AGENCIA PARA LA REINCORPORACIÓN Y NORMALIZACIÓN (ARN)

GUÍA DE GESTIÓN DE VULNERABILIDADES

BOGOTÁ D.C. JUNIO DE 2021

Tabla de contenido

1. OBJETIVO GENERAL 3
2. OBJETIVOS ESPECÍFICOS 3
3. ALCANCE 3
4. DEFINICIONES 3
5. JUSTIFICACION 9
6. COMPONENTES PRINCIPALES DE LA GESTIÓN DE VULNERABILIDADES 9
6.1 ANÁLISIS DE VULNERABILIDADES 9
6.2 PRUEBAS DE PENETRACIÓN (PENTEST) 10
6.3 METODOLOGÍA 13
7. RECURSOS NECESARIOS 14
7.1 EQUIPO DE TRABAJO 14
7.2 HERRAMIENTAS 15
7.3 REQUERIMIENTOS 15
8. ENTREGABLES 16
9. CRONOGRAMA 16

1. OBJETIVO GENERAL

Identificar el nivel de exposición a vulnerabilidades en los sistemas operativos, servicios y aplicaciones mediante pruebas de penetración y vulnerabilidades sobre los dispositivos de la infraestructura tecnológica de la ARN.

2. OBJETIVOS ESPECÍFICOS

- Garantizar el cubrimiento total y análisis de los dispositivos definidos por la ARN, los cuales componen su infraestructura.
- Realizar acompañamiento en la remediación de las vulnerabilidades resultantes del análisis realizado a los dispositivos definidos por la ARN, los cuales hacen parte de su infraestructura.
- Generar la respectiva matriz con la identificación de las vulnerabilidades detectadas, recomendaciones y gestión correspondiente.

3. ALCANCE

Realizar el análisis de vulnerabilidades basado en el cronograma de ejecución previamente presentado y aprobado por la ARN, a los dispositivos definidos por la entidad, presentando informes técnicos y gerenciales con los resultados encontrados sobre los activos de TI objeto de los análisis incluyendo recomendaciones y remediación correspondiente.

4. DEFINICIONES

ACTIVE DIRECTORY: Active Directory o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadoras

ACTIVO DE INFORMACIÓN: Es todo recurso que genera, procesa, transporta y/o resguarda información necesaria para la operación y el cumplimiento de los objetivos del BCE, por lo tanto, se requiere proteger su confidencialidad, integridad y disponibilidad de las amenazas propias de su naturaleza y características.

ANALÍSTA DE CIBERSEGURIDAD: Encargado de planificar, implementar, mejorar, o monitorean medidas de seguridad para proteger las redes de computadoras y la información.

ATAQUE DE MOVIMIENTO LATERAL: Son técnicas de ataques de hackers informáticos que son utilizadas para propagarse a través de una red buscando assets e información clave

BACKDOOR: Un backdoor o puerta trasera, es un tipo de virus diseñado para dar acceso a usuarios maliciosos al control de un equipo infectado de manera remota. Estas “puertas traseras” permiten al usuario malicioso controla el equipo infectado, pudiendo enviar y recibir archivos, ejecutarlos o eliminarlos, mostrar mensajes, borrar o robar datos, reiniciar el equipo, etc. Es decir, puede controlar el equipo como si estuviese sentado delante de él y a los mandos.

BSOD (Blue Screen Of Death): La llamada pantalla azul de la muerte o pantallazo azul hace referencia a la pantalla mostrada por el sistema operativo Microsoft Windows cuando no puede recuperarse de un error del sistema

CENTRO DE OPERACIONES DE SEGURIDAD - SOC: encargado de monitorear la seguridad informática del cliente y generar alertas y eventos en caso de que se identifique situaciones que afecten la seguridad del cliente

CLIENTE/SERVIDOR: La arquitectura cliente/servidor es un modelo de diseño de software en el que las tareas se reparten entre los proveedores de recursos o servicios, llamados servidores, y los demandantes, llamados clientes. Un cliente realiza peticiones a otro programa, el servidor, quien le da respuesta.

CONSECUENCIAS: Es todo hecho o evento derivado o que resulta inevitable posterior a una vulnerabilidad explotada.

CVSS (Common Vulnerability Scoring System): Es un sistema (métrica) de score con el que poder medir el impacto que una vulnerabilidad puede tener si es explotada.

DISPOSITIVO DE SEGURIDAD PERIMETRAL: Es todo tipo de herramientas y técnicas de protección informática que tienen como propósito establecer una línea de defensa relacionada con la red interna y toda la prolongación que forma parte del entorno bajo el que se encuentra la tecnología de la información de una empresa.

DOMINIO: Un nombre de dominio (a menudo denominado simplemente dominio) es un nombre fácil de recordar asociado a una dirección IP física de Internet. Se trata del nombre único que se muestra después del signo @ en las direcciones de correo y después de www. en las direcciones web.

DoS: Un ataque de denegación de servicio, llamado también ataque DoS, es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos.

EQUIPOS INFORMÁTICOS: Son equipos que permiten almacenar y procesar información.

ESCANEO: Es la identificación, análisis y reporte de vulnerabilidades (entendida como una falla que permite que una amenaza se convierta en un riesgo).

ESPECIALISTA: Persona encargada de desarrollar periódicamente tareas de pentest (penetration testing) y todo tipo de ataque ético (Ethical Hacking) con el fin de identificar y medir vulnerabilidades eliminando los falsos positivos.

ETHICAL HACKING O PENTEST: Utilizado para explotar las vulnerabilidades existentes en el sistema que se requiere evaluar, valiéndose de un test de intrusión, que permite verificar y evaluar la seguridad física y lógica de sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, entre otros componentes de la infraestructura tecnológica, con la intención de ganar acceso y demostrar que un sistema es vulnerable.

EXPLOIT: En el ámbito de la informática es un fragmento de software, fragmento de datos o secuencia de comandos o acciones, utilizada con el fin de aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

EXPLOTACIÓN: Es el aprovechamiento de una debilidad o una brecha de seguridad. También es entendido como un código, método o vía, que permite a un atacante informático o a un auditor de seguridad, explotar una vulnerabilidad conocida, para poder comprometer la seguridad de un sistema informático, y tomar posesión y control de este.

FALSOS POSITIVOS: Detección de errores o defectos presentados por inestabilidad del sistema, bases de datos corruptas o por alguna causa externa que haga que el entorno no esté funcionando como debería.

FIREWALL: En informática, un Firewall o cortafuegos es la parte de un sistema informático o una red informática que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Los cortafuegos. pueden ser implementados en hardware o software, o en una combinación de ambos.

GHDB: Es un índice de consultas de búsqueda que se utiliza para encontrar información disponible públicamente, destinado a pentesters e investigadores de seguridad.

HALLAZGO DE SEGURIDAD: Vulnerabilidad encontrada en los activos de información y sistemas objeto de los ejercicios de escaneo de vulnerabilidades y ethical hacking.

HTTPS: El Protocolo seguro de transferencia de hipertexto es un protocolo de aplicación basado en el protocolo HTTP, destinado a la transferencia segura de datos de hipertexto, es decir, es la versión segura de HTTP.

INCIDENTE: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

LAN (Red de área local): son un conjunto de dispositivos electrónicos conectados entre sí que comparten una línea de comunicación común o un enlace inalámbrico con un servidor.

LÍDER DE SERVICIO: Profesional designado por la ARN el cual es responsable de la correcta funcionalidad de los servicios y activos de información de la entidad.

MITIGACIÓN: Es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

MEDIOS PÚBLICOS: Son todos los servicios de la ARN que se encuentran expuestos en internet.

NCSC (National Computer Security Council): Consejo Nacional de Seguridad Informática

NERC (North American Electric Reliability Corp): Conjunto de estándares que abordan la seguridad de ciber activos esenciales para la operación confiable del sistema eléctrico.

NIST (National Institute of Standards and Technology): El Marco de Ciberseguridad del NIST ayuda a los negocios de todo tamaño a

comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos.

NIVEL DE RIESGO ASOCIADO: Probabilidades de que ocurran eventos adversos en una infraestructura, así como sus consecuencias.

OSSTMM (Open Source Security Testing Methodology Manual): Es una metodología que reúne las diversas pruebas y métricas de seguridad, utilizadas por los profesionales durante las Auditorías de Seguridad.

OWASP (Open Web Application Security Project): Es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.

PENETRACIÓN CAJA BLANCA: En este tipo de pruebas, los pentesters o analistas de ciberseguridad tienen total conocimiento del funcionamiento interno del sistema, y trabaja con información que puede tener acceso uno o varios empleados dentro de la organización.

PENETRACIÓN CAJA GRIS: En este tipo de pruebas, los pentesters o analistas de ciberseguridad pueden tener conocimiento sobre algunos aspectos del funcionamiento del sistema y de otros no.

PENETRACIÓN CAJA NEGRA: En este tipo de pruebas, los pentesters o analistas de ciberseguridad no tienen conocimiento del funcionamiento interno del sistema, y trabaja con la información que puede conseguir por sus propios medios, igual que lo podría hacer un delincuente informático.

PLAN DE REMEDIACIÓN: Permite identificar los riesgos asociados a cada vulnerabilidad reportada, así como definir los controles que deben ser implementados para mitigar dichos riesgos.

POST EXPLOTACIÓN: Es una serie de pasos que se deben seguir posterior a la obtención de penetración en un sistema, estos pasos consisten en entendimiento de la víctima, escalamiento de privilegios, eliminación de logs y procesos de monitorización, recolección de información, establecimiento de puertas traseras, movimiento lateral.

PRUEBAS DE PENETRACIÓN (PENTEST): Una prueba de penetración, o pentest, es un ataque a un sistema informático con la intención de encontrar las debilidades de seguridad y todo lo que podría tener acceso a ella, su funcionalidad y datos. El proceso consiste en identificar el o los sistemas del objetivo.

PRUEBAS DE VULNERABILIDAD: Las pruebas de vulnerabilidades (también llamadas evaluación de vulnerabilidades o en inglés," Vulnerability Assessment") son un tipo de prueba de software que se realiza para evaluar los riesgos de seguridad de un software con el fin de reducir la probabilidad de amenazas y futuros ataques que puedan explotar las vulnerabilidades de dicho software.

PUNTO DE RED: Un punto de conexión es un lugar físico donde la gente puede acceder a Internet, habitualmente por medio de Wi-Fi, vía una red de área local inalámbrica (WLAN) con un enrutador conectado a un proveedor de servicio de Internet

RECONOCIMIENTO: Es la fase de preparación donde el atacante obtiene toda la información necesaria de su objetivo y/o víctima antes de lanzar un ataque.

RED DE SERVIDORES DE DESARROLLO: Es el espacio de trabajo donde el programador desarrolla el código de la aplicación, realiza pruebas iniciales y comprueba si la aplicación se ejecuta correctamente con ese código.

RED DE SERVIDORES DE PRODUCCIÓN: El entorno de producción es el entorno donde finalmente se ejecuta la aplicación donde acceden los usuarios finales y donde se trabaja con los datos de negocio en sí mismos.

REMEDIACIÓN: Acción que permite minimizar el impacto de las vulnerabilidades en la organización.

SEGMENTO DE RED: Refiere a un LAN el cual hace referencia a un conjunto o agrupación de varios equipos (computadoras y/o periféricos que están conectados entre sí en una red, a través de realizar una segmentación de red se obtienen ventajas de aumento en el rendimiento y favorece la seguridad.

SISTEMAS DE INFORMACIÓN: Es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo.

SMTP: Es una abreviatura para **Simple Mail Transfer Protocol** y se encarga de los correos salientes. Este protocolo permite a aplicaciones transmitir mensajes a través de Internet.

SNMP (Simple Network Management Protocol): Es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Los dispositivos que normalmente soportan SNMP

incluyen routers, switches, servidores, estaciones de trabajo, impresoras, bastidores de módem y muchos más.

SQL (Structured Query Language): En español, lenguaje de consulta estructurada) es un lenguaje de dominio específico utilizado en programación, diseñado para administrar, y recuperar información de sistemas de gestión de bases de datos relacionales.

SUBDOMINIO: Un subdominio es un subgrupo o subclasificación del nombre de dominio el cual es definido con fines administrativos u organizativos, que podría considerarse como un dominio de segundo nivel. Normalmente es una serie de caracteres o palabra que se escriben antes del dominio.

SYSLOG: Es un estándar de facto para el envío de mensajes de registro en una red informática IP. Por syslog se conoce tanto al protocolo de red como a la aplicación o biblioteca que envía los mensajes de registro.

VLAN: Una VLAN, acrónimo de virtual LAN, es un método para crear redes lógicas independientes dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física.

VULNERABILIDAD: Es una debilidad o deficiencia de seguridad, que puede ser materializada por una amenaza.

5. JUSTIFICACION

La gestión de vulnerabilidades es un proceso continuo de TI consistente en la identificación, evaluación y corrección de vulnerabilidades en los sistemas de información y las aplicaciones de una organización, que, de acuerdo con las buenas prácticas, atraviesa por un ciclo de vida desde que el error se encuentra, se identifica y se genera; hasta que es completamente eliminado y controlado, ofreciendo a las empresas un medio rentable para proteger las infraestructuras de TI fundamentales frente a las fallas de seguridad.

6. COMPONENTES PRINCIPALES DE LA GESTIÓN DE VULNERABILIDADES

6.1 ANÁLISIS DE VULNERABILIDADES

Para la ejecución de las pruebas de análisis de vulnerabilidades, se tendrá como referencia el siguiente enfoque que permite determinar metodológicamente como realizarlas a sistemas operativos, aplicaciones, redes inalámbricas y/o Infraestructuras críticas.

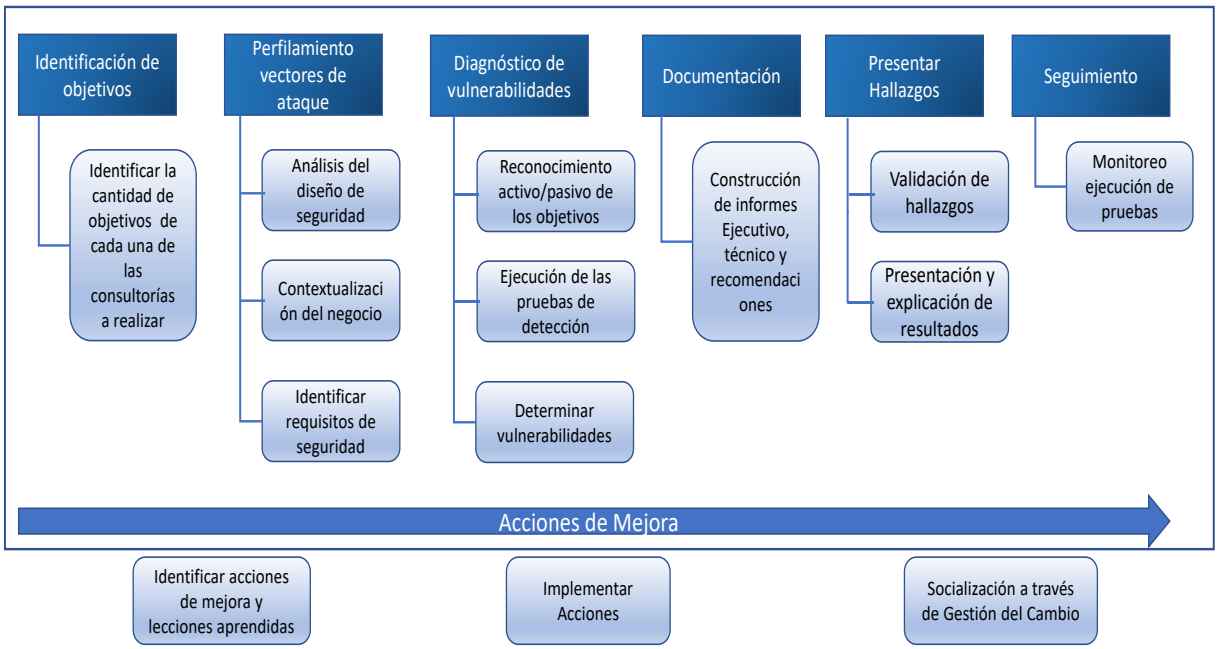

Gráfico 1 Distribución. Fuente SOC

El análisis de vulnerabilidades se realiza con el uso de herramientas para la detección de las mismas con el apoyo especialistas que permitan tipificar los resultados eliminando los falsos positivos. El servicio de análisis de vulnerabilidades se diferencia del Ethical Hacking por la fase de explotación la cual requiere el uso de varias herramientas y el conocimiento del especialista para su ejecución.

Finalizados los ejercicios, se entregará un informe ejecutivo y la respectiva matriz de vulnerabilidades que contiene la información detallada de los hallazgos de seguridad detectados, el nivel de riesgo asociado para el seguimiento de las mismas, al profesional especializado en seguridad y redes de la ARN.

6.2 PRUEBAS DE PENETRACIÓN (PENTEST)

Pruebas de penetración (Pentest) es un conjunto de pruebas de seguridad, en donde un profesional de seguridad ejecuta ataques reales, así como utilizar técnicas especializadas para la detección y explotación de vulnerabilidades que poseen los activos de TI de una organización.

En este servicio el especialista toma el rol de un atacante real que busca explotar y aprovecharse de las vulnerabilidades detectadas para penetrar los sistemas y obtener información de carácter confidencial para la organización.

Al finalizar la ejecución de las pruebas, se entrega un reporte a nivel técnico y ejecutivo que contiene la información detallada de los hallazgos de seguridad detectados, el nivel de riesgo asociado, el escenario de riesgo (posibles consecuencias), las respectivas recomendaciones para la mitigación del hallazgo de seguridad y una evidencia de la explotación de la vulnerabilidad.

Ambiente: Externo
Tipo Prueba: Penetración de Caja Negra

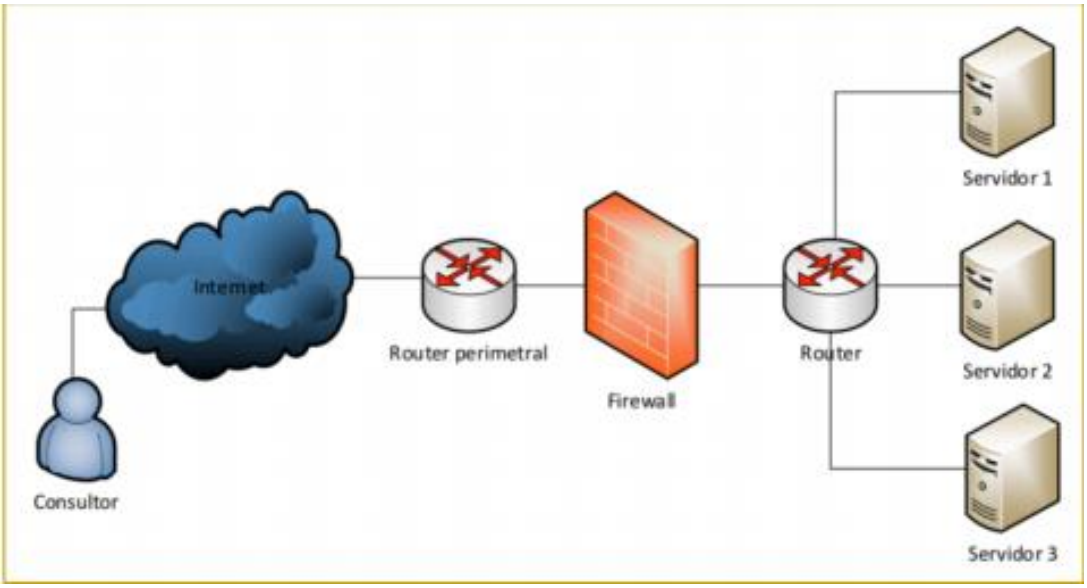

Gráfico 2 Diagrama Caja Negra. Fuente SOC

Las pruebas son realizadas por los especialistas desde cualquier punto fuera de la infraestructura de TI. El objetivo de este tipo de pruebas es simular el accionar de un atacante remoto hacia los activos tecnológicos de la infraestructura de TI, que se encuentran expuestos en Internet. Este tipo de pruebas permite valorar la visibilidad que tiene el atacante externo y el impacto asociado a la explotación de las vulnerabilidades detectadas.

Los especialistas no reciben ningún tipo de información sobre los sistemas informáticos y activos, por lo que se trabaja con la información que se pueda recolectar a través de medios públicos. Este tipo de pruebas son realizadas desde fuera de las instalaciones de la Entidad.

Ambiente: Interno
Tipo de Prueba: Penetración Caja Gris

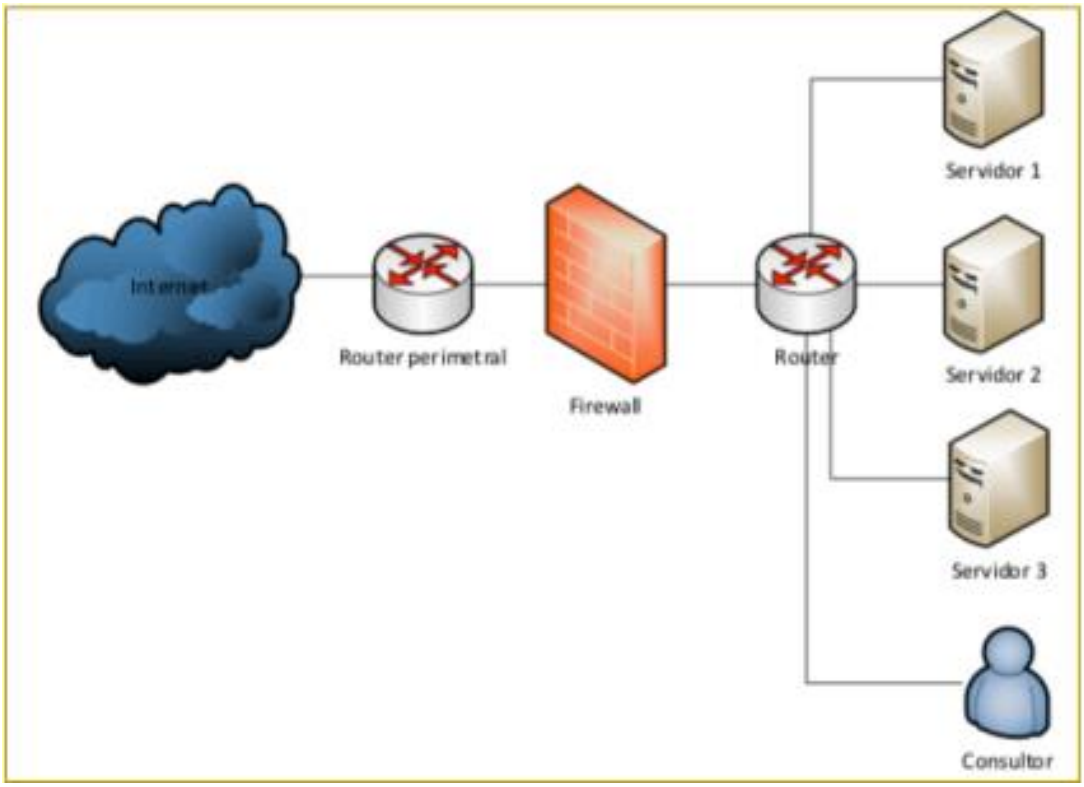

Gráfico 3 Diagrama Caja Gris. Fuente SOC

El objetivo de estas pruebas es el de medir el daño que podría causar un atacante que se encuentre dentro de la red interna. Para llevar a cabo las pruebas internas, los especialistas se sitúan en una estación de trabajo de la Entidad y suministrándole acceso a la red interna.

En coordinación con la Entidad se puede simular un atacante interno que posee acceso a la red de usuarios administrativos, a la red de servidores de desarrollo, red de servidores de producción, entre otros. Generalmente, las pruebas internas son las que obtienen mayores hallazgos de seguridad, además que sirven para evaluar el accionar, la efectividad y el tiempo de reacción ante el manejo de incidentes por parte del personal que integre el equipo de atención de incidentes de seguridad.

6.3 METODOLOGÍA

Para la ejecución de las pruebas, se tendrá como referencia el siguiente enfoque que permite determinar metodológicamente la realización de las pruebas independientemente si se trata de unas pruebas internas/Externas a sistemas operativos, aplicaciones, redes inalámbricas y/o Infraestructuras críticas.

Gráfico 4 Metodología. Fuente SOC

6.3.1 Reconocimiento

En esta fase se busca la recolección de la mayor cantidad de información a través de medios públicos y servicios expuestos que no interactúen de manera directa con la organización a evaluar, tales como sitios públicos de internet, redes sociales y GHDB. También se hace la identificación de dominios, subdominios, Reconocimiento, Escaneo, Explotación, Post Explotación, Generación de Reporte segmentos de red y servicios de correo recopilación de información con técnicas como Trashing, Shoulder surfing, tailgating, Phishing y Fake AP.

6.3.2 Escaneo

Una vez identificados los activos pertenecientes a la Entidad y que se encuentren dentro del alcance, los especialistas realizan la ejecución de técnicas con el uso de herramientas que permitan identificar activos expuestos, tales como: servidores, sistemas operativos, puertos, versiones de servicios, aplicaciones web, portales de autenticación, entre otros. También, durante esta etapa, se realizará el escaneo y análisis de vulnerabilidades asociadas a los activos encontrados, la validación de los hallazgos y la investigación de las vulnerabilidades, las cuales se alojan en la ruta compartida \\acr.int\Data\EVIDENCIAS_VULNERABILIDADES

6.3.3 Explotación

Después de descartar los falsos positivos, y de identificar información asociada a los mecanismos de explotación de las vulnerabilidades detectadas, se analiza la posibilidad de la explotación de cada hallazgo, con el objetivo de evitar alteraciones e interrupciones no deseadas en los activos evaluados (DoS, BSOD). Al finalizar la evaluación anterior, los especialistas realizan la ejecución de las exploits para aprovecharse de las vulnerabilidades previamente detectadas y que no representen un riesgo de afectación a la disponibilidad de los servicios.

6.3.4 Post Explotación

Esta etapa fue definida para simular un ataque, aprovechando el acceso logrado a los sistemas y servicios, tal como un atacante lo haría. Algunas de las técnicas y ataques ejecutadas en esta etapa son: Ataques de movimiento lateral, búsqueda de información sensible, recuperación de credenciales, compromiso de la infraestructura de Active Directory. Al finalizar la simulación del ataque, se realiza el proceso de borrado de backdoors y herramientas desplegadas en los sistemas y servidores comprometidos, así como la eliminación de usuarios añadidos.

6.3.5 Generación de Reporte

Debido a la importancia del reporte, se definió esta etapa para la generación de los reportes técnico y ejecutivo. El reporte técnico contiene información sobre el alcance de las pruebas, los activos que se evaluaron, la metodología empleada, los detalles técnicos de hallazgos de seguridad, recomendaciones de para la mitigación de las vulnerabilidades, la evidencia de la intrusión y las conclusiones. Mientras que el reporte ejecutivo contiene un breve resumen, evitando utilizar lenguaje técnico, sobre los activos evaluados, los hallazgos más relevantes de seguridad, evidencias de intrusión y conclusiones.

6.3.6 Remediación de Vulnerabilidades

Con base en los reportes técnicos de escaneo de Vulnerabilidades y Pentest, se debe realizar la remediación, por parte de los administradores de las plataformas de la ARN, de las vulnerabilidades reportadas.
Para lo anterior, el SOC creará un caso padre en la herramienta de gestión, asociando a este los casos hijo respectivos, estos casos hijo serán agrupados dependiendo de la vulnerabilidad encontrada (críticas, altas y medias), para posteriormente generar el caso con esta categoría y asignar al administrador de la plataforma encargado de la mitigación de las vulnerabilidades, una vez creados y asignados los casos, el SOC comunicará a la supervisión del contrato y al oficial de seguridad informática de la ARN los casos creados.

7. RECURSOS NECESARIOS

7.1 EQUIPO DE TRABAJO

Los servicios propuestos serán ejecutados por el equipo de especialistas y analistas de ciberseguridad con experiencia en gestión de vulnerabilidades, Ethical Hacking, análisis forense quienes validan otras variables del entorno para complementar los planes de mitigación existentes de forma real y eficiente.

La gestión de vulnerabilidades se realiza con los siguientes recursos cuya dedicación se articula con el cronograma acordado:

- Líder del servicio ARN: Aprueba los Informes y coordinará los recursos.
- Especialistas (SOC): Realizan la ejecución del servicio de forma remota. En caso de ser necesario se trasladará un recurso a sitio para validaciones o pruebas particulares. Serán los responsables de generar los informes técnico y gerencial en el cual se relacionan las vulnerabilidades encontradas.
- Responsable calidad SOC: Realiza el aseguramiento de calidad de los informes técnico y gerencial donde se relacionan las vulnerabilidades encontradas, antes de presentarlo al Líder del Servicio.

7.2 HERRAMIENTAS

La solución tecnológica utilizada para el análisis de vulnerabilidades, debe cumplir con los siguientes criterios como mínimo:

- Estar basada en estándares de seguridad como OSSTMM, OWASP, NCSC, NIST, NERC, entre otros
- Ser accedida utilizando navegador web o aplicación cliente/servidor.
- Estar integrada como mínimo por dos herramientas con el fin de reducir la identificación de falsos positivos.
- La administración de usuarios debe ser ilimitada basada en roles.
- Permitir la creación de colecciones o grupos de activos y diferenciación de perfiles de evaluación para programar escaneos periódicos (internos y externos) sin que impacte la red de la entidad.
- Generar tendencias de vulnerabilidades sobre grupos de activos en diferentes escalas de tiempo.
- Clasificación automática de riesgos críticos usando una escala de 1,0-10,0, según CVSS, adaptado a sus parámetros y modificaciones
- Permitir la integración flexible vía Syslog, SNMP, SMTP, SQL, HTTPS entre otros.

7.3 REQUERIMIENTOS

7.3.1 Pruebas a infraestructura TI.

Es necesario contar con los siguientes requerimientos antes de ejecutar la actividad:

Pruebas de Vulnerabilidad

- Socializar la prueba con los dueños de los activos o servicios de TI de la ARN, para las pruebas de vulnerabilidades.
- Utilizar un equipo de cómputo donde se instalará el sensor del scan para la ejecución.
- Garantizar conectividad a nivel de red en las diferentes Vlan de los activos y en caso de contar con dispositivos de seguridad perimetral sobre las redes de la ARN, realizar las respectivas reglas de exclusión para garantizar su alcance.
- Pruebas de Penetración (Pentest)
- Para pruebas internas se requiere puntos de red para dar conectividad a los especialistas del SOC que ejecutarán las pruebas y acceso al segmento de red de los servidores a evaluar. En caso de Caja Blanca, contar con el usuario con nivel de consulta.
- Para Pruebas Externas: En caso de Caja Blanca, contar con un usuario de red que posea nivel de consulta.

8. ENTREGABLES

Para los servicios de análisis de vulnerabilidades y Pentest se presentan los siguientes informes:

Entregable	Descripción	Servicio	
		Vulnerabilidades	Pentest
Matriz de Vulnerabilidades	Se registran las vulnerabilidades vs los equipos afectados, permite hacer seguimiento de cierre de brechas de seguridad	Aplica	Aplica
Infiorme Ejecutivo	Archivo en formato pptx y realizar presentación ejecutiva con los resultados y recomendaciones más relevantes.	Aplica	Aplica
Informe Tecnico	Contiene descripción del escenario en el que se hicieron las pruebas, descripción de la vulnerabilidad, nivel de criticidad, equipos y puertos afectados, que principio de seguridad afecta (Integridad, Confidencialidad y Disponibilidad), recomendaciones, evidencias, información adicional.	N/A	Aplica

Gráfico 5 Documentos Entregables. Fuente SOC

9. CRONOGRAMA

Para el cubrimiento de los activos de la ARN descritos en el alcance se propone la ejecución de dos (2) ciclos de evaluación, sobre los cuales se realizará la fase de evaluación de vulnerabilidades, documentación de los hallazgos, informe técnico, informe ejecutivo y matriz de vulnerabilidades) y una presentación de los resultados al equipo de trabajo de la ARN.

En el primer ciclo se debe realizar el escaneo de vulnerabilidades a los activos de la infraestructura de la ARN definidos, desde la subred a la cual pertenecen, de tal forma que el firewall no presente bloqueos a nivel de red, de igual forma, al finalizar el ciclo uno, se deben realizar las pruebas de Pentest o Ethical Hacking, haciendo foco especifico a las provistas por la ARN, las cuales deben ser parte de su infraestructura.

Para el segundo ciclo de pruebas se debe realizar el escaneo de vulnerabilidades a los activos de la infraestructura de la ARN definidos desde una red de funcionarios, con esta prueba se pretende verificar los controles aplicados sobre las diferentes subredes a nivel de firewall. Posteriormente se debe realizar prueba de Pentest con base en los escenarios descritos anteriormente y acordado entre el SOC y el profesional de seguridad informática de la ARN.

Actividad	CICLO I						CICLO II					
	ene	feb	mar	abr	may	jun	jul	ago	sep	oct	nov	dic
	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4	Sem 1 - 4
Pruebas de vulnerabilidad												
Documentación												
Presentación de resultados												
Pruebas pentest externo												
Documentación												
Presentación de resultados												
Pruebas pentest interno												
Documentación												
Presentación de resultados												

Gráfico 6 Cronograma Actividades Fuente SOC