GESTIÓN Y SOPORTE DE SEGURIDAD EN HARDWARE Y SOFTWARE

Autenticación y protocolos de seguridad

Unidad 3

ESCUELA DE CONSTRUCCIÓN E INGENIERÍA

Director: Marcelo Lucero Yañez

ELABORACIÓN

Experto disciplinar: Felipe Reyes Cáceres

Diseñador instruccional: Antonio Colmenares Prieto

Editora instruccional: María José Fonseca Palacios

VALIDACIÓN

Experto disciplinar:

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Didactic

AÑO

2022

Tabla de contenidos

Aprendizaje esperado 4

Introducción 5

1. Políticas de sistema informático 5

2. Instalación de software de detección de problemas de seguridad en plataformas de servicios 8

2.1 Configuración IDS Snort 12

3. Criterios y políticas 19

Cierre 21

Referencias bibliográficas 22

Aprendizaje esperado

Implementan políticas y protocolos de seguridad informática, considerando gestión de hardware y software de red.

Introducción

Una política de seguridad se define a un alto nivel, es decir, qué se debe proteger y cómo, es decir, el conjunto de controles que se deben hacer cumplir. Esto se encuentra formulado en una serie de instrucciones técnicas y de procedimiento, que incluyen medidas técnicas y organizativas para el cumplimiento de las políticas antes mencionadas.

La definición de una política de seguridad debe basarse en una preidentificación y análisis de los riesgos de exposición de la información y debe incluir a todos los procesos, sistemas y personas de la organización. Además, debe ser aprobado por la dirección de la organización y comunicado a todos los empleados.

En esta ocasión, estudiaremos lo relacionado a las políticas de sistema informático. Además, revisaremos la instalación de software de detección de problemas de seguridad en plataformas de servicios.

1. Políticas de sistema informático

La creación de una política ISMS compatible con ISO27001 es un paso necesario, sin importar cuán exigente sea con respecto a cumplir con el estándar ISO. Lo que es difícil es entender el significado de los nombres de las siglas. La política de SGSI describe los objetivos que debe lograr el SGSI, así como otros detalles clave. También define las medidas y métodos que utilizará para lograr esos objetivos. Además, explica cómo

se implementará el SGSI en ubicaciones específicas dentro de la organización.

Esencialmente, la política ISMS es un medio para establecer reglas y pautas que también sirven para armonizar las expectativas antes de embarcarse en un proyecto tan grande. Un SGSI, o Sistema de Gestión de Seguridad de la Información, es una medida de seguridad que salvaguarda la información. ¿No es esto redundante? La norma ISO 27001 recomienda utilizar este sistema de procesamiento de datos para gestionar cualquier riesgo que pueda dañar información vital. Esto se debe a que el SGSI protege nuestra información digital, física y conversacional con medidas de seguridad. Es una estrategia y un programa de seguridad.

La política ISMS se forma oficialmente mediante el uso de un documento escrito. Llamada política ISMS, declara formalmente que se implementará un programa de seguridad dentro de la empresa. Después de su creación, sirve como punto de partida para el proyecto. Este recurso cubre muchas áreas temáticas diferentes, que incluyen: Antes de implementar un SGSI, una empresa debe comprender exhaustivamente su contexto, incluidos todos los materiales externos e internos relevantes. Esto lleva a formalizar los objetivos de la empresa, que son las metas específicas que se desean lograr a través del SGSI.

Antes de establecer un SGSI, es importante determinar el alcance o la variedad de temas, procedimientos y servicios que se verán afectados por el sistema. Decidir sobre los recursos, como dinero, personas y

tecnología, necesarios para implementar el SGSI. Determinar métodos para evaluar el desempeño y mejorar el sistema: pasos necesarios para mantener un SGSI exitoso. La creación de una política SGSI requiere definir su alcance, objetivos y validez. Comience por establecer el objetivo del documento.

Aunque todavía no hemos formulado los objetivos reales del SGSI, este paso sienta las bases de cómo funcionará la política. Una vez que esto esté completo, podemos pasar a definir los objetivos del programa. Además de ellos es importante destacar que los datos críticos de la empresa deben incluirse en el alcance de una política de SGSI.

Se deben incluir procesos y áreas tanto internas como externas para asegurar la vigencia de la política, por lo que es fundamental comunicar cuándo entra en vigor esta política, así como sus medidas asociadas. La creación de una política ISMS requiere definir quién está a cargo de sus responsabilidades. Estas personas supervisarán los deberes relacionados con la comunicación de las políticas, la aprobación de recursos y la capacitación de otros empleados para que comprendan las pautas.

Muchas empresas prefieren separar algunas de sus funciones en tres categorías principales. Por ejemplo, pueden optar por poner a cargo el rol de Alta Gerencia si no tienen un comité. Cualquier auditor debe familiarizarse con la autoridad que creó, revisó y publicó el documento que se examina, Esto debido a que se les debe explicar todas las áreas de un negocio afectadas por la política SGSI.

Debido a su importancia, el proyecto generalmente involucra la seguridad de la información o la alta dirección.

Definir el contexto de nuestra empresa e identificar los recursos que utilizaremos para cumplir con nuestros objetivos de seguridad es necesario para implementar un SGSI o programa de seguridad. Además, necesitamos identificar a las personas responsables de planificar e implementar nuestro programa de seguridad.

2. Instalación de software de detección de problemas de seguridad en plataformas de servicios

Un sistema de detección de intrusos o IDS es un programa que detecta la entrada no autorizada a una computadora o red. Un sistema de detección de intrusos generalmente viene equipado con sensores virtuales, como un rastreador de red. Estos sensores proporcionan al kernel de IDS datos sobre el entorno circundante. De esa forma, pueden detectar anomalías que indiquen posibles ataques o falsas alarmas.

Estas herramientas analizan el tráfico de red en busca de signos de un ataque, como escanear puertos o paquetes con formato incorrecto. Una vez analizados, detectan cualquier tráfico potencialmente malicioso y lo comparan con firmas de ataques conocidos. Los IDS

también observan el comportamiento y el contenido del tráfico que analizan. Un firewall normalmente viene con esta herramienta, combinadas, estas dos herramientas se vuelven excepcionalmente poderosas y luchan contra los intrusos gracias a la inteligencia del detector de intrusos y al poder de bloqueo del cortafuegos.

En tal sentido, es una herramienta eficaz para combatir los ataques. Los datos almacenados en el IDS a menudo contienen "firmas" de ataques anteriores. Estas firmas ayudan al IDS a diferenciar entre el uso legítimo de la computadora y el fraude. También distingue entre el tráfico regular de la red y los posibles ataques. Actualmente existen muchos IDS, como programas antivirus y de tipo jerárquico.

Cuando los intrusos intentan tomar el control de una computadora que ha sido HIDSed, dejan evidencia que puede usarse para encontrar e informar sus acciones. Así es como funcionan los HIDS: están diseñados para detectar señales de intrusión y notificar a las autoridades. Un IDS basado en la red que detecta ataques en todo el segmento de la red.

Este software debe operar en modo promiscuo y capturar todo el tráfico de la red. El software antivirus utiliza patrones preconfigurados para coincidir con una base de datos de firmas. De manera similar, un IDS basado en firmas compara todos los paquetes en la red y los compara con la base de datos.

Los IDS basados en anomalías observan la normalidad comparando el tráfico detectado con una línea de base establecida, estos sistemas notifican a los administradores cuando ocurre una actividad inusual para

que puedan tomar medidas correctivas. Un sistema IDS pasivo simplemente monitorea el área y alerta al administrador de seguridad de cualquier intrusión. Este bloqueo sirve como medida preventiva. La función de identificación reactiva alerta al administrador sobre posibles amenazas y también contiene y neutraliza la amenaza.

Un sistema de prevención de intrusiones o IPS es un sistema que reacciona ante un ataque evitando que continúe. Por ello, el acrónimo en inglés de esta medida de seguridad es Inprovement in Security, o IIS. Un IDS detecta una posible intrusión y almacena información sobre ella en una base de datos. Esta información luego se envía a través de una señal de alerta que se almacena en la base de datos. Un sistema pasivo solo responde a la actividad; activamente no detecta nada.

Un firewall usa una conexión externa para determinar si ocurrió una intrusión. Luego bloquea el acceso entre redes para evitar futuras intrusiones, sin embargo, los cortafuegos no suelen detectar las intrusiones que se producen dentro de la propia red, por el contrario, un sistema de detección de intrusos analiza la situación cuando ocurre. Cuando lo hace, hace sonar una alarma, los IDS supervisan los ataques que se originan en el sistema examinando las líneas de comunicación y detectando patrones comunes conocidos como firmas, identifican a través de heurísticas, o comportamientos aprendidos, sistemas que ya han sido clasificados como ataque y alertan a los operadores del sistema.

Los IDS también funcionan en conjunto para impedir que los usuarios maliciosos crucen el perímetro de la red y obtengan acceso a una organización. Snort es el Sistema de prevención de intrusiones oSys de código abierto líder en el mundo, sus reglas definen la actividad de red maliciosa y usan esa definición para encontrar paquetes coincidentes y generar alertas para el Sys. Además, se puede utilizar como rastreador de paquetes como el proporcionado por tcpdump, como registrador de paquetes e incluso como un sistema completo de prevención de intrusiones en la red.

Snort se puede descargar y configurar para uso personal y comercial por igual. Las reglas de Snort se descargan y configuran una vez que están disponibles para su distribución. Estas reglas se dividen en dos conjuntos: el **"Conjunto de reglas de la comunidad"** y el **"Conjunto de reglas de suscriptor de Snort"**.

Cisco Talos lanza un conjunto de reglas actualizado para sus clientes antes de probarlo. Este proceso se conoce como conjuntos de reglas de suscriptor de Snort. Snort.org contiene información sobre cómo implementar el conjunto de reglas en cualquier red. Cisco ya prueba y aprueba los conjuntos de reglas, y cualquier persona con una suscripción puede descargar las reglas y aplicarlas de inmediato. El conjunto de reglas de control de calidad para Cisco Talos se desarrolla utilizando datos de la comunidad de Snort. Puede ser accedido libremente por cualquier usuario.

2.1 Configuración IDS Snort

Paquetes a instalar

```
felipe@ubuntu:~$ sudo apt-get install traceroute
felipe@ubuntu:~$ sudo apt-get install snort
felipe@ubuntu:~$ sudo apt-get install tcpdump_
felipe@ubuntu:~$ sudo apt-get install netcat_
```

Figura 1. Paquetes a instalar

Fuente: Reyes, F. (2022)

Comentar desde la línea 549 hasta la 732, como se muestra en las siguientes imágenes:

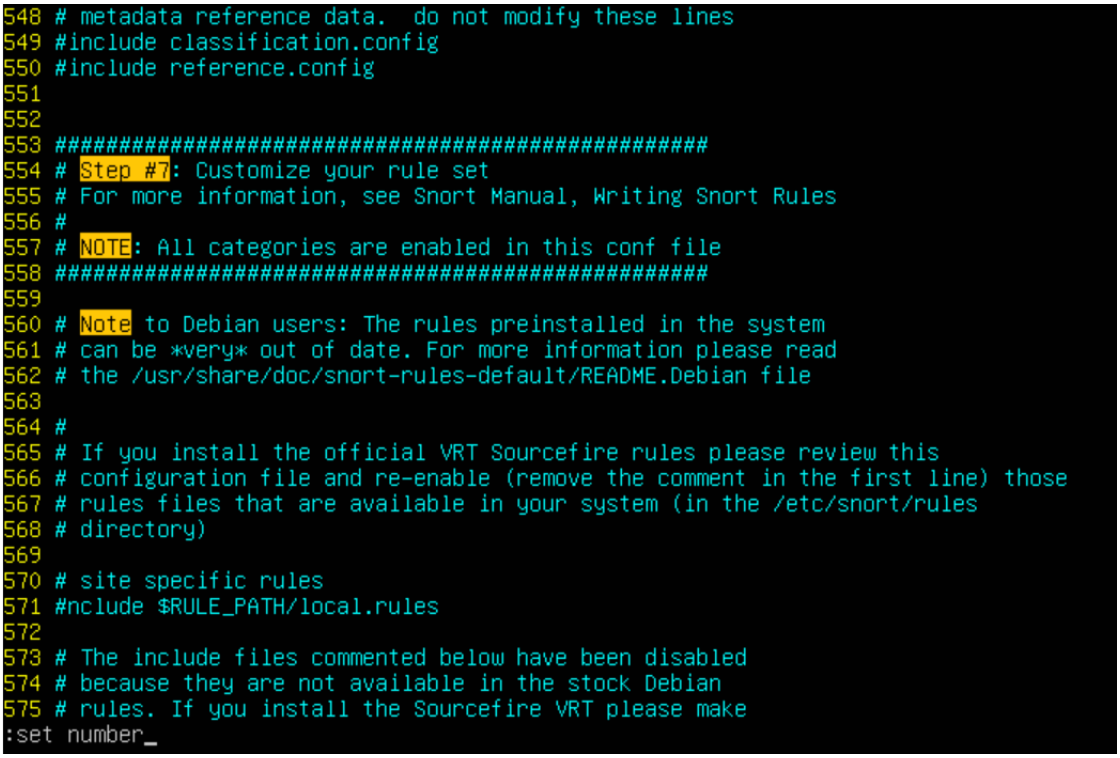


Figura 2. Configuración a realizar

Fuente: Reyes, F. (2022)

Ejemplo de alarmas

En la siguiente figura, podrán observar como se refleja un ejemplo de alarma en la herramienta.

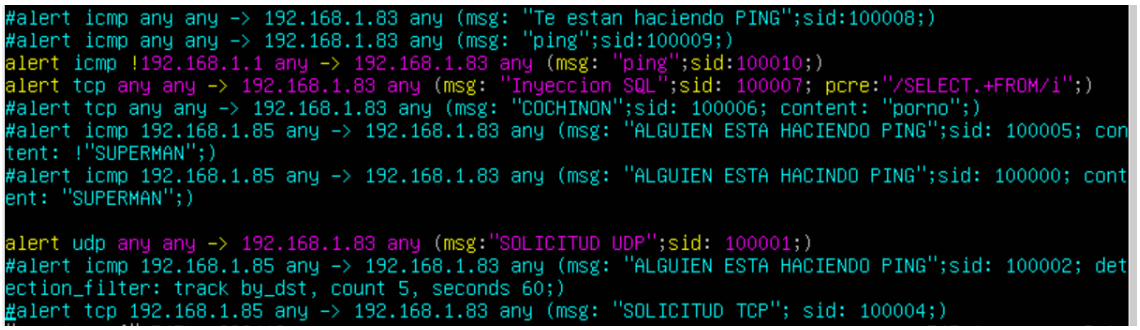


Figura 3. Ejemplo de alarmas

Fuente: Reyes, F. (2022)

Activar alarmas Snort

Figura 4. Activación de alarmas Snort

Fuente: Reyes, F. (2022)

Análisis de exclusiva de ICMP Ping

```
felipe@felipe:/etc/snort$ sudo tcpdump -nni enp0s3 -X icmp
[sudo] password for felipe:
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:15:48.522540 IP 192.168.1.88 > 192.168.1.13: ICMP echo request, id 1, seq 4786, length 40
        0x0000:  4500 003c 44f7 0000 8001 7214 c0a8 0158  E..<D.....r....X
        0x0010:  c0a8 010d 0800 3aa9 0001 12b2 6162 6364  ......:.....abcd
        0x0020:  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efghijklmnopqrst
        0x0030:  7576 7761 6263 6465 6667 6869            uvwabcdefghi
16:15:48.522595 IP 192.168.1.13 > 192.168.1.88: ICMP echo reply, id 1, seq 4786, length 40
        0x0000:  4500 003c f124 0000 4001 05e7 c0a8 010d  E..<.$..@.......
        0x0010:  c0a8 0158 0000 42a9 0001 12b2 6162 6364  ...X..B.....abcd
        0x0020:  6566 6768 696a 6b6c 6d6e 6f70 7172 7374  efghijklmnopqrst
        0x0030:  7576 7761 6263 6465 6667 6869            uvwabcdefghi
```

```
alert icmp any any -> any any (msg:"solicitud de Ping";sid:100003; content: "|1011 1213 1415|";)
```

Figura 5. Análisis de exclusiva ICMP Ping

Fuente: Reyes, F. (2022)

Análisis de exclusiva de ICMP Traceroute

```
16:47:56.228665 IP 192.168.1.13 > 192.168.1.153: ICMP 192.168.1.13 udp port 33439 unreachable, lengt
h 68
        0x0000:  45c0 0058 2fea 0000 4001 c604 c0a8 010d  E..X/...@.......
        0x0010:  c0a8 0199 0303 812d 0000 0000 4500 003c  .......-....E..<
        0x0020:  471a 0000 0211 eda0 c0a8 0199 c0a8 010d  G...............
        0x0030:  a440 829f 0028 5fc2 4041 4243 4445 4647  .@...(_.@ABCDEFG
        0x0040:  4849 4a4b 4c4d 4e4f 5051 5253 5455 5657  HIJKLMNOPQRSTUVW
        0x0050:  5859 5a5b 5c5d 5e5f                      XYZ[\]^_
```

```
alert icmp any any -> any any (msg: "Solicitud de traceroute";sid: 100000; content: "SUPERMAN";)
```

Figura 6. Análisis de exclusiva de ICMP Traceroute

Fuente: Reyes, F. (2022)

Alerta de contenido pornográfico

En la siguiente figura podrán observar la alerta al detectar un ingreso a contenido pornográfico.

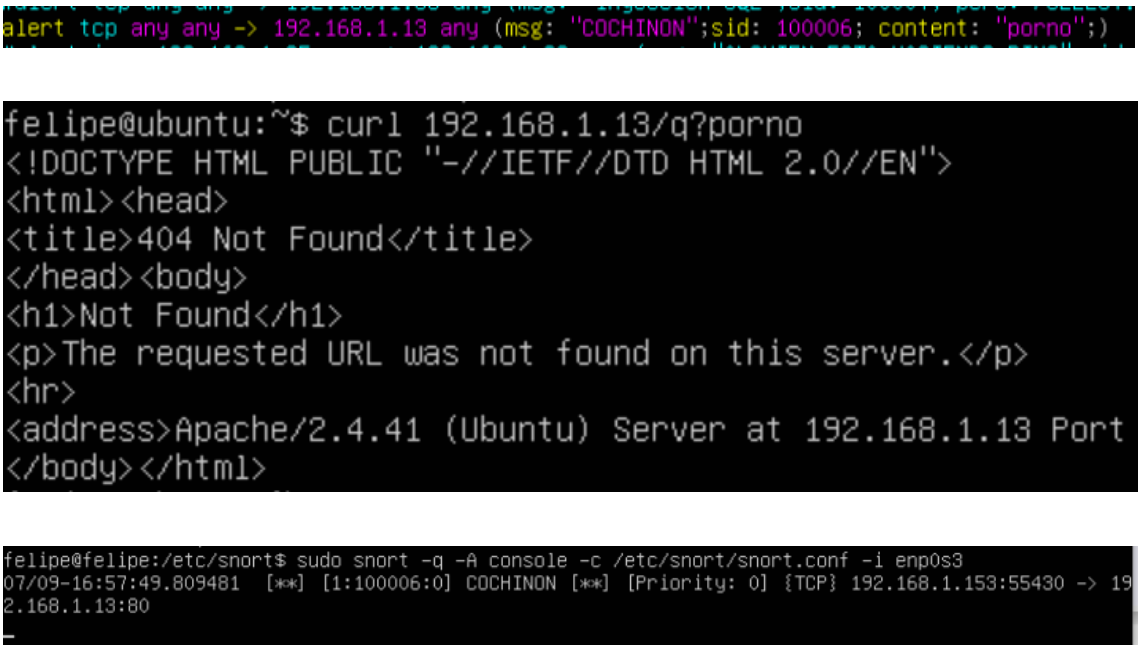


Figura 7. Alerta de contenido pornográfico

Fuente: Reyes, F. (2022)

Alerta inyección SQL

En la siguiente figura podrán observar la alerta al detectar un ingreso de una inyección SQL.

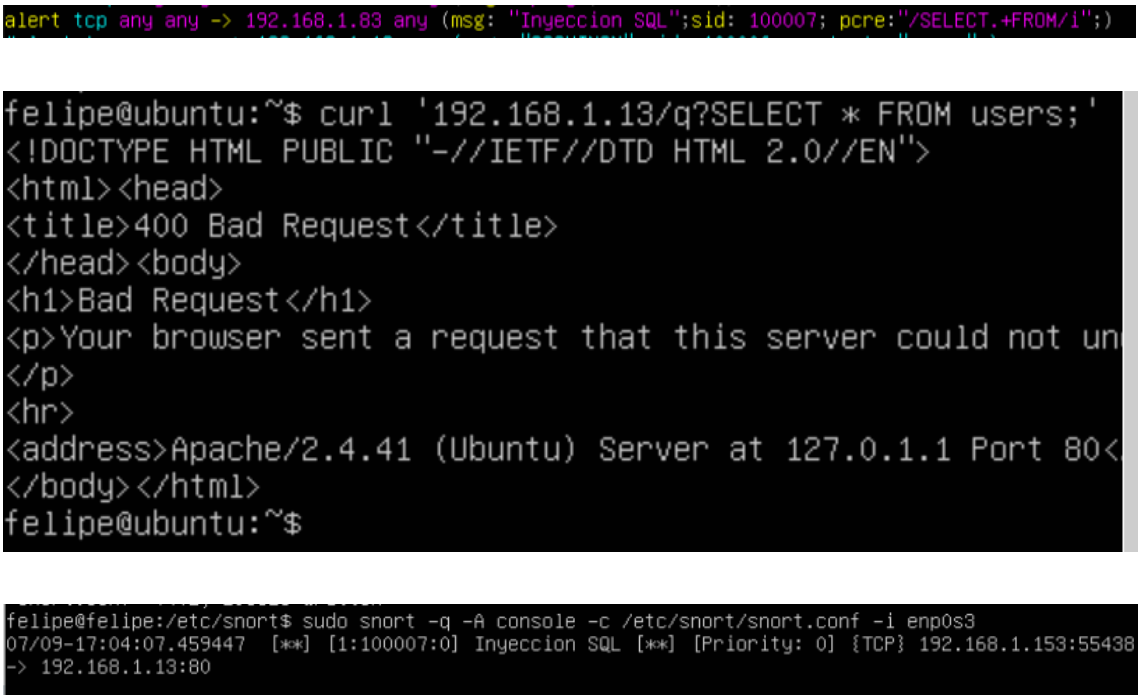
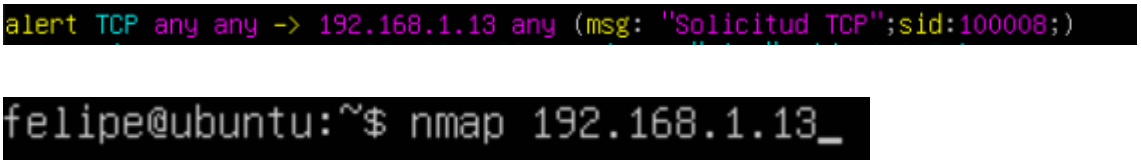


Figura 8. Alerta de inyección SQL

Fuente: Reyes, F. (2022)

Solicitud TCP

Al momento de realizar la solicitud TCP, deberá reflejarse de la siguiente manera:



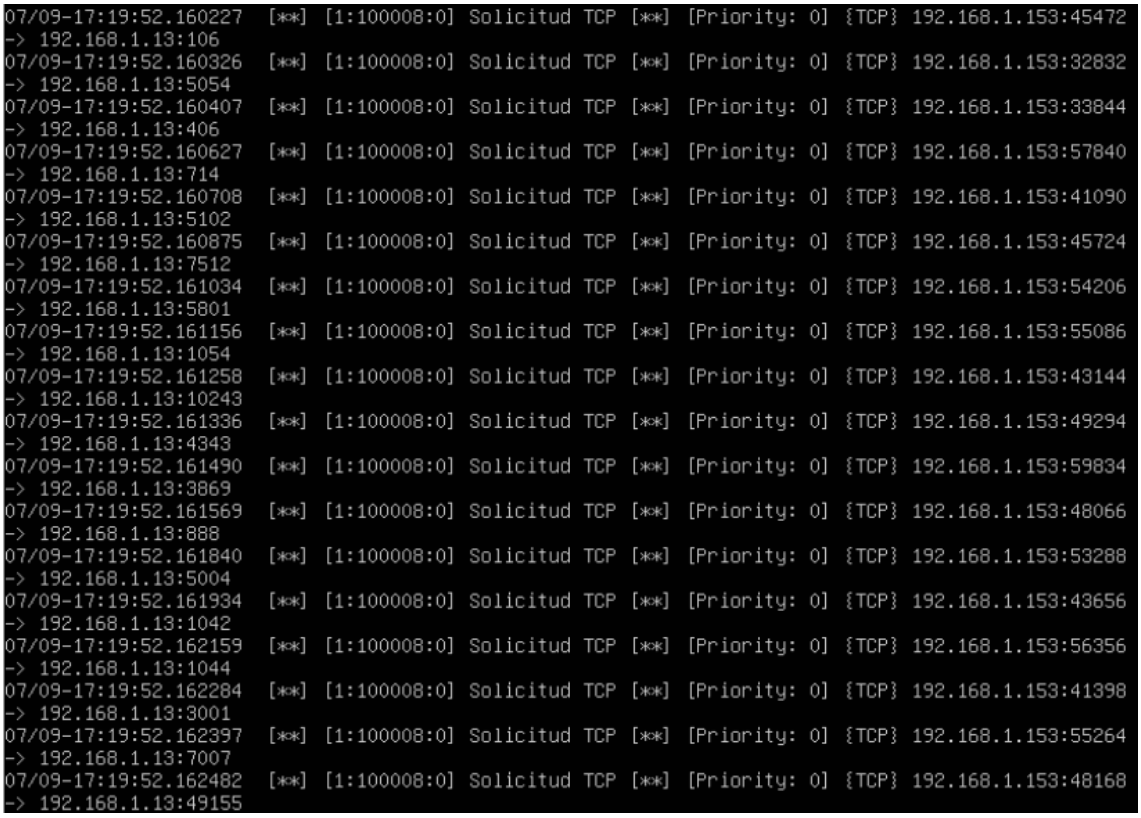


Figura 9. Solicitud TCP

Fuente: Reyes, F. (2022)

Solicitud UDP

Al momento de realizar la solicitud UDP, deberá reflejarse de la siguiente manera:

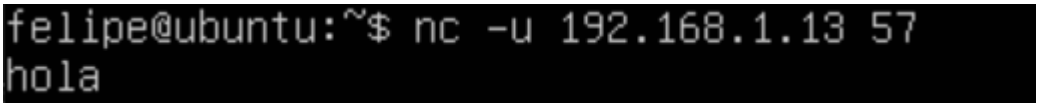


Figura 10. Solicitud UDP

Fuente: Reyes, F. (2022)

3. Criterios y políticas

La creación de una política de seguridad de la información requiere discordia porque muchos creen que el producto terminado debe incluir todos los aspectos de la seguridad. La gente argumenta que esto es necesario porque la norma ISO27001 redacta el documento de acuerdo con lo tradicional.

La política de seguridad de la información ISO 27001, debe seguir un estándar establecido. Comprender esto es importante al crear el plan de seguridad de la información de una empresa. ¿Qué significa ISO 27001? ¿Cómo define este documento la seguridad de la información? Y lo que debería estar en él. Algunas organizaciones todavía no entienden la importancia de la Seguridad de la Información, como tal, está claro que muchas personas no son conscientes de su importancia.

El papel que juega en la protección de la organización es clave. La política de Seguridad de la Información describe los objetivos principales de la implementación del sistema. Es por esto, que el primer propósito de la política es transmitir los objetivos pretendidos de la gestión. Idealmente, el propósito de un documento es ayudar a las personas a comprender lo que está escrito sin exigirles que conozcan los detalles del

sistema, como los factores de evaluación de riesgos o quién es el responsable final de su creación.

El estándar establece que desarrollar una política de Seguridad de la Información requiere poco esfuerzo, por lo que, para garantizar el cumplimiento de las políticas de la empresa, cualquier documento debe adaptarse a las necesidades de la organización antes de ser utilizado.

Copiar el trabajo de otra organización también sería problemático debido a las diferencias significativas entre las necesidades de un fabricante industrial tradicional y un gran minorista virtual. Este documento debe detallar cómo se deben lograr los objetivos de seguridad de la información sin explicaciones específicas sobre los procesos de revisión e implementación.

El apartado inicial del documento es un compromiso, por lo que la Alta Dirección de la organización debe declarar claramente que está absolutamente dedicada a terminar con el propósito previsto del sistema: cumplir con los criterios de seguridad de la información establecidos por las partes interesadas.

Después de la creación del sistema, sus desarrolladores deben comunicar a las partes interesadas sobre futuros cambios, actualizaciones o mejoras. Esto debería incluir la evolución del sistema y su alcance.

Los programas de Seguridad de la Información deben ser revisados periódicamente e incluidos en sus correspondientes documentos. Estas

revisiones también deben abordar cuándo se llevará a cabo cada revisión y cuánto durará. La política de Seguridad de la Información debe ser lo más breve posible y clara en donde una extensión fácil de leer ayuda a evitar confusiones y facilita la implementación de las políticas. Las políticas adicionales del sistema, como el control de acceso, el uso aceptable y la clasificación, ayudan a lograr este objetivo.

Cierre

Después de estudiado lo correspondiente a la semana, se puede destacar lo siguiente:

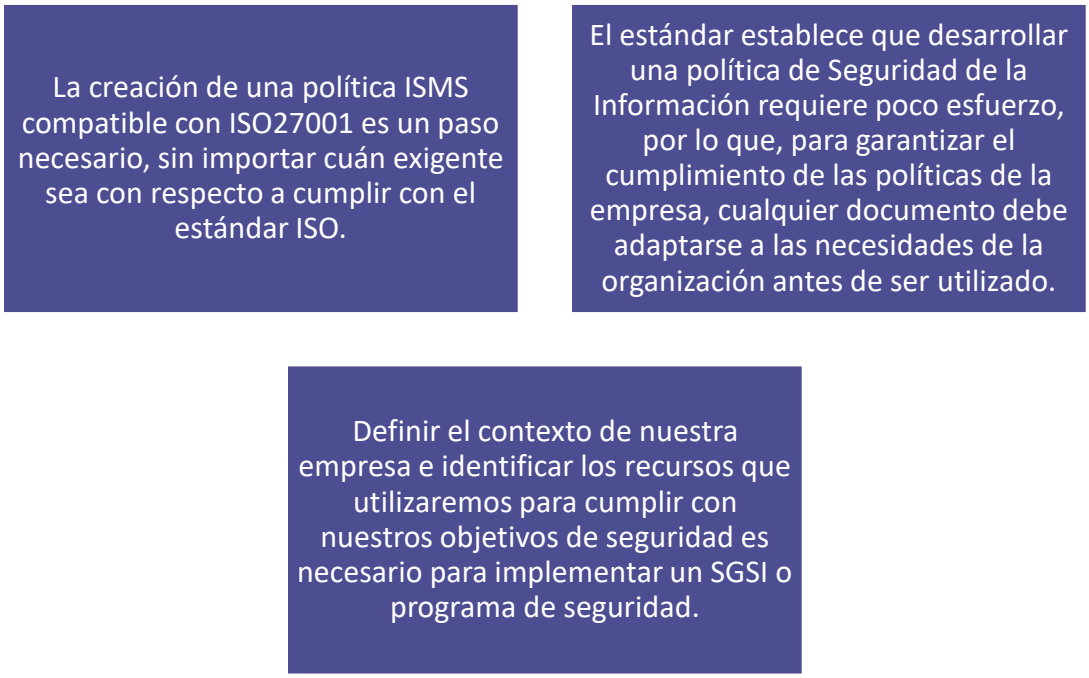


Figura 11. Ideas Claves, semana 6

Fuente: Reyes, F. (2022)

Referencias bibliográficas

CCNA Security 210-260 Official Cert Guide (Santos, Stuppi 2016)