Unidad 4 / Escenario 8

Lectura fundamental

Procedimiento y manual técnico de seguridad en el ciclo de desarrollo

Contenido

Palabras clave: implementación, seguridad, ciclo, desarrollo, consejos, sensibilización, motivación.

1. Introducción

En este último escenario de la unidad continuaremos hablando de la documentación existente para la seguridad en el ciclo de desarrollo de software. En específico, durante el escenario observaremos en qué consiste el "como", a diferencia del escenario anterior donde observábamos el "que" hacer en cuanto a seguridad en el ciclo de desarrollo.

Específicamente observaremos en que consiste:

- Un procedimiento de seguridad en el ciclo de desarrollo
- Un manual técnico

Adicionalmente realizaremos una serie de importantes consejos a la hora de redactar la documentación de seguridad en el ciclo de desarrollo, de manera que se adapte a las particularidades que puede tener cada empresa.

2. Procedimiento de seguridad en el ciclo de desarrollo de software

El procedimiento de seguridad en el ciclo de desarrollo es el documento que continua en el siguiente nivel en la pirámide de documentación definida en el escenario número siete, es decir es el documento que se elabora después del proceso de seguridad en el ciclo de desarrollo de software, este último es el siguiente a la política de seguridad.

2.1. Definición

Por definición, un procedimiento de seguridad es el método de ejecutar las cosas. En otras palabras, se trata de un paso a paso debidamente ordenado, orientado a obtener un resultado u objetivo específico.

2.2. Ejemplo

A continuación observaremos un ejemplo de la documentación de un procedimiento de seguridad en el ciclo de desarrollo, específicamente lo relacionado con la actividad escaneo de vulnerabilidades:

El escaneo de vulnerabilidades definido en el proceso de seguridad en el ciclo de desarrollo deberá seguir la metodología tradicional utilizada por los hackers éticos. En este sentido, el escaneo deberá seguir el siguiente orden:

- *Recolección de información: en esta etapa se deberá realizar la mayor recolección de información técnica de los objetivos a escanear. Dentro de la información que se debe recolectar (mientras sea posible) se encuentra:*
  - *Direcciones IP*
  - *Nombres de host*
  - *Versión de sistema operativo*
  - *Versión del servidor WEB*
  - *Lenguaje de programación*
  - *Mensajes de error*
  - *Otra información*
- *Escanear: con la información técnica recolectada, procederemos a realizar el escaneo de los objetivos. Para tal fin es importante realizar el escaneo de la siguiente manera:*
  - *El escaneo se debe realizar con la herramienta Nessus Tenable (Tenable, 2016)*
  - *Se debe gestionar con el área de seguridad de la empresa los permisos requeridos para evitar que la IP sea bloqueada por firewalls, IPS u otros mecanismos.*
  - *La política a configurar para el escaneo debe ser la más agresiva o paranoica posible, teniendo en cuenta los resultados obtenidos en la etapa de recolección de información, es decir configurar los plugins de sistema operativo, versión del servidor, etc.*
  - *Se debe realizar un escaneo interno (desde la red LAN) sin credenciales de autenticación*
  - *Se debe realizar un escaneo interno (desde la red LAN) con credenciales de autenticación*
  - *Se deber realizar un escaneo externo (desde Internet) sin credenciales de autenticación*
  - *Se deber realizar un escaneo externo (desde Internet) con credenciales de autenticación*
- *Reportar: una vez realizados los cuatro escaneos, se consolidarán los reportes en uno único. El reporte se debe generar en formato PDF y será entregado a los administradores y/o responsables de los objetivos.*

- *Descartar falsos positivos: se deberá realizar una evaluación completa de las vulnerabilidades reportadas para descartar que sean falsos positivos, de manera que únicamente se tengan en cuenta las verdaderas vulnerabilidades. Una vez realizado el ejercicio, se deberá elaborar un consolidad final de vulnerabilidades a remediar.*
- *Priorizar: la priorización de las vulnerabilidades se realizará mediante el nivel de criticidad reportado por Nessus Tenable (Tenable, 2016) para cada vulnerabilidad. Se ordenarán desde el nivel mayor (criticas) al nivel menor (información).*
- *Implementación: los responsables de los objetivos deberán establecer un plan de trabajo para remediar cada una de las vulnerabilidades. Se debe tener en cuenta lo definido en el proceso de seguridad en el ciclo de desarrollo para tener claro cuáles son los límites de tiempo que se tienen para remediar la vulnerabilidad, dependiendo de su criticidad.*
- *Re-test: con la confirmación del cierre o finalización del plan de tratamiento de vulnerabilidades, se procederá a realizar un re-test o re-escaneo. Para tal fin se debe tener en cuenta lo siguiente:*
  - *El escaneo se debe realizar con la herramienta Nessus Tenable (Tenable, 2016) nuevamente*
  - *Los escaneos se realizarán con la misma policía configurada inicialmente.*
  - *Se generará un reporte diferencial, es decir un reporte que compare el resultado anterior con el actual.*
  - *Las vulnerabilidades nuevas o las que se mantengan se trabajarán como si fueran nuevas, es decir se deberá seguir desde la sección "reportar" de este procedimiento hasta que se confirme que no quedan vulnerabilidades abiertas.*

Como se pudo observar, el procedimiento incluye muchísimo más detalle técnico y una estructura organizada de ejecutar las acciones para lograr un objetivo. De igual manera se observa como inicia el procedimiento relacionándolo con el proceso, observando así que se deriva de dicho documento.

3. Manual técnico de seguridad en el ciclo de desarrollo de software

El manual técnico de seguridad en el ciclo de desarrollo es el último documento de la pirámide de documentación definida en el escenario número siete. Este es el documento con el mayor nivel de detalle técnico existente y se deriva del procedimiento de seguridad en el ciclo de desarrollo de software.

3.1. Definición

Por definición, el manual es un documento muy fácil de entender, esto siempre y cuando el lector tenga las competencias y conocimientos necesarios.

3.2. Ejemplo

Continuando con el mismo ejemplo, observaremos como se realiza los últimos 4 pasos de la etapa "escanear" definida en el procedimiento de la sección 3.2:

Para realizar un escaneo de vulnerabilidades con credenciales, desde la red interna, se deberán realizar las siguientes actividades:

- *Abra la herramienta Nessus Tenable (Tenable, 2016)*
- *Ingrese su usuario y contraseña*
- *Confirme que el equipo desde el cual ejecutará el escaneo tiene configurada una dirección interna, es decir que tenga la estructura 10.0.X.X*
- *En la página Scans / My Scans, seleccione New Scan. Aparecerá la página Scan Library.*
- *Seleccione la plantilla Advance Scan*
- *Configure el escaneo utilizando los enlaces Basic, Discovery, Assessment, Report y Advanced*
- *Seleccione la opción Credentials*
- *DIgite el usuario y contraseña*
- *Seleccione la opción Compliance*
- *Seleccione las opciones aplicables*
- *Seleccione la opción Plugins*
- *Seleccione los plugins aplicables*
- *Haga clic en Save y posteriormente en Launch para lanzar el escaneo*

Para realizar un escaneo de vulnerabilidades sin credenciales, desde la red interna, se deberán realizar las siguientes actividades:

- *Abra la herramienta Nessus Tenable (Tenable, 2016)*
- *Ingrese su usuario y contraseña*
- *Confirme que el equipo desde el cual ejecutará el escaneo tiene configurada una dirección interna, es decir que tenga la estructura 10.0.X.X*
- *En la página Scans / My Scans, seleccione New Scan. Aparecerá la página Scan Library.*
- *Seleccione la plantilla Advance Scan*
- *Configure el escaneo utilizando los enlaces Basic, Discovery, Assessment, Report y Advanced*
- *Seleccione la opción Compliance*
- *Seleccione las opciones aplicables*
- *Seleccione la opción Plugins*
- *Seleccione los plugins aplicables*
- *Haga clic en Save y posteriormente en Launch para lanzar el escaneo*

Para realizar un escaneo de vulnerabilidades con credenciales, desde la red externa, se deberán realizar las siguientes actividades:

- *Abra la herramienta Nessus Tenable (Tenable, 2016)*
- *Ingrese su usuario y contraseña*
- *Confirme que el equipo desde el cual ejecutará el escaneo tiene configurada una dirección pública en Colombia, es decir que pertenezca a la siguiente lista de rangos de IP, pero no haga parte del rango de la IP públicas configuradas en la empresa:*

Tabla 1. Rangos de referencia de direcciones IP públicas de Colombia

3.0.4.0/24	8.38.24.0/24	11.56.0.0/24	23.32.192.0/19	23.46.2.0/23
23.61.245.0/24	23.61.247.0/24	23.67.16.0/20	23.219.48.0/20	23.220.64.0/20
24.197.179.0/24	45.5.160.0/21	45.5.172.0/22	45.5.180.0/20	45.7.132.0/22
45.65.136.0/22	45.65.200.0/24	45.65.232.0/22	45.70.168.0/22	45.71.180.0/22
49.18.35.0/24	57.74.192.0/19	58.47.186.0/24	62.160.242.0/24	63.163.180.0/23
63.168.93.0/24	63.171.232.0/24	63.174.200.0/21	63.245.64.0/23	63.245.80.0/21
63.245.96.0/21	64.76.48.0/20	64.76.80.0/20	64.76.112.0/21	64.76.176.0/22

64.76.184.0/21	64.76.208.0/21	64.86.224.0/23	65.167.48.0/20	65.167.80.0/20
65.168.52.0/23	65.199.244.0/23	65.208.64.0/21	65.243.120.0/23	65.247.206.0/23
65.247.240.0/23	65.247.244.0/22	66.231.64.0/20	69.42.114.0/23	69.164.46.0/23
69.195.210.0/23	70.35.154.0/24	70.35.156.0/24	70.35.159.0/24	72.46.230.0/23
76.218.64.0/24	82.250.14.0/24	92.122.210.0/23	92.123.240.0/22	104.77.198.0/23
104.91.128.0/18	104.132.160.0/24	107.180.148.0/20	113.171.244.0/24	128.90.108.0/24
128.90.115.0/24	131.0.136.0/22	131.100.1.0/24	131.108.168.0/22	131.196.208.0/21
131.221.40.0/22	132.255.20.0/22	138.0.40.0/22	138.0.88.0/22	138.36.64.0/22
138.94.0.0/22	138.97.56.0/22	138.97.80.0/22	138.117.40.0/22	138.117.84.0/22
138.117.108.0/22	138.117.136.0/22	138.121.4.0/22	138.121.12.0/22	138.121.156.0/22
138.122.200.0/22	138.186.20.0/22	138.186.141.0/24	138.186.188.0/22	138.204.238.0/24
138.255.96.0/24	141.101.109.0/23	143.0.92.0/22	143.0.102.0/23	143.0.108.0/22
143.137.96.0/22	143.208.64.0/22	147.75.112.0/20	148.177.116.0/24	150.125.100.0/24
152.194.84.0/24	152.200.0.0/13	152.231.24.0/21	156.115.186.0/24	157.240.6.0/24
157.253.0.0/16	161.10.0.0/16	161.18.0.0/16	162.168.12.0/24	162.212.213.0/24
166.238.141.0/24	167.0.0.0/16	167.249.40.0/22	167.250.120.0/22	168.0.244.0/22
168.90.12.0/22	168.90.92.0/22	168.176.0.0/16	168.197.68.0/22	168.227.0.0/22
168.227.104.0/22	168.227.244.0/22	168.228.108.0/22	168.228.124.0/22	170.78.40.0/22
170.78.56.0/22	170.78.185.0/24	170.79.88.0/22	170.80.8.0/22	170.80.96.0/22
170.81.24.0/22	170.81.252.0/22	170.82.40.0/23	170.83.59.0/24	170.238.64.0/23
170.238.168.0/23	170.238.226.0/23	170.238.236.0/22	170.246.112.0/22	170.247.0.0/22
170.254.0.0/22	170.254.228.0/22	177.252.0.0/14	178.31.40.0/24	179.0.9.0/23
179.0.15.0/24	179.0.27.0/24	179.0.29.0/24	179.0.146.0/24	179.0.154.0/24
179.0.205.0/24	179.1.0.0/16	179.12.0.0/14	179.18.0.0/15	179.32.0.0/15
179.42.64.0/24	179.42.77.0/18	179.42.144.0/20	179.42.172.0/22	179.43.104.0/21
179.49.128.0/16	179.51.96.0/19	179.60.32.0/20	179.60.240.0/22	179.61.15.0/24
179.61.112.0/20	181.32.0.0/15	181.48.0.0/17	181.48.123.0/16	181.49.40.0/13

181.56.200.0/13	181.68.0.0/14	181.78.0.0/19	181.118.144.0/20	181.119.30.0/24
181.128.0.0/12	181.143.71.0/11	181.174.0.0/18	181.192.128.0/17	181.204.0.0/14
181.224.160.0/22	181.225.64.0/18	181.232.0.0/17	181.234.0.0/14	181.240.0.0/12
183.60.156.0/24	184.29.43.0/24	186.0.0.0/17	186.1.128.0/18	186.1.248.0/21
186.27.128.0/16	186.28.47.0/14	186.43.0.0/17	186.80.0.0/13	186.86.152.0/15
186.97.0.0/14	186.102.0.0/15	186.112.0.0/13	186.121.0.0/17	186.144.0.0/17
186.144.84.0/14	186.148.160.0/19	186.154.0.0/15	186.159.1.0/17	186.159.112.0/22
186.168.0.0/16	186.169.1.0/14	186.179.96.0/20	186.180.0.0/15	186.183.128.0/17
190.0.0.0/18	190.0.240.0/21	190.1.64.0/19	190.1.128.0/17	190.3.192.0/18
190.5.192.0/20	190.6.160.0/19	190.7.64.0/17	190.8.176.0/22	190.8.192.0/18
190.9.64.0/18	190.9.192.0/18	190.12.128.0/19	190.13.0.0/18	190.13.96.0/20
190.13.192.0/20	190.14.224.0/18	190.24.0.0/13	190.52.0.0/19	190.60.0.0/20
190.60.17.0/20	190.60.28.0/23	190.60.31.0/24	190.60.64.0/18	190.60.192.0/16
190.61.128.0/19	190.61.161.0/18	190.61.206.0/23	190.61.210.0/20	190.61.220.0/19
190.61.251.0/21	190.65.0.0/13	190.84.0.0/19	190.84.20.0/15	190.85.110.0/16
190.90.0.0/20	190.90.13.0/20	190.90.24.0/20	190.90.40.0/20	190.90.54.0/24
190.90.56.0/20	190.90.68.0/20	190.90.81.0/23	190.90.84.0/22	190.90.89.0/24
190.90.91.0/24	190.90.93.0/20	190.90.104.0/20	190.90.120.0/20	190.90.132.0/24
190.90.134.0/22	190.90.138.0/21	190.90.147.0/18	190.90.190.0/22	190.90.195.0/21
190.90.204.0/24	190.90.207.0/23	190.90.212.0/23	190.90.216.0/22	190.90.224.0/21
190.90.234.0/24	190.90.236.0/24	190.90.238.0/22	190.90.242.0/20	190.93.128.0/19
190.96.128.0/17	190.97.64.0/19	190.97.128.0/19	190.97.192.0/19	190.98.144.0/24
190.98.167.0/24	190.99.128.0/17	190.102.160.0/18	190.103.96.0/19	190.105.207.0/24
190.105.229.0/24	190.107.16.0/20	190.109.0.0/19	190.109.96.0/17	190.109.190.0/23
190.110.64.0/19	190.115.224.0/19	190.120.128.0/20	190.121.128.0/19	190.124.96.0/19
190.125.0.0/14	190.128.237.0/24	190.130.64.0/18	190.131.192.0/18	190.131.235.0/23
190.131.238.0/19	190.143.0.0/17	190.144.0.0/14	190.151.192.0/20	190.151.202.0/18

190.156.0.0/14	190.165.0.0/16	190.171.64.0/19	190.182.0.0/17	190.184.128.0/18
190.184.200.0/21	190.211.140.0/22	190.216.128.0/20	190.216.152.0/21	190.216.192.0/20
190.217.48.0/20	190.217.96.0/19	190.240.0.0/16	190.241.112.0/23	190.242.0.0/22
190.242.4.0/23	190.242.16.0/22	190.242.22.0/23	190.242.30.0/23	190.242.36.0/20
190.242.54.0/23	190.242.58.0/21	190.242.72.0/20	190.242.89.0/21	190.242.98.0/22
190.242.103.0/19	190.242.124.0/21	190.242.138.0/23	190.242.142.0/21	190.242.152.0/24
190.242.157.0/24	190.242.163.0/15	190.248.0.0/13	190.253.143.0/14	191.64.0.0/12
191.83.20.0/24	191.88.0.0/13	191.98.0.0/17	191.102.0.0/20	191.102.60.0/17
191.102.192.0/18	191.103.128.0/12	191.144.0.0/12	192.5.22.0/24	192.68.21.0/24
192.140.124.0/23	192.160.88.0/24	192.162.5.0/24	192.200.10.0/24	192.231.116.0/22
197.205.100.0/24	198.49.128.0/22	198.51.71.0/24	198.68.240.0/21	198.160.1.0/24
198.161.169.0/24	198.164.1.0/24	200.0.0.0/21	200.0.187.0/24	200.0.201.0/24
200.1.64.0/18	200.1.124.0/24	200.1.126.0/23	200.1.173.0/24	200.1.175.0/24
200.1.192.0/21	200.2.64.0/21	200.3.128.0/19	200.3.147.0/19	200.3.192.0/23
200.3.244.0/22	200.4.16.0/20	200.6.160.0/19	200.9.72.0/24	200.9.94.0/24
200.9.158.0/23	200.10.136.0/23	200.10.154.0/24	200.10.164.0/24	200.10.174.0/23
200.11.40.0/21	200.12.170.0/24	200.12.175.0/19	200.13.192.0/18	200.14.40.0/21
200.14.112.0/23	200.14.205.0/22	200.14.231.0/23	200.14.234.0/21	200.14.253.0/24
200.16.68.0/24	200.16.70.0/24	200.16.79.0/24	200.16.117.0/22	200.21.0.0/16
200.23.115.0/24	200.24.0.0/20	200.24.16.0/18	200.24.96.0/19	200.25.0.0/17
200.25.224.0/19	200.26.128.0/19	200.29.96.0/19	200.29.232.0/21	200.30.42.0/22
200.30.47.0/24	200.30.54.0/24	200.30.64.0/18	200.31.12.0/20	200.31.64.0/19
200.31.192.0/19	200.32.80.0/22	200.34.0.0/24	200.34.171.0/24	200.35.32.0/19
200.41.4.0/22	200.41.9.0/24	200.41.50.0/24	200.41.76.0/22	200.47.172.0/22
200.47.216.0/22	200.58.192.0/18	200.69.96.0/19	200.69.126.0/23	200.71.32.0/19
200.74.128.0/19	200.75.32.0/18	200.81.56.0/21	200.85.224.0/19	200.89.96.0/19
200.89.192.0/21	200.89.201.0/23	200.89.206.0/18	200.91.192.0/18	200.93.128.0/18

200.106.160.0/18	200.109.141.0/24	200.110.168.0/21	200.112.192.0/19	200.114.0.0/18
200.115.178.0/24	200.115.180.0/23	200.116.0.0/17	200.116.73.0/16	200.118.0.0/15
200.122.192.0/18	200.124.124.0/23	200.192.106.0/24	201.130.16.0/22	201.131.46.0/24
201.131.78.0/24	201.131.90.0/23	201.131.97.0/24	201.131.114.0/24	201.131.188.0/22
201.131.216.0/22	201.150.96.0/22	201.182.248.0/22	201.184.0.0/15	201.185.28.0/16
201.190.64.0/18	201.216.0.0/18	201.217.192.0/19	201.219.112.0/20	201.219.192.0/19
201.219.240.0/21	201.220.30.0/17	201.221.122.0/24	201.221.124.0/23	201.221.128.0/18
201.228.0.0/16	201.232.0.0/15	201.234.64.0/20	201.234.176.0/20	201.234.240.0/21
201.236.192.0/18	201.244.0.0/15	204.97.192.0/20	204.183.104.0/21	205.160.32.0/22
206.48.18.0/24	206.49.38.0/23	206.49.76.0/24	206.49.120.0/24	206.49.139.0/21
206.49.176.0/21	206.105.64.0/21	206.106.248.0/21	206.223.124.0/24	206.231.72.0/21
207.67.0.0/24	207.248.81.0/24	208.8.170.0/23	208.30.40.0/23	208.31.200.0/21
208.102.92.0/24	208.214.208.0/21	208.217.32.0/20	209.58.119.0/24	209.88.8.0/21
209.88.63.0/24	209.88.104.0/23	209.88.142.0/23	209.88.168.0/23	209.88.171.0/24
216.6.100.0/22	216.58.92.0/24	216.72.4.0/22	216.72.67.0/23	216.72.79.0/22
216.72.116.0/24	216.72.135.0/20	216.72.156.0/23	216.72.197.0/21	216.72.203.0/23
216.72.227.0/20	216.72.238.0/24	157.253.0.0 – 157.253.255.255	168.176.0.0 – 168.176.255.255	179.18.0.0 - 179.19.255.255
179.51.96.0 - 179.51.127.255	181.48.0.0 - 181.55.255.255	181.118.144.0 – 181.118.159.255	181.152.0.0 – 181.159.255.255	181.204.0.0 – 181.207.255.255
181.232.0.0 – 181.232.127.255	186.0.0.0 - 186.0.63.255	186.28.0.0 - 186.28.255.255	186.43.0.0 - 186.43.127.255	186.97.64.0 - 186.97.127.255
186.102.0.0 – 186.102.255.255	186.121.0.0 – 186.121.127.255	186.159.0.0 - 186.159.63.255	186.179.96.0 – 186.179.111.255	190.0.0.0 - 190.0.31.255
190.1.160.0 - 190.1.191.255	190.3.224.0 - 190.3.255.255	190.7.64.0 - 190.7.79.255	190.7.128.0 - 190.7.143.255	190.9.64.0 - 190.9.95.255
190.12.128.0 - 190.12.159.255	190.13.192.0 - 190.13.207.255	190.24.0.0 - 190.24.255.255	190.28.0.0 - 190.28.255.255	190.65.0.0 - 190.65.255.255
190.70.128.0 - 190.70.255.255	190.90.0.0 - 190.90.255.255	190.96.192.0 - 190.96.207.255	190.97.80.0 - 190.97.95.255	190.102.160.0 – 190.102.191.255
190.103.112.0 – 190.103.127.255	190.109.160.0 – 190.109.191.255	190.121.128.0 – 190.121.143.255	190.126.0.0 – 190.127.255.255	190.130.64.0 – 190.130.127.255

190.144.0.0 – 190.147.255.255	190.165.0.0 - 190.165.63.255	190.182.0.0 - 190.182.63.255	190.240.64.0 – 190.240.127.255	190.248.0.0 – 190.249.255.255
191.88.0.0 - 191.95.255.255	191.102.192.0 - 191.102.223.255	191.144.0.0 - 191.159.255.255	200.6.160.0 - 200.6.175.255	200.13.224.0 - 200.13.255.255
200.24.48.0 - 200.24.63.255	200.25.224.0 - 200.25.239.255	200.29.112.0 - 200.29.127.255	200.31.64.0 - 200.31.95.255	200.35.48.0 - 200.35.63.255
200.61.128.0 - 200.61.159.255	200.71.48.0 - 200.71.63.255	200.74.128.0 - 200.74.159.255	200.85.224.0 - 200.85.239.255	200.89.192.0 - 200.89.207.255
200.91.192.0 - 200.91.223.255	200.106.160.0 - 200.106.191.255	200.114.0.0 - 200.114.15.255	200.116.128.0 - 200.116.255.255	200.119.32.0 - 200.119.63.255
200.122.240.0 - 200.122.255.255	201.216.32.0 - 201.216.63.255	201.220.32.0 - 201.220.47.255	201.221.128.0 - 201.221.143.255	201.228.0.0 - 201.228.127.255
201.233.0.0 - 201.233.127.255	201.244.0.0 - 201.244.255.255			

Fuente: elaboración propia

En la página Scans / My Scans, seleccione New Scan. Aparecerá la página Scan Library.

Seleccione la plantilla Advance Scan

Configure el escaneo utilizando los enlaces Basic, Discovery, Assessment, Report y Advanced

Seleccione la opción Credentials

DIgite el usuario y contraseña

Seleccione la opción Compliance

- *Seleccione las opciones aplicables*
- *Seleccione la opción Plugins*
- *Seleccione los plugins aplicables*
- *Haga clic en Save y posteriormente en Launch para lanzar el escaneo*

Para realizar un escaneo de vulnerabilidades sin credenciales, desde la red externa, se deberán realizar las siguientes actividades:

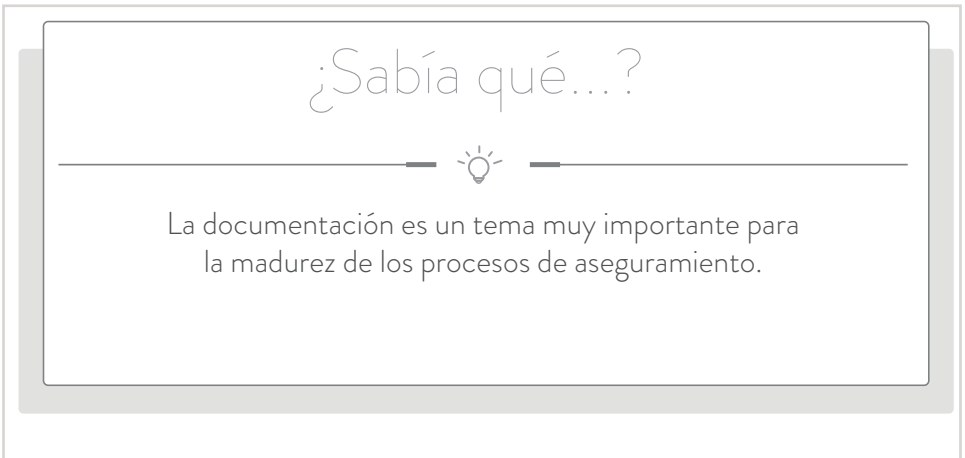
- *Abra la herramienta Nessus Tenable (Tenable, 2016)*
- *Ingrese su usuario y contraseña*

- *Confirme que el equipo desde el cual ejecutará el escaneo tiene configurada una dirección pública en Colombia, es decir que pertenezca a alguno de los siguientes rangos de IP pero no haga parte del rango de la IP públicas referenciados en la Tabla 1.*
- *En la página Scans / My Scans, seleccione New Scan. Aparecerá la página Scan Library.*
- *Seleccione la plantilla Advance Scan*
- *Configure el escaneo utilizando los enlaces Basic, Discovery, Assessment, Report y Advanced*
- *Seleccione la opción Compliance*
- *Seleccione las opciones aplicables*
- *Seleccione la opción Plugins*
- *Seleccione los plugins aplicables*
- *Haga clic en Save y posteriormente en Launch para lanzar el escaneo*

Evidentemente el nivel de detalle y tecnicismo es mucho mayor en el manual, por lo que el tamaño de igual manera se incrementa significativamente.

4. Recomendaciones

Veamos algunas recomendaciones finales a la hora de redactar la documentación de seguridad en el ciclo de desarrollo de software:



- Esté 100% seguro de lo que va a escribir, si usted no se lo cree, los demás menos lo harán.
- Trate de redactar eficaz y eficientemente:
  - Calidad Vs Cantidad
  - Póngase en los zapatos de quien leerá los documentos: cargo, profesión, experiencia, conocimientos
- Adaptese a la cultura de las organizaciones:
  - Algunas compañías no les gusta "llenarse" de documentos: Política y Procedimiento.
  - Algunas compañías no les gusta el papel: todo digitalizado.

Escribir en positivo o en negativo, dependiendo de la postura de la empresa.

Referencias

Tenable. (2016). *Nessus Tenable (Tenable, 2016) 6.8 User Guide*. Recuperado de https://static.tenable.com/prod_docs/Nessus Tenable (Tenable, 2016)_6.8_User_Guide.pdf

INFORMACIÓN TÉCNICA

FACULTAD DE
INGENIERÍA, DISEÑO
E INNOVACIÓN

Módulo: Seguridad en el Ciclo de Desarrollo

Unidad 4: Políticas sobre la seguridad en el ciclo de desarrollo en la empresa

Escenario 8: Procedimiento y manual técnico de seguridad en el ciclo de desarrollo

Autor: Miguel Ángel Zambrano Puentes

Asesor Pedagógico: Edwin Mojica Quintero

Diseñador Gráfico: Brandon Steven Ramírez Carrero

Asistente: Ginna Quiroga

Este material pertenece al Politécnico Grancolombiano. Por ende, es de uso exclusivo de las Instituciones adscritas a la Red Ilumno. Prohibida su reproducción total o parcial.