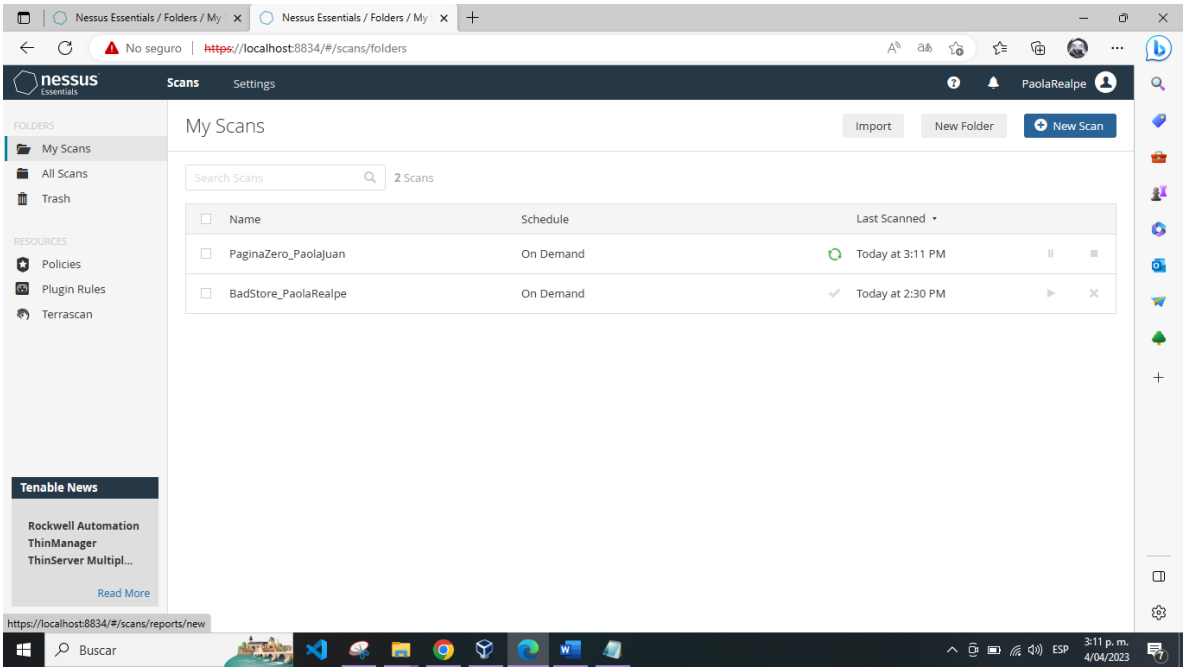
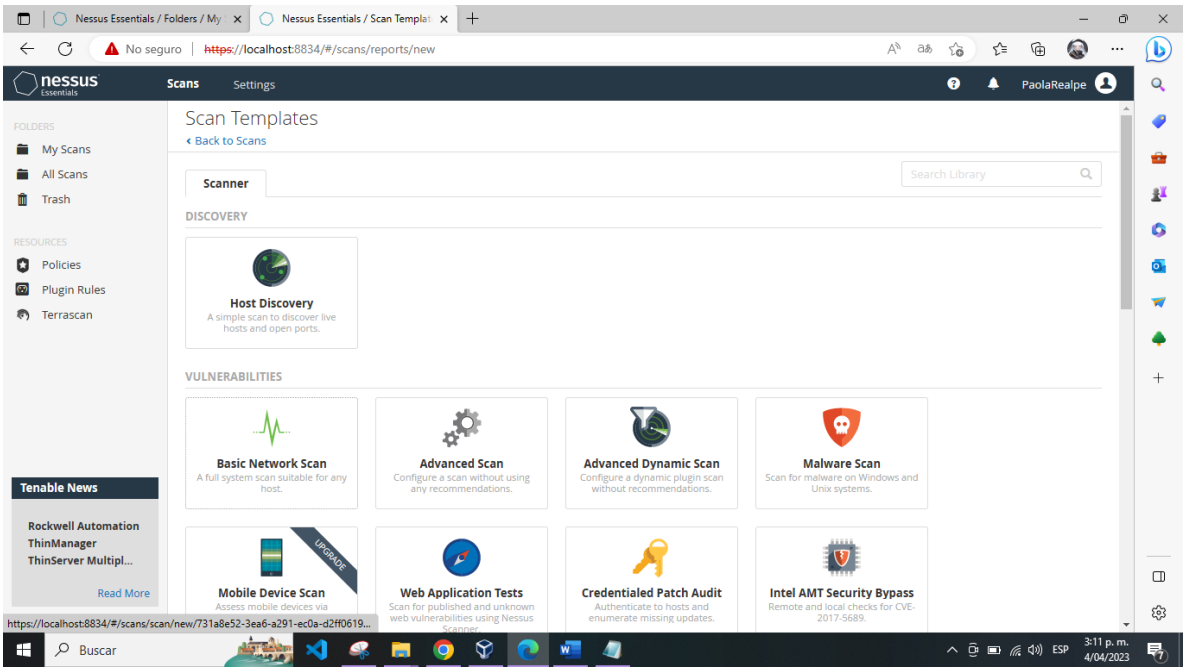
2 SITIO WEB CON FINES DE ESCANEO

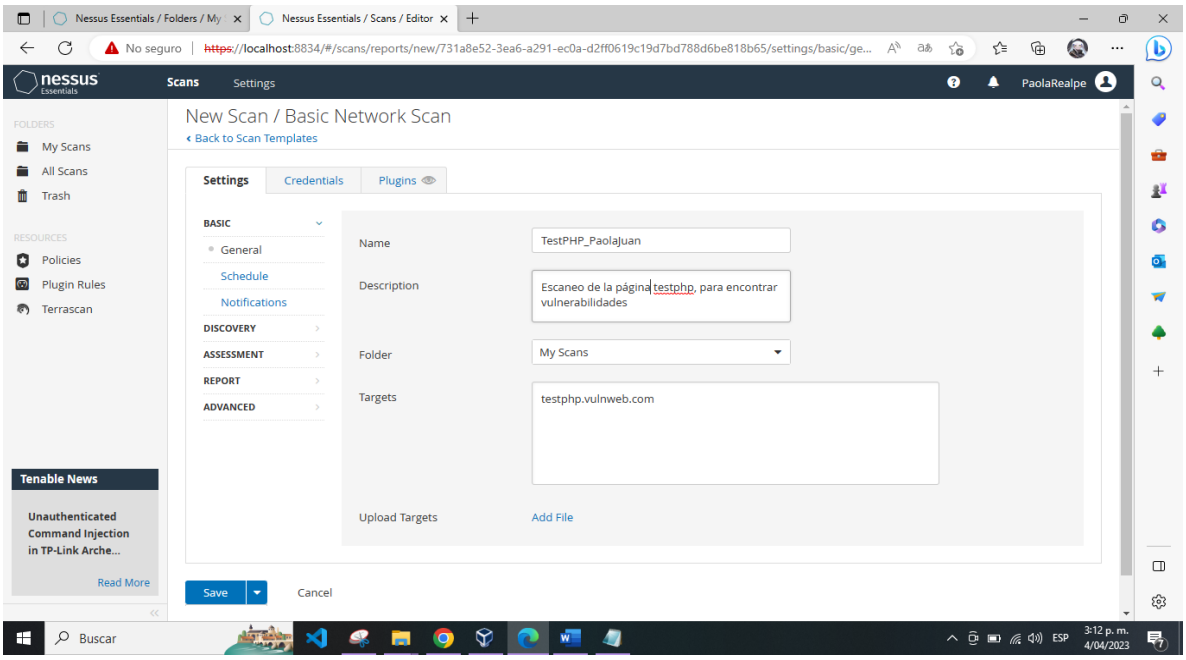
Se realiza otro escaneo de un sitio web por lo que nos vamos a la opción de **New Scan**



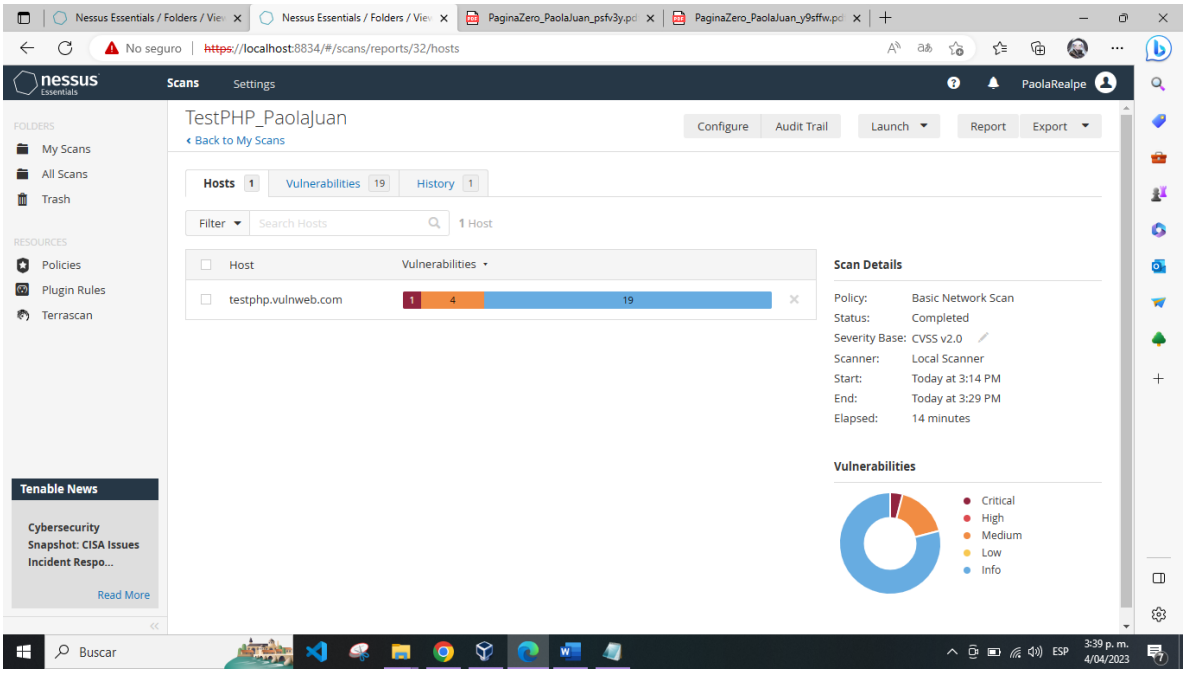
Nos ubicamos en la opción de un básico escaneo de red



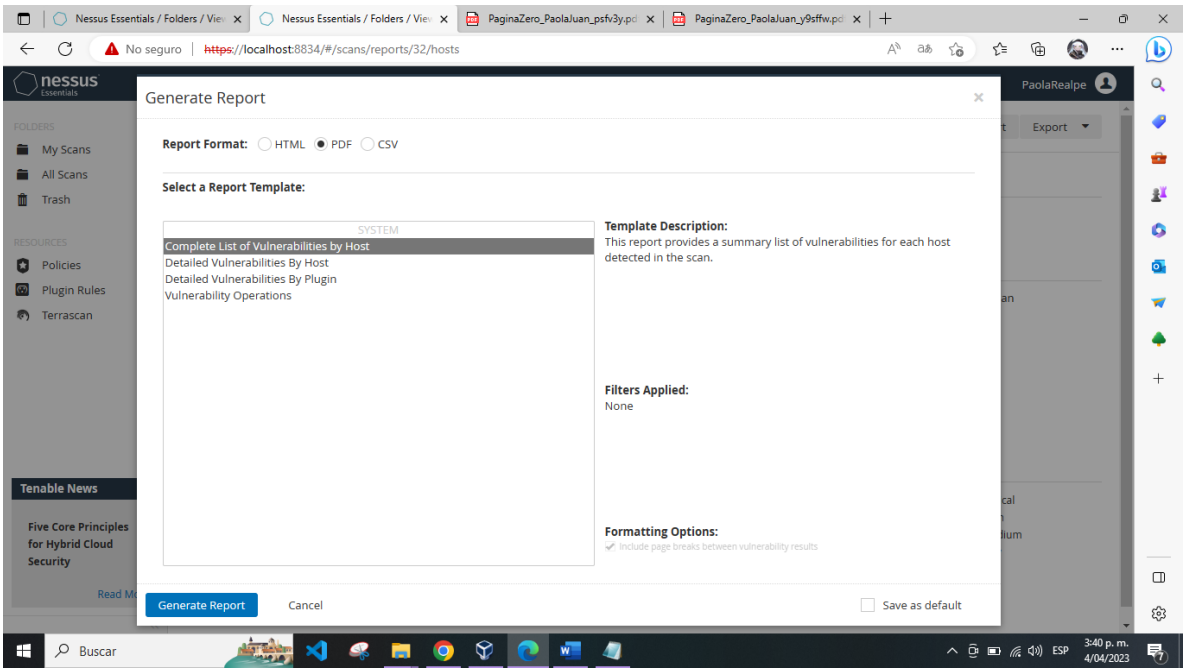
Agregamos un nombre que en este caso es **TestPHP_PaolaJuan**, una descripción y en la target escribimos el enlace para luego dar clic al botón S**ave**

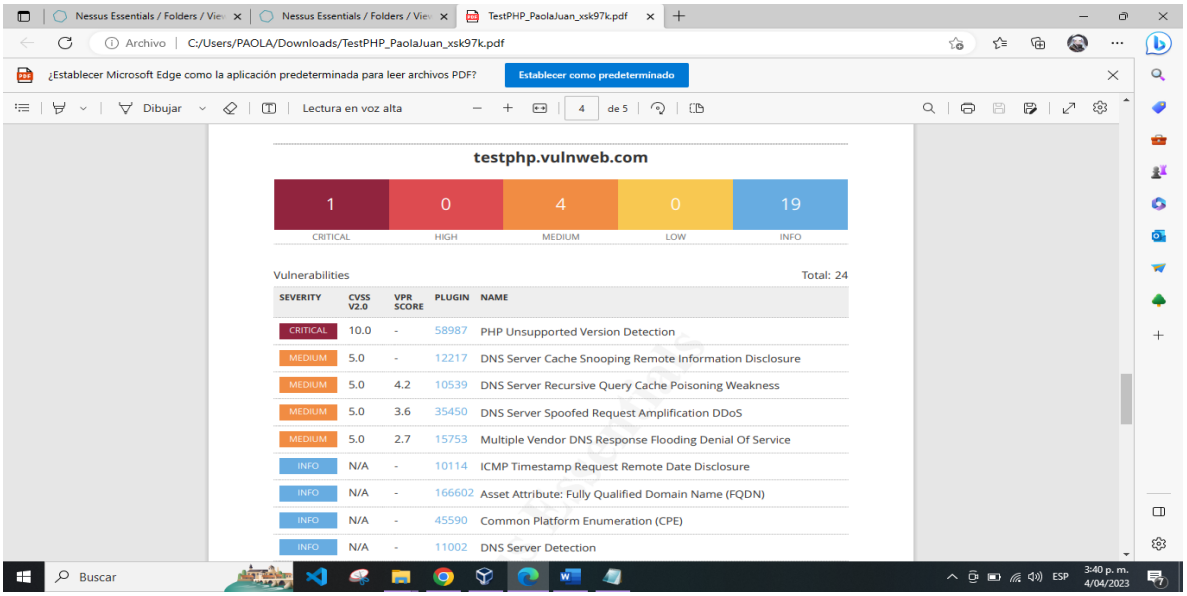


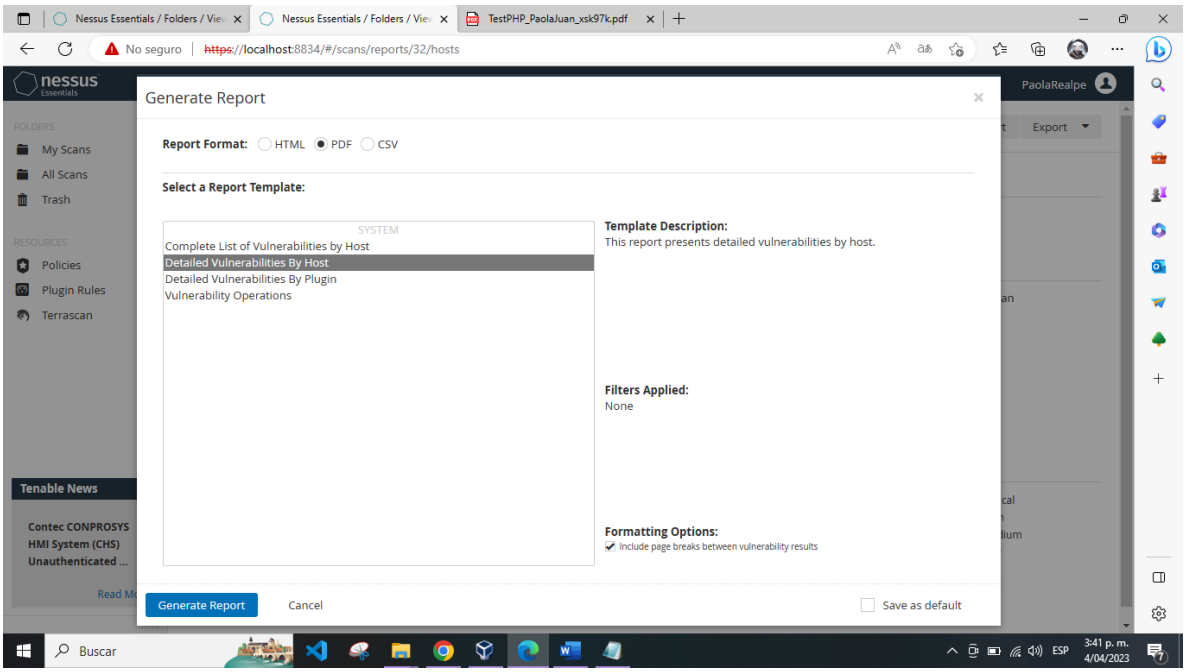
Se espera unos minutos para que termine el proceso de escaneo y luego podemos observar las vulnerabilidades encontradas

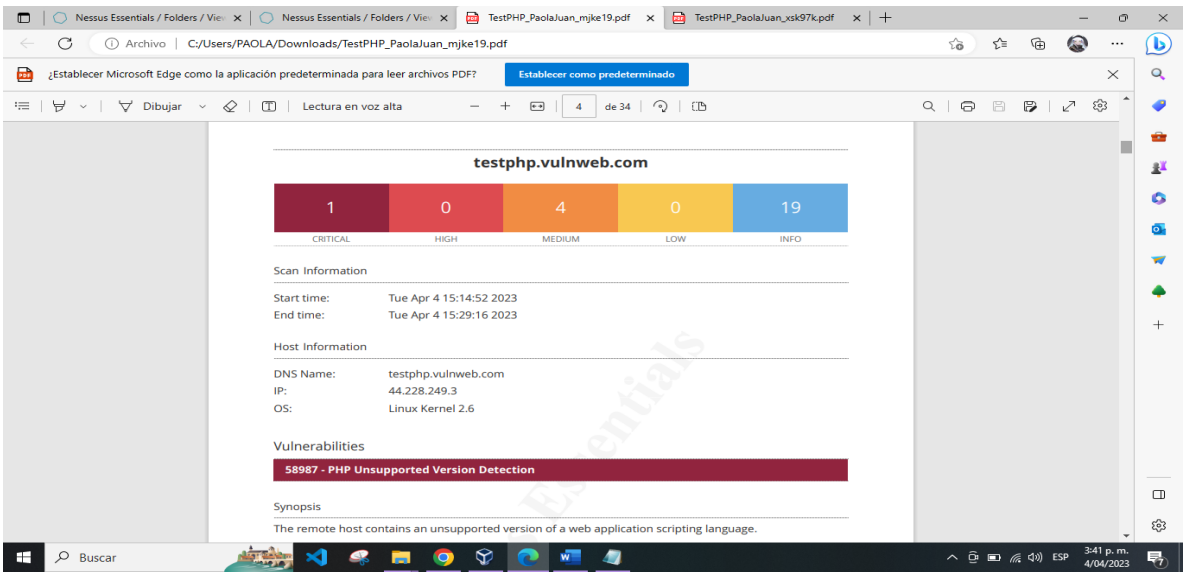


Descargamos los reportes ubicándonos en la parte superior y dando clic a la opción **Report** y los creamos dando un formato de PDF y seleccionando la opción de **Complete List** y luego se realiza los mismos pasos, pero con la opción **Detailed Vulnerabilities**


Nessus Essentials / Folders / Vie
Nessus Essentials / Folders / Vie
PaginaZero_PaolaJuan_psfv3y.pd
PaginaZero_PaolaJuan_y9sffw.pd
No seguro
https://localhost:8834/#/scans/reports/32/hosts
nessus
Essentials
PaolaRealpe
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Five Core Principles for Hybrid Cloud Security
Read M
Export
Generate Report
Report Format: HTML PDF CSV
Select a Report Template:
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations
Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.
Filters Applied:
None
Formatting Options:
Include page breaks between vulnerability results
Generate Report
Cancel
Save as default
Buscar
ESP
3:40 p. m.
4/04/2023


Nessus Essentials / Folders / Vie
Nessus Essentials / Folders / Vie
TestPHP_PaolaJuan_xsk97k.pdf
Archivo
C:/Users/PAOLA/Downloads/TestPHP_PaolaJuan_xsk97k.pdf
¿Establecer Microsoft Edge como la aplicación predeterminada para leer archivos PDF?
Establecer como predeterminado
Dibujar
Lectura en voz alta
4
de 5
testphp.vulnweb.com
1 CRITICAL
0 HIGH
4 MEDIUM
0 LOW
19 INFO
Vulnerabilities
Total: 24
SEVERITY CVSS V2.0 VPR SCORE PLUGIN NAME
CRITICAL 10.0 - 58987 PHP Unsupported Version Detection
MEDIUM 5.0 - 12217 DNS Server Cache Snooping Remote Information Disclosure
MEDIUM 5.0 4.2 10539 DNS Server Recursive Query Cache Poisoning Weakness
MEDIUM 5.0 3.6 35450 DNS Server Spoofed Request Amplification DDoS
MEDIUM 5.0 2.7 15753 Multiple Vendor DNS Response Flooding Denial Of Service
INFO N/A - 10114 ICMP Timestamp Request Remote Date Disclosure
INFO N/A - 166602 Asset Attribute: Fully Qualified Domain Name (FQDN)
INFO N/A - 45590 Common Platform Enumeration (CPE)
INFO N/A - 11002 DNS Server Detection
Buscar
ESP
3:40 p. m.
4/04/2023





A. Describa con sus propias palabras las vulnerabilidades encontradas en cada caso y describa con sus palabras teniendo en cuenta la documentación que sugiere nessus, como se debería solucionar o qué medidas se deben tomar para resolver la vulnerabilidad

CRITICAL - PHP Unsupported Version Detection (Detección de versiones no compatibles con PHP)

Esta vulnerabilidad de nivel crítico que se encontró en la página web TestPHP, menciona que el PHP en el host remoto, ya no es compatible con la versión que esta implementada, por lo que los proveedores ya no lanzan actualizaciones o parches de seguridad nuevos, permitiendo que este tenga una gran cantidad de vulnerabilidades.

SOLUCION NESSUS

La solución que nos sugiere Nessus es la implementación de una versión más nueva de PHP, con el propósito de que tenga mejoras en la seguridad, el rendimiento del sitio web para que sea más rápido su uso, nuevas características, funcionalidades y compatibilidad con las nuevas tecnologías y plataformas más recientes.

SOLUCION INTEGRANTES DEL GRUPO

Existe también la posibilidad de la modificación de código para que sea compatible con la de PHP pero no es recomendable por lo que la actualización de la versión brinda una mejor seguridad.

MEDIUM - DNS Server Recursive Query Cache Poisoning Weakness (Debilidad de envenenamiento de caché de caché de consultas recursivas del servidor)

Esta vulnerabilidad de nivel medio que se encontró en la página web TestPHP, puede corromper el cache del servidor, al introducir información falsa a los usuarios. Se tiene en cuenta que este problema viene con otras afectaciones como la consulta de los nombres remotos para los terceros, en caso de que el servidor sea interno entonces los ataques se limitan en el acceso de empleados o invitados, por lo que los ciberdelincuentes aprovechan esto para el envenenamiento de cache contra el host o el uso de las consultas recursivas de UDP para rebotar ataques de denegación de servicio en la red, con solicitudes falsificadas usando la dirección IP de la víctima como dirección de origen para la sobrecarga de tráfico

SOLUCION NESSUS

Las soluciones que ofrece Nessus es la restricción de las consultas recursivas, como el caso de las conexiones de LAN.

En tal caso de que se utilice bind 8, entonces se debe tener en cuenta el empleo de allow-recursión en las opciones de named.config para permitir que los clientes realicen las consultas al navegador, junto con las restricciones acceso apropiados.

Si se utiliza el bind 9 entonces se deben implementar las agrupaciones de direcciones internas con las listas de control de acceso (acl).

Dado que se utilice un servidor diferente, se debe consultar en la documentación las recomendaciones para mejorar la seguridad.

SOLUCION INTEGRANTES DEL GRUPO

Para evitar esta vulnerabilidad se aconseja actualizar el software DNS, realizar configuraciones para impedir las consultas recursivas a personas no autorizadas, limitar el número de respuestas que se alojan en el cache del servidor, con figurar el firewall y los filtros y tener aplicaciones de monitorización de servidor para detectar actividades sospechosas.

MEDIUM - DNS Server Spoofed Request Amplification DDoS (DDoS de amplificación de solicitudes falsificadas del servidor DNS)

El servidor DNS responde a cualquier solicitud en otras palabras, terceros pueden realizar consultas y obtener respuestas, por lo es vulnerable a la falsificación de direcciones de IP.

Los ciberdelincuentes pueden utilizar el servidor DNS mal configurado para inundar al objetivo con tráfico malicioso en donde se responde enviando datos amplificados al objetivo, provocando una sobrecarga en el ancho de banda y la disminución del procesamiento de solicitudes.

SOLUCION NESSUS

La solución que sugiere Nessus es restringir el acceso al DNS para prevenir posibles ataques por la amplificación de solicitudes falsificadas, en conclusión, los administradores de la red deben limitar las consultas y bloquear las solicitudes sospechosas.

SOLUCION INTEGRANTES DEL GRUPO

También se puede tomar otras medidas de seguridad como es el caso de la configuración de servidores el filtrado de paquetes que provienen de direcciones IP sospechosas, la actualización e implementación de firewall, difusión con red anycast, filtración de agujeros negros para canalizar el tráfico a una ruta invalida, minimización del área expuesta ataques, poniendo recursos detrás de balanceadores de carga o el CDN, etc.