UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

ESPECIALISTA EN RESPUESTA A INCIDENTES Y CÓMPUTO FORENSE

INFORME DE ACTIVIDADES PROFESIONALES

Que para obtener el título de

Ingeniera en Computación

P R E S E N T A

Nayely Morales Perales

ASESOR DE INFORME

Ing. Rafael Sandoval Vázquez

Ciudad Universitaria, Cd. Mx., 2019

Contenido

Introducción

En el presente documento describo las actividades que realicé en el proyecto de Seguimiento a Incidentes de Seguridad Informática en la Red Universitaria y la experiencia que adquirí como Especialista en Respuesta a Incidentes y Cómputo Forense. El objetivo principal del proyecto es gestionar los incidentes de seguridad informática reportados a la Coordinación de Seguridad Informática/UNAMCERT (CSI/UNAM-CERT), tanto en las dependencias de la UNAM (Red-UNAM) como en las entidades externas que lo soliciten. Para cumplir con el objetivo de este proyecto me basé en el Proceso de Manejo de Incidentes, el cual consta de 3 etapas principales: Detección, Gestión y Análisis.

Este proceso me permitió prepararme como miembro del equipo de respuesta a incidentes del CSI/UNAM-CERT para la identificación, contención, remediación y recuperación de Incidentes de Seguridad Informática, acorde a la dependencia que atendía(Red-UNAM, Externas). También pude aprender de los incidentes atendidos para lograr una mejora continua en la atención de los mismos.

Una actividad que me ayudó a cumplir con el objetivo del proyecto fue la actualización de la base de contactos del Sistema de Atención de Incidentes (SAI). Esto con la finalidad de contar con una base confiable para reportar oportunamente los incidentes que ocurrieran a los administradores a cargo del equipo afectado y, al mismo tiempo, brindarles asesoría en la solución de los incidentes en caso que ellos lo solicitaran, así como darle seguimiento para poder concluirlos en el menor tiempo posible.

De igual manera, otra actividad que desempeñaba cuando ocurría un incidente de seguridad era el análisis forense del equipo afectado o comprometido, por lo cual me fue imprescindible tener el conocimiento y aplicación de una metodología de análisis para otorgar confiabilidad a los hallazgos del mismo. Esta metodología la explico con ejemplos aplicables en equipos con sistema operativo LINUX o UNIX, ya que en mi experiencia profesional me enfoqué en estos sistemas.

1. Descripción de la organización

1.1. Historia

El UNAM-CERT fue fundado en 1993 a raíz de un incidente de seguridad en la supercomputadora Cray Y-MP4/46, que se encontraba en posesión de la Dirección General de Servicios de Cómputo Académico (DGSCA); dicho incidente consistió en un acceso no autorizado. Para detallar este incidente me referiré a la tesis de Licenciatura del Doctor Zamboni:

> El 10 de Julio de 1993, la Lic. Martha A. Sánchez Cerezo, jefa del Departamento de supercómputo, descubrió en la supercomputadora una cuenta llamada *god*, asignada a un usuario no existente. La falsedad de esta cuenta era evidente desde su nombre: *god* es "Dios" en inglés. Al hacer una revisión detallada de la cuenta, se vio que pertenecía a todos los grupos y tenía activados todos los permisos, situación en la que ningún usuario de la Cray (ni siquiera root) se encuentra.

Este incidente puso en evidencia la importancia de la seguridad en cómputo en la UNAM y, percatándose de esta vulnerabilidad, el mismo Doctor Zamboni crea el equipo de respuesta a incidentes de seguridad en cómputo que perteneció a DGSCA.

Durante el período de 1999-2001 UNAM-CERT realizó su trámite de acreditación ante el *Forum of Incident Response Security Teams* (FIRST), convirtiéndose en el primer equipo de respuesta a incidentes reconocido internacionalmente en México. Esto condujo a su vez a UNAM-CERT a ser el punto de contacto internacional para atender incidentes no sólo en Red-UNAM, sino en México.

En 2005 se unió al proyecto Honeynet con Honeynet UNAM-CHAPTER. Este proyecto le permite al UNAM-CERT estar en contacto con otras organizaciones internacionales para intercambiar nuevas tecnologías de detección de intrusos y demás temas de interés para la seguridad de la información.

En 2014 se convirtió en la CSI/UNAM-CERT (Coordinación de Seguridad de la Información) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC).

1.2. Misión y Visión

Misión:

Contribuir al desarrollo de la UNAM, a través de la prestación de servicios especializados, la formación de capital humano y el fomento de la cultura de seguridad de la información.

Visión:

Consolidar a la UNAM como la entidad líder en materia de Seguridad de la Información en el país.

1.3. Objetivos

- Proporcionar servicios de seguridad de la información para la UNAM y otras organizaciones.
- Promover la cultura de seguridad de la información.
- Formar especialistas que desarrollen y apliquen estrategias de protección de la información.
- Difundir contenidos especializados en seguridad de la información.
- Colaborar con instituciones nacionales e internacionales en materia de detección y respuesta a incidentes.
- Elaborar políticas y lineamientos de seguridad de la información para las dependencias y entidades académicas universitarias.

1.4. Principios

La CSI (Coordinación de Seguridad de la Información) de la Dirección General de Cómputo y de Tecnologías de Información y Comunicación es un punto de encuentro al cual puede acudir la comunidad de cómputo para obtener información, asesorías o servicios de seguridad; así como para intercambiar experiencias y puntos de vista, logrando con ello, establecer políticas de seguridad adecuadas, disminuir la cantidad y gravedad de los problemas de seguridad y difundir la cultura de la seguridad en cómputo.

1.5. Ética

Para los miembros de la Coordinación de Seguridad de la Información de la UNAM, el UNAM-CERT, es un honor que la Universidad los privilegie depositando su confianza y coadyuven en el aseguramiento de los activos tecnológicos de la misma.

Por esto se conducen en base a los siguientes principios éticos:

- Proteger y preservar la infraestructura tecnológica de la Universidad y las organizaciones que nos privilegien con su confianza.

- Actuar de forma honorable, honesta, responsable y legal.
- Proveer servicios profesionales y de forma expedita.

Para alcanzar estas metas la CSI/UNAM-CERT:

- Proporciona información clara y expedita en materia de seguridad informática en situaciones de desastre o contingencias tecnológicas a la comunidad en general en caso de ser requerido.
- Asegura la privacidad de la información que maneja a lo largo de cualquiera de los procesos o servicios que la CSI/UNAM-CERT proporcione la Universidad o cualquier Institución o persona que lo solicite.
- Garantiza la confidencialidad de la información de usuarios y/o sistemas que nuestros clientes o usuarios pongan a nuestra disposición.
- Todos nuestros servicios serán prestados de forma profesional, expedita y en base a estándares de calidad.

1.6. Servicios que ofrece

UNAM-CERT pone a disposición de organizaciones internas y externas los siguientes servicios de Seguridad en Tecnologías de la Información:

1.6.1. **Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo al estándar ISO 27001:2013**

Contempla el ciclo de implantación del sistema de gestión de seguridad de la información de acuerdo al estándar ISO 27001. Se basa en el ciclo PDCA (*plan, do, check, act*) de mejora continua. Además de la implantación de los controles del estándar de acuerdo al alcance definido y del análisis de riesgos en búsqueda de la certificación por parte de una autoridad avalada por ISO**.**

1.6.2. **Auditoría informática**

Permite determinar el grado de cumplimiento de gestión de seguridad de la información que realiza el cliente respecto a recomendaciones y lineamientos de las mejores prácticas y estándares en materia de seguridad informática.

Su objetivo es dar a conocer las fortalezas y debilidades en la gestión de la seguridad de la información y emitir recomendaciones para mejorar su desempeño.

1.6.3. Análisis forense

Permite identificar huellas específicas de actividad en un sistema informático y determinar los eventos relevantes para una investigación. Los resultados obtenidos pueden ser útiles como elemento para deslindar responsabilidades y para mejorar la seguridad de la infraestructura informática de la organización.

1.6.4. Análisis de vulnerabilidades y pruebas de penetración

Permite identificar defectos de configuración presentes en la infraestructura tecnológica de una organización, también evalúa efectividad de los mecanismos de seguridad existentes ante un ataque.

1.6.5. Análisis de tráfico de red

Se caracterizan los flujos de información existentes en la red del cliente, identificando así el tráfico malicioso que no es visible por el usuario final o por el administrador, también se pueden identificar ataques internos o robo de información. Al final se emiten recomendaciones que permitirán filtrar el tráfico de la red, aumentando la eficiencia de la operación interna.

1.6.6. Análisis de riesgos

A través de la metodología OCTAVE Allegro, este servicio permite identificar el inventario de activos de la información valiosos para la organización. Tras esta identificación se calculan los riesgos de acuerdo a las amenazas y vulnerabilidades presentes.

1.6.7. Respuesta a incidentes de seguridad de la información

Este servicio permite identificar, contener, erradicar y recuperar la estabilidad de la infraestructura tecnológica ante un incidente de seguridad de la información.

1.6.8. Revisión de configuraciones

Se lleva a cabo la revisión de configuraciones de seguridad de los equipos con base en las mejores prácticas de seguridad. Identificando errores en la implantación de mecanismos de seguridad como firewalls, IPSs, IDSs, anti-spam y antivirus.

1.6.9. Creación de políticas de seguridad de la información

Se identifican las necesidades de seguridad de la información del cliente y se generan recomendaciones que podrán ser traducidas en políticas

conjuntamente con los responsables dentro de la organización. Dichas políticas proveen el marco necesario para la instauración de un esquema integral de seguridad de la información.

1.6.10. Programas y cursos de capacitación

- *Programa de Becas de Formación en Seguridad Informática*

  Este programa tiene como objetivo formar recursos humanos especializados en el campo de seguridad informática, a través de capacitación en metodologías y técnicas para proteger la información y la infraestructura tecnológica de las organizaciones. Este programa tiene un año y medio de duración.

- *Congreso de Seguridad en Cómputo*

  Durante este evento se imparten cursos de alta especialización sobre seguridad de la información y se desarrollan conferencias con la participación de destacados especialistas nacionales e internacionales. Se realiza de manera anual.

Líneas de especialización y talleres que se imparten:

- L1 Cómputo forense y legislación relacionada
- L2 Análisis de vulnerabilidades, técnicas de intrusión y pentest
- L3 Detección de intrusos y tecnologías honeypot
- Desarrollo seguro de aplicaciones web
- Seguridad en Apache HTTPD y manejadores de contenido
- Análisis de software malicioso
- Hardening en sistemas operativos Linux
- Implementación del SGSI (ISO/IEC-27001:2013)
- Seguridad en servicios en redes Windows
- Aspectos legales de la seguridad informática

1.7. Organigrama

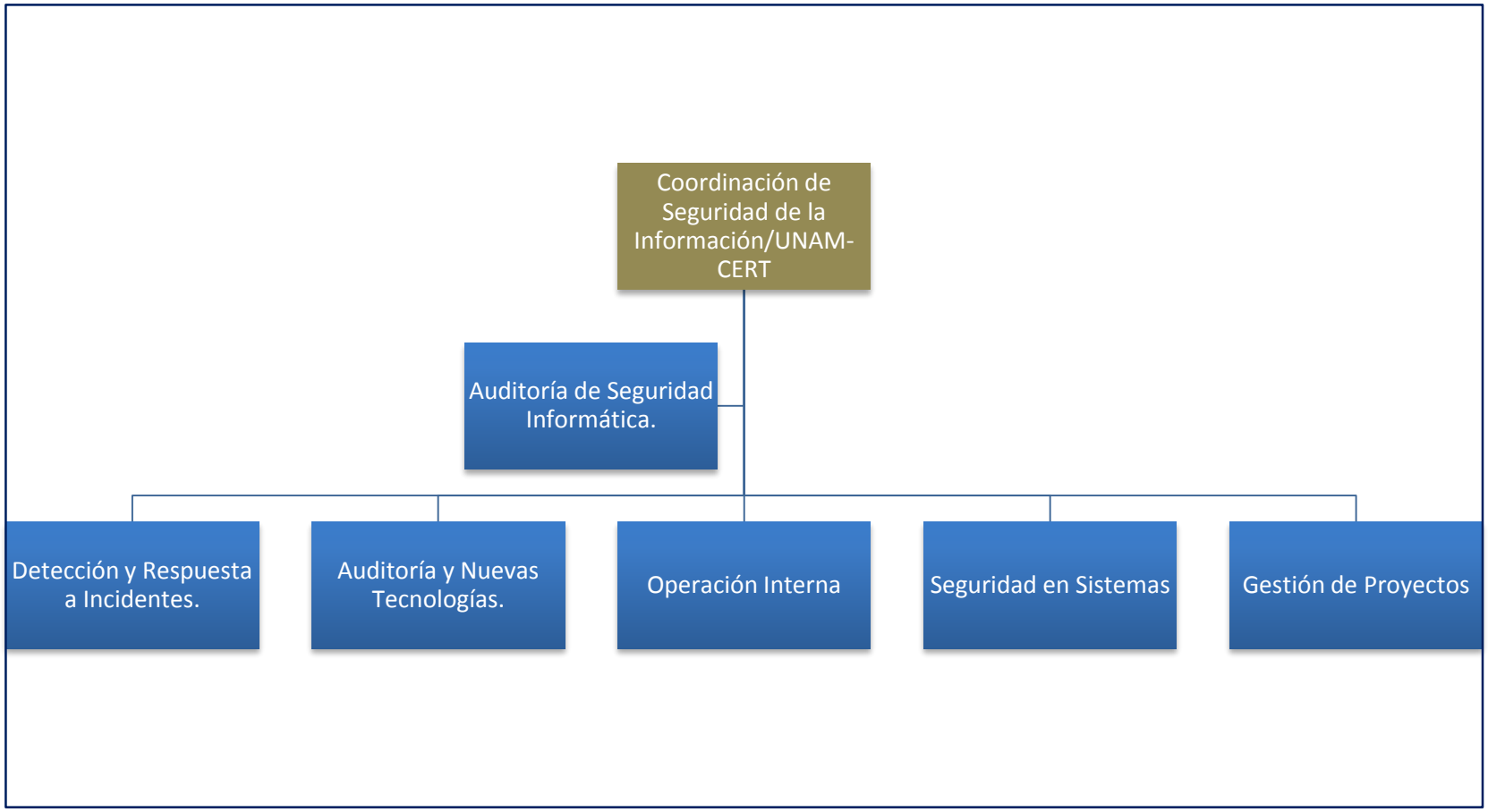

Figura 1. Organigrama CSI/UNAM-CERT. El puesto de Especialista en Respuesta a Incidentes y Cómputo Forense se desempeña en el departamento de Detección y Respuesta a Incidentes. Fuente: elaboración propia.

2. Especialista en Respuesta a Incidentes y Cómputo forense

2.1. Definición de conceptos básicos de Respuesta a Incidentes y Cómputo forense

A continuación defino y cito conceptos básicos que son indispensables conocer por un especialista en Respuesta a Incidentes y cómputo forense para la realización de sus actividades y funciones.

Definición de Incidente de seguridad informática.

Jason T. Luggens (2014), define Incidente de seguridad informática como "cualquier evento que tiene las siguientes características: Intenta causar daño, fue realizado por una persona e implica un recurso informático"

ESET (2012) lo define como "un hecho u evento que atenta contra la Confidencialidad, Integridad y Disponibilidad de un sistema informático."

Por lo tanto considero que Incidente de seguridad informática se define como:

Cualquier evento que afecte la integridad, disponibilidad y/o confidencialidad de un recurso o sistema informático.

Definición de Respuesta a Incidentes.

Jason T. Luggens (2014), define respuesta incidentes como "un enfoque coordinado y estructurado para pasar de la detección de incidentes a la resolución."

FIRST (2018) lo define como "Proceso para manejar el ciclo de vida de un incidente" y consiste en "detectar e identificar primero un incidente, luego clasificar y analizar, resolver y prevenir la repetición de un incidente, el objetivo principal es garantizar una pronta recuperación de los sistemas afectados".

Por lo tanto considero que Respuesta a Incidentes se define como:

El proceso mediante el cual se detectan, gestionan, analizan y se resuelven incidentes de seguridad. Así mismo implica prevenir la ocurrencia de un incidente. Su principal objetivo es recuperarse del incidente en el menor tiempo posible para continuar con la operación normal.

Definición de cadena de custodia.

Andre Arnes (2017) define cadena de custodia como “la documentación de la adquisición, control, análisis y disposición de evidencia física y digital”

En esta documentación, de acuerdo a la norma ISO/IEC 27037:2012 “Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence”, se debe registrar como mínimo la siguiente información de la evidencia:

- Un identificador unívoco de la evidencia
- Quién, Cuándo y Dónde se accede a la evidencia
- El traslado de la evidencia de un sitio a otro y tareas realizadas.
- Todo cambio potencial en la evidencia, con el nombre del responsable y la justificación de las acciones realizadas.

Definición de análisis forense.

Robert C. Newman (2017) define Análisis forense como: “la ciencia de adquirir, recuperar, conservar y presentar información que ha sido procesada electrónicamente y almacenada en medios informáticos”

Gerard Johansen (2017) lo define como: “la aplicación de métodos forenses digitales que permite a la respuesta a incidentes obtener una comprensión clara de la cadena de eventos que llevaron a una acción maliciosa,”

Por ello, considero que análisis forense se define como:

La adquisición y análisis de información utilizando métodos y herramientas que permitan preservar la integridad de la misma para poder reconstruir la cadena de eventos que determinen acciones maliciosas ocurridas en un sistema.

Proceso del análisis forense.

De acuerdo a Gerard Johansen (2017) el proceso del análisis forense consiste en las siguientes fases:

- Identificar las fuentes potenciales de evidencia durante un incidente.
- Preservación, protegerla de cualquier tipo de modificación o eliminación.
- Adquisición de la evidencia.
- Examinación, donde se detalla las herramientas y técnicas utilizadas para extraer información de la evidencia.
- Analizar información relevante obtenida de la fase de Examinación.

- Presentación de un reporte de los hallazgos.

Con base a los conceptos definidos anteriormente considero que los objetivos del analista forense son:

- Identificar y determinar qué y de dónde la evidencia será adquirida
- Examinar y analizar la información obtenida de la evidencia.
- Reconstruir la cadena de eventos ocurridos.
- Presentación de un reporte que ayude a determinar las causas del incidente.

Tipos de análisis forense:

*"**Análisis vivo***. Se refiere al análisis realizado cuando el sistema está activo y ejecutándose, donde la información puede alterarse a medida que los datos se procesan continuamente." Lessing (2008)

*"**Análisis Muerto***. Se realiza cuando el sistema está apagado y se adquiere una copia de los dispositivos de almacenamiento." Brian Carrier (2005)

2.2. Funciones

Respuesta a Incidentes:

Aplicación de técnicas y metodologías para la recolección de información referente a incidentes de seguridad informática, para su identificación. Así como la participación en la asesoría y solución de los mismos.

Cómputo forense:

Análisis de la evidencia digital y la determinación de las causas que propiciaron un incidente de seguridad informática.

2.3. Actividades

Respuesta a Incidentes:

- Asesorar a dependencias internas de Red-UNAM y entidades externas para la solución de incidentes de seguridad informática.
- Revisar y apoyarse de los sensores de tráfico malicioso instalados en la infraestructura de Red-UNAM para la atención e identificación de incidentes de seguridad informática.
- Investigar y desarrollar material relacionado con la respuesta a incidentes de seguridad informática del UNAM-CERT.

Cómputo forense:

Analizar equipos en los que ha sucedió algún incidente de seguridad informática.

2.4. Habilidad y competencias requeridas

- Capacidad de análisis e identificación de vulnerabilidades en los sistemas.
- Completar tareas asignadas dentro de los plazos requeridos y bajo presión.
- Establecer y mantener relaciones de trabajo cooperativo con individuos y grupos que provienen de diversos orígenes.
- Comunicarse de forma eficaz de forma escrita y oral.
- Capacidad de prestar especial atención a los detalles.
- Interactuar pacientemente con personas que puedan tener poca o ninguna experiencia técnica o conocimiento en seguridad informática.
- Capacidad para comunicar de manera efectiva cuestiones de seguridad informática y temas relacionados con los demás miembros de TI.

- Conocimientos básicos en redes.
- Conocimientos en análisis de vulnerabilidades, identificación y clasificación de amenazas de seguridad informática.
- Comprensión de conceptos básicos en Respuesta a incidentes.
- Comprensión de conceptos básicos de análisis forense, sus objetivos y los tipos de análisis que existen.

3. Participación en Proyectos

3.1. Respuesta a incidentes de seguridad informática en Red Universitaria

3.1.1. **Problemática**

Dar atención a los incidentes de seguridad informática reportados al CSI/UNAM-CERT ocurridos dentro de la Red-UNAM.

3.1.2. **Objetivos**

- Gestionar los incidentes de seguridad informática en las dependencias de Red-UNAM reportados a la CSI/UNAM-CERT.
- Apoyar a los administradores de las dependencias de Red-UNAM con los incidentes detectados en los equipos pertenecientes a sus redes de cómputo.

3.1.3. **Actividades desarrolladas**

En esta actividad seguí el Proceso de Manejo de incidentes que está definido en la documentación del UNAM-CERT, conlleva las etapas de detección, gestión y análisis.

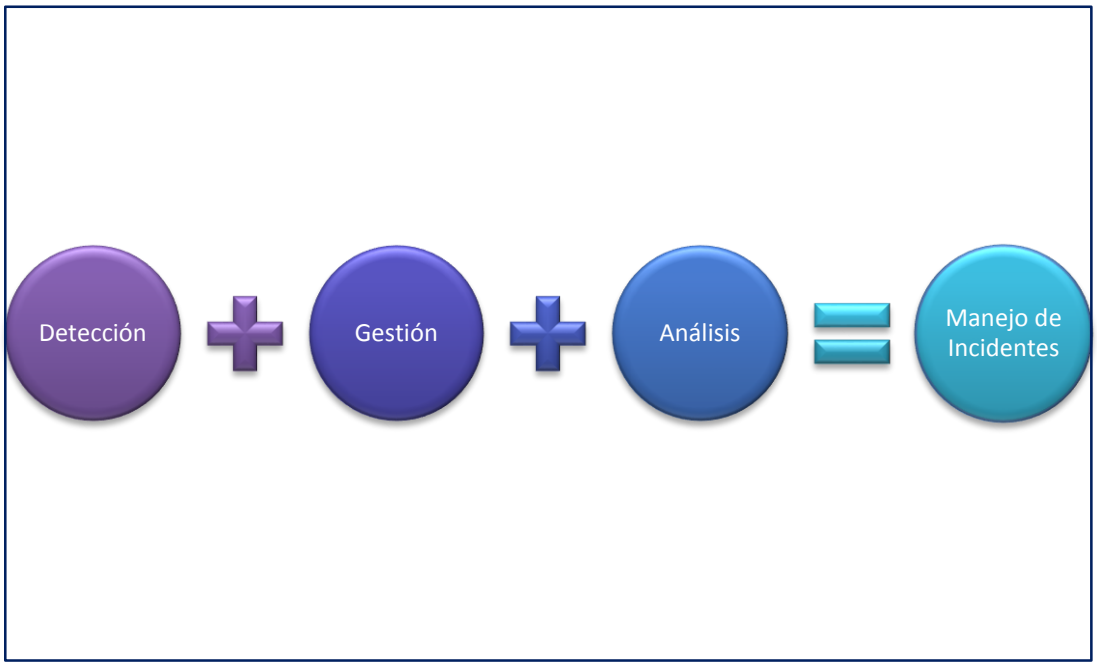

Figura 2. Proceso de Manejo de Incidentes. Fuente: Documentación de proceso a incidentes del UNAM-CERT.

A continuación, describo en que consiste cada una de las etapas mencionadas.

3.1.3.1. **Detección**

Para la detección de incidentes dentro de la Red-UNAM se tiene como fuente información el Telescopio de Seguridad UNAM (TSU), este sistema concentra, correlaciona y clasifica información del Plan de Sensores de Core y Distribución (PSCD) y el analizador de flujos de Peakflow.

La herramienta Peakflow analiza flujos de red y basado en el comportamiento detecta amenazas como ataques de DDoS, así mismo envía notificaciones de incidentes detectados. Se ubica en el perímetro de Red-UNAM.

El PSCD es resultado de la colaboración entre la Coordinación de Seguridad de la Información/UNAM-CERT y el Departamento de Operación de la Red (Dirección de Telecomunicaciones, DGTIC). El Departamento de Operación de la Red transfiere hacia los equipos administrados por la CSI/UNAM-CERT el tráfico perteneciente a los cuatro core de Red-UNAM: DGTIC, Zona Cultural, IIMAS y Arquitectura. Cada core contiene herramientas para capturar y procesar la información del tráfico malicioso que reciben. El tráfico se procesa, almacena y analiza en la base de datos del TSU. Para acceder a esta información procesada, consultaba el Sistema de Atención a Incidentes (SAI).

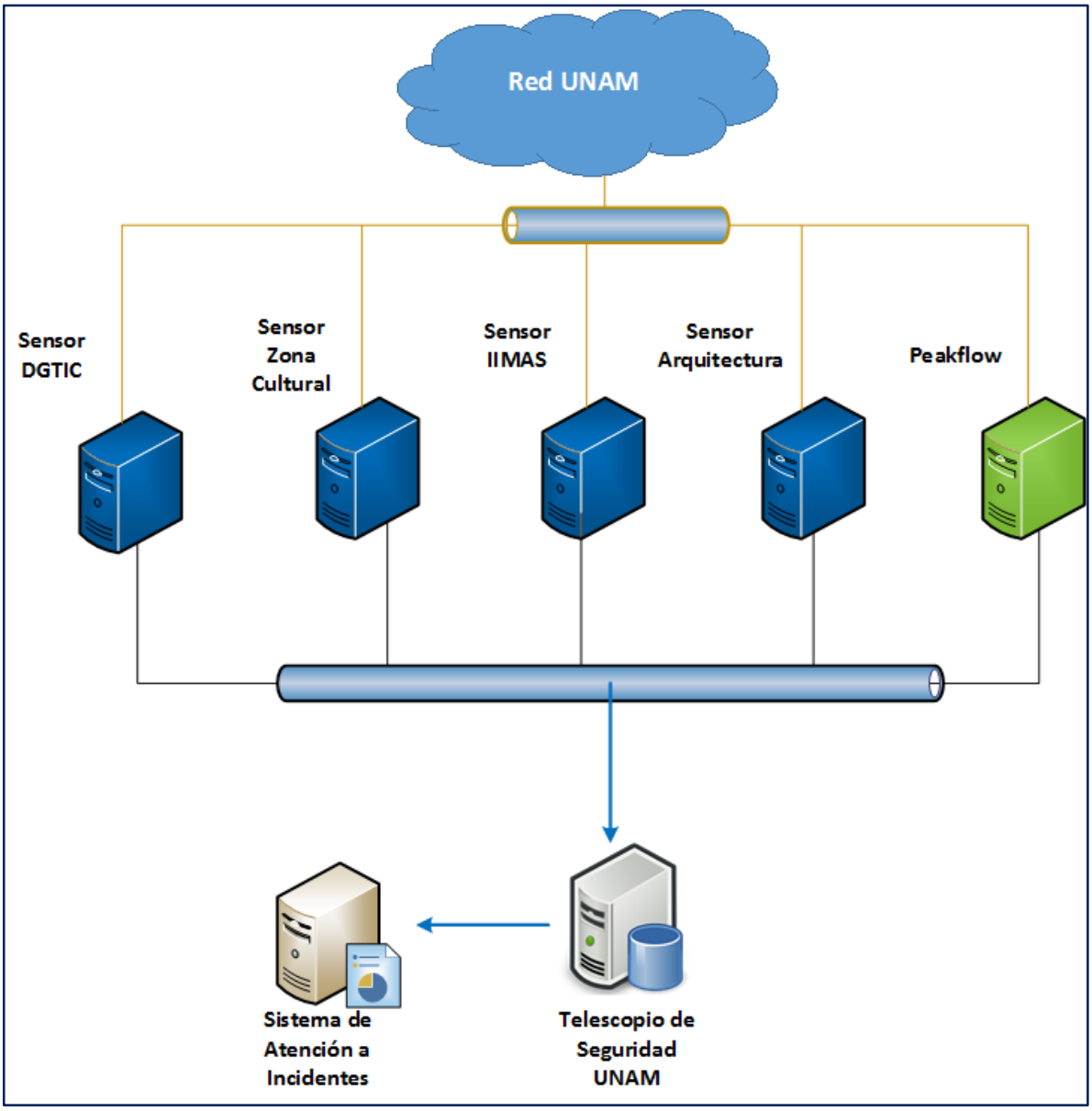

Figura 3. Arquitectura de Telescopio de Seguridad UNAM. Fuente: elaboración propia.

3.1.3.2. **Gestión**

En la gestión del incidente realizaba las actividades clasificación, determinación de la prioridad, notificación y seguimiento, las cuales describo a continuación.

3.1.3.2.1. **Clasificación**

En esta actividad determinaba el tipo de incidente, de acuerdo a la siguiente clasificación:

Tabla 1. Clasificación de tipo de incidente. Fuente: Sophos Threatsaurus.

Tipo de incidente	Descripción
DoS (Denegación de Servicio)	Este ataque intenta sobrecargar o cerrar un servicio para que los usuarios legítimos ya no puedan acceder a el. Los ataques DoS típicos se dirigen a los servidores web y tienen como objetivo hacer que los sitios web no estén disponibles. La interrupción del servicio puede ser costosa para una organización.
Malware	Su nombre deriva del acrónimo de Malicious Software, el cual es un código utilizado para realizar acciones maliciosas en el equipo infectado y está diseñado para dar un beneficio al atacante acosta de la víctima.
Phishing	El ataque consiste en el envío de correos electrónicos que parecen provenir de una organización acreditada(Bancos, Redes Sociales), con el fin de engañar a los destinatarios para que compartan información confidencial con un tercero desconocido (criminal cibernético).
Redirecciona-miento	Ocurre cuando un usuario utiliza un enlace que apunta a un sitio en particular, este redirige a una página phishing o de descarga de malware de manera automática.
Bots	Programa informático que una vez ejecutado en el equipo permite a un atacante ejecutar de manera remota una serie de comandos específicos sobre el mismo mediante un centro de control. Los bots pueden ocasionar que los equipos infectados ataquen a otros equipos, envíen spam, contengan pharming e inyección web, así como la descarga y almacenamiento de otros programas maliciosos.
Spam	Se define como el envío de correo electrónico masivo no solicitado. Puede llegar a través de direcciones de correo electrónico legítimas cuyas credenciales de usuario se han visto comprometidas.

Bruteforce	El ataque de fuerza bruta consiste en probar gran número de posibles combinaciones de palabras clave o contraseñas para obtener acceso no autorizado a un sistema, servicio o archivo.
Scanners	Analizar por medio de un programa el estado de los puertos de un equipo perteneciente a una red, detectando así servicios que ofrece y tener acceso a estos mediante la explotación de una vulnerabilidad de seguridad presente.
Defacement	Consiste en la modificación no autorizada de un sitio web, es decir en su aspecto visual. Lo que conlleva al atacante primeramente a vulnerar el sistema operativo que alberga el sitio, el servicio web o las aplicaciones que se ejecutan sobre el mismo.
Mailer	Programa utilizado para el envío masivo de correo electrónico. Generalmente se encuentra en forma de una aplicación web insertada en un sitio vulnerado de manera no autorizada y utilizada por atacante para el envío de SPAM.

3.1.3.2.2. **Determinación de la prioridad**

Una vez que había realizado la clasificación del incidente de seguridad reportado, determinaba la prioridad del mismo tomando en cuenta el impacto que podría causar, mediante los siguientes parámetros.

Tipo de incidente:

Para cada tipo de incidente verificaba el nivel de prioridad de acuerdo a una tabla ya establecida en la documentación del Proceso de Manejo de Incidentes. Esta tabla da prioridad a un incidente tomando en cuenta el número de usuarios afectados, así como el tiempo de respuesta que puede trascurrir antes de que el ataque ocasione un daño mayor en el equipo o la red.

Tabla 2. Prioridad de Incidente. Fuente: elaboración propia.

Prioridad	Incidente
1	DDOS
2	Phishing
3	Bruteforce
4	Malware
5	SPAM
6	Bots
7	Mailer
8	Scanners
9	Defacement

Volumen:

De acuerdo a lo establecido en la documentación del Proceso de Manejo de Incidentes, me basaba en la cantidad de incidentes del mismo tipo que hubieran sucedido en un periodo de tiempo breve y en una sola dependencia. Basándome en esto determiné el nivel de prioridad.

Tabla 3. Nivel de prioridad de Incidente. Fuente: elaboración propia.

Nivel	Número de incidentes por día
Bajo	5
Medio	> 5 y < 50
Alto	50 o más

3.1.3.2.3. **Notificación**

Para el caso de la notificación de incidentes en Red-UNAM, el SAI envía un correo notificando a los contactos registrados como administradores del equipo. A su vez, genera un número de incidente de manera automática. Este número se asocia con la IP y tipo de incidente ocurrido. Adicionalmente generaba un identificador de caso para agrupar incidentes similares.

Los casos generados tenían uno de estos cuatro estados:

Tabla 4. Estado de casos. Fuente: elaboración propia.

Estado	Descripción
Asignado	Estado inicial.
En proceso	El administrador de la dependencia ha accedido al sistema para conocer los detalles del caso.
Solicita concluir	El administrador de la dependencia informa que se han tomado acciones y requiere que se concluya el caso.
Concluido	Se han comprobado las acciones correctivas y el incidente se ha concluido

El SAI envía tres avisos vía correo electrónico (con diferencia de un día entre ellos) a los administradores de las dependencias de la UNAM de manera automática.

3.1.3.2.4. **Seguimiento**

Para dar seguimiento del incidente de seguridad, revisaba el caso hasta que este quedaba resuelto. Esta revisión la hacía tomando en cuenta los siguientes escenarios a partir del envío de correos de notificación del SAI:

I. *El administrador atiende y soluciona el incidente satisfactoriamente, por lo que solicita concluir el caso generado en el SAI*: mi revisión consistía en corroborar con el administrador las acciones realizadas para la solución del incidente, así como validar en el SAI que no se siguieran detectando más incidentes del mismo tipo en el equipo de la dependencia. Una vez validada esta información procedía a atender su solicitud de concluir el caso.

II. *El administrador solicita más información sobre el incidente o asesoría para solucionarlo*: para atender a su solicitud, obtenía información del caso de las siguientes fuentes:
   - Peakflow
   - Sensores PSCD
   - Telescopio de Seguridad UNAM

También el administrador podía solicitar una revisión del equipo afectado por parte del equipo UNAM-CERT. Por lo que realizaba un revisión remota o en sitio.

III. *El administrador recibió un tercer aviso y aún no ha dado atención al incidente:* para este caso me ponía en contacto vía telefónica con los administradores de la dependencia para poder indagar en la causa por la que no se había atendido el incidente, por ejemplo: validar si las cuentas de contacto de los administradores eran erróneas, si ya no laboraban en la dependencia o si el administrador no había tenido tiempo de atender dicho incidente. Esto con el objetivo de dar atención al caso lo más pronto posible.

3.1.3.2.5. **Conclusión de casos en el SAI**

En esta actividad marcaba como *Concluido* los casos en el SAI en los que había dado seguimiento y validado que se habían tomado las acciones necesarias para solucionar el incidente.

3.1.3.3. **Análisis**

Para realizar el análisis solo consideraba los casos en que el administrador del equipo afectado hubiera solicitado al equipo de respuesta a incidentes atención del incidente en sitio, con previa cita. En este escenario, como especialista de respuesta a incidentes realizaba un Análisis forense. Este análisis conlleva otro proceso que describo detalladamente en el capítulo 3.3.5. Análisis forense.

3.1.4. **Resultados**

Gestioné y asesoré a los administradores de las dependencias sobre los incidentes ocurridos en los equipos a su cargo, también los apoyé en la solución de los incidentes notificados. Todos los casos quedaron documentados en el sistema SAI como base de conocimientos para futuras consultas. Así mismo, actualicé o añadí información a la documentación de los incidentes que aportaron nuevo conocimiento o fueron casos especiales, quedando como lecciones aprendidas. Compartiéndolos de esta manera con los demás miembros del equipo. En total de mi experiencia laboral realicé la gestión de 380 incidentes.

3.2. Respuesta a incidentes de seguridad informática en entidades Externas

3.2.1. **Problemática**

Dar atención a los incidentes de seguridad informática reportados al CSI/UNAM-CERT ocurridos en entidades externas. Se consideran entidades externas organizaciones que no pertenecen a la UNAM y público en general.

3.2.2. **Objetivos**

- Notificar a los contactos correspondientes, sobre incidentes ocurridos en entidades externas.
- Lograr que los incidentes ocurridos en entidades externas sean atendidos y resueltos en el mismo día que se reportan.

3.2.3. **Actividades desarrolladas**

En esta actividad igualmente seguía el Proceso de Manejo de Incidentes, que conlleva las actividades de detección, gestión y análisis para aquellas entidades externas, es decir no pertenecientes a la Red-UNAM.

3.2.3.1. **Detección**

Para la detección de incidentes de seguridad entidades externas tomaba como fuente de información los incidentes reportados a las direcciones de correo pertenecientes al departamento de Detección y Respuesta a Incidentes: *incidentes@cert.unam.mx* y *phishing@cert.unam.mx*, o bien vía telefónica. Estos reportes provenían del público en general o de otros equipos de respuesta a incidentes con los que colabora el UNAM-CERT.

3.2.3.2. **Gestión**

Como mencioné anteriormente, conlleva las actividades de clasificación, determinación de la prioridad, notificación y seguimiento.

Para la clasificación y determinación de la prioridad, la determinaba de igual manera que los incidentes internos; sin embargo, para notificar, revisar y analizar un incidente que afecte a instituciones externas como podrían ser los ataques de *phishing* a instituciones bancarias realicé los siguientes pasos:

I. Obtener la dirección IP correspondiente al dominio o dominios involucrados (ver Anexo 1).

Cuando el incidente ocurrido tenía un nombre de dominio obtenía la dirección IP con las siguientes herramientas:

- Mediante el comando nslookup.
- Servicio en línea de DNS lookup, por ejemplo www.tcpiputils.com
- Plug-in del navegador dependiendo del navegador web utilizado.

II. Obtener el Código de país y ASN

Una vez que identificaba la dirección IP, buscaba el código país (*CC Country Code*) y ASN (*Autonomous System Number*). El primero me servía para determinar en qué idioma (inglés o español) enviar el correo de notificación y el segundo lo utilizaba para almacenar en el SAI la Entidad Externa que se relacionaba con el incidente, así como asociar cuentas de correo para la notificación con el ASN que identificaba.

Para obtener estos datos realizaba una consulta a la base de datos WHOIS, mediante el siguiente comando de sistemas LINUX/UNIX:

```
#whois dir_IP
```

En la respuesta del comando utilizado ubiqué el campo del Código de país, CC y posteriormente buscaba a que país correspondía en la página:
http://www.iso.org/iso/english_country_names_and_code_elements.

III. Obtener correo electrónico para notificar el incidente.

En la respuesta del comando anterior, ubicaba también el campo de correo especificado para reportar incidentes o “abusos” etiquetados con algunos de los siguientes nombres:

- OrgAbuseEmail
- abuse-c
- abuse-mailbox
- admin-c
- tech-c

3.2.3.2.1. **Notificación**

Una vez obtenida la información anterior, notificaba mediante correo electrónico el incidente utilizando las plantillas de correo predefinidas para cada tipo de incidente y en el lenguaje español o inglés, dependiendo el país en el que estaba registrada la dirección IP a reportar. También notificaba el incidente mediante los formularios existentes en la página web involucrada.

En caso de que en las dos opciones anteriores para notificación no tuviera una respuesta y el sitio malicioso siguiera activo, contactaba vía correo electrónico al equipo de respuesta a incidentes del país al que estaba asociada la dirección IP del sitio malicioso para solicitar su apoyo y reportar el incidente.

Dependiendo el tipo de incidente, la notificación la realizaba mediante los siguientes procedimientos específicos:

a) Phishing

En caso de que el *phishing* afectara a una institución financiera mexicana, notificaba a los contactos de la institución que se tenían registrados en el SAI.

b) SPAM/Phishing Scam por correo electrónico

Buscaba en las cabeceras completas del correo electrónico la dirección IP donde se originaba dicho correo para obtener la información descrita en el punto I y II.

c) Malware

Cuando el malware era enviado por correo electrónico, notificaba a los contactos de la dirección IP el origen del correo, es decir notificaba el malware y el spam de forma separada. Si solo nos era reportado el servidor web seguía el procedimiento descrito en el punto I y II para obtener la dirección IP.

d) Redireccionamiento a malware

Seguía el mismo procedimiento que para *Malware*, pero utilizaba la plantilla correspondiente a *Redireccionamiento a Malware* en la notificación.

e) Redireccionamiento a phishing

Seguía el mismo procedimiento que para *Phishing*, pero utilizaba la plantilla correspondiente a *Redireccionamiento a phishing* en la notificación.

3.2.3.2.2. **Registro de incidentes en el SAI**

Por último, registraba la siguiente información del incidente en el Sistema de Atención a Incidentes.

- Dirección IP
- Dependencia externa involucrada.
- Entidad Afectada (Bancaria, Gubernamental, etc.)
- URL
- País de la dirección IP

3.2.3.2.3. **Seguimiento**

Daba seguimiento vía correo electrónico con el contacto al que notificaba el incidente y él quedaba a cargo de la solución del caso. También lo hacía validando si la URL del sitio malicioso seguía activa o no.

3.2.3.3. **Análisis**

Dado que se consideraban los casos en que el administrador del equipo afectado hubiera solicitado al equipo de respuesta a incidentes atención del incidente en sitio, el alcance solo era para los equipos pertenecientes a la Red-UNAM, por lo que en los incidentes de entidades externas no realizaba el Análisis Forense.

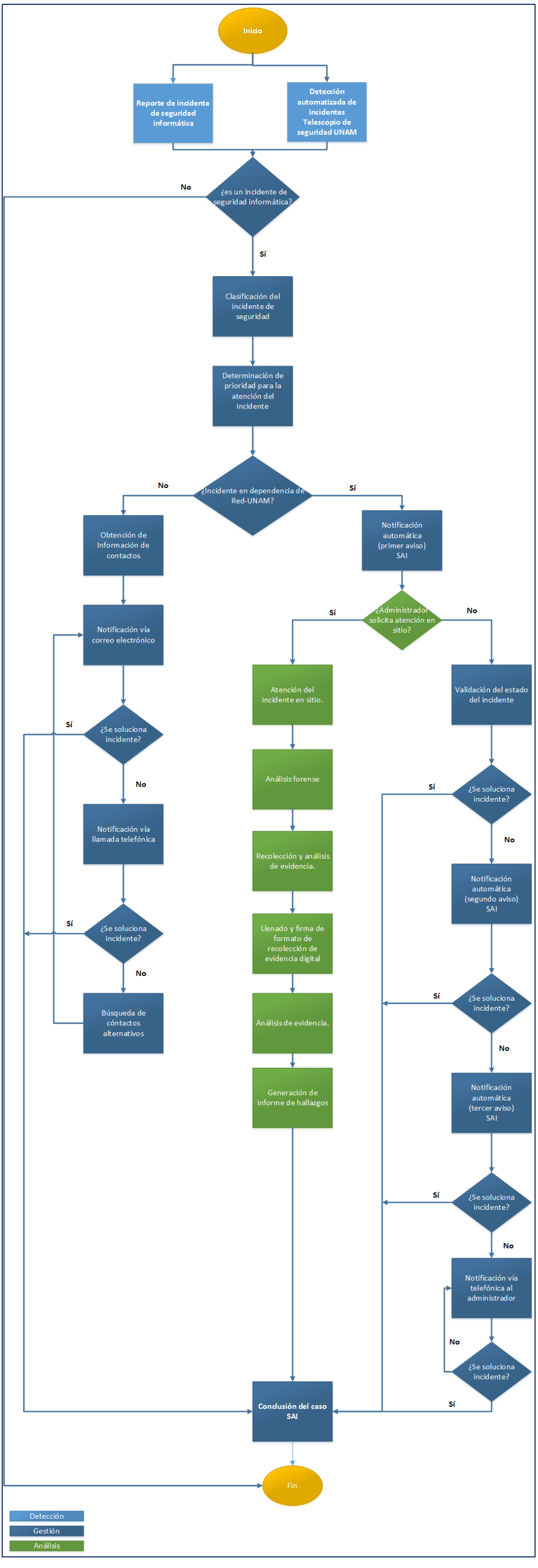

Figura 4. Proceso de Manejo de Incidentes. Fuente: elaboración propia.

3.2.4. **Resultados**

Realicé la gestión de 200 incidentes de seguridad informática, informando a los responsables a través de reportes telefónicos o vía correo electrónico. Sobre todo en los casos de *phishing* reportaba a la brevedad las páginas fraudulentas para que estuvieran abajo en un máximo de 2 horas.

3.3. Actualizar base de contactos del Sistema de Atención a Incidentes

3.3.1. **Problemática**

Se requería actualizar la base de datos del Sistema de Atención de Incidentes (SAI) de la CSI/UNAM-CERT. El SAI contiene el registro de incidentes, así como la dirección IP del equipo afectado, la dependencia a la que pertenecía dicha dirección IP dentro de Red-UNAM y dependencias externas, de igual manera los datos de contacto del administrador como teléfono y correo electrónico. Este sistema es la principal fuente de información al momento de detectar y notificar los incidentes de seguridad.

3.3.2. **Objetivo**

Tener una base de datos actualizada de los administradores de red de las dependencias de Red-UNAM, a través del Sistema de Atención a Incidentes de la CSI/UNAM-CERT.

3.3.3. **Actividades desarrolladas**

Validé mediante correo electrónico y vía telefónica con los administradores de las dependencias de Red-UNAM, los datos de contacto que teníamos registrados en la base de datos del SAI.

Al presentarse un incidente de seguridad en una entidad externa de la cual no teníamos registrado datos de contacto, investigué y añadí el contacto de dicha entidad al sistema.

3.3.4. **Resultados**

Actualicé los datos de contacto de las dependencias de Red-UNAM, logrando corregir datos erróneos e inválidos, esto me permitía agilizar y reportar correctamente la notificación de incidentes.

También añadí un nuevo contacto de un proveedor de internet en el que se nos había reportado por primera vez una página phishing en su red, esto permitió reportar en corto tiempo incidentes futuros en la red de dicho proveedor.

3.4. Monitoreo de las elecciones internas realizadas en la plataforma de Voto Electrónico de la UNAM

3.4.1. **Problemática**

Realizar el monitoreo de las elecciones internas de dependencias de la Universidad, así como elaborar el informe correspondiente.

3.4.2. **Objetivo**

- Detectar y gestionar incidentes de seguridad informática durante los procesos de elecciones internas.

3.4.3. **Actividades desarrolladas**

Realicé el monitoreo de las elecciones internas realizadas en la plataforma de Voto Electrónico de la UNAM. Para este monitoreo revisaba el log del servidor web y el de base de datos de la plataforma de Voto, para detectar cualquier registro que indicara un ataque o inyección de código malicioso.

Al final de cada monitoreo elaboré el informe correspondiente indicando si la jornada de Voto había presentado algún incidente.

3.4.4. **Resultados**

Realicé el monitoreo del posible tráfico malicioso que pudiera afectar en 8 jornadas electorales de las votaciones internas de la UNAM ocurridas en 11 dependencias. Así mismo elaboré el informe correspondiente en el que notifiqué que todas habían trascurrido sin ataques ni tráfico malicioso.

3.5. Monitoreo del Programa de Resultados Electorales Preliminares 2015 en el Difusor de la UNAM

3.5.1. **Problemática**

Realizar el monitoreo del Programa de Resultados Electorales Preliminares 2015 en el Difusor de la UNAM, así como elaborar el correspondiente informe.

3.5.2. **Objetivo**

- Monitorear el posible tráfico malicioso que pudiera afectar el Programa de Resultados Electorales Preliminares 2015 en el Difusor de la UNAM.

3.5.3. **Actividades desarrolladas**

Mediante el sistema de prevención de intrusos (IPS) administrado por la CSI/UNAM CERT, realicé el monitoreo de la Red-UNAM para detectar el posible tráfico malicioso que pudiera afectar el Programa de Resultados Electorales Preliminares 2015 en el Difusor de la UNAM, llevado a cabo en el periodo entre el 7 y 8 de junio del 2015.

3.5.4. **Resultados**

Realicé el monitoreo del posible tráfico malicioso y durante mi jornada de monitoreo no se presentó ninguna incidencia.

3.6. Análisis forense

3.6.1. **Problemática**

Atender a las solicitudes de análisis forense realizadas por las dependencias de la Red-UNAM en equipos en los que se presentó un incidente de seguridad informática.

3.6.2. **Objetivos**

Recabar y presentar la mayor cantidad de evidencia, para proporcionar información útil sobre los incidentes de seguridad a los administradores de los equipos afectados pertenecientes a las dependencias de Red-UNAM.

3.6.3. **Actividades desarrolladas**

En mi experiencia de análisis forense, analicé equipos en los que sucedió un incidente de seguridad informática y en los que el administrador del mismo solicitó apoyo del CSI/UNAM-CERT para dicho análisis. Para realizar el análisis efectuaba las siguientes actividades:

- Descripción del equipo afectado
- Llenado y firma de formato de recolección de evidencia digital
- Adquisición de evidencia
- Montado de imagen o dispositivo.
- Descripción del sistema
- Análisis de cuentas de usuario
- Análisis de línea de tiempo
- Revisión de bitácoras
- Búsqueda de archivos sospechosos

- Recuperación de datos
- Reporte de resultados

3.6.3.1. **Descripción del Equipo Afectado**

En este primer paso hice un reconocimiento del equipo afectado, es decir, tener conocimiento previo de los siguientes datos:

- *Sistema operativo y Arquitectura:* para prepararme con las herramientas necesarias a utilizar durante el análisis.
- *Capacidad del almacenamiento del equipo*: con la finalidad de llevar un disco externo con la capacidad suficiente para realizar la copia.
- *Red.*
- *Administrador del equipo.*
- *Servicios que se ejecutan en el equipo.*

3.6.3.2. **Llenado y firma de formato de recolección de evidencia digital**

En este paso realicé el llenado de un formato de recolección de evidencia, el cual contiene los siguientes campos:

- Número de caso
- Fecha y hora en que se obtuvo la evidencia
- Lugar donde se obtuvo la evidencia
- Descripción
- Marca/modelo
- Número de serie
- Capacidad
- HASH-SHA256 (generado por la copiadora forense, durante la adquisición de evidencia.)
- Etiqueta del disco.
- Declaración general de las acciones que se realizarán para el análisis de la evidencia.
- Nombre completo y firma de quienes recolectaron la evidencia.
- Nombre completo y firma del administrador del equipo afectado.

En el *Anexo 2*, muestro un ejemplo de un formato de recolección de evidencia.

3.6.3.3. **Adquisición de evidencia**

En el análisis forense es fundamental preservar el estado de la evidencia, por lo que con las herramientas utilizadas para la recolección de la misma evitaba modificarla.

Por consecuencia realizaba una copia del disco original del equipo afectado. Dicha copia la realicé con un kit forense, este kit me permitía realizar una copia bit a bit del disco duro de equipo comprometido para posteriormente hacer el análisis forense sobre la copia.

Una vez finalizada la copia etiquetaba el disco en el que se realizó la copia con el identificador del caso, y a su vez guardaba el disco en una bolsa antiestática para protegerlo de daños.

Figura 4. Kit Forense y Copiadora de discos. Fuente: https://www.edatarec.com/

En los siguientes pasos del análisis, describo los comandos que utilicé para realizar el análisis forense de sistemas LINUX o UNIX, ya que mi experiencia profesional adquirida fue sobre estos sistemas operativos. Sin embargo los pasos pueden ser aplicados para cualquier sistema operativo.

3.6.3.4. **Montado de imagen o dispositivo**

Una vez que obtenía la copia del disco en el laboratorio, lo montaba en el sistema que utilizaría para su análisis. Para esto utilizaba la máquina virtual SANS Investigative Forensic Toolkit (SIFT), que contiene herramientas útiles instaladas que me facilitaban el análisis.

El montado de discos lo realizaba con el siguiente comando, considerando las opciones necesarias para no sobrescribir o alterar la evidencia.

```
#mount -o ro,noexec  -t ext3 dispositivo_evidencia directorio_de_montado
```

Donde:

-t: tipo de sistema de archivos (ext3, ntfs)

-o: Opciones separadas por comas:

- **ro**: Monta como sólo lectura.
- **noexec**: No permite ejecución de binarios

En caso de que el disco de evidencia fuera un ***Logical Volume Manager, LVM,*** utilizaba la siguiente herramienta para realizar el montado:

```
#kpartx -a -v dispositivo
```

Donde:

-a: Realiza el mapeo de las particiones.
-v: Modo verbose

-l: Lista el mapeo de particiones que podrían agregarse.
-d: Borra el mapeo de particiones.

El dispositivo puede ser un disco o un archivo de imagen.

Una vez realizado el mapeo de las particiones, utilizaba el comando, `mount.`

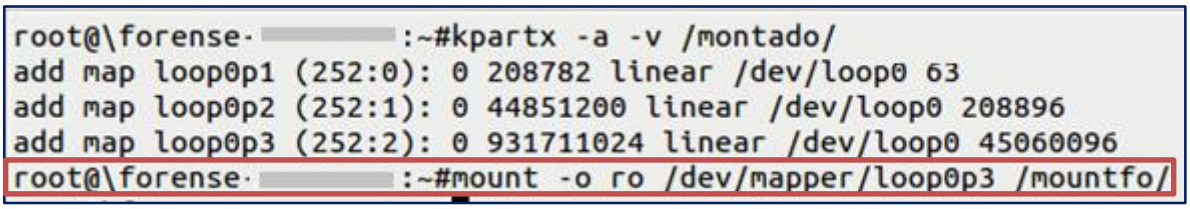

Figura 5. Montado de LVM. Fuente: elaboración propia.

3.6.3.5. **Descripción del sistema**

Obtenía la descripción del sistema mediante los siguientes comandos:

Tabla 5. Comandos para descripción del sistema. Fuente: elaboración propia.

Comando	Descripción
# cat /etc/issue	Versión del sistema operativo
# cat /etc/hostname	Nombre del equipo
# cat /etc/sysconfig/network	Nombre del equipo CentOS
# ls -lcrt /bin/* | less	Fecha de instalación del sistema.
# cat /etc/localtime	Hora local

3.6.3.6. **Análisis de Cuentas de usuario**

Dado que el objetivo principal de un atacante es mantener el acceso al sistema, revisaba las cuentas de usuario que podía haber creado el atacante, así como el historial de comandos de los usuarios o archivos en su directorio personal. Revisando toda esta información podía identificar actividad maliciosa.

Tabla 6. Comandos para obtener cuentas de usuario. Fuente: elaboración propia.

Comando	Descripción
# more /etc/shadow	Contiene las cuentas de usuario activas, así como su contraseña cifrada. Este archivo es útil para saber si la

	contraseña de un usuario fue cambiada.
#more /etc/passwd	Contiene la lista de los usuarios del sistema e información que es requerida para el inicio de sesión como: ID usuario, ID grupo, home directory, shell, etc. Este archivo es útil para saber si un usuario fue agregado recientemente.
#more/home/nombre_usuario/.bash_history	Historial de comandos
/home/nombre_usuario	Directorio de usuario

3.6.3.7. Análisis de Línea de tiempo

3.6.3.7.1. Generación de Línea de tiempo

Este paso implica la reconstrucción de los hechos a partir de los atributos de tiempo de los archivos del disco a analizar, llamados MACtimes. Estos tiempos MAC depende del sistema de archivos, en la siguiente tabla muestro los más comunes:

Tabla 7.Tiempos MAC. Fuente: elaboración propia.

Marca de tiempo	Descripción
Acceso (A)	Consulta de archivo
Modificacion (M)	Cambio en el contenido del archivo
Cambio (C)	Cambio en los metadatos
Creación (B)	Creación del archivo
Borrado (D)	Archivo borrado

Tabla 8.Comparación de tiempos MAC por sistema de archivos. Fuente: Forense en sistemas Linux Congreso de seguridad en cómputo 2015

Sistema de Archivos	M	A	C	B	D
Ext2/Ext3	✓	✓	✓		✓
Ext4	✓	✓	✓	✓	✓
FAT	✓	✓	✓	✓	✓
NTFS	✓	✓		✓	✓

La línea de tiempo la generaba con todos los tiempos MAC de cada archivo presente en el disco a analizar.

Para esto, utilizaba los comandos incluidos en la herramienta Sleuth Kit, la cual es una biblioteca de C y una colección de línea de comandos que sirven como apoyo al análisis forense y no son intrusivas, es decir no dañan o modifican la evidencia.

- **fls**

  Esta herramienta me permitía obtener todos los tiempos MAC del sistema, nombres de archivos, directorios incluso de aquellos que hayan sido borrados recientemente. La sintaxis del comando es la siguiente:

  ```
  #fls –m punto_de_montaje –r
  dispositivo_analizado > Archivo_de_salida.txt
  ```

  Donde:

  - -m punto_de_montaje: La cadena dada como punto_de_montaje se antepondrá a los nombres de archivo como el punto de montaje, ejemplos: /, /home, /usr, etc.
  - -r: Forma recursiva
  - dispositivo_analizado: Especificamos la ruta del dispositivo que estamos analizando.
  - Archivo_de_salida.txt: Redirigimos la salida del comando a un archivo.

Ejemplo:

```
#fls -m / -r /mnt/análisis/disco_evidencia > mac_times.txt
```

- **Ils**

  Con esta herramienta listaba la información de los inodos, además de mostrar los detalles del inodo en formato que el comando mactime pudiera leer con la opción –m.

  La salida de este comando lo agregaba al archivo creado anteriormente con fls:

```
#ils -m /mnt/análisis/disco_evidencia >> mac_times.txt
```

- **mactime**

  Por último para generar la línea del tiempo que pudiera analizar en un formato legible y fácil, utilizaba el comando mactime:

```
#mactime -b mac_times.txt -z CST6CDT 2014-10-01 > linea_tiempo_numcaso.txt
```

  Donde:

  - –b mac_times.txt: Indica la ubicación del Archivo generado por las herramientas fls e ils.
  - linea_tiempo_numcaso.txt: Se redirige la salida al archivo que nos servirá para realizar el análisis de Línea de tiempo.
  - -z: Para indicar el formato de la zona horaria

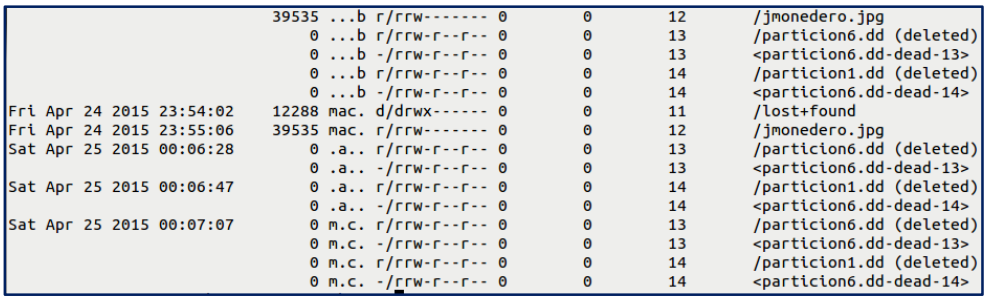

Figura 6. Ejemplo de Línea del tiempo. Fuente: elaboración propia.

Una vez que generaba la Línea de tiempo final, obtenía un archivo de gran extensión, es decir miles de líneas, por lo que para realizar un análisis eficiente tomaba en cuenta lo siguiente con la finalidad de facilitar esta tarea:

- Establecía una ventana de tiempo:
  - En función de una fecha y hora, podría ser en la que se detectó el incidente.
  - En función de un archivo, algún archivo malicioso que encontremos durante el análisis.
- Filtraba eventos en la línea de tiempo, eventos en particular.
- Analizaba el contexto de los eventos.

3.6.3.8. **Análisis de bitácoras.**

Durante esta etapa del análisis buscaba los eventos o acciones que se llevaron a cabo en el equipo y me ayudaran a reconstruir los hechos. Estos eventos quedan registrados en las bitácoras del sistema y de los servicios que tenía en ejecución como un servidor web, correo, etc. A continuación, listo las bitácoras más importantes o comunes que analizaba.

3.6.3.8.1. **Bitácoras del sistema**

- `/var/log/syslog`: está bitácora contiene el registro de mensajes del sistema y programas.

3.6.3.8.2. **Bitácoras de inicio de sesión:**

- `/var/log/lastlog`: proporciona información acerca del último acceso de cada usuario al sistema. Para ingresar a esta bitácora se utiliza el comando `lastlog`.
- `/var/log/wtmp`: registra los inicios de sesión exitosos del usuario al sistema. Para ingresar a esta bitácora se utiliza el comando `last`.

- `/var/log/btmp`: registra los inicios de sesión fallidos del usuario al sistema. Para ingresar a esta bitácora se utiliza el comando `lastb`.

- `/var/log/auth.log`: registra los inicios de sesión fallidos y exitosos, las veces que se ejecuta el comando `su`. Se puede leer como un archivo de texto. Este archivo es común en sistemas operativos Debian, Ubuntu. Se puede visualizar los inicios de sesión fallidos de forma remota con las líneas que contienen la leyenda "Failed password for <usuario>". Permitiendo identificar si se realizó un ataque de fuerza bruta al equipo analizado.

- `/var/log/secure`: al igual que la bitácora anterior registra los inicios de sesión fallidos y exitosos, las veces que se ejecuta el comando `su`. Se puede leer como un archivo de texto. Este archivo es común en CentOS, Red Hat.

3.6.3.8.3. Bitácoras de correo y servidor web

- `/var/log/mail.log`: contienen los registros del servidor de correo que haya en el sistema. Entre otros datos, podremos encontrar información sobre los e-mails enviados.

- `/var/log/apache2/access.log`, `/var/log/nginx/access.log`: dado que muchos ataques a servidores se realizan mediante algún plug-in vulnerable de una aplicación web, el revisar estas bitácoras me ayudaban a visualizar peticiones maliciosas al servidor, si se subieron archivos sospechosos, etc.

3.6.3.9. Búsqueda de archivos sospechosos.

En este paso buscaba archivos que el atacante hubiera instalado en el servidor mediante las siguientes técnicas:

3.6.3.9.1. Archivos y directorios ocultos

- Inician con un punto "." ".." "…"
- Inician con espacio " "

3.6.3.9.2. Nombres de archivos o directorios con caracteres no imprimibles

- El nombre inicia con uno o varios caracteres ASCII no imprimibles.

- El comando `#ls -b`, permite listar el contenido de un directorio desplegando los nombres en formato C para caracteres no gráficos.

3.6.3.9.3. Tareas programas en cron

El atacante pudo programar tareas en el equipo para ejecutar archivos maliciosos en el equipo a su conveniencia. Para revisar estas tareas programadas revisaba los siguientes archivos:

- `#cat /etc/cron*`
- `#/var/spool/cron/crontab/nombre_usuario`

3.6.3.9.4. Archivos en `/boot` o `/tmp`

Estos directorios suelen ser utilizados para esconder software malicioso, por lo que identificaba si existían archivos ejecutables en estos directorios con el comando file.

- `#file /tmp/*`
- `#file /boot/*`

3.6.3.9.5. Archivos regulares en /dev

Este directorio suele ser utilizado para esconder software malicioso. Los podía diferenciar de los directorios para dispositivos de hardware que suele tener `/dev` porque se mostraban como archivos regulares.

Los identificaba con el comando:

```
#find /montado/analisis/dev/ -type f –print
```

3.6.3.9.6. Análisis de cadenas de archivos sospechosos

Cuando encontraba un archivo sospechoso ejecutable, realizaba un análisis de cadenas para identificar algunas otras referencias a archivos maliciosos, usuarios o rutas dentro del ejecutable, ya que no contaba con el código fuente.

Para este fin utilizaba el comando:

```
#strings nombre_archivo
```

El comando `strings` muestra cadenas de caracteres imprimibles con al menos 4 caracteres de longitud seguidas de un carácter no imprimible. Es útil para visualizar el contenido de archivos que no son de texto como lo son los archivos ejecutables.

3.6.3.10. **Recuperación de datos**

Para la recuperación de datos realizaba Carving, a continuación cito la definición de carving de Michael Hale Ligh:

"el proceso de extraer una serie de datos de un gran conjunto de datos. La técnica de data carving se utiliza habitualmente durante una investigación digital cuando se analiza el espacio no ubicado de un sistema de archivos para extraer archivos. Los archivos son 'desenterrados' del espacio no ubicado utilizando valores para las cabeceras y pies específicos del tipo de archivo. Las estructuras manejadas por el sistema de archivos no se tienen en cuenta durante el proceso"

Michael Hale Ligh, The Art of Memory Forensics

La recuperación de archivos parte de los encabezados, en los cuales se tiene un número mágico que identifica a cada tipo de archivo. Esto me permitía recuperar archivos por su tipo siempre y cuando conociera ese número. A su vez me era necesario el pie de archivo.

Si bien se puede realizar carving de manera "manual", existen herramientas que facilitaban mi trabajo como analista y contienen tipos de archivos ya definidos que se pueden recuperar, por ejemplo .jpg, .png, .eml, etc. A su vez podía editar el archivo de configuración para agregar los encabezados de archivos que ocupaba dependiendo el caso. A continuación explico la sintaxis de algunas herramientas.

- **Foremost**

  ```
  #foremost -v -t tipo(s)_archivo(s) –i dispositivo_in
  –o dispositivo_out
  ```

  Donde:

  - El dispositivo puede ser un disco o un archivo de imagen
  - -t: Indica el tipo de archivos a recuperar (png,all).
  - -v: Modo verboso
  - -i: Indicamos la ruta del dispositivo de entrada a recuperar archivos.
  - -o: ruta del dispositivo de salida, donde almacenará los archivos recuperados.

El archivo de configuración de foremost es `/etc/foremost.conf`, se puede editar para añadir archivos específicos, considerando los campos que muestro en la tabla:

Tabla 9. Datos para añadir un archivo .pst al archivo de configuración de foremost. Fuente: elaboración propia.

Tipo de archivo	Case sensitive	Tamaño máximo de archivo	Cabecera del archivo
pst	Y	400000000	\x21\x42\x4e\xa5\x6f\xb5\xa6

```
#----------------------------------------------------------------------
#
# Word documents
#       (NOTE THIS FORMAT HAS A BUILTIN EXTRACTION FUNCTION)
        doc     y       12500000  \xd0\xcf\x11\xe0\xa1\xb1
#
# Outlook files
        pst     y       400000000 \x21\x42\x4e\xa5\x6f\xb5\xa6
        ost     y       400000000 \x21\x42\x44\x4e
#
# Outlook Express
#       dbx     y       4000000 \xcf\xad\x12\xfe\xc5\xfd\x74\x6f
#       idx     y       4000000 \x4a\x4d\x46\x39
#       mbx     y       4000000 \x4a\x4d\x46\x36
#
#----------------------------------------------------------------------
```

Figura 7. Ejemplo de archivo de configuración /etc/foremost.conf. Fuente: elaboración propia.

- **Scalpel**

  Es una herramienta muy parecida a Foremost, en cuanto a sintaxis y el archivo de configuración.

  ```
  #scalpel  -v dispositivo_in –o dispositivo_out
  ```

  Donde:

  El dispositivo puede ser un disco o un archivo de imagen.

  - -v: modo verboso.
  - -o: ruta del dispositivo de salida, donde almacenará los archivos recuperados.

Archivo de configuración `/etc/scalpel/scalpel.conf`

3.6.3.11. **Reporte de resultados: Informe**

Al finalizar la revisión del equipo afectado entregaba un reporte de los resultados. En este informe consideraba los siguientes puntos:

- Antecedentes del caso.
- Descripción del sistema analizado.
- Pasos que se seguí durante el análisis de manera que sean repetibles.
- Información técnica del análisis. Herramientas utilizadas, descripción de los hallazgos.
- Reporte ejecutivo. Una explicación no técnica del resultado del análisis.
- Conclusiones. Basadas en los hallazgos encontrados.
- Recomendaciones como analista. Para evitar futuros incidentes del mismo tipo.

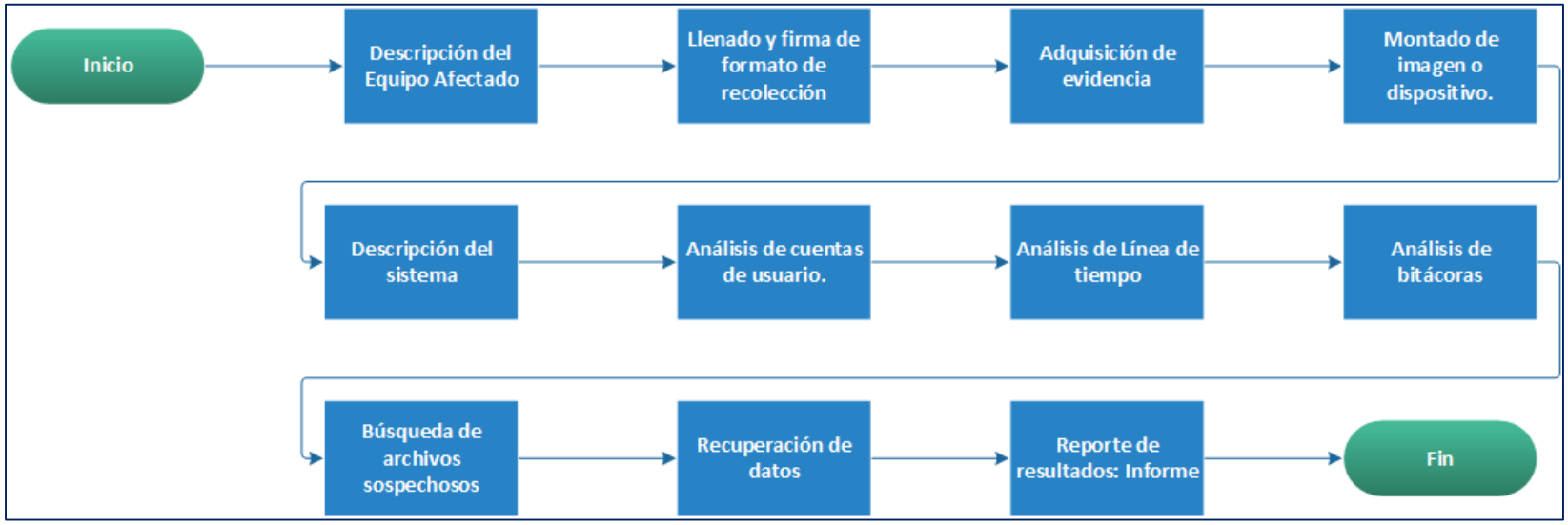

Figura 8. Actividades realizadas para el Análisis Forense. Fuente: elaboración propia.

3.6.4. **Resultados**

Realicé análisis forense en equipos pertenecientes a Red-UNAM, cuando las dependencias que los administraban solicitaron el apoyo en la revisión de los mismos.

Así mismo, actualice o añadí información a la documentación interna de los análisis que aportaron nuevo conocimiento o fueron casos especiales, quedando como lecciones aprendidas para el equipo de respuesta a incidentes.

4. Análisis Forense en equipo de la Red Universitaria.

4.1. Problemática

UNAM-CERT recibe un oficio de parte de una dependencia de la UNAM solicitando apoyo para la revisión de un equipo con dirección IP 192.168.X.X en el que se había detectado y notificado un incidente de seguridad, el cual consistía en el envió de constantes peticiones desde el equipo hacia otros equipos entre el 12 de febrero del 2017 y el 13 de febrero del 2017.

4.2. Objetivo

- Realizar el análisis forense al equipo con dirección IP 192.168.X.X

4.3. Actividades

A continuación se listan las actividades que realicé y mostraron resultados relevantes:

- Descripción del equipo afectado
- Llenado y firma de formato de recolección de evidencia digital
- Adquisición de evidencia
- Montado de imagen
- Descripción del sistema
- Análisis de cuentas de usuario
- Análisis de línea de tiempo
- Revisión de bitácoras
- Búsqueda de archivos sospechosos
- Revisión de tareas programadas

4.4. Resultados de las actividades realizadas

4.4.1. **Descripción del equipo afectado**

De acuerdo a información proporcionada por el administrador del equipo afectado obtuve los siguientes datos del equipo:

- Dirección IP: 192.168.X.X
- Sistema Operativo: CentOS 6
- Capacidad de almacenamiento: 500 GB
- Administrador: Administrador dependencia UNAM

4.4.2. **Llenado y firma de formato de recolección de evidencia digital**

En esta actividad llené el formato correspondiente de recolección de evidencia tomando los siguientes datos:

Fecha y hora
11.02.17 15:17
Número de caso
00745
Nombre del responsable del equipo
Administrador dependencia UNAM
Nombre del responsable de toma de Evidencia. Analista Forense.
Nayely Morales Perales
Descripción del dispositivo
Sistema Operativo: CentOS 6
Sistema de Archivos: ext4
Capacidad: 500 GB
Modelo: HP2147G8
Número de Serie: 474836480
SHA-256 evidencia: 81f51533b559138680696d2e5ce8b88
Etiqueta del disco o imagen: discoAnalisis745

4.4.3. **Adquisición de evidencia**

Realicé una copia bit a bit del disco del equipo afectado con el kit forense. Al finalizar la copia obtuve el Hash con cifrado SHA-256 del disco copiado y lo registré en el formato de recolección de evidencia digital.

Así mismo, etiquete el disco como: `discoAnalisis745`.

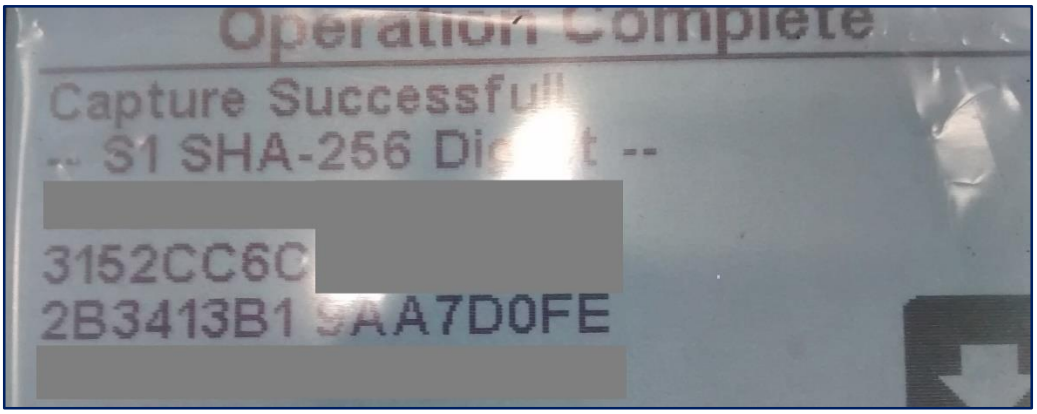

Figura 9. Hash del disco copiado durante adquisición de evidencia. Fuente: elaboración propia.

4.4.4. **Montado de imagen**

Una vez que trasladé el disco copiado al laboratorio. Utilicé la SIFT para revisar las particiones del disco y montarlo para el análisis.

Identifiqué las siguientes particiones del disco:

- /boot
- LVM
  - /home
  - /root

Dado que el disco contenía un LVM, liste las particiones disponibles para montar.

Para posteriormente montar la partición raíz / que se encontraba en el mapeo con la etiqueta `loop0p3`.

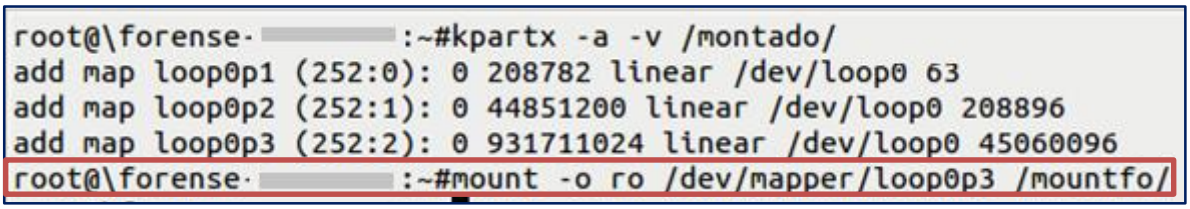

Figura 10. Montado de disco para análisis. Fuente: elaboración propia.

4.4.5. **Descripción del sistema**

De acuerdo a la información obtenida previamente con el administrador del equipo, validé que el sistema operativo del equipo afectado era `CentOS 6.0`:

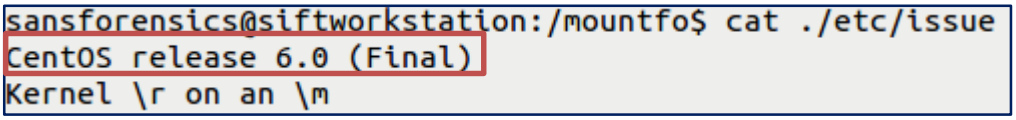

Figura 11. Sistema operativo del equipo afectado. Fuente: elaboración propia.

Igualmente identifiqué que el nombre del equipo era `EquipoA`:

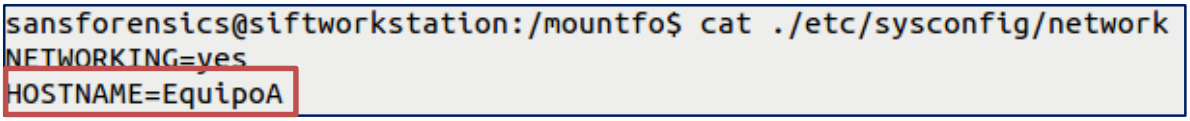

Figura 12. Nombre del equipo afectado. Fuente: elaboración propia.

4.4.6. **Análisis de cuentas de usuario**

Revisé las cuentas de usuarios ubicadas en el archivo `/etc/passwd`, las cuales listo en la siguiente imagen, y todos los usuarios contaban con una Shell del sistema válida:

```
sansforensics@siftworkstation:/mountfo$ cat ./etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
saslauth:x:499:76:Saslauthd user:/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
ouser:x:500:500::/home/ouser:/bin/bash
```

Figura 13. Archivo /etc/passwd del equipo afectado. Fuente: elaboración propia.

De igual manera identifiqué la última fecha de modificación del archivo `/etc/passwd` y fue realizada el 14 de noviembre del 2016, por lo que no se creó usuarios posteriormente:

```
sansforensics@siftworkstation:/mountfo$ stat ./etc/passwd
  File: `./etc/passwd'
  Size: 2067            Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 32115887    Links: 1
Access: (0644/-rw-r--r--)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2017-02-17 06:03:56.139603485 +0000
Modify: 2016-11-14 06:03:56.099603484 +0000
Change: 2016-11-14 06:03:56.103603484 +0000
 Birth: -
```

Figura 14. Fecha de última modificación de archivo /etc/passwd. Fuente: elaboración propia.

Para el archivo `/etc/shadow` la última fecha de modificación se realizó el 14 de noviembre del 2016, por tanto no se modificó ninguna contraseña posterior a esta fecha:

```
sansforensics@siftworkstation:/mountfo$ stat ./etc/shadow
  File: `./etc/shadow'
  Size: 620             Blocks: 8          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 30147019    Links: 1
Access: (0000/----------)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2017-02-17 06:03:56.139603485 +0000
Modify: 2016-11-14 06:03:56.099603484 +0000
Change: 2016-11-14 06:03:56.103603484 +0000
 Birth: -
```

Figura 15. Fecha de última modificación de archivo /etc/shadow. Fuente: elaboración propia.

Así mismo, observé que en el archivo `/etc/sudoers`, el usuario `root` era el único con privilegios administrativos en el sistema:

```
## Next comes the main part: which users can run what software on
## which machines (the sudoers file can be shared between multiple
## systems).
## Syntax:
##
##      user    MACHINE=COMMANDS
##
## The COMMANDS section may have other options added to it.
##
## Allow root to run any commands anywhere
root    ALL=(ALL)       ALL

## Allows members of the 'sys' group to run networking, software,
## service management apps and more.
# %sys ALL = NETWORKING, SOFTWARE, SERVICES, STORAGE, DELEGATING,
VERS

## Allows people in group wheel to run all commands
# %wheel        ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL
```

Figura 16. Archivo /etc/sudoers del equipo afectado. Fuente: elaboración propia.

Verifiqué la última fecha de modificación del archivo `/etc/sudoers y` fue el 08 de diciembre del 2015. Esto me indicó que después de esta fecha el usuario `root` era el único con privilegios de administrador:

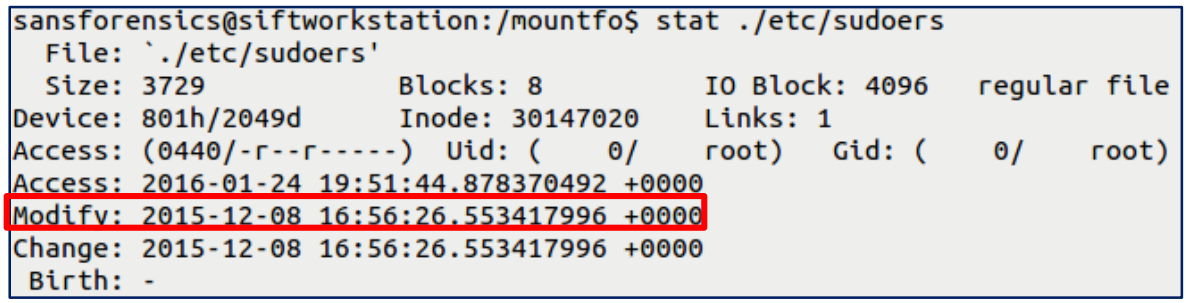

Figura 17. Fecha de última modificación del archivo /etc/sudoers. Fuente: elaboración propia.

Realicé la revisión del historial de comandos, pero no encontré ningún comando sospechoso en el equipo. Sin embargo, en la línea de tiempo identifiqué que el día 13 de febrero del 2017 a las 00:42:19 horas hubo una modificación en el contenido del archivo `/root/.bash_history` y en los metadatos.

```
Mon Feb 13 2017 00:42:19 17805 m.c. r/rrw------- 0
0 42 /root/.bash_history
```

Corroboré la información proporcionada por la línea del tiempo con el comando `stat` y la fecha de modificación del archivo `/root/.bash_history` 13 de febrero del 2017 a las 00:42:19 horas coincidió:

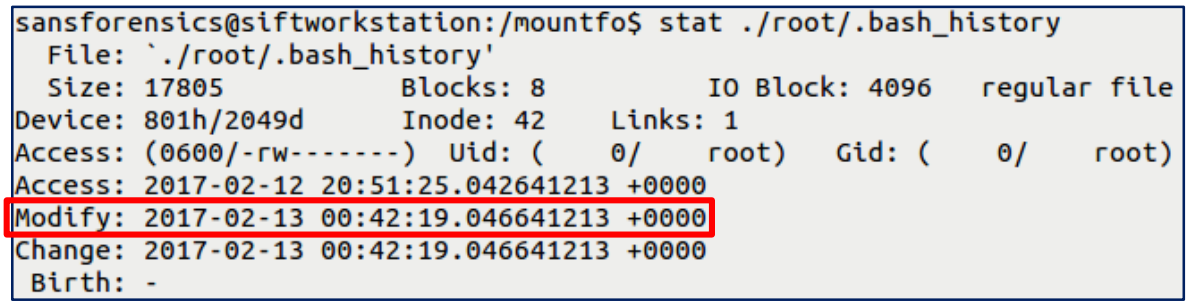

Figura 18. Fecha de última modificación del archivo /root/.bash_history. Fuente: elaboración propia.

4.4.7. **Análisis de línea de tiempo**

Generé una línea de tiempo en la cual me fue posible identificar la creación, modificación o cambios en distintos archivos coincidentes con la fecha del segundo acceso exitoso con la cuenta `root` mediante el protocolo `SSH` el 07 de Febrero del 2017 a las 19:27:53 horas, desde una IP externa a Red-UNAM.

El 07 de Febrero del 2017 a las 19:28:02 horas se inició la creación, modificación y acceso de los siguientes archivos:

Tabla 10. Archivos que se crearon, modificaron y accedieron el 07 de Febrero del 2017 a las 19:28:02. Fuente: elaboración propia.

MACtime	Archivo
Feb 07 2017 19:28:02 (creación)	/boot/pxrofmurbz
Feb 07 2017 19:28:02 (cambio en metadatos y modificación del contenido)	/etc/cron.hourly
Feb 07 2017 19:28:02 (creación)	/etc/cron.hourly/cron.sh

```
Thu Feb 07 2017 19:28:02   317 ...b r/rrwxr-xr-x
2903798712 2903798712 150116   /boot/pxrofmurbz

Thu Feb 07 2017 19:28:024096 m.c. d/drwxr-xr-x 0
0        259073   /etc/cron.hourly

Thu Feb 07 2017 19:28:02   223 ...b r/rrwxr-xr-x 0
0        263748   /etc/cron.hourly/cron.sh
```

De igual modo, el 12 de febrero del 2017 a las 21:59:45 horas, observé un último acceso al archivo `pxrofmurbz` y coincidió con la fecha en la que se detectó el incidente de seguridad:

```
Sun Feb 12 2017 20:59:45 317 ...a r/rrwxr-xr-x
2903798712 2903798712 150116   /boot/pxrofmurbz
```

4.4.8. **Revisión de bitácoras**

Revisé el log `/var/log/secure` en el que se registran los inicios de sesión fallidos y exitosos e identifiqué varios intentos de acceso fallidos que se efectuaron del 12 de Enero al 06 de Febrero del 2017 con el usuario `root` a través del protocolo `SSH`. Esto nos indica un ataque de fuerza bruta.

```
Jan 12 11:48:16 EquipoA sshd[1834]: Failed password for root from 192.126.120.  port 566
32 ssh2
Jan 12 11:48:16 EquipoA sshd[1835]: Failed password for root from 192.126.120.  port 566
33 ssh2
Jan 12 11:48:16 EquipoA sshd[1832]: Failed password for root from 192.126.120.  port 566
30 ssh2
Jan 12 11:48:18 EquipoA sshd[1823]: Failed password for root from 192.126.120.  port 566
22 ssh2
Jan 12 11:48:18 EquipoA sshd[1861]: Failed password for root from 192.126.120.  port 566
38 ssh2
Jan 12 11:48:18 EquipoA sshd[1828]: Failed password for root from 192.126.120.  port 566
27 ssh2
Jan 12 11:48:18 EquipoA sshd[1825]: Failed password for root from 192.126.120.  port 566
24 ssh2
Jan 12 11:48:18 EquipoA sshd[1829]: Failed password for root from 192.126.120.  port 566
28 ssh2
Jan 12 11:48:18 EquipoA sshd[1826]: Failed password for root from 192.126.120.  port 566
25 ssh2
Jan 12 11:49:43 EquipoA sshd[1888]: Failed password for root from 192.126.120.  port 566
48 ssh2
Jan 12 11:49:43 EquipoA sshd[1881]: Failed password for root from 192.126.120.  port 566
41 ssh2
Jan 12 11:49:43 EquipoA sshd[1887]: Failed password for root from 192.126.120.  port 566
47 ssh2
```

Figura 19. Archivo /var/log/secure/ del equipo afectado. Fuente: elaboración propia.

```
Jan 23 11:49:45 EquipoA sshd[1881]: Failed password for root from 117.21.227.  port 5664
1 ssh2
Jan 23 11:49:45 EquipoA sshd[1887]: Failed password for root from 117.21.227.  port 5664
7 ssh2
Jan 13 11:49:45 EquipoA sshd[1886]: Failed password for root from 117.21.227.  port 5664
6 ssh2
Jan 23 11:49:45 EquipoA sshd[1885]: Failed password for root from 117.21.227.  port 5664
5 ssh2
Jan 23 11:49:45 EquipoA sshd[1880]: Failed password for root from 117.21.227.  port 5664
0 ssh2
Jan 23 11:54:08 EquipoA sshd[1937]: Failed password for root from 117.21.227.  port 5665
9 ssh2
Jan 23 11:54:08 EquipoA sshd[1936]: Failed password for root from 117.21.227.  port 5665
8 ssh2
Jan 23 11:54:08 EquipoA sshd[1940]: Failed password for root from 117.21.227.  port 5666
2 ssh2
Jan 23 11:54:08 EquipoA sshd[1939]: Failed password for root from 117.21.227.  port 5666
1 ssh2
Jan 23 11:54:08 EquipoA sshd[1938]: Failed password for root from 117.21.227.  port 5666
0 ssh2
Jan 23 11:54:08 EquipoA sshd[1944]: Failed password for root from 117.21.227.  port 5666
6 ssh2
```

Figura 20. Archivo /var/log/secure/ del equipo afectado. Fuente: elaboración propia.

Conforme a las direcciones IP registradas, el ataque se realizó desde IPs de EU `192.126.120.X` y China `117.21.227.X` de acuerdo a la base de datos `whois`:

```
sansforensics@siftworkstation:~$ whois 192.126.120.
OrgName:        HOSTSPACE NETWORKS LLC
OrgId:          HNL-17
Address:        1788 SIERRA LEONE AVE #108-100
City:           Los Angeles
StateProv:      CA
PostalCode:     91748
Country:        US
RegDate:        2012-09-24
Updated:        2017-01-28
```

Figura 21. Salida de comando whois IP 192.126.120.X. Fuente: elaboración propia.

```
sansforensics@siftworkstation:~$ whois 117.21.227.
inetnum:        117.21.0.0 - 117.21.255.255
netname:        CHINANET-JX
descr:          CHINANET Jiangxi province network
descr:          China Telecom
descr:          No.31,jingrong street
descr:          Beijing 100032
country:        CN
admin-c:        CH93-AP
tech-c:         JN113-AP
```

Figura 22. Salida de comando whois IP 117.21.227.X. Fuente: elaboración propia.

Identifiqué que el día 06 Febrero del 2017 a las 21:05:26 horas se registró un primer acceso exitoso al equipo y el 07 de Febrero del 2017 a las 19:27:53 horas hubo un segundo acceso. Ambos accesos al equipo se realizaron desde direcciones IP ajenas a Red-UNAM mediante el protocolo `SSH` utilizando la cuenta de usuario `root`.

```
sansforensics@siftworkstation:/mountfo/var/log$ grep "Accepted password" secure*
secure:Feb 6 21:05:26 EquipoA sshd[2010]: Accepted password for root from 192.126.120.
port 56680 ssh2
secure:Feb 7 19:27:53 EquipoA sshd[2010]: Accepted password for root from 23.226.153.
port 56680 ssh2
```

Figura 23. Conexiones exitosas con la cuenta root protocolo SSH. Fuente: elaboración propia.

Consulté nuevamente la base de datos de `whois` el origen de las direcciones e indica que la dirección IP `192.126.120.X` es de Los Ángeles, CA y la IP `23.226.67.X` es de Phoenix, Arizona.

```
sansforensics@siftworkstation:~$ whois 192.126.120.
OrgName:        HOSTSPACE NETWORKS LLC
OrgId:          HNL-17
Address:        1788 SIERRA LEONE AVE #108-100
City:           Los Angeles
StateProv:      CA
PostalCode:     91748
Country:        US
RegDate:        2012-09-24
Updated:        2017-01-28
```

Figura 24. Salida de comando whois IP 192.126.120.X. Fuente: elaboración propia.

```
sansforensics@siftworkstation:~$ whois 23.226.67.
OrgName:        Input Output Flood LLC
OrgId:          IOFL
Address:        3402 E University Dr. #6
City:           Phoenix
StateProv:      AZ
PostalCode:     85034
Country:        US
RegDate:        2011-05-02
Updated:        2017-01-28
```

Figura 25. Salida de comando whois IP 23.226.67.X. Fuente: elaboración propia.

4.4.9. **Búsqueda de archivos sospechosos**

Inicié la búsqueda de archivos maliciosos en el directorio `/boot` e identifiqué los archivos `/boot/pxrofmurbz` y `/boot/komkshzuhx`.

```
sansforensics@siftworkstation:/mountfo/boot$ ls -la
total 26244
drwxrwxr-x 3 root root     1024 Aug 15 16:19 efi
drwxrwxr-x 2 root root     1024 Aug 15 16:23 grub
-rw-r--r-- 1 root root   108282 Aug 15 18:54 config-2.6.32-754.el6.x86_64
-rw------- 1 root root 18504172 Aug 15 18:54 initramfs-2.6.32-754.el6.x86_64.img
-rw-r--r-- 1 root root   216063 Sep 25 08:19 symvers-2.6.32-754.el6.x86_64.gz
-rw-r--r-- 1 root root  2652834 Sep 25 08:20 System.map-2.6.32-754.el6.x86_64
-rwxr-xr-x 1 root root  4315504 Sep 25 08:20 vmlinuz-2.6.32-754.el6.x86_64
drwxrwxr-x 2 root root    12288 Feb 10 17:20 lost+found
-rwxr-xr-x 1 root root   534245 Feb 12 21:58 komkshzuhx
-rwxr-xr-x 1 root root   530234 Feb 12 21:59 pxrofmurbz
drwxrwxr-x 2 root root     4096 Feb 12 21:59 .
drwxrwxr-x 6 root root     4096 Feb 12 21:59 ..
```

Figura 26. Archivos maliciosos encontrados en /boot. Fuente elaboración propia.

Revisé el tipo y el formato del archivo `/boot/pxrofmurbz`, y correspondía a un ejecutable.

```
sansforensics@siftworkstation:/mountfo/boot$ file pxrofmurbz
pxrofmurbz: ELF 64-bit LSB executable, x86-64, version 1 (SYSV),dynamically li
nked (use shared libs), for GNU/Linux 2.6.24, BuildID[sha1]=3fa0af38a451b09079
363b7aa2c0c4adf5221c4, not stripped
```

Figura 27. Tipo del archivo /boot/pxrofmurbz. Fuente: elaboración propia.

Comprobé el último acceso al archivo `/boot/pxrofmurbz` y fue el 12 de febrero del 2017 a las 21:59:45 horas, como se muestra a continuación:

```
sansforensics@siftworkstation:/mountfo/boot$ stat pxrofmurbz
  File: `pxrofmurbz'
  Size: 530234          Blocks: 8432       IO Block: 4096   regular file
Device: 801h/2049d      Inode: 30146962    Links: 1
Access: (0755/-rwxr-xr-x)  Uid: ( 0/root)   Gid: ( 0/root)
Access: 2017-02-12 21:59:45.7089793532 +0000
Modify: 2017-02-12 21:57:34.9608793532 +0000
Change: 2017-02-12 21:57:34.9608793532 +0000
 Birth: -
```

Figura 28. Fecha de último acceso al archivo /boot/pxrofmurbz. Fuente: elaboración propia.

De igual forma llevé a acabo un análisis de cadenas al archivo /boot/pxrofmurbz y encontré las siguientes.

Cadenas referentes a tareas programadas en /etc/cron.hourly/:

```
esac
/etc/init.d/%s
/etc/cron.hourly/cron.sh
/etc/rc%d.d/S90%s
/etc/rc.d/rc%d.d/S90%s
--add
chkconfig
defaults
update-rc.d
sed -i '/\/etc\/cron.hourly\/cron.sh/d' /etc/crontab && echo '*/3 * * * * root
 /etc/cron.hourly/cron.sh' >> /etc/crontab
%s%s
insmod
--del
remove
```

Figura 29. Cadenas encontradas en el archivo /boot/pxrofmurbz. Fuente: elaboración propia.

Cadenas que contenían la palabra "DDOS" la cual es la abreviación del ataque distributed denial-of-service.

```
1%o2
1Lo2
1So2
1Zo2
/home/usa/OnlineBuildDDOS_64/upload/build/6DDAB70981EE7CC514F56B717DD4A0C5
/home/usa/OnlineBuildDDOS_64/upload/header/3C9A021D44440BF77B6038281CF6C9E6/ar
ch/x86/include/asm
include/linux
include/asm-generic
include/net
include/linux/hdlc
include/net/netns
```

Figura 30. Cadenas encontradas en el archivo /boot/pxrofmurbz. Fuente: elaboración propia.

También encontré las siguientes cadenas que parecían parte de un script en bash:

```
72F/.V6
#!/bin/sh
PATH=/bin:/sbin:/usr/bin:/usr/sbin:/usr/local/bin:/usr/local/sbin:/usr/X11R6/bin
for i in `cat /proc/net/dev|grep :|awk -F: {'print $1'}`; do ifconfig $i up& done
cp /lib/udev/udev /lib/udev/debug
/lib/udev/debug
BB2FA36AAA9541F0
103.25.9.228
8.8.8.8
```

Figura 31. Cadenas encontradas en el archivo /boot/pxrofmurbz. Fuente: elaboración propia.

Seguidamente, analicé el archivo /`boot/pxrofmurbz` con el servicio de *VirusTotal,* este lo identificó como un `backdoor` para Linux y una herramienta para realizar `ataques de denegación de servicio`. Este archivo es detectado por 8 de 57 motores antivirus, como se muestra en la imagen a continuación:

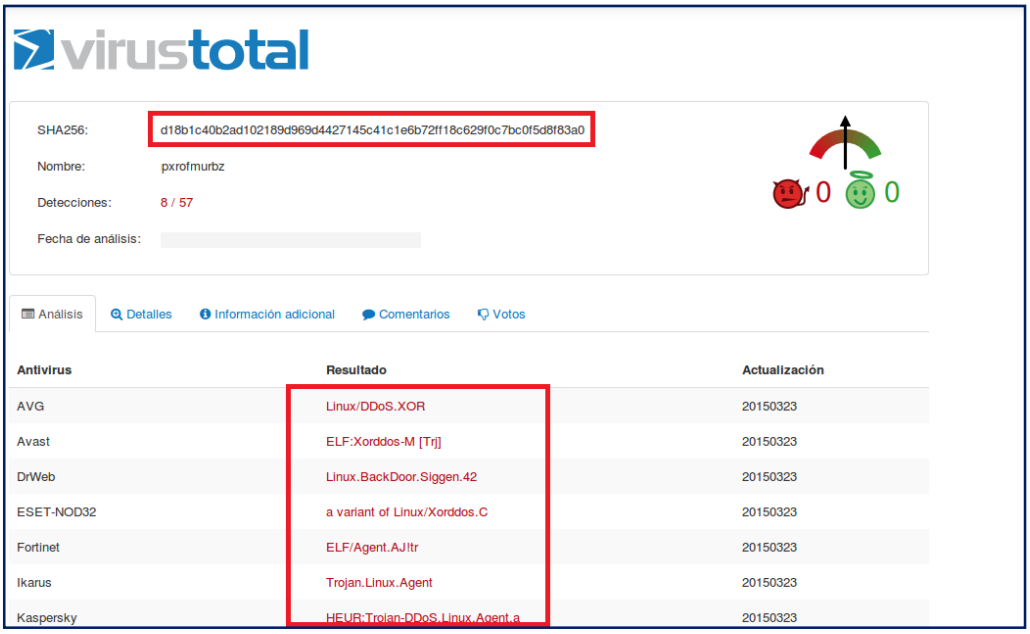

Figura 32. Análisis con VirusTotal del archivo /boot/pxrofmurbz. Fuente: VirusTotal.

Posteriormente, analicé el tipo y formato del archivo `/boot/komkshzuhx` y al igual que el archivo `/boot/pxrofmurbz` era un ejecutable:

```
sansforensics@siftworkstation:/mountfo/boot$ file komkshzuhx
komkshzuhx: ELF 64-bit LSB executable, x86-64, version 1 (SYSV),dynamically li
nked (use shared libs), for GNU/Linux 2.6.24, BuildID[sha1]=3fa0af38a451b09079
363b7aa2c0c4adf5221c4, not stripped
```

Figura 33. Tipo de archivo /boot/komkshzuhx. Fuente: elaboración propia.

El último acceso al archivo `/boot/komkshzuhx` fue el 12 de febrero del 2017 a las 21:58:50 horas:

```
sansforensics@siftworkstation:/mountfo/boot$ stat komkshzuhx
  File: `komkshzuhx'
  Size: 534245          Blocks: 8432       IO Block: 4096   regular file
Device: 801h/2049d      Inode: 30147146    Links: 1
Access: (0755/-rwxr-xr-x)  Uid: ( 0/root)   Gid: ( 0/root)
Access: 2017-02-12 21:58:50.908999532 +0000
Modify: 2017-02-12 21:57:07.838999532 +0000
Change: 2017-02-12 21:57:07.838999532 +0000
 Birth: -
```

Figura 34. Fecha de último acceso al archivo /boot/komkshzuhx. Fuente: elaboración propia.

De igual manera, efectué un análisis de cadenas en el archivo `/boot/komkshzuhx` y las cadenas que encontré fueron coincidentes con las del archivo `/boot/pxrofmurbz`. En la siguiente imagen muestro una de las coincidencias:

```
-/lL:ZZ
!-/i
!-/i
!-/i
KLY/
Y;uh
include/asm-generic
/home/usa/OnlineBuildDDOS_64/upload/header/3C9A021D44440BF77B6038281CF6C9E6/ar
ch/x86/include/asm
include/linux
/home/usa/OnlineBuildDDOS_64/upload/build/6DDAB70981EE7CC514F56B717DD4A0C5
include/trace/events
int-ll64.h
posix_types_64.h
types.h
```

Figura 35. Cadenas encontradas en el archivo /boot/komkshzuhx. Fuente: elaboración propia.

Analicé con el servicio *VirusTotal* el archivo `/boot/komkshzuhx` y lo identificó como una herramienta para realizar `ataques de denegación de servicio`. Este archivo fue detectado por 12 de 56 motores antivirus como se muestra en la siguiente imagen:

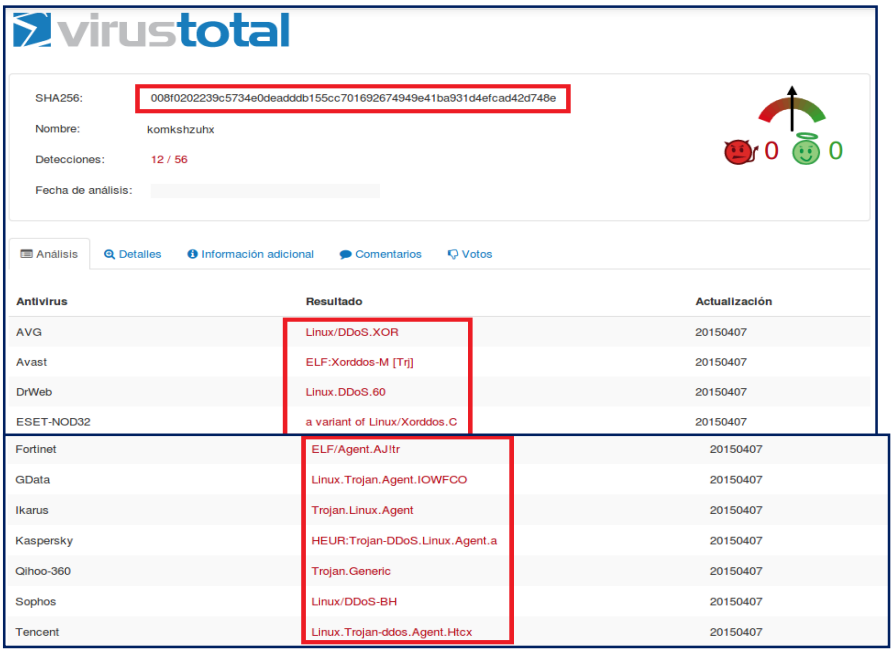

Figura 36. Análisis con VirusTotal de archivo /boot/komkshzuhx .Fuente: VirusTotal

4.4.10. **Revisión de tareas programadas**

En el directorio de tareas programadas por hora `/etc/crontab/cron.hourly`, identifiqué el script `cron.sh` que hace referencia al archivo malicioso `/lib/udev/udev`. Pude observar que el contenido del script coincide con las cadenas encontradas en los archivos maliciosos `/boot/pxrofmurbz` y `/boot/komkshzuhx`.

En la siguiente imagen muestro el contenido del script:

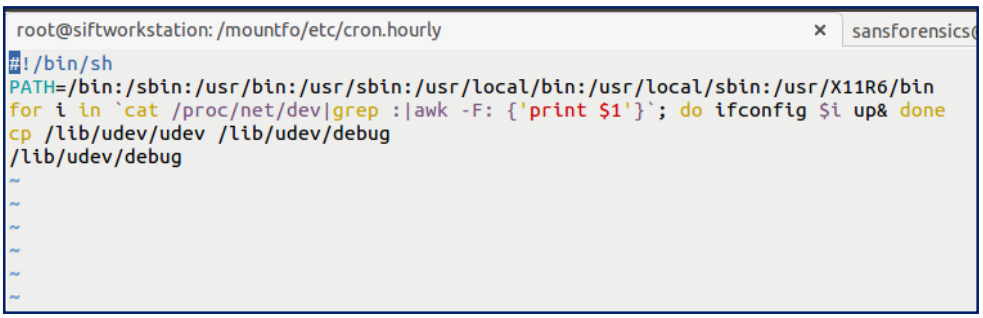

Figura 37. Contenido del script cron.sh. Fuente: elaboración propia.

El archivo `/etc/cron.hourly/cron.sh` fue creado el 07 de febrero del 2018 a las 19:28:02 horas, esta hora coincide un minuto después con la fecha 07 de Febrero del 2017 a las 19:27:53 horas, en la que observé el segundo acceso con la cuenta `root` mediante el protocolo `SSH` al equipo desde una IP ajena a Red-UNAM. También se realizó una modificación en el contenido y metadatos el día 12 de febrero a las 21:58:49 horas y se registró un último acceso al mismo el 13 de febrero las 00:33:01 horas.

```
Thu Feb 07 2017 19:28:02      223 ...b r/rrwxr-xr-x 0
0         263748    /etc/cron.hourly/cron.sh

Sun Feb 12 2017 21:58:49      223 m.c. r/rrwxr-xr-x 0
0         263748    /etc/cron.hourly/cron.sh

Mon Feb 13 2017 00:33:01      223 .a.. r/rrwxr-xr-x 0
0         263748    /etc/cron.hourly/cron.sh
```

Así mismo, al realizar un análisis de cadenas del archivo `/lib/udev/udev`, encontré que también era un ejecutable y las cadenas eran coincidentes con las de los otros archivos maliciosos. En las siguientes imágenes muestro algunas de estas coincidencias:

```
1Lo2
1So2
1Zo2
/home/usa/OnlineBuildDDOS_64/upload/build/6DDAB70981EE7CC514F56B717DD4A0C5
/home/usa/OnlineBuildDDOS_64/upload/header/3C9A021D44440BF77B6038281CF6C9E6/arch/x86/include/asm
include/linux
include/asm-generic
include/net
include/linux/hdlc
include/net/netns
include/trace/events
lkm.c
```

Figura 38. Cadenas encontradas en archivo /lib/udev/udev. Fuente: elaboración propia.

```
NR_FREE_PAGES
x86_init_resources
file_disp
pud_t
/home/usa/OnlineBuildDDOS_64/upload/build/6DDAB70981EE7CC514F56B717DD4A0C5/dhcp.mod.c
safe_wait_icr_idle
release_pte
```

Figura 39. Cadenas encontradas en archivo /lib/udev/udev. Fuente: elaboración propia.

El archivo `/lib/udev/udev` fue creado el 09 de febrero del 2018 a las 19:28:06 horas, se realizó una modificación en el contenido y metadatos el día 12 de febrero a las 21:51:01 horas y se registró un último acceso al mismo el 13 de febrero las 00:42:04 horas.

```
Thu Feb 09 2017 19:28:06    534223 ...b r/rrwxr-xr-x
0         0         42486    /lib/udev/udev

Sun Feb 12 2017 21:51:01    534223 m.c. r/rrwxr-xr-x
0         0         42486    /lib/udev/udev

Mon Feb 13 2017 00:42:04    534223 .a.. r/rrwxr-xr-x
0         0         42486    /lib/udev/udev
```

Realicé también el análisis con el servicio *VirusTotal* y lo identificó como una herramienta para realizar `ataques de denegación de servicio`. Este archivo fue detectado por 9 de 57 motores antivirus:

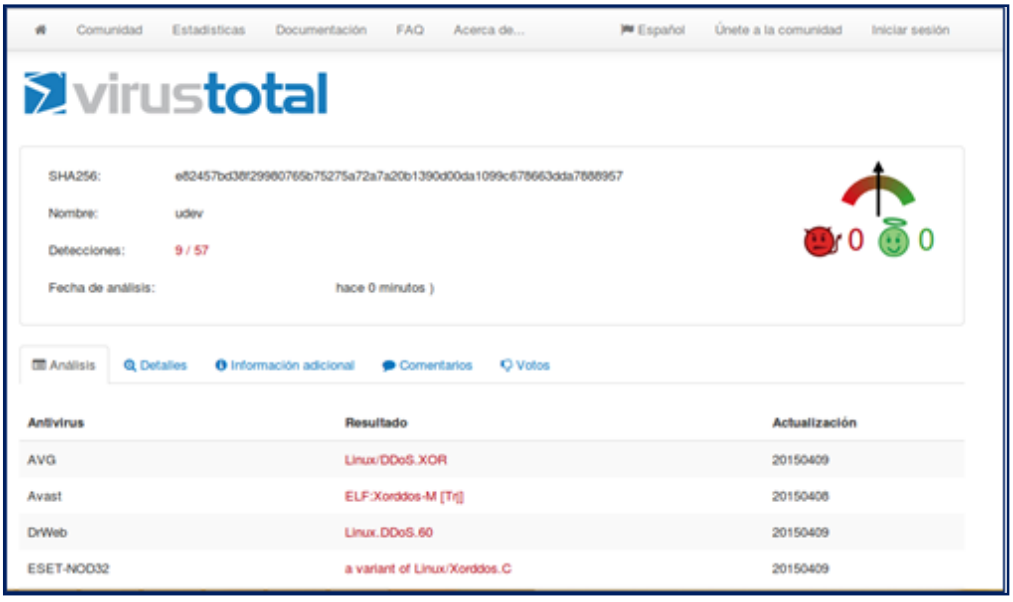

Figura 40. Análisis con VirusTotal del achivo /lib/udev/udev. Fuente: VirusTotal

4.5. Conclusiones

De acuerdo a la evidencia obtenida, corroboré el acceso al equipo por parte de un atacante resultado de un ataque de fuerza bruta que se realizó del 12 de enero al 06 de febrero del 2017 con la cuenta `root` mediante el protocolo `SSH`, conforme a lo que observé en el log `\var\log\secure`. Mediante el ataque de fuerza bruta el atacante tuvo un acceso exitoso por primera vez al `EquipoA` el día 06 de febrero del 2017 a las 21:05:26 horas con la cuenta `root` desde la dirección IP `192.126.120.XX` proveniente de Los Ángeles, CA.

Posteriormente el día 07 de febrero del 2017 a las 19:27:53 horas identifiqué un segundo acceso exitoso con la cuenta `root` por parte del atacante desde la dirección IP `23.226.67.XX` proveniente de Phoenix, Arizona.

A las 19:28:02 horas del mismo día, aproximadamente un minuto después del acceso de las 19:27:53 horas, validé la creación del archivo malicioso `/boot/pxrofmurbz`, el cual reconocí mediante el servicio de *VirusTotal* como un `backdoor` para Linux y una herramienta para realizar `ataques de denegación de servicio.`

Al mismo tiempo y de acuerdo al análisis de cadenas que realicé al archivo malicioso `/boot/ pxrofmurbz`, este creó la tarea programada en el directorio `/etc/cron.hourly`, además del script `cron.sh`

El script `cron.sh` hacía referencia al archivo malicioso `/lib/udev/udev` que era una herramienta para realizar `ataques de denegación de servicio.`

Adicionalmente, en la partición `/boot` encontré el archivo malicioso `/boot/komkshzuhx` el cual era otra herramienta para realizar `ataques de denegación de servicio.`

Como resultado de mi análisis de las cuentas de usuario activas en el `EquipoA`, observé que no se creó alguna cuenta adicional ni se cambió la contraseña de ninguna cuenta durante el periodo de tiempo en que el equipo estuvo comprometido, ya que determiné el 14 de noviembre del 2016 como la última vez que se creó un usuario en el sistema.

Adicionalmente, validé que la cuenta `root` era la única con privilegios de administración en el sistema y que los 4 archivos maliciosos encontrados tenían la cuenta `root` como propietaria.

Determiné que la fechas de modificación y de último acceso a los archivos maliciosos `/lib/udev/udev`, `/etc/cron.hourly/cron.sh.`,

/boot/pxrofmurbz, /boot/komkshzuhx ocurrieron entre 12 de febrero del 2017 21:51:01 horas y el 13 de febrero del 2017 00:42:04 horas. Este periodo de tiempo coincide con la fecha en la que se detectó que el EquipoA envió de repetidas peticiones hacia otros equipos.

De igual forma, el 13 de febrero del 2017 a las 00:42:19 horas observé que se modificó el contenido del archivo /root/.bash_history, lo que indica que el atacante pudo haber borrado parte del contenido del archivo para borrar los comandos ejecutados por él y no dejar evidencia de demás acciones maliciosas.

Obtenida la evidencia y resultado de mi análisis, puedo concluir que el equipo estaba comprometido desde 06 de febrero del 2017 21:05:26 horas, fecha en que el atacante utilizó la cuenta root mediante el protocolo SSH para acceder al equipo. Así mismo, con la cuenta root creo los cuatro archivos maliciosos /lib/udev/udev,/etc/cron.hourly/cron.sh, /boot/pxrofmurbz, /boot/komkshzuhx para mantener el acceso remoto en el EquipoA y para realizar ataques de denegación de servicio a otros equipos entre el 12 de febrero del 2017 y el 13 de febrero del 2017.

A continuación, muestro los eventos relacionados a la intrusión en orden cronológico.

Tabla 11. Eventos relacionados a la intrusión en orden cronológico. Fuente: elaboración propia.

Fecha	Evento	Descripción
12 de enero - 06 de febrero del 2017	Ataque de Fuerza Bruta	En este periodo se realizó un ataque de fuerza bruta hacia el servicio de SSH puerto 22 con la cuenta root, al servidor desde IPs provenientes de China y Estados Unidos.
06 de febrero del 2017 21:05:26 horas	Primer acceso exitoso con la cuenta root al EquipoA	Después del ataque de fuerza bruta efectuado, en la bitácora \var\log\secure se observa un acceso exitoso con la cuenta root mediante el protocolo SSH desde la IP 192.126.120.XX proveniente de los Los Ángeles, CA.

07 de febrero del 2017 19:27:53 horas	Segundo acceso exitoso con la cuenta `root` al `EquipoA`	Se hace la segunda conexión con la cuenta `root` mediante el protocolo `SSH` desde la IP `23.226.67.XX` proveniente de Phoenix,Arizona.
07 de febrero del 2017 19:28:02 horas	Creación de archivos maliciosos.	Se crea el archivo malicioso `/boot/pxrofmurbz` que detecté como como un `backdoor` para Linux y una herramienta para realizar `ataques de denegación de servicio` y el archivo `/etc/cron.hourly/cron.sh` el cual era un script que se ejecutaba mediante una tarea programada por el atacante y hacía referencia al archivo malicioso `/lib/udev/udev`.
09 de febrero del 2017 19:28:06 horas	Creación de archivo malicioso	Se crea archivo malicioso `/lib/udev/udev` el cual identifiqué como una herramienta para realizar `ataques de denegación de servicio.`
12 de febrero del 2017 21:51:01 horas	Modificación de contenido de archivo malicioso y cambio en metadatos.	Modificación de contenido y cambio en metadatos de archivo malicioso `/lib/udev/udev`.
12 febrero del 2017 21:58:49 horas	Modificación de contenido de archivo malicioso y cambio en metadatos.	Modificación de contenido y cambio en metadatos de archivo malicioso `/etc/cron.hourly/cron.sh`
12 de febrero del 2017 21:58:50 horas	Ultimo acceso a archivo malicioso.	Se realiza último acceso al archivo malicioso `/boot/komkshzuhx`, el cual identifiqué como una herramienta para realizar `ataques de denegación de servicio.`

12 de febrero del 2017 21:59:45 horas	Ultimo acceso a archivo malicioso.	Se realiza último acceso al archivo malicioso `/boot/pxrofmurbz`.
13 de febrero del 2017 00:33:01	Ultimo acceso a archivo malicioso.	Se realiza último acceso al archivo malicioso `/etc/cron.hourly/cron.sh`.
13 de febrero del 2017 00:42:04	Ultimo acceso a archivo malicioso.	Se realiza último acceso al archivo malicioso `/lib/udev/udev`.
13 de febrero del 2017 00:42:19	Modificación de contenido de archivo y cambio en metadatos.	Modificación de contenido y cambio en metadatos de archivo `/root/.bash_history`.

4.6. Reporte Ejecutivo

Conforme a la evidencia obtenida, el envió de constantes peticiones desde el equipo afectado hacia otros equipos, fue consecuencia de la ejecución de 4 archivos maliciosos en el servidor entre el 12 de febrero del 2017 21:51:01 horas y el 13 de febrero del 2017 00:42:04 horas.

Estos 4 archivos maliciosos, `/lib/udev/udev` y `/boot/komkshzuhx` fueron identificados como herramientas para realizar *ataques de denegación de servicio*, `/boot/pxrofmurbz`, como un *backdoor* para Linux y una herramienta para realizar *ataques de denegación de servicio*, así como el script `/etc/cron.hourly/cron.sh` que hacía referencia al archivo malicioso `/lib/udev/udev`.

De igual modo se identificó que el equipo afectado estaba comprometido desde el 06 de febrero del 2017 a las 21:05:26 horas resultado de un ataque de fuerza bruta a la cuenta `root` mediante el protocolo `SSH`.

De acuerdo con los hallazgos, se concluye que un atacante obtuvo acceso al equipo afectado mediante la cuenta `root` y la utilizó para crear y ejecutar 4 archivos maliciosos. Estos archivos maliciosos los empleó para mantener

el acceso remoto al equipo y para realizar *ataques de denegación de servicio* a otros equipos.

4.7. Recomendaciones

Para fortalecer la seguridad del equipo afectado, recomendé las siguientes acciones al administrador del equipo:

- Establecer políticas de contraseñas seguras las cuales requieran el uso de caracteres alfanuméricos, símbolos especiales, y con una longitud mínima de 12 caracteres.
- Establecer una política de cambio de contraseñas, donde se solicite a los usuarios cambiarlas cada 6 meses
- El uso de la herramienta **logwatch** para ayudar a monitorizar los archivos de log del sistema y además mandar un mensaje al correo electrónico del administrador del equipo en caso de algún intento de intrusión.
- Instalar un antivirus en el equipo para detectar archivos maliciosos, por ejemplo ClamAV.
- Usar **secthemall**, es un script en bash que analiza archivos de logs y bloquea las direcciones IPs que intenten ataques de fuerza bruta, además de escaneo de puertos, entre otros ataques.
- Implementar reglas de firewall o instalar alguna herramienta para mitigar ataques de fuerza bruta. Se puede hacer uso del firewall de host *iptables* o de la herramienta *fail2ban.*
- Realizar la siguientes modificaciones en la configuración de protocolo SSH(archivo `/etc/ssh/ssh_config`) para fortalecer la seguridad:
    - Deshabilitar el acceso al servicio SSH con el usuario root, `PermitRootLogin no`.
    - Crear una lista de usuarios permitidos con la opción `AllowUsers`.
    - Limitar el número de intentos de inicio de sesión mediante `MaxAuthTries`.
    - Permitir solo autenticación con clave pública editando el archivo `/etc/ssh/sshd_config` en la siguientes líneas:
        - `PubkeyAuthentication yes`
        - `PasswordAuthentication no`
    - En caso de usar contraseñas, no permitir contraseñas vacías, `PermitEmptyPasswords no`

Conclusiones

Las actividades que realicé en mi experiencia como Especialista en respuesta a Incidentes y Cómputo forense, me ayudaron a adquirir conocimientos en esta especialidad de Seguridad Informática. Permitiéndome poner en práctica metodologías y procesos que me ayudaron a obtener mejores resultados y cumplir con los objetivos definidos del Proyecto Seguimiento a incidentes de seguridad informática en la Red Universitaria.

De igual manera, si bien el Proceso de Manejo a Incidentes descrito anteriormente es de vital importancia para la atención de incidentes de seguridad informática; consideró que una de las etapas más importantes es lecciones aprendidas, puesto que estas me preparaban para poder detectar, gestionar y analizar futuros incidentes de manera más eficiente, reflejándose en los tiempos de respuesta.

También considero importante, para el caso de los incidentes de seguridad informática en entidades Externas, reportarlos lo más pronto posible y trabajar en colaboración con los proveedores de hosting para la desactivación del sitio. Tal es el caso del phishing de instituciones Bancarias que pueden afectar a un gran número de personas en poco tiempo. Por esta razón, di seguimiento a estas páginas de forma constante una vez que me eran notificadas y en caso de no tener una pronta respuesta del proveedor, solicité el apoyo de otros equipos de Respuesta Incidentes del país donde se alojaba la página fraudulenta.

Esto me llevó a tomar conciencia de como los cibercriminales unen esfuerzos entre diferentes países para afectar la seguridad de los ciberciudadanos. En vista de estas acciones y con mayor razón los equipos de respuesta a incidentes deben aliarse para combatirlos, ya que sus acciones no afectan solo a un país.

Así mismo, pienso que la mejora continua en la atención de respuesta a incidentes se cumple con la aportación de cada uno de los miembros del equipo de respuesta. Por lo que documenté los casos que se presentaron para generar una base de conocimientos que se pudiera compartir no solo a los miembros internos, si no entre equipos de respuesta a incidentes de diversos países.

En cuanto a análisis de los incidentes, para ser específica, en el análisis forense, considero de vital importancia una vez detectados cuales fueron los puntos débiles que llevaron a un atacante a vulnerar un equipo, dar recomendaciones y asesoría que ayuden al administrador a tener un mejor control y seguridad de sus equipos y evitar futuros incidentes. Así mismo,

obtienen un mayor conocimiento y concientización sobre las amenazas a las que están expuestos.

La concientización del público en general también es de vital importancia para que puedan identificar ataques como scam, phishing, páginas de descarga de malware, etc. y dado que ellos son una fuente de información para reportar incidentes externos, sigamos colaborando en conjunto para evitar el daño que ocasionan. Concientizarlos sobre la importancia de reportar estos incidentes y a qué instituciones de confianza como lo es el CSI/UNAM-CERT, nos beneficia para que menor número de personas sean víctimas de estos fraudes.

Dado lo anterior, opino que es indispensable que el público en general tenga conocimiento de las instituciones a la que puede denunciar incidentes de seguridad informática, ya que a pesar de ser muy comunes hoy en día, muchas personas no saben a dónde acudir cuando se les presenta alguno a pesar de identificarlo. Por lo que sugiero que se haga mayor difusión de estas instituciones, sobre todo del CSI/UNAM-CERT que puede ser de apoyo o bien, dada su experiencia y siendo conocido por otras instituciones del área, dirigir a estas personas a la institución más adecuada.

Por último, puedo decir que mi formación como Especialista en respuesta a Incidentes y Cómputo forense en el CSI/UNAM-CERT me permitió adquirir una base de conocimientos sólida, con mejores prácticas y metodologías aplicadas a la gran cantidad de dependencias tanto de Red-UNAM como externas a las que da atención y demás instituciones dentro y fuera del país con las que colabora.

Glosario

Análisis forense	La adquisición y análisis de información utilizando métodos y herramientas que permitan preservar la integridad de la misma para poder reconstruir la cadena de eventos que determinen acciones maliciosas ocurridas en un sistema.
Análisis muerto	Se realiza cuando el sistema está apagado y se adquiere una copia de los dispositivos de almacenamiento.
Análisis vivo	Se refiere al análisis realizado cuando el sistema está activo y ejecutándose, donde la información puede alterarse a medida que los datos se procesan continuamente.
AS	Autonomous System, es un grupo de redes IP operadas por uno o más operadores de red que posee una política de enrutamiento externa única y claramente Los protocolos de enrutamiento exterior se utilizan para intercambiar información de enrutamiento entre sistemas autónomos.
ASN	Autonomous System Number, es el número único global asociado al AS. Este número se usa tanto en el intercambio de información de enrutamiento exterior (entre sistemas autónomos vecinos) como como un identificador del propio AS.

Cadena de custodia	La documentación de la adquisición, control, análisis y disposición de evidencia física y digital.
CERT	Equipo de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team) es un centro de respuesta a incidentes de seguridad de la información. Grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidentes de seguridad en los sistemas de información.
Dependencias de Red-UNAM	Facultades, institutos y organizaciones en general que pertenecen a la UNAM.
Entidades Externas	Organizaciones que no pertenecen a la UNAM y público en general.
FIRST	Es el Foro de Respuesta a Incidentes y Equipos de Seguridad (*Forum of Incident Response and Security Teams, en inglés)***,** reúne a distintos equipos de seguridad y de respuesta a incidentes incluyendo especialmente los equipos de seguridad de productos por parte del gobierno, comerciales y sectores académicos de todo el mundo.
Incidente de Seguridad Informática	Cualquier evento que afecten la integridad, disponibilidad y/o confidencialidad de un recurso o sistema informático.

Inodo	Estructura de datos que contiene información sobre un archivo como: número de inodo, tipo de archivo, propietario del archivo, permisos, fecha de creación.
IPS	Sistema de Prevención de Intrusos (IPS) es una tecnología de software más hardware que ejerce el control de acceso en una red de computadoras para protegerla de ataques, toman decisiones de control de acceso basados en los contenidos del tráfico de red.
Peakflow	Herramienta de hardware y software que analiza flujos de red. Se ubica en el perímetro de Red-UNAM.
Respuesta a Incidentes	El proceso mediante el cual se detectan, gestionan, analizan y se resuelven incidentes de seguridad. Así mismo implica prevenir la ocurrencia de un incidente. Su principal objetivo es recuperarse del incidente en el menor tiempo posible para continuar con la operación normal.
Sensor	Equipo de cómputo equipado que posee herramientas para la recolección de información a partir del tráfico de red que estos reciben.

Bibliografía

¿En qué consiste el análisis forense de la información? (25 de 06 de 2018). Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2013/08/12/en-que-consiste-analisis-forense-de-informacion/

Ajijola, A. (22 de 11 de 2018). *A Review and Comparative Evaluation of Forensics Guidelines of NIS T SP 800-101 Rev. 1 :2014 and ISO/IEC 27037:2012 .* Obtenido de researchgate: https://www.researchgate.net/profile/Pavol_Zavarsky/publication/271910758_A_review_and_comparative_evaluation_of_forensics_guidelines_of_NIST_SP_800-101_Rev12014_and_ISOIEC_270372012/links/58d2bf51aca2723c0a77741c/A-review-and-comparative-evaluation-of-fo

Albert Marcella, J. D. (2010). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. Auerbach Publications.

APNIC. (25 de 11 de 2018). *Autonomous System numbers – FAQs*. Obtenido de https://www.apnic.net/get-ip/faqs/asn/#what-is-an-asn

Arnes, A. (2018). DIGITAL FORENSICS. John Wiley & Sons.

Carrier, B. (2005). File system Forensics Analysis. Addison Wesley Professional.

FIRST. (28 de 06 de 2018). *Trainings. CSIRT Fundamentals*. Obtenido de https://www.first.org/education/trainings

Installing ClamAV. (23 de 02 de 2018). Obtenido de ClamAV: https://www.clamav.net/documents/installing-clamav#rhel

IPTables. (23 de 02 de 2018). Obtenido de CentOS: https://wiki.centos.org/HowTos/Network/IPTables

Johansen, G. (2017). Digital Forensics and Incident. Birmingham: Packt Publishing Ltd.

Johnson, L. (2014). Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response. USA: ELSEVIER.

Kolhe, M. (22 de 11 de 2018). *Live Vs Dead Computer Forensic Image Acquisition.* Obtenido de International Journal of Computer Science and Information Technologies: https://ijcsit.com/docs/Volume%208/vol8issue3/ijcsit2017080331.pdf

Luggens, J. T. (2014). Incident Response & Computer Forensics. McGraw Hill Education.

Newman, R. C. (2007). Computer Forensics: Evidence Collection And Management. Auerbach Publications.

Nosotros - Acerca de, Misión y Visión. (11 de 03 de 2018). Obtenido de UNAM-CERT: https://www.seguridad.unam.mx/nosotros

OpenSSH security and hardening. (23 de 02 de 2018). Obtenido de Linux Audit: https://linux-audit.com/audit-and-harden-your-ssh-configuration/

SECTHEMALL. (23 de 02 de 2018). Obtenido de https://github.com/SECTHEMALL/secthemall

Servicios de la CSI/UNAM-CERT a la Universidad. (11 de 03 de 2018). Obtenido de UNAM-CERT: https://www.seguridad.unam.mx/servicios

Sleuthkit. (25 de 03 de 2018). *Open Source Digital Forensics*. Obtenido de https://www.sleuthkit.org/

strings(1) - Linux man page. (25 de 05 de 2018). Obtenido de https://linux.die.net/man/1/strings

Threatsaurus. (20 de 05 de 2018). *SOPHOS*. Obtenido de https://www.sophos.com/en-us/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf?la=en

Zamboni, D. (10 de 03 de 2018). *Proyecto UNAM/Cray de Seguridad en el Sistema Operativo Unix*. Obtenido de http://132.248.67.3:8991/cgi-bin/multibase/frames.pl

Anexos

Anexo 1. Obtención de dirección IP de páginas phishing

a) Por plug-in en el navegador.

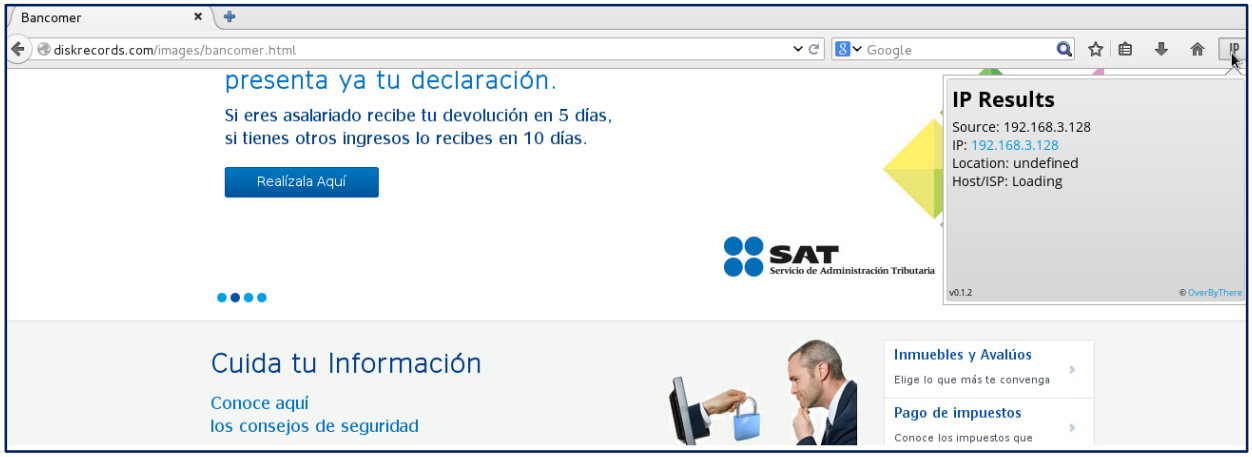

Figura 41. Plug-in en navegador para obtener dirección IP. Fuente: elaboración propia.

b) Herramientas DNSlookup en línea, página *http://whois.domaintools.com/*:

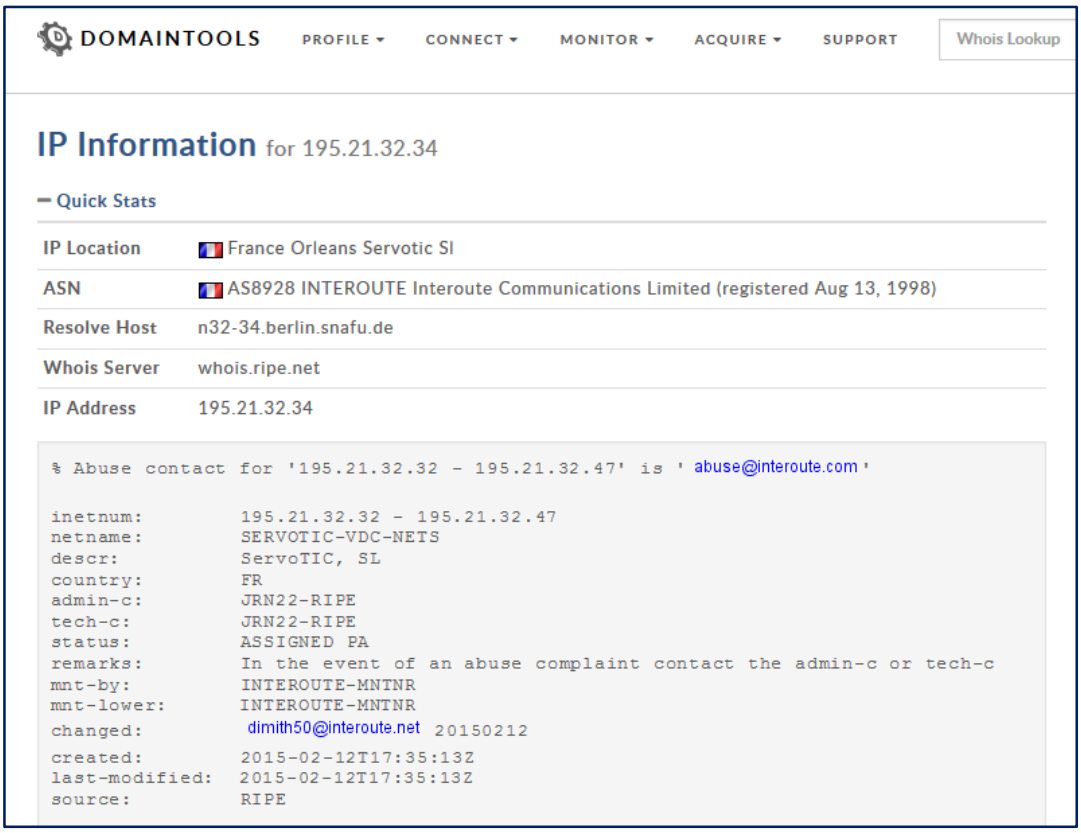

Figura 42. DOMAINTOOLS herramienta DNSLookup en linea. Fuente: http://whois.domaintools.com/

c) Salida de comando **whois:**

```
OrgName:        New Dream Network, LLC
OrgId:          NDN
Address:        417 Associated Rd.
Address:        PMB #257
City:           Brea
StateProv:      CA
PostalCode:     92821
Country:        US
RegDate:        2001-04-17
Updated:        2015-09-07
Comment:        Address location was created regardless of geographic location.
Ref:            http://whois.arin.net/rest/org/NDN


OrgNOCHandle: NETOP274-ARIN
OrgNOCName:   NetOPs
OrgNOCPhone:  +1-714-706-4182
OrgNOCEmail:  netops@dreamhost.com
OrgNOCRef:    http://whois.arin.net/rest/poc/NETOP274-ARIN

OrgAbuseHandle: DAT5-ARIN
OrgAbuseName:   DreamHost Abuse Team
OrgAbusePhone:  +1-714-706-4182
OrgAbuseEmail:  abuse@dreamhost.com
```

Figura 43. Salida de comando whois. Fuente: elaboración propia.

Anexo 2. Ejemplo de Formato de recolección de evidencia

FORMATO DE RECOLECCIÓN DE EVIDENCIA

	Fecha y hora
	21.04.15 23:17
	Número de caso
	GYFJHM458
	Nombre del responsable del equipo
	Isaac Mendoza.
	Nombre del responsable de toma de Evidencia. Analista Forense.
	Nayely Morales Perales
	Descripción del dispositivo
	Sistema Operativo: Debian 7
	Sistema de Archivos: ext4
	Capacidad: 21 GB
	Modelo: HP2147G8

Número de Serie: 1474836480
Md5 evidencia: 81f51533b559138680696d2e5ce8b88
Etiqueta del disco o imagen: discoSC

CSIRT-BECSEG informa que la toma de esta evidencia tiene como objetivo realizar el análisis forense, los hallazgos encontrados serán enviados al responsable del equipo mediante un reporte. La información manejada durante este proceso se mantendrá en absoluta confidencialidad.

Responsable del Equipo

Analista forense.