CAPACIDADES TECNICAS, LEGALES Y DE GESTION
BLUETEAM Y REDTEAM

ANDERSON SALAZAR ACOSTA

UNIVESIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTA
2020

CAPACIDADES TECNICAS, LEGALES Y DE GESTION BLUETEAM Y REDTEAM

ANDERSON SALAZAR ACOSTA

ETAPA CAPACIDADES TECNICAS, LEGALES Y DE GESTION BLUETEAM Y REDTEAM

DIRECTOR DEL CURSO INGENIERO JOHN FREDDY QUINTERO

UNIVESIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
SEMINARIO ESPECIALIZADO: EQUIPOS ESTRATÉGICOS EN CIBERSEGURIDAD: RED TEAM & BLUE TEAM
BOGOTA
2020

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Bogotá, Colombia. Octubre 2020

Dedico este trabajo a mis familiares, allegados y en especial a mi pequeña hija, quien ya está en casa, alegrándonos nuestras vidas.

AGRADECIMIENTOS

Dedico mis agradecimientos a mi hija, la institución, familiares, amigos y tutor de este curso por la oportunidad de adquirir más conocimiento y brindarme las bases necesarias para la identificación de herramientas y metodologías para prevenir ataques de seguridad informática.

CONTENIDO

FIGURAS

GLOSARIO

HARDENIZACION: [1](palabra en inglés que significa endurecimiento) en seguridad informática es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, etc; innecesarios en el sistema; así como cerrando puertos que tampoco estén en uso además de muchas otros métodos y técnicas que veremos durante este pequeño resumen introductorio al Hardening de sistemas.

SIEM: [2]Gestión de Eventos e Información de Seguridad (Security Information and Event Management) es una categoría de software que tiene como objetivo otorgar a las organizaciones información útil sobre potenciales amenazas de seguridad de sus redes críticas de negocio, a través de la estandarización de datos y priorización de amenazas. Esto es posible mediante un análisis centralizado de datos de seguridad, obtenidos desde múltiples sistemas, que incluyen aplicaciones antivirus, firewalls y soluciones de prevención de intrusiones.

Ley 1273: Ley colombiana modificada en el código penal en el año 2009, con el objetivo de recular el amparo de los datos.

Código de Ética: Es un documento donde se establecen las normas y valores, que normalizan actuaciones que hacen parte de diferentes contextos.

COPNIA: Es una entidad pública que vigila, inspecciona y controla el ejercer de las ingenierías sus profesionales y auxiliares en Colombia.

MS17-010: Vulnerabilidad que permite la ejecución de comando a nivel de consola. También realiza la deshabilita el protocolo SMBv1.

SMBv1: Protocolo de red utilizado por computadores con sistema operativo Microsoft Windows, el cual permite compartir archivos.

---

[1] BLOG SMARTKH, GRUPO SMARTEKH, ¿Qué es Hardening ?, Disponible en https://blog .smartekh.com/que-es-hardening.

[2] HELPSYSTEMS, El Blog de HelpSystems, Disponible en https://www.helpsystems.Com/es/ blog /que-es-un-siem.

Kali Linux: sistema operativo con fundamentos en Debian enfocado a la seguridad Informática.

Windows: Sistema operativo que ha venido evolucionado a través de los años, ajustando mejoras a sus sistemas, existen variaciones de este sistema operativo tanto para servicios en el hogar y empresarial.

RESUMEN

En el desarrollo de este trabajo, se realiza el análisis a varios problemas planteados por el tutor del seminario. Donde se hace necesario un levantamiento de información, con el objetivo de identificar herramientas y procedimientos que nos permitan la identificación de ataques en tiempo real que puedan o tengan la intención de realizar procesos de irrupción de nuestros sistemas he identificado el marco normativo vigente para Colombia.

1. INTRODUCCIÓN

En el desarrollo de esta guía, se pretende identificar y dar uso práctico en nuestros entornos de trabajo con Hardening, y la identificación de herramientas que nos permitan prevenir y contener ataques a nuestros sistemas. Permitiendo así poner en práctica los conocimientos adquiridos en este entorno controlado para posteriormente llévenlo a nuestros sistemas en producción. Se hace necesario que para las prácticas aquí desarrolladas las mismas se realizaron en entornos seguros y controlados con el objetivo de mitigar riesgos a plataformas en producción, las maquinas con sistemas operativos Windows que fueron vulneradas mediante ataques a la vulnerabilidad MS17_010 fueron imágenes proporcionadas por nuestro tutor y las mismas aun que tenían el mismo sistema operativo “Windows 7 ” la arquitectura de las mismas si variaban la una con arquitectura x86 y la otra con x64.

En las practicas se utilizaron varias herramientas para logar la vulnerabilidad de las maquinas Windows como NMAP. METASPLOIT, KALI LINUX. Esto con el ánimo de realizar análisis, diagnósticos he implementación de hardening con objetivo de minimizar los riesgos a los que nuestros sistemas están expuestos. Gracias a estas prácticas se pueden realizar diagnósticos que frente a un escenario real generaría una imagen positiva frente al equipo de trabajo y a la compañía que valores la importancia de la información manteniéndola siempre disponible, confiable he integra, ya que son los pilares de la seguridad de la información.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Dar solución a la guía etapa 5 donde se han planteado las siguientes metas a cumplir.

2.2 OBJETIVOS ESPECÍFICOS

I. Identificar aspectos estratégicos de RedTeam & BlueTeam.

II. Planteamiento de estrategias que permitan endurecer los aspectos de seguridad.

3 PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

The WhiteHose Security desea un informe técnico donde se plasme el proceso de los escenarios propuestos en cada una de las acciones como Blue team, Red team y aspectos legales que logró usted como experto en Ciberseguridad dentro del período de prueba de la organización. El informe es solicitado para ser analizado por los analistas Seniors en Seguridad con los que cuenta WhiteHouse Security, esto ayudará al proceso de selección de los expertos que harán parte de esta prestigiosa organización.

3.2 JUSTIFICACIÓN

Cumplir con el informe técnico, nos permite la identificación con claridad las actividades realizadas, las metodologías aplicadas y establecer un plan de acción de mitigación, para posibles ataques que se puedan producir posterior. También permitirá a WhiteHouse Security tener una vista ms clara sobre el perfil del profesión a contratar.

4. MARCO TEÓRICO

Las actividades de pentesting, son un riesgo latente para los entornos tecnológicos bien se en empresas de privadas o del sector gubernamental, lo que ha conllevado a la creación de diferentes grupos, empresas, personas. Con el objetivo de buscar, desarrollar e implementar medidas que minimice los riesgos a los que estamos expuestos en nuestros entornos tecnológicos, bien sean de telecomunicaciones o informáticos esto dado el avance que se tiene día a día en las nuevas metodologías y sistemas que avanzan a grandes pasos. Según informe del ministerio de tecnologías de la información y las comunicaciones, se han logrado para el año 2011 550 ataques exitosos a entidades del estado[3].

Ahora bien, el punto de partida para la implementación de alguna de las herramientas tales como sistemas de gestión para seguridad de la información - SGSI, manuales y políticas de buenas prácticas en seguridad informática, etc., es la realización de un diagnostico que permita conocer el nivel de seguridad informática con que cuenta una entidad u organización, cuáles son sus riesgos asociados y si estos están controlados, además de cuáles son sus posibles amenazas o vulnerabilidades en materia de seguridad informática. Para lo anterior es pertinente la aplicación de metodologías, prácticas o herramientas que permitan establecer estos criterios y tomar las directrices necesarias, relacionadas con el objetivo de proteger la información y OSSTMM, es una de ellas. El Manual de la Metodología Abierta de Testeo de Seguridad u Open Source Security Testing Methodology Manual, es una metodología desarrollada por el Instituto para la Seguridad y Metodologías Abiertas o ISECOM, por sus siglas en inglés (Institute for Security and Open Methodologies), y fue publicada a finales del año 2000, lo cual marcó un hito pues hasta el momento no existían documentos que de manera abierta y estandarizada, agruparan las actividades a tener en cuenta, por parte de un profesional en seguridad informática, a la hora de realizar una evaluación de seguridad[4].

[3] MINTIC. Ministerio de Tecnologías de la Información y las Comunicaciones. Obtenido de Fortalecimiento de la gestión en el estado: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/

[4] DRAGONJAR. Osstmm, Manual de la Metodología Abierta de Teste. Obtenido de Fortalecimiento de la gestión en el estado: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

5. MATERIALES Y MÉTODOS

5.1 MATERIALES

Se realiza consulta a varias fuentes bibliográficas, que estén dedicadas a temas relacionados con ciberseguridad.

5.2 METODOLOGÍA

Aprendizaje basado en Problemas y lecturas

6 ASPECTOS ESTRATEGICOS REDTEAM & BLUETEAM.

6.1 RED TEAM

En los escenarios de seguridad informática, hacen parte fundamental tres equipos de trabajo Purple Team, Red Team y Blue Team. Para el caso de estudio revisaremos los aspectos estratégicos para los grupos REDTEAM & BLUETEAM. Esto dado que son dos grupos fundamentales ya que se complementan entre sí, permitiendo minimizar las amenazas, detectar falos y realizar endurecimiento de los sistemas informáticos.

El equipo de Red Team, en ciertos momentos es interpretado con pentesters, cabe aclarar que no son lo mismo pese a que algunas funciones son muy similares. Dentro de las funciones principales de un equipo Red Team esta:

- Crear ataques de forma controlada dentro de la misma organización con el objetivo de identificar fallas o vulnerabilidades.
- En entornos no productivos emular amenazas a las que puede estar expuesta la compañía, para luego validarlo en los entornos de producción.

Por consiguiente, el equipo de Red Team nos permite identificar y cuantificar el escenario real al cual esta expuesta o protegida la organización.

6.2 BLUE TEAM

Este equipo, ya se encarga de defender de ataques a las empresas o individuos que así lo requieran. Dentro de las funciones realizadas esta:

- Realizar monitoreo, supervisión, análisis de conductas poco comunes dentro de los entornos tecnológicos y del personal.
- Implementan soluciones de forma continua identificando vulnerabilidades, fallas, errores, realizando estudios a las maquinas afectadas.

7 RECOMENDACIONES HARDENIZACION.

Como recomendación para la HARDENIZACION y gracias a la actividad realizada, etapa 4 del desarrollo de este seminario, y según mi concepto frente a lo analizado, propondría las siguientes actividades con el objetivo de realizar el endurecimiento de nuestros aspectos de seguridad. Estas están enfocadas a actividades que no

general ningún tipo de costo en las organizaciones o en nuestros entornos familiares.

1. Mantener Actualización de parches de seguridad, bien sea si se trata de una compañía por medio de un servidor de actualización para que las mismas están centralizadas. Y si es a nivel personal o de hogar permanecer las actualizaciones automáticas activas.
2. Mantener un antivirus activo en nuestro sistema.
3. Bloquear Macros/Scripts de Office.
4. Si es una organización realizar pruebas de PENTESTING a los servicios publicados.
5. Mantener e firewall activo.
6. Como lo propuso Microsoft en su momento, deshabilitar el protocolo SMBv1. “No es la mejor opción, pero funciona”.
7. Instalación de sistemas operativos seguros.
8. Implementación de políticas de contraseñas seguras.
9. Bloqueo de instalación a Software a usuarios no permitidos.
10. Configuración de seguridad a carpetas y archivos. Según perfiles de usuarios.
11. Eliminar configuración por defecto de los equipos.
12. Establecer políticas de seguridad a escritorios remotos.
13. Bloqueos de pantalla por inactividad.
14. Segmentar la red de servidores y de equipos del grupo de trabajo.
15. Establecer un plan de perfilamiento de cuentas de usuario.
16. Bloqueo de trafico de red por MAC de cada equipo en la compañía.
17. Bloqueo de puertos por defecto.
18. Establecer políticas de acceso a servidores Físicos.
19. Establecer un registro o bitácora de ingreso a las áreas de servidores.
20. Encriptar los discos al inicio del sistema operativo.
21. Crear una unidad encriptada en el equipo que no sea C.
22. Bloqueo de usuario no permitidos
23. Bloqueo por más de tres intentos de inicio de sección.

8 INFORME TECNICO

En el siguiente informe se plasman las actividades realizadas tanto como equipo de Blue team y Red team

8.1 INFORME RED TEAM

En los informes técnicos se debe establecer un logo un código y la versión del documento. Para efectos prácticos y entendiendo que los informes deben estar alineados a alguna metodología, para este caso ISO 27001, el siguiente informe utilizara el logo de la Universidad Nacional Abierta y a Distancia – UNAD y sin codificación. Para la codificación solo se dejará el campo.

Se realizan los informes técnicos los cuales se encuentra disponible en el anexo1_ Informe_BlueTeam y anexo2_ Infrome_RedTeam

9 ENLACE VIDEO SEMINARIO

Adjunto link de enlace video Seminario Especializado: Equipos Estratégicos en ciberseguridad: Red Team & Blue Team https://www.youtube.com/watch?v=MCfQBebZUHg

10 CRONOGRAMA

Cronograma de actividades Etapa 5

Figura 4. Cronograma de Actividades

CONCLUSIONES

Tener conocimiento de las fallas a las que estamos expuestos nos permite, una toma de decisiones de una forma oportuna con el objetivo de mitigar y garantizar la continuidad del negocio. También nos deja identificar que un sistema actualizado, mitiga las vulnerabilidades a los que se encuentre expuesto.

RECOMENDACIONES

Mantener las versiones de nuestros sistemas operativos en especial la plataforma Windows con sus parches y actualizaciones al día, junto con su sistema de antivirus ahí que recordar que Windows ya trae un antivirus preconfigurado. Mantener el firewalll activo he implementar políticas de seguridad de la información o sistema SGSI es importante ya que nos permite robustecer nuestro entorno informático.

BIBLIOGRAFÍA

Helpsystems, Que es un SIEM, 04 octubre de 2020, Disponible en https://www.Helpsystems.com /es/blog/que-es-un-siem

UNIRRESVISTA, Fundación Unir Universidad Internacional de la Rioja, Red Team, Blue TEam y Purpuple Team, ¿Cuáles son sus funciones y diferencias, 07 de enero 2020, Disponible en https://www.unir.net/ingenieria/revista/noticias/red-blue-purple-team-ciberseguridad/549204773062/?

MINTIC. Ministerio de Tecnologías de la Información y las Comunicaciones. Obtenido de Fortalecimiento de la gestión en el estado: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/

DRAGONJAR. Osstmm, Manual de la Metodología Abierta de Teste. Obtenido de Fortalecimiento de la gestión en el estado: https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

COPNIA, CONSEJO PROFESIONAL NACIOAL DE INGENIERIA, Código de ética, 28 de agosto 2020. Disponible en https://copnia .gov.co/sites /default /files/ uploads /codigo _etica.pdf

OAS, MARCO JURIDICO. Disponible en https://www.oas.org/juridico /english/cyb _pry_ convenio.pdf

MINTIC, POLITICAS GENERALES, Disponible en https://www.mintic. Gov .co/ gestionti /615/articles-5482_G2_Politica_General.pdf

MINTIC, LEY 1273, Disponible en https://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

MINTIC, DECRETO 1377, Disponible en https://www.mintic.gov.co/portal/604/articles-4274_documento.pdf

UEES, VILMA KARINA ALVAREZ INTRIAGO, Propuesta de una metodología de pruebas de penetración orientada a riesgos, 28 de agosto 2020 https://pdfs .seman ticscho lar .org/f3be/44039e5f4c1bfced6ad23455291b2a304c77.pdf

UNAD, ALLEN DAVID ZULUAGA MATEUS, HACKING ETICO BASADA EN LA METODOLOGIA ABIERTA DE TESTO DE SEGURIDAD – OSSTMM, APLICADO A LA RAMA JUDICIAL, SECCIONAL ARMENIIA, 28 de agosto 2020

https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/17410/1/94288061.pdf

ALCALDIA MAYOR DE BOGOTA, MARIA DEL PILAR NIÑO CAMPOS, GUARDIANES DE LA INFORMATICA, 28 de agosto 2020, http://ticbog ota. Gov .co/ sites /default /files /seguridad-de-la-informacion/ambito2.pdf

NULLSECTOR, EXPLOTA VULNERABILIDAD ETERNALBLUE CON METASPLOIT. Disponible https://nullsector.co/explotar-vulnerabilidad-eternalblue-con-metasploit/

CREADPAG, ACCESO A WINDOWS 7 CON ETERNALBLUE DESDE METASPLOIT CON KALI LINUX, Disponible en https://www.creadpag.com/2018 /05/acceso-windows-7-con-eternalblue-desde.html

JROLIVA, Juan Oliva, Explotando Vulnerabilidad MS17-010 o WAnnaCry, 25 de septiembre 2020, Disponible en https://jroliva.net/2017/06/01/explotando-vulnerabilidad-wannacry-o-ms17010/#:~:text=Ello%20es%20en%20resumen%2C% 20t%C3 %A9cnica mente,es% 20decir%20existe%20un%20parche

CIS, POWERFUL Best Practices. Disponible https://learn.cisecurity.org/cis-controls-download

Microsoft, Microsoft Security Bullentin MS17-010 Critical. Disponible https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2017/ms17-010

CIS, Cyber Alert: WannaCry Ransomware. Disponible https://www.cisecurity.org/ms-isac/cyber-alert-wannacry-ransomware/

Cybersecurity & infrastructure Security Agency, Indicators Associated With WannaCry Ransomware. Disponible https://us-cert.cisa.gov/ncas/alerts/TA17-132A

ANEXOS

ANEXO1: Informe_BlueTeam

	PROCEDIMIENTO ESPECÍFICO	CÓDIGO:
UNAD	GESTIONAR INCIDENTE MS17_010	FECHA: 12/10/2020
		VERSIÓN: 01
		CATEGORIA: APOYO
		PAGINA: 1
		USO INTERNO

1. OBJETIVO

Atender y solucionar las incidencias sobre los servicios reportados por WhiteHouse, bien sea por sus integrantes de operación o miembros del grupo de trabajo.

2. ALCANCE

El proceso inicia desde recibir notificación de un incidente, falla, vulnerabilidad por parte de WhiteHouse o las herramientas de monitoreo que la empresa tenga, hasta la solución del caso.

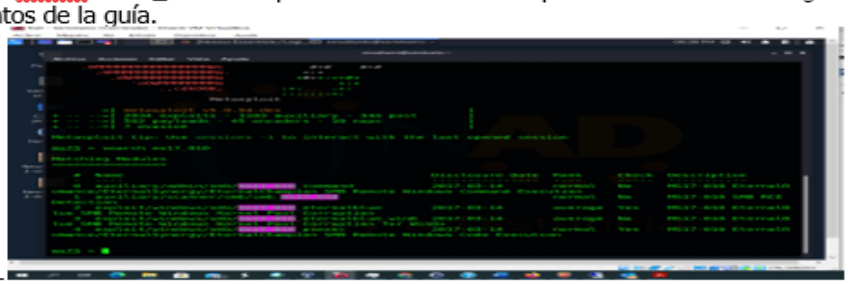
3. DEFINICIONES

- **Incidente:** Una interrupción no planificada de un servicio, o la reducción de la calidad de un servicio
- **Incidente Proactivo:** Son los incidentes que son detectados por la herramienta de monitoreo o los Project, antes de recibir notificación por parte del cliente
- **Incidente Reactivo:** Son los incidentes que son notificados por el cliente sin que se haya evidenciado durante la gestión de la operación
- **Incidente Sencillo:** Son incidentes proactivos o reactivos que tienen afectación sobre un cliente especifico
- **Incidente Masivo:** Son incidentes proactivos o reactivos que generan afectación a dos o más servicios o clientes y deben ser registrados bajo un tipo de registro del caso Incidente.
- **Vulnerabilidad**: debilidad o falla que pone en riesgo todos los activos de información junto con su integridad y disponibilidad.

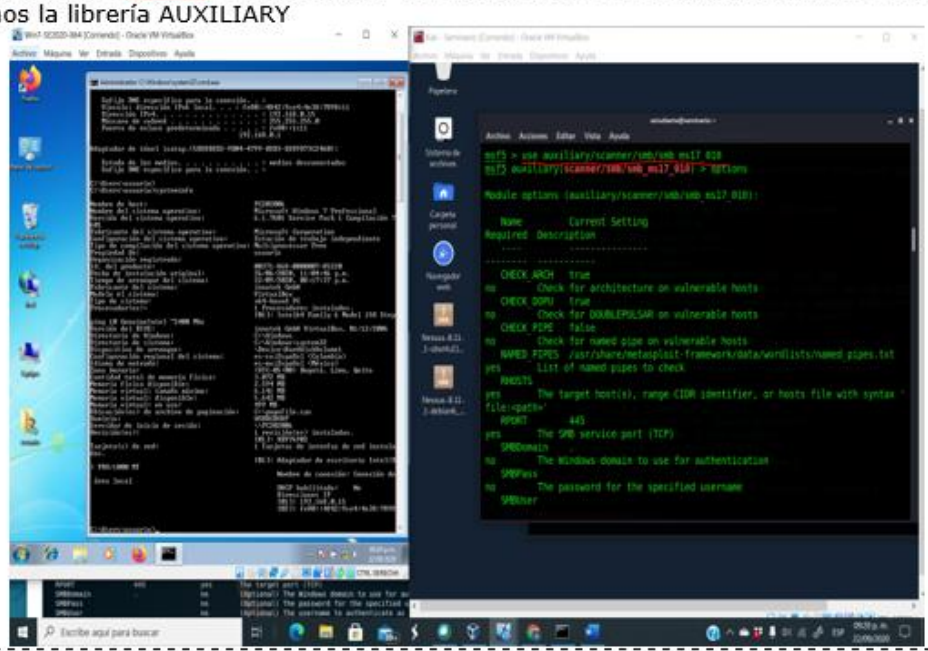
4. Actividades

1. Para el 14/02/2020 se recibe reporte por parte del grupo RedTeam donde se evidencia que el equipo 192.168.0.15 con sistema operativo Windows 7 x64, es vulnerable al MS17_010 CVE-2017-0143. Comolo muestra la imagen

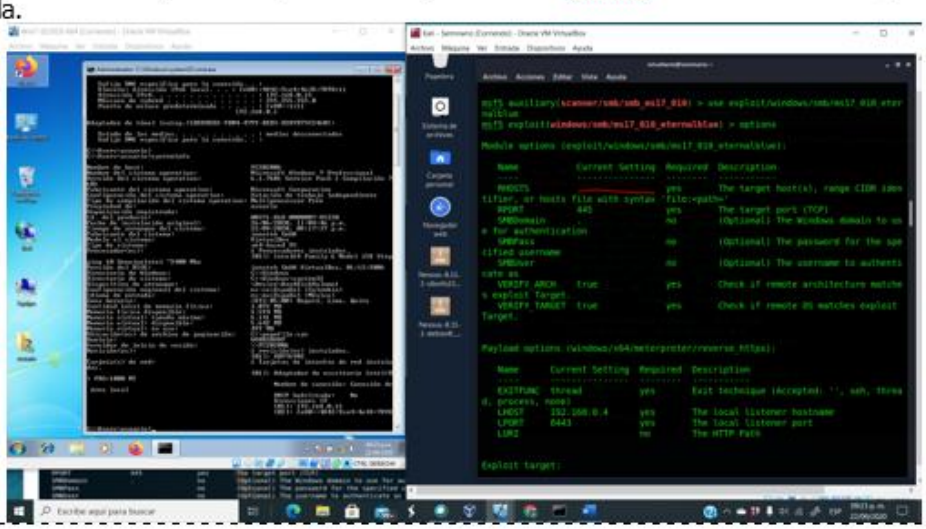
2. Identificada la vulnerabilidad se prepara el ataque al host 192.168.0.15 buscando el exploit con el siguiente comando "search ms17_010". Ya que es la vulnerabilidad que se está buscando según los lineamientos de la guía.



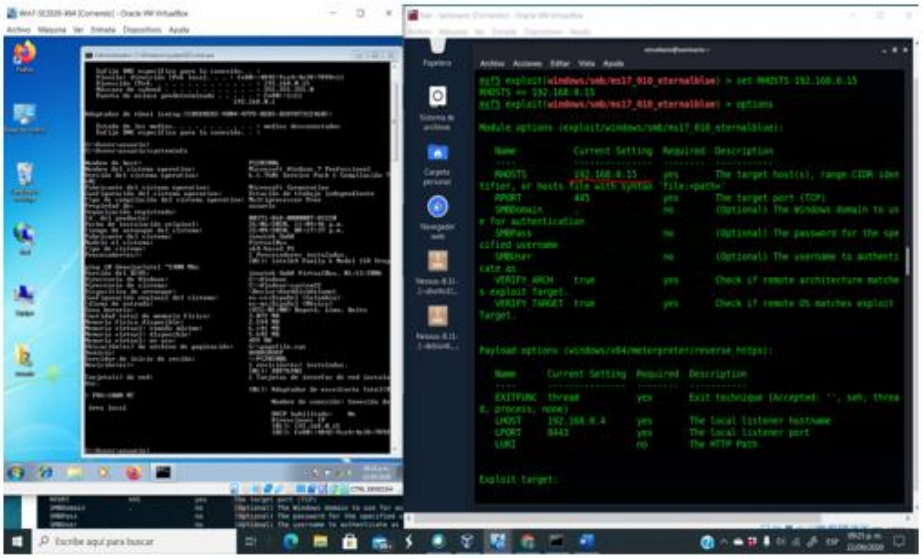
3. Verificamos los exploit a utilizar junto con sus opciones de configuración. Para este caso usamos la librería AUXILIARY



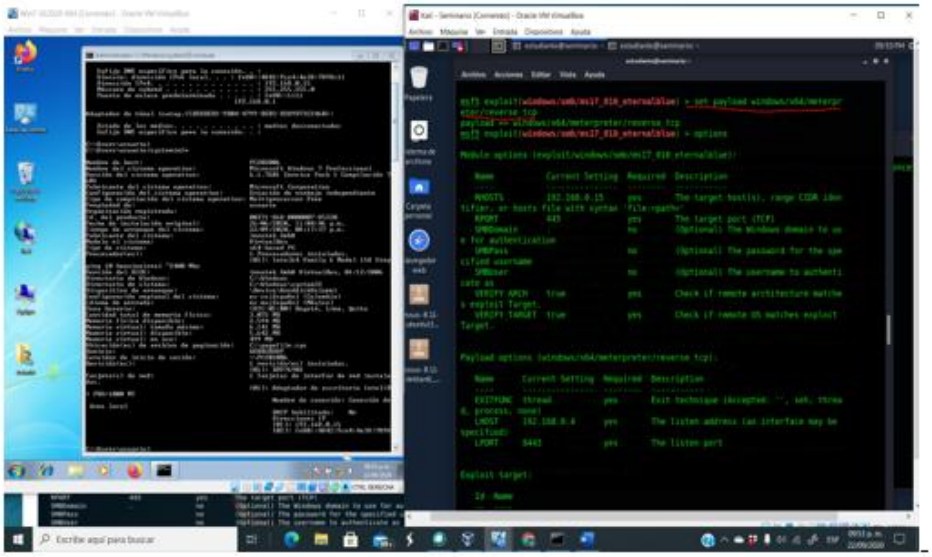
4. Validamos si está cargada la maquina victima para nuestro exploit. Para el caso vemos que no está cargada.



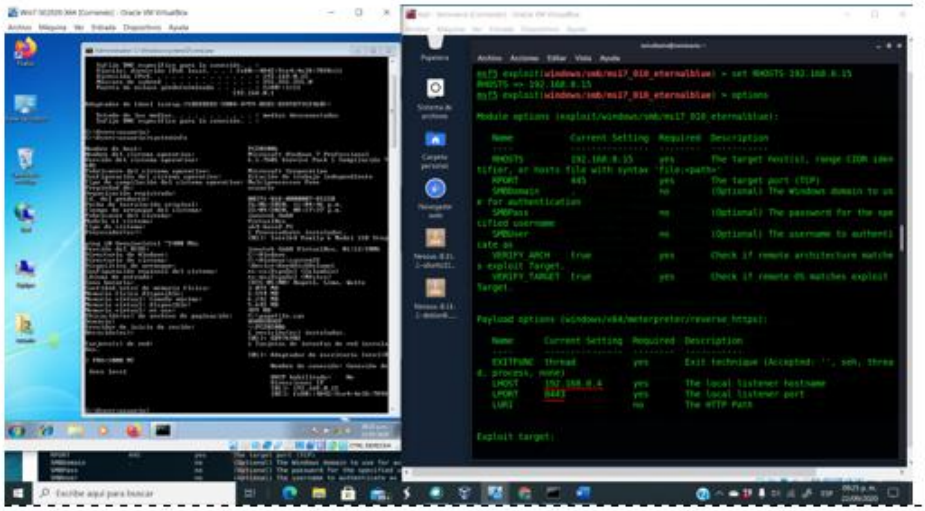
5. Identificando que no está la debemos asignar o apuntar. Para mi caso se debe cargar la maquina victima la cual esta identificada con la ip 192.168.0.15



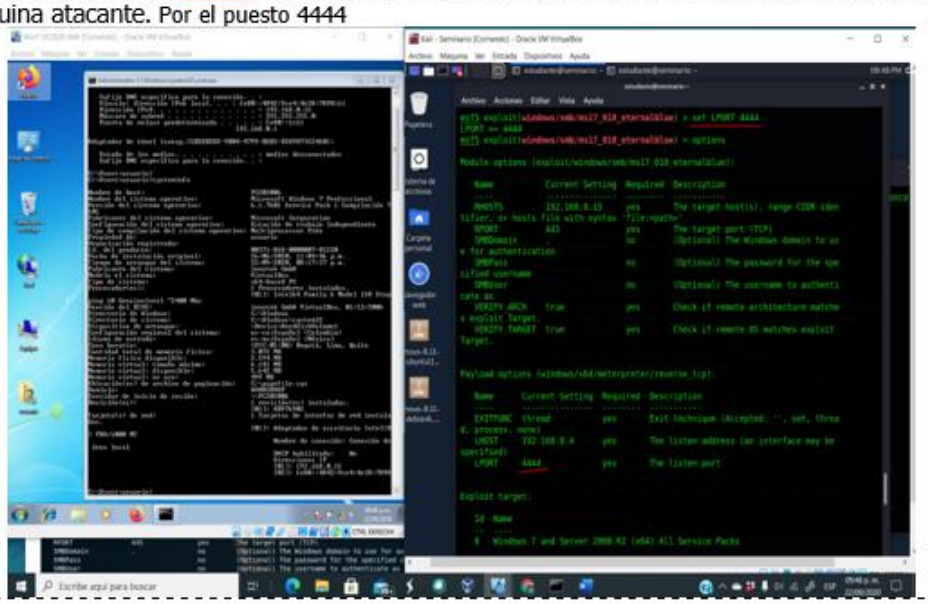
6. Ya cargada la maquina victima realizamos ya PAYLOAD



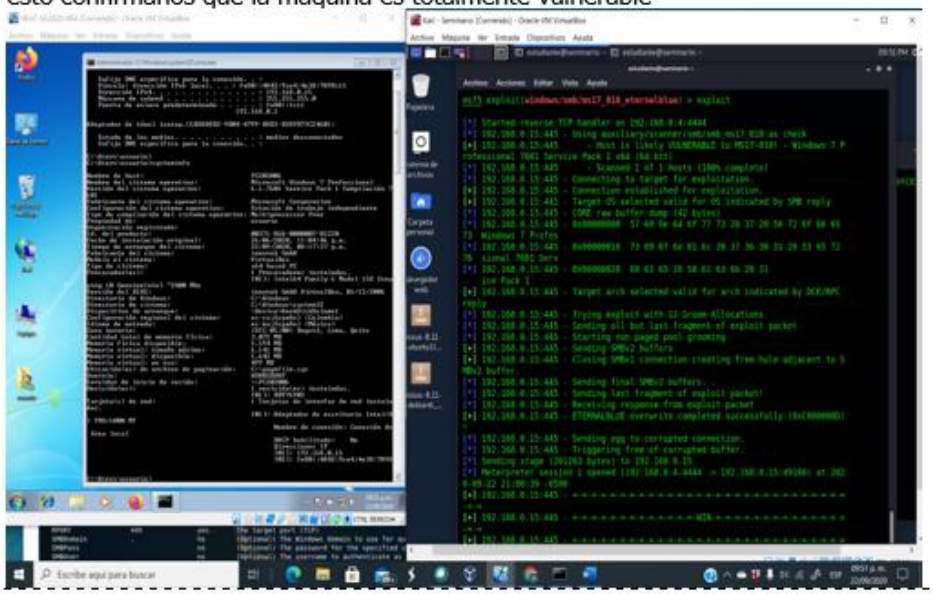
7. Ya teniéndola carga se debe tener en cuenta que aun que esta apunada a la maquina víctima. Nuestro equipo atacante está identificado con la IP 192.168.0.4 pero está saliendo por defecto por el puerto 8443



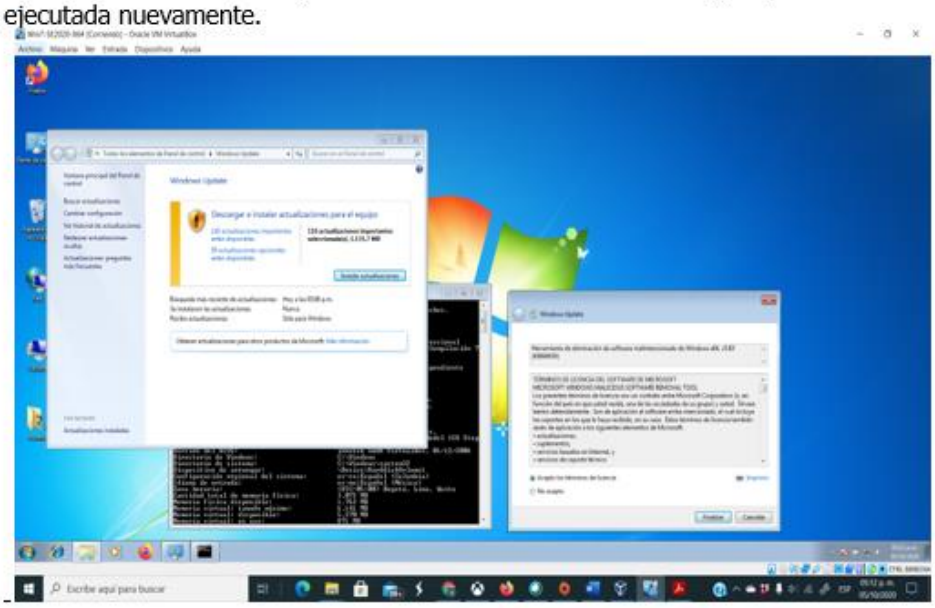
8. Por lo que al realizar el exploit nos da falla. Lo que nos indica que se debe configura el puerto de la máquina atacante. Por el puesto 4444



9. Con figuramos el puerto al puerto 4444, realizando el exploit y no sindica que fue exitoso. Con esto confírmanos que la maquina es totalmente vulnerable



10. Para solventar la vulnerabilidad se pone a punto el host 192.168.0.15, realizando actualizaciones y activación de firewall con lo que se da solución a la vulnerabilidad, ya que la misma no puede ser ejecutada nuevamente.



7. SALIDAS		
No.	**DESCRIPCIÓN**	**RESPONSABLE**
1.	Envío de Informe vulnerabilidad solventada a whitehose. Con el detalle de las actividades realizadas	Postulante al cargo Anderson Salazar Acosta
8. SOPORTE TECNOLÓGICO		**RESPONSABLES**
1.	Evidencia grafica	Postulante al cargo Anderson Salazar Acosta
2.	Correo electrónico	Postulante al cargo Anderson Salazar Acosta

9. POSIBLES FALLAS (RIESGOS POR TRANSACCIÓN)			
No.	**FALLA**	**ACCIÓN**	**RESPONSABLE**
1.	Casos escalados erróneamente	Informar el escalamiento erróneo para el direccionamiento correcto por medio de correo a la cuenta de **postulantealcargo@whitehouse.com**	Postulante al cargo Anderson Salazar Acosta

10. CONTROLES		
1.	**RIESGO ASOCIADO**	Tiempo elevado de diagnóstico
	COMO SE CONTROLA	Notificación por la herramienta de gestión o personal de compañía **whitehouse** cuando el tiempo transcurrido en diagnóstico sea mayor a 30 minutos.
	FRECUENCIA	Cada vez que se reporte una vulnerabilidad.
	CRITERIO DE ACEPTACIÓN	Diagnóstico preliminar realizado en un tiempo no mayor a 30 minutos.
	ACCIONES POR TOMAR	Grupo BLUETEAM toma de decisiones y acciones correctivas.
	EVIDENCIA	Herramienta de Gestión de **whitehose** y correo electrónico.

12. CONTROL DE VERSIONES				
No.	**Fecha**	**Cambio /Modificación**	**Aprobado por**	**Elaborado Por**
1.		Versión Inicial	**Whitehouse**	Postulante al cargo Anderson Salazar Acosta

Informe_BlueTeam.pdf

ANEXO2: Informe_RedTeam

	PROCEDIMIENTO ESPECÍFICO	CÓDIGO:
UNAD	GESTIONAR INCIDENTE MS17_010	**FECHA:** 12/10/2020
		VERSIÓN: 01
		CATEGORIA: APOYO
		PAGINA: 1
		USO INTERNO

1. OBJETIVO

Atender y solucionar las incidencias sobre los servicios reportados por WhiteHouse, bien sea por sus integrantes de operación o miembros del grupo de trabajo.

2. ALCANCE

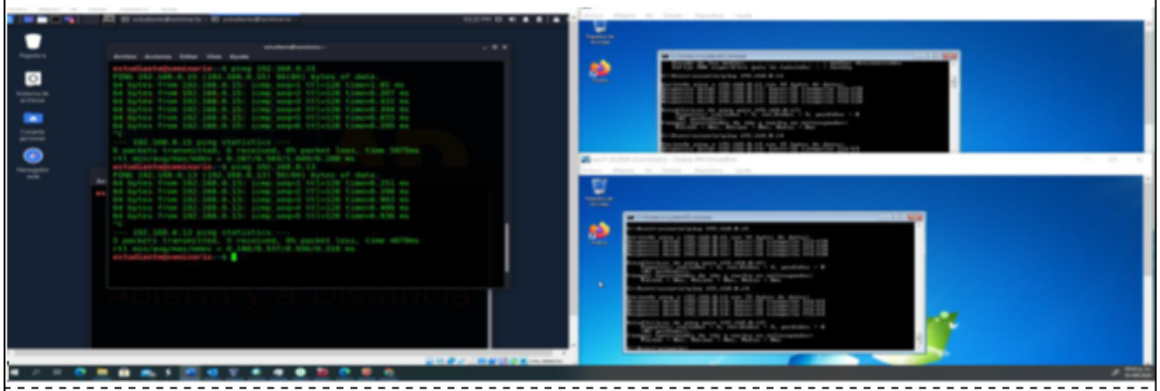
El proceso inicia desde recibir notificación de un incidente, falla, vulnerabilidad por parte de WhiteHouse o las herramientas de monitoreo que la empresa tenga, hasta la solución del caso.

3. DEFINICIONES

- **Incidente:** Una interrupción no planificada de un servicio, o la reducción de la calidad de un servicio
- **Incidente Proactivo:** Son los incidentes que son detectados por la herramienta de monitoreo o los Project, antes de recibir notificación por parte del cliente
- **Incidente Reactivo:** Son los incidentes que son notificados por el cliente sin que se haya evidenciado durante la gestión de la operación
- **Incidente Sencillo:** Son incidentes proactivos o reactivos que tienen afectación sobre un cliente especifico
- **Incidente Masivo:** Son incidentes proactivos o reactivos que generan afectación a dos o más servicios o clientes y deben ser registrados bajo un tipo de registro del caso Incidente.
- **Vulnerabilidad**: debilidad o falla que pone en riesgo todos los activos de información junto con su integridad y disponibilidad.

4. Actividades

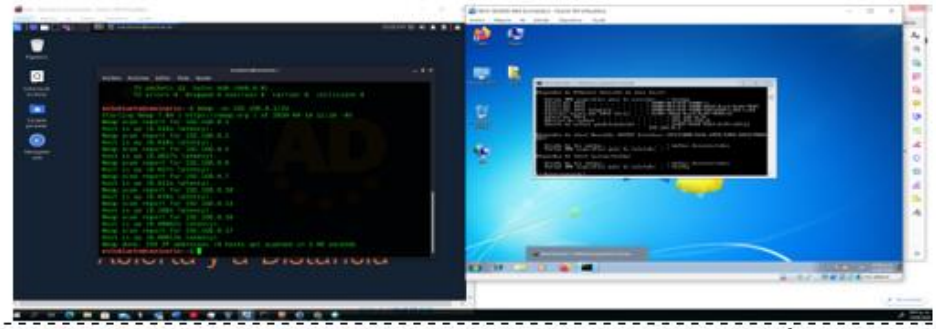
1. Para el 14/02/2020 se realiza instalación de 3 máquinas virtuales, las cuales son facilitadas por nuestro tutor en nombre de la práctica para la empresa WhiteHose. Las mismas son 2 maquina con sistema operativo Windows con arquitecturas de X64, X86 y una maquina con Kali Linux. Se realizaría instalación y posterior verificación de conectividad entre los hosts



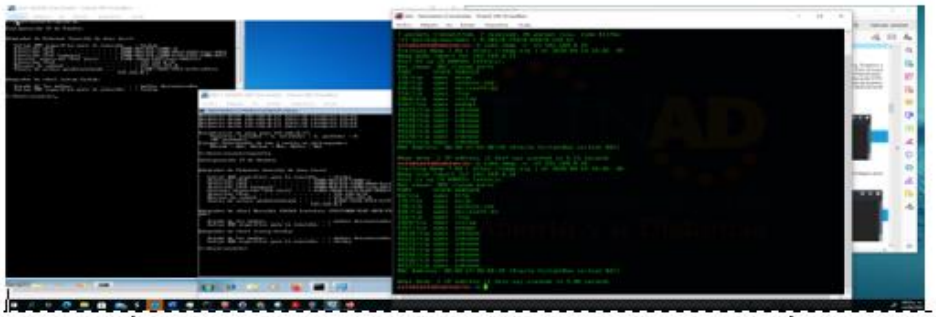
2. Se realiza inventario de máquinas para el caso:

S.O	Memoria	Discos	Procesador
Kali Linux	2 G.B	50 G.B	1
Windows 7 (64 bit)	4 G.B	50	1
Windows 7 (64 bit)	4 G.B	50	1

3. Se utiliza la herramienta NMAP con el Comando -sn, para el escaneo de red a los equipos que en la misma nos responda con estado UP . Es decir, que dentro de la red nos respondan a ICMP

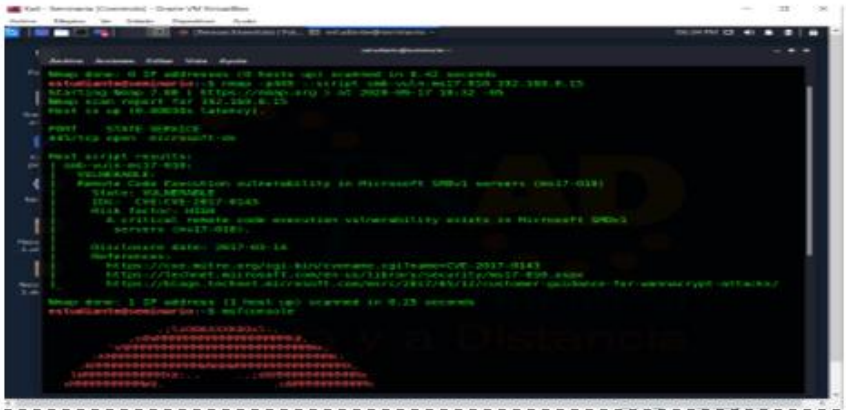


4. Identificadas las maquinas que respondes con estado UP, y con la información previa de las IP de las maquinas victimas que para el caso son 192.168.0.15 y 192.168.0.16, se realiza un escaneo de los puertos que se estén en escucha o en estado OPEN y su servicio. Información que nos aporta en siguiente comando.



5. Dada la información previa suministrada de los sistemas operativos que están corriendo. Como buena práctica, se confirman las versiones por medios de NMAP a cada una de las maquinas víctima para el caso a las IP 192.168.0.15 y 192.168.0.16

6. Se envía un script vuln, a la primera máquina victima identificada como 192.168.0.15. Con lo que identificamos que la maquina es vulnerable al ms17-010.



7. Aunque no es necesario o de carácter obligatorio, se realiza un scaneo con NESSUS para confirmar la información suministrada por el NMAP

8. Se encuentran vulnerabilidades en el equipo con IP 192.168.0.15 con Hostname PC202006. Aparte de la MS 17-010 se encuentran las siguientes MS 16-047, MS 11-030, WMI not Available, Unsupported Windows OS (remote). Es de aclarar que con Nessus encontramos mas vulnerabilidades que con Nmap dado que a Nmap al momento de crear el Scrip se apunto solo a buscar la vulnerabilidad MS17-010.

9. En los detalles de la vulnerabilidad MS 17-010, se identifica el CVE-2017-0144 según lineamientos de la guía al igual que con NMAP

7. SALIDAS		
No.	**DESCRIPCIÓN**	**RESPONSABLE**
1.	Envío de Informe con evidencia de la Vulnerabilidad encontrada al grupo de trabajo BLUETEAM, para toma de decisiones y acciones correctivas.	Postulante al cargo Anderson Salazar Acosta

8. SOPORTE TECNOLÓGICO		**RESPONSABLES**
1.	Evidencia grafica	Postulante al cargo Anderson Salazar Acosta
2.	Correo electrónico	Postulante al cargo Anderson Salazar Acosta

9. POSIBLES FALLAS (RIESGOS POR TRANSACCIÓN)			
No.	**FALLA**	**ACCIÓN**	**RESPONSABLE**
1.	Casos escalados erróneamente	Informar el escalamiento erróneo para el direccionamiento correcto por medio de correo a la cuenta de **postulantealcargo@whitehouse.com**	Postulante al cargo Anderson Salazar Acosta

10. CONTROLES		
1.	**RIESGO ASOCIADO**	Tiempo elevado de diagnóstico
	COMO SE CONTROLA	Notificación por la herramienta de gestión o personal de compañía **whitehouse** cuando el tiempo transcurrido en diagnóstico sea mayor a 30 minutos.
	FRECUENCIA	Cada vez que se reporte una vulnerabilidad.
	CRITERIO DE ACEPTACIÓN	Diagnóstico preliminar realizado en un tiempo no mayor a 30 minutos.
	ACCIONES POR TOMAR	Direccionar el caso al grupo BLUETEAM para toma de decisiones y acciones correctivas.
	EVIDENCIA	Herramienta de Gestión de **whitehose** y correo electrónico.

12. CONTROL DE VERSIONES				
No.	**Fecha**	**Cambio /Modificación**	**Aprobado por**	**Elaborado Por**
1.		Versión Inicial	**Whitehouse**	Postulante al cargo Anderson Salazar Acosta

Informe_RedTeam.pdf