ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"IMPLEMENTACIÓN DE UNA HERRAMIENTA HONEYPOT PARA DETECCIÓN Y RESPUESTA A ATAQUES."

EXAMEN DE GRADO (COMPLEXIVO)

Previo a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

YURY LISSETTE AVILÉS BAJAÑA

GUAYAQUIL – ECUADOR

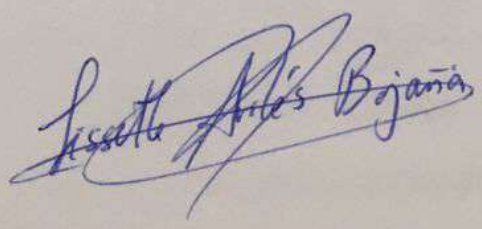
AÑO: 2016

AGRADECIMIENTO

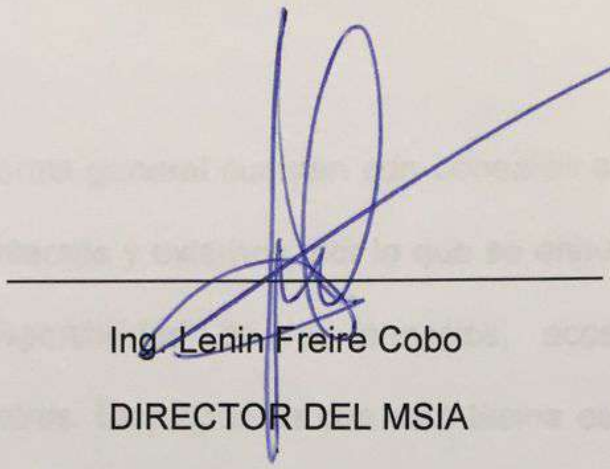
Gracias a Dios, a mis padres, familiares, compañeros y amigos por su apoyo en el desarrollo de esta tesis. Agradezco también a los maestros por sus enseñanzas e inspiración para poder seguir motivando a la adquisición de conocimientos y hacer que todo se vea más sencillo.

DEDICATORIA

La presente tesis es dedicada a mi familia, amigos cercanos que me apoyaron con su tiempo y equipos. En especial a mi padre que en paz descanse Colón Olmedo Avilés, madre Lucia Bajaña y entre mis amigos Stefanía Pazmiño, mis familiares como hermanos Karina Avilés y cuñado Raúl Orellana; Luis Avilés y cuñada Mónica Rodríguez.

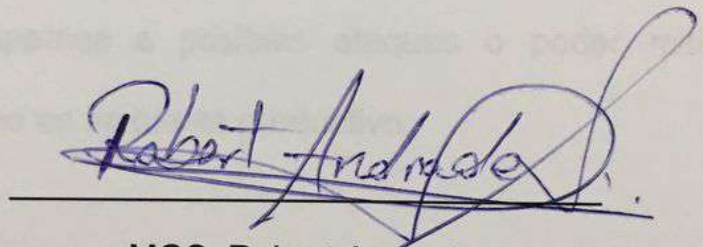


TRIBUNAL DE SUSTENTACIÓN



Ing. Lenin Freire Cobo

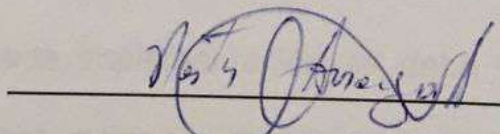
DIRECTOR DEL MSIA



MGS. Robert Andrade

PROFESOR DELEGADO POR

LA UNIDAD ACADÉMICA



MGS. Néstor Arreaga

PROFESOR DELEGADO POR

LA UNIDAD ACADÉMICA

RESUMEN

Las empresas de forma general cuentan con conexión a Internet, y brindan diversos servicios internos y externos, por lo que se encuentran expuestos a ataques en la disponibilidad de los servicios, acceso a información confidencial, entre otros. La propuesta con esta tesina es la implementación e investigación del tema de honeypots para lograr tener una herramienta que nos permita anticiparnos a posibles ataques o poder mitigar mejor la ocurrencia de alguno en ambiente productivo.

Para el desarrollo de esta tesina se ha investigado la definición y funcionamiento de los honeypots, ventajas y desventajas, el rol de los mismos en la seguridad total, la clasificación de los mismos. Para poder realizar una adecuada implementación se debe tener claro lo que desea hacer con el honeypot, elegir alguna solución, nivel de interacción, comercial o versión hecha por la misma empresa, cuantos honeypots se utilizara. Así mismo indicar en qué ubicación se colocara. Vamos también a determinar la clase de datos y cantidad de datos a capturar e identificar los riesgos a los que se expone la organización y definir los pasos para su mitigación.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Todo equipo con conexión a Internet es un objetivo para los hackers o atacantes al día de hoy aunque realmente no tengamos la suficiente conciencia de la ocurrencia de aquello pensando que nuestra información no es valiosa bueno en el caso de las empresas conocen que un activo valioso es la información. De forma tradicional, la seguridad ha sido defensiva o reactiva. Los honeypots cambian este esquema. Existe una tecnología que permite que se tome la ofensiva adelantándonos a las acciones recibidas.

En este apartado se comentara lo que es un honeypot, como funciona y el valor que representa para la organización. El objetivo de este escrito es dar a conocer el mejor empleo de la solución honeypot para una empresa grande una multinacional que maneja su información confidencial, se tratará también las ventajas y desventajas. Se revisara también el empleo y mantenimiento del honeypot. La idea es aumentar el conocimiento y habilidades para dar seguimiento a los hackers.

Finalmente, al aumentar el conocimiento respecto de honeypots no solo logramos tener indicios de ataques y forma de los mismos sino que logramos mejorar la seguridad en general de nuestra organización. Un honeypot es muy diferente de los mecanismos de seguridad tradicionales. Se trata de un recurso de seguridad que está siendo probado, atacado o comprometido. En la empresa en que laboro se recibe con cierta frecuencia comunicados o informes de actividades maliciosas hacia honeypots de ahí surge el interés por revisar este tema de seguridad que se nota afecta a diversidad de usuarios de la Internet.

Poco se sabía acerca de cómo actúan los hackers actualmente ya existen cursos y más información acerca del mundo de hacking sin embargo mediante esta herramienta se lograría captar incluso ataques de día cero. De forma regular, el hacker siempre tuvo la iniciativa, eligiendo a quien atacar, cómo, cuándo y dónde. Por otro lado, los encargados de la seguridad restaban utilizar medidas de seguridad y detectar cuando estas medidas fallaban en su propósito. Esto es una limitante en la forma en que la organización enfrenta a los cyberataques.

Inicialmente se desarrollan herramientas como DTK o cyberCop ambos están limitados en el punto de que emulan servicios y el atacante no encuentra un sistema real contra el cual pueda realmente interactuar. Tener en cuenta que para implementar un honeypot debemos tener un sólido conocimiento de una variedad de tecnologías [1]. El tema de los honeypots se trata hace quince años aproximadamente pero debido a malos entendidos acerca de su concepto e implementación da como consecuencia que pocos se hayan atrevido a utilizar este tipo de mecanismo de seguridad. Muchas personas imaginan que su atacante al descubrir el honeypot puede tomar represalias contra la organización y también que su implementación requiere mucho trabajo. Así mismo si en caso el honeypot es mal configurado podría volverse en su contra dando un acceso a la red real o de producción.[1]

CAPÍTULO 1

GENERALIDADES

1.1 DESCRIPCIÓN DEL PROBLEMA

Como se ha mencionado antes todos los equipos conectados a Internet son susceptibles de ataque por lo que hace conveniente conocer cómo trabajan los atacantes y sus motivaciones para poder tener una mejor valoración del honeypot. Así mismo acorde con el atacante identificado y nuestro objetivo a proteger podremos definir el tipo de solución a aplicar para lograr el objetivo de proteger y detectar las intrusiones a nuestro sistema.

Tenemos entonces dos tipos de atacantes identificados: aquellos que aprovechan la oportunidad, se les suele llamar script kiddies, estos individuos buscan atacar la mayor cantidad de equipos sin importar si es un usuario promedio o una gran empresa, utilizan script ya probados, son poco sofisticados. De este tipo de ataques son la mayoría que se detectan al día de hoy.

Y por otro lado, están los ataques dirigidos los cuales suelen estar patrocinados ya sea por terrorismo o nacionalismo. En estos ataques es difícil poder darse cuenta del ataque recibido ya que son hackers de alto nivel de habilidades por lo que su experiencia también da para que se ocupen de no dejar huellas de las acciones realizadas en el sistema.

Se puede llegar a tener el mal concepto de que porque se utiliza direcciones dinámicas nadie podrá encontrarnos o atacarnos mientras estamos conectados. El atacante podría utilizar los equipos comprometidos como bots, para atacar otros equipos y no ser

descubierto, o el almacenamiento de datos de tarjetas de créditos robadas.

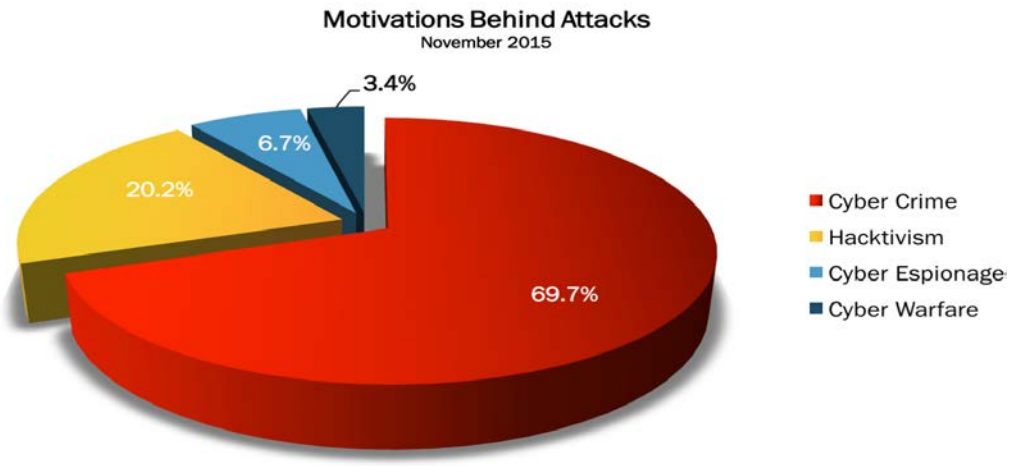


Figura 1 Motivos detrás de ataques a nov 2015[4]

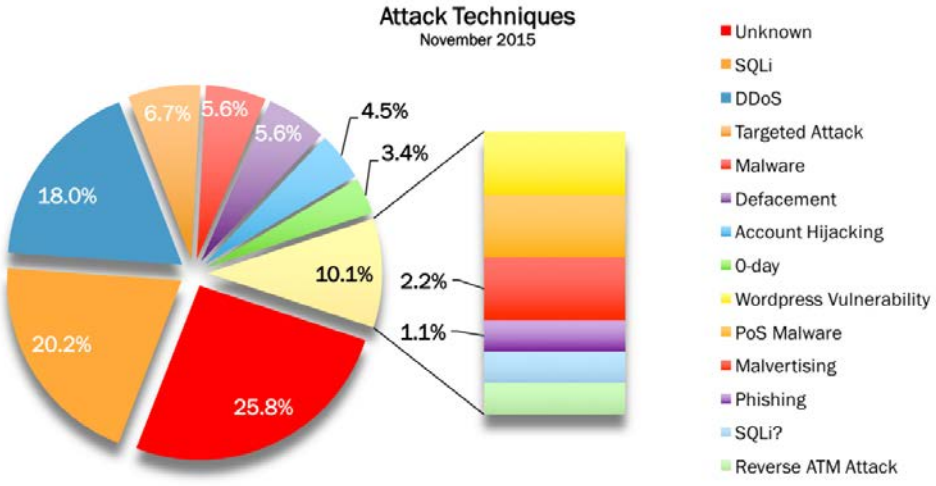


Figura 2 Tecnicas de ataques a nov 2015[4]

Fuente: HACKMAGEDDON Information Security Timelines and Statistics[4]

Como se puede verificar en las técnicas de ataques la mayor cuota es ataque desconocido. Actualmente no se requieren grandes habilidades para realizar ataques, solo se descarga herramientas de internet para que realicen el ataque.

A nivel organizacional se ha conocido eventos en los que no se tiene funcionalidad del servicio de correo como este tema se maneja en otras áreas las mismas que no revelarían la causa de que la afectación de servicio se deba a un ataque de red. Los scripts kiddie es un conjunto amplio de los atacantes pero sin embargo los más peligrosos en la organización serian los ataque dirigidos ya que estos no hacen alarde de sus logros y pueden estar días, meses e incluso años sin ser detectados haciendo uso de cuentas de usuario, y accediendo a recursos críticos.[1]

Los ataques sofisticados muchas veces son difíciles de detectar por los varios saltos entre naciones que realiza el hacker experimentado. En el contexto de empresas que se manejan con promociones diferenciadas podría

haber algún filtro de la información sensible como es nuevos productos que podrían llegar a la competencia antes que al cliente final.[1]

Entre algunos eventos que se ha conocido, denegación de servicio de correo, problemas de accesos al servicio de telefonía por red interna. El uso de encriptación en los ataques con lo cual el administrador de red no puede monitorear el trafico a nivel de red y la modificación a nivel de kernel haciendo que el sistema mienta al administrador acerca del estado real del equipo. Los sistemas deben ser validados fuera de línea y comprobados por un sistema confiable para ser validos.

1.2 SOLUCION PROPUESTA

La solución propuesta es la revisión de la implementación de un honeypot tipo ManTrap, el cual es un recurso de seguridad quien será probado, atacado y comprometido. Este honeypot no tendrá valor a nivel de servicios en producción, de modo que nadie debería estar interactuando con el honeypot.[1]

En el caso de que algún servicio sea vulnerado como pudiera ser el correo al momento en que tenemos un servicio de correo honeypot que puede sufrir también este ataque al estar expuesto se puede recolectar información de la actividad realizada. El tener el honeypot no hará que nos ataquen sino más bien poder tener información detalles de lo que se realizo en el equipo. Se realiza el análisis en paralelo a fin de no afectar servicios que no pueden estar afectados por ser vitales en funcionamiento organizacional.

Se conoce que existen dos posibles usos al honeypot: de producción y de investigación. El honeypot de producción lo usaremos para proteger la organización mientras que el honeypot de investigación se utiliza por aprendizaje. [1][5]

Nuestro honeypot seria de producción lo que agregara valor a la seguridad y ayudara a mitigar el riesgo. Al realizar la implementación de honeypot no se solventara un problema especifico más bien se trata de una contribución a la arquitectura de seguridad total. El valor que tenga

nuestro honeypot dependerá en gran parte de la forma en que se construya, la implementación y el uso que se le dé.[1]

Se tratara las ventajas y desventajas del honeypot Mantrap [1].

Con el honeypot obtendremos los siguientes beneficios asociados:

El **valor de los datos** recolectados, en las empresas se recolecta gran cantidad de información al orden de Gigabyte pero estos son positivos y falsos positivos, por lo que requieren de alguien que los pueda interpretar, por otro lado el honeypot no tiene falsos positivos ya que como no está en producción nadie debería interactuar de modo que cualquier interacción es sospechosa siendo un escaneo, un sondeo o ataque de información de alto valor. La menor cantidad de información lo vuelve más fácil de cotejar. [6][1]

Bajo el escenario de que el atacante está intentando validar que servicios están activos bajo un barrido de ping con puertos aleatorios altos para no ser detectado por el IDS, en este caso realizara interacción con el honeypot y se notara claramente el barrido de ping o el escaneo que se está realizando a la red. Cuando la empresa colecta gran cantidad de

datos puede pasar por alto este tipo de evento debido a que el atacante usualmente enmascara su IP y varía el puerto de conexión.

A nivel de **recursos** utilizados para su implementación no se requiere que sea la última tecnología o una cantidad de memoria exorbitante, podría ser un computador que ya no se tiene en uso. Sin embargo, otros equipos si podrían llegar a saturarse por el manejo de la información que cursan.

Esta solución aporta **simplicidad** ya que lo único que se requiere es tomar el equipo honeypot, ubicarlo en algún lugar en la organización y esperar a que detecte interacción alguna. Con la complejidad suelen venir las caídas, malas configuraciones y fallos.

El **retorno de inversión** con los honeypots es evidente al tener los datos de los ataques, no así cuando se utiliza el firewall, encriptamiento y claves fuertes en los cuales se los aplican y entonces no se tiene ataques debido a su apoyo, pero para que sea evidente al personal de

administración estos elementos y acciones tendrían que no estar en uso para poder notar su eficacia.

Como se mencionó antes los honeypots no son una solución de seguridad más bien una herramienta de apoyo, algunas **desventajas** del uso de honeypots:

Tiene **limitado el campo de visión**, es decir solo capturara datos del dispositivo que interactúe con él, no se puede capturar datos de otro punto de la estructura que pudiera ser afectado por otro ataque.[6]

Puede ser **reconocido** o **detectado** (**fingerprinting**), otra desventaja que tiene es que tienen un comportamiento esperado por lo que podría ser detectado por el atacante, puede haber ciertas inconsistencias que pudieran delatar al sistema honeypot como estar emulando plataforma Windows pero tener a la vez características como de un servidor Solaris. En ningún caso, se desea que sea detectado el honeypot.

El **riesgo** va asociado con el nivel de interacción del atacante con este sistema virtual.

CAPÍTULO 2

IMPLEMENTACIÓN MANTRAP

2.1 CÓMO FUNCIONA MANTRAP

Mantrap funciona con un sólo sistema operativo y crea subcopias lógicas del mismo. Estas subcopias se les llaman celdas y son el sistema con que va a interactuar el atacante. El objetivo es poder asegurar a los intrusos en estas celdas y poder registrar sus acciones. El atacante podría pensar que esta en un sistema real dada su funcionalidad. Ninguna celda tiene conocimiento de la otra, así como del sistema host.[1].

Sistema Operativo Host			
Celda 1	Celda 2	Celda 3	Celda 4

Tabla 1 Un Mantrap host con cuatro celdas lógicas

Mantrap para poder realizar esto realiza modificaciones a dos componentes del sistema operativo: el funcionamiento del kernel y el sistema de archivos.

Ajustes al Kernel:

El kernel se comunica directamente al sistema hardware. Su propósito es el manejo de la infraestructura interna del sistema y así los procesos se pueden enfocar en su objetivo. Los procesos y actividades que interactúan con el kernel ocurren en el espacio del usuario. Esto significa que como usuarios ejecutamos un proceso o comando, esto es en el espacio del usuario. Es como casi todas las aplicaciones del sistema las cuales ocurren en el espacio del usuario como son: servidor web, servidor de correo o el servicio DNS y estas interactúan con el kernel. Otros comandos de unix como ls (1) o ps (1) ellos también interactúan con el kernel. Se crean subdivisiones dentro del kernel, creando el ambiente de celda, el hecho de compartir el kernel habilita

a ManTrap en sus capacidades de captura de datos. El sistema host puede capturar la actividad de cada proceso y usuario sobre la celda. Esto se efectúa con llamadas al kernel con procesos como *open()* o *exec(), y* procesa la actividad dentro de las celdas. Toda actividad es grabada en el kernel desde el momento en que accede a la celda. Al bajo nivel del kernel no es tan sencillo esconder las acciones del hacker. Tomar en cuenta, el caso de la conexión SSH la cual es encriptada pero si esto es realizado en la celda será grabado debido a que la encriptación que se realiza es a nivel de usuario y no al kernel.

Manejo del sistema de Archivos en ManTrap.

El sistema de archivos no es compartido con las celdas. Cada celda tiene su propia copia del sistema de archivos. De esta forma cuando el atacante se encuentra en la celda y realiza copia de archivos o alguna modificación esto afecta únicamente a dicha celda.

ManTrap opera en el principio similar a forensia con loopback. Durante la instalación, se crea una imagen de cada partición del nuevo sistema

instalado. Cada celda toma la imagen y la monta, creando su sistema de archivos. Cuando nuestro atacante interactúa con el sistema lo está haciendo con un archivo.

A continuación Figura 3 desde el sistema host se puede identificar en negrillas el sistema de archivos asociado a la celda 1 que no es más que una copia de la imagen del archivo host sin incluir obviamente el software ManTrap.

```
mantrap #df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/dev/dsk/c0t0d0s0    19248745 11537202 7519056    61%    /
/proc                       0        0       0     0%    /proc
fd                          0        0       0     0%    /dev/fd
mnttab                      0        0       0     0%    /etc/mnttab
/dev/dsk/c0t0d0s1       96455     7595   79215     9%    /var
swap                   400544        0  400544     0%    /var/run
swap                   400552        8  400544     1%    /tmp
/dev/fbk0             1406026    46889 1218535     4%    /usr/rti/cage1/root
/dev/fbk1             2812324   656997 1874095    26%    /usr/rti/cage1/root/usr
/dev/fbk2               93583     7512   76713     9%    /usr/rti/cage1/root/var
/dev/fbk3             2343558   703760 1405443    34%    /usr/rti/cage2/root
/dev/fbk4               93583     7401   76824     9%    /usr/rti/cage2/root/var
/dev/fbk5             1874792   703814  983499    42%    /usr/rti/cage3/root
/dev/fbk6             1406026      553 1264871     1%    /usr/rti/cage3/root/export/
home
/dev/fbk7               93583     7912   76313    10%    /usr/rti/cage3/root/var
/usr/rti/cage1        19248745 11537202 7519056    61%    /usr/rti/mc1
/proc                       0        0       0     0%    /usr/rti/mc1/root/proc
/usr/rti/cage2        19248745 11537202 7519056    61%    /usr/rti/mc2
/proc                       0        0       0     0%    /usr/rti/mc2/root/proc
/usr/rti/cage3        19248745 11537202 7519056    61%    /usr/rti/mc3
/proc                       0        0       0     0%    /usr/rti/mc3/root/proc
```

Figura 3 Sistema de archivos de cada celda

De esta forma Figura 2.2 luce el sistema de archivos que vera el atacante en la celda 1.

```
cage-1 $df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/proc                      0       0       0     0%    /proc
/dev/dsk/c0t0d0s0    1406026   46890 1218534     4%    /
/dev/dsk/c0t0d0s6    2812324  656997 1874095    26%    /usr
/dev/dsk/c0t0d0s1      93583    7608   76617    10%    /var
```

Figura 4Sistemas de archivos de celda 1

Las limitaciones y las celdas resultantes.

El resultado de las celdas es un ambiente operativo lógico que parece ser un sistema operante, el sistema cuenta con 5 interfaces de red una por cada celda y la celda solo puede observar su propia interfaz.

Las limitaciones que presentan las celdas es que no se pueden insertar módulos kernel ya que este se puede llevar a cabo únicamente en el sistema host real. Ahora siempre se tiene el riesgo de que el atacante identifique que se encuentra en una celda, pueda obtener privilegios de súper usuario dentro del ambiente celda, y pueda acceder a la memoria, disco duro real e

identificar la naturaleza del ambiente. Esto dependerá de las habilidades del hacker.[1]

2.2 INSTALACIÓN Y CONFIGURACIÓN DE MANTRAP

Para la instalación, se requiere conocer del sistema operativo base que es Solaris. Se tiene que conocer los requerimientos de hardware. [2]

Vamos a necesitar un sistema que soporte las múltiples celdas y su actividad. De lo investigado, el software ManTrap fue adquirido por Symantec quien lo denomina luego como Symantec Decoy Server.

Requerimiento de Host

Solaris 7 SPARC™ con distribución completa y que soporte OEM, parchado al 106541-04 o superior

Solaris 7 Intel® con distribución full, parchado al 106542-04 o superior

Solaris 8 (SPARC or Intel) 10/01 HCL o superior, con distribución completa y que soporte OEM.

Consola de Administración

• Microsoft® Windows® 98, NT® 4.0 or 2000

• Solaris 7 or 8/Intel or SPARC

• Java™ Runtime Environment 1.3.1

2.3 CONSTRUCCIÓN DEL SISTEMA HOST

Para la construcción del sistema Host se toma nuevamente información de la fuente bibliográfica [1] en que se debe instalar el sistema solaris con la instalación más larga posible que es la Developer Plus OEM, requiriendo todos los paquetes. No se soporta versiones minimizadas.

Después de que hemos instalado, debemos fijarnos que a cada interfaz se le haya asignado una MAC diferente porque esto nos podría dar conflictos con el software Mantrap, esto debe tenerse en cuenta ya que solaris por defecto pondrá la misma mac a todas las interfaces.[1]

Para esto se usa el comando:

Host# eeprom local-mac-address?=true

iButton y Opciones de Configuración

Existe un componente llamado iButton, es el componente físico que se conecta a la caja física. Por medio de este elemento las celdas podrán tener estampas de tiempo, autenticación de los datos de login y licencias de celdas.

En la figura siguiente se podrá ver el menú de configuración para identificar clave del sistema, número de celdas y la ubicación de recursos específicos.

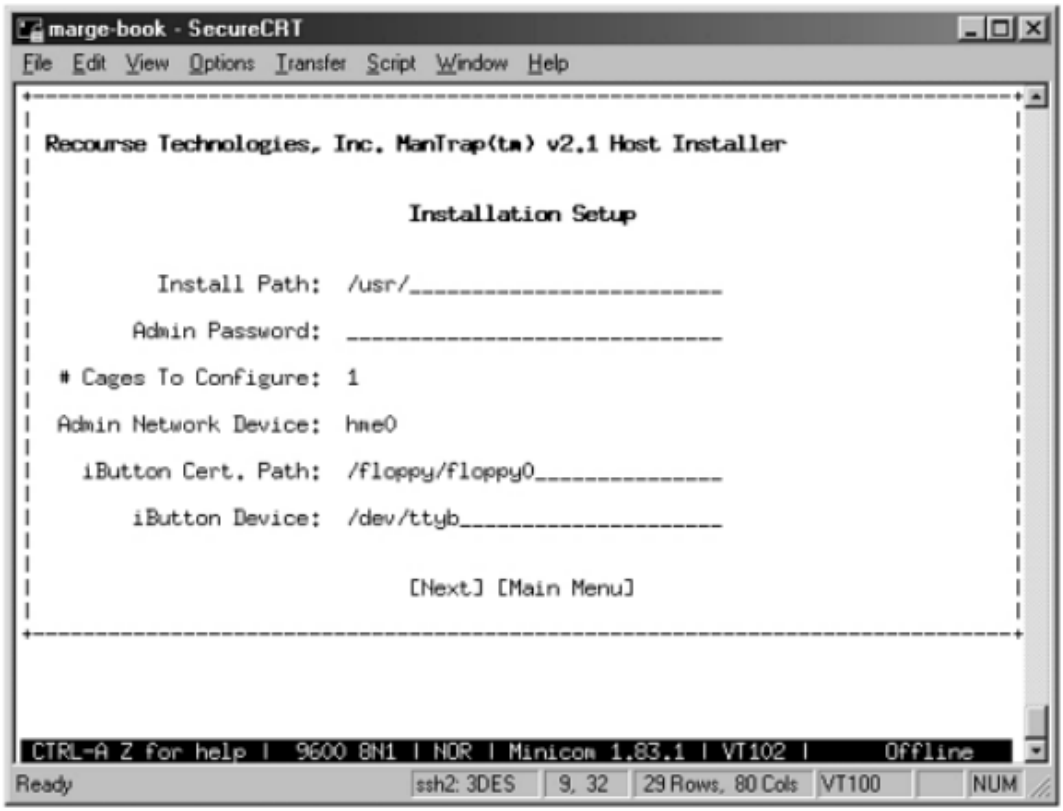


Figura 5 Menú de configuración

Mantrap cuenta con una sola caracteristica es el CGM(Content Generation Modules) este se va implementando durante la instalacion. Con esta caracteristica lograremos generar contenido diferente para cada celda, ya que debemos recordar que si no los personalizamos unicamente tendremos instalacion estándar por defecto del sistema Host. Incluso se tiene plantillas según lo que aplique a nuestra organización. [1]

2.4 ADMINISTRACIÓN DEL CLIENTE

La administración del cliente es remota. Es un sistema separado, la interfaz que comunica el cliente directamente con el Host en la red. Por medio del sistema se puede administrar las cuatro celdas. El cliente está basado en Java, por esto mismo funciona en cualquier plataforma que soporte Java.[1]

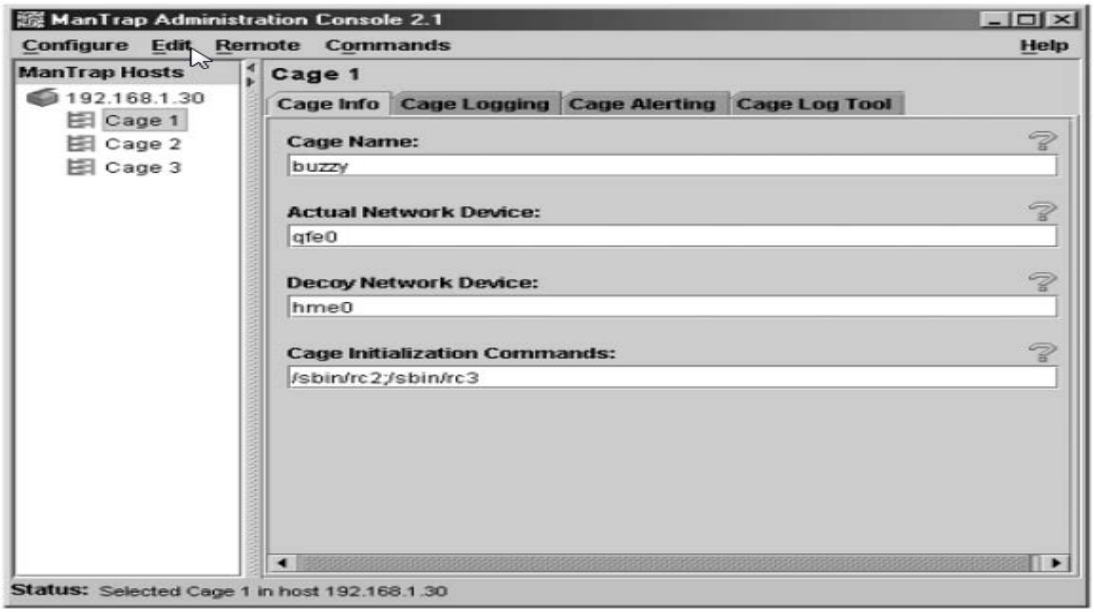


Figura 6 Interface de Mantrap para configurar registros y alertas en las celdas

2.5 IMPLEMENTACIÓN Y USO DEL MANTRAP

Al implementar Mantrap tenemos dos elementos lo que son el sistema host y las celdas. El host es donde se encuentra físicamente el equipo o PC. Y las celdas en cambio son lógicas y estas se ubicaran lógicamente

en algún punto de la red. Las celdas tienen su propia tarjeta de red con las cuales se pueden conectar a la red. Se debe determinar la arquitectura sobre la cual estarán las celdas.

Para la implantación de las celdas debemos tener claro lo que deseamos obtener de las mismas. Por ejemplo: Tenemos conocimiento que se ha recibido ataques a la granja de servidores web, los cuales están ubicados en una red separada del firewall. Quisiéramos determinar cuándo un intruso está haciendo pruebas de reconocimiento o escaneo para atacar nuestro servicio Web. Para este caso, tendríamos que colocar las celdas dentro de la granja de servidores. De esta forma, Mantrap nos servirá como honeypot para la investigación del evento suscitado con la cual detectamos y analizamos nuevas tendencias de ataques. Cada celda está conectada a la red y cada elemento se haría pasar por un servidor web de la granja.

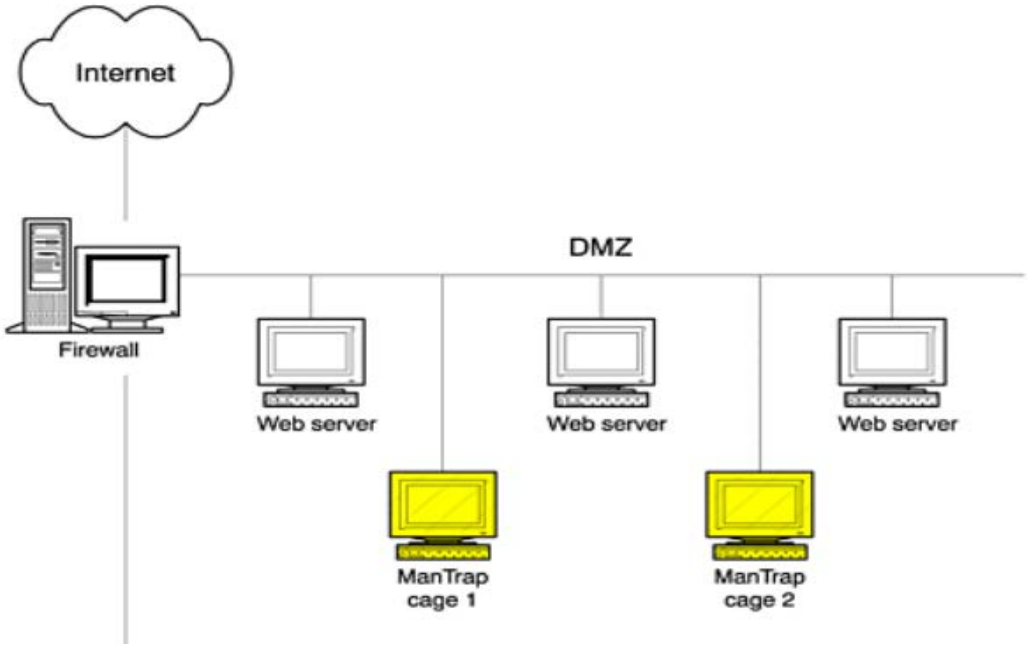


Figura 7 Implementando las ubicaciones para dos celdas dentro de la granja de servidores con el fin de detectar y responder ataques

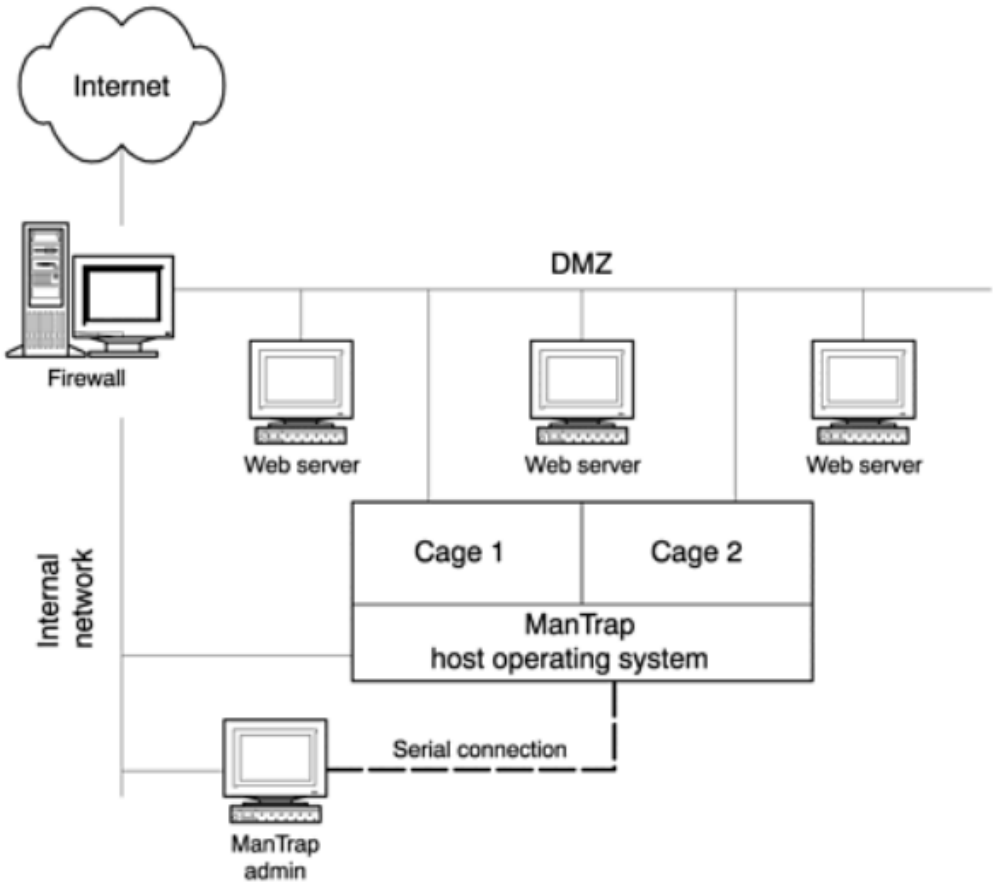


Figura 8 Implementación actual del honeypot que incluye el sistema Host y la administración remota

2.6 INTEGRACIÓN CON SYMANTEC DECOY SERVER

Esta integración se la realiza con Symantec Network Security y al configurarlo podremos recibir eventos desde ManTrap 2.1 y posteriores como Decoy Server 3.1. [3].

Para **integrar eventos del Symantec Decoy Server** dentro de Symantec Network Security.

1. ***Configurar alertas*** de respuesta a políticas para celdas del Symantec Decoy Server. Basándose en dichas alertas, SDS (Symantec Decoy Server) enviara eventos a SNS y estos eventos aparecen en la consola del SNS (Symantec Network Security). Por ejemplo: en una celda se configura enviar todos los eventos de *Root User Exec* y *Opened for Writing* a la consola de Seguridad.
2. En la consola de NS (Network Security), **creamos un nodo sensor externo para cada dirección IP por la cual enviaremos datos al SNS,** el que es un nodo separado por cada celda y host.
3. **Aplicar políticas de respuesta en SNS para el SDS**

   Esta opción está disponible para administradores.

Iniciar desde una nueva ubicación.

Para aperturar la consola del SDS desde una nueva ubicación.

1. Clic derecho en algún objeto sensor externo en su topología y clic en Start Decoy Console.
2. La primera vez aparece un mensaje de Decoy Console Not Found, dar OK.
3. En Select the Symantec Decoy Server Console Directory, navegar al directorio que contiene *mtadmin.jar,* y dar clic en Open

El archivo es normalmente ubicado en Program Files\Symantec\Mantrap

4. En Start Decoy Console, clic Yes para confirmar la ruta al archive jar. Después de iniciar la consola del SDS desde la nueva ubicación, la ubicación del archivo del *mtadmin.jar* es almacenada en memoria.

Iniciar desde una ubicación conocida.

Para iniciar la consola del SDS desde una ubicación conocida.

1. Clic derecho en algún objeto sensor en la topología y clic en Start Decoy Console.
2. En Start Decoy Console, clic Yes para confirmar la ruta del archivo *mtadmin.jar.*

La consola del SDS es independiente del cierre de la consola de NS.

CAPÍTULO 3

ANÁLISIS DE LOS RESULTADOS

3.1 CAPTURA DE DATOS EN PRÁCTICA

Por los métodos de captura de datos de información que tiene Mantrap se convierte en una tecnología poderosa. Para poder entender mejor esto, se revisara un ataque capturado por ManTrap. [1]

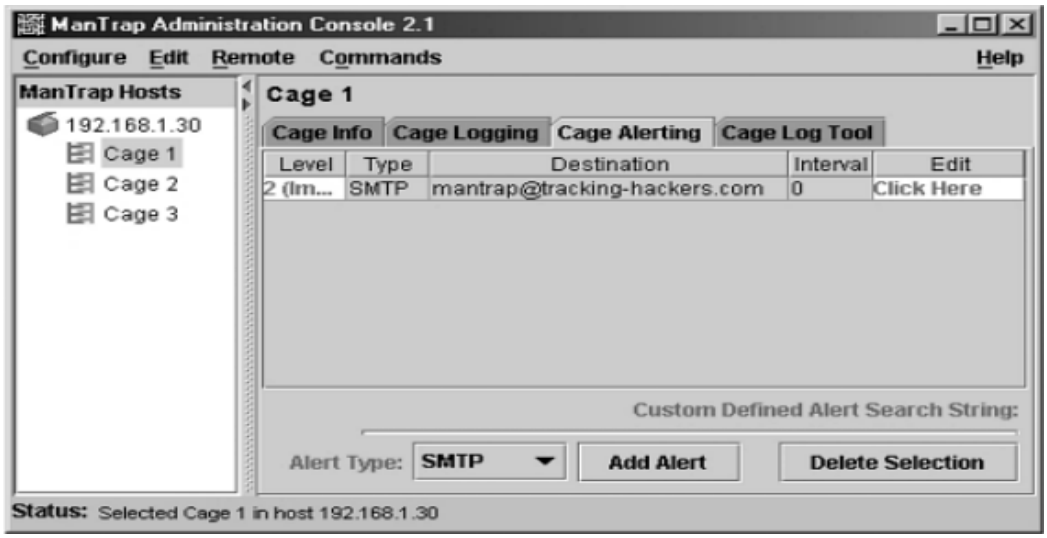


Figura 9 Consola de administración configurada para activar alertas

3.2 DISMINUCIÓN DE INCIDENTES

Con la prevención se optimiza la cantidad de incidentes recibidos. Se anticipa a las acciones de los atacantes que interactúan con los equipos honeypot.

3.3 VALIDACIONES DE MECANISMOS DE SEGURIDAD

Como las celdas o señuelos para los atacantes manejan configuración similar podemos prevenir alguna mala configuración a dichos servicios. Se valida los mecanismos de seguridad al detectar los ataques que se intentan realizar hacia los servicios internos y expuestos.

3.4 LIMITACIONES.

Entre las limitaciones para el honeypot elegido es que solo funciona con solaris. Es de costo, por lo que va orientado a organización multinacional de gran infraestructura para validar el costo beneficio.

El acceso saliente es un riesgo en los honeypot de alta interacción. En el supuesto que nuestra configuración sea débil es decir fácil de quebrantar su seguridad y el hacker logre darse cuenta de la celda y realizar denegaciones de servicio, o incluso atacar otros sistemas. Este riesgo puede ser mitigado mediante el firewall con políticas hacia el tráfico entrante y saliente a través del sistema del honeypot, se permite cualquier tráfico entrante no así el saliente.

CONCLUSIONES Y RECOMENDACIONES

1. Se concluye que los honeypots son herramientas de apoyo a la seguridad, no sustituye al firewall o buenas políticas de seguridad. El ámbito de acción del honeypot está limitado al segmento o ambiente de producción donde fue implementado.

2. La efectividad del honeypots va por la forma de su implementación, uso y hasta configuración del mismo.

BIBLIOGRAFÍA

[1]Honeypots: Tracking Hackers By Lance Spitzner Publisher: Addison Wesley Pub Date: September 13, 2002 ISBN: 0-321-10895-7

[2]http://www.taarak.com/solintrusion.html, fecha de consulta 11 de enero de 2016

[3]http://www.manualslib.com/manual/595268/Symantec-10521146-Network-Security-7120.html?page=286#manual, fecha de consulta 12 de enero de 2016

[4]http://www.hackmageddon.com/2015/12/11/november-2015-cyber-attacks-statistics/

[5] http://www.cybsec.com/upload/ESPE_Honeypots.pdf

[6] http://web.archive.org/web/20080202010804/http://www.linux.com/articles/39244, fecha de consulta 10 de enero de 2016