DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD, EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL EN BASE A LA NORMA ISO/IEC (MARZO 2015)

Autor: Zura A.
Director: MSc. Maya E.

***Resumen* —El GAD Municipal de Otavalo proporciona distintos servicios de telecomunicaciones en beneficio de la población, para ello posee una red de datos distribuida en red interna, enlaces inalámbricos y acceso a las TIC's tanto en el sector urbano como en el rural; razón por la cual es importante que su infraestructura ofrezca alta disponibilidad y calidad de servicio, soportando grandes cantidades de tráfico, además de poseer escalabilidad, flexibilidad y seguridad.**

El presente trabajo plantea un diseño de modelo de seguridad multicapa, conocido como defensa en profundidad; el mismo que será aplicado en tres niveles; en el nivel de usuario se elaboró un Manual de Normas y Procedimientos de seguridad de información en base a la Norma ISO IEC 27002, el cual se socializó en conjunto con el administrador de red hacia los usuarios; en el nivel de red interna se diseñó un modelo jerárquico basado en el estudio por capas; y en la red perimetral mediante herramientas de detección de intrusos basados en motores Suricata bajo una plataforma unificada denominada SELKS.

Además mediante un presupuesto referencial se demostró que es posible migrar de una solución propietaria a una solución bajo software libre; lo que permite minimizar costos y aprovechar mejor los recursos.

I. INTRODUCCIÓN

En la actualidad las instituciones públicas tienden a proporcionar distintos servicios de telecomunicaciones en beneficio de la población. El GAD Municipal de Otavalo no es la excepción, ya que posee una red de datos distribuida en red interna, enlaces inalámbricos y acceso a las TIC's tanto en el sector urbano cómo en el rural. Para lograr dicho objetivo, en los últimos años hán mejorado su infraestructura.

Año tras año ha incremento los usuarios de la red del GAD Municipal de Otavalo, causando dificultad en la administración de la red ya que no se ha tomado las consideraciones de segmentación en la misma, ocasionando caída en la enlaces. Pero el aumento de los usuarios no solo trae consigo problemas de administración, sino también problemas en la seguridad de la información, a pesar de que este tema ha sido tomado en cuenta y que no se ha presentado ningún tipo de amenaza o ataque activo, se ha tomado como un mecanismo de seguridad, la adquisición de dos Firewalls Sophos UTM, los cuales se han configurado con mínimas políticas de seguridad basadas en la restricción de páginas web para la intranet, políticas que no son suficientes para prevenir ataques de acceso, de modificación, así como también ataques de denegación de servicios, entre otros; haciendo que la red sea aun vulnerable tanto externa como internamente.

Debido a estos inconvenientes, será necesario implementar mecanismos que permitan contrarrestar estas vulnerabilidades, tomando en cuenta que el nivel de seguridad no solo se debe considerar de forma interna sino fuera de ella, por lo que se debe segmentar la red aplicando controles de listas de acceso hacia las VLANs, implementar el modelo de seguridad basado en la "Defensa en Profundidad" en los niveles de usuario, red interna y red perimetral; y considerar nuevas políticas de seguridad que ayudará a prevenir ataques, detectándolos a tiempo y dando una respuesta oportuna para evitar daños posteriores.

II. ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED DE DATOS

Existen varias metodologías para realizar el análisis del nivel de seguridad de información dentro de una organización. En éste caso de estudio se eligió la metodología de OSSTMM[1] (Manual de la Metodología Abierta de Testeo de Seguridad) debido a las ventajas y caracteristicas que esta metodología ofrece.

Esta metodología abarca toda la seguridad operativa, y comprometerse en las diferentes áreas o canales como lo describe el manual, y se observa en la Tabla I:

[1] Representa uno de los estándares profesionales más completos y utilizados en Auditorías de Seguridad para analizar la Seguridad de los Sistemas. Describe minuciosamente, las fases que habría que realizar para la ejecución de la auditoria. (Alvarado)

Tabla I

ÁMBITO DE OSSTMM				
Seguridad Física[a]		**Seguridad de Espectro[a]**	**Seguridad de Comunicaciones[a]**	
Humano[b]	*Físico[b]*	*Comunicaciones Inalámbricas[b]*	*Telecomunicaciones[b]*	*Redes de Datos[b]*
Comprende el elemento humano de la comunicación.	Comprende el elemento tangible de la seguridad.	Comprende todas las comunicaciones electrónicas, señales, y las emanaciones que se producen en el (EM).	Comprende todas las redes de telecomunicación, digitales o analógicas.	Comprende todos los sistemas electrónicos y redes de datos.

Nota: La tabla fue adaptada de (Herzog, OSSTMM 3.0)
[a] Clases: Son definidas como áreas de estudio, de investigación o de operación.
[b] Canales: son los medios específicos de la interacción con los activos.

A. CANAL HUMANO

La evaluación de seguridad en el canal humano, fue enfocada a al nivel de acceso y confianza que éste factor proporciona en la seguridad de la información. Para ello se realize pruebas de observación directa y de ingeniería social, con lo que se pudo obtener información valiosa que compromete la seguridad de la información.

Los resultados obtenidos se muetsran en la Fig.1, los mismos que reflejan acorde a los parámetros de la metodolgía que la seguridad operacional es bastante baja, tomando en cuenta que ésta evalúa las diferentes políticas y procedimientos implementados por la administración.

Fig. 1 Resultado del cálculo de RAVs en el canal humano
Fuente: Calculadora OSSTMM

Al ser los controles los mecanismos de seguridad puestos en marcha para proteger las operaciones, cabe recalcar que se tiene mucha prioridad en cuanto a la indemnización del personal, más no así en otros controles que son totalmente nulos como la Subyugación y la Continuidad.

Las limitaciones se ponderan individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, es así que debido a ello se tiene limitaciones nulas como en el no repudio; y casi nulas en cuanto a confidencialidad, privacidad, integridad y alarma.

B. CANAL FÍSICO

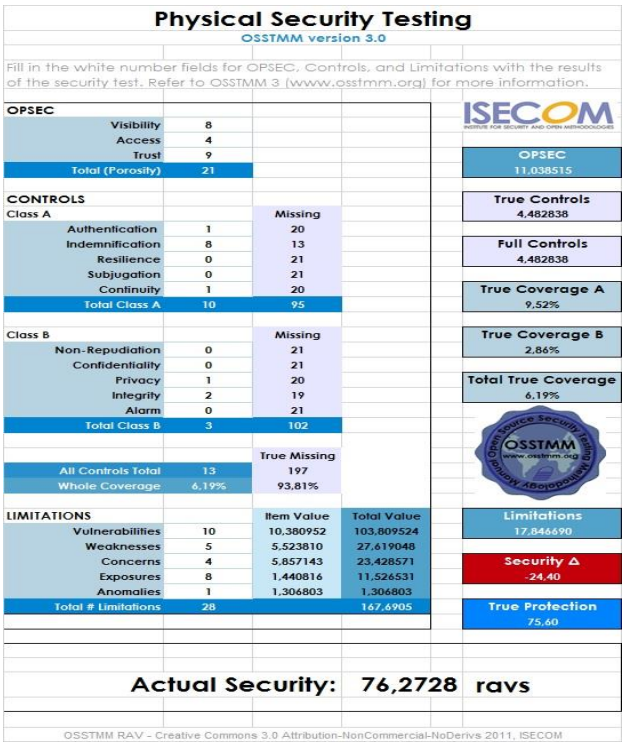
La evaluación de seguridad en el canal físico, fue enfocada al nivel de acceso al cuarto de equipos, a la disponibilidad de los dispositivos, y sobre todo a la respuesta ante eventualidades del mismo.

Los resultados obtenidos se muetsran en la Fig 2., los mismos que reflejan acorde a los parámetros de la metodolgía que la seguridad operacional es relativamente alta, tomando en cuenta que ésta evalúa las diferentes políticas y procedimientos implementados por la administración. Esto refleja la prioridad que se le ha dado a la seguridad física.

Al ser los controles los mecanismos de seguridad puestos en marcha para proteger las operaciones, cabe recalcar que de acuerdo al test realizado, lamentablemente no se tienen implementados controles respectivos a la seguridad física, siendo ésta un blanco para los atacantes informáticos.

Las limitaciones se ponderan individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, es así que debido a que los valores en seguridad operacional son relativamente altos, estos valores predominan para que el cálculo de las limitaciones sea también relativamente alto. Y resulta así una gran preocupación debido

a que se tiene una limitación de vulnerabilidad muy alta en relación a los demás valores.



Physical Security Testing
OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC			
Visibility	8		
Access	4		
Trust	9		
Total (Porosity)	21		

CONTROLS			
Class A		Missing	
Authentication	1	20	
Indemnification	8	13	
Resilience	0	21	
Subjugation	0	21	
Continuity	1	20	
Total Class A	10	95	
Class B		Missing	
Non-Repudiation	0	21	
Confidentiality	0	21	
Privacy	1	20	
Integrity	2	19	
Alarm	0	21	
Total Class B	3	102	
		True Missing	
All Controls Total	13	197	
Whole Coverage	6,19%	93,81%	

LIMITATIONS		Item Value	Total Value
Vulnerabilities	10	10,380952	103,809524
Weaknesses	5	5,523810	27,619048
Concerns	4	5,857143	23,428571
Exposures	8	1,440816	11,526531
Anomalies	1	1,306803	1,306803
Total # Limitations	28		167,6905

OPSEC 11,038515
True Controls 4,482838
Full Controls 4,482838
True Coverage A 9,52%
True Coverage B 2,86%
Total True Coverage 6,19%
Limitations 17,846690
Security Δ -24,40
True Protection 75,60

Actual Security: 76,2728 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

Fig. 2. Resultado del cálculo de RAVs en el canal físico.
Fuente: Calculadora OSSTMM

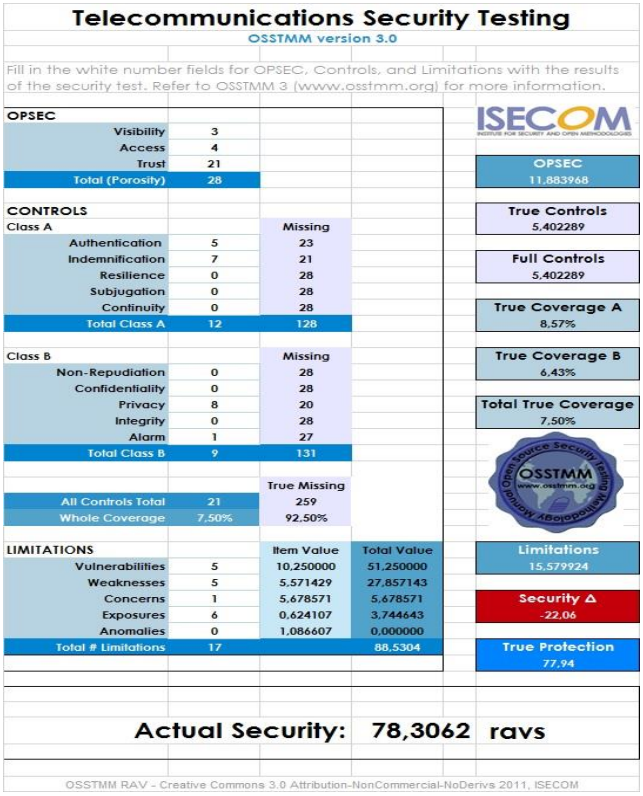
C. CANAL DE TELECOMUNICACIONES

La evaluación de seguridad en el canal de telecomunicaciones, se realizó un mapa de los protocolos de comunicación con la ayuda del software NetScan, con el que se realizó un escaneo de puertos, dejando en evidencia el nivel de acceso que se tiene a las apliaciones.

Los resultados obtenidos se muetsran en la Fig.3, los mismos que reflejan acorde a los parámetros de la metodolgía que la seguridad operacional es alta, principalmente en el aspecto de Confianza, en el que se ha considerado todos los puertos que están abiertos, analizando el porqué de su estado. Esto refleja la importancia que se le ha dado a la seguridad de las telecomunicaciones.

Al ser los controles los mecanismos de seguridad puestos en marcha para proteger las operaciones, cabe recalcar que de acuerdo al test realizado, se tienen únicamente controles de Indemnización, autenticación y privacidad; mientras tanto los demás controles son nulos; dejando así una brecha para la inseguridad de la información.

Las limitaciones se ponderan individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, es así que debido a que los valores en seguridad operacional son relativamente altos, estos valores predominan para que el cálculo de las limitaciones sea también relativamente alto. Es así que resaltan limitaciones como las Vulnerabilidades, debilidades y exposiciones las mismas que reflejan una administración no adecuada que expone a la red a ciertas amenazas hacia la seguridad de información.



Telecommunications Security Testing
OSSTMM version 3.0

Fill in the white number fields for OPSEC, Controls, and Limitations with the results of the security test. Refer to OSSTMM 3 (www.osstmm.org) for more information.

OPSEC			
Visibility	3		
Access	4		
Trust	21		
Total (Porosity)	28		

CONTROLS			
Class A		Missing	
Authentication	5	23	
Indemnification	7	21	
Resilience	0	28	
Subjugation	0	28	
Continuity	0	28	
Total Class A	12	128	
Class B		Missing	
Non-Repudiation	0	28	
Confidentiality	0	28	
Privacy	8	20	
Integrity	0	28	
Alarm	1	27	
Total Class B	9	131	
		True Missing	
All Controls Total	21	259	
Whole Coverage	7,50%	92,50%	

LIMITATIONS		Item Value	Total Value
Vulnerabilities	5	10,250000	51,250000
Weaknesses	5	5,571429	27,857143
Concerns	1	5,678571	5,678571
Exposures	6	0,624107	3,744643
Anomalies	0	1,086607	0,000000
Total # Limitations	17		88,5304

OPSEC 11,883968
True Controls 5,402289
Full Controls 5,402289
True Coverage A 8,57%
True Coverage B 6,43%
Total True Coverage 7,50%
Limitations 15,579924
Security Δ -22,06
True Protection 77,94

Actual Security: 78,3062 ravs

OSSTMM RAV - Creative Commons 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

Fig. 3. Resultado del cálculo de RAVs en el canal telecomunicaciones.
Fuente: Calculadora OSSTMM

D. CANAL REDES DE DATOS.

La evaluación de seguridad en el canal de redes de datos, se realizó con el uso de sniffing de red para identificar los protocolos que emanan respuesta de los servicios de red o peticiones en su caso. Por ejemplo, Netbios, ARP, SAP, NFS, BGP, OSPF, MPLS, RIPv2, etc.

Los resultados obtenidos se muetsran en la Fig.4, los mismos que reflejan acorde a los parámetros de la metodolgía que la seguridad operacional es demasiado alta, principalmente en el aspecto de Confianza, en el que se ha utilizado metodologías de sniffing de red para identificar los protocolos que emanan respuesta de los servicios de red o peticiones en su caso.

Al ser los controles los mecanismos de seguridad puestos en marcha para proteger las operaciones, cabe recalcar que de acuerdo al test realizado, ay valores nulos en controles como subyugación, no repudio, confidencialidad e integridad; dejando así una brecha para la inseguridad de la información.

Las limitaciones se ponderan individualmente, pero éstas se relacionan directamente con algunos controles y seguridad operacional, es así que debido a que los valores en seguridad operacional son muy altos, estos valores predominan para que el cálculo de las limitaciones sea también relativamente alto. Es así que resaltan limitaciones como las Vulnerabilidades y exposiciones las mismas que reflejan una administración no adecuada que expone a la red a ciertas amenazas hacia la seguridad de información.

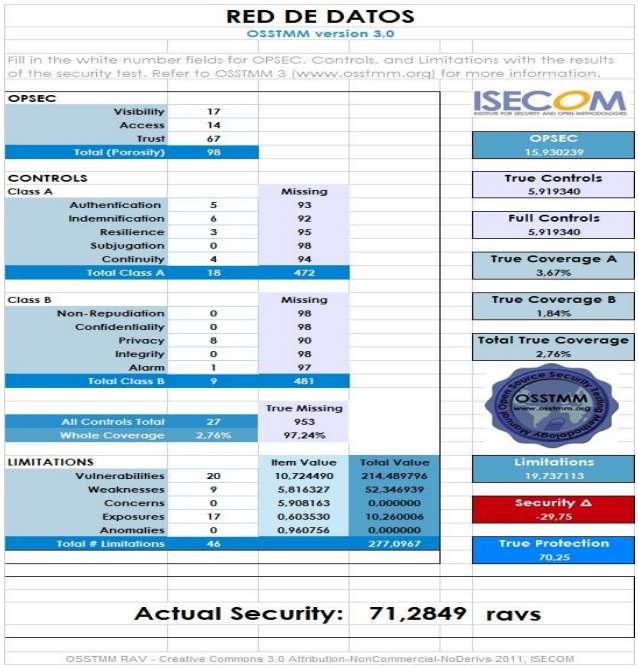


Fig. 4. Resultado del cálculo de RAVs en el canal redes de datos.
Fuente: Calculadora OSSTMM

III. DISEÑO DEL MODELO DE SEGURIDAD DEFENSA EN PROFUNDIDAD

Dentro del diseño del modelo de seguridad defensa en profundidad, se plantea normas y políticas de seguridad establecidas en la norma ISO/IEC 27002, el diseño de la segmentación de la red, de igual manera los diseños del IDS/IPS, firewalls de acuerdo a los resultados obtenidos en el levantamiento de información previa.

A. DISEÑO DEL MODELO DE DEFENSA EN EL NIVEL DE USUARIO.

La educación al usuario mediante normas y procedimientos es la base de seguridad en el primer nivel del modelo Defensa en Profundidad; es por ello que, en esta sección se desarrollará una guía práctica para el desarrollo de normas de seguridad en el GADMO, para crear confianza en las actividades de dicha entidad. (NTE INEN-ISO/IEC 27002, 2009).

Gracias a los resultados obtenidos en el Análisis de Riesgos realizados anteriormente con la Metodología OSTMM, se podrá "determinar la acción de gestión adecuada y las prioridades para la gestión de los riesgos de la seguridad de la información, así como para implementar los controles seleccionados para la protección contra estos riesgos". (NTE INEN-ISO/IEC 27002, 2009)

En base a dichos resultados se ha propuesto crear una guía de seguridad; la misma que tiene por objetivo mantener y mejorar la gestión de la seguridad de la información en la organización, así como también tener una concientización en los funcionarios del GADMO del buen uso de la información, y "el cumplimiento de requisitos legales, estatutos, reglamentos y contractuales que debe cumplir la institución, sus socios comerciales, los contratistas y los proveedores de servicio, así como su entorno socio-cultural." (NTE INEN-ISO/IEC 27002, 2009).

Dicho manual se estructuró en base a los siguientes dominios que se tomaron de referencia de la Norma NTE INEN-ISO/IEC 27002:2009:

1. Política de la seguridad
2. Organización de la seguridad de la información.
3. Gestión de activos
4. Seguridad de los recursos humanos
5. Seguridad física y del entorno
6. Gestión de comunicaciones y operaciones
7. Control del acceso
8. Adquisición, desarrollo y mantenimiento de sistemas de información
9. Gestión de los incidentes de la seguridad de la información
10. Gestión de la continuidad del negocio
11. Cumplimiento

B. DISEÑO DEL MODELO DE DEFENSA EN EL NIVEL PERIMETRAL.

Para el dieño del modelo de defensa en profundidad en el nivel perimetral se describen las características y funciones del software Suricata, que fue el escogido para el diseño del IDS/IPS sobre software libre, además se describe el proceso para su elaboración, definiendo los parámetros de configuración necesarios para su correcto funcionamiento. Adicionalmente se describe las características del Firewall tanto físico como lógico del GADMO, así como su configuración. Finalmente se describirá las aplicaciones de la granja de servidores y la propuesta de la configuración de una DMZ, que permita minimizar los riesgos de seguridad en la institución.

1) IDS/IPS

Para la elección del sistema de detección y prevención de intrusos se realizó una previa comparación entre diferentes soluciones, sean estas propietarias o bajo software libre, la misma que se detalla en la Tabla II.

Tabla II

COMPARACIÓN DE LOS DIFERENTES SOFTWARES LIBRES Y COMERCIALES DE IDS/IPS.

CARACTERÍSTICAS	SISTEMAS DE DETECCIÓN Y PREVENCIÓN DE INTRUSOS			
	BRO	SNORT	SOLUCIONES COMERCIALES	SURICATA
Multi-Hilos	No	No	No	Si
Soporte para IPv6	Si	Si	Cisco, IBM, Stonesoft	Si
IP Reputation	Algo	No	Cisco	Si
Detección automática de protocolos	Si	No	No	Si
Aceleración con GPU	No	No	No	Si
Variables Globales/Flowbits	Si	No	No	Si
Análisis Avanzado de HTTP	Si	No	No	Si
HTTP Access Logging	Si	No	No	Si
SMB Access Logging	Si	No	No	Si
Anomaly Detection	No	No	Si	No
Alta Disponibilidad	No	No	Si	No
GUI de Administración	No	No	Si	No
Gratis	Si	Si	No	Si

En base a la comparación de las diferenctes soluciones, la elección del software a utilizarse en el Sistema de detección y prevención de intrusos es Suricata.[2]

Una vez elegido y configurado el software, el siguiente paso es la ubicación física del mismo dentro de la red de datos; el mismo que se pondrá entre el firewall y la red interna, con esta ubicación se pueden obtener ciertas ventajas, tales como:

- Permite monitorear intrusiones que pueden atravesar el firewall.
- Puede detectar ataques dirigidos contra los servidores.
- Permite identificar ataques y escaneos más communes.

Como todo sistema de detección de intrusos, también existen ciertas desventajas, las mismas que se presentan a continuación.

- No permite identificar ataques que utilicen métodos de encriptación
- Dependiendo de la cantidad de tráfico el IDS-IPS, puede o no analizarlo todo. Esto dependerá del diseño del sistema.

[2] Suricata es un motor IPS/IDS de código abierto bajo licencia GPLv2y desarrollado por la comunidad de OISF (Open Infomation Security Foundation), es relativamente nuevo pero con muy buenas características siendo la más importante su arquitectura Multi-hilos, además es totalmente compatible con las reglas Snort y Emerging Threads. (Alfon, 2011).

En la Fig.5 se presenta una representación gráfica de la ubicación del sistema de detección y prevención de intrusos.

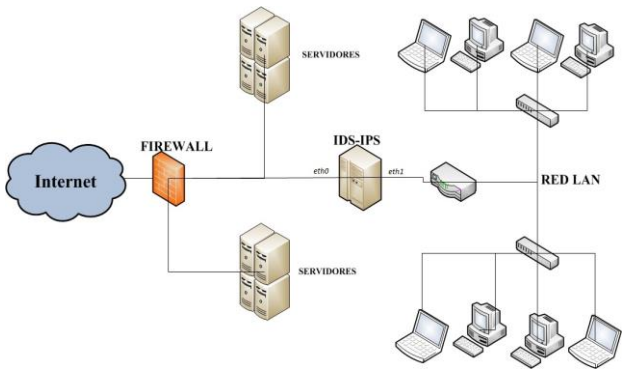


Fig.5. Ubicación del IDS-IPS en la red.
Fuemte: Elaborada por Andrea Zura

2) FIREWALL

El GADMO cuenta actualmente (Enero 2015) con dos firewall, ASTARO Gateway 320; los mismos que se encuentran configurados de modo que protegen la granja de servidores de los ataques externos.

Dicho firewall tiene ciertas características técnicas que se presentan en la Tabla 2.

Tabla III

|INFORMACIÓN TÉCNICA DEL FIREWALL SOPHOS UTM

Figura	Capacidad	Especificaciones del hardware:
Astaro Security Gateway 320 	Rendimiento del cortafuegos: 3.4 Gbit/s Rendimiento de la VPN: 700 Mbit/s Rendimiento del IPS: 1300 Mbit/s Rendimiento del UTM: 165 Mbit/s Correos electrónicos por hora: 600,000 Usuarios: Sin restricción Conexiones simultáneas: 600,000 Almacenamiento en cuarentena: 60 GB Almacenamiento de registros/informes: 80 GB.	Unidad de disco duro: 160 GB Puertos Ethernet: 8 Puertos USB: 4 Puertos COM: 1 (RJ-45) Puertos VGA: 1 (trasero) Pantalla LCD: 1

Además se realizarón ciertas configuraciones básicas en el software, tales como activar el acceso SSH lo que permite al administrador, acceder de forma remota y segura, en situaciones en las que no se puedan resolver problemas por medio del WebAdmin; además activar el envío automático de backups, permitiendo tener éstos siempre a mano, para que el administrador los pueda utilizar cuando los necesite; cabe recalcar que estos ocupan muy poco espacio y se guardan ya sea en el servidor o en nuestro correo electrónico, entre otras.

3) ZONA DESMILITARIZADA (DMZ)

Para realizar el diseño de la DMZ se debe tener conocimiento de todos los servicios que brinda el GADMO, en que plataformas se encuentran instalados, tanto a nivel de hardware como software. Además la granja de servidores se encuentra protegida por dos Firewall, pero en una distribución no recomendada debido a que podría haber intentos de intrusión.

Teniendo claro los tres elementos principales que forman parte de la red perimetral, se muestra en la Fig.6, el diseño planteado para la red de datos del GADMO, en el que se detalla cada una de estas partes.

Se observa que en la zona desmilitarizada se encuentran los servicios de Correo electrónico y servidor WEB; los mismo que se encuentran protegidos por el primer firewall, siguiendo continuamente del siguiente firewall, adicionalmente se tiene el IDS-IPS en la ubicación ya antes explicada el mismo que permitirá conservar la seguridad de la LAN.

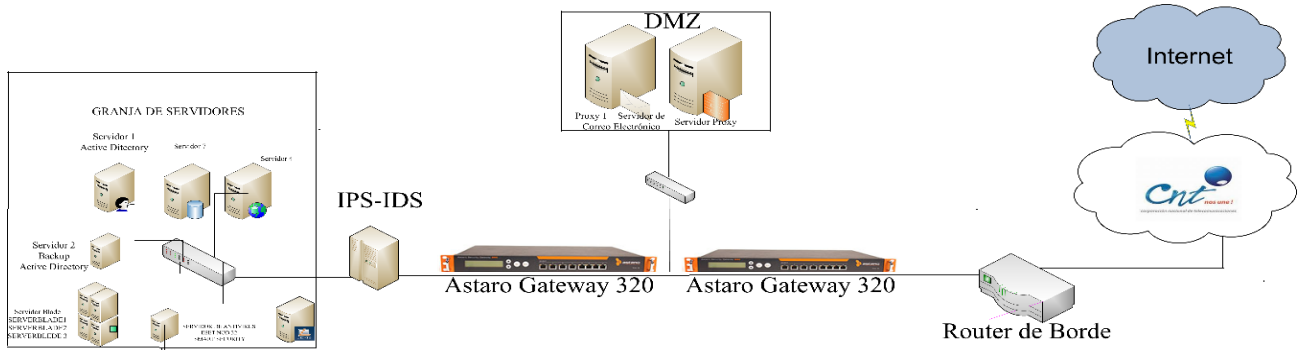


Fig.6. Diseño de red perimetral
Fuente: Elaborada por Andrea Zura

C. DISEÑO DEL MODELO DE DEFENSA EN EL NIVEL DE RED INTERNA

Considerando la infraestructura y requerimientos actuales de la red de datos del GADMO, se propone un modelo jerárquico y la segmentación lógica de la red. Brindando así una solución que mejore las prestaciones y servicios.

1. DISEÑO DEL MODELO DE RED

El modelo jerárquico de red presenta varias ventajas que permitirán que la red de datos del GADMO sea más segura, escalable, redundante, flexible y eficiente.

Dicho modelo se basa en el diseño y estructuración por capas independientes que cumple funciones específicas. La separación de la diferentes funciones existentes en una red hace que el diseño de la red se vuelva modular, ésto facilita la escalabilidad y el rendimiento. El modelo de diseño jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa núcleo. (CISCO), el mismo que se presenta en la Fig. 7.

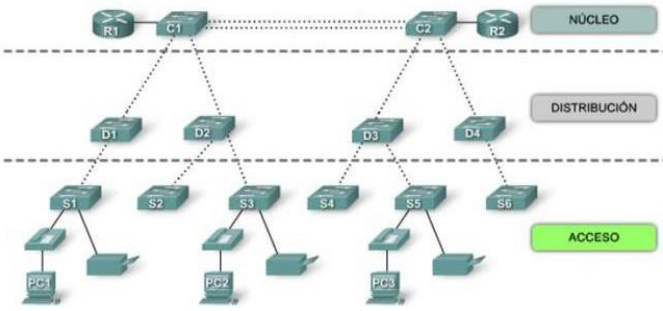


Figura 7. Modelo jerarquico de red
Fuente: Imagen extraída de (CISCO)

En base a dicho modelo se describirán las características de los switches con los que cuenta el GADMO; en base a sus características serán clasificados en las diferentes capas del modelo jerárquico.

1) Switches de capa de acceso

Los switches de la capa de acceso facilitan la conexión de los dispositivos de nodo final a la red. Por esta razón, necesitan admitir características como seguridad de puerto, VLAN, Fast Ethernet/Gigabit Ethernet, PoE y agregado de enlaces. La seguridad de puerto permite que el switch decida cuántos y qué dispositivos específicos se permiten conectar al switch. La seguridad de puerto se aplica en la capa de acceso. En consecuencia, es una importante primera línea de defensa para una red.

Acorde a las características que se necesitan para los switches de acceso, se presenta en la Tabla IV un resumen de los elegidos con sus respectivas características.

Tabla IV

CARACTERÍSTICAS SWITCHES CAPA DE ACCESO

Switch	Velocidad	Rendimiento	IEEE 802.1Q	ACL
3COM 2924 SFP 24P	10/100/1000	MCS[a] :48Gbps MCT[b]:35,5Mbps	✓	✓
3COM 4400 48P	10/100	MCS: 13,6Gbps MCT: 10,1 Mbps	✓	✓
3COM 2816 16P	10/100/1000	MCS: 104 Gbps MCT: 74 Mbps	✓	✓
3COM 2226 SFP PLUS 24P	10/100	MCS: 8.8 Gbps	✓	✓
3COM 2824 SFP PLUS 24P		MCS: 48 Gbps MCT: 35,5 Mbps	✓	✓
3COM 4500G 48P		MCS: 13,6 Gbps MCT: 10,1 Mbps	✓	✓
3COM 2928 SFP 24P	10/100/1000	MCS: 56 Gbps MCT:41.7 Mbps	✓	✓
3COM 4500G 24P	10/100	MCS: 8.8 Gbps	✓	✓
3Com 4900 12P	10/100/1000		✓	✓
3Com 4210 18P	10/100		✓	✓
3COM 2952 48P	10/100/1000	MCS: 104 Gbps. MCT: 74 Mpps;	✓	✓

Al ser la capa de acceso un enlace directo con el usuario final, esta integra a todos los equipos finales, tales como, computadores, cámaras, teléfonos IP, scanner, impresoras, copiadoras, etc.; lo que permite que el administrador controle todos los equipos que se conecten a la red. Para ello se ha considerado segmentar lógicamente la red. Se presenta en la Fig. 8.

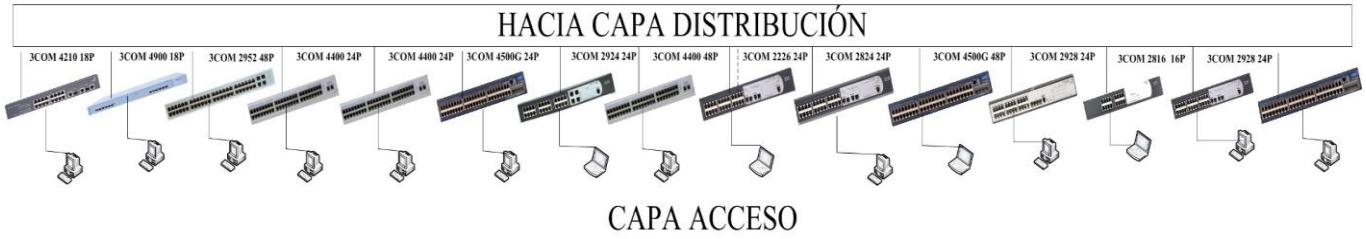


Fig.8. Switches capa acceso
Fuente: Elaborada por Andrea Zura

En el estudio de la situación actual se determinó que los usuarios se encuentran agrupados acorde a la función que éstos desempeñan y acorde a los recursos que utilizan.

Antes de realizar la segmentación hay que tener en cuenta varios aspectos:

- Se debe asignar a cada usuario una dirección IP, la misma que no debe ser modificada sin autorización; para controlar esto; se debe asociar la dirección MAC de cada equipo, con la dirección IP asignada, de tal forma que si las dos no coinciden, el usuario no podrá acceder a la red.
- Se debe tener un registro actualizado de los cambios que se registren la infraestructura de la red.
- Segmentación y Direccionamiento IP

La segmentación de una red permite mejorar significativamente la seguridad, ya que los administradores pueden configurar segmentos de tal forma que transmiten y reciben paquetes únicamente desde su subred, asegurándose que los paquetes no autorizados no se envían dentro o fuera del segmento.

Para realizar la segmentación se ha considerado la agrupación que se mantiene en el GADMO, agrupación por las diferentes direcciones, coordinaciones y/o jefaturas, funciones desempeñadas por cada usuario y los recursos que estos usen y necesiten usar.

La distribución de VLAN se puede diferenciar las siguientes:

- VSERV: VLAN de servidores y equipos; la misma que ha sido destinada para el direccionamiento IP de los servidores y del equipamiento activo de la Coordinación de TIC's.
- VADMIN: VLAN de administración; la misma que ha sido destinada para el direccionamiento IP de los administradores de la red, es decir los técnicos e ingenieros de la Coordinación de TIC´s.
- VTECN: VLAN de técnicos y colaboradores; la misma que ha sido destinada para el direccionamiento IP del personal de todas las direcciones que requieren el uso páginas web públicas, páginas web informativas y/o comerciales y correo electrónico para su trabajo.
- VASIST: VLAN de asistentes; la misma que ha sido destinada para el direccionamiento IP de los asistentes y/o secretarias que únicamente necesitan el correo electrónico para su trabajo.
- VDIREC: VLAN directores; la misma que ha sido destinada para el direccionamiento IP de los directores y/o coordinadores, los cuales tendrán acceso prioritario para todos los servicios.

Dicha distribución se muestra en el Tabla V.

Tabla V

EXTRACTO DE LA DISTRIBUCIÓN DE VLANS EN LA RED DE DATOS DEL GADMO

Dependencia		**#VLAN**	**Nombre VLAN**
COORDINACIÓN TIC's	Conmutadores y Enrutadores	VLAN 2	VLAN Native
	Servidores	VLAN	VSERV
	Unidad de Desarrollo Unidad de Redes Unidad de Mantenimiento	VLAN 3	VADMIN
AGUA POTABLE	Director	VLAN 4	VDAP
	Técnicos Alcantarillado	VLAN 5	VTAP
	Técnicos Comercialización		
	Técnicos Laboratorio		
	Asistentes	VLAN 6	VAAP
ALCALDÍA	Alcaldía	VLAN 7	VALCAL
	Auditoría Interna	VLAN 8	VTALCAL
	Asesoría Jurídica		
	Secretaría General		
	Fiscalización		
	Asistentes	VLAN 9	VAALCAL
AVALUOS Y CATASTROS	Director	VLAN 10	VDAVAL
	Avalúos Urbanos	VLAN 11	VTAVAL
	Avalúos Rurales		
	Asistentes	VLAN 12	VAAVAL

2) Switches de capa distribución

Los switches de capa de distribución recopilan los datos de todos los switches de capa de acceso y los envían a los switches de capa núcleo, además proporcionan funciones de enrutamiento entre las VLAN.

Entre las características que deben soportar los switches de capa distribución son la tasa de envió alta, puertos Gigabit Ethernet/ 10Gigabit Ethernet, componentes redundantes, políticas de seguridad/listas de control de acceso, agregado de enlaces y calidad de servicio. (CISCO)

Acorde a las características que se necesitan para los switches de acceso, se presenta en la Tabla VI un resumen de los elegidos con sus respectivas características:

Tabla VI.

SWITCH 2952 SFP PLUS 48P

Funcionalidades	Descripción
Rendimiento	48 10BASE-T/100BASE-X/1000BASE-T 4 Gigabit SFP ports Máxima Capacidad de switching: 104 Gbps. Máxima capacidad de transmisión 74 Mpps;
SWITCHING DE CAPA 2	VLANs basadas en protocolo IEEE 802.1Q Protocolo Spanning Tree (STP) IEEE 802.1D Protocolo Rapid Spanning Tree (RSTP) IEEE 802.1w
SWITCHING DE CAPA 3	Rutas estáticas: 32 Virtual VLANs Interface: 8
Priorización de tráfico	Clase de Servicio/Calidad de Servicio (CoS/QoS) IEEE 802.1p en salida
Seguridad	Filtros ACLs basadas en direccionamiento IP y MAC para filtrar el tráfico de red y mejorar el control de la red. ACL basadas en tiempo permiten una mayor flexibilidad con acceso a la red de gestión.

- Consideraciones del diseño

La capa de distribución agrega los datos recibidos de los switches de la capa de acceso antes de que se transmitan a la capa núcleo para el enrutamiento hacia su destino final. (CISCO)

Los switches 3COM 2952 SFP PLUS 48P manejarán los enlaces de conexión con todos las conexiones hacia los servidores, conexiones en la red interna así como también el manejo de inter VLANs de la red del GADMO. Adicionalmente estos equipos se configuraran como backup asegurando así la disponibilidad de la red. Dicha topología se muestra en la Fig.9.

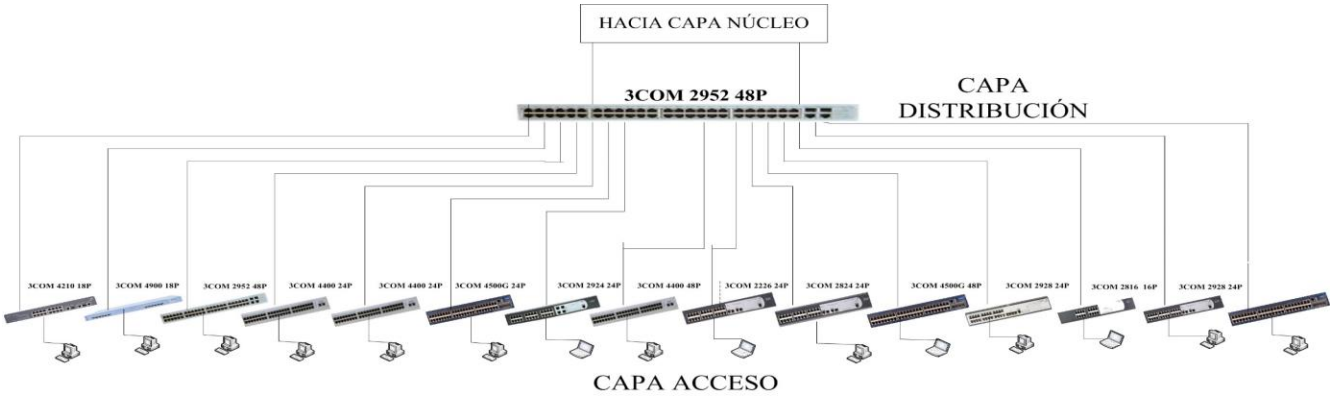


Fig.9. Switches capa distribución.
Fuente: Elaborada por Andrea Zura

3) Switches de capa núcleo.

La capa núcleo de una topología jerárquica es una backbone de alta velocidad de la red y requiere switches que pueden manejar tasas muy altas de reenvío. La velocidad de reenvío requerida depende en gran medida del número de dispositivos que participan en la red. Por ello un switch de capa núcleo debe soportar capa 3, sus puertos deberán se Gigabit Ethernet/10 Gigabit Ethernet, tener componentes redundantes, agregado de enlace y soportar calidad de servicio. (CISCO).

Acorde a las características que se necesitan para los switches de acceso, se presenta en la Tabla VII un resumen del switch elegido con sus respectivas características

Tabla VII

SWITCH 3COM 5500 SFP 24P

Funcionalidades	Descripción
Rendimiento	24 puertos 10/100/1000 Mbps 4puertos 1000 Mbps SFP Máxima Capacidad de switching: 184 Gbps. Máxima capacidad de transmisión 136.9 Mbps;
SWITCHING DE CAPA 2	VLANs basadas en protocolo IEEE 802.1Q Protocolo Spanning Tree (STP) IEEE 802.1D Protocolo Rapid Spanning Tree (RSTP) IEEE 802.1w
SWITCHING DE CAPA 3	Routing basado en hardware Rutas estáticas: 100 Interfaces Virtuales IP: 64 RIP (Protocolo de información de ruteo), v1 y v2 Open Shortest Path First (OSPF)
Priorización de tráfico	Clase de Servicio/Calidad de Servicio (CoS/QoS) IEEE 802.1p en salida
Seguridad	Las listas de control de acceso basadas en el tiempo

• Consideraciones del diseño

La capa de núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. Además puede conectarse a los recursos de Internet. (CISCO)

Además se pudo evidenciar que la topología actual de la red de datos del GADMO tiene los switches en configuración en cascada por la necesidad de dar servicio a la mayoría de los usuarios, sin embargo esto reduce el rendimiento de la red.

La red de datos del GADMO, cuenta con equipamiento COM, marca propietaria con tecnología XRN, la misma que permite mejorar el funcionamiento de la red, mediante la administración de los diferentes switches como una sola unidad. Se muetsra en el Fig.10.

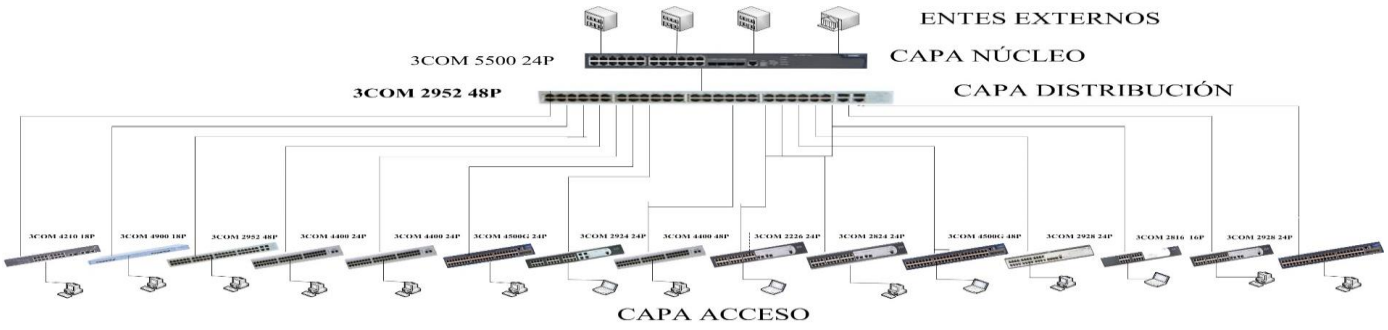


Fig.10.Switch capa Núcleo
Fuente: Elaborada por Andrea Zura

D. PRUEBAS DE FUNCIONAMIENTO.

Las pruebas de funcionamiento se las realizará utilizando métodos de Hacking Ético; el mismo que según (Plata) consiste en la simulación de posibles escenarios donde se reproducen ataques de manera controlada, así como actividades propias de los delincuentes cibernéticos, esta forma de actuar tiene su justificación en la idea de que: "Para atrapar a un intruso, primero debes pensar como intruso"

1) Detección de vulnerabilidades

El atacante por lo general, buscara vulnerabilidades en el sistema que pueda aprovechar para transformarlas en ataques o amenazas. Dichas vulnerabilidades pueden ser Consultas a bases de datos, consultas de cabeceras de mails, escaneo de puertos, peticiones http, búsqueda de datos dentro de archivos, entre otros (Tori).

Dado esto, se realizará un escaneo de puertos mediante la herramienta Nmap, cuyo objetivo es la identificación de puertos abiertos, que estén a la espera de nuevas conexiones, permitidas o no.

Cabe aclarar que todas las pruebas realizadas son en base al método White Box Test; que de acuerdo a (Tori): este es un chequeo que es llevado a cabo por un pentester que tiene toda la información acerca del sistema.

a) Ataques o intrusiones por capas

Los objetivos que persigue el Hacking ético de acuerdo a (Plata) son:

- Evaluar vulnerabilidades a través de la identificación de debilidades provocadas por una mala configuración de las aplicaciones.
- Analizar y categorizar las debilidades explotables, con base al impacto potencial y la posibilidad de que la amenaza se convierta en realidad.
- Proveer recomendaciones en base a las prioridades de la organización para mitigar y eliminar las vulnerabilidades y así reducir el riesgo de ocurrencia de un evento desfavorable.

En base a dichos objetivos se realizaron las pruebas en las diferentes capas del modelo OSI, y tomando como referencia la Fig.11

CAPAS MODELO OSI	ATAQUES POR CAPA
Aplicación	Buffer overflows, exploit code, software maliciosos, virus, gusanos, troyanos.
Presentación	NetBIOS enumeration, protocol attack
Sesión	Session hijacking, SYN attacks
Transporte	Port scanning, DOS ttacks
Red	IP attacks, routing attacks, ARP Poisoning, MAC flooding and ICMP assaults such as Smurf
Enlace de Datos	Passive and active snniffing, MAC spoofing, and WEP cracking
Física	Kardware hacking, lock picking, physical access attacks.

Fig. 11. Ataques para cada capa del Modelo OSI.
Fuente: Extraída de (Cabrera, 2012)

I. Capa Enlace de datos.

ARP spoffing fue la técnica elegida para realizar el hacking ético en esta capa; dicha técnica según (Thomas Demuth) es una técnica donde el atacante deliberadamente transmite un paquete ARP falso.

- Mitigación.

En el directorio de las reglas de suricata, encontraremos el archivo scirius.rules; en el cual se pude combatir este ataque; activando la alerta en dicho protocolo.

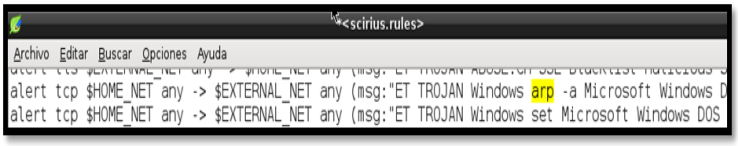


Fig. 12 Mitigación ataque Arp Spoofing
Fuente: Extraído de SELKS

El IDS-IPS, mostrará las alertas debido a que este ataque de ARP Spoffing. En la pantalla se muestran todas las direcciones MAC que están haciendo peticiones en la red; y acorde al número de veces que cada dirección MAC haga una petición se observará un resumen de alertas por dicho evento, en el que se indica entre los parámetros más importantes la dirección IP origen y destino. Se muestra en la Fig. 12.

View: Table / JSON / Raw

Field	Action	Value
@timestamp		2015-02-04T05:48:58.943Z
@version		1
_id		BByTFosfTgubmAWY__7ffQ
_index		logstash-2015.02.04
_type		SELKS
dest_ip		192.168.4.1
dest_port		443
event_type		tls
flow_id		35998032
host		SELKS
in_iface		eth1
path		/var/log/suricata/eve.json
proto		TCP
src_ip		192.168.4.11
src_port		5135
timestamp		2015-02-04T00:48:58.943158
tls.fingerprint		a2:13:46:5c:0a:d3:e7:3f:3a:c3:7f:0a:d6:57:b8:5e:57:1d:6a:90
tls.issuerdn		C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
tls.subject		C=FR, ST=IDF, L=Paris, O=Stamus, CN=SELKS
tls.version		TLS 1.2
type		SELKS

Fig. 13 Detalle de alertas producidas
Fuente: Extraído de SELKS

II. Capa de Red

En esta capa se puede realizar diferentes tipos de ataques los mismos basan su objetivo en imposibilitar el acceso normal a los servicios y recursos de una organización durante un tiempo indefinido.

- ICMP Flood

Satura el un equipo con solicitudes de ICMP Echo Request para que no pueda responder a las peticiones reales.

- Mitigación

En el directorio de las reglas de suricata, encontraremos el archivo scirius.rules; en el cual se pude combatir este ataque; activando la alerta en dicho protocolo.

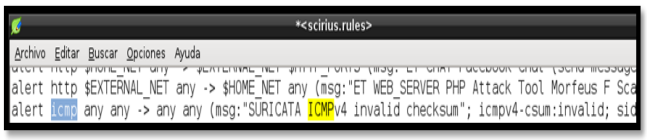


Fig. 14 Mitigación ataque ICMP Flood

El resultado mostrado por Suricata, se lo puede apreciar de diferentes modos; uno de ellos es mediante un gráfico estadístico en donde se muestran todas las alertas suscitadas en la red.

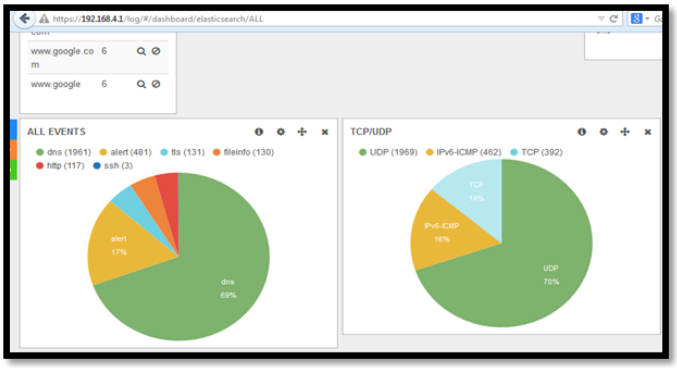


Fig. 15 Resultado estadístico de Suricata

III. Capa de Transporte

En esta capa existen diferentes tipos de ataques, en los que se encuentra el Escaneo y fingerprinting[3], técnica que permite recopilar información significativa al apuntar un escaneo a los hosts del objetivo o al procesar la información que brinda éste como resultado. (Tori).

- Escaneo de puertos

Descubrir que puertos están abiertos, filtrados o cerrados, además de averiguar qué tipo y versión de aplicación está corriendo en estos puertos y servicios. En base a estos

[3] Es una técnica que consiste en analizar las huellas que deja un sistema operativo en sus conexiones de red. Está basada en los tiempos de respuesta a los diferentes paquetes, al establecer una conexión en el protocolo TCP/IP, que utilizan los diferentes sistemas operativo. http://urlmin.com/4qp95

conceptos preliminares; se realizó un escaneo de puertos, utilizando la herramienta nmap. Se muestra en la figura 17.

- Mitigación

En el directorio de las reglas de suricata, encontraremos el archivo scirius.rules; en el cual se pude combatir este ataque; activando la alerta en dicho protocolo.

Fig. 16 Mitigación Ataque de escaneo de puertos
Fuente: Extraído de SELKS

El resultado en Suricata es:

Field	Action	Value
@timestamp		2015-01-28T13:27:02.287Z
@version		1
_id		eVlqKdPNQz2FUzkCOYr0KQ
_index		logstash-2015.01.28
_type		SELKS
dest_ip		192.168.4.1
dest_port		22
event_type		ssh
flow_id		52660336
host		SELKS
in_iface		eth1
path		/var/log/suricata/eve.json
proto		TCP
src_ip		192.168.4.11
src_port		1325
ssh.client.proto_version		2.0
ssh.client.software_version		PuTTY_Release_0.60

Fig 17. Resultado de alertas por escaneo de puertos
Fuente: Extraído de SELKS

En donde destacan información proporcionada por la alerta; tal como la dirección IP desde donde se realizó la petición, el servicio o protocolo; la hora y fecha exacta; así como también el software y la versión utilizada para realizar la intrusión.

IV. Capa de Sesión

En esta capa se puede hacer diferentes ataques tales como escaneo TCP SYN, técnica que envía un paquete SYN. Si la respuesta es un paquete SYN/ACK, el puerto está abierto, mientras que si es un RST, se encuentra cerrado.

- Mitigación

En el directorio de las reglas de suricata, encontraremos el archivo stream-events.rules; en el cual se pude combatir este ataque; activando la alerta en dicho protocolo.

Fig. 18 Mitigación ataque escaneo TCP SYN
Fuente: Extraído de SELKS

El resultado de Suricata se presenta en un resumen en el que se indica la dirección IP de origen de la intrusión el tipo de intrusión, la hora en la que sucinto; entre otros.

Fig. 19 Resultado de alerta ante intrusión TCP-SYN
Fuente: Extraído de SELKS

V. . Capa de Aplicación

En esta capa se puede realizar ataques mediante la descarga de aplicaciones de dudosa procedencia.

- Mitigación

En el directorio de las reglas de suricata, encontraremos el archivo files.rules; en el cual se pude combatir este ataque; activando la alerta en dicho ataque.

Fig.20 Mitigación ataques de descargas de archivos dudosos
Fuente: Extraído de SELKS

Es así que el software muestra un gráfico estadístico de las descargas realizadas

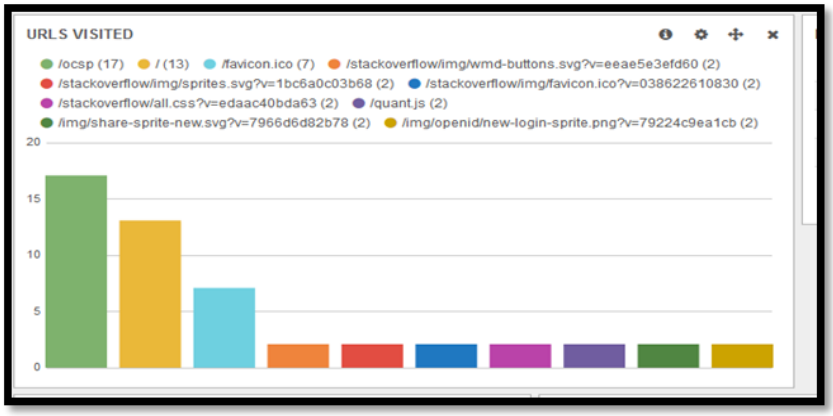


Fig 20 Gráfico estadístico de descargas realizadas
Fuente: Extraído de SELKS

E. PRESUPUESTO REFERENCIAL

Se realizará un presupuesto referencial tomando en cuenta una comparación de tener una solución licenciada y una solución en software libre, en la instalación de un IDS-IPS.

Cabe recalcar que el análisis del presupuesto referencial tiene como objetivo principal proporcionar una medida del presupuesto invertido en la realización de un proyecto.

1) Cálculo

Antes de iniciar con el cálculo del presupuesto, es necesario aclarar que para el diseño del modelo presentado en el presente proyecto; en la red interna se realizó con los equipos de conmutación existentes en el GADMO; en la red perimetral de igual manera. En ésta última, se implementó un sistema de detección y prevención de intrusos en software libre, en base a ello se realizará el presupuesto referencial.

Para la migración de un sistema o programa de Software Propietario (no libre) a Software Libre (SL) se utilizará el siguiente método para calcular el Costo Total de la Solución (CTS). Este método deberá aplicarse tanto al Software Propietario como al Software Libre. Si el costo de este último es menor que el del propietario se deberá realizar la migración. (Secretaría Nacional de la Administración Pública, 2014)
Además en el portal web (Secretaría Nacional de la Administración Pública, 2014), se recalca que como requisitos previos de la migración de un sistema comercial a un sistema bajo software libre es necesario tener las siguientes consideraciones:

- Tener las capacidades mínimas funcionales y técnicas requeridas por la organización y los usuarios.
- Mantener o incrementar la productividad de la organización y los usuarios.
- Ser compatible o integrable en las plataformas de hardware y software existentes.

Tabla VIII

PRESUPUESTO REFRENCIAL

Costo total de la Solución		**Sophos UTM**	**SURICATA**
CTI	CP	4,285.00	0.40
	CI	0	0
	CADH	2,875.00	479
	CADS	13,000.00	0
	CM	0	0
CTA	CMH	1,750.00	180.00
	CASS	1,465.00	0 .40
	CRH	1,5	1.50
CTC	CT	0	5000
	CU	0	0

Cabe recalcar que los cálculos se los realizarón en base a los siguientes cálculos.

- Costo Total de la Solución (CTS)

Para el cálculo del Costo Total de la Solución (CTS) según (Secretaría Nacional de la Administración Pública, 2014) se considera 3 componentes:

$$CTS = CTI + CTA + CTC$$

Ecuación 1 Costo Total de Solución
Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Donde:

- CTI: Costo Total de Implementación
- CTA: Costo Total Administrativo
- CTC: Costo Total de Capacitación

a. Costo Total de Implementación (CTI)

Es el costo total de rubros y actividades necesarios para poner a funcionar la solución. Se incluye adquisición de equipos, licencias y recurso humano puntual para la implementación. El CTI se calcula de la siguiente forma:

$$CTI = CP + CI + CADH + CADS + CM$$

Ecuación 2 Costo Total de Implementación
Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Donde:

• CP: Costos de las licencias del software considerando la arquitectura
• CI: Costos de instalación, configuración y adaptación (si fuera el caso)
• CADH: Costos adicionales de hardware e infraestructura
• CADS: Costos adicionales de software
• CM: Costos de migración de datos e integración

b. Costo Total Administrativo (CTA)

Es el costo total promedio anual de rubros y actividades necesarios para garantizar la disponibilidad, capacidad y continuidad de la solución implantada. Incluye el costo total promedio anual del recurso humano empleado en estas actividades. El CTA se calcula de la siguiente forma:

$$CTA = CMH + CASS + CRH$$

Ecuación 3 Costo Total Administrativo
Fuente: Recuperado de (Secretaría Nacional de la Administración Pública, 2014)

Donde:

• CMH: Costos de actualización y mantenimiento del hardware e infraestructura
• CASS: Costos de actualización y soporte del software
• CRH: Costos del Recurso Humano

c. Costo Total de Capacitación (CTC)

Es el costo promedio anual para la capacitación continua del personal (técnico y usuarios) en la operación y explotación de la solución.

$$CTC = CT + CU$$

Ecuación 4 Costo Total de Capacitación

Donde:

CT = Costo hora capacitación técnica * número de técnicos * número de horas * número años de funcionamiento de la solución

CU = Costo hora capacitación usuario * número de usuarios * número de horas * número años de funcionamiento de la solución.

RESULTADO

Si el costo del software libre es menor que el del propietario se deberá realizar la migración.

Entonces:

Si $CTS_{Propietario} = \$23{,}376.50$

Y $CTS_{Libre} = \$5661.30$

Se cumple que: $CTS_{Libre} < CTS_{Propietario}$

SE DEBE REALIZAR LA MIGRACIÓN.

F. CONCLUSIONES

Se realizó un diseño de seguridad, utilizando un modelo multicapas denominado "Defensa en Profundidad" en la red de datos del GAD Municipal de Otavalo, aplicando nuevas políticas de seguridad en base a la norma ISO/IEC 27002, de manera que ataques externos e internos puedan ser detectados y evitados oportunamente.

La norma ISO/IEC 27002, fue la base principal para la realización del diseño, ya que en ella se establecen ciertas directrices y objetivos que permiten identificar claramente los riesgos a los que puede estar expuesta la organización, y gracias a ello se pudo crear un Manual de Normas y procedimientos de seguridad de la información; además de crear políticas de acceso en la red perimetral y red interna.

El levantamiento de información se ejecutó con OSSTM 3.0; una metodología de pruebas de penetración que permite realizar un análisis de riesgos en los canales, Humano, Físico, Telecomunicaciones y Redes de Datos, obteniendo resultados que permitieron elaborar un Manual de Normas y Procedimientos en Base a la Normo ISO/IEC 27002, la misma que es compatible con la metodología antes mencionada.

El estudio de la situación actual, en cuanto a la infraestructura de red permitió identificar las características y prestaciones de todo el equipamiento; en base a ello se utilizó dicha infraestructura en una nueva topología que ayudará al mejoramiento del servicio y el mejoramiento de la administración.

El beneficio de contar con dos Firewalls, en la infraestructura de Red de datos, ayuda a combatir los focos de inseguridad; siempre y cuando éstos se ubiquen de manera tal,

que se aprovechen todas las funciones que dichos equipos ofrecen.

Un modelo de red jerarquizado utilizado para realizar el diseño de red interna, permite optimizar el uso de los recursos de la red; gracias a la aplicación de una topología de red basada en capas se obtienen características de escalabilidad, flexibilidad, y sobre todo seguridad.

Se realizaron pruebas de simulación de ataques en base a los objetivos de hacking ético; en las diferentes capas del modelo OSI, con lo que se pudo verificar el funcionamiento adecuado del IDS-IPS y su sistema de alertas.

Después de realizar el presupuesto referencial, y de establecer las diferencias entre tener una solución licenciada y una solución bajo software libre, se concluyó que el costo total solución bajo software libre es menor a la solución licenciada.

REFERENCIAS

[1]Alfon. (22 de Febrero de 2011). Seguridad y Redes. Obtenido de http://seguridadyredes.wordpress.com/2011/02/22/ids-ips-suricata-entendiendo-y-configurando-suricata-parte-i/

[2]Alvarado, M. S. (s.f.). OSSTMM 3. Análisis y Diseño de Sistemas de Información, 2.

[3]Bertolín, J. A. (2008). Seguridad de la Información . España: Paraninfo.

[4]Cabrera, E. C. (2012). Metodologías y marcos de trabajo en seguridad de la información. Ataques comunes en capa 3. Pereira.

[5]CISCO. (s.f.). CCNA 3.

[6] Networking Academic. (s.f.). CCNA Exploration 4.0. En Conmutación y conexión inalámbrica de LAN.

[7] Estrada, A. C. (2011). *Seguridad por NIveles.* España: DarFE.

[8] Febrero, B. M. (2011). *ANÁLISIS DE TRÁFICO CON WIRESHARK.* España.

[9] Gómez, D. G. (Julio de 2003). Sistemas de Detección de Intrusiones.

[10] Guiovanni, A. (s.f.). *GUIOOS' Blog*. Obtenido de https://guioos.wordpress.com

[11] Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (México). *Metodología de la Ivestigación.* MCGRAW-HILL.

[12] Herzog, P. (s.f.). *OSSTMM 2.1*.

[13] Herzog, P. (s.f.). *OSSTMM 3.0*.

[14] López, P. A. (s.f.). *Seguridad Informática.* Editex.

[15] Martínez, C. G. (2010). Modelo de Defensa en Profundidad.

[16] Mathon, P. (2002). *ISA Server 2000 Proxy y Firewall.* Barcelona: EMI.

[17] Microsoft. (2004). Guía de defensa en profundidad antivirus.

[18] NTE INEN-ISO/IEC 27002. (2009). *Tecnología de la Información- Técnicasde la Seguridad - Códifo de Práctica para la Gestión de la Seguridad de la Información.* Quito.

[19]Plata, A. R. (s.f.). *Ethical Hacking.*

[20]Secretaría Nacional de la Administración Pública. (22 de Enero de 2014). *Gobierno Elecctrónico* . Obtenido de http://www1.gobiernoelectronico.gob.ec

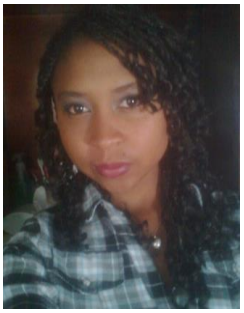
[21]Tanenbaum, A. (2003). *Redes de Computadoras.* Mexico: Pearson.

[22]Thomas Demuth, A. L. (s.f.). *ARP Spoofing y Poisoning, TRUCOS DE TRÁFICO.*

[23]Tori, C. (s.f.). Hacking Ético. Rosario .

[24] Toth, J., & Sznek, G. (2014). Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM. Neuquén.

BIOGRAFÍAS



Zura Ch. Andrea Y. Nació en Ibarra -Ecuador el 10 de mayo de 1990. Sus estudios primaries los realize en la Unidad Educativa Sagado Corazón de Jesus,; en el año 2007 obtuvo su bachillerato Técnico especialización Informática en el Colegio Nacional Ibarra; en el mismo año ingresó como estudiante de pre-grado a la Universidad Técnica del Norte en la Carrera de Ingeniería Electrónica y Redes de Comunicación. Realizó sus practices preprofesionales en la empresa FIX WIRELESS en el departamento técnico, reaizando tareas de studio técnico previo instlación de servicio, soporte técnico en sitio y via telefónica, e instlación del servicio de internet en el norte del país; en el Gobiero Autónomo Descentralizado Municipal de Otavalo realizó tareas de Instalación de puntos de red, soporte técnico, configuración de equipos L2 y L3, levantamiento de información, monitoreo e inventario IP.
Actualmente trabaja como Site Engennier en el Proyecto de MODERNIZACIÓN 2G de CLARO en la ciudad de Quito.

.