ANÁLISIS DE HERRAMIENTAS DE CÓDIGOS ABIERTOS QUE PERMITAN LA SEGURIDAD DE LA DATA EN LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO

Oviedo, Byron., Zhuma, Emilio., Gracia, Andrés.
{boviedo, ezhuma, andres.gracia2014}@uteq.edu.ec
Universidad Técnica Estatal de Quevedo

Resumen: En este documento se podrá evidenciar la seguridad en la data que posee la Universidad Técnica Estatal de Quevedo, a su vez proponer distintas herramientas de código abierto que se puedan implementar para mejorar dicha seguridad en la institución en caso de ser requerido, ayudando de así que la institución cumpla con las cuatro características fundamentales del acceso a esta información, se realizó usando el sistema operativo KALI LINUX ya que este software posee herramientas muy potentes para realizar pruebas de pentesting, como veremos en el documento utilizamos unas cuantas de las miles que existen se pueden realizar otras acciones gracias a este sistema operativo como vulnerar las redes WI-FI , para culminar se obtuvieron resultados con las herramientas que se pusieron a modo prueba para la realización de la investigación utilizando un sniffer IDS/IPS y simulando una intrusión para ver que valores nos proporcionaba y como se comportaba dicha seguridad.

Palabras Clave: Kali, Seguridades, Ataque, Redes

Abstract: This document will be able to demonstrate the securit Kali Linux, Seguridad, Datos, Ataque, Redes y in the data that has the state Technical University of Quevedo, in turn proposing different tools of open source that can be implemented to improve this security in the institution if it is required, Helping so that the institution meets the four fundamental characteristics of access to this information, was made using the operating system KALI LINUX because this software has very powerful tools to perform tests of pentesting, such as We will see in the document we use a few of the thousands that exist other actions can be done thanks to this operating system like violating the WI-FI networks, to culminate results were obtained with the tools that were put to test mode for the Conducting the investigation using a sniffer IDS/IPS and simulating an intrusion to see what values provided us and how it behaved security.

Key words: Kali, security, attack, networks

I.INTRODUCCIÓN

La seguridad de la información, según la norma ISO 27002:2013 es un proceso que busca proteger la confidencialidad, integridad y disponibilidad de la información, contra un compendio de amenazas, en pro de asegurar la continuidad del negocio, disminuir los posibles daños y maximizar el retorno de la inversión en la organización (ISO/IEC, 2012). [1], podemos entender como seguridad un estado de cualquier tipo de información que nos indica que ese sistema está libre de peligro, daño o riego. Para la mayoría de expertos el concepto de seguridad informática es supuesto porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características: integridad, confidencialidad, disponibilidad, no repudio. [2]

La interconexión entre redes ocasiona riesgos en la Red de Área Local, los cuales pueden ser ataques que provienen desde fuera o incluso pueden ser desde la misma red interna, algunos atentados cibernéticos pueden ser virus, gusanos, o hackers que aprovechando la poca seguridad del sistema informático explotan algunas vulnerabilidades que son descuidadas por los administradores la red, en este documento se podrá evidenciar la seguridad en la data que posee la Universidad Técnica Estatal de Quevedo, a su vez proponer distintas herramientas de código abierto que se puedan implementar para mejorar dicha seguridad en la institución en caso de ser requerido, ayudando de así que la institución cumpla con las cuatro características fundamentales del acceso a esta información. [3]

II.METODOLOGÍA

Analizar la seguridad de la data utilizando herramientas de código abierto que permitan brindar mayor integridad a estas en la Universidad Técnica Estatal de Quevedo.

Fase1. Situación actual de la seguridad de la data que posee la universidad técnica estatal de quevedo(uteq) utilizando el sistema operativo kali linux

Mediante el sistema operativo Kali Linux se se ha obtenido los dispositivos conectados para determinar que dispositivo atacar una vez que se posea la dirección lógica y la dirección física, es decir; la mac del equipo

ISSN 1316-4821 / 2542-3401 UNIVERSIDAD, CIENCIA y TECNOLOGÍA *Volumen Especial Nº 04 (pp. 156-161)*

conectado, esto usando un comando:

nmap –v –sn (ip de la red/mascara)

El resultado de la ejecución del comando puede dar mejores resultados seleccionado el perfil de escaneo intenso como lo muestra la figura 1 y 2.

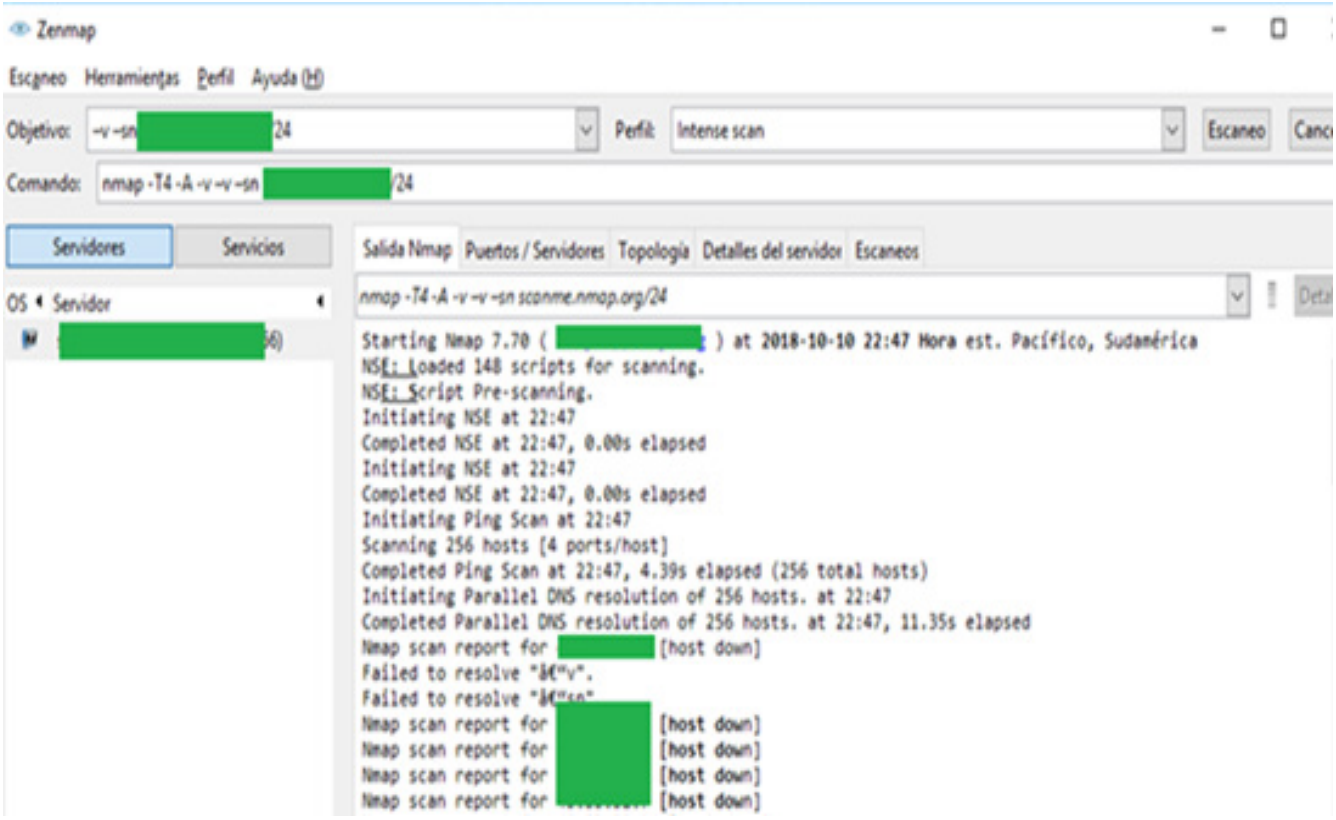

Figura 1. Resultado comando nmap –v –sn

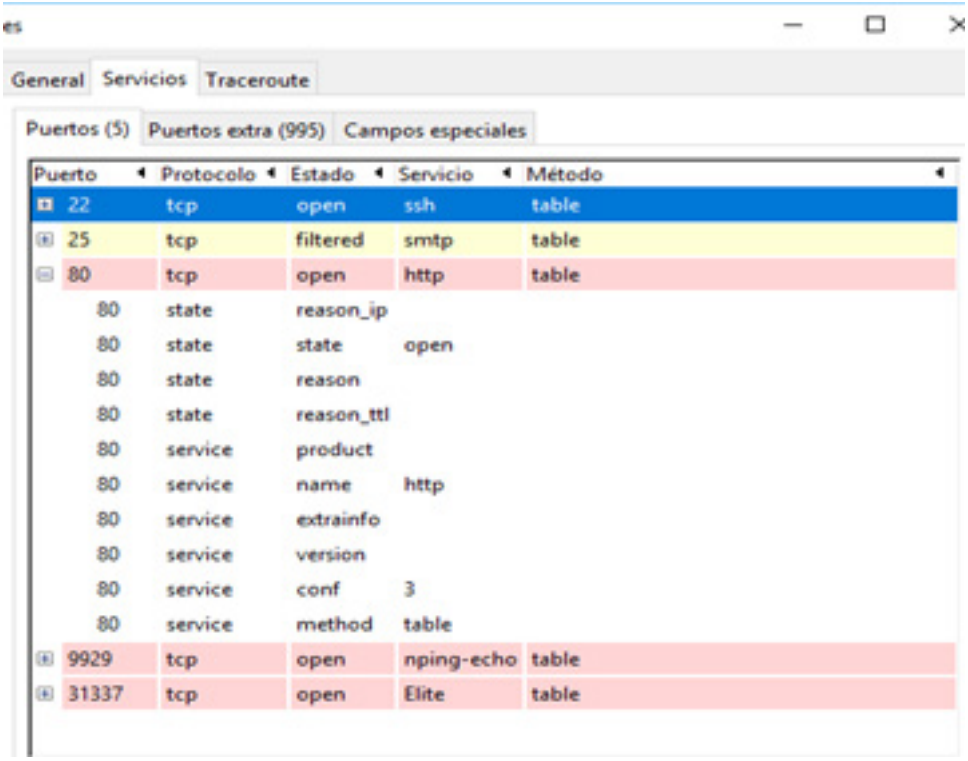

Figura 2. Puertos abiertos nmap –v –sn

Otro comando es el script safe que se utiliza cuando queremos ejecutar secuencias de comandos que son menos intrusivas para el target o víctima, de manera que será menos probable que causen la interrupción de algunas aplicaciones. Podemos ver en la próxima imagen, descubierta la dirección IP del router, el nombre de dominio de la red y más información.

Sintaxis: nmap –f - - script safe {ip de la víctima}

Este script safe se lo usa para ejecutar una serie de subcomandos para saber más información sobre el dispositivo que se está auditando o atacando, de esta forma tenemos datos más precisos por ejemplo que servidor nos está brindando dominio y una ip para acceder al servicio de internet dentro de la institución, la figura 3, 4 y 5 nos dan resultados sobre el equipo que se está revisando

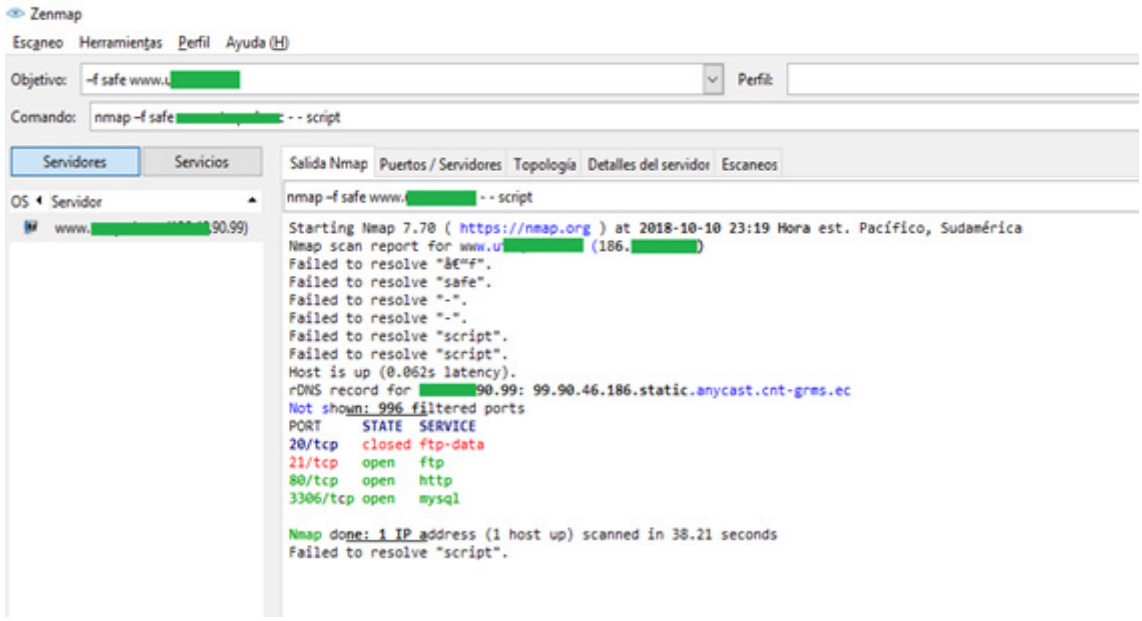

Figura 3. script safe – verificando información de equipo

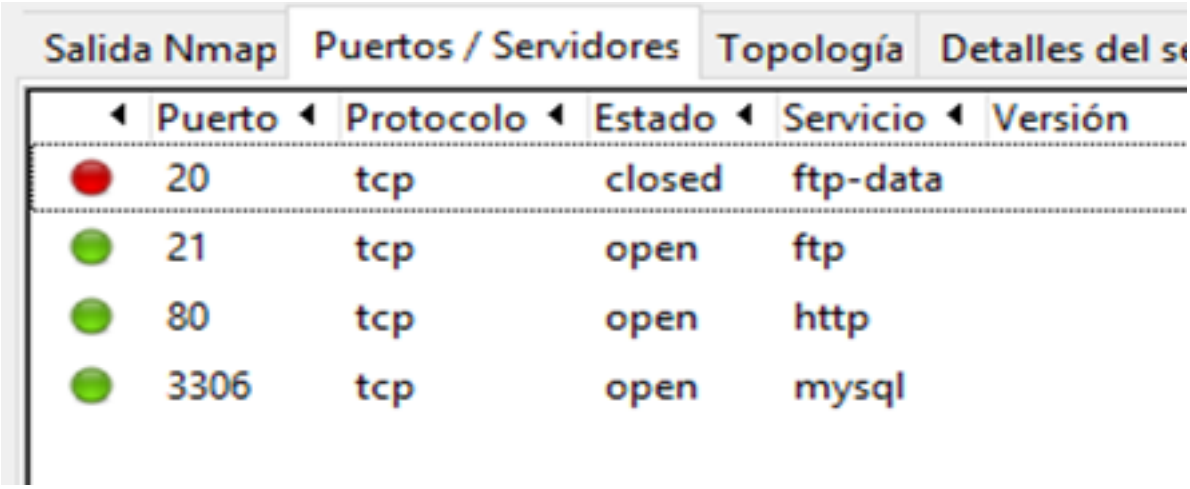

Figura 4. script safe – puertos open - closed

ISSN 1316-4821 / 2542-3401 UNIVERSIDAD, CIENCIA y TECNOLOGÍA *Volumen Especial Nº 04 (pp. 156-161)*

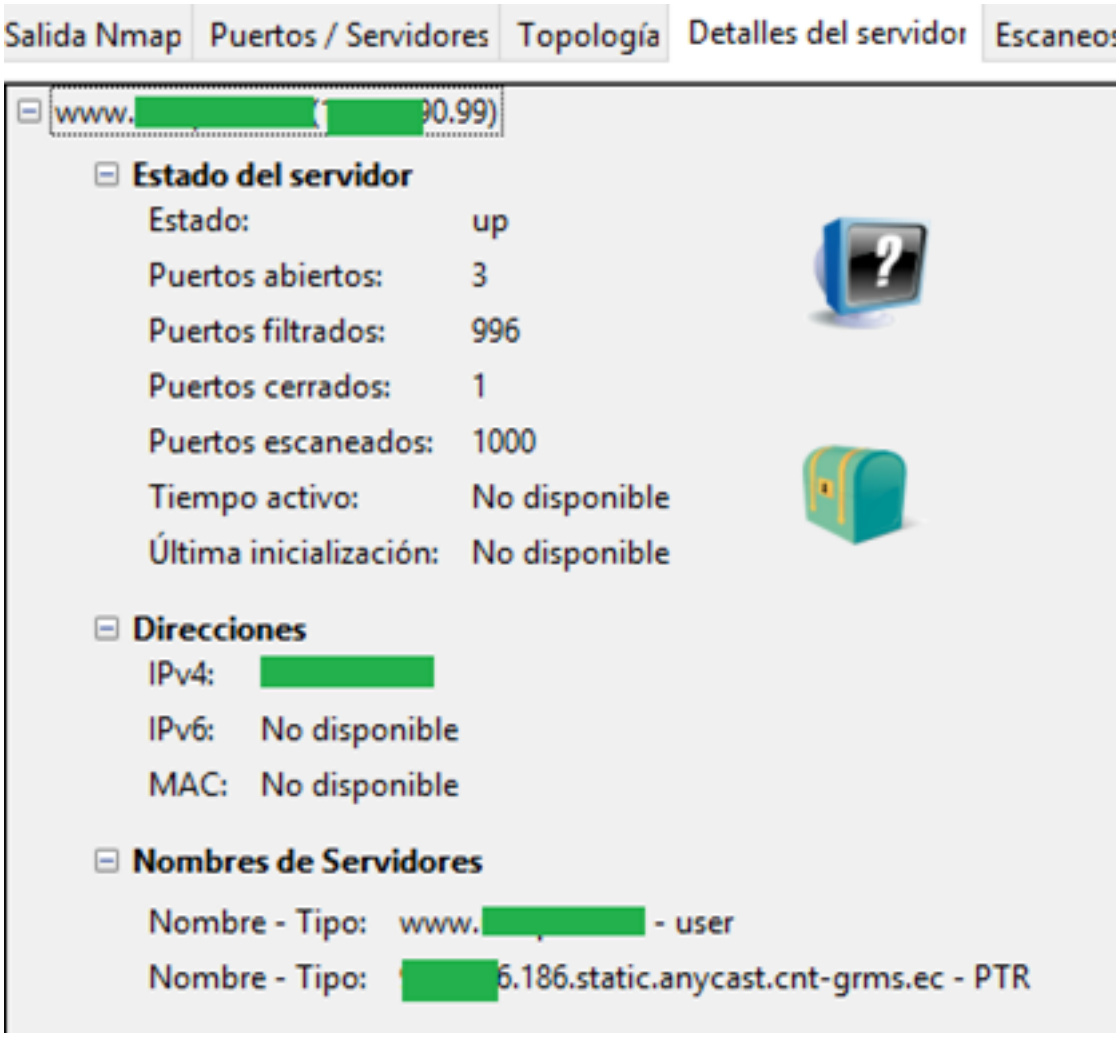

Figura 5. script safe – detalles del servidor

Se muestra el resultado de un script de nmap aplicado a un servidor donde me dirá si hay alguna vulnerabilidad de autenticación, es decir si hay login predeterminados como por ejemplo usuario: admin y contraseña: admin. Como podemos observar en este análisis esa vulnerabilidad no existe.

Sintaxis: nmap –f –sS –sV - -script auth (ip de la víctima).

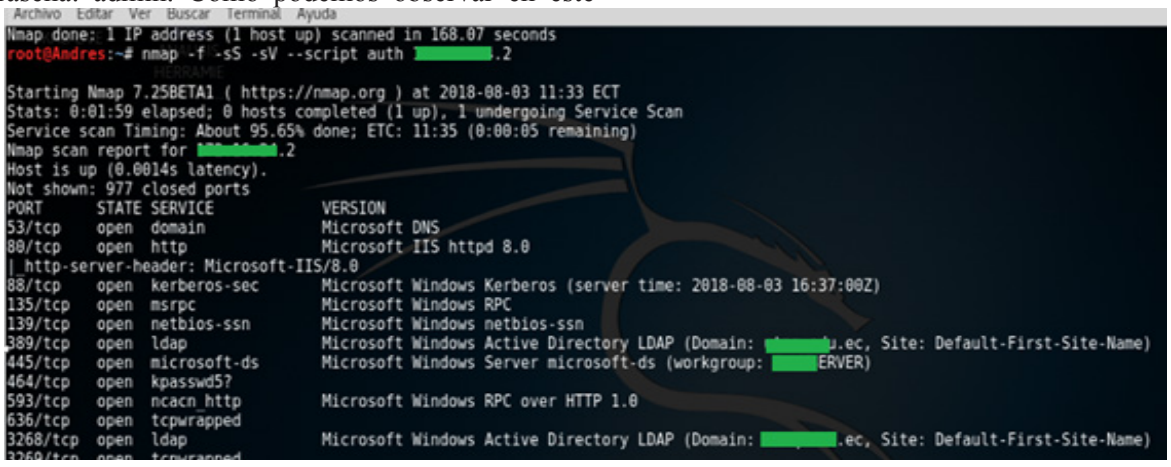

Figura 6. script auth

ISSN 1316-4821 / 2542-3401 UNIVERSIDAD, CIENCIA y TECNOLOGÍA *Volumen Especial Nº 04 (pp. 156-161)*

La figura 6 nos informa que no hay una vulnerabilidad en el servidor o que tenga alguna clave y usuario predeterminada a más de eso también nos muestra los puertos que están abiertos en el dispositivo al cual estamos escaneando

Fase 2. Herramientas de códigos abiertos de seguridad que permitan mejorar la seguridad de la data.

Sistemas de Detección de Intrusos

Un Sistema de Detección de Intrusos (IDS) basado en red (IDSN) open source. Cuenta con un lenguaje de creación de reglas en el que se pueden definir los patrones que se utilizarán a la hora de monitorizar el sistema. Además, ofrece una serie de reglas y filtros ya predefinidos que se pueden ajustar durante su instalación y configuración para que se adapte lo máximo posible a lo que deseamos. [4]

NetCat: trabaja sobre distintos sistemas operativos, y su principal aportación es que permite abrir puertos de seguridad en un servidor, además de encontrar errores de seguridad y apertura de puertos en aplicaciones de red. [3].

TCPDump: es una herramienta que permite el monitoreo de sistemas en red, así como la adquisición de datos, con lo cual pueden generarse informes sobre el tráfico y por lo tanto mantener en constante vigilancia los accesos al sistema. [3].

Zentyal Server: es una plataforma web basada en Linux, con modelo de software libre de código abierto que funciona como una aplicación web que utiliza un servidor web apache para la administración de servicios de red como DNS, Proxy, Firewall. [5].

III.RESULTADOS

Nuevo estado de seguridad en la data en la uteq poniendo a prueba el funcionamiento de la herramienta de seguridad instalada en el departamento de TIC's.

Para que este objetivo se pueda cumplir se realizó otro escaneo de la red, para poder comparar el comportamiento de la herramienta antes vistas cabe recalcar que se utilizó un IDS/IPS llamado Snort

Snort es un IDS/IPS cuenta con un lenguaje de creación de reglas en el que se pueden definir los patrones que se utilizarán a la hora de monitorizar el sistema. Además, ofrece una serie de reglas y filtros ya predefinidos que se pueden ajustar durante su instalación y configuración para que se adapte lo máximo posible a lo que deseamos. [6].

Snort puede funcionar como sniffer, registro de paquetes o como un IDS normal (en este caso NIDS). Cuando un paquete coincide con algún patrón establecido en las reglas de configuración, se loguea. Así se sabe cuándo, de dónde y cómo se produjo la amenaza.

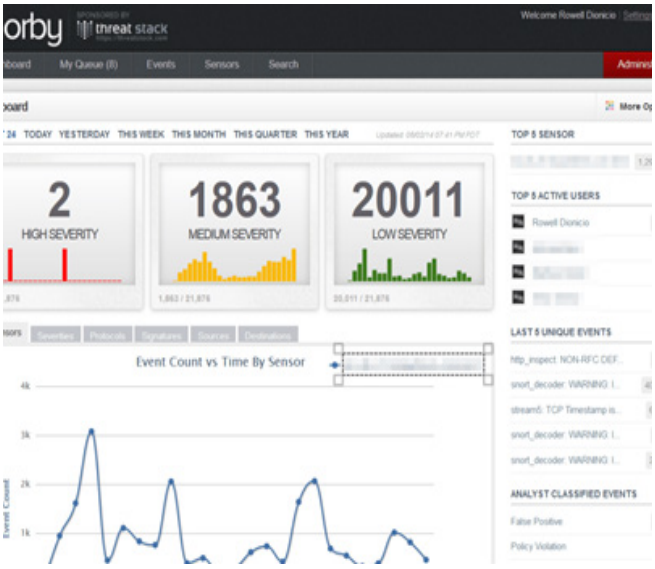

Figura 7. Alertas mediante snorby

La figura 7 nos muestra el número de alertas que se producen de acuerdo a las reglas que se le aplican, las cuales las divide jerárquicamente las alertas a cuáles hay que ponerle mayor atención y cuales se les puede dejar pasar por alto. Las pruebas que se hicieron no era de una intrusión severa por eso tenemos números elevados en los que son amenazas bajas.

En el caso de que el acto de intrusión sea considerado severo por este sistema cambiarían los valores depende el caso que esté ocurriendo y como haya sido configurado en sniffer.

Acerca de este tema existen muchas interrogantes de las formas de vulnerar la seguridad de la información, ya que dicho activo a más de ser muy importante para cualquier organización se vuelve atractivo para personas ajenas al contenido que se protege ya sea para hacer daño, obtener beneficios propios como ganar dinero secuestrando la información y pidiendo dinero a cambio para devolver lo robado integro, entre otras formas de usar lo tomado sin consentimiento, por eso analizando las diferentes herramientas de seguridad ya sean físicas o de software y porque mejor aun haciendo uso de las dos para hacer más robusta nuestra seguridad haciendo que la persona que se ha propuesto infiltrarse en la red y robar la información desista porque la seguridad es casi invulnerable, se dice invulnerable porque un sistema cien por ciento seguro no hay, lo que sí se puede asegurar es que el riesgo de ser vulnerado es bien bajo para así tener segura la información contando con las cuatro características más importantes acerca de la protección de los datos como son confidencialidad, integridad, disponibilidad y no repudio.

ISSN 1316-4821 / 2542-3401 UNIVERSIDAD, CIENCIA y TECNOLOGÍA Volumen Especial Nº 04 (pp. 156-161)

IV.CONCLUSIONES

•Mediante el análisis realizado al estado de la red de la UTEQ, se ha evidenciado que, aunque está establecida de manera correcta, con excelentes equipos y una buena seguridad, esta tiene una vulnerabilidad en uno de los servidores como pudimos darnos cuenta en lo que se realizó este proyecto, sin embargo, el nivel de impacto que tiene este fallo no es muy grave ya que con el avance de la tecnología y las seguridades se puede mitigar en su mayor parte a esta vulnerabilidad.

•Se logró analizar y definir qué herramientas se pueden implementar en la red para lograr una mejor seguridad de la data, lo cual proporciona una mayor confidencialidad, seguridad, disponibilidad y de más a la información almacenada solo a las personas que están autorizadas para tener el texto en claro, legible y sin que en el trascurso sufra alguna modificación dentro de ella conllevando a la integridad de los datos o información mostrada.

•Al realizar las pruebas se puede concluir que al instalar una herramienta de seguridad ayuda a detectar y actuar mientras estén pasando los sucesos o a su vez antes de que el daño sea mayor y casi irreparable, dando así una mayor confiabilidad, disponibilidad, integridad tanto en la data como en la infraestructura de la red física y lógica.

V.REFERENCIAS

[1] D. J. Parada, A. Flórez y U. Gómez, «Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas,» Scielo, Febrero 2018.

[2] H. L. T. CARRIÓN, Diseño de la Seguridad Informática en la implementacion del Data Center de la Universidad Nacional de Loja, Loja, 2010.

[3] J. A. Amaro López y C. R. Rodríguez Rodríguez, «Seguridad en internet,» Scielo, 2015.

[4] G. Kumar and K. Kumar, «The Use of Multi-Objective Genetic Algorithm Based Approach to Create Ensemble of ANN for Intrusion Detection,» International Journal of Intelligence Science, Vol. 2 No. 4A, pp. 115-127, 2012.

[5] Cristín Jaime Seguí, «Servicios Internet para pymes con zential,» 2015. [En línea]. [Último acceso: 2018].

[6] D. Ortego Delgado, «Openwebinars,» 21 Marzo 2017. [En línea]. Available: https://openwebinars.net/blog/que-es-snort/.

[7] speedguide.net, «speedguide.net,» 29 Enero 2014. [En línea]. Available: https://www.speedguide.net/port.php?port=139.

[8] Iván Cruz Aceves, José Miguel Campos, «http://roa.uveg.edu.mx/repositorio/licenciatura2015/237/HerramientasdeSeguridad.pdf,» 2015. [En línea]. [Último acceso: 2018].