la información. Finalmente, se deben ofrecer recomendaciones para fortalecer las prácticas de ciberseguridad.

La tarea comprende los siguientes ítems:

Informe:

- Alcance y descripción del estudio
 - Propósito principal, alcance, objetivos, funcionalidades generales, etc. 10 puntos
- Metodología utilizada. 5 puntos
- Presentación y definición de vulnerabilidades detectadas. 60 puntos
 - Estas deben ir descritas en un cuadro (ver *) con lo siguiente:
 - Nombre
 - Descripción
 - Valoración cualitativa (Crítica, alta, media, baja, etc)
 - Impacto
 - Elementos afectados
 - Evidencia
 - Acción
 - Estado
 - Referencias
 - Gráfica explicativa (x ejemplo un histograma o gráfico circular con los tipos de vulnerabilidades)
 - Ejemplo:



Nivel de Severidad	Color
Critical	Rojo oscuro
High	Rojo
Medium	Naranja
Low	Amarillo
Info	Azul
-
- Recomendaciones y plan de acciones correctivas. 10 puntos
- Conclusiones. 10 puntos
- Bibliografía. 5 puntos

Se evaluará la habilidad para abordar el tema en el informe, así como el uso de soporte visual específico para describir la auditoría. El informe debe incluir todas las vulnerabilidades clasificadas en las siguientes categorías: Críticas, Altas y Medias (al menos dos de cada una), Bajas e Informativas (al menos una de cada una).

Deberá presentar su estudio de manera ejecutiva en 10 minutos, con la participación de todos los integrantes del grupo. La entrega del informe y la presentación tienen como fecha límite el lunes 8 de julio al mediodía. Las presentaciones se llevarán a cabo ese mismo día durante el horario habitual de la clase, con asistencia obligatoria.

(*)

VI-01 – Cisco IOS XE Cluster Management Protocol Telnet Option Handling RCE (cisco-sa-20170317-cmp).

Descripción	Al dispositivo remoto le falta un parche de seguridad proporcionado por el proveedor.
Criticidad	 CRITICAL
Impacto	<p>De acuerdo con su versión y configuración auto informadas, el software Cisco IOS XE que se ejecuta en el dispositivo remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el subsistema del Protocolo de administración de clústeres (CMP) debido al manejo inadecuado de las opciones de Telnet específicas de CMP.</p> <p>Un atacante remoto no autenticado puede explotar esto para establecer una sesión de Telnet con opciones de telnet específicas de CMP con formato incorrecto, para ejecutar código arbitrario.</p>
Elementos afectados/ URL	<p>IPs:</p> <ul style="list-style-type: none">10.100.132.1
Evidencia / PoC	<pre>Cisco bug ID : CSCvd48893 Installed release : 3.7.2E Note: Either valid host / enable credentials were not provided for the remote device or the device is not licensed for the feature. It is, therefore, not possible to determine whether this vulnerability applies to your configuration.</pre>
Acción	Actualice a la versión corregida relevante a la que se hace referencia en el Id. de bug Cisco CSCvd48893. Alternativamente, como solución alternativa, deshabilite el protocolo Telnet para las conexiones entrantes.
Estado	Resolución pendiente (en el momento de la preparación del informe de auditoría)
Referencias	<p>CVSS v3.0 Base Score - 9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)</p> <p>CVSS v3.0 Temporal Score - 9.4 (CVSS:3.0/E:H/RL:O/RC:C) CVSS</p> <p>Base Score - 10.0 (CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C)</p> <p>CVSS Temporal Score - 8.7 (CVSS2#E:H/RL:OF/RC:C)</p> <p>BID 96960</p> <p>CVE CVE-2017-3881</p> <p>XREF CISCO-BUG-ID:CSCvd48893 XREF IAVA:2017-A-0073</p> <p>XREF CISCO-SA:cisco-sa-20170317-cmp XREF CISA-KNOWN-EXPLOITED:2022/04/15</p>

Listado de URL's:

<https://carlataramasco.cl/>

<https://quida.cl/>

<https://rmid.cl/>

<https://itisb.cl/>

<https://gescamas.cl/>

<https://tablet.gescamas.cl/>

<https://cecancontigo.cl/>

2.- Entregar los resultados de la Guía 2 de la materia de Sniffer, indicando las vulnerabilidades que se presentan, su impacto y recomendaciones para mitigarlas.