Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Análisis de vulnerabilidades de seguridad en la red del CUD

Grado en Ingeniería Mecánica

ALUMNO: Armando Rubio García

DIRECTORES: Pablo Sendín Raña

Belén Barragáns Martínez

CURSO ACADÉMICO: 2014-2015

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE GRADO

Análisis de vulnerabilidades de seguridad en la red del CUD

Grado en Ingeniería Mecánica

Intensificación en Tecnología Naval

Cuerpo General

Universidade Vigo

RESUMEN

Tras Estados Unidos y Reino Unido, España es el país del mundo que más ciberataques ha recibido el pasado año. Día a día, se libra una batalla constante en la red en la que trata de mantenerse la privacidad de los individuos y las organizaciones tanto públicas como privadas, frente a los numerosos ataques que tienen lugar en busca de información sensible o de interés para estos ciberdelincuentes.

A nadie se le escapa que, en los próximos años, la Defensa Nacional estará inevitablemente ligada a la ciberdefensa. El descubrimiento de posibles vulnerabilidades en cualquiera de sus servidores informáticos de forma activa e interna, es decir, siendo la propia organización la que detecte estas vulnerabilidades para encontrarles solución, es un factor crítico para toda la organización. Este ámbito, el de la auditoría informática o *pentesting*, proviene de la consideración de que no hay mejor demostración de la baja seguridad de un sistema que el someterlo a un ataque, ver hasta dónde llega el atacante y cómo podría haberse evitado. De este modo, el presente TFG se ha enfocado al análisis de vulnerabilidades de seguridad en una red mediante la realización de una auditoría en una de las redes corporativas, la red del Centro Universitario de la Defensa (CUD), con el fin de verificar la seguridad de esta red empleando las opciones que se encuentran disponibles en la actualidad en el ámbito del *pentesting*. Para ello, de todas las opciones, plataformas y herramientas posibles de las que se encuentran disponibles se elegirán unas determinadas que serán explicadas en el presente documento con la intención de adquirir una idea general e integral del empleo de dicha herramienta. Como objetivo secundario, pero no menos importante, se pretende conocer el panorama actual real en materia de ciberseguridad y, más en concreto, de la ciberdefensa.

PALABRAS CLAVE

Ciberseguridad, Ciberdefensa, Auditoría informática, *Pentesting*, Test de intrusión, Kali Linux, Redes

Si vis pacem, para bellum

CONTENIDO

ÍNDICE DE FIGURAS

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Presentación.

Los Estados desarrollados viven inmersos en la era de las nuevas tecnologías, la información y las telecomunicaciones. La ciberseguridad y la ciberdefensa son críticas para hacer frente a una de las amenazas más relevantes que podemos encontrar en la actualidad y que nos acompañará en las próximas décadas, la ciberdelincuencia. Ésta es fruto del uso masivo que se hace en los Estados occidentales de todas estas tecnologías, haciéndonos altamente dependientes de las mismas y originando así una necesidad que el atacante bien ha sabido interpretar como lo que es, una vulnerabilidad a explotar.

En esta introducción se analiza el panorama actual fuertemente marcado por la globalización y el desarrollo tecnológico, y se presentan los objetivos que se persiguen en la realización de este TFG. También se muestran la estructura y el contenido de este trabajo.

1.2 Introducción y motivación.

La Edad de los Metales es una de las dos grandes etapas tecnológicas en las que tradicionalmente se ha subdividido la Prehistoria euroasiática. Por definición, es el período que siguió a la Edad de Piedra y durante el cual el hombre empezó a fabricar objetos de metal fundido. Este avance tecnológico fue de tal magnitud que le dio denominación al periodo histórico. Esto fue así debido al cambio que produjo este descubrimiento y a la facilitación en el trabajo diario que supuso para el ser humano. ¿Nos encontramos en la edad de las telecomunicaciones y la información? En el día a día de cualquier ciudadano occidental tienen lugar infinidad de actividades de las cuales un muy bajo porcentaje ocurren al margen de las nuevas tecnologías. El ciudadano de a pie se ha convertido en un "esclavo de la tecnología", nada parece posible hoy en día sin los ordenadores, los móviles, las televisiones…, etc. ¿Alguien es capaz de imaginar un día completo sin poder utilizar todos estos avances tecnológicos? La dependencia es vulnerabilidad y claro está que nuestra sociedad es altamente dependiente de la tecnología.

Aquellos capaces de controlar los sistemas informáticos de un Estado tienen en su mano la capacidad para crear caos y terror. En este contexto, ha aparecido un nuevo concepto en los últimos años, clave para la Defensa de cualquier nación y los derechos y libertades de sus ciudadanos, enmarcado dentro de la ciberseguridad: la ciberdefensa. Un Estado seguro ya no es aquel que cuenta con unas fuerzas del orden y unas Fuerzas Armadas preparadas y eficientes. Necesita también tener pleno control de su ciberespacio.

Y es que nada de esto es ya ciencia ficción, ni queda relegado a la gran pantalla. Nos encontramos bajo ataques continuos. Nuestra intimidad es vulnerable, nuestra competitividad empresarial fundamentada en la investigación y el desarrollo nacional también. Nuestra información más sensible a nivel gubernamental y de defensa. Todo eso está al alcance de aquel capaz de acceder a los servidores informáticos que almacenan nuestra información y a los nodos que nos conectan con el resto del mundo en esa gran red conocida como Internet. Es ya una realidad y está ocurriendo ahora mismo. El año pasado, las empresas e instituciones españolas sufrieron más de 13000 ataques informáticos. Estos ataques fueron registrados por el CERT [47], el primer Centro de Prevención y Respuesta a las amenazas cibernéticas en España, que nace de la necesidad de proteger las consideradas infraestructuras críticas. Estas infraestructuras críticas las conforman el conjunto de recursos, servicios, tecnologías de la información y redes, que, en el caso de sufrir un ataque, causarían un gran impacto en la seguridad tanto física como económica, de los ciudadanos o el buen funcionamiento del Gobierno de la nación. La criticidad de estas estructuras se mide en base a tres factores:

- El número potencial de víctimas mortales o graves que podría provocar un ataque en dicha infraestructura.

- El impacto económico, en función de las pérdidas económicas que podría provocar o el impacto medioambiental.

- El impacto público, la influencia en la confianza de la población, el sufrimiento físico y la alteración de la vida cotidiana.

Es deber de la nación el proteger estas infraestructuras ya que con ellas se protege el bienestar de todos y el correcto funcionamiento empresarial y económico del Estado. Se entiende mucho mejor sólo imaginando que pasaría si la red eléctrica del Estado dejara de operar, si las líneas de transporte no pudieran utilizarse o el mercado y la bolsa se vieran bloqueados. El nivel de caos en todo el país sería inimaginable. Nadie hoy en día puede pasar sin el uso de las telecomunicaciones. Imaginemos qué sucedería si las grandes empresas de telecomunicaciones fueran incapaces de prestar sus servicios y con ellas todas las líneas de telefonía e Internet. Lo mismo ocurriría si se viese comprometida la seguridad en los servicios que ofrece la banca online, los sistemas de distribución de agua o gas, etcétera.

Las infraestructuras críticas se agrupan en 12 sectores:

1. La Administración.
2. El sector aeroespacial.
3. El sector energético.
4. El de la industria.
5. El nuclear.
6. La industria química.
7. El sector de investigación.
8. El de la salud.
9. El del transporte.
10. El de la alimentación.
11. El financiero y tributario.
12. El de las tecnologías de la información y las comunicaciones.

La Secretaría de Estado de Seguridad es la encargada de la dirección, coordinación y supervisión de la protección de infraestructuras críticas de la nación.

Resulta muy impactante y sorprendente, y escapa a la mayor parte de los ciudadanos, que España está sufriendo estos ataques constantemente y con un incremento exponencial en los últimos años. Como demuestra [2], ministros y secretarios de Estado del gobierno sufrieron ataques este pasado año por parte de hackers rusos y chinos en sus móviles y ordenadores personales con la intención de rastrear datos y conseguir información. Los ministros de Defensa, Interior, Exteriores y Presidencia del Gobierno sufrieron los ataques más complejos. Ya en 2009 varios ministerios y empresas fueron infectados con virus que tardaron en detectarse tres años.

Los expertos en Ciberseguridad sostienen que el valor de la información estratégica obtenida con las agresiones cibernéticas duplica la inversión realizada por los atacantes. Contratar a un equipo de piratas para inocular un virus en el ordenador de un organismo oficial puede costar hasta tres millones de euros, según las mismas fuentes. El mercado negro comercializa también las llamadas vulnerabilidades, que es como se denomina a los agujeros de seguridad desconocidos de un sistema operativo o navegador. Los *hackers* fabrican con estos descuidos de los programadores sus virus.

La amenaza dentro del ciberespacio es patente, y todo apunta a que la capacidad de un Estado para hacerle frente será vital en los próximos años para mantener la privacidad en la red y, la seguridad de todas aquellas infraestructuras con conexión a Internet.

La presente obra expone, de forma detallada, el contexto actual en ciberseguridad, mostrando tanto la amenaza como la reacción por parte de los Estados y organizaciones, con el fin de proteger su privacidad y sus servicios informáticos. La parte principal de la obra muestra un ejemplo práctico de cómo proteger estas instalaciones en una organización concreta, detectando primero sus vulnerabilidades e implementando las medidas necesarias para alcanzar un nivel de protección adecuado frente a posibles ataques.

1.3 Objetivos.

Este TFG persigue una serie de objetivos, de los cuales el objetivo principal es la realización de la auditoría en sí y el desarrollo de un plan para llevar a cabo lo que se denomina un test de intrusión, de forma lógica y ordenada. En los siguientes párrafos se desglosan éste y otros objetivos menores del TFG.

1.3.1 Situación actual de la ciberseguridad y la ciberdefensa. Este TFG expone la realidad actual en torno a los ataques informáticos que se sufren a diario en gran número. Se pretende adquirir una visión clara, objetiva y veraz. También se pretende mostrar las reacciones gubernamentales y de organizaciones internacionales de las que España es miembro, como la OTAN y la UE, y las estrategias implementadas con el fin de hacer frente a esta amenaza y proteger los derechos y libertades de sus ciudadanos y la integridad de sus infraestructuras críticas.

1.3.2 Plataformas y herramientas de *pentesting*. Una de las finalidades es presentar algunas de las herramientas más empleadas por los profesionales del sector y sus amplias capacidades, de modo que, logremos familiarizarnos con dichas herramientas desconocidas al comienzo de este TFG. También se pretende presentar ciertas plataformas que ya trabajan a modo de "laboratorio" integrando gran parte de estas herramientas.

1.3.3 Desarrollo de la auditoría. Ésta constituye la parte principal del TFG. Aquí se pretende hacer una elección de las herramientas con las que se pasará a atacar la red. Los test de intrusión o *pentesting* sirven para analizar el nivel de seguridad de un sistema informático o red mediante la simulación, en un entorno controlado, de un ataque por un usuario malicioso, un *hacker*. Al final del proceso, se le presenta al propietario un informe de vulnerabilidades y un análisis del impacto que éstas tienen en la seguridad de la organización junto a posibles soluciones. Antes de comenzar, se llegará a un acuerdo con el propietario sobre el alcance de la auditoría para asegurarse de que no se está violando la intimidad del cliente y que no se traspasan los límites que éste establezca. Este TFG plantea el desarrollo y aplicación de un test de intrusión para que cualquiera sin conocimientos avanzados en el ámbito de la informática sea capaz de seguirlo y entenderlo, mostrando todo el proceso en detalle. Por ello, se busca realizar un desarrollo del ataque estructurado y claro de forma también que sea mucho más sencilla la elaboración del informe final en el que se obtengan las conclusiones después del proceso y en el que se presenten las soluciones que se consideren, resuelven las carencias de seguridad.

1.4 Estructura de la memoria.

En este primer capítulo se ha realizado una presentación de lo abordado en este TFG. Se pueden ver las principales líneas de acción en las que se centra el esfuerzo del TFG; la contextualización de la obra, la descripción del panorama internacional en materia de ciberdefensa y la importancia que ha adquirido en materia de Seguridad. Finalmente, se presentan los objetivos con los que se ha iniciado la realización de la obra.

En el capítulo 2, se analiza el contexto actual en el que se ha elaborado la obra. Se revisa el proceso histórico a través del cual la ciberdefensa ha alcanzado tal relevancia, comenzando por el inicio, con los primeros ataques cibernéticos y su posterior evolución y expansión. Se presenta también el proceso en el cual los Gobiernos son víctimas de estos ataques, cada vez en mayor número, y, por ello, toman conciencia de la necesidad de implementar una defensa eficaz, desarrollando las diferentes estrategias y planes que hoy se llevan a cabo en todo el panorama internacional. Se termina presentando algunas de las plataformas más usadas en el ámbito de la auditoría informática, así como las herramientas más empleadas en el *pentesting*. Se describe un gran número de estas herramientas, como punto de partida para la familiarización con su empleo, indicando en que ámbito tienen utilidad y cómo se emplean, ya que posteriormente, son las herramientas que se utilizan para llevar a cabo el test de intrusión. Así mismo, se presenta la información que proporcionan cada una de ellas, mostrando su utilidad y cómo se integran dentro del proceso que se ha seguido en la realización de la auditoría.

En el capítulo 3, se presenta todo el proceso de la auditoría realizada en la red del CUD (Centro Universitario de la Defensa). Tras analizar las diferentes metodologías más comúnmente utilizadas por la mayoría de *pentesters*, se ha implementado una metodología propia. En este apartado, se desarrolla esta metodología paso a paso. Se acompaña al trabajo con una amplia recopilación gráfica de todo el proceso realizado, por medio de capturas de pantalla de cada parte del test, siendo explicadas cada una de ellas.

En el capítulo 4, se explica el porqué de la metodología empleada y se expone el razonamiento seguido. También se presenta de forma más detallada cada paso de la auditoría, por qué se ha atacado cierto servidor en ese momento y no antes o de ese modo y no de otro. Así mismo, se revisa todo el trabajo que se ha presentado en el capítulo anterior con el fin de obtener conclusiones y terminar de comprender todo el trabajo realizado. Finalmente, este capítulo termina recogiendo una serie de medidas para mejorar la seguridad en la red y lo que, en una auditoría estándar, representaría el

informe final, exponiendo las vulnerabilidades encontradas, en qué grado afectan a la seguridad de la organización y de qué modo pueden paliarse.

En el último capítulo, se presentan las conclusiones finales tras la realización de este TFG. Conclusiones finales, circundantes al test realizado, a los objetivos fijados inicialmente y al panorama futuro que se espera entorno a la ciberdefensa. Además, se han marcado unas líneas futuras de continuación del trabajo, para servir de referencia a futuros auditores que decidan testar de nuevo la seguridad de la red.

2 ESTADO DEL ARTE

2.1 Presentación.

En esta parte del trabajo, se analizan las diferentes medidas que se han ido tomando desde que se tomó conciencia del papel clave que iba a tomar la ciberseguridad para la defensa de los Estados y en las que España se encuentra inmersa, tanto a nivel nacional como a nivel OTAN y Unión Europea. Se presenta, de forma cronológica, este proceso de toma de conciencia a medida que se van sufriendo diferentes ataques en el panorama internacional. Se realiza una descripción de cómo se articula la Defensa Nacional en España y cómo queda enmarcada en ésta la ciberdefensa. También se muestra la estructura y los diferentes organismos que han surgido como actores principales para combatir la ciberdelincuencia. Se termina este capítulo con una revisión de las principales herramientas y plataformas integradoras que podemos adquirir para realizar estos test de intrusión e implementar así una seguridad eficiente en nuestros servidores y redes.

2.2 Estrategias y planes de Ciberdefensa.

Los ataques cibernéticos son muy rentables. El nivel de exposición del atacante es bajo, los recursos necesarios no son muy elevados y, sin embargo, la recompensa obtenida puede ser muy valiosa a nivel empresarial o gubernamental. Además, es posible realizar un ataque a un amplio sector de la sociedad, a un individuo en concreto, a las grandes organizaciones o a la administración pública. El abanico de objetivos es amplio. Todas las naciones de nuestro entorno se han concienciado y están desarrollando iniciativas y planes tratando de hacer frente a estas amenazas que están emergiendo. Gran parte de ellas se basan en fortalecer la capacidad técnica y coordinarla, interviniendo en forma de respuesta y sólo en caso de que la amenaza ya se haya materializado.

En España las responsabilidades en el Ciberespacio están muy fragmentadas. Es por esto que uno de los esfuerzos en los que se trabaja es en la coordinación y el trabajo colaborativo entre todos los agentes implicados. Estos agentes son la industria, la administración pública, el individuo y los aliados y organizaciones internacionales de las que España forma parte. Es vital también el presupuesto que se le dedique si se pretende alcanzar una capacidad técnica competente capaz de hacer frente a las amenazas emergentes y más exigentes manteniéndose actualizado en un mundo con un carácter evolutivo tan volátil.

En el siguiente eje cronológico se muestran solo algunos de los ataques más relevantes a lo largo de la historia y los planes y estrategias implementados por los Estados y organizaciones internacionales:

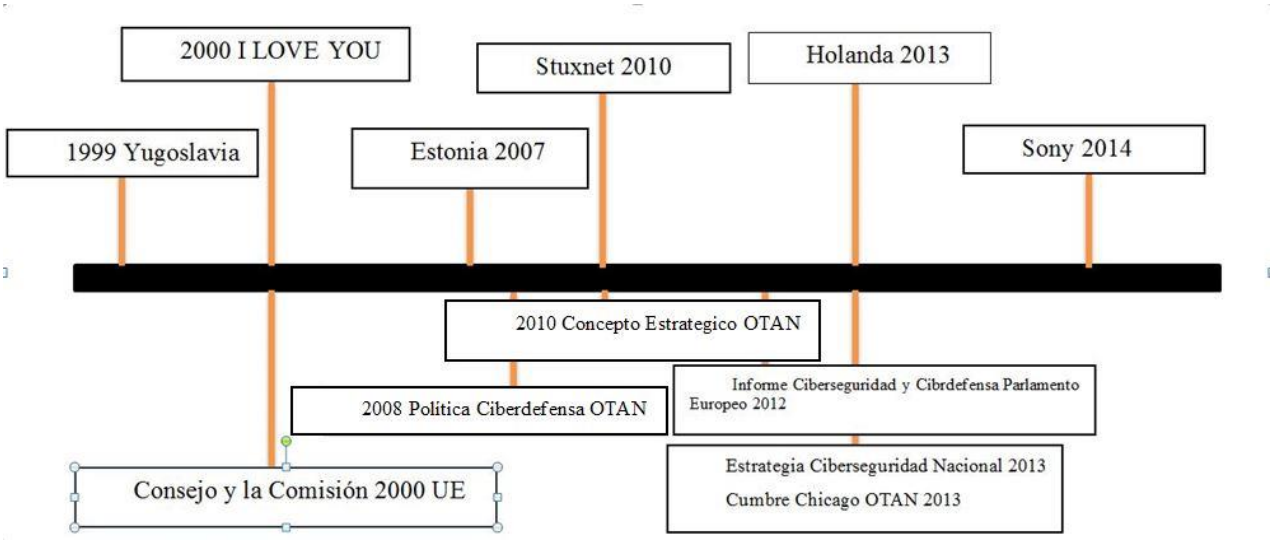


Figura 2-1 Eje cronológico. Ataques frente a directivas promulgadas

El eje cronológico no mantiene la proporcionalidad. De hacerlo, se apreciaría aún mejor el agrupamiento de las directivas en torno al 2010 mientras los ataques se encuentran más repartidos. Puede deducirse entonces que la reacción de los diferentes Estados y organismos ha sido un poco tardía.

2.2.1 La ciberseguridad y la Defensa Nacional.

La Ley de la Defensa Nacional [3] refleja el cambio en el que se encuentra inmerso el mundo y las consecuencias que éste conlleva en cuanto a nivel estructural para la Defensa Nacional y el orden internacional. En el escenario estratégico, se ha pasado de la política de bloques de la guerra fría a la globalización y las relaciones internacionales. Es remarcable la interdependencia de los Estados, y las organizaciones que estos han creado para respaldar la paz y la estabilidad, como la ONU, la OSCE, la

UE o la OTAN, entre otras. Destaca también la revolución tecnológica sufrida en las últimas décadas y la influencia de ésta en Defensa. Según el Art.8 de dicha Ley, el Consejo de Defensa Nacional es el encargado de asesorar al Presidente del Gobierno y al Rey en materia de defensa así como elaborar las directrices de la política de defensa.

La Ley de acceso electrónico de los ciudadanos a los Servicios Públicos [4] establece la obligatoriedad de proporcionar los diferentes servicios de la administración en el ciberespacio. Además establece que las Administraciones Públicas usarán las tecnologías de la información garantizando la integridad, disponibilidad, el acceso, la autenticidad, la confidencialidad, y la conservación de los datos y los flujos de los medios de comunicación y de la información.

El Consejo de Defensa Nacional presentó por primera vez en 2013 un Informe Anual de Seguridad Nacional [5], documento en el que se trata de sintetizar la situación actual en España en materia de defensa, y permite la elaboración de la Estrategia de Seguridad Nacional, fundamentada en la unidad de acción y la prevención y anticipación. La Estrategia de Seguridad Nacional [6] evalúa el entorno estratégico en el que se desenvuelve España e identifica doce riesgos y amenazas; y marca los objetivos y líneas de acción para hacerles frente. También sienta las bases de un Sistema de Seguridad Nacional, en cuya cúspide está el Consejo de Seguridad Nacional. En las diversas reuniones llevadas a cabo por este Consejo se llegó al acuerdo de la creación de Grupos de Apoyo de Ciberseguridad con la denominación de Consejo Nacional de Ciberseguridad y la Estrategia de Ciberseguridad Nacional. La Estrategia de Ciberseguridad Nacional (ECSN) [7] trata de hacer una previsión en este campo con el fin de prevenir, detectar y responder a las ciberamenazas. Trata de coordinar y armonizar todos los actores y recursos del Estado y la colaboración público-privada de los españoles en materia de ciberdefensa.

El Informe Anual de Seguridad dedica uno de sus apartados (el inmediatamente siguiente al dedicado al terrorismo) a la ciberseguridad. Esto muestra la importancia y relevancia que ha tomado la ciberseguridad a la hora de mantener la seguridad nacional y el nivel de conciencia que han alcanzado todos los Estados desarrollados en la actualidad. En este apartado, se citan los retos que nos encontramos para hacer frente a las diversas vulnerabilidades que pueden aparecer en esta materia y las medidas que se han tomado al respecto y se están implementando en la actualidad. En cuanto a los retos, la creciente dependencia cibernética de nuestra sociedad en la actualidad tanto a nivel público como privado no hace más que aumentar las vulnerabilidades ante potenciales ataques. Para lograr un ciberespacio seguro debemos lograr la integridad en el flujo de información, al mismo tiempo que alcancemos la confidencialidad ante terceros en este traspaso de información. Es también necesario garantizar la disponibilidad de estos sistemas de información. Por último, debemos ser capaces de negar el acceso a información clasificada o sensible para los intereses nacionales a estos atacantes del ciberespacio. La ciberseguridad puede verse comprometida por factores naturales o técnicos que nos nieguen el uso de un sistema de información, o por ataques ilícitos perpetrados por diversos agentes, entre los que cabe destacar, los sistemas de inteligencia y las unidades especializadas en operaciones de información, *hackers*, terroristas y crimen organizado. En cuanto a la tipología de los ataques, tenemos la realizada en [17]:

- Crimen organizado: estas organizaciones se centran en la captura de información bancaria como las tarjetas de crédito, el fraude telemático o el falseamiento de certificados digitales que les permite lucrarse a costa del ciudadano.
- Espionaje industrial: son compañías o gobiernos que buscan la obtención de información crítica en el ámbito tecnológico industrial y empresarial para realizar una competencia "sucia" de mercado desleal.
- Hacking ético o político: estos ataques se pueden ver en los medios de información, sobre todo en las zonas más inestables, con conflictos regionales y donde se pugna por el poder y el control del Estado. Suelen consistir en ataques de denegación de servicio pero a nivel de página web y muy raramente a nivel interno, por lo que no son muy dañinos.

- Servicios de inteligencia: ésta es la pugna entre Estados en sí misma, suelen buscar información muy sensible relacionada con la Defensa, sus ataques son difícilmente detectables, disponen de grandes medios y recursos y sus ataques son prolongados en el tiempo.
- Terrorismo: se basan en cuatro frentes de interés:
  - La comunicación entre sus células desplegadas en cualquier lugar.
  -El reclutamiento y la captación de adeptos y seguidores.
  -La obtención de información de posibles objetivos.
  -La consecución de fuentes de financiación y medios que les permitan continuar su guerra.

No es extraño dentro de este sector la contratación de *hackers* y mercenarios que sean los que lleven a cabo el ataque si ellos carecen de los medios oportunos.

Otra clasificación, aceptada a nivel internacional [22], divide las amenazas en: Ciberespionaje, Ciberdelincuencia, el hacktivismo y el Ciberterrorismo, que, como puede observarse, es bastante similar a la anterior clasificación. La aprobación por el Consejo de Seguridad Nacional, el 5 de diciembre de 2013, de la primera Estrategia de Ciberseguridad Nacional y la creación del Consejo Nacional de Ciberseguridad son dos hitos fundamentales para la actuación coordinada y cooperativa de los diferentes departamentos, organismos y agencias de las Administraciones Públicas con responsabilidades en este ámbito.

Cabe destacar la creación del Mando Conjunto de Ciberdefensa en las FAS (MCCD) [8] para planear y ejecutar las acciones en ciberdefensa militar en las redes, y responder ante amenazas que puedan afectar a la Defensa Nacional. Su creación, el 26 de febrero de 2013, por Orden Ministerial 10/2013, del 19 del mismo mes, determina su ámbito de actuación en las redes y sistemas de información y telecomunicaciones de las Fuerzas Armadas así como otras redes y sistemas que se le encomienden por ser claves para la Defensa Nacional. Su misión es el planeamiento y ejecución de las acciones relativas a la ciberdefensa, al mismo tiempo que debe ser capaz de dar respuesta a ataques y amenazas que puedan perjudicar a la Defensa Nacional. La creación del CERT de Seguridad e Industria como Centro de Respuestas a Incidentes de Seguridad cibernética para proteger infraestructuras críticas y del sector privado es también un hito a tener en cuenta. Tiene responsabilidades en ciberataques sobre sistemas clasificados, sistemas de la Administración General, Autonómica y Local y, en coordinación con el Centro Nacional de Protección de Infraestructuras Críticas, de los sistemas que gestionan estas infraestructuras. También proporciona el nivel de amenaza a modo informativo a Presidencia del Gobierno.

Se están llevando a cabo también numerosos programas con el objeto de fomentar el I+D+i. La implantación de una cultura en ciberseguridad sólida es otro de los objetivos que se está llevando a cabo mediante la concienciación y sensibilización de empresas y particulares sobre el uso seguro de las redes. Así mismo, España se encuentra inmersa en la participación y elaboración de ejercicios que permiten testar y aumentar el nivel de seguridad en sus redes, así como la capacidad de reacción ante posibles ataques tanto a nivel Unión Europea, como a nivel OTAN e internacional.

La Estrategia de Seguridad Nacional comienza afirmando en su primera página, "*el ciberespacio es hoy el ejemplo más claro de un ámbito accesible, poco regulado y de difícil control, y, en consonancia, la ciberseguridad es uno de los principales ámbitos de actuación de esta Estrategia*". Además, marca seis líneas de acción a seguir para hacer frente a esta amenaza:

- Aumentar la capacidad de detección, prevención, investigación y respuesta a las ciberamenazas en la Administración Pública, en el entorno de Defensa y en los organismos públicos y privados de relevancia crítica para la seguridad nacional.
- Garantizar la seguridad y disponibilidad de los sistemas de información y redes.
- Colaboración Público-Privada que fortalezca la resilencia de las tecnologías de la información.
- Promocionar la capacitación de profesionales en ciberseguridad y la I+D+i.
- Implantación de una cultura de ciberseguridad sólida.

- Intensificación de la colaboración internacional.

La Estrategia de Ciberseguridad Nacional es una extensión de esta Estrategia de Seguridad Nacional.

Figura 2-2 Estructura orgánica de la ciberseguridad nacional (Estrategia de Ciberseguridad Nacional)

El Consejo de Seguridad Nacional asiste al presidente en la dirección de la política de Seguridad Nacional. Como puede verse en la Figura 2-2, el Comité Especializado de Ciberseguridad dará apoyo al Consejo de Seguridad Nacional y asesoramiento al Presidente en materia de ciberseguridad además de reforzar la colaboración y cooperación de los organismos públicos y privados. El Comité Especializado de Situación será convocado para llevar a cabo la gestión de las situaciones de crisis en el ámbito de la ciberseguridad y será apoyado por el Centro de Situación del departamento de Seguridad Nacional facilitando el seguimiento, control y transmisión de las decisiones.

2.2.2 La ciberseguridad dentro de la OTAN.

Ya en 1999 *hackers* serbios realizaron diversos ataques sobre servidores OTAN y de EEUU. Cuando empezó el ataque aliado sobre Yugoslavia, piratas informáticos de todo el mundo, sobre todo rusos y alemanes, se pusieron en contacto con el capitán Dragan, héroe nacional serbio durante la guerra de la Krajina (Croacia), líder del ejército de voluntarios en contra de los aliados, para ofrecerle sus servicios. "*Les pedí que nos ayudaran a atacar a los que nos estaban bombardeando. El segundo día (25 de marzo) las computadoras del portaaviones norteamericano Nimitz y el sistema informático principal de la OTAN fueron penetrados. Las páginas web de la Casa Blanca quedaron bloqueadas durante todo el fin de semana. Fueron demostraciones de fuerza que no tuvieron mucho efecto*", dice Dragan en un reportaje ofrecido por el diario EL MUNDO [9].

En [10] podemos ver como en 2007 Estonia sufrió un conjunto de ciberataques que, supuestamente respaldados por Moscú, colapsaron los servicios web de todo el país marcando un hito y un reto para la OTAN. La que se conoce ya como "ciberguerra estonia" fue motivada por el traslado del Soldado de Bronce de Tallin, que había sido levantado en agradecimiento a los soviéticos que liberaron a Estonia de los nazis. El problema para los estonios es que su país fue absorbido por la URSS y muchos estonios consideran invasores al Ejército Rojo. El ataque, inusitado por su envergadura, es estudiado hoy por muchos países y estrategas militares. El Ministro de Exteriores estonio acusó inmediatamente al Kremlin de estar detrás de la guerra informática desencadenada contra su país. Aunque hasta el momento no se sabe con certeza si el Kremlin estuvo detrás de los

ataques o no, los especialistas sostienen que, dada la magnitud del ataque, los piratas informáticos tuvieron que contar, al menos, con el visto bueno del Kremlin. Un año después de aquella guerra, en 2008, la OTAN decidió crear en Tallin el Centro de Excelencia para la Ciberdefensa [39], un proyecto en el que participa España junto a otros seis países para diseñar estrategias de defensa contra ataques por Internet. En el centro trabajan dos españoles, uno militar y otro civil, y funciona con presupuesto de Defensa de los países participantes.

Así mismo, la Alianza, elaboró por primera vez una "Política de Ciberdefensa" [11], aprobada en enero de 2008, que estableció tres pilares fundamentales en la política de la Alianza en el ciberespacio:

- La subsidiariedad, es decir, la asistencia se proporciona sólo a petición, de lo contrario, se aplica el principio de la soberanía de los estados con su responsabilidad propia.
- No duplicación, es decir, evitar la duplicación innecesaria de las estructuras o capacidades en los planos internacional, regional, y nacional.
- Seguridad, es decir, la cooperación basada en la confianza, teniendo en cuenta la sensibilidad de la información de los sistemas que deben hacerse accesibles y sus posibles vulnerabilidades.

En el Concepto Estratégico de la OTAN presentado en Lisboa (2010), se estableció que los ciberataques constituían una de las nuevas amenazas a las que debía hacer frente la Alianza y se estableció el Nuevo Concepto de Ciberdefensa de la Alianza [12]. Con las decisiones adoptadas, la Alianza estableció con éxito las bases para un examen de esta cuestión. De este modo, la OTAN no sólo proporcionaba una actualización muy necesaria a las estructuras existentes con capacidad de respuesta ante incidentes, sino que también comenzaba de forma conjunta, como una alianza, a enfrentarse a los retos, muy reales y en crecimiento, que plantea la ciberdefensa. En consonancia con el nuevo Concepto Estratégico, se revisó la Política de Ciberdefensa que define las amenazas informáticas como una fuente potencial para la defensa colectiva de conformidad con el artículo 5, del Tratado de Washington, de la OTAN. En febrero de 2012, se firmó un contrato de 58 millones de euros para establecer una Capacidad de Respuesta ante Incidentes Informáticos (NCIRC), plenamente operativa en octubre de 2013.

Durante la Cumbre de Chicago de 2012, los Jefes de Estado y de Gobierno reafirmaron su compromiso de mejorar la ciberdefensa de la Alianza protegiendo todas sus redes de forma centralizada y aplicando los elementos críticos de la capacidad operativa plena del NCIRC en octubre de 2013.

2.2.3 La ciberseguridad en el contexto de la UE.

En el informe del 17 de octubre de 2012 del Parlamento Europeo [13], sobre ciberseguridad y ciberdefensa (2012/2096 INI), el Parlamento Europeo sanciona que, dado el carácter globalizado del panorama internacional en la actualidad, la UE y sus estados miembros dependen de forma crucial de la seguridad en el ciberespacio y de un uso seguro de las tecnologías de la información. Las amenazas, los desafíos y los ataques cibernéticos están creciendo de manera exponencial hoy en día y éste es un problema que afecta tanto a la Administración Pública como al sector privado. La Agencia Europea de Defensa (EDA), considera la ciberdefensa como una de las prioridades máximas. La educación y concienciación de los ciudadanos es la base de cualquier estrategia de Defensa global, y el carácter sin fronteras de las redes requiere colaboración y cooperación internacional. También afirma que, ante un ataque importante a un Estado miembro, podría llevarse a cabo la aplicación de la cláusula de solidaridad (artículo 222 del TFUE Tratado de Funcionamiento de la UE) así como la cláusula de defensa mutua (artículo 42, apartado 7, del TUE, Tratado de la UE). Subraya también que los ataques realizados hasta ahora sobre la UE ya han causado pérdidas millonarias y cuantiosos daños a la UE. Además, señala la necesidad de crear equipos de respuesta a emergencias informáticas (CERT) dentro de la UE y CERT nacionales. Aparecen los primeros ejercicios para adiestramiento y reacción ante ciberataques de carácter conjunto.

En Alemania, según informes de McAfee [14], las pérdidas económicas alcanzan el 1,65% del Producto Interior Bruto. La ciberseguridad ha estado entre las prioridades de la agenda política de la UE desde ya hace bastantes años. Se podría fijar el comienzo en la Comunicación conjunta del Consejo y la Comisión de 2000. El Convenio de Budapest, firmado por España en el 2010, es universal y transatlánticamente el documento más importante en materia de ciberseguridad con objeto de armonizar el derecho y la persecución penal. En 2013 se publica la Estrategia de la Ciberseguridad de la Unión Europea. A principios del mismo año se crea el Centro Europeo de Lucha contra la Ciberdelincuencia que parte de la policía europea Europol como punto central para el tratamiento de los ciberataques y un CERT europeo que colabora con los diversos CERT nacionales.

La Estrategia de Ciberseguridad de la Unión Europea [15] señala cinco estrategias prioritarias:

- La resilencia contra ciberataques.
- La reducción de la delincuencia en la red.
- El desarrollo de una política de Ciberdefensa y las capacidades necesarias en el marco de la Política Común de Seguridad y Defensa (PCSD).
- El desarrollo de los recursos tecnológicos necesarios en ciberseguridad
- El establecimiento de una política internacional coherente del ciberespacio en la Unión Europea.

Lo que hace fuerte la política de la Unión Europea entorno a la ciberseguridad es la ciberdefensa. Para comprenderla hay que entender que se basa en la minoración y prevención de daños mediante la colaboración y cooperación público-privada. Es, por tanto, totalmente diferente a la implementada en Estados Unidos, fundamentada en la capacidad de disuasión y de lanzar ataques.

2.2.4 Conclusión.

Empresas, organizaciones e instituciones están expuestas cada día a ataques cibernéticos que pueden tener consecuencias devastadoras. Estos riesgos en la red podrían provocar un shock global similar a la crisis financiera de 2008. A esta conclusión han llegado los autores de un estudio elaborado por el Grupo Zurich, en colaboración con la Harvard Kennedy School [23]. En 2013, se calcula que 740 millones de datos pudieron ser robados en todo el mundo. El 89 % se podría haber evitado con los mecanismos y estrategias adecuados. Los más extremistas hablan de un posible *Pearl Harbor* cibernético o una Tercera Guerra Mundial librada a través de las redes.

El número de ataques que se llevan a cabo en nuestro país es muy elevado, del orden de decenas de miles de ataques y la tendencia es positiva, es decir, que es de esperar que, en los próximos años, el número sea mucho más elevado aún. Remarcar que el crecimiento es exponencial por lo que cabe pensar que son necesarias medidas que cambien esta tendencia, de otro modo la cantidad de ataques en un futuro no muy lejano será desorbitada. Es necesaria una concienciación masiva del estado actual de las vulnerabilidades que existen en torno a los sistemas de información para que se deje de creer que los ciberataques y la ciberdelincuencia son algo que sólo tiene cabida en las películas, tomando conciencia así de que la única forma de evitarlo es el protegerse activamente y teniendo unos conocimientos mínimos básicos. Igualmente la conciencia en cuanto al alcance que pueden tener estos ataques, que son capaces de poner en jaque a una ciudad entera o a un Estado, es totalmente necesaria, sabiendo que podría llegar a causar el caos. Los Estados ya han tomado conciencia y dentro de occidente, y entre los países más desarrollados, se encuentran pocos que no estén desarrollando una estrategia en ciberdefensa. Se han elaborado estrategias y planes que permiten crear una línea de acción de referencia común que facilita la comunicación entre los diversos países. También se han elaborado ejercicios a modo de simulacro, los cuales ya se están llevando a cabo, estableciendo así unos procedimientos y una doctrina común. Fruto de esta concienciación y de las líneas de acción que ya se trazan, los Estados están aportando los recursos necesarios para que todos estos proyectos se materialicen. Se está fomentando la formación en torno a la ciberdefensa y los programas desarrollados con este objeto, así como la investigación, el desarrollo y la innovación que permita

seguir el ritmo acelerado que marca la tecnología actual en su proceso de actualización y así, estar siempre un paso por delante de los cibercriminales. La finalidad con la que se realizan los ataques queda claro que es diversa, de la ciberdelincuencia al ciberterrorismo pasando por el ciberespionaje. Pero todos con un mismo resultado: la falta de seguridad en el ciberespacio de un Estado, que traerá consigo deficiencias en los derechos y privacidad de sus ciudadanos, o incluso la pérdida de información muy sensible a nivel de defensa o empresarial. Y, por último, de todo lo anterior expuesto también se concluye que es necesaria y vital la cooperación y colaboración entre diferentes Estados y organismos y, dentro de éstos, entre el sector público y privado de forma, y de este modo, que se logre estandarizar las respuestas y procedimientos haciendo más fácil el entendimiento y la colaboración y permitiendo que entre todos siempre se encuentre la solución ante los diversos ataques.

En cuanto a las previsiones futuras, el Director Regional de *Intel Security* en España, Javier Perea [16] apunta al robo de credenciales, el secuestro de datos o la guerra cibernética como los riesgos previstos más a corto plazo. Se pronostica un aumento muy notable del ciberespionaje con el fin de llevar a cabo el robo de la propiedad intelectual y la obtención de información privilegiada para venderla. Además los *hackers* están dejando de ser actores individuales y ya se organizan en pequeñas estructuras. Los *exploits* más recientes son los *ransomware*, los cuales cifran ficheros de un dispositivo inutilizándolos y pidiendo un pago por la reactivación en modo de bitcoin para que sea imposible la localización. Los móviles y tabletas se presentan como los dispositivos más "apetecibles" por lo personal de la información que contienen y el valor para usarlo como chantaje. La tecnología NFC (*Near Field Communication*) de pagos inalámbricos también es muy vulnerable a sufrir ataques. Los usuarios siguen siendo el eslabón más débil y, por lo tanto, el punto a explotar por los ciberdelincuentes.

2.3 Amenazas y retos en las redes.

En primer lugar, se pueden clasificar los ataques o amenazas dependiendo de si alteran el tráfico entre el usuario y los servidores o no. Los ataques pasivos son aquellos en los que el atacante no modifica la información que circula por la red. En este tipo de ataques, el atacante simplemente se coloca a la escucha monitorizando todo el flujo de información, siendo capaz de recopilarlo y analizarlo. Este suele ser el primer paso a la hora de recopilar toda la información posible, incluso capturando claves y nombres de usuario empleados por la víctima. El ejemplo más claro es el ataque conocido como *sniffing*.

La web profunda [18], es un punto de encuentro conocido entre *hackers* e interesados en ejecutar alguno de estos ataques sobre una organización, sin contar con los conocimientos necesarios. La conforman el conjunto de recursos y páginas web que quedan fuera de los buscadores por no estar indexadas. Esto quiere decir que si realizamos la búsqueda de palabras relacionadas con su contenido, los motores de búsqueda más conocidos como Google o Yahoo no nos ofrecen estas páginas y hay que conocer, por tanto, su dirección concreta para acceder a ellas. Esto se debe a varios motivos. En algunos casos, son estos propios buscadores los que deciden dejarles al margen por el contenido de estas páginas. En otros casos, sin embargo, son los propios dueños de las páginas los que prefieren permanecer en el anonimato y cifran sus páginas con contraseñas de modo que permanecen en la sombra. También cabe destacar que la mayoría de las páginas en la web profunda se encuentran en diferentes capas de modo que el usuario va saltando de unas a otras mientras su IP, su dirección con la que es posible identificarlo, permanece por lo tanto oculta. Este anonimato hace de la web profunda el hogar ideal de la delincuencia [19] en el Ciberespacio pudiendo encontrar todo tipo de actividades ilícitas, tráfico de armas, tráfico de drogas, tráfico de órganos, distribución de contenido pederasta, etc. El único modo de realizar una búsqueda en esta red es usando Tor, *The Onion Router*, cuyo nombre proviene de su modo de funcionamiento, ya que, al acceder, la información personal del usuario se cifra en capas, quedando oculta. Tor nace fruto de un proyecto de la Marina de los Estados Unidos en 2002 con el fin de proteger las comunicaciones gubernamentales y para apoyar el espionaje. Hoy en

día permanece como Tor Project, una organización sin ánimo de lucro cuyo fin es capacitar el acceso libre a la red manteniendo la privacidad y el anonimato.

En los ataques activos, el atacante modifica el flujo de información que está teniendo lugar a través de la red. Esta alteración suele ir asociada a uno de los siguientes objetivos:

- Suplantación de la identidad. El atacante se hace pasar por un punto de acceso, un servidor o un administrador, con el fin de que la víctima encamine hacia su equipo todo el tráfico de datos, o abra un *malware* o virus que le haga ceder alguna clave o usuario y permita el control de su equipo en remoto o el acceso a sus ficheros.
- Alteración del contenido de un mensaje. Puede ser útil para crear cierto caos en una organización o conseguir que la víctima realice ciertas actividades que le solicite un supuesto administrador o jefe.
- Denegación de servicio (DoS). El atacante, normalmente, deja al usuario sin acceso a un servidor o computadora haciendo uso de todo el ancho de banda de la red de la víctima. Satura los puertos con un flujo de datos que el servidor no es capaz de procesar sin sobrecargarse. Por esta razón, el servidor es incapaz de continuar trabajando con normalidad y deja de prestar servicio.
- SQL *injection*. Cuando una serie de usuarios se comunican con una página web, lo hacen a través de aplicaciones que utilizan bases de datos. Para tener acceso a estas bases de datos, el usuario ha de autenticarse. Pero un *hacker* puede realizar lo que se conoce como una inyección SQL: puede inyectar un código intruso a través del proceso de identificación, sin necesidad de *password*, y así, realizar diferentes operaciones en diferentes tablas, dentro de la base de datos, siempre que la página cuente con alguna vulnerabilidad.

Dentro de las redes inalámbricas, encontramos las siguientes amenazas [20]:

1-*Warchalking y wardriving*. Se denomina *warchalking* a una práctica generada a la par que se desarrolló la tecnología WiFi (*Wireless Fidelity*) en los países anglosajones, la cual consistía en marcar en las paredes desde donde se tenía cobertura de algún punto de acceso con un dibujo y unas letras. Indicaban si se trataba de un nodo abierto o cerrado y, en su caso, el nombre de la red ESSID (*Extended Service Set Identifier*), el ancho de banda o el tipo de cifrado. Del mismo modo, se desarrolló el *Wardriving*, consistente en ir detectando todos los puntos de acceso WiFi existentes en una zona desde un dispositivo inalámbrico, circulando en coche. Para ello, es necesario que este dispositivo cuente con una tarjeta de red capaz de entrar en modo monitor y suele acompañarse de un GPS para ir registrando además la zona en la que se encuentran. Se genera un mapa interactivo con posibles puntos de acceso y sus propiedades como el que se muestra en la Figura 2-3. Aunque, a primera vista, estas actividades puedan parecer de las menos importantes, además de la actividad ilícita que supone el uso del ancho de banda de un individuo con los daños que se le causa, no hay que obviar que se puede utilizar esta información para terminar usando estas redes WiFi como punto para lanzar un virus o *malware* o crear una red de *zombies*. Los *zombies* son aquellos ordenadores que han sido infectados y que infectan a otros, expandiendo así el *malware* por toda la red. Se consigue así expandir el *malware* por todo el planeta, pudiendo, en último lugar, emplear todos estos ordenadores para implementar un ataque de denegación de servicio, tan potente como el número de computadoras que se haya logrado infectar. Recordemos el famoso *I Love You* que se expandió por toda la red en el año 2000.

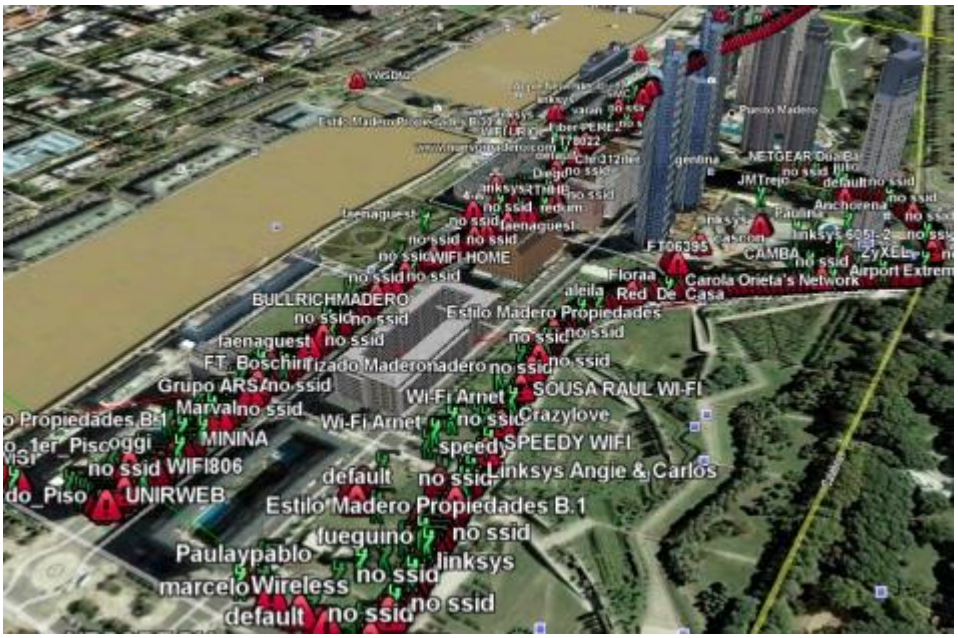


Figura 2-3 Ejemplo *Wardriving* recopilación de WiFi en un área. [40]

2-DoS ataque de denegación de servicio. Si se trata de una red inalámbrica, esta DoS se puede lograr con un productor de ruido que deje "ciego" al usuario, siendo incapaz de recibir el servicio. También se puede llevar a cabo por un flujo continuo del proceso de autenticación que deje al punto de acceso fuera de servicio debido a la gran cantidad de datos que requiere este procesamiento que, elaborado de forma continua, incapacita al punto de acceso. También se puede modificar el tráfico en la red, desviándolo del usuario y dejándolo sin servicio. Otra forma de llevarlo a cabo es dejar al usuario desacreditado en una lista de usuarios no permitidos que le niegue el acceso. Son difíciles de detectar y evitar, fáciles de implementar, suelen durar poco tiempo y son bastante demandados, llegando a ofertarse estos servicios vía Internet para dejar a cierta organización sin servidores en cierto momento clave por un módico precio. Estos servicios no se encuentran en el Internet de uso común, pero sí en la web profunda donde se considera que se encuentra el 95% de la información que circula por internet debido al supuesto anonimato que ofrece.

3-La falsificación de identidades. Bien se ataca al punto de acceso haciéndole creer que el atacante es uno de los usuarios o bien se ataca a uno de los usuarios haciéndole pensar que el atacante es el punto de acceso.

3.1-*Honeypots*. Lo primero que se debe hacer es negar el acceso a cualquiera de los usuarios de nuestra red a los puntos de acceso que utiliza habitualmente. Además los atacantes tratan de crear los conocidos como *honeypots*, puntos de acceso con igual nombre ESSID que el del usuario pero con mayor cobertura por lo que, a la hora de tratar de acceder, el usuario elegirá el punto de acceso malicioso entregando información sensible como usuario y contraseña. Un usuario malicioso colocará en las proximidades a nuestro WiFi su punto de acceso de forma que pueda recopilar nuestra actividad a la vez que se ofrece para que usuarios de nuestra red intenten acceder a este punto de acceso malicioso. Esta actividad se respalda en el derecho que tienen otros usuarios como nuestros vecinos u otros usuarios de tener otros puntos de acceso.

3.2-*MAC Address spoofing*. Cuando el mecanismo de protección de un punto de acceso consiste en limitar el acceso según la MAC, el atacante captura la MAC de uno de los clientes y espera a que éste se desvincule del punto de acceso para simular tener su MAC y acceder.

3.3-*MIM (Man in the Middle)*. Con este ataque, el atacante se coloca entre el usuario y el punto de acceso siendo un punto de paso de todo el flujo de datos. Así, el atacante puede decidir entre permanecer a la escucha visualizando todo el traspaso de información y pudiendo obtener información

de interés o interactuar y modificar la información que el usuario requiere o simplemente haciendo que ésta se pierda y nunca llegue a su destino.

4-Robo de información, *sniffing*. Consiste en la utilización de un programa capaz de capturar todo el tráfico que circula por una tarjeta de red. Esto es posible debido al funcionamiento por defecto del protocolo Ethernet, el cual envía todos los paquetes en *broadcast* y es cada ordenador el que, según la cabecera, acepta el paquete o no. Por lo tanto, basta con poner la tarjeta de red en modo monitor para que acepte todo el tráfico que le llegue. Además, estos programas van almacenando la información permitiendo su filtrado posterior, mostrando por pantalla la que circula por los puertos más comunes o que deseemos, y permitiendo así la posterior interpretación y análisis.

En la Figura 2-4 vemos una captura del programa *airodump* realizando *sniffing*. Se aprecian los diferentes puntos de acceso inalámbrico y los distintos usuarios en la parte inferior de la captura, en el apartado *station.*

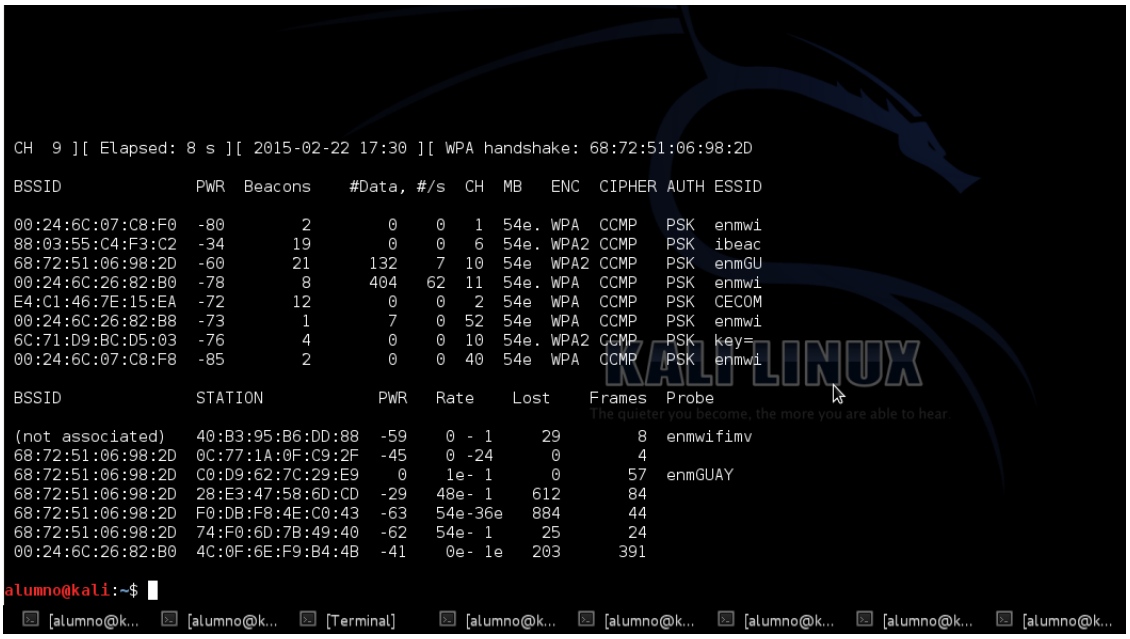


Figura 2-4 Ejemplo de *Sniffing* con *airodump*

5- Ataques de intrusión. Este ataque consiste en acceder a una red, a la que se tenía el acceso denegado, por medio de la ruptura de alguna clave de acceso o explotando alguna de las vulnerabilidades. El ataque básicamente consiste en monitorizar el flujo en la red a través de una tarjeta de red en modo promiscuo. Una vez capturado dicho tráfico, se lanzará un ataque de denegación de servicio sobre alguno de los clientes, los cuales intentarán acceder de nuevo. Es, en este momento, en el que se captura el *arp request* o el *handshake*. Al capturar esta solicitud, el atacante será capaz de la contraseña de acceso a la red mediante un ataque de fuerza bruta, de diccionario o un análisis de las tramas.

2.4 Plataformas para *pentesting*.

Existe un amplio número de plataformas en el mercado las cuales integran numerosas herramientas para la realización de las auditorías. Entre otras, podemos mencionar *Kali Linux, BackBox, NodeZero, Pentoo, Parrot Linux, ArchAssault,* etc.

Se describen las tres principales a continuación:

2.4.1 Kali Linux.

Kali [36] es una distribución Linux diseñada para su empleo en el ámbito de la seguridad informática. Como la mayoría de distribuciones Linux, es de código abierto y gratuito así como la mayoría de sus herramientas.

Figura 2-5 Kali Linux.

En *Kali Linux,* los usuarios son creados por defecto con privilegios de súper usuario *root*. Este sistema operativo contiene una gran colección de herramientas dedicadas a la auditoría informática entre las que se encuentran las populares *Hydra, Maltego, Ettercap* o *Zaproxy*. *Kali Linux* fue desarrollada para continuar la sexta distribución de *Backtrack*. Sin embargo, mientras *Backtrack* estaba basada en la distribución Ubuntu, Kali está basado en Debian, considerada más segura y eficiente, aunque menos intuitiva que Ubuntu. Además, se facilitaron los accesos, haciéndola más agradable de manejar, y se actualizaron los programas, corrigiendo errores y añadiendo nuevas funcionalidades. Está fundada y mantenida por *Offensive Security*. *Kali* cuenta con más de 300 herramientas para su empleo por el *pentester*. De todas las herramientas con las que contaba *Backtrack*, en *Kali Linux* sólo se han incluido las que mejor funcionaban y cumplían con los estándares de desarrollo seguro. El desarrollo seguro consiste en que los *scripts* o herramientas solamente realicen las actividades para las que están diseñados sin permitir realizar ningún otro tipo de actividad diferente o maliciosa o que atente contra la seguridad del equipo que la ejecuta. El equipo de desarrollo de *Kali* es un grupo reducido de personas con alto nivel técnico y de personas de confianza. El entorno es completamente personalizable permitiendo así adaptarlo a cada usuario; incluso permite alterar la configuración *kernel* según el criterio de aquellos usuarios avanzados. Posee una lista con las diez herramientas más utilizadas (“*Top 10 security tools”).*

2.4.2 BackBox.

BackBox [35] es otra de las distribuciones Linux para *pentesting,* está basada en Ubuntu y es altamente configurable. Es de origen italiano. Presenta un conjunto completo de herramientas estando disponibles, frecuentemente, nuevas actualizaciones. Cuenta con menos seguidores que *Kali Linux* por lo que encontrar información o soporte para actualizar alguna de sus herramientas o encontrar consejo

en su empleo puede ser más complicado. Comparte gran cantidad de las herramientas que encontramos en *Kali Linux* como *ettercap, wireshark, sqlmap, se-toolkit*, etc.

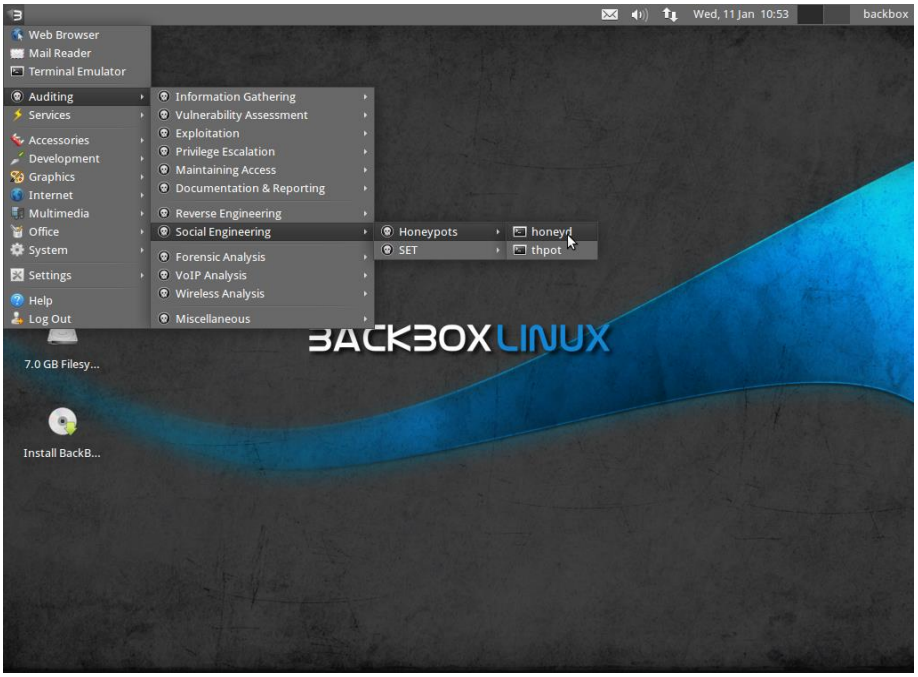


Figura 2-6 Escritorio de *BackBox*. [41]

2.4.3 NodeZero.

NodeZero [37] también viene de la mano de Linux, basada en Ubuntu y, al igual que las mencionadas anteriormente, contiene un gran número de herramientas para las pruebas de penetración. *NodeZero* usa los repositorios de Ubuntu para que su sistema esté siempre al día. La configuración del sistema es básica y permite cierta personalización. De igual modo, cuenta con menos adeptos que *Kali Linux* por lo que existe menos información en la red y menos soporte a la hora de interactuar con la plataforma. El equipo de desarrollo no recomienda su implementación a través de USB o CD si se pretende trabajar con la plataforma a pleno rendimiento: se deben instalar en un equipo si se pretenden realizar auditorías con una frecuencia considerable.

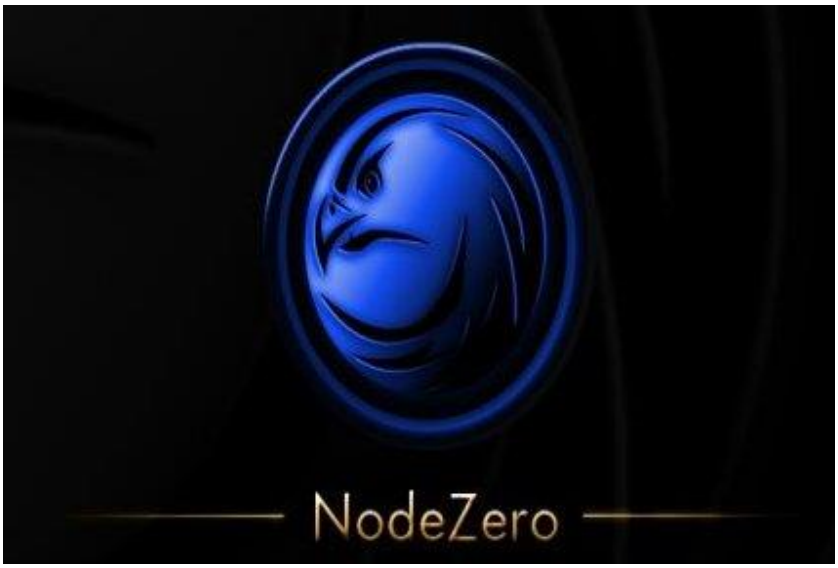


Figura 2-7 Icono de *NodeZero* Tomada de [42]

2.5 Herramientas para el *pentesting*.

Existen una serie de herramientas que capacitan al auditor para elaborar el análisis de seguridad de las redes. Estas herramientas permiten la recolección de información, conocer los puntos de acceso disponibles y sus propiedades, acceder a los servidores, interacción con los usuarios, información de estos, topología, tráfico en la red, etc. Permiten, también, el análisis de las vulnerabilidades existentes, la ruptura de claves de acceso, ataques a conexiones inalámbricas, explotación de las vulnerabilidades halladas, envenenar el tráfico en la red, crear puertas traseras o túneles por los que lograr acceder. A continuación, se presentan algunas de las más utilizadas con una breve descripción de sus propiedades y capacidades.

2.5.1 Nmap.

Nmap [24] (*Network MAPper*) es una herramienta para exploración y auditoría de seguridad de redes TCP/IP. Es un escáner de puertos de código abierto válido para sistemas multiplataforma.

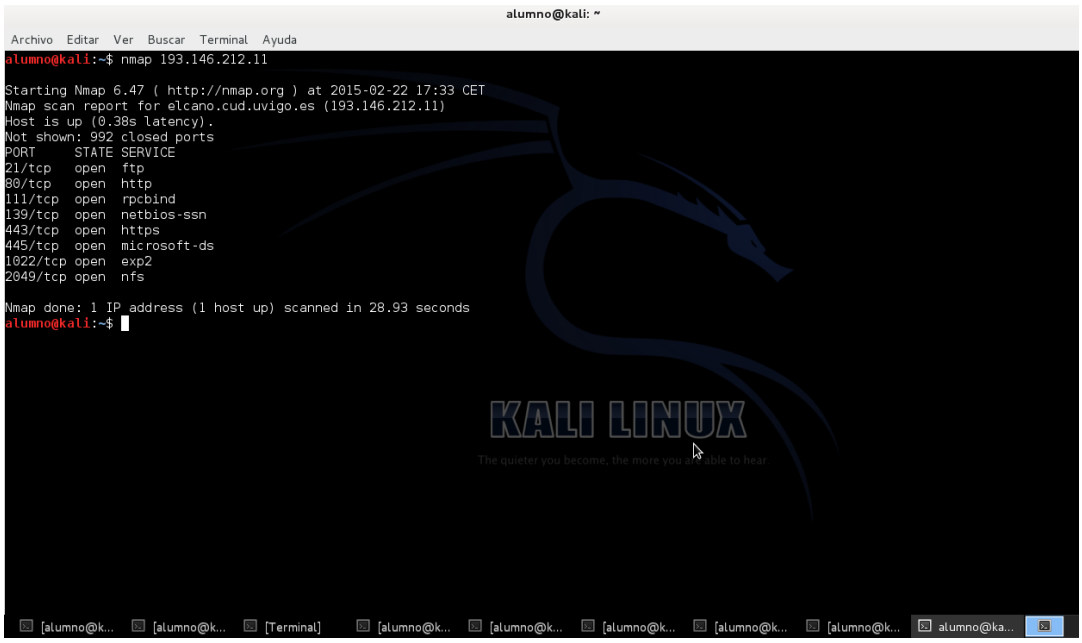


Figura 2-8 Escaneo simple con *Nmap* mostrando los puertos abiertos.

Es uno de los más empleados debido a las capacidades que posee. Trabaja tanto bajo línea de comandos como con interfaz gráfica en su versión *Zenmap*. *Nmap* es capaz de identificar el sistema operativo del equipo escaneado usando la huella TCP, de descubrir aquellos puertos que se encuentran abiertos y qué servicios son los que se encuentran a la escucha. Es capaz de detectar la topología de una subred, qué puertos están cerrados o cuáles tienen algún tipo de cortafuegos y algunas características del hardware, entre otras. Sus amplias capacidades le permiten operar de forma eficaz y realizar un escaneo sigiloso. El formato de comando de *Nmap* responde a la siguiente sintaxis:

```
Nmap –técnicas –opciones –modificadores objetivos
```

En *Nmap* se definen las siguientes técnicas: técnica de descubrimiento de equipos y técnicas de escaneo de puertos.

Los objetivos se especifican mediante URL (*Uniform Resource Locator*), IP, intervalo de direcciones IP separadas por un guión, o bloque de direcciones en CIDR (*Classless Inter-Domain Routing*) (192.168.0.0/24).

Un puerto abierto es aquel en el que se encuentra un servicio a la escucha de un paquete TCP o UDP (*User Datagram Protocol*). Un puerto que sea alcanzable pero que no tenga un servicio a la escucha será considerado un puerto cerrado. Si enviamos una sonda y no recibimos respuesta se debe a

que existe un elemento que bloquea la comunicación, un cortafuegos, por lo que el puerto aparecerá como filtrado. Además, *Nmap* permite utilizar un equipo como señuelo y dejar registrada otra IP que no sea la nuestra en los logs del equipo sondeado para enmascarar nuestro ataque.

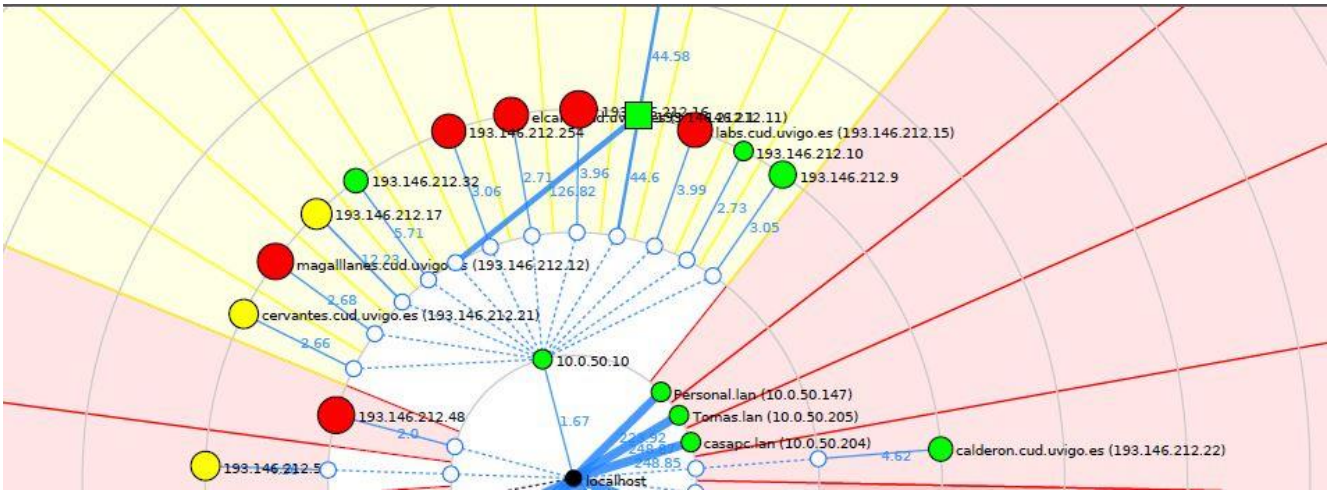


Figura 2-9 Topología de la red obtenida con *Zenmap* desde uno de los puntos de acceso inalámbrico.

2.5.2 La suite air.

La *suite air [25]* se trata de un conjunto de software de seguridad inalámbrica que incluye un analizador de paquetes de red, un crackeador de redes con cifrado WEP (*Wired Equivalent Privacy*), WPA/WPA2-PSK (*WiFi Protected Access/Pre-Shared Key*) y un conjunto de herramientas para la auditoría inalámbrica. *Aircrack-ng* es un crackeador de contraseñas, usa la inyección de tráfico para descifrar las claves WEP y la captura del *handshake* para las WPA/WPA-PSK y el posterior descifrado usando diccionarios o por medio de la fuerza bruta. *Airodump-ng* escanea las redes inalámbricas existentes y permite la captura del tráfico inalámbrico permitiendo la identificación de las diferentes BSSID (*Basic Service Set Identifier*) asociadas a sus ESSID y de los clientes en cada una, permitiendo también la captura de tráfico selectiva en una sola BSSID.

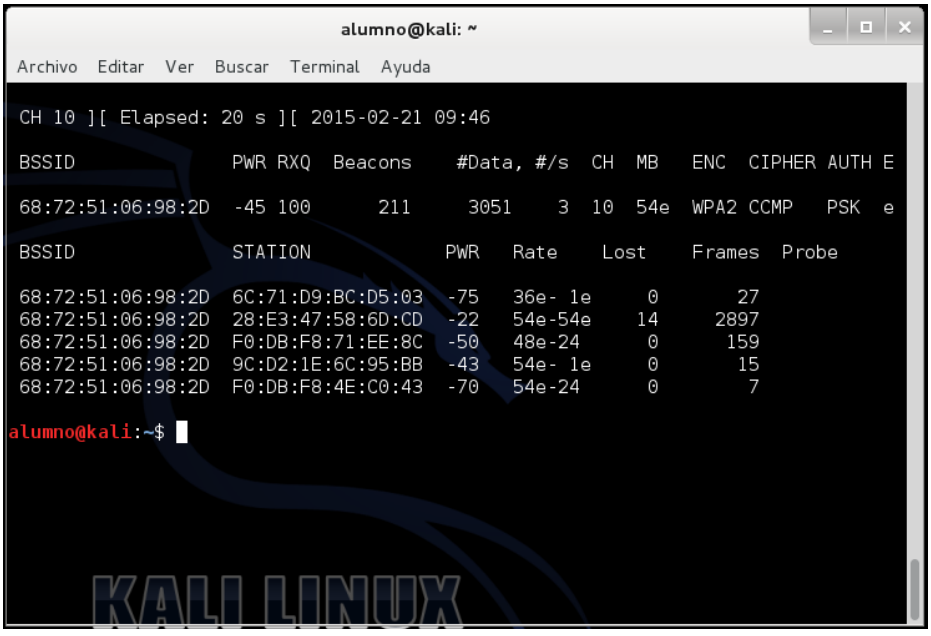


Figura 2-10 Captura de tráfico inalámbrico con *Airodump-ng*.

Los campos que proporciona *airodump* son los siguientes:

- Bssid. Identifica la dirección MAC de un punto de acceso.
- PWR. Intensidad de la señal.
- Beacons. Número de paquetes *broadcast* enviados por el AP (*Access Point*).
- Data. Número de paquetes de datos. En WEP, solo cuentan los IVS (*Vectores de Inciciación*).
- #/s. Paquetes por segundo.
- CH. Canal.
- MB. Velocidad mínima soportada por el punto de acceso.
- ENC. Algoritmo de cifrado. Puede ser OPN (Open), WEP, WPA o WPA2.
- CIPHER. Tipo de cifrado. Puede ser WEP, TKIP (*Temporal Key Integrity Protocol*) (WPA) o CCMP (*Counter Mode Cipher Block Chaining Message Authentication Code Protocol)* (WPA2).
- AUTH. Método de autentificación. PSK en lugares con clave compartida.
- ESSID. Nombre de la red Wi-Fi.
- Station. Dirección MAC de un cliente asociado al punto de acceso.
- Probe. Son los paquetes en los que un cliente intenta identificar una red Wireless, gracias a los cuales se puede obtener el nombre de las redes que un cliente está buscando e intentar verificar que se encuentran en su radio de ataque.

Con esta herramienta podemos capturar todo el tráfico de la red inalámbrica.

Airmon-ng permite establecer la tarjeta de red en modo promiscuo de forma que capture todo el tráfico existente capacitando a *airodump-ng* a realizar su trabajo.

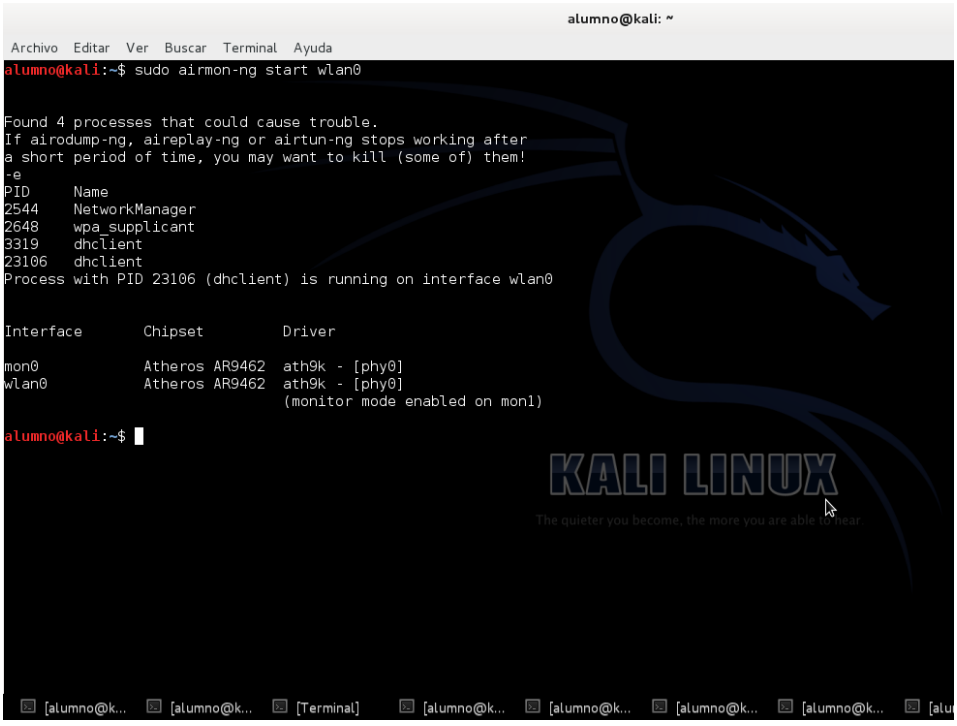


Figura 2-11 Establecido el modo monitor *mon1* con *Airmon-ng*.

Con *aireplay-ng* se pueden inyectar paquetes. Su función principal es generar tráfico para usarlo más tarde con *aircrack-ng* y poder crackear claves WEP y WPA-PSK. Hay varios ataques diferentes que se pueden utilizar para hacer desautenticaciones con el objetivo de capturar un *handshake* WPA, para realizar una falsa autenticación, un reenvío interactivo de un paquete o una reinyección automática de un *ARP-request*. Con el programa *packetforge-ng* es posible crear paquetes *ARP request* de forma arbitraria.

2.5.3 Setoolkit.

La ingeniería social consiste en conseguir información confidencial a través de la manipulación de usuarios. Con esta información, el atacante puede obtener acceso o privilegios en sistemas de información de forma que se exponga o comprometa la seguridad del organismo. Este concepto se sustenta en el fundamento de que toda cadena es tan fuerte como su eslabón más débil y el eslabón más débil de toda organización es el individuo. Se tratará de obtener esta información mediante correos maliciosos pidiendo al usuario que se autentique con nombre de usuario y contraseña, llamadas telefónicas, control de acceso a redes sociales, etc.

Setoolkit [26] (Social Engineer Toolkit) es una completísima suite para explotar la ingeniería social. Nos permite automatizar tareas, desde el envío de SMS falsos a clonar páginas web. Por ejemplo, desde correos maliciosos o falsas páginas web se le solicitará al usuario que acceda con su usuario y contraseña, siendo estos redirigidos al atacante.

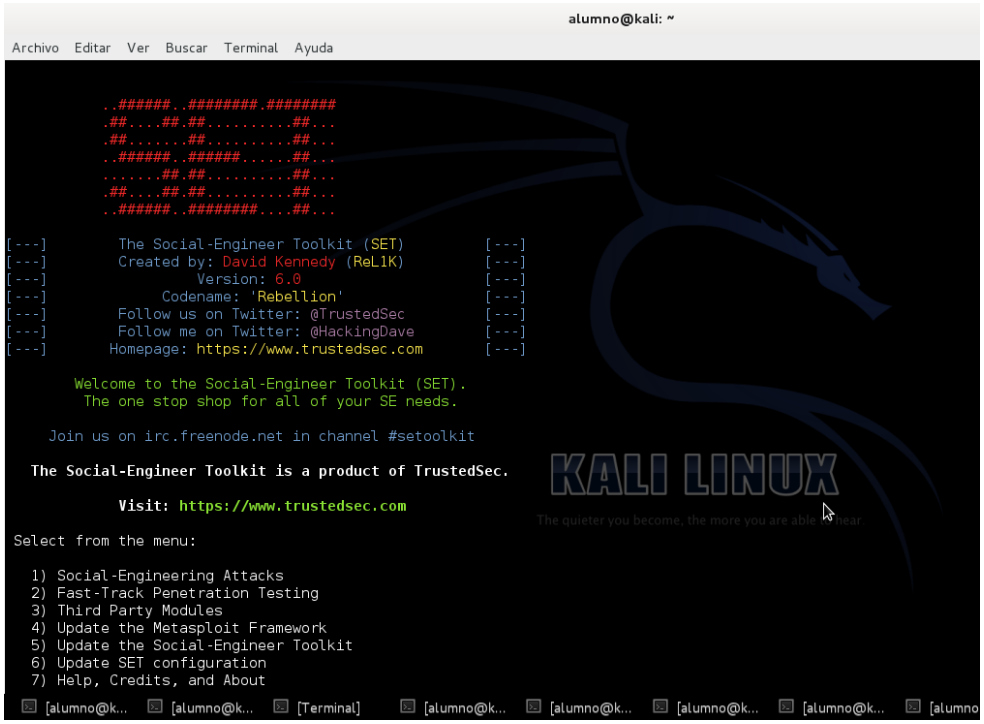


Figura 2-12 Menú de inicio de *Setoolkit*.

2.5.4 Owasp Zap.

Owasp Zap [27] es una herramienta libre escrita en Java que permite realizar test de penetración en aplicaciones web, recomendada para aquellos que se están iniciando en el *pentesting*, ya que realiza la búsqueda de vulnerabilidades en la web prácticamente en automático con poco más que indicarle la URL a testar. Esta aplicación realiza un escáner activo. Esto se traduce en que va probando todo tipo de ataques en toda URL descubierta. Estas URL las detecta con un *spider* que se dedica a buscar en toda la web en busca de diferentes URL y sus propias vulnerabilidades. Con *forced browsing* intenta descubrir todos los archivos y directorios no indexados en el sitio como páginas de inicio de sesión. Termina con un informe en forma de alertas clasificando las diferentes vulnerabilidades detectadas.

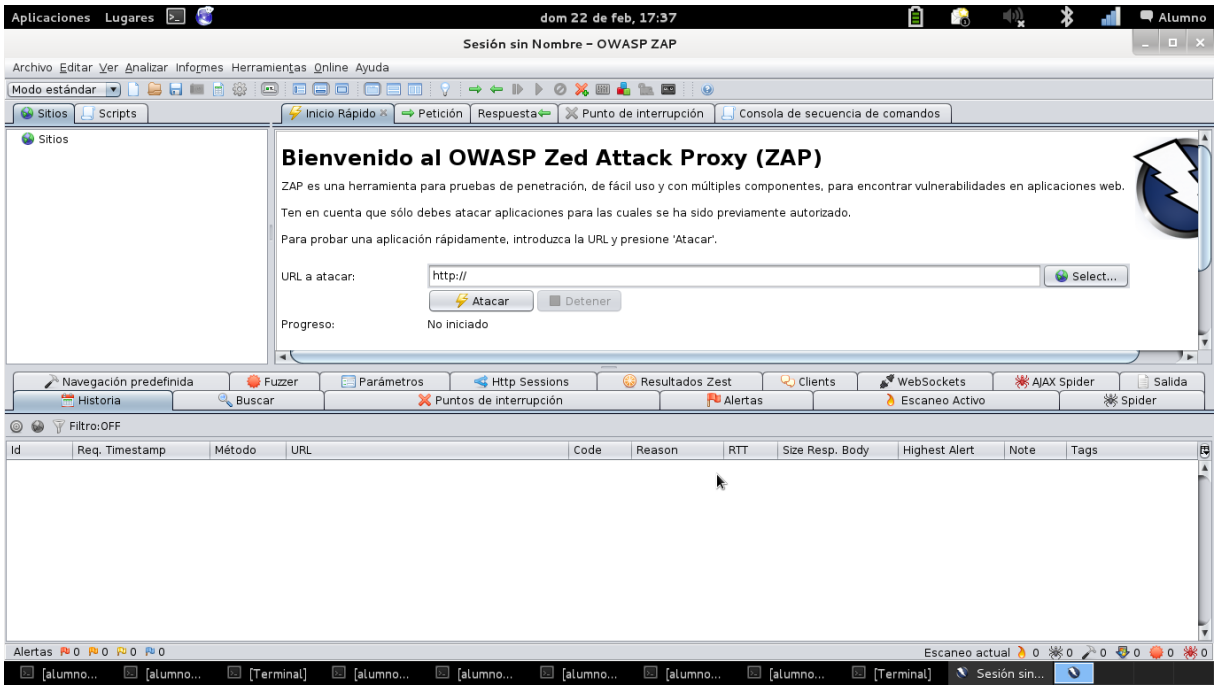


Figura 2-13 Pantalla de presentación de *Owasp Zap*.

2.5.5 Maltego.

Maltego [28] es una de las herramientas principales para el *gathering* o recogida de información. Es capaz de enlazar información de diversas fuentes y obtener el mapa de la infraestructura que hay detrás de un determinado dominio. Es capaz de conseguir correos, usuarios y sitios web donde se han utilizado estos correos. Sondea redes sociales como *Twitter* y *Facebook* y, a través de estos, incluso intenta la geolocalización. Se basa en la ingeniería inversa y en el uso de las transformadas, así nos permite aplicar gran cantidad de transformadas siendo capaces de ir desglosando la estructura de la red y la dependencia entre hosts. Una transformada es una unidad conceptual que realiza determinadas búsquedas para recolectar toda la información posible. Estas transformadas buscan en Internet información indexada dentro de su ámbito. Por ejemplo, *phone numbers*, buscará información acerca de los números de teléfono.

Figura 2-14 Pantalla de presentación de *Maltego*.

2.5.6 Nikto.

Nikto [29] es considerada una de las mejores herramientas de auditoría web. Su sintaxis de utilización es `<nikto -h pagina_web>`. Lanza un escaneo de todo el sitio web detectando la versión del servidor, la tecnología utilizada, vulnerabilidades, etcétera. Su uso, junto a otras herramientas como *Nmap* y *Metasploit*, facilita en gran parte la tarea de explotación. Con el *Scan tunning*, podemos personalizar el escaneo para reducir el ruido generado por la herramienta. Estos son algunos de los tests que realiza:

-Archivos de interés

-Fallos de configuración

-Descubrimiento de información

-Inyecciones

-Obtención de archivos remotos

-Denegación de servicio

-Ejecución de comandos

-Inyección SQL

-Subida de archivos

-Evasión de autenticación

-Identificación de software

-Inclusión de código remoto

También realiza descubrimiento de interfaces de administración y páginas de login conocidas, que pueden ser objeto de ataques de fuerza bruta.

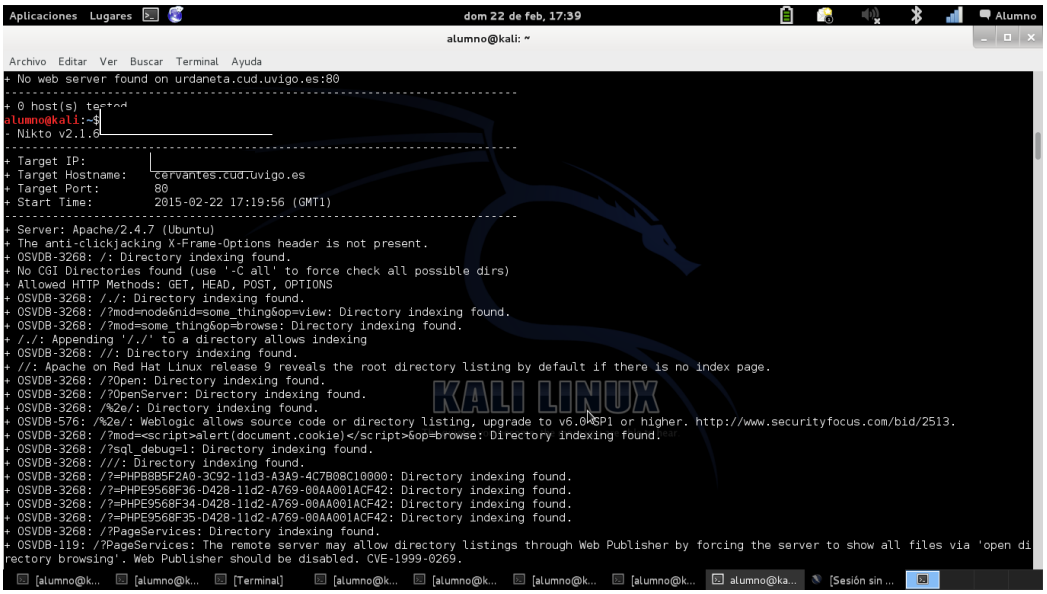


Figura 2-15 Escaneo con *Nikto* en el servidor *Cervantes*.

2.5.7 WhatWeb.

WhatWeb [30] es una herramienta que sirve para identificar los sitios web. Se basa en el reconocimiento de la tecnología aplicada en la página web. Gestores de contenido, blogs, análisis de paquetes, librerías javascript, servidores web y dispositivos embebidos son detectados empleando *whatweb*. La sintaxis de utilización es `<whatweb -v pagina_web>`. Al detectar los gestores de

contenido, nos está detectando posibles vulnerabilidades que podremos auditar con mediante otras herramientas como *Nikto*.

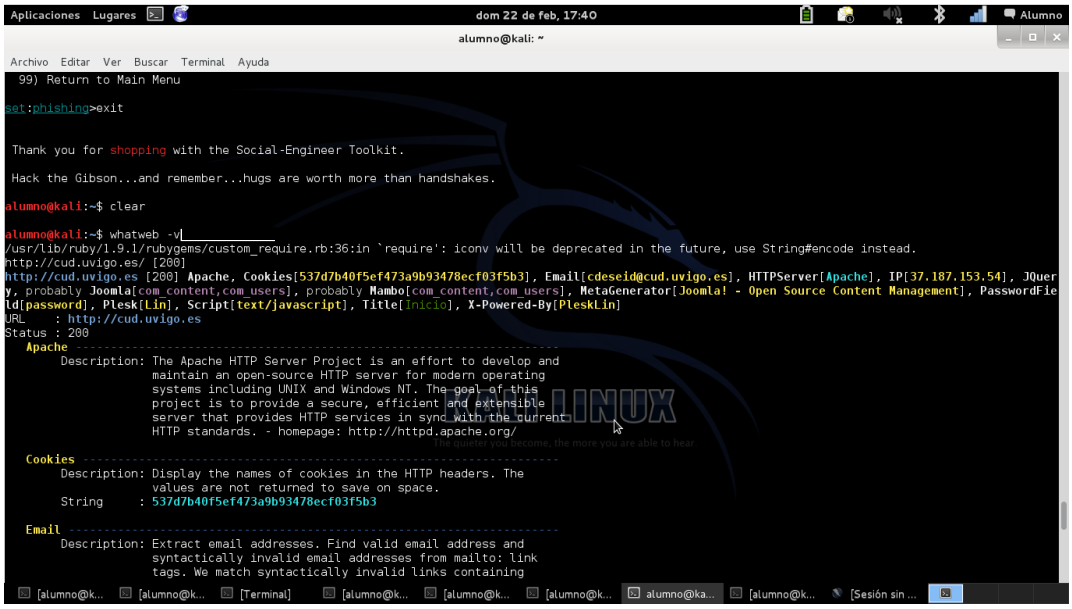


Figura 2-16 Análisis del sitio web del CUD con *WhatWeb*.

2.5.8 Ettercap.

Ettercap [32] es un interceptador para LAN (*Local Area Network*) que permite capturar el tráfico en una red, tanto física como inalámbrica e incluso inyectar datos en el proceso de comunicación interceptado. Su mayor potencial es la facilidad con la que permite implementar un *MIM* paso a paso, mostrando las posibles víctimas, realizando el envenenamiento de la tabla *arp* y llevando a cabo toda la captura del tráfico de forma gráfica. Variando algunos parámetros dentro de su configuración podemos lograr que muestre por pantalla de forma explícita el usuario y contraseña de alguna de las víctimas que hayan enviado sus credenciales a través de la red. Ofrece varias posibilidades más, entre ellas, tenemos la opción de envenenar la configuración del *DNS* (*Domain Name System*) que le ofrecemos a la víctima para redirigirlo a la página que deseemos. Combinado con otra herramienta como *drifnet*, podemos llegar a monitorizar todas las imágenes que los usuarios de la red atacada estén visualizando en su pantalla. También permite invalidar alguna de las conexiones, o todas, que esté realizando un usuario llevando a cabo un DoS. Por último, mencionar que es una herramienta de código abierto, cuyos desarrolladores buscan colaboradores para desarrollar dicho código. No es compatible con el sistema operativo Windows.

Figura 2-17 Logotipo de *Ettercap*

2.5.9 Metasploit.

Tras haber realizado la recogida de información y los análisis de vulnerabilidades en la red a testar, llega el momento de analizar esta información, que será clave en el desarrollo de la auditoría. Se debe analizar minuciosamente en busca de cualquier posible fallo o punto débil en las defensas de la red. Una vez encontrados estos, se procede a explotarlos, es decir, utilizar herramientas que permitan obtener la información que estábamos buscando, el acceso a los servidores, a sus computadoras, al control en remoto de sus sistemas; sus contraseñas. En definitiva, a hacerse con el mayor control posible del sistema. En ocasiones, se irá "pivotando", ganando un mayor control yendo de un usuario a otro, o de un equipo o red a otro, una vez que se logra acceder. Las herramientas que se utilizan para explotar estas vulnerabilidades se conocen como *exploits*.

Metasploit [31] es una de las herramientas más conocidas con esta finalidad. Nos ofrece multitud de *scripts* adecuándose a la vulnerabilidad encontrada según el servicio que esté usando y el sistema operativo. Un *exploit* es una aplicación que nos permite explotar una vulnerabilidad, un código escrito que usaremos para aprovecharnos de un fallo de implementación. Se puede lograr dejar inoperativa una aplicación, modificarla, obtener información sensible de una base de datos o el objetivo principal, hacerse con el control remoto de la computadora. El *exploit* sirve como "pasarela" a un *payload* o *shellcode*, un código que se ejecuta en la máquina atacada. Con un poco de práctica, su uso es sencillo. Existe una aplicación muy interesante, *searchsploit*, la cual realiza búsqueda de *exploits* según la plataforma, aplicación o protocolo.

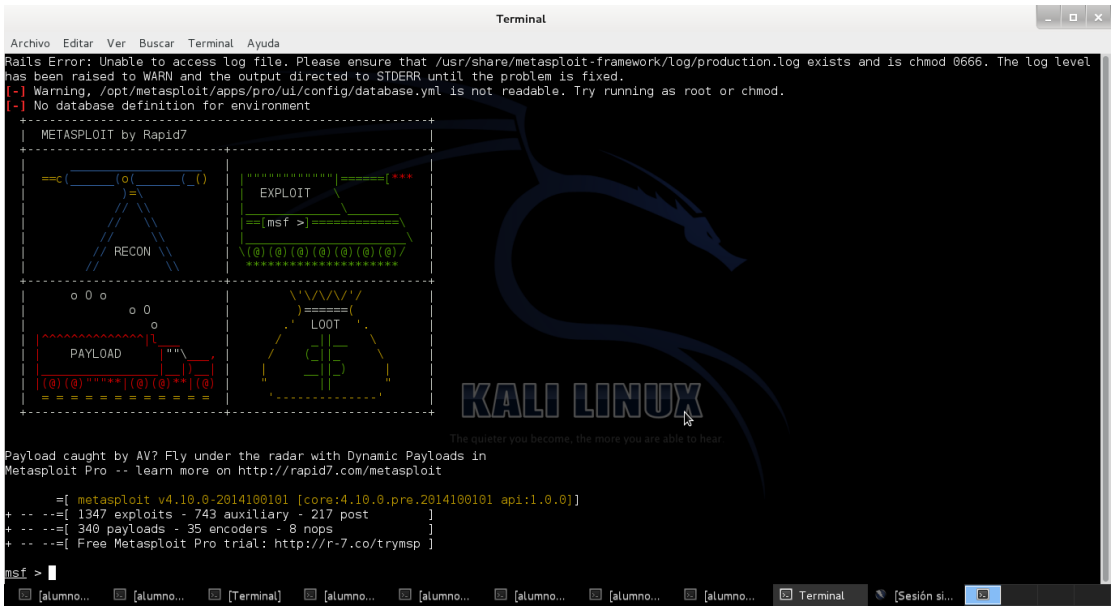


Figura 2-18 Presentación inicial de *Metasploit.*

2.5.10 Armitage.

Armitage [33] es una herramienta que combina las posibilidades que nos ofrece *Metasploit*, en una vertiente gráfica, en la que nos presenta posibles objetivos, nos recomienda *exploits* a utilizar y nos permite el empleo de acciones de la fase de post explotación. Nos permite realizar un gran número de pruebas de las que conforman el test de intrusión. Es posible realizar escaneos de una IP o de un rango de ellas, tanto con *Nmap*, como con *Metasploit.* Después podemos realizar una búsqueda de los posibles ataques que podemos llevar a cabo sobre cada uno de los *host.* Nos permite ver los diferentes servicios que están trabajando en cada uno de los puertos abiertos que encontremos. Podríamos pasar a lanzar estos ataques a través de los *exploits* y ver los resultados pudiendo llegar a abrir una *Shell* en

remoto. También es posible pivotar entre los diferentes equipos que componen la red y escalar en ésta, ganando mayor accesibilidad y privilegios. Es una herramienta muy completa, de uso sencillo e intuitivo.

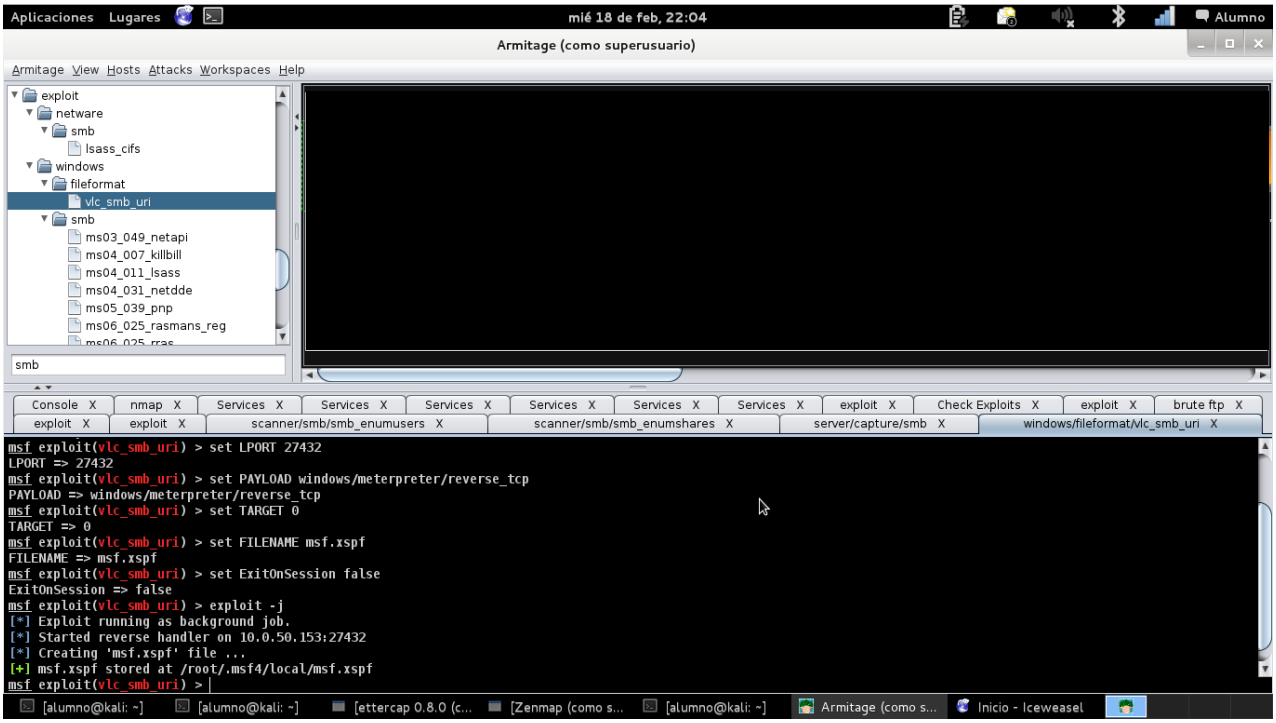


Figura 2-19 Empleando *Armitage* en la red.

3 DESARROLLO DEL TFG

3.1 Presentación.

En este capítulo se describe el test de intrusión llevado a cabo en la red del CUD. Se comienza por el proceso de *gathering* o recogida de información. El proceso estándar al implementar la auditoría en una organización comienza por determinar los límites del análisis, quedando recogido el acuerdo en un documento firmado por ambas partes como respaldo legal. Según el *Penetration Testing Execution*

Standard [43] el siguiente paso es el considerado *External Footprinting,* pues lo habitual es no tener acceso a la organización en un primer momento. Éste se divide a su vez en dos: *Active Footprinting*, donde se interactúa con la infraestructura de la empresa directamente, y el *Pasive Footprinting*, que recoge la información que han ido dejando los usuarios, como la información recogida de motores de búsqueda, foros, etcétera. Lo que se busca aquí es recolectar toda la información posible de forma ordenada y clasificarla en función de las posibilidades que nos ofrezcan para su explotación. Así, en un inicio, nos encontramos ante una red desconocida en su totalidad. Lo que haremos será ir determinando cuál es la topología de dicha red y, de alguna forma, lograr determinar su estructura, adquiriendo una visión de la misma, sus servidores, sus usuarios, etc., pues estos serán los objetivos posteriores. Por lo tanto, en primer lugar, se tratará de determinar la estructura de la red y sus diferentes entidades, tratando también de adquirir la mayor información posible de cada una de estas entidades, pues sabemos que la seguridad de una organización o red es tan fuerte como la del más débil de sus elementos. Así, podemos marcar como primer objetivo el encontrar este o estos puntos más vulnerables. Una vez localizadas estas vulnerabilidades, pasaremos a explotarlas. En este apartado, se pretende realizar un ataque multivector contra todos los puntos posibles, bases de datos, usuarios y sus correos y passwords, página web, etc. Tras implementar el ataque, se trabajará toda la información lograda hasta el momento, filtrándose en lo posible de forma que se logre un informe o resumen final de usuario en el que se presenten las vulnerabilidades detectadas, las consecuencias que éstas tienen en la organización y las posibles soluciones.

3.2 Recogida de información.

El ataque se va a realizar en la red del Centro Universitario de la Defensa ubicado en la Escuela Naval Militar (Marín) el cual cuenta con un sitio web, diferentes equipos para sus alumnos y profesores y su administración. En primer lugar, recolectamos la información pública que está al alcance de cualquiera. Comenzamos por su sitio web.

3.2.1 Análisis del sitio web.

En su página principal vemos que se encuentra vinculado a la Escuela Naval Militar, a la Armada, al Ministerio de Defensa, al Centro Universitario de la Defensa de Cartagena, al Centro Universitario de la Defensa de Zaragoza y al Centro Universitario de la Defensa de Madrid. Tiene un apartado para que los usuarios registrados se identifiquen y dos ayudas, una en caso de no recordar la contraseña y otra en caso de no recordar el usuario. La figura 3-1 muestra parte de la información que puede ser de interés y es pública.

En primer lugar, encontramos el equipo de gobierno formado por el Director del centro, el Subdirector, la Secretaria y el Gerente, así como sus nombres, despachos, teléfonos, la dirección postal del centro y su correo elctrónico, la web, su número de teléfono y de fax.

Figura 3-1 Equipo de gobierno.

Vemos asimismo que el centro cuenta con una biblioteca. La Figura 3-2 nos presenta su dirección postal, sus números de teléfono tanto externos como internos y su correo electrónico.

Figura 3-2 Datos de la biblioteca del Centro.

Por último, como se puede ver en la Figura 3-3 hemos conseguido un listado muy interesante con todo el personal, su función en el centro, sus números de teléfono (tanto internos como externos) y su dirección de correo electrónico.

Figura 3-3 Datos del personal del centro.

Pasamos ahora a utilizar alguna de las herramientas comentadas en el capítulo anterior.

3.2.1.1 Análisis con Whatweb.

Utilizando esta herramienta contra la web del CUD obtenemos la siguiente información:

- Las *Cookies* de la web son [redacted].
- El servidor *http* es [redacted].
- El gestor de contenidos es [redacted].

Las *Cookies* son asignadas por el sitio web al usuario de forma que se puede monitorizar su actividad en la red, llevando una especie de control de los sitios visitados por este. Entre otras utilidades, los sitios web utilizan estas *cookies* para presentarle al usuario su sitio web de forma mucho más personalizada. Es entonces una forma de identificar al usuario, y por lo tanto, se pueden emplear para vulnerar la privacidad de los individuos incluso logrando acceder a sus cuentas de correo electrónico. Esto se demuestra en [45] durante un evento *Black Hat*, uno de los más importantes en la agenda de la seguridad informática. Es posible la recopilación de estas *cookies* al quedar registradas cuando se visitan la mayoría de sitios web, desde un ordenador de uso público, por ejemplo, sin tener posibilidad de eliminarlas y dejando así nuestro correo expuesto al *hacker*.

Se puede ver una captura de este análisis realizado con *whatweb* en la Figura 3-4

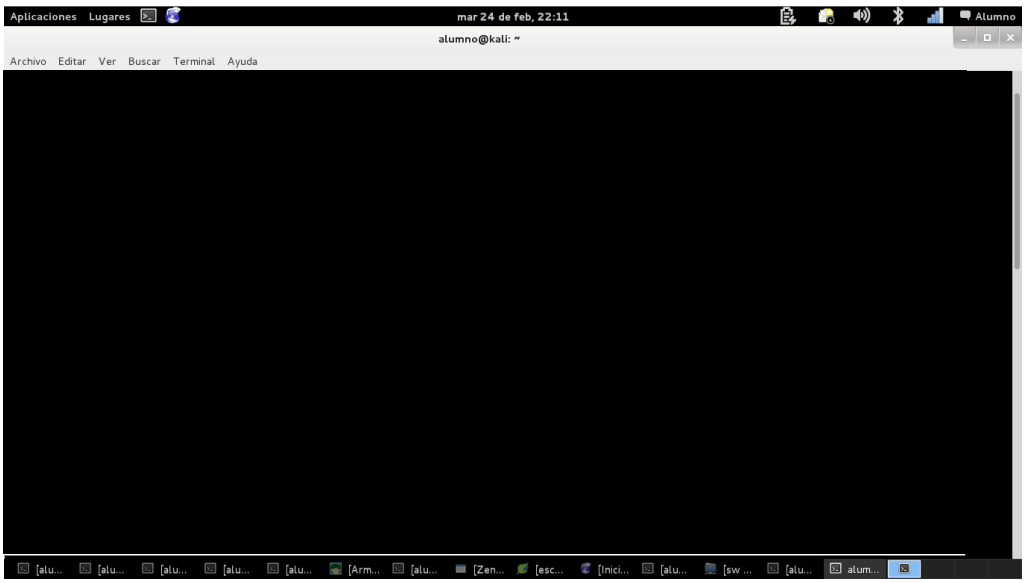


Figura 3-4 Análisis de la Web del CUD con *Whatweb*.

3.2.1.2 Nikto.

Al emplear nikto sobre la página web vemos que existen algunos archivos que podrían ser visibles al ejecutar el exploit adecuado y algunos directorios que podrían ser vulnerables a un ataque XSS (Cross-Site Scripting). Este último consiste en que se puede inyectar código en el código fuente de la página a través de un motor de búsqueda o de la URL si es del tipo reflejado, y se podría almacenar en el código de la página si es del tipo permanente. Esto quiere decir que se puede modificar el formato de la página incluyendo imágenes o texto. Uno de los ejemplos más conocidos es el que sufrió la página de Presidencia del Gobierno, bajo la presidencia de José Luis Rodríguez Zapatero, durante su mandato en la Presidencia Europea [46].

La Figura 3-5 muestra una captura de pantalla con el resultado del ataque:

Figura 3-5 Web de Presidencia del Gobierno hackeada.

Posteriormente se ataca una de las páginas del CUD, en concreto, la que los empleados utilizan para fichar demostrando que es vulnerable a este tipo de ataque. Describimos este ataque en particular en el apartado 3.2.3

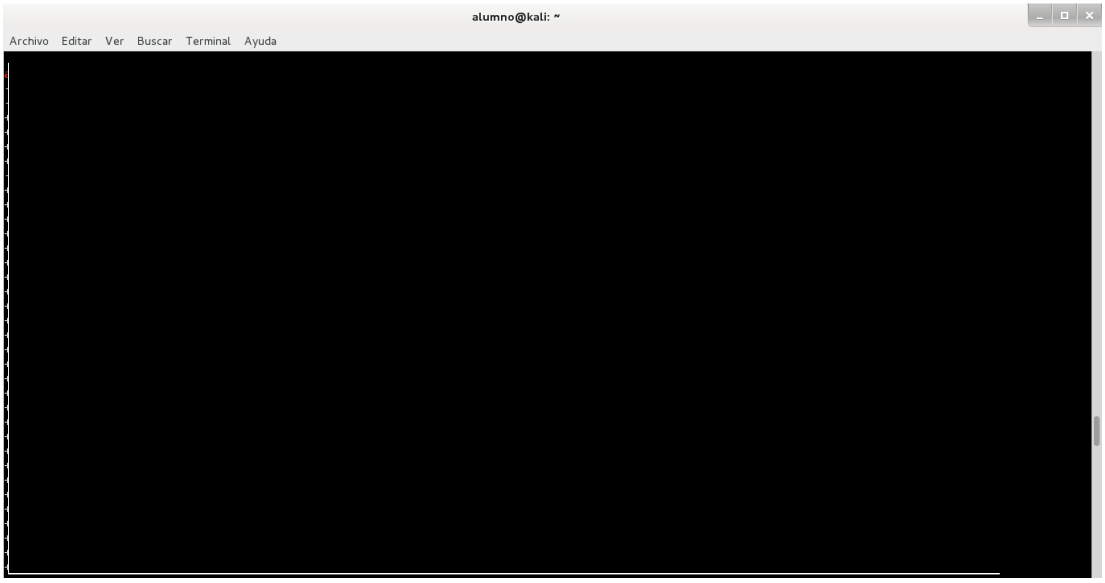


Figura 3-6 Análisis de la Web del CUD con *Nikto*.

3.2.2 Topología de la red.

Antes de nada, dejaremos clara la diferencia entre *Hubs, Switches, Routers y Access Points*.

Un *Hub* sirve para unir varios terminales, por ejemplo si queremos enlazar nuestros ordenadores personales. Han quedado en desuso ya que sólo uno de los ordenadores enlazados podía enviar tráfico mientras el resto tenían que estar a la escucha y el tráfico se enviaba en modo *broadcast* hasta que uno de los terminales lo aceptaba, haciéndolo muy lento. Esto ha dado paso al *switch*, cuyo funcionamiento es el mismo pero sin estos inconvenientes. Un paso más allá iría el *router*, que como su nombre indica, encamina el tráfico permitiendo el enlace entre dos redes como podría ser la personal enlazada por un *switch* e Internet mediante el uso de un módem. El *router* permite establecer *firewalls* de protección. Por último, tenemos los *Access Points*, estos permiten la conexión de un terminal de manera inalámbrica dentro de una red. La Figura 3-6 ayuda a comprender lo anterior.

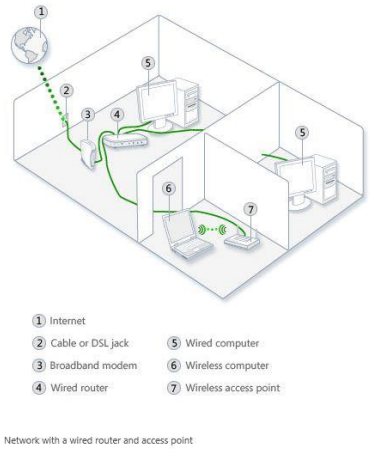


Figura 3-7 Elementos para establecer las conexiones en una red [44]

Pasamos ahora a utilizar la primera herramienta. Utilizaremos *Nmap* (y su vertiente gráfica *Zenmap)* para intentar determinar la topología de la red.

En cuanto al escaneo con *Nmap*, se realizarán varios, en diferentes momentos, pues dependiendo del instante temporal, algunos *hosts* pueden ser alcanzables o no.

Tras realizar este escaneo, obtenemos la información que se muestra en la Figura 3-8:

Figura 3-8 Usuarios conectados en el cuartel de alumnos Marqués de la Victoria.

La imagen de la Figura 3-8 procede de una captura de pantalla tras haber ejecutado *Zenmap*. Vemos que ya conocemos quienes son los usuarios que se encuentran conectados a esta LAN (*Local Area Network*). Se trata del punto de acceso *WiFi* del cuartel de alumnos *Marqués de la Victoria*. También se observa incluso a través de que dispositivo han realizado la conexión. Esto es importante a la hora de elegir el *exploit* más eficaz a emplear contra la víctima.

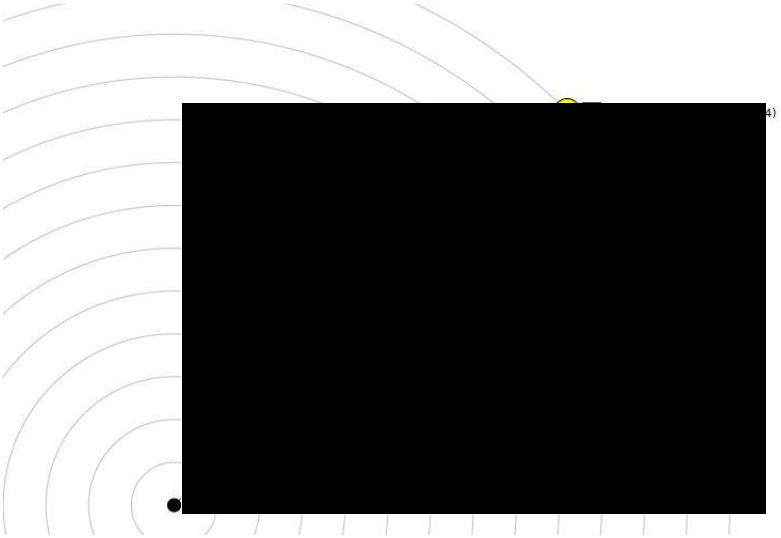


Figura 3-9 Ruta al servidor Web obtenida con *Traceroute* en *Zenmap*.

Vemos por un lado los saltos que son necesarios entre el *host* local y el servidor que almacena la IP correspondiente a la web del CUD, con cada uno de los nodos intermedios a través de los cuales viaja nuestra solicitud hacía el servidor. Es obvio entonces que de fallar alguno de estos nodos existe la posibilidad de perder el acceso a la web. Puede observarse cada uno de estos saltos en la Figura 3-9.

Tras realizar una búsqueda por la red, recabando información acerca de la IP utilizada por la web del CUD, encontramos que esta misma IP la utilizan otras páginas de la zona, como [redacted], [redacted] *o* [redacted], entre otras. El *DNS* asociado es

[redacted]. El propietario de esta IP es ovh sas en Francia [38]. Y esta es la localización del servidor: 140 Quai Du Sartel, 59100 Roubaix, France.

Organization:	OVH SAS
ISP:	OVH SAS

Figura 3-10 Localización física del servidor.

Si observamos la ruta que sigue la información hasta el servidor vemos que el segundo salto después de la LAN del cuartel es la puerta de enlace [redacted]. Si realizamos un escaneo en modo *broadcast* obtenemos la información que se muestra en la Figura 3-11. Observamos que en este escalón se encuentran todos los servidores empleados en la red del CUD.

Figura 3-11 Usuarios y servidores de la red. Obtenida con *Zenmap*.

Pasamos a definir la *simbología* usada por *Zenmap* para comprender el gráfico de la Figura 3-11. Los círculos toman su tamaño y color en función del número de puertos abiertos. Verde contiene menos de 3 puertos abiertos, amarillos entre 3 y 6 puertos abiertos y rojo más de 6. Las líneas de unión azules son líneas de unión primaria. Las naranjas indican que existen caminos alternos. Las negras discontinuas se emplean cuando no se ha registrado el tiempo de enlace y las azules discontinuas indican que existe un nodo intermedio sin determinar. La información hasta aquí obtenida es la

estructura básica de la red del CUD. Esta nos servirá de "mapa" para tener una referencia en la auditoría, siendo la base sobre la que se trabaja.

3.2.3 Información de cada host.

Ahora analizamos la información recogida, realizando un escaneo sobre cada uno de los *host*, comprobando qué puertos son los que tienen abiertos cada uno de ellos. Como se puede observar en la Figura 3-10, vemos nodos a los que se les ha dado un *DNS*, por lo que todo parece indicar que son de mayor relevancia. Por lo tanto, terminaremos de determinar cuál es la función de cada nodo dentro de la red comprobando qué servicios son los que ofrece. Tenemos que tener en cuenta que nos encontramos aún en la fase de recopilación de información, por lo tanto no debe preocuparnos tanto la finalidad o utilidad del *host* sino el recoger toda la información posible para su posterior análisis.

Se puede observar que, a tres saltos del *host* local, tenemos los servidores [redacted].

Del mismo modo, tras monitorizar la red diariamente, sabemos cuáles son los equipos en funcionamiento 24 horas, 7 días a la semana, indicativo también de ser importantes dentro de la red.

Pasamos a recopilar información sobre cada uno de ellos. Esta información se ha recopilado empleando *Nmap, Zenmap, Whatweb, Nikto, Armitage* y *Metasploit* en cada uno de los *host.* Además, se ha realizado su búsqueda en la barra del buscador, y se ha comprobado si montaban el servicio de archivos *samba.*

- [redacted]: Se trata del *router* que hace de puerta de enlace. Comprobamos que para acceder requiere usuario y contraseña, y el análisis con *Nikto* tampoco es posible sin clave de acceso. *Zenmap* afirma, con un 99% de posibilidad, que se trata de un *Cisco 870 router*, con un sistema operativo Linux y el software IOS (*Internet working*) 12.2/12.4 instalado, sin el cual no puede funcionar un router Cisco. La Figura 3-11 muestra que es necesaria la autenticación para llevar a cabo el escaneo con *Nikto.*

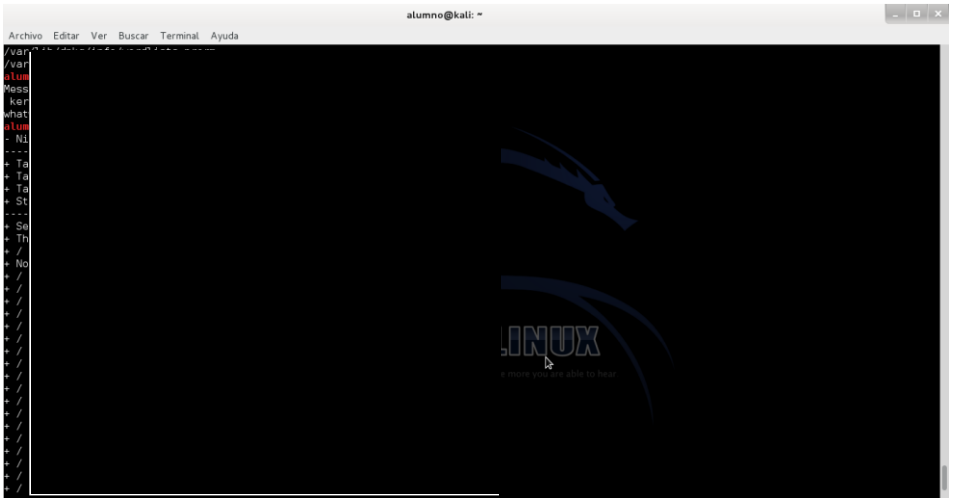


Figura 3-12 *Nikto* en la puerta de enlace.

- [redacted]: Se trata de un *switch* Cisco con sistema operativo Linux y el software IOS, tiene habilitada su gestión en remoto a través del puerto 23. También podemos observar en la Figura 3-13 que es posible abrir una *shell* [redacted] de conseguir el acceso al servidor.

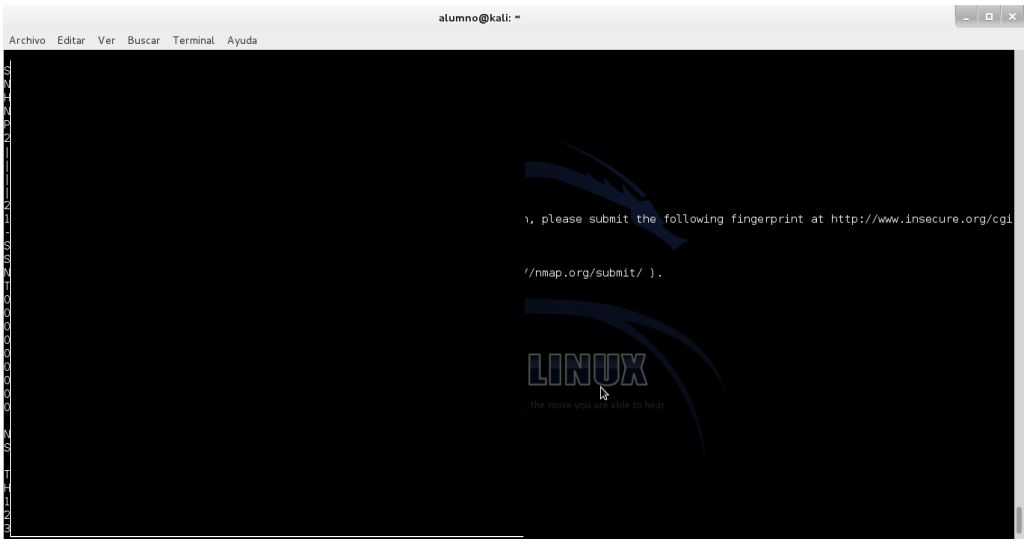


Figura 3-13 Información proporcionada por *Nmap switch*.

- [redacted]: Se trata del servidor [redacted]. En primer lugar, tras ejecutar *Nmap* en el servidor vemos que monta el servicio *samba* por lo que sirve de almacenamiento de archivos. En la Figura 3-13 y 3-14 vemos el resultado.

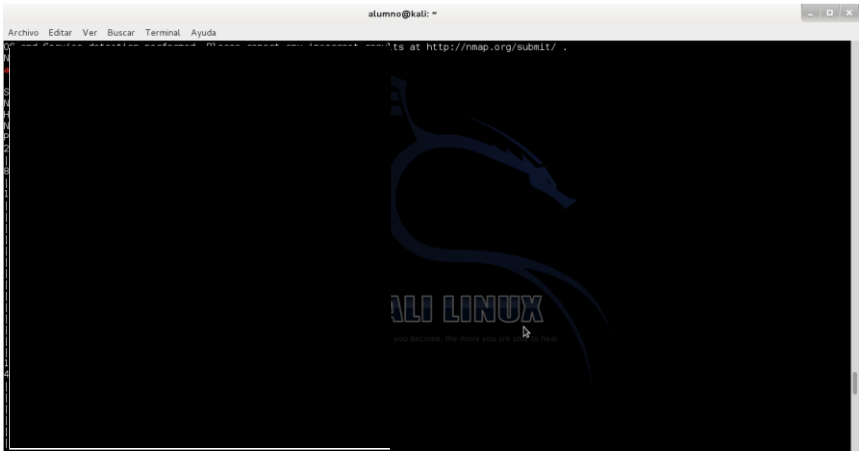


Figura 3-14 Resultados al emplear *Nmap* en el servidor [redacted].

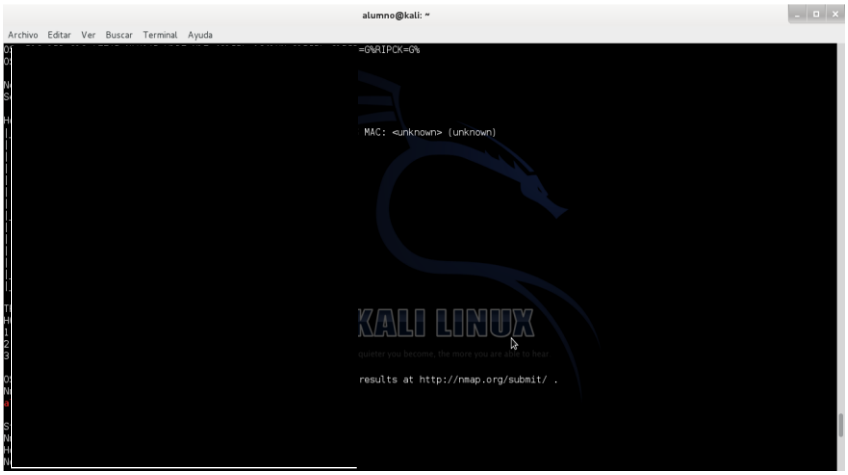


Figura 3-15 Resultados de emplear *Nmap* en el servidor [redacted] (bis)

La Figura 3-16 muestra cómo hemos logrado acceder al directorio IPC del servidor. Tras haber descubierto que el servidor trabaja con el servicio *samba* se ha procedido a acceder a este como cliente.

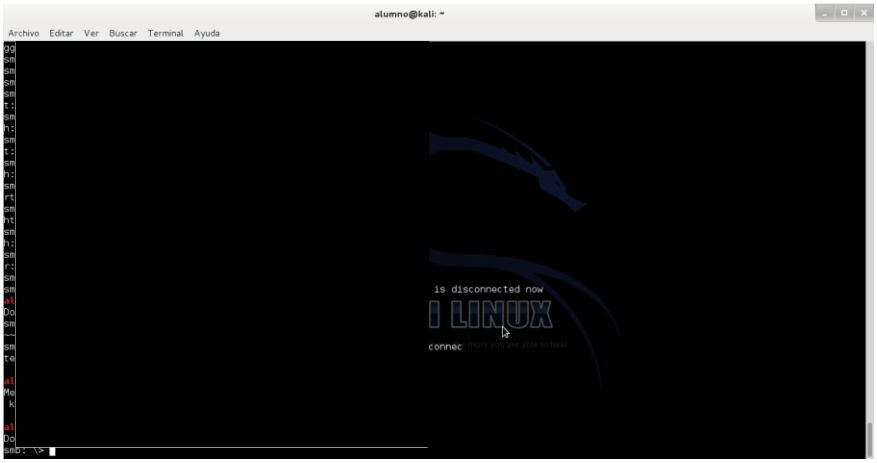


Figura 3-16 Dentro del directorio IPC

Posteriormente se decide ejecutar alguno de los *exploits* de utilidad sobre equipos que montan *samba*. Las Figuras 3-17 y 3-18 muestran el resultado, respectivamente se muestran los usuarios y los directorios con los que cuenta el servidor [redacted]. Se ha lanzado este *exploit* de forma simultanea sobre los servidores que se sabía utilizaban el servicio *samba* obteniendo los nombres de usuario y los directorios no solo del servidor [redacted] sino también de [redacted].

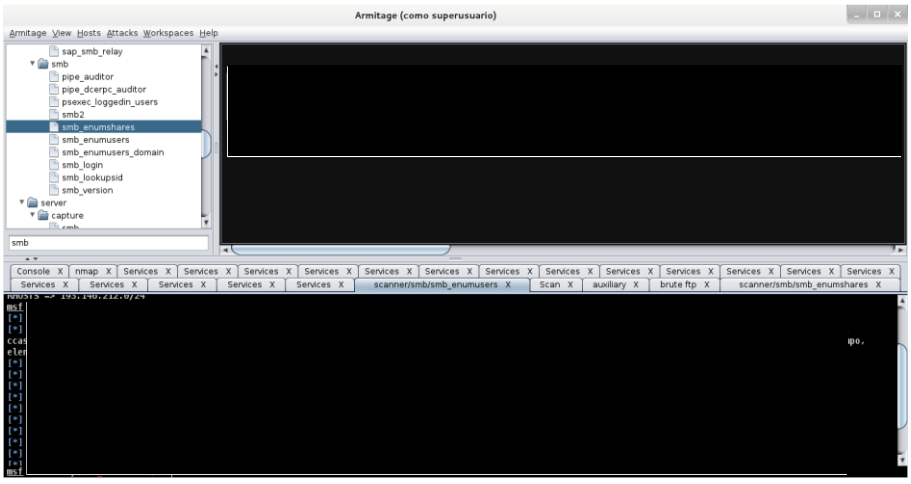


Figura 3-17 Usuarios registrados en los servidores [redacted]

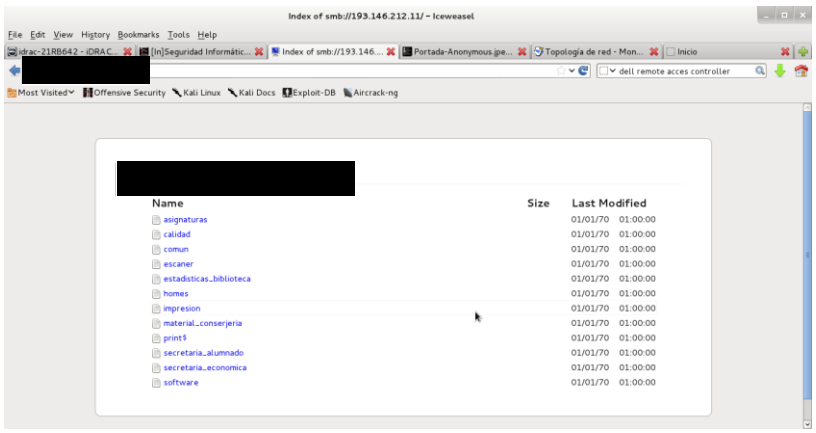


Figura 3-18 Directorios en el servidor [redacted].

El servidor [redacted], con [redacted], contiene al grupo de trabajo CUDGROUP y emplea el sistema operativo Unix. El nombre del servidor es [redacted], el nombre de dominio es cud.uvigo.es. Los métodos permitidos por HTTP son [redacted]. Es el servidor en el que están registrados todos los profesores, como hemos podido ver en la Figura 3-17. *Nikto* nos advierte de que está habilitado el *mod_negotiation* en *multiviews*, en *Apache*, el cual es el responsable de que podamos ver el nombre de los directorios.

- [redacted]: se trata del servidor [redacted]. Los usuarios registrados en este servidor pueden verse en la Figura 3-17. De esto, se puede deducir que es el servidor empleado por el personal de la secretaria del centro.

El resultado de la ejecución de *Nmap* en este servidor se muestra en la Figura 3-19. Vemos, que al igual que el servidor [redacted], utiliza el servicio *samba* en el puerto 139.

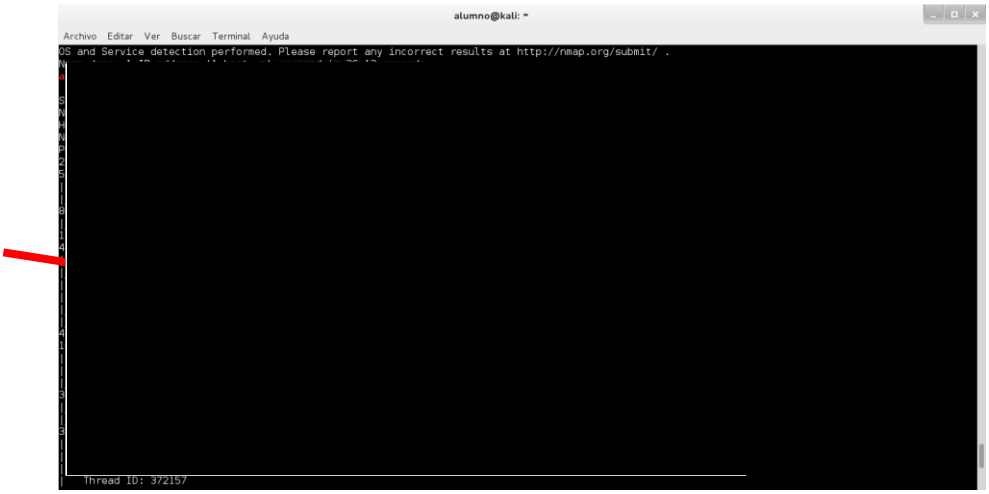


Figura 3-19 Resultados de ejecución de *Nmap* en [redacted].

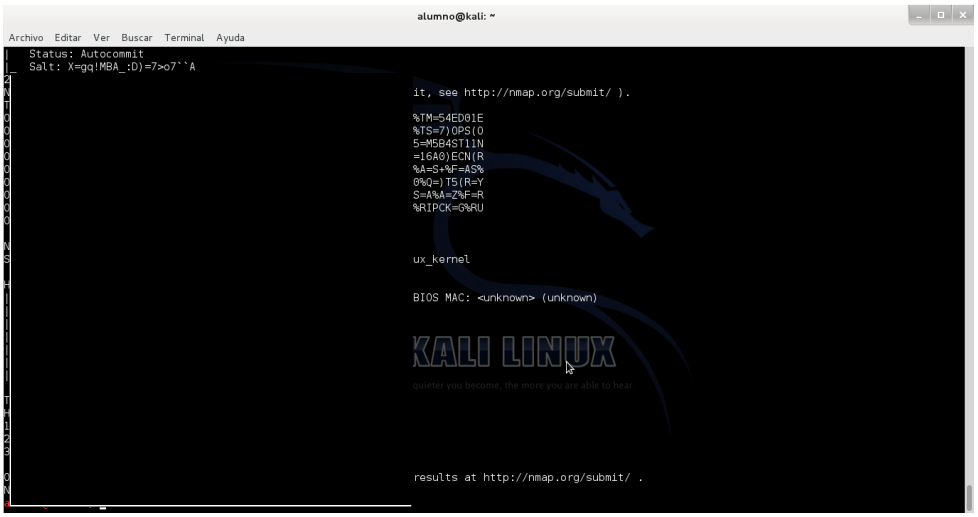


Figura 3-20 Resultados de ejecución de *Nmap* en [redacted] (bis)

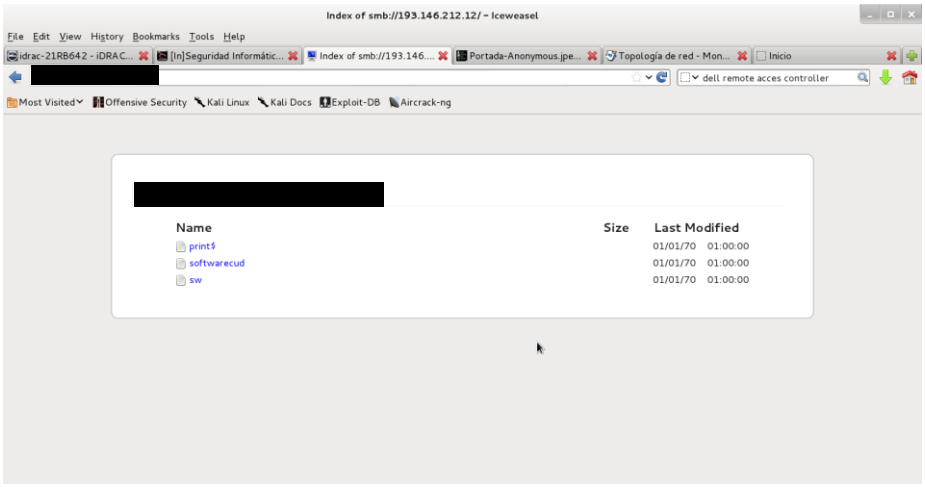


Figura 3-21 Directorios en el servidor [redacted].

El servidor [redacted] con IP [redacted], emplea el sistema operativo Linux y contiene al grupo de trabajo WORKGROUP. Encontramos el mismo problema en *Apache*, que en [redacted], que al estar habilitada la opción *multiviews* permite al atacante ver los directorios y usuarios. Contiene un apartado llamado [redacted]. Contiene archivos tanto *.HTML* como *.PHP*. Los métodos permitidos por HTTP son [redacted]. Al igual que en *Elcano*, somos capaces de acceder a *IPC*.

- El servidor [redacted], con IP [redacted], emplea el sistema operativo Linux. Contiene dos grupos de trabajo llamados CUDGROUP. El host es CUDLABS.LOCAL por lo que se deduce que es el servidor empleado por los laboratorios. El nombre del ordenador es [redacted]. El nombre del dominio es *cudlabs.enm*. Los métodos permitidos por HTTP son [redacted]. Así mismo, los usuarios también aparecen en la Figura 3-17.

La Figura 3-22 muestra el directorio almacenado en el servidor [redacted].

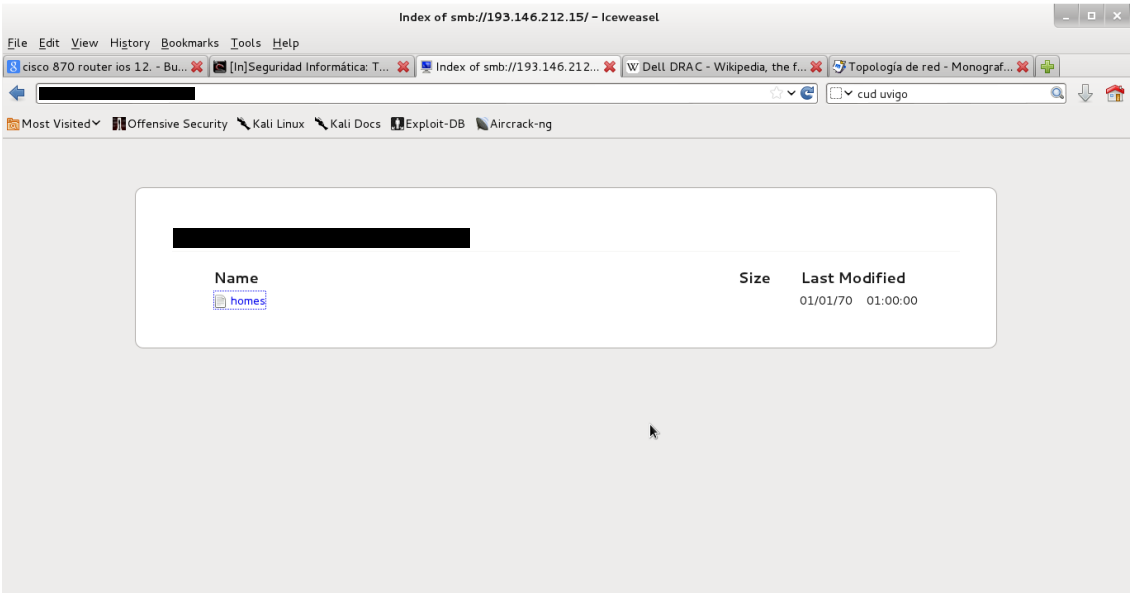


Figura 3-22 Directorios en el servidor [redacted].

Las Figuras 3-23 y 3-24 muestran los resultados de la ejecución de *Nmap* en el servidor [redacted]. Vemos que utiliza el servicio [redacted].

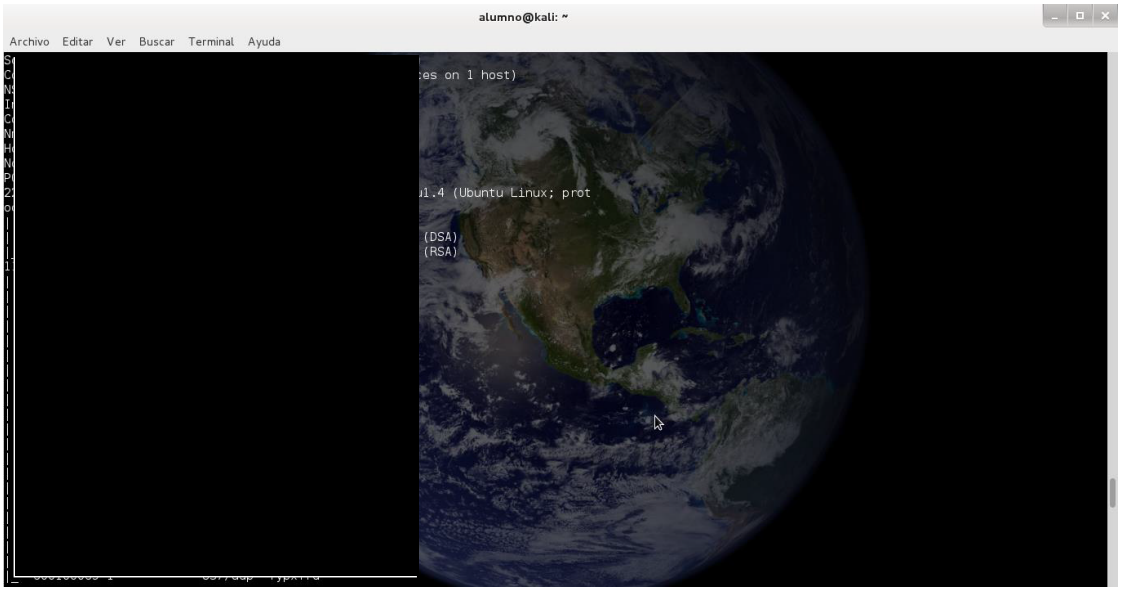


Figura 3-23 Resultados de la ejecución de *Nmap* en [redacted].

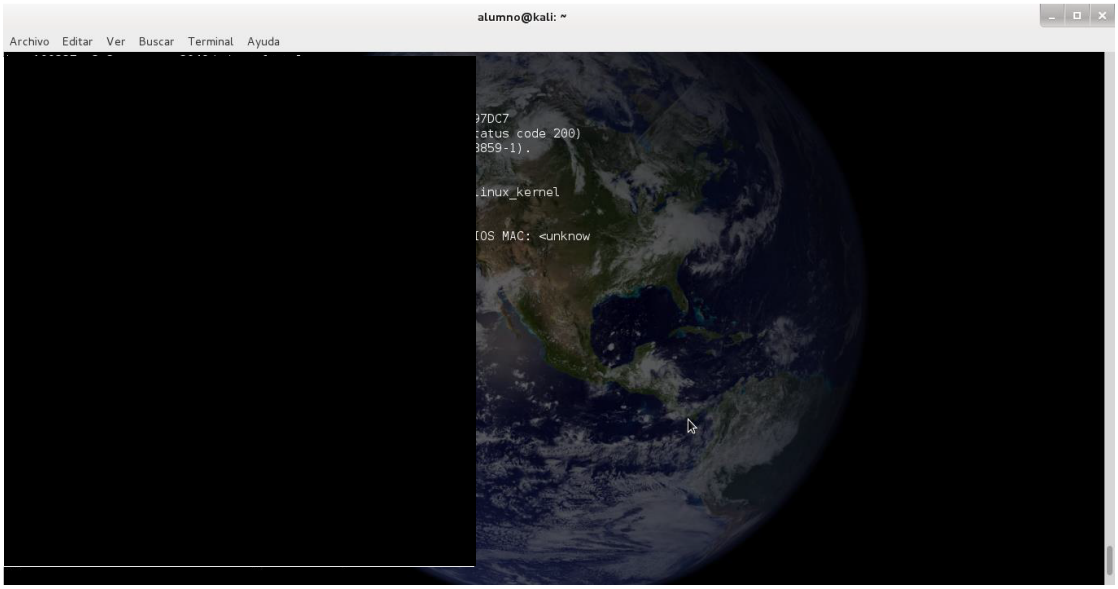


Figura 3-24 Resultados de la ejecución de *Nmap* en [redacted] (bis).

- El servidor [redacted] soporta los métodos [redacted]. Como puede observarse en la Figura 3-25 el sistema operativo que emplea es Windows Server 2008 y su dirección *MAC* es: 78:e3:b5:95:7d:5a. Emplea *Microsoft-HTTPAPI,* lo que hace pensar que emplea un *WAF* (*Web Application Firewall*). El nombre en NetBIOS es WINCUD. Contiene tres grupos de trabajo diferentes: WINCUD, WORKGROUP y AladinHasp. El nombre del ordenador es wincud. El servidor es un gestor de usuarios con [redacted].

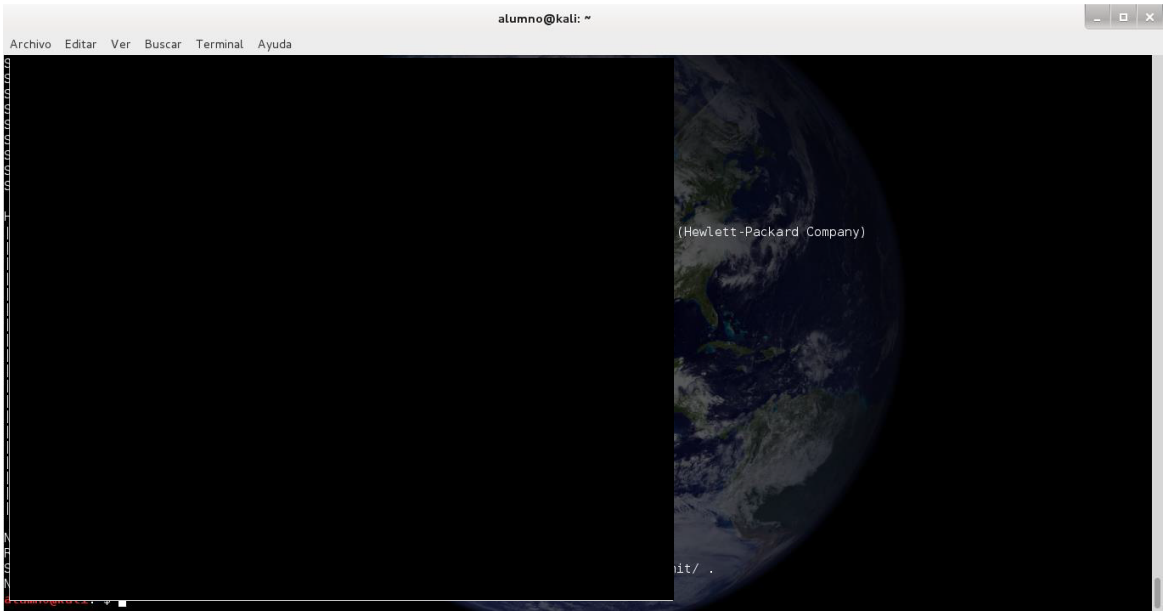


Figura 3-25 Resultados de la ejecución de *Nmap* en el servidor [redacted].

- La dirección IP [redacted] corresponde a un controlador de acceso remoto, el *IDRAC-21RB642 DELL*. Se ha realizado una búsqueda exhaustiva de información acerca de este tipo de controlador de acceso remoto a través de la red, entre otros se ha estudiado su manual de configuración donde se refleja que el usuario administrador por defecto es *root* y su clave de acceso es *calvin*. Se ha logrado acceder a este servidor como *root* ya que no se había modificado la clave de acceso por defecto. Posteriormente, se ha modificado la clave para ganar los derechos de administrador. Por lo tanto, se ha logrado el acceso al usuario que gestiona este controlador del servidor. Este proceso se muestra en las Figuras 3-26 y 3-27.

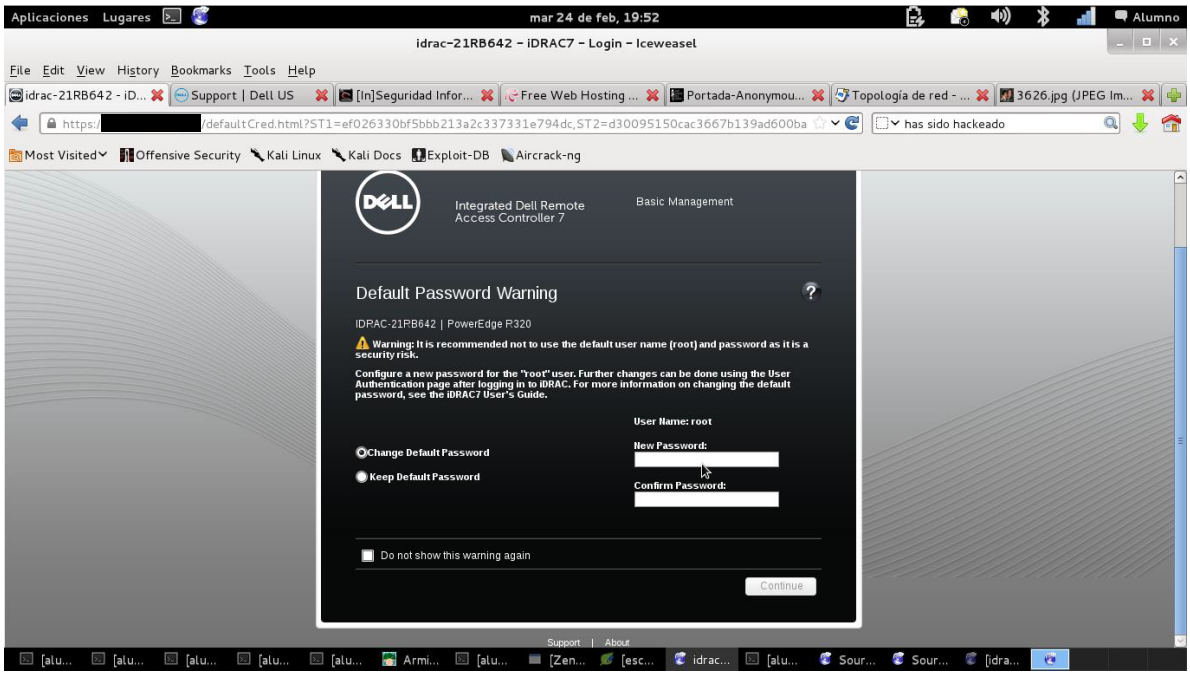


Figura 3-26 Captura del momento en el que se está modificando la password en el servidor [redacted].

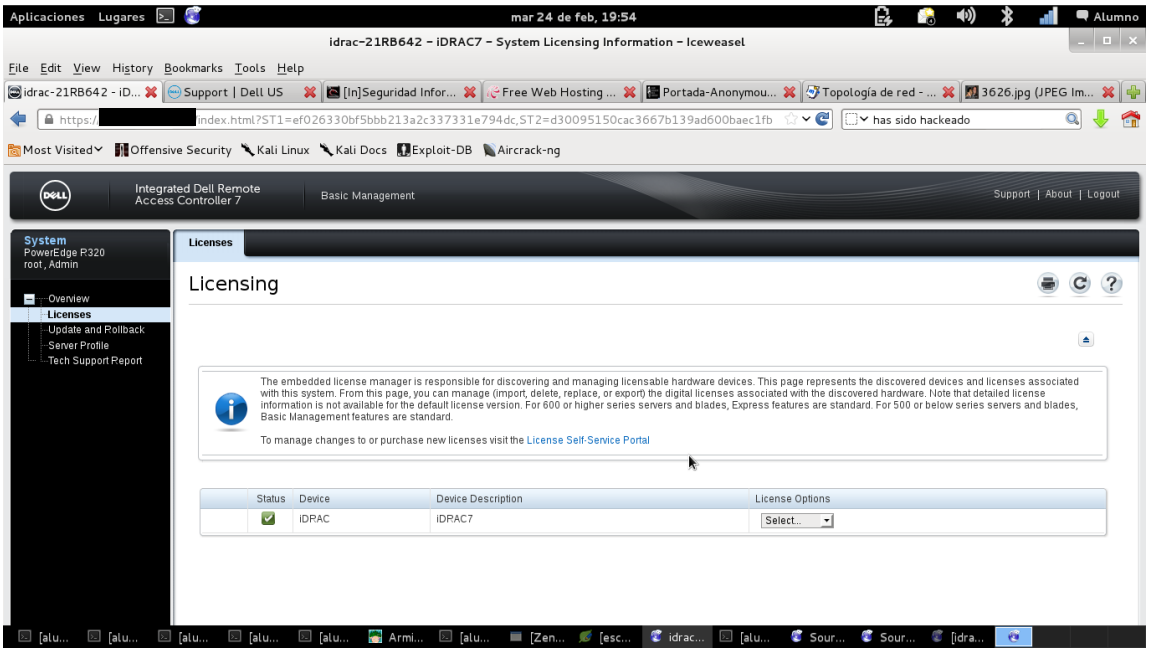


Figura 3-27 Acceso conseguido.

- El servidor [redacted] es un servidor de archivos que utiliza el sistema de ficheros *samba* y con sistema operativo Windows Server 2008. El nombre del ordenador es WIN-PFLQC2HE70E. Posee un grupo de trabajo llamado WORKGROUP. Esto se muestra en la Figura 3-28.

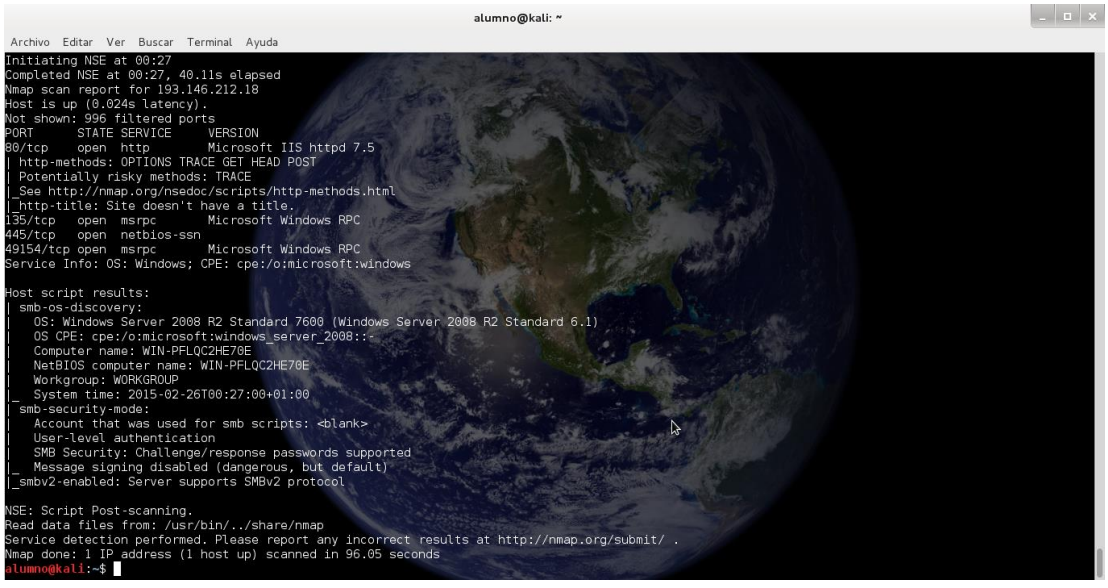


Figura 3-28 Resultado de la ejecución de *Nmap* en el servidor [redacted].

- Del servidor [redacted], [redacted] solo detectamos el puerto [redacted] abierto para *ssh* (*Secure Shell*).
- Con el servidor [redacted], establecemos conexión por puerto 80. Vemos que monta el servicio *Apache 2.4.7* (Ubuntu). Tiene registrada una aplicación, la cual se había mencionado en el apartado 3.2.1.2, que sirve para fichar a la entrada y salida del trabajo a los empleados y es vulnerable a un ataque XSS como puede verse en las Figuras 3-29 y 3-

30. Y almacena también un analizador de seguimiento web, *Piwik*. Se procede a introducir código a través del apartado que permite al usuario introducir su nombre de identificación, esta aplicación toma este código y pasa a formar parte del código de la propia página. Por ello, si el código que introducimos es parte de la configuración de la página, en este caso, una imagen en mitad de la página, modifica el diseño de la página, como puede verse en la Figura 3-30.

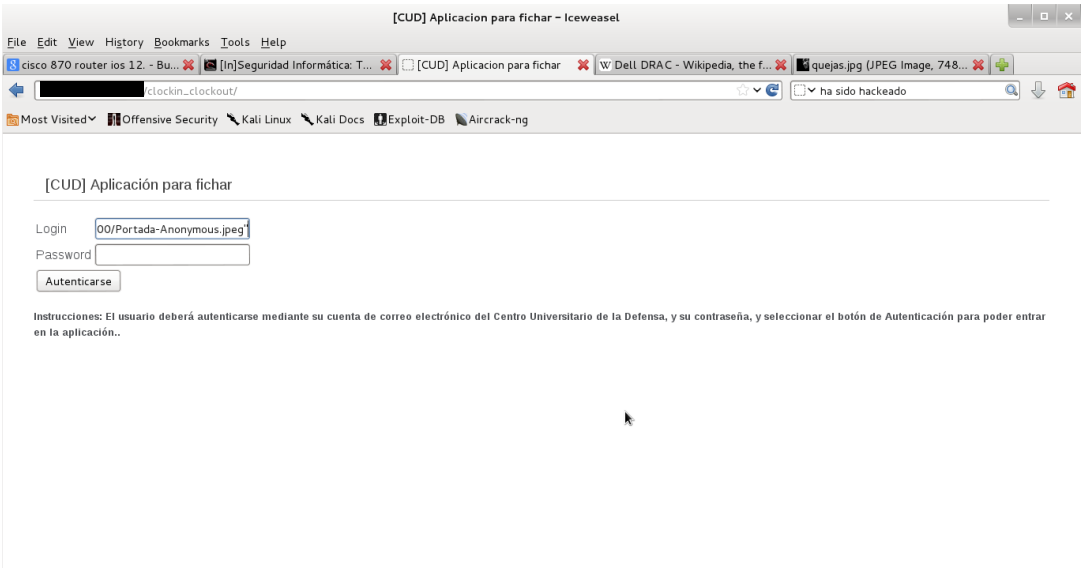


Figura 3-29 XSS reflejado, la página web toma el código que le introducimos.

Figura 3-30 XSS, somos capaces de modificar la web de forma no permanente.

El siguiente paso sería modificar la configuración de esta página web de forma permanente. Por el tiempo disponible es inviable, por lo que se recoge y se plantea en el capítulo cinco como una de las posibles líneas futuras.

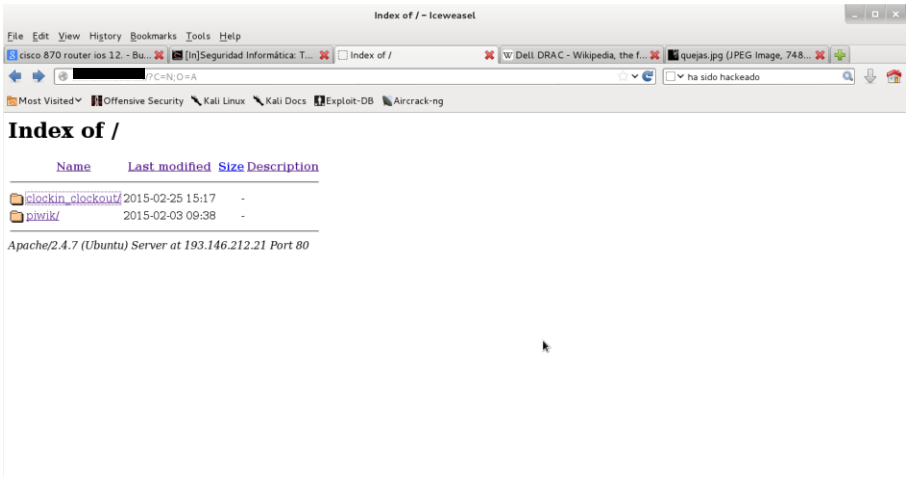


Figura 3-31 Directorios en el servidor *Cervantes*.

- El servidor [redacted] posee el puerto [redacted] abierto en el que monta el servicio *ssh* el cual sirve para abrir una *Shell* en remoto y así poder administrar el servidor en remoto.
- El servidor [redacted] monta el sistema operativo Linux. El nombre del ordenador es [redacted]. El nombre del dominio es cud.uvigo.es. Se ha conseguido acceder a este servidor observando que sirve como almacenamiento de software para su empleo en la organización.

Tras adquirir la clave de acceso al punto de acceso inalámbrico *wcud*, como se explica en el apartado *3.3.2 (Man In The Middle MIM)*, se realiza una captura de tráfico de datos en esta red con *ettercap*. En ella, además de algunos correos, se captura el usuario *cámara* y su contraseña. Con este usuario, se lanza un ataque con *armitage* y se logra abrir una *shell* en el servidor, teniendo así acceso al servidor con los privilegios del usuario *cámara*, como se muestra en las Figuras 3-32, 3-33 y 3-34.

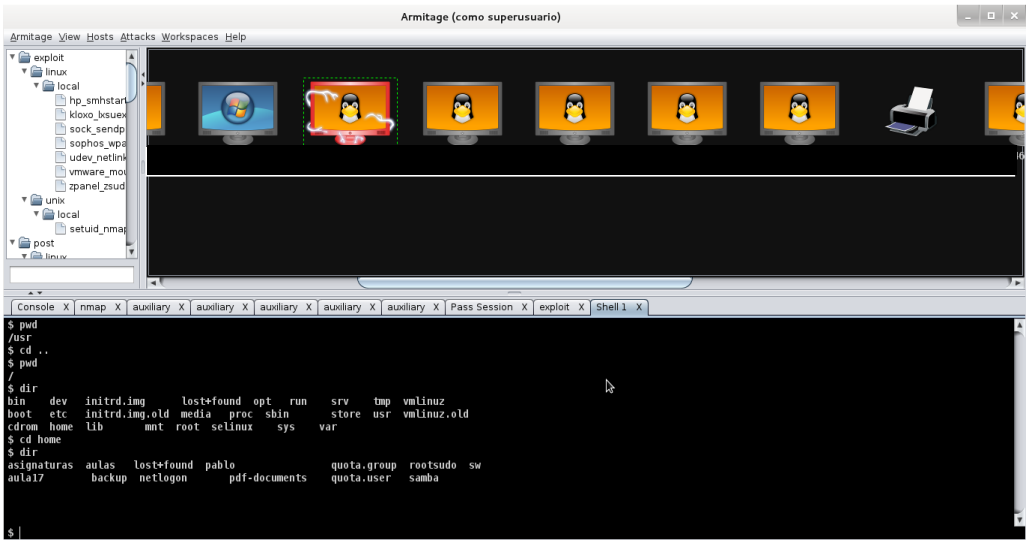


Figura 3-32 Directorios en [redacted] tras abrir una *shell* con el usuario Camara.

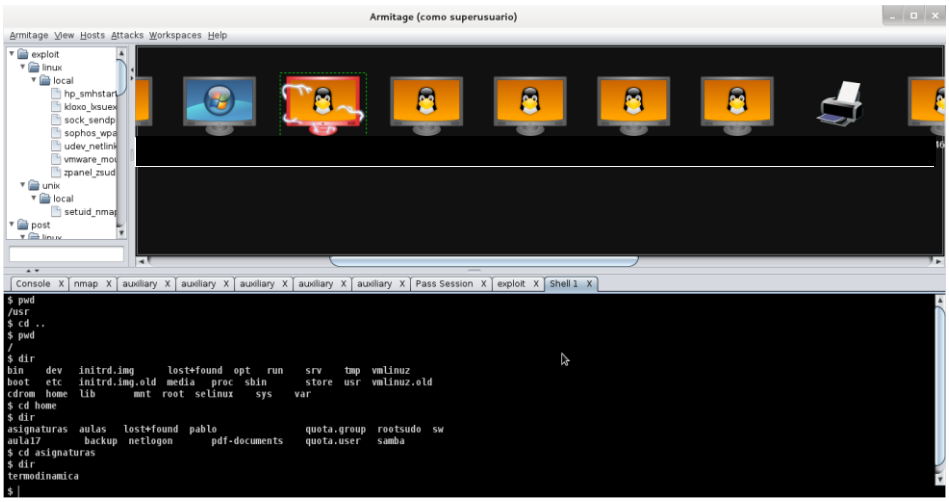


Figura 3-33 Vemos los directorios contenidos en 193-146.212.23.

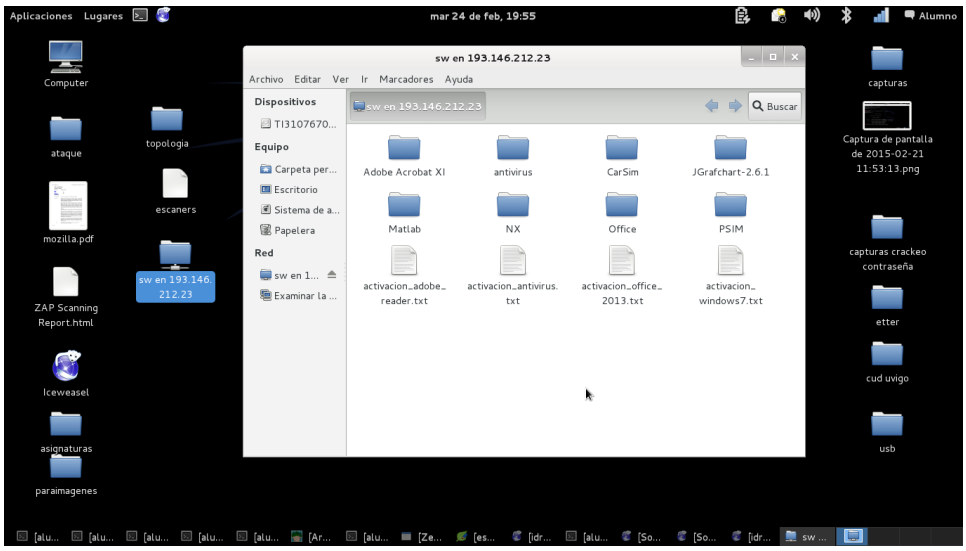


Figura 3-34 *Software* almacenado en el servidor [redacted].

- El servidor [redacted] es un *switch* protegido y bloquea incluso los *ping* de escaneo. Pasamos a ejecutar *Nmap* de forma más sigilosa (empleando el comando -Pn) pudiendo realizar esta vez el escaneo, como se muestra en la Figura 3-35.

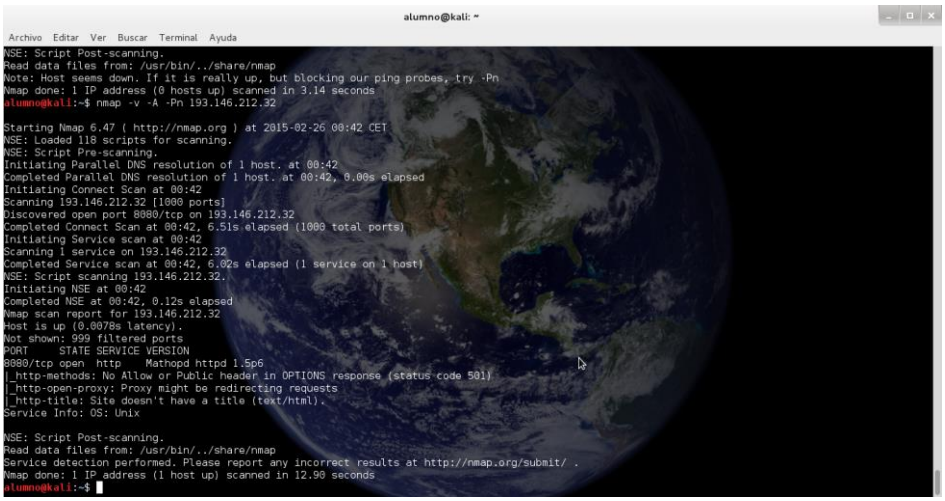


Figura 3-35 Resultados de la ejecución de *Nmap* en el servidor [redacted].

- El *host* con IP [redacted] es un router de acceso inalámbrico *Aruba*. El nombre del sistema es *Aruba3200*. En la Figura 3-36 vemos el servidor web con el que cuenta para su configuración. Se observa también que se encuentra protegido siendo necesario autenticarse.

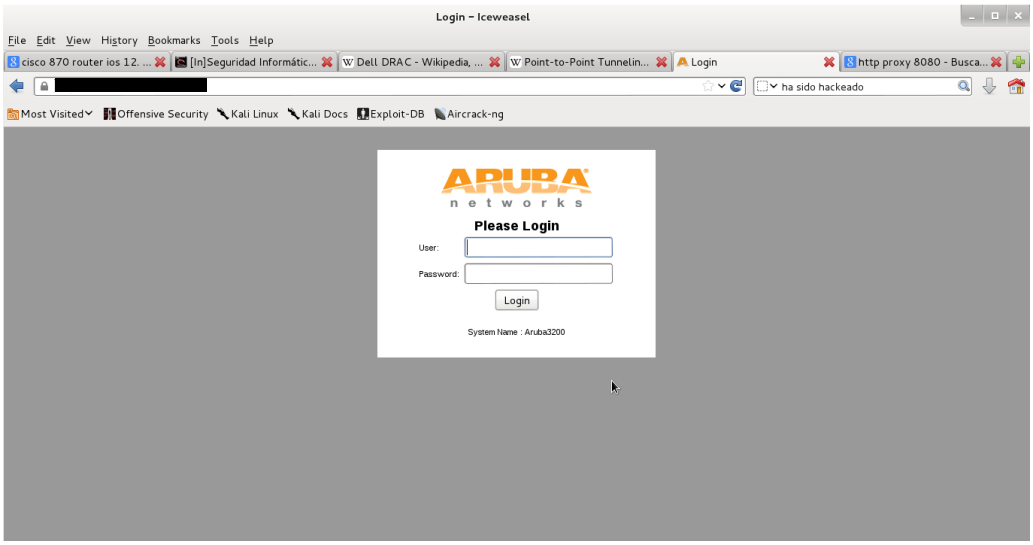


Figura 3-36 *Aruba router*.

- El host con IP [redacted] es un *switch* de *Allied Telesyn*, modelo AT-S63. Este *switch* es configurable mediante su acceso web, como muestra la Figura 3-37. También vemos que la MAC del *switch* es: EC:CD:6D:03:05:31 y su nombre es *BackBone Red CUD*.

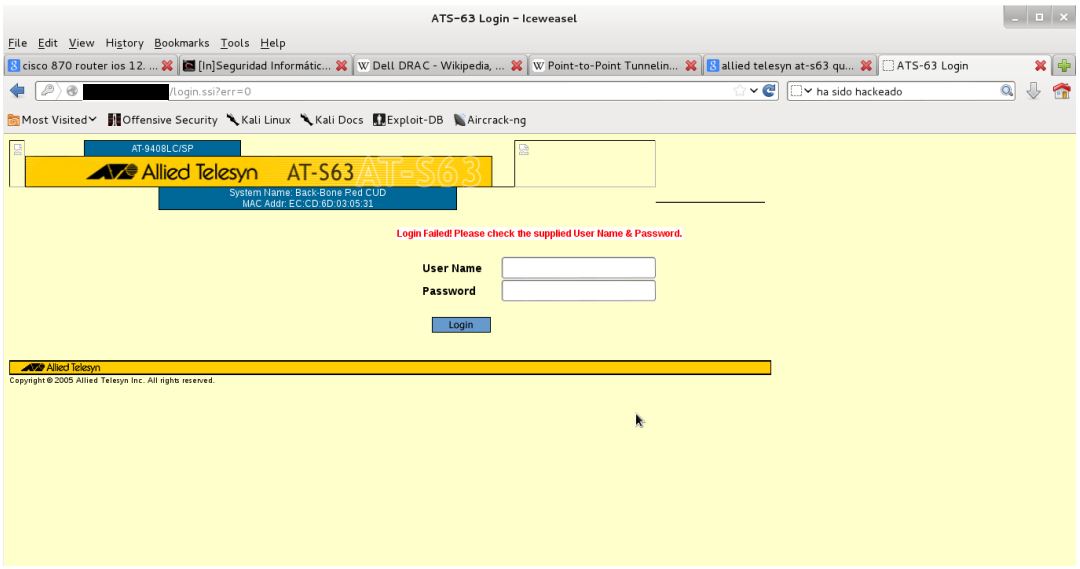


Figura 3-37 *Switch Allied Telesyn* en el servidor [redacted].

- El *host* SMCWBR14S-N4, con dirección IP [redacted], monta el servicio *Sveasoft Alchemy firmware telnetd* en el puerto 23 propio de un *router*.
- El *host mathinger*, [redacted], es un servidor de correo con sistema operativo Linux. En la Figura 3-38 puede observarse que utiliza el servicio *smtpd* en el puerto 25, propio de un servidor de correo.

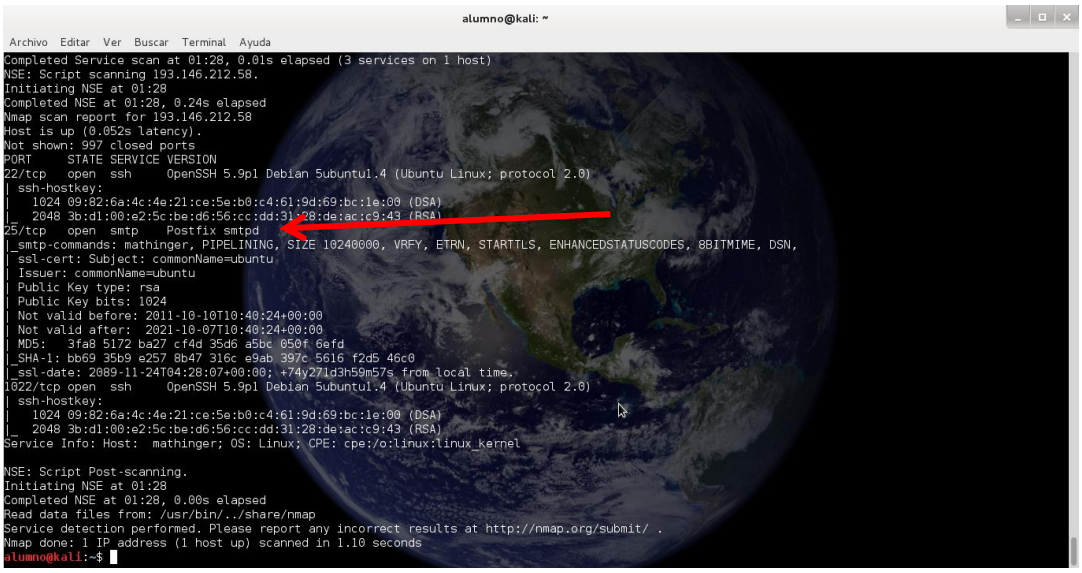


Figura 3-38 Resultados de la ejecución de *Nmap* en el servidor [redacted].

- Con dirección [redacted] tenemos un *router Cisco* con sistema operativo Linux y el software IOS instalado.

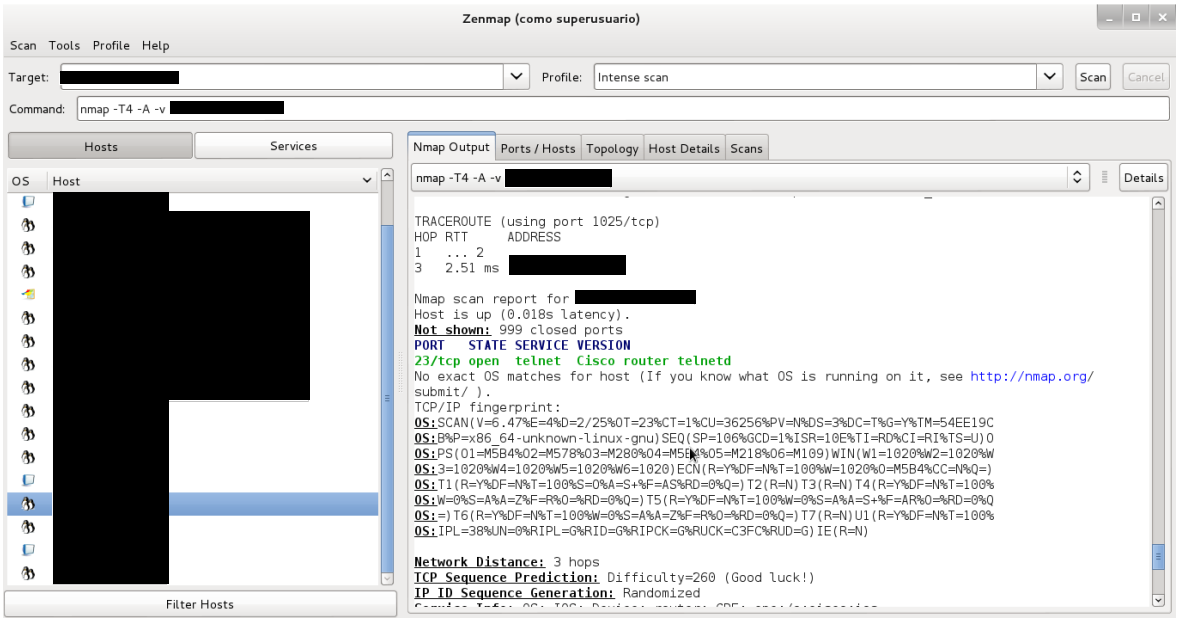


Figura 3-39 Resultado de la ejecución de *Zenmap* en el servidor [redacted]

- En [redacted] tenemos el servicio de videoconferencia de *Polycom Viewstation Video Conferencing*. Su acceso está protegido por clave.

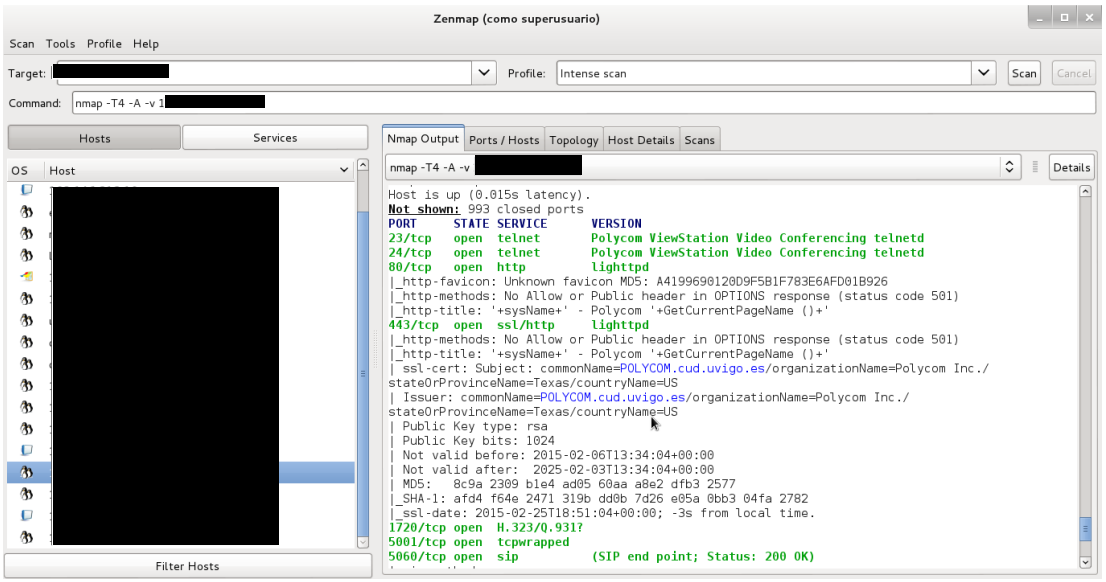


Figura 3-40 Servicio Videoconferencia detectado al emplear *Zenmap*.

3.3 Ataque a la red.

3.3.1 Crackeando contraseña WiFi.

Existen varias posibilidades a la hora de intentar adquirir la clave de acceso a un punto de acceso WiFi. Se puede intentar un ataque por fuerza bruta, el cual consiste en intentar romper la clave de acceso después de probar con un gran número de combinaciones las cuales podemos definir de algún modo. Podemos elegir que sean alfanuméricas, con mayúsculas, etc. Este tipo de ataque consume muchísimos recursos y lleva muchísimo tiempo obtener la clave. De hecho, no es eficaz 100% pues si la clave de acceso es de un gran tamaño podría ser que el tiempo necesario para crackearla fuese de años, siendo esto inviable. Es, por esto, que sólo se emplea en caso de que tengamos cierta información previa acerca de la clave, de forma que el abanico de posibilidades quede reducido.

El otro modo de ataque es el ataque por diccionarios. Existen en la red infinidad de diccionarios que contienen una amplia gama de contraseñas, entre ellas las más comunes y de uso por defecto. Por lo tanto, si nuestro usuario no ha cambiado esta clave que venía preconfigurada, es bastante posible conseguir un diccionario en el que se encuentre.

El fundamento del proceso es el siguiente. En primer lugar, decir que usaremos la *suite air* para romper la clave. Debemos configurar nuestra tarjeta de red en modo monitor, de modo que comience a capturar todo el flujo de datos inalámbrico. Esto se logra con *airmon-ng*. Una vez configurada nuestra tarjeta de red en modo monitor, pasa a llamarse *mon0*, y pasamos a capturar el tráfico de datos. Matamos los procesos que podían entrar en conflicto al realizar la captura de datos y el crackeo. De esta primera captura, obtenemos el ESSID, el nombre del punto de acceso, y el BSSID, o dirección MAC del punto de acceso, así como el canal en el que opera. Para realizar la captura de datos, empleamos *airodump-ng*. Una vez conocida la MAC del punto de acceso, empleamos de nuevo *airodump-ng*, pero esta vez, sólo sobre el punto de acceso que nos interesa. Así, logramos ver los clientes que están conectados y sus MAC´s. El siguiente paso será monitorizar, de nuevo, el intercambio de datos en este punto de acceso pero esta vez crearemos un archivo donde registraremos la captura. Empleando *aireplay-ng* desautenticaremos a alguno de los clientes del punto de acceso, obligándolo a acceder de nuevo. Será, en este momento, en el que quede registrado el *handshake*.

Para entender qué es el *handshake*, debemos saber que es el proceso que se lleva a cabo al establecer conexión entre dos entidades empleando el Protocolo de Control de Transmisión (TCP). Para establecer dicha conexión, se realiza lo que se conoce cómo *3-way-handshake* por constar de tres pasos. El cliente le solicita establecer la conexión al punto de acceso, éste si lo recibe correctamente, le contesta diciendo que se ha establecido la conexión y, por último, el cliente le contestaría de nuevo diciendo que se ha enterado, quedando así la conexión abierta entre ambos. En el envío del cliente al punto de acceso, entre otros datos, se encuentra la clave de acceso codificada. Es por esto que al capturar el *handshake* estaremos capturando también la clave de acceso.

Finalmente, sólo resta emplear *aircrack-ng* sobre el archivo creado al realizar la captura, y emplear uno de los diccionarios con los que contemos para romper la clave. En las siguientes imágenes podemos ver el proceso. En la Figura 3-41 vemos como en primer lugar establecemos la tarjeta de red en modo monitor empleando para ello *airmon-ng*. Vemos que hay algunos procesos corriendo en el ordenador que podrían entrar en conflicto al ejecutar *airmon-ng* por lo que lo mejor es proceder a eliminarlos con el comando `kill`. La tarjeta de red queda en modo monitor, en la interfaz *mon0*.

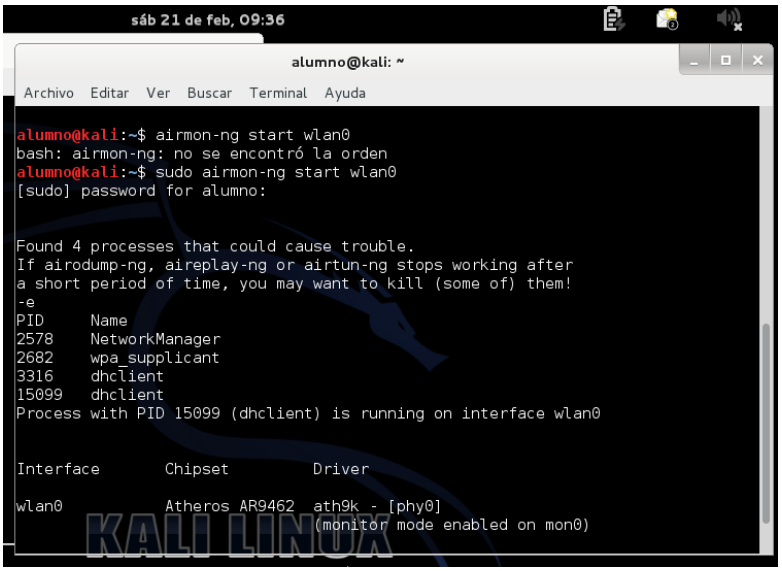


Figura 3-41 Resultado de ejecutar *airmon-ng*.

El siguiente paso es el que muestra la Figura 3-42 que consiste en capturar el tráfico inalámbrico existente en la zona.

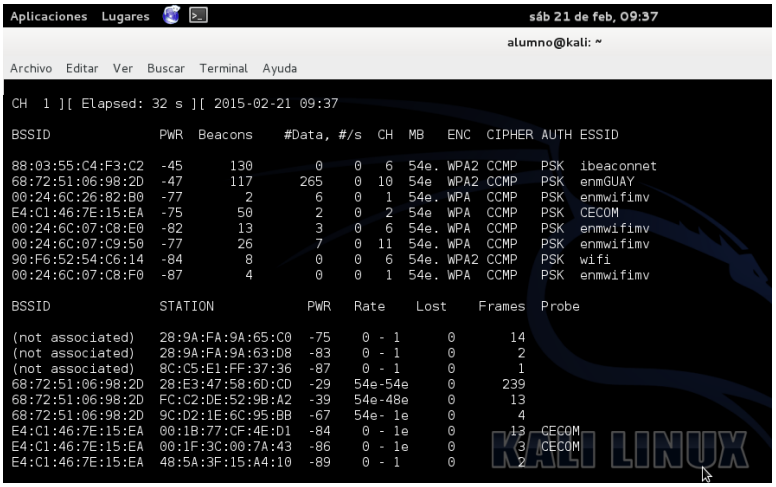


Figura 3-42 Monitorizando el tráfico de datos entre los usuarios y los diferentes puntos de acceso.

Pasamos a capturar el tráfico de modo selectivo, sólo sobre el punto de acceso del cual queremos obtener la clave de acceso.

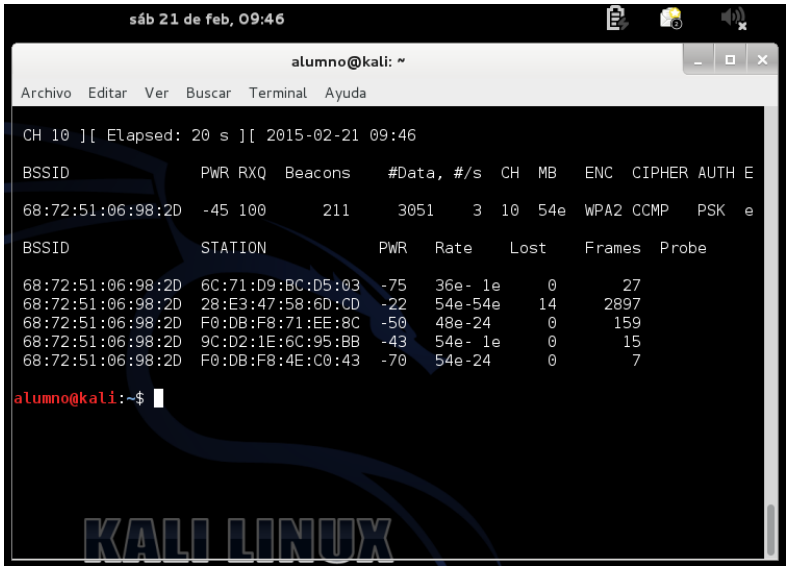


Figura 3-43 Monitorizando el flujo d datos en el punto de acceso objetivo.

Se procede a desautenticar a alguno de los usuarios con *aireplay-ng* para que al volver a identificarse sea posible capturar el *handshake* como vemos en la Figura 3-44.

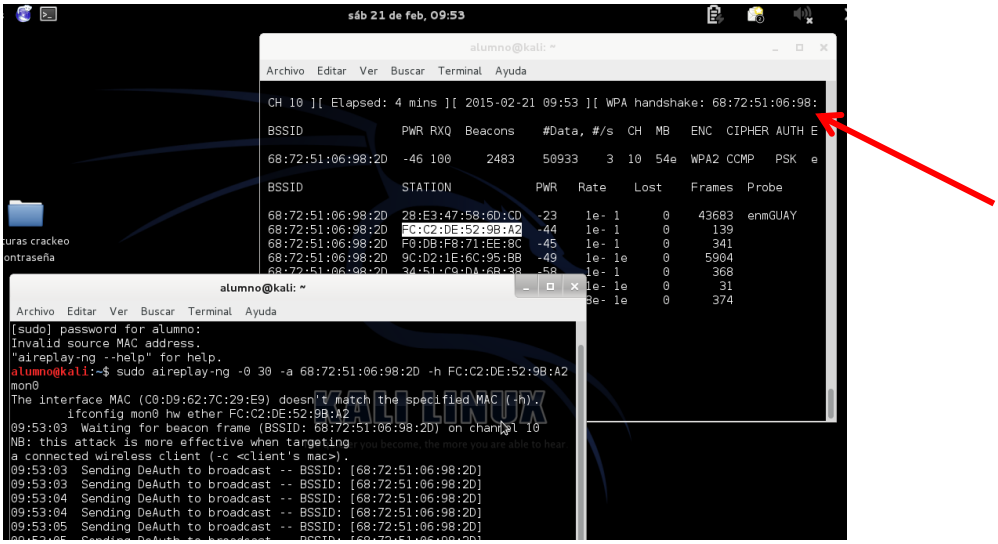


Figura 3-44 Obtención del *handshake*.

Finalmente, en la Figura 3-45, vemos la ejecución de *aircrack-ng* utilizando el diccionario llamado "*diccionario.txt"* y almacenado en el directorio llamado "*alumno"*. Vemos que se consigue romper la clave de acceso y se obtiene así la contraseña.

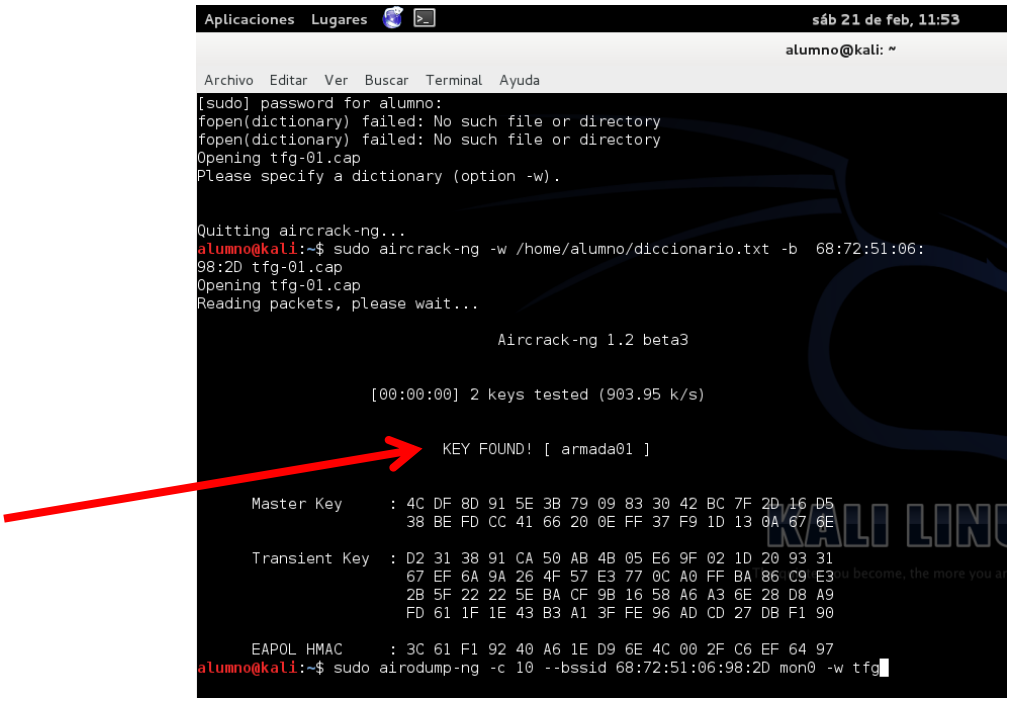


Figura 3-45 Clave de acceso descubierta.

3.3.2 Man in the Middle MIM.

Una vez hemos obtenido la clave de uno de los puntos de acceso, pasamos a monitorizar el flujo de datos en dicho punto de acceso realizando un ataque *Man in the Middle.* Para ello, empleamos la herramienta *ettercap.* Con este ataque, podemos obtener toda la información que uno de los usuarios intercambia con la red. *MIM* consiste en hacerle creer al usuario que nosotros somos el punto de acceso de forma que nos direccione todas sus peticiones a nuestro equipo, siendo así capaces de monitorizarlo y modificarlo, si se desea.

Abrimos la herramienta y realizamos una búsqueda de los *hosts* conectados a la red. Después, comenzamos a capturar el tráfico de datos e implementamos un *MIM* envenenando la *arp* de las víctimas. Esto no es más que modificar su tabla *arp.* La tabla *arp* recoge el listado de direcciones IP y sus MAC´s asociadas, incluida la de la puerta de enlace. Será aquí donde introduciremos nuestra MAC, así, todo el flujo de información de las víctimas queda redireccionado a nuestro ordenador. Para monitorizar lo que la víctima ve por pantalla hacemos uso de *driftnet*. El resultado es muy interesante vemos que se pueden controlar todas las conexiones existentes en la LAN a la que nos encontramos conectados. Por pantalla iban saliendo todas las imágenes que los diferentes compañeros iban viendo en sus pantallas. La Figura 3-45 muestra el escritorio de uno de los compañeros mientras realizaba una búsqueda por la red. Vemos que estaba navegando en el sitio web de la Armada viendo imágenes del Elcano.

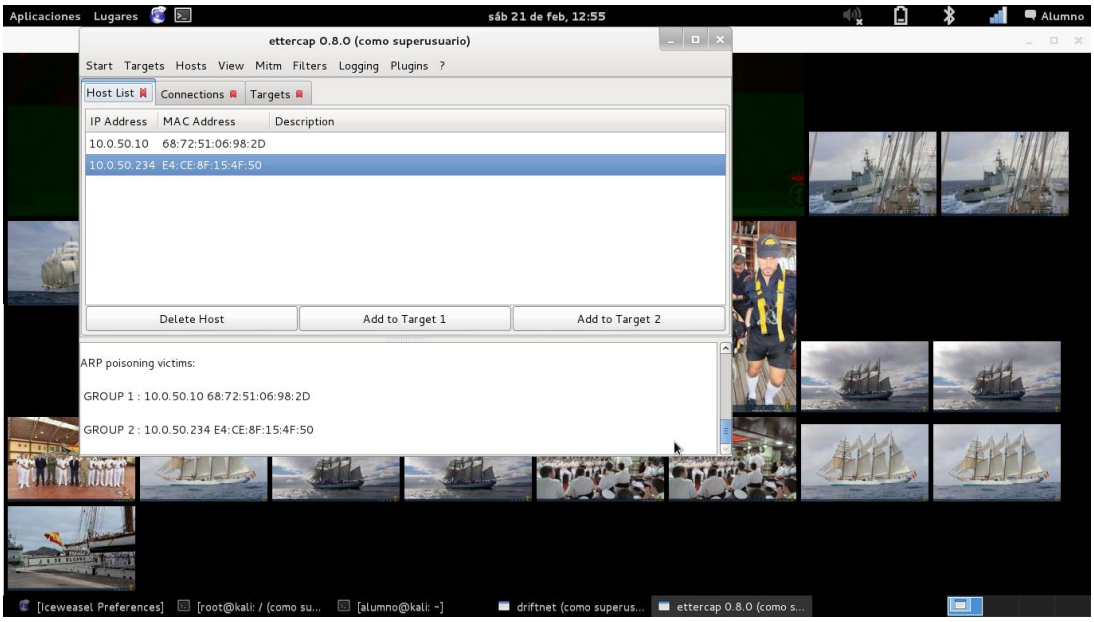


Figura 3-46 Monitorizando el equipo de un compañero.

Una vez tenemos monitorizado el ordenador de la víctima, podemos obtener sus credenciales cuando trate de acceder a su cuenta de correo, de Facebook, o a la web de la organización.

El siguiente paso será realizar un *DNS Spoofing*. Éste consiste en modificar la configuración del DNS, el cual asigna direcciones IP´s a las búsquedas nominales. Lo que hacemos ahora es redireccionar la página a la que se espera que deseen acceder los usuarios a nuestra IP. Si redireccionamos una página web a nuestra dirección IP, estaremos dirigiendo los datos que se introduzcan en esta página web a nuestro ordenador. Vemos como queda redireccionado el sitio web cud.uvigo.es a nuestra IP 10.0.50.153.

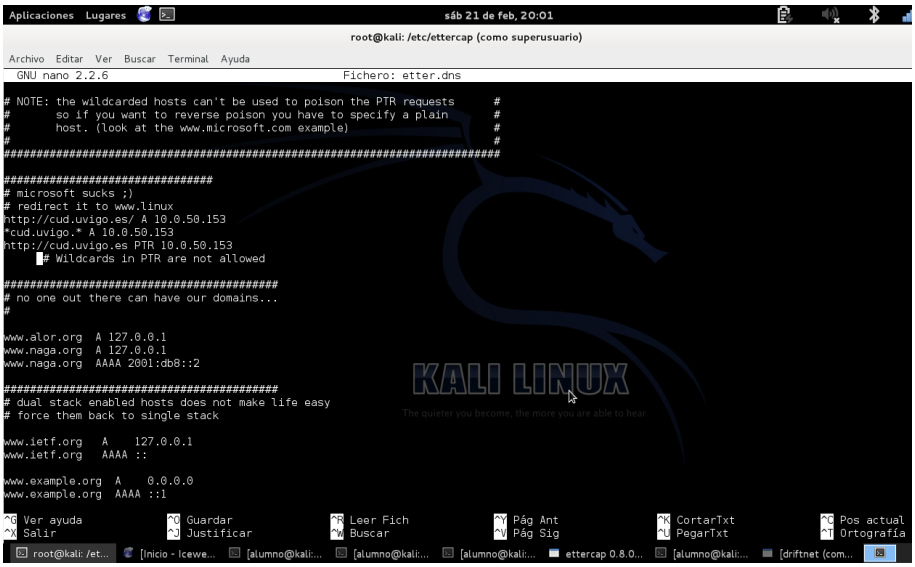


Figura 3-47 Modificación de DNS.config para redireccionar al usuario.

Tendremos que hacer uso de una herramienta más, *Setoolkit*, ya descrita en los apartados anteriores. Con *SET*, clonaremos la página web en cuestión como se muestra en la Figura 3-48. Por lo tanto, el resultado será el siguiente: el usuario que es víctima de un *MIM* intentará acceder a una página web direccionando la petición a través de nuestro ordenador.

Figura 3-48 Página clon del sitio web del CUD.

Le redireccionaremos a una página clon, idéntica a la que él desea acceder, pero que en realidad tiene como URL nuestra IP. Así, tras tratar de autenticarse, recibiremos en nuestro equipo usuario y contraseña de la víctima. Al haber modificado la configuración del DNS no aparecerá nuestra dirección IP en la barra del buscador, sino la dirección de la página en cuestión.

Si dejamos corriendo *ettercap*, vemos, en la Figura 3-49 cómo esta herramienta captura la clave y usuario que se ha introducido. En este caso, `profesor y profesor01`, a modo de ejemplo.

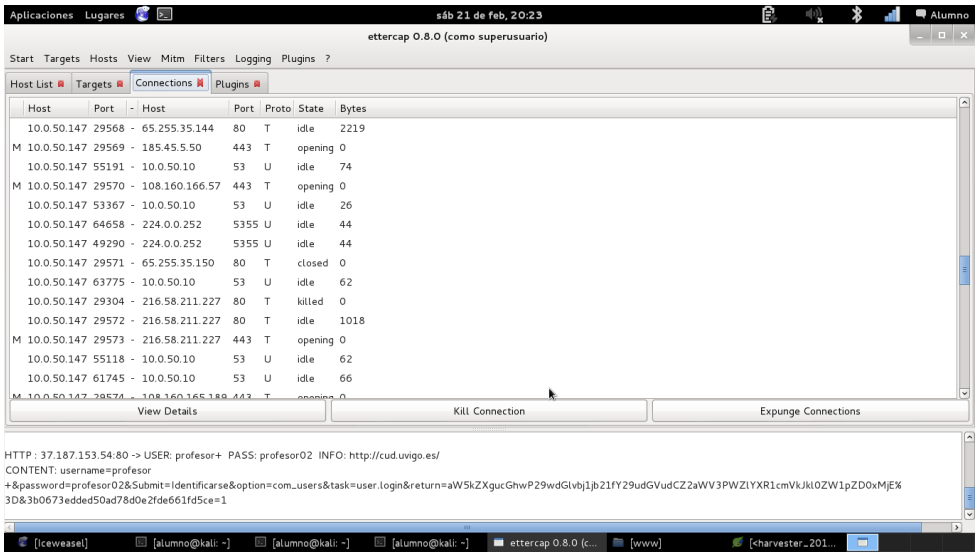


Figura 3-49 Captura de clave de acceso con *ettercap*.

Es necesario resaltar la infinidad de posibilidades que ofrece la ingeniería social y la posibilidad de crear página clon y obtener en nuestro ordenador la autenticación realizada por el usuario. Tras comentar a uno de los usuarios que estamos desarrollando una nueva página web y estamos realizando alguna prueba, ha accedido con su usuario y contraseña, abriendo así la puerta al atacante que pasa a tener acceso a la red. Dentro de la web, en la zona restringida a usuarios registrados, hemos podido comprobar que las posibilidades son muy amplias, ya que, como es de esperar, gran parte de la gestión se realiza a través de la web en la mayoría de las organizaciones hoy en día, y cada vez serán más las organizaciones que así lo hagan. Entre otras, nada más acceder, vemos que el sitio web nos ofrece la contraseña del punto de acceso inalámbrico *wcud*, por lo que ya son dos los nuevos puntos de acceso

que hemos conseguido tras este ataque. Además, existe la posibilidad de solicitar un permiso, modificar la domiciliación de la nómina que el empleado tiene con el centro, etc. También éste es un punto para la post-explotación hacia la consecución de las credenciales del administrador, pudiendo pivotar entre algún usuario más.

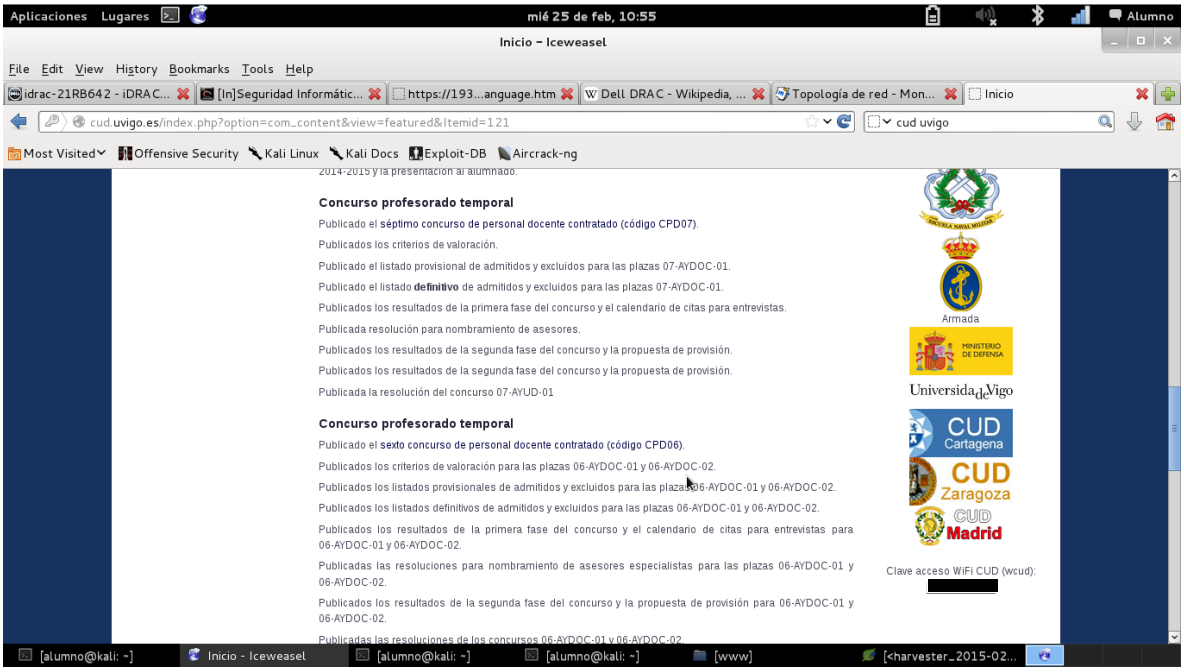


Figura 3-50 Acceso a la zona restringida para empleados del sitio web.

3.3.3 USB infectado.

Empleamos la herramienta *Setoolkit* la cual nos permite crear un *autorun*, un ejecutable en el ordenador que queramos atacar y que, dependiendo de la configuración, puede generar la apertura de una *Shell* en remoto, un túnel, etc. Esto lo podemos realizar a través de la opción *infectious media generator*. Podemos modificar el archivo para cambiar su apariencia y hacerlo más atractivo. Una de las opciones que permite es crear un archivo pdf. También se puede modificar su nombre. De esta forma, si introducimos el archivo en un *USB* que no contenga ningún otro archivo, lo dejamos en alguno de los pasillos de la organización y le damos un nombre del tipo: “fotocopia DNI.pdf” o “mejores playas de España.pdf”, etc, prácticamente nos estamos, asegurando que, si alguien decide coger el *USB* e introducirlo en su ordenador para comprobar que contiene o si puede averiguar quién es el propietario, abrirá el ejecutable.

Al realizar la prueba dentro de la red que estamos auditando, el archivo es detectado por el antivirus instalado, el cual procede inmediatamente a eliminar el archivo.

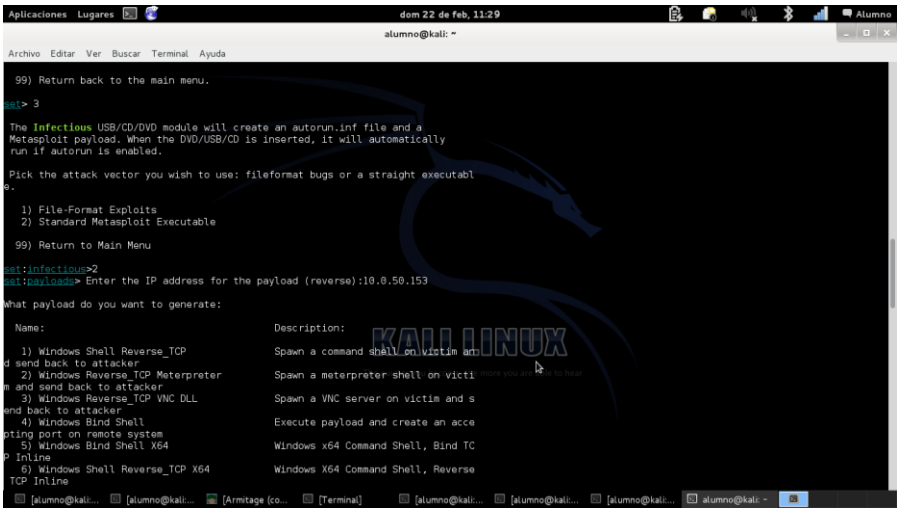


Figura 3-51 Proceso de creación del *autorun* empleando *Setoolkit.*

4 INTERPRETACIÓN DE LOS RESULTADOS

4.1 Descripción detallada de la auditoría.

4.1.1 Fundamentos del test de intrusión.

Como se ha mencionado en el apartado 3.1, se ha tomado como referencia el *Penetration Testing Execution Estándar*, y después se ha desarrollado una metodología propia. Este proceso se ha realizado por nivel de dificultad, es decir, se ha accedido primero a la información al alcance de todos, la información pública, como la mostrada en la página web de la organización, para ir avanzando hacia objetivos con mayor protección, como servidores y usuarios. De igual modo, y en coherencia con lo mencionado anteriormente, se ha comenzado atacando las partes de la organización alcanzables desde el exterior, para después, y a medida que íbamos consiguiendo cierta información, ir introduciéndonos en la red. Resumiendo, las piezas de toda organización más susceptibles de sufrir ataques son aquéllas que están más expuestas, la página web, los puntos de acceso inalámbrico, el tráfico de datos inalámbrico y, sobre todo, los usuarios. Volvemos a mencionar esa máxima de "toda cadena, es tan fuerte como lo sea su eslabón más débil". No se debe caer en el error de pensar que sólo las técnicas en las que son necesarios gran cantidad de conocimientos informáticos y programación son las adecuadas. Si somos capaces de obtener cierta información de la manera más simple, el atacante también lo es, y son estas técnicas las que menos rastro dejan y menos sospechas levantan dentro de la empresa. Esto se

ha podido apreciar claramente al lograr acceder al servidor [redacted] y abrir una *Shell* tras haber capturado la clave y usuario de *cámara.* Esto ha sido posible después de capturar el tráfico en *wcud.* A su vez, se ha podido realizar este *sniffing* debido a que se había accedido a la página web a través del uso de la ingeniería social, consiguiendo las credenciales de uno de los empleados que se autenticó en una página falsa redireccionada a nuestra IP, y en ésta aparecía la clave de acceso a este punto de conexión WiFi. Vemos así las consecuencias que puede tener una falta de seguridad a cualquier nivel.

4.1.2 La auditoría paso a paso.

El primer punto a explotar ha sido el sitio web, por ser uno de los elementos más expuestos. Toda información es importante y puede hacer que todo encaje en momentos posteriores, cuando la cantidad de información con la que se trabaje sea muy elevada y toda ayuda sea buena para terminar de entender la función de cierto elemento dentro de la red o los usuarios que manipulan este elemento y por qué ellos y no otros. El procesar gran cantidad de información también nos hará avanzar en la dirección adecuada, evitando perdernos en el proceso con elementos que carecen de interés.

Tras analizar toda la información disponible se obtiene una estructura de la organización, sabiendo quien ocupa cada puesto, sus correos y sus teléfonos. Los teléfonos, aunque puedan parecer inútiles para el ataque posterior, son de utilidad. Siempre se puede recibir una llamada del servicio informático que gestiona la red de la empresa advirtiendo de que se están realizando ciertas pruebas y es necesario que el usuario acceda con su clave para verificar el buen funcionamiento del servicio. El número de usuarios que expondrían sus credenciales de esta forma es bastante elevado en la mayoría de las organizaciones. Desde este momento, ya podríamos empezar a interactuar con los usuarios.

El siguiente paso ha sido determinar la topología de la red. La primera posibilidad de ataque, tras conocer la estructura de la red, podrían ser los mencionados puntos de acceso inalámbricos, puntos de acceso físicos poco protegidos o el ataque físico en sí a alguno de los servidores o equipos. En un primer escaneo, vemos quienes son los usuarios que están empleando la red local, como observamos en la Figura 3-7. En un segundo escaneo, avanzando en los escalones obtenidos al hacer un *traceroute* en la red, vemos que es en este nivel donde se encuentran todos los servidores, *routers*, puntos de acceso y demás elementos de interés que permiten el uso y la gestión de la red, y que, evidentemente, son de mayor interés. En este momento, nos limitamos a recoger toda la información posible y posteriormente se pasará a interpretarla.

Después pasaremos a lograr el acceso a través de uno de los puntos de acceso. Para ello, podemos hacer uso de la ingeniería social o de las diferentes de herramientas que se han mostrado, que son de utilidad para romper las claves de acceso. Tras analizar los diferentes puntos de acceso, se atacará aquél con el menor nivel de seguridad. En el capítulo anterior, se han expuesto los dos casos. Hemos sido capaces de ejecutar un ataque por diccionarios a uno de los puntos de acceso inalámbricos, como se muestra en el apartado 3.3.1 y, también, se ha empleado la ingeniería social, para adquirir usuario y contraseña de uno de los empleados, y tener así acceso a la página web y como consecuencia a otro de los puntos de acceso inalámbrico.

En el caso de la red del CUD, los puntos de acceso tienen seguridad WAP y las claves son de la complejidad necesaria para hacer inviable un ataque por fuerza bruta. Así mismo, no se han encontrado diccionarios públicos que contuviesen la clave de acceso, por lo que se pone de manifiesto que el nivel de protección es adecuado.

El tener acceso a uno de estos puntos de acceso inalámbricos implica que somos capaces de monitorizar toda la información que los diferentes usuarios intercambian con la red tras realizar un *MIM* y, de forma sencilla, obtener toda la información personal de los usuarios. Se puede redireccionar a los usuarios a las páginas deseadas logrando así adquirir más credenciales dentro de la red de la organización.

Se probó también el ataque directo a varios de los ordenadores de la red, introduciendo un *USB* infectado. El antivirus instalado en los equipos de la red lo detectó inmediatamente, destruyendo el archivo, mostrando ser eficiente ante un ataque de esta naturaleza.

No existe la metodología estándar de modo que siempre se pueda emplear un mismo procedimiento. Como hemos visto, hay ciertos recursos para el atacante o el *pentester* que tienen infinidad de posibilidades.

Como último test, se ejecutó el ataque sobre los diferentes servidores de la red siendo éste el ataque de mayor interés, y el más laborioso, ya que son estos los equipos más importantes dentro de la red. Lograr acceder a dichos equipos y a la información almacenada dentro de los mismos implicaría un amplio abanico de posibilidades para el atacante aunque no suele ser tarea fácil.

Este ataque se ha llevado a cabo empleando diferentes herramientas para contrastar la información obtenida con todas ellas. Se realizaron escaneos intensivos con *Nmap y Zenmap,* se empleó *Whatweb* y *Nikto,* también se empleó *armitage* y *metasploit,* y se analizaron todos los *hosts* a través de la barra de búsqueda, probando también si montaban el servicio *Samba.* El atacante podrá conseguir gran cantidad de información si después de todo este análisis realiza una búsqueda de cada uno de los servicios que monta cada *host.* Así, vemos que se puede determinar tanto qué tipo como el sistema operativo de cada uno de los *routers* y *switches* de la red. Todos ellos deben estar protegidos con usuario y contraseña con cierta complejidad, como ya se ha mencionado en apartados anteriores y, en ningún caso, se debe mantener el usuario y clave por defecto, pues, en este caso, el atacante lo encontrará, accederá y podrá incluso modificar la clave, pasando a tener este servidor bajo control.

En los servidores de almacenamiento de archivos, y que montan *samba,* tras un análisis con *nikto,* vemos que la causa de que seamos capaces de ver los archivos almacenados y los usuarios registrados en el servidor es tener el modo *negotiation_multiview* activado en *Apache.* Esto, como se viene explicando en el capítulo anterior, permite que un usuario detrás de un *proxy* sea capaz de ver el listado de los directorios. La solución sería implementar la otra posibilidad que admite *Apache,* el modo *type maps,* el cual para ver un archivo, requiere que el usuario implemente previamente la ruta al directorio, siendo así necesario, que el usuario conozca previamente el directorio. Este modo sería un poco menos eficiente para los usuarios y ya que, mantener los directorios visibles no es una vulnerabilidad importante, se suele emplear el modo *multiview.* Es al ver estos directorios y usuarios, y tras comparar con la información recogida inicialmente en la web, que somos capaces de deducir qué *host* es empleado, por ejemplo, en la secretaría.

Comenzaría aquí un proceso ya mucho menos lineal, que consistiría en incidir desde distintos enfoques, en las posibles vulnerabilidades. También se debería emplear todo lo posible Internet para conocer a fondo cada servicio empleado en cada uno de los servidores, modelos de *switches* y *routers* y emplear esta información para lanzar nuevos ataques.

Resumiendo, éstas son las principales vulnerabilidades detectadas y los puntos fuertes dentro de la red:

1. Vulnerabilidades:
   - Uno de los empleados entrega sus credenciales al atacante.
   - Tras capturar el tráfico de datos en *wcud* se obtienen las credenciales de un nuevo usuario *camara.*
   - Se abre una *Shell* sobre el servidor [redacted] tras autenticarnos con el usuario *camara.*
   - Se observan los directorios contenidos en los servidores que montan el servicio *Samba.*
   - Se observan los usuarios registrados en los servidores que montan el servicio *Samba.*
   - Se accede al servidor del controlador de acceso remoto como administrador cambiando la contraseña.
   - Se demuestra que la aplicación que usan los empleados para fichar es susceptible de sufrir un ataque XSS.

- Se monitoriza la actividad de los usuarios en el cuartel de alumnos.

2. Puntos fuertes:
   - Clave de acceso a los puntos de conexión WiFi seguras.
   - Archivos protegidos dentro de los directorios a los que se ha tenido acceso. No se tiene acceso a la información contenida en los mismos.
   - Sistema antivirus eficaz contra ataque a través de un USB.
   - Sitio web seguro frente a ataques XSS.

4.1.3 Soluciones e informe final.

Para seguir el mismo orden que se ha llevado hasta ahora, comencemos por las partes más expuestas y más visibles. La información de la página web se debe elegir siempre teniendo en cuenta la seguridad informática, no poniendo en manos del atacante información muy útil para acceder a la red. De todos modos, como es habitual dentro de la ingeniería, se debe tener en cuenta que todo radica en una solución de compromiso, en este caso, entre la información expuesta y la accesibilidad a la organización y a sus empleados por parte de organizaciones externas.

En cuanto a los usuarios, y ésta es la medida clave por excelencia, se les debe de concienciar a través de charlas formativas en las que llegue a exponerse el amplio abanico de posibilidades y la cantidad de información, tanto personal como corporativa, que va a quedar expuesta si no siguen los procedimientos estándar de seguridad de la organización.

Dicho esto, es evidente que toda organización debe contar con una política de seguridad informática conocida por todos sus empleados y lograr que estos la empleen día a día. De no ser así, sería también imposible que el usuario actúe de forma segura.

La principal medida a tomar por la organización será establecer la política de seguridad informática que proteja la red de forma adecuada. Debe ser una política clara y concisa, con ejemplos prácticos y que se entienda por todos, evitando el uso de tecnicismos, en la medida de lo posible. Después, a través de actividades formativas, es necesario que el empleado conozca esta política, la entienda, y comprenda la necesidad de emplearla por el bien de la organización y de su privacidad. Además, es necesario mantener informado al usuario de la variedad de ataques que existen y que van apareciendo, y que podría sufrir realizando su trabajo. Hecho esto, conseguiremos un nivel de seguridad adecuado en las capas más expuestas y más vulnerables. Ésta será la clave para el éxito y la seguridad de la organización.

Todo servidor, *router* o *switch* debe encontrarse protegido. Para que esta protección sea adecuada se deben emplear contraseñas fiables. Dependiendo del nivel de importancia del servicio dentro de la red, se protegerá con una clave más compleja. Esto se logra, por ejemplo, estableciendo una periodicidad para modificar la clave, y unos requisitos en cuanto a patrón y longitud. También se debe obligar a los usuarios a esta política de seguridad. El dejar un servidor con el usuario por defecto es igual que dejar la puerta de casa abierta cuando no estamos. Siempre que se instale un nuevo servidor, se deberá modificar el usuario administrador y su clave en el momento.

Es importante también contar con un antivirus y un *software* de protección adecuado en cada uno de los equipos, y sobre todo, mantenerlo actualizado, pues se descubren nuevas vulnerabilidades cada día.

Resumiendo hasta aquí, las soluciones a las vulnerabilidades detectadas son las siguientes:

- Las dos vías para hacer frente a un ataque por medio de la ingeniería social son: el ser selectivo con la información pública de la organización y el lograr una conciencia de seguridad informática en cada uno de los empleados.

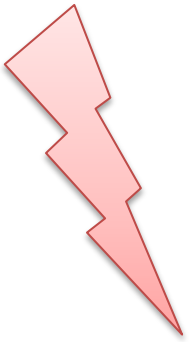
- Para evitar ceder las credenciales de alguno de los usuarios a través de una captura de datos en un punto de acceso inalámbrico se deben enviar estas de modo seguro.
- Se puede evitar el acceso a un servidor o a un punto de acceso inalámbrico por parte de un atacante si se limitan los accesos a estos servidores a través de las MAC con acceso permitido. Aunque en el caso de que un usuario quiera emplear un nuevo dispositivo, si se mantiene el filtrado MAC, deberá solicitar permiso al administrador.
- Como se ha mencionado se puede evitar que sean visibles los directorios y usuarios registrados de los diferentes servidores modificando la configuración de *Apache* en los servidores, desactivando el modo *multiview*.
- Se pueden proteger las distintas páginas web y aplicaciones frente a ataques XSS empleando filtros que deshabiliten la posibilidad de introducir código en la fuente de la página web del tipo *htmlspecialchars*.
- Se deben modificar todas las claves, no permaneciendo ninguna de las establecidas por defecto, y empleando una clave con un nivel de seguridad alto, como se ha descrito anteriormente.

La red auditada posee un nivel adecuado de seguridad. Aun así, se deben emplear las medidas antes mencionadas. Hacer hincapié en la necesidad de que todo usuario de la red ha de ser consciente de que la posibilidad del ataque es algo real y habitual y que las consecuencias pueden ser nefastas para la organización, y para su privacidad. Se considera necesario establecer un coloquio informativo para todos los usuarios de la red de forma semestral, así como implementar y hacer pública una política de seguridad informática dentro de la organización y tomar las medidas necesarias para que sea conocida y llevada a cabo por todos. Es necesario comprender que una red será tan segura como lo sean todos sus elementos. De nada sirve tener un nivel de seguridad excelente en cada uno de los puntos de acceso o de los servidores, si uno de nuestros empleados u otro de los servidores en el que se almacenan todas las claves no lo tienen. Mantener la seguridad en la red es un trabajo constante y requiere de un esfuerzo por parte de todos, el éxito para el atacante, sin embargo, solo requiere de "un día de suerte".

Mencionar por último, que como ya se ha comentado, es importante alcanzar la relación de compromiso adecuada entre seguridad y disponibilidad o accesibilidad. El tener expuesta una información que carezca de relevancia y que no compromete la seguridad no implica ser vulnerable.

A continuación, se muestra un ejemplo de cómo sería un informe. En él se recogen los puntos principales de la auditoría de forma visible y sencilla a ojos del contratante.

Informe final



Vulnerabilidades:

- Obtenida clave de acceso de un empleado.
- Obtenida clave de acceso a través de la actividad de la cámara.
- Abierta *Shell* en [redacted] con el usuario cámara.
- Directorios visibles en los servidores con servicio *samba*.
- Usuarios visibles en los servidores con servicio *samba*.
- Acceso a un servidor con privilegios de administrador.
- Página susceptible de taques XSS
- Monitorizada la actividad en la red de parte de los usuarios.

Consecuencias:

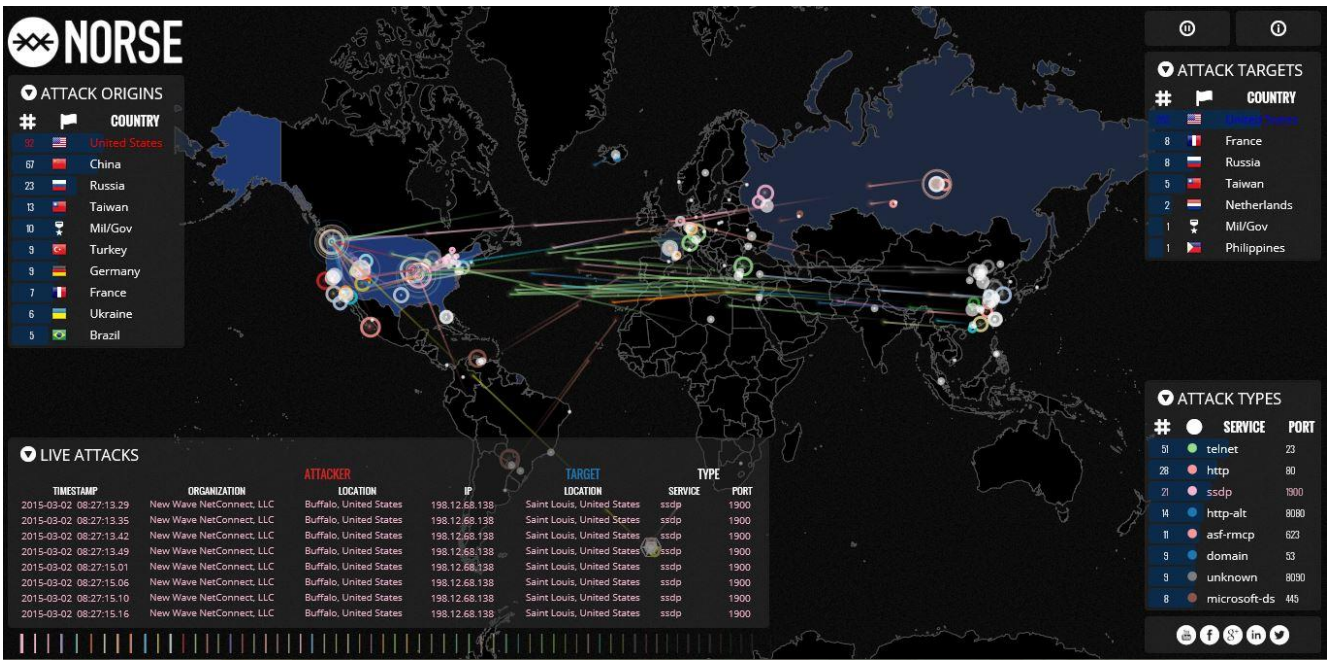
- Posibilidad de modificar el contenido en alguno de los servidores. Grave.
- Posibilidad de escalar alcanzando mayores privilegios. Medio.
- Posibilidad de romper la privacidad de los usuarios. Medio.
- Posibilidad de modificar una página de la organización. Baja.

Soluciones:

- Ser selectivo con la información pública de la organización y el lograr una conciencia de seguridad informática en cada uno de los empleados.
- Se deben enviar las credenciales de modo seguro.
- Limitar el número de usuarios en los puntos de acceso a través de las MAC permitidas.
- Emplear filtros que deshabiliten la posibilidad de introducir código en la fuente de la página web del tipo *htmlspecialchars*.
- Establecer claves de acceso con un nivel de protección alto.

Pentester: Armando Rubio García. Fecha de informe: 06/03/2015

5 CONCLUSIONES Y LÍNEAS FUTURAS



5.1 Conclusiones generales.

Tras haber realizado este trabajo, es momento de comprobar si se han alcanzado los objetivos establecidos inicialmente.

En cuanto al contexto en el que se enmarca la obra, en primer lugar, se ha adquirido una visión clara de la situación actual en Ciberdefensa en los organismos en los que se encuentra integrada España, como son, la OTAN y la UE, además de conocer los planes y estrategias implementados por el Gobierno español. Se adquieren, tras la lectura de la obra, por todo aquel que no posea ningún conocimiento inicial en materia de Ciberseguridad, unos conocimientos básicos al respecto y, sobre todo, conciencia de cuál es la situación actual en este campo, es decir, de la guerra que se está librando cada día a través de la red. Del mismo modo, se aprecia la infraestructura a nivel internacional y nacional en materia de Ciberdefensa, que se está desarrollando, conociendo cuál es su estructura básica, las relaciones entre los distintos organismos y cuál es el papel que juega cada uno de los actores principales que interactúan en éste. Todos los gobiernos occidentales han implementado unas líneas de acción para hacer frente a esta amenaza que se ha alzado como una de las más importante de las amenazas actuales para un Estado. En este TFG se han presentado y comentado las estrategias planteadas por la OTAN, la UE y el Gobierno español. Así, el lector de la obra conoce ya cuales son

los objetivos que se han marcado estas organizaciones y nuestra nación, y el modo en que han planeado alcanzarlos. Además, se están llevando a cabo ejercicios combinados entre las distintas naciones aliadas y creando centros de formación, con el fin de mejorar la formación en Ciberdefensa. Se están ejecutando programas de concienciación a todos los niveles, así como trabajo coordinado y conjunto entre distintos organismos del Estado, tanto públicos como privados.

Se ha trabajado con un gran número de herramientas, reconociendo que los conocimientos iniciales eran muy básicos. Tras haber realizado este TFG, se han adquirido unos conocimientos razonables y se ha logrado familiarizarse con cada una de las herramientas utilizadas las cuales eran totalmente desconocidas al inicio de la obra. Se tiene ahora una visión clara de algunas de las plataformas que existen en el mercado de la auditoría informática y de gran parte de las herramientas que éstas recogen. Este proceso de familiarización requiere paciencia y tiempo, existe gran cantidad de información disponible en la red y en una abundante bibliografía en formato libro o publicación. En la bibliografía se citan gran parte de estas fuentes. Todo aquel que lea este TFG obtendrá unos conocimientos básicos acerca del funcionamiento de dichas herramientas, los cuales pueden ser reforzados si a la par se trabaja de forma práctica con las propias herramientas, y se realiza un pequeño trabajo autodidacta y de investigación propia en la red.

Por último, se ha realizado el test de intrusión del modo previsto, secuencial y gradualmente, de fácil comprensión y seguimiento por cualquiera sin grandes conocimientos en auditoría de red. En primer lugar, se desarrolla un propio plan para llevar a cabo el test de intrusión el cual se detalla en el capítulo cuatro. Se ejecuta este plan y se registra cada uno de los pasos seguidos mostrándolos en el capítulo anterior acompañados de una explicación detallada que permite su seguimiento de forma fácil y amena.

Se han encontrado ciertas vulnerabilidades y se ha comprobado que la red tiene un nivel de seguridad alto. Finalmente, se han realizado una serie de recomendaciones o posibles soluciones para paliar estas vulnerabilidades encontradas. Estas recomendaciones son las que entregaría en modo de informe una empresa privada al auditar nuestra red.

Debido al bajo nivel de conocimientos con el que se ha comenzado al inicio de este TFG y al tiempo limitado, no se ha podido avanzar más en el test de intrusión, lo que no quiere decir que no existan muchas más posibilidades, las cuales se plantean como líneas futuras. La parte que ha sido menos trabajada es la parte de post-explotación y aquellas que requieren mayor tiempo para su desarrollo.

5.2 Líneas futuras.

Como líneas futuras, en caso de que un futuro auditor esté dispuesto a continuar este TFG y testar de nuevo la seguridad de la red, apoyándose en esta obra, puede familiarizarse con las herramientas de *pentesting*. El futuro auditor puede pasar a comprobar si la situación es similar a la expuesta en esta obra, y de ser así, continuar el trabajo aquí recogido. Lo primero sería lograr comprender la estructura de la red y la funcionalidad de cada uno de sus elementos. Después podría avanzar. Para ello, debería seguir un proceso mucho más convergente y cíclico. Una de las posibilidades sería la de pivotar entre los diferentes usuarios, tratando de ganar los derechos de administración de la red. Esto consistiría en intentar obtener las credenciales de los diferentes usuarios registrados ya sea a través de la captura de datos o del empleo de la ingeniería social. Existen algunas páginas en la red susceptibles de un ataque XSS. Podría tratar de obtener credenciales por esta vía. Para ello tendría que hacer uso de un servidor de uso gratuito como los que podemos encontrar en la red. Encontrará más información al respecto en foros y tutoriales que detallan el proceso al ejecutar este tipo de ataques. Y evidentemente, debería explotar en gran medida la ingeniería social, ya que se ha mostrado como una de las mayores vulnerabilidades en la red auditada y, en cualquier organización considerando toda la información aquí expuesta. De implementarse las medidas aquí recomendadas, sería oportuno verificar así si son de utilidad y si existen otras complementarias que eleven la seguridad en la red. También han de tenerse

en cuenta todas las posibles actualizaciones y novedades que hayan surgido tanto en la red y su topología como en cada uno de sus elementos tanto a nivel de *hardware* como de *software*. Esto en cuanto a una posible continuación del TFG aquí expuesto. A modo de resumen, las futuras líneas de acción que se recomienda tome el futuro *pentester* que continue este TFG son las siguientes:

- Aplicar *exploits* específicos de *metasploit* sobre los servidores.
- Ejecutar las técnicas XSS indicadas en los capítulos anteriores
- Realizar un ataque DoS
- Penetrar en las redes locales protegidas por los *routers* detectados. La presencia de *firewall* hace intuir que existe algo importante al otro lado.
- Utilizar la ingeniería social.

5.3 Conclusión personal.

En cuanto a la ciberdefensa, resumir todo lo expuesto en esta obra. Se trata de una amenaza constante, actual, nos afecta cada día y en la mayoría de los casos, es invisible para la gran mayoría de los usuarios. Por esto, el único modo de mantener la seguridad en la red es con la aplicación y ejecución de un plan de seguridad y una serie de medidas que nos protejan frente a los atacantes. Todo esto llevado a cabo con la máxima disciplina. Un fallo de seguridad, un punto vulnerable, y será suficiente para ser susceptibles de sufrir un ataque y que el resto de la seguridad implementada no sirva de nada. Que vamos a ser atacados es prácticamente una realidad si hablamos de grandes organizaciones con gran influencia en el mercado y con relevancia en el sector de la innovación. Del mismo modo, las Fuerzas Armadas y los organismos vinculados a Defensa de prácticamente todos los países desarrollados también van a ser víctimas de estos ataques. Solo resta, por tanto, implementar una buena defensa y estar preparados. La clave del éxito se sustenta sobre dos pilares fundamentales: la preparación previa a sufrir el ataque (estrategias, planes, infraestructuras, formación, concienciación, cultura de Defensa, etc., y el trabajo conjunto entre los distintos organismos tanto a nivel nacional como internacional.

6 BIBLIOGRAFÍA

[1] «Web de La Razón, ciberataques durante el 2014» http://www.larazon.es/detalletecnologia/noticias/8662923/sociedad+tecnologia/espana-tercer-pais-del-mundo-que-mas-ciberataques-recibio-en-2014#.Ttt1vULChyF60hK [Ultimo acceso: 07 Febrero 2015]

[2] «Web de El País, actualidad de la Ciberdefensa» http://elpais.com/elpais/2014/12/15/opinion/1418671318_894689.html [Último acceso: 07 Febrero 2015]

[3] Ley Orgánica 5/2005 de 17 de noviembre, Jefatura del Estado, BOE 18 noviembre de 2005, núm. 276, página 37717; Ley de la Defensa Nacional.

[4] Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. «BOE» núm. 150, de 23 de junio de 2007, páginas 27150 a 27166 (17 págs.)

[5] Informe Anual de Seguridad Nacional. Gobierno de España. Presidencia del Gobierno. Departamento de Seguridad Nacional.

[6] Estrategia de Seguridad Nacional, Un Proyecto Compartido. Gobierno de España. Presidencia del Gobierno.

[7] Estrategia de Ciberseguridad Nacional 2013. Gobierno de España. Presidencia del Gobierno.

[8] BOD núm. 40, Martes 26 de febrero de 2013, Sec. I, Página 4154, Orden Ministerial 10/2013, de 19 de febrero, por la que se crea el Mando Conjunto de Ciberdefensa de las Fuerzas Armadas.

[9] «Web de El Mundo, Guerra informática en Serbia» http://www.elmundo.es/navegante/99/abril/16/hackers.html [Último acceso: 07 Febrero 2015]

[10] «Web de El País, el ataque sufrido por Estonia» http://elpais.com/diario/2009/05/30/internacional/1243634402_850215.html [Último acceso: 07 Febrero 2015]

[11] «Web del IEEE Instituto Español de Estudios Estratégicos, evolución de los ataques» https://www.esup.edu.pe/descargas/boletines/julio/5%20la%20amenaza%20cibernetica.pdf [Último acceso: 07 Febrero 2015]

[12] Documento informativo del IEEE 09/2011, Nuevo Concepto de Ciberdefensa de la OTAN.

[13] «Web del Parlamento Europeo, política de Ciberddefensa» http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A7-2012-0335+0+DOC+XML+V0//ES [Último acceso: 07 Febrero 2015]

[14] Henning Wegener, La Ciberseguridad en la Unión Europea, IEEE.

[15] Cybersecurity Strategy o the European Union: An Open, Safe and Secure Cyberspace, Brussels 07/02/2013, European Commission.

[16] «Web de 20minutos, amenazas cibernéticas» http://www.20minutos.es/noticia/2323397/0/amenazas-2015/robo-credenciales/ciberguerra/ [Último acceso: 07 Febrero 2015]

[17] Ciberseguridad. Retos y amenazas la seguridad nacional en el ciberespacio, Ministerio de Defensa. Cuadernos de Estrategia 149. Instituto Español de Estudios Estratégicos.

[18] «Wikipedia, la web profunda» http://es.wikipedia.org/wiki/Internet_profunda [Último acceso: 07 Febrero 2015]

[19] «Web de El Mundo, Internet profunda» http://www.elmundo.es/tecnologia/2014/04/06/53411182268e3ec11c8b456b.html [Último acceso: 07 Febrero 2015]

[20] Guía de Seguridad de las TIC (CCN-STIC-406), Seguridad en Redes Inalámbricas basadas en el estándar 802.11. Centro Criptológico Nacional. Gobierno de España. Ministerio de la Presidencia.

[21] «Web de Microsoft, elementos de la red» http://windows.microsoft.com/en-us/windows/hubs-switches-routers-access-points-differ#1TC=windows-7 [Último acceso: 11 Febrero 2015].

[22] Informe de amenazas CCN-CERT IA-03/14, Ciberamenazas 2013 y tendencias 2014.

[23] «Web de EFE: Empresas, ataques cibernéticos» http://www.efeempresas.com/noticia/las-empresas-cada-vez-mas-expuestas-a-los-ataques-ciberneticos/ [Último acceso: 18 Febrero 2015].

[24] «Web de Nmap» http://nmap.org/ [Último acceso: 23 Febrero 2015].

[25] «Web de aircrack-ng» http://www.aircrack-ng.org/ [Último acceso: 23 Febrero 2015]

[26] «Web de Social-Engineer Toolkit» https://www.trustedsec.com/social-engineer-toolkit/ [Último acceso: 23 Febrero 2015]

[27] «Web de OwaspZap» https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project [Último acceso: 23 Febrero 2015]

[28] «Web de thehackerway, tutorial *Maltego*» http://thehackerway.com/2011/08/02/conceptos-basicos-avanzados-y-herramientas-de-footprintingfingerprinting-%E2%80%93-maltego/ [Último acceso: 23 Febrero 2015]

[29] «Web de Nikto» https://cirt.net/Nikto2 [Último acceso: 23 Febrero 2015]

[30] «Web de WhatWeb» http://whatweb.net/ [Último acceso: 23 Febrero 2015]

[31] «Web de Metasploit» http://www.metasploit.com/ [Último acceso: 23 Febrero 2015]

[32] «Web de Ettercap» http://ettercap.github.io/ettercap/ [Último acceso: 24 Febrero 2015]

[33] «Web de FastandEasyHacking, *Armitage*» http://www.fastandeasyhacking.com/ [Último acceso: 24 Febrero 2015]

[35] «Web de BackBoxLinux» (www.concise-courses.com/security/kali-linux-vs-backbox) [Último acceso: 23 Febrero 2015]

[36] P.González, G.Sánchez y J.M Soriano, Pentesting con Kali, Editorial 0xWORD, 2013.

[37] «Web de NodeZero» http://www.nodezero-linux.org/ [Último acceso: 24 Febrero 2015]

[38] «Web de IPaddress, localización de la IP del CUD» http://cud.uvigo.es.ipaddress.com/ [Último acceso: 25 Febrero 2015]

[39] «Web del Centro de Excelencia para la Ciberdefensa de la OTAN » https://ccdcoe.org/ [Último acceso: 2 de marzo de 2015]

[40] Imagen ejemplo de *Wardriving* http://www.wlanbook.com/wp-content/uploads/2010/09/ekoparty-wardrive-2008.jpg [Último acceso: 3 de marzo de 2015]

[41] Escritorio de BackBox http://www.linuxuser.co.uk/wp-content/uploads/2012/01/backbox2-tools.png [Último acceso: 3 de marzo de 2015]

[42] Logotipo de NodeZero http://3.bp.blogspot.com/_2WIz3mHrq6Q/TS9CwvkdUmI/AAAAAAAAAR4/bNg_NF_GyCc/s1600/NdZ4.jpg [Último acceso: 3 de marzo de 2015]

[43] «Web de *Penetration Execution Test Standard*» http://www.pentest-standard.org/index.php/Main_Page [Último acceso: 03 de marzo 2015]

[44] «Web de Microsoft, elementos de la red» http://windows.microsoft.com/en-us/windows/hubs-switches-routers-access-points-differ#1TC=windows-7 [Último acceso: 05 de marzo 2015]

[45] «Web de seguridad.internautas, *hackear* a través de las *cookies*» http://seguridad.internautas.org/html/4304.html [Último acceso: 05 demarzo de 2015]

[46] «Web del Confidencial, ataque en la web de presidencia del gobierno» http://www.elconfidencial.com/espana/hacker-web-presidencia-espanola-foto_mrbean_20100104.html

[Último acceso: 04 de marzo de 2015]

[47] «Web del CERT» https://www.ccn-cert.cni.es/ [Último acceso: 05 de marzo de 2015]