ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN

“Análisis Experimental del Estado de Seguridad en la Red Inalámbrica de la ESPOL mediante Ataques Controlados detallando Vulnerabilidades y presentando Técnicas de Prevención y Mitigación”

INFORME DE PROYECTO DE GRADUACIÓN

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN TELEMÁTICA

Presentado por

José María Briones Venegas

Mario Alejandro Coronel Peláez

Guayaquil - Ecuador

AÑO 2013

AGRADECIMIENTO

Agradezco inmensamente a mis padres por su constante apoyo incondicional durante mi vida estudiantil ya que ellos fueron el pilar fundamental para la consecución de este título.

Al Ing. Ignacio Marín por sus consejos para la realización de este trabajo y un especial agradecimiento para la Ing. Patricia Chávez por su iniciativa y esfuerzo para que parte de este trabajo sea publicado internacionalmente.

José María Briones Venegas

AGRADECIMIENTO

Agradezco a Dios por la vida y la sabiduría, a mi familia por la unión y respaldo que siempre me han brindado, a mi madre por su esfuerzo y consejos oportunos, a mi padre y hermanos por el aliento y la compañía, a mi esposa por su gran apoyo y cariño que fueron parte fundamental para finalizar el proyecto, a mi hijo por la motivación e inspiración que me harán conseguir muchos más logros.

Agradezco a mis Profesores por la paciencia y entrega hacia mí, principalmente a la Ing. Patricia Chávez por su gran colaboración dentro de mi formación de Igual Manera al Ing. Ignacio Marín y al Ing. Gonzalo Luzardo por su gran apoyo.

Mario Alejandro Coronel Peláez

DEDICATORIA

Quiero dedicar este proyecto a Dios, a mis padres Victoria Elizabeth y Luis Briones por su paciencia y por estar siempre conmigo, a todos mis profesores que aportaron a mis conocimientos actuales, a mis amigos que de alguna manera me incentivaron durante mis años de estudio y a mi novia Johanna.

José María Briones Venegas

Dedico este Proyecto a Dios por guiarme siempre en el buen camino, a mi familia por el amor que siempre me entrego, a mi esposa e hijo por el apoyo incondicional y el cariño que siempre fueron parte fundamental.

Mario Alejandro Coronel Peláez

TRIBUNAL DE SUSTENTACIÓN

Director

Ing. Patricia Chávez

Sub Decano

Dr. Boris Vintimilla

Vocal Principal

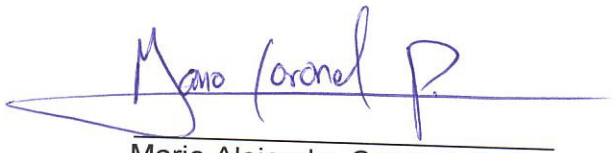
Ing. Gonzalo Luzardo

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este informe, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

(Reglamento de Graduación de la ESPOL)

José María Briones Venegas



Mario Alejandro Coronel Peláez

RESUMEN

Este proyecto se enfocó en la seguridad de la red inalámbrica implementada en la ESPOL, a la cual todos los usuarios con cuentas del dominio espol.edu.ec tienen acceso, mediante ataques controlados. Se presentaron además las consecuencias que traen la falta de seguridad y algunas medidas de prevención para mitigar las vulnerabilidades.

En el primer capítulo se describe con más detalle la situación de seguridad en que se encuentra la red inalámbrica ESPOL, el problema identificado, motivos para la realización de este proyecto, objetivos del mismo y restricciones para el desarrollo de la metodología.

En el segundo capítulo se presentan conceptos generales sobre el estándar IEEE 802.11 tales como características de sus revisiones, interferencias que sufren, tipos de seguridad disponibles, posibles formas de ataque, entre otras.

En el tercer capítulo se procedió con la primera parte de la metodología de ataque que consistió en lograr acceder a la red interna de la ESPOL por medio de los puntos de acceso inalámbrico. Para esto se siguieron pasos ordenados que nos llevaron hacia ese objetivo mediante recopilación de

información, identificación de puntos de acceso y el uso de herramientas y técnicas para obtener acceso no autorizado.

El cuarto capítulo detalló la segunda parte de la metodología y consistió en que una vez dentro la red interna se identificó los dispositivos de administración con herramientas de mapeo.

El quinto capítulo fue una etapa de análisis de los ataques realizados presentados en la metodología que describe las vulnerabilidades encontradas. Aquí se detallaron los motivos por los que los ataques de cada etapa tuvieron éxito.

El sexto capítulo fue concerniente a un análisis de las consecuencias de los ataques exitosos. Se concientiza sobre los daños que pudieron haber causado las intrusiones, y la exposición de información confidencial. Además se presentaron medidas de control y seguridad que buscan contrarrestar los ataques descritos.

Finalmente el capítulo 7 muestra políticas de seguridad recomendadas y su importancia en una implementación de red en general. Se presentan también herramientas de auditoría que son utilizadas tanto por hackers y profesionales en cuanto a seguridad inalámbrica.

ÍNDICE GENERAL

Pág.

RESUMEN VII

ÍNDICE GENERAL IX

ÍNDICE DE FIGURAS XIII

ÍNDICE DE TABLAS XV

ABREVIATURAS XVI

INTRODUCCIÓN XXII

1. PLANTEAMIENTO DEL PROYECTO 1
    1.1. Situación actual de niveles de seguridad inalámbrica 2
    1.2. Problemas y oportunidades 2
    1.3. Alcance y restricciones 3
    1.4. Objetivos 3
        1.4.1. Objetivo general 3
        1.4.2. Objetivo especifico 4
    1.5. Justificación 4
2. REDES INALÁMBRICAS, ESTANDAR IEEE 802.11 7
    2.1. Conceptos y generalidades 8
    2.2. Arquitectura básica 10
    2.3. Topología de red 11
    2.4. Interferencia y atenuación 17
    2.5. Ventajas y desventajas 19
    2.6. Seguridad inalámbrica 19
        2.6.1. Redes abiertas 20
        2.6.2. Cifrado WEP 20
        2.6.3. Cifrado WPA, WPA2 21
        2.6.4. Seguridad WPS 23
        2.6.5. Simbología y búsqueda de redes 24

2.7. Tecnologías actuales 25
2.8. Tipos de ataque 26
2.9. Consecuencias de un bajo nivel de seguridad 26
3. METODOLOGÍA DE ATAQUE INALÁMBRICO 28
3.1. Recopilación de información 29
3.1.1. Ingeniería social 29
3.1.2. Ubicación geográfica de la red inalámbrica 32
3.1.3. Red a la que pertenece 33
3.1.4. Administradores de estas redes 34
3.2. Escaneo de puntos de acceso 35
3.2.1. Identificación de puntos de acceso inalámbrico 35
3.2.2. Puntos de acceso ocultos 39
3.2.3. Tipo de seguridad presente 39
3.2.4. Clientes conectados 40
3.3. Penetración por la red inalámbrica 41
3.3.1. Red no protegida 41
3.3.2. Red protegida 41
4. METODOLOGÍA DE ATAQUE DENTRO DE LA RED 48
4.1. Escaneo de la red interna 48
4.1.1. Hosts activos 50
4.1.2. Puertos y servicios 51
4.1.3. Identificación del sistema operativo de los hosts 52
4.1.4. Identificación del dispositivo inalámbrico 53
4.1.5. Diagrama de la red 53
4.1.6. Escaneo de vulnerabilidades 54
4.2. Ataque al dispositivo inalámbrico 59
4.2.1. Ruptura de contraseñas de administración 59
4.2.2. Explotación de vulnerabilidades 60
4.2.3. Ataques del tipo hombre en el medio 60
4.3. Ataque a otros servidores 60

5. ANÁLISIS EXPERIMENTAL DE VULNERABILIDADES 65
5.1. Información obtenida por Ingeniería Social 66
5.2. Redes inalámbricas sin protección de acceso administrativo 67
5.3. Seguridad WEP 67
5.4. Contraseñas WPA, WPA2 no seguras 68
5.5. Seguridad WPS 68
5.6. Suplantación de identidad 69
5.7. Firmware de dispositivos inalámbricos desactualizado 70
5.8. Contraseñas de administración no seguras 71
5.9. Ataques DoS 71
6. ANÁLISIS DE RESULTADOS Y MECANISMOS DE DEFENSA 73
6.1. Análisis de riesgos y vulnerabilidades reportados 74
6.2. Soluciones de seguridad frente a las vulnerabilidades encontradas 76
6.3. Ventajas y desventajas de las soluciones propuestas 78
7. HERRAMIENTAS DE CONTROL, AUDITORÍA Y POLÍTICAS EN REDES WAN 80
7.1. Seguridad de acceso inalámbrico a datos 81
7.2. Seguridad en la configuración de puntos de acceso 83
7.3. Seguridad en el cifrado de información 84
7.4. Herramientas para auditorias 84
7.5. Políticas de administración y operación 85
CONCLUSIONES 88
RECOMENDACIONES 90
ANEXO B1. UBICACIÓN DE PUNTOS DE ACCESO EN ESPOL 93
ANEXO B2. UBICACIÓN DE PUNTOS DE ACCESO EN ESPOL 94
ANEXO C1. RESULTADO DE WARDRIVING ESPOL (1) 95
ANEXO C2. RESULTADO DE WARDRIVING ESPOL (2) 96
ANEXO D. ARCHIVO */etc/dhcp3/dhcpd.conf* 97
ANEXO E. ACTIVIDAD DEL PUNTO DE ACCESO FALSO 98

ANEXO F. ACTIVIDAD DEL SERVICIO DHCP 99

ANEXO G. CREDENCIALES CAPTURADAS POR SET 100

ANEXO H1. ESCANEO DE LA RED 200.126.24.0 (1) 101

ANEXO H2. ESCANEO DE LA RED 200.126.24.0 (2) 102

ANEXO I. ESCANEO DE LA RED 200.126.24.0 (3) 103

ANEXO J1. Escaneo del WLC (1) 104

ANEXO J2. ESCANEO DEL WLC (2) 105

ANEXO K. DIRECCIÓN IP DEL SERVIDOR DHCP 106

ANEXO L. DIRECCIONES IP Y NOMBRES DE DOMINIO 107

BIBLIOGRAFIA 108

ÍNDICE DE FIGURAS

Figura 2.1. Redes Independientes. [4] 12

Figura 2.2. Figura Redes de Infraestructura. [4] 13

Figura 2.3. Conectando con otras redes 802 LAN [8] 14

Figura 2.4. Canales sin solapamiento [11] 18

Figura 2.5 Simbología utilizada en Warchalking [39] 25

Figura 3.1 Creación de interfaz en modo monitor 36

Figura 3.2 Interfaz mon0 creada a partir de wlan0 37

Figura 3.3 Puntos de acceso disponibles en el medio 38

Figura 3.4 Interfaz para clonar páginas web. SET 45

Figura 3.5 Interfaz web de autenticación clonada 46

Figura 3.6 Captura de credenciales 47

Figura 4.1. Host Activos Zenmap 51

Figura 4.2. Puertos y servicios, Nmap 52

Figura 4.3. Detección de Sistema operativo, Zenmap 52

Figura 4.4. Diagrama de la red inalámbrica 54

Figura 4.5. Reporte de vulnerabilidad del enrutador 55

Figura 4.6. Reporte de vulnerabilidad del WLC..... 56

Figura 4.7. Reporte de vulnerabilidad del servidor DHCP 56

Figura 4.8. Reporte de vulnerabilidad de servidores DNS..... 57

Figura 4.9. Reporte de vulnerabilidad de CTI..... 58

Figura 4.10. Reporte de vulnerabilidad de CTI..... 58

Figura 4.11. Ataque DoS al CTI 62

Figura 4.12. Ataque DoS al SIDWeb..... 63

Figura 4.13. Sitio web cti.espol.edu.ec inaccesible 63

Figura 4.14. Sitio web cti.espol.edu.ec inaccesible 64

Figura 5.1. Análisis WPS con Wireshark [42]..... 69

Figura 6.1. Página de ingreso a Intermático..... 77

ÍNDICE DE TABLAS

Tabla I. Cuadro comparativo de estándares 802.11. [1], [2], [3], [36] 10

Tabla II. Canales de frecuencia DSSS PHY [8]..... 18

Tabla III Diferentes modos de WPA y WPA2 [17] 22

ABREVIATURAS

AP	“Access Point” (Punto de Acceso)
BSS	“Basic Service Set” (Conjunto Básico de Servicio)
CEH	“Certified Ethical Hacker” (Hacker Ético Certificado)
CES	Consejo de Educación Superior
CSI	Centro de Servicios Informáticos
CSMA/CA	“Carrier Sense, Multiple Access, Collision Avoidance” (Acceso Múltiple por Detección de Portadora con Evasión de Colisiones)
CTI	Centro de Tecnologías de Información
CSI	Centro de Servicio de Información
DFS	“Dynamic Frequency Selection” (Selección Dinámica de Frecuencia)
DHCP	“Dynamic Host Configuration Protocol” (Protocolo de Configuración Dinámica de Host)
DNS	“Domain Name Server” (Servidor de Nombre de Dominio)
DoS	“Denial of Service” (Denegación de Servicio)
DSE	“Dynamic Station Enablement” (Habilitación de

	Estación Dinámica)
DSS	“Distribution System Service” (Servicio del Sistema de Distribución)
DSSS	“Direct-Sequence Spread Spectrum” (Espectro Ensanchado de Secuencia Directa)
EAP	“Extensible Authentication Protocol” (Protocolo de Autenticación Extensible)
EAP-GTC	“Extensible Authentication Protocol – Generic Token Card” (Protocolo de Autenticación Extensible - Tarjeta de Testigo Genérico)
EAP-LEAP	“Lightweight Extensible Authentication Protocol – Protocolo de Autenticación Extensible Ligero”
EAP-SIM	“Extensible Authentication Protocol – Suscriber Identity Module” (Protocolo de Autenticación Extensible – Módulo de Identidad de Suscriptor)
ENC	“Encryption” (Cifrado)
ESS	“Extended Service Set” (Conjunto Extendido de Servicio)
ESSID	“Extended Service Set Identifier” (Identificador de Conjunto Extendido de Servicio)
ETSI	“European Telecommunications Standards Institute” (Instituto Europeo de Normas de Telecomunicaciones)
FHSS	“Frequency Hopping Spread Spectrum” (Espectro Ensanchado de Salto de Frecuencia)

GHz	Gigahercios
HTTP	“Hypertext Transfer Protoco” (Protocolo de Transferencia de Hipertexto)
HTTPS	“Hypertext Transfer Protocol Secure” (Protocolo de Transferencia de Hipertexto Seguro)
IAEN	Instituto de Altos Estudios Nacionales
IBSS	“Independent Basic Service Set” (Conjunto Básico de Servicio Independiente)
ICMP	“Internet Control Message Protocol” (Protocolo de Mensajes de Control de Internet)
IEEE	“Institute of Electrical and Electronics Engineers” (Instituto de Ingenieros Eléctricos y Electrónicos)
IP	“Internet Protocol” (Protocolo de Internet)
IR	“Infrared” (Infrarrojo)
ISM	“Industrial, Scientific and Medical” (Industrial, Científica y Médica)
L2TP	“Layer 2 Tunneling Protocol” (Protocolo de Encapsulamiento de Capa 2)
LAN	“Local Area Network” (Red de Área Local)
MAC	“Media Access Control” (Control de Acceso al Medio)
MSCHAP	“Microsoft Challenge Handshake Authentication Protocol” (Protocolo de Autenticación por Desafío

	Mutuo de Microsoft)
MSDU	“MAC Service Data Unit” (Unidad de Datos del Servicio MAC)
NAT	“Network Address Translation” (Traducción de Dirección de Red)
OFDM	“Orthogonal Frequency-Division Multiplexing” (Multiplexación por División de Frecuencias Ortogonales)
OPN	“Open” (Abierto)
OSI	“Open Systems Interconnection” (Interconexión de Sistemas Abiertos)
PC	“Personal Computer” (Computador Personal)
PEAP	“Protected Extensible Authentication Protocol” (Protocolo de Autenticación Extensible Protegido)
PSK	“Pre-shared Key” (Clave Pre compartida)
QoS	“Quality of Service” (Calidad de Servicio)
RADIUS	“Remote Authentication Dial-In User Server” (Servidor de Autenticación Remota Telefónica de Usuario)
RC4	Rivest Cipher 4
RFC	“Request for Comments” (Petición de Comentarios)
SET	“Social Engineer Toolkit” (Kit de Herramientas de

	Ingeniería Social)
SS	“Spread Spectrum” (Espectro Ensanchado)
STA	“Estación de trabajo”
SSH	“Secure Shell” (Intérprete de Órdenes Seguro)
SSID	“Service Set Identifier” (Identificador de Conjunto de Servicio)
SSL	“Secure Sockets Layer” (Capa de Conexión Segura)
TCP	“Transmission Control Protocol” (Protocolo de Control de Transmisión)
TLS	“Transport Layer Security” (Seguridad en la Capa de Transporte)
TPC	“Transmit Power Control” (Control de Potencia)
TTLS	“Tunneled Transport Layer Security” (Seguridad en la Capa de Transporte Encapsulada)
URL	“Uniform Resource Locator” (Localizador de Recursos Uniforme)
VI	Vector de Inicialización
WEP	“Wired Equivalent Privacy” (Privacidad Equivalente a Cableado)
WLAN	“Wireless Local Area Network” (Red de Área Local Inalámbrica)

WLC	Wireless LAN Controller (Controlador de Redes Inalámbricas)
WPA	“Wi-Fi Protected Access” (Acceso Wi-Fi Protegido)
WPS	“Wi-Fi Protected Setup” (Configuración Wi-Fi Protegida)

INTRODUCCIÓN

La Escuela Superior Politécnica del Litoral (ESPOL) en su Campus Prosperina cuenta con 47 puntos de acceso inalámbrico distribuidos en sus diferentes edificios, que tienen como finalidad proveer servicio de Internet a toda la comunidad politécnica. Este acceso a Internet se encuentra disponible solamente para usuarios que poseen una cuenta de la ESPOL, que además puede ser utilizada para acceder a otros servicios en línea que la universidad ofrece.

Si bien es una excelente solución que beneficia más que todo a los estudiantes, aun no se ha realizado un estudio formal sobre la seguridad que presenta este sistema. Como se mencionó anteriormente las credenciales utilizadas para la verificación del usuario en la red inalámbrica son las mismas que las utilizadas por algunos servicios informáticos que provee la ESPOL, de manera que este sistema debe estar protegido contra el robo de identidad ya que si esto llega a suceder puede desencadenar ataques informáticos y robo de información dentro de la red de ESPOL.

En este proyecto se realizó un estudio de las falencias de seguridad y vulnerabilidades que existen a nivel de acceso y a nivel administrativo en la

red inalámbrica ESPOL ,mediante ataques informáticos controlados sin perjuicios a la institución, simulando procedimientos reales de un hacker con fines maliciosos pudiera realizar. Luego de obtener los resultados de estas pruebas se presentó un reporte detallando cada una de las falencias encontradas en cuanto a seguridad, junto con técnicas de mitigación.

CAPÍTULO 1

1. PLANTEAMIENTO DEL PROYECTO

En este capítulo se da a conocer detalles generales previos al desarrollo de este proyecto, así como los motivos del surgimiento del mismo, la justificación de su estudio y objetivos que se buscan satisfacer como su desarrollo.

1.1. Situación actual de niveles de seguridad inalámbrica

El campus Gustavo Galindo de la ESPOL cuenta con una red inalámbrica disponible para todos sus estudiantes y docentes. Los puntos de acceso a esta red están distribuidos en diferentes lugares del campus, proporcionando así cobertura a la mayor parte de su extensión. Esta red es administrada por el Centro de Tecnologías de Información (CTI) y se la encuentra con el nombre de “ESPOL”.

En la red ESPOL para hacer uso de Internet el usuario debe autenticarse a través de un servidor mediante un nombre de usuario y contraseña (credenciales) que son los mismos que pertenecen a las cuentas de correo electrónico @espol.edu.ec otorgadas a los estudiantes al ingresar a la universidad. La credencial es verificada por un servidor de autenticación RADIUS que se encuentra en el Centro de Servicios Informáticos (CSI). Luego de verificada, el usuario está autorizado a utilizar los servicios de red de la ESPOL.

1.2. Problemas y oportunidades

La autenticación por medio de servidores dedicados (RADIUS) impide el acceso a usuarios que no cuenten con credenciales para acceder a la red. Sin embargo, la persona que ingresa las

credenciales no es necesariamente la propietaria de las mismas. Esto conlleva a que un usuario malicioso pueda utilizar una cuenta ajena con fines no éticos.

1.3. Alcance y restricciones

El análisis de esta red abarca toda su seguridad desde el momento de ingreso por el punto de acceso hasta el control de los dispositivos de administración de la misma mediante pruebas de seguridad. Es claro que para llevar a cabo estas pruebas sobre la red en cuestión se nos ha otorgado el debido permiso por parte del administrador de red.

1.4. Objetivos

1.4.1. Objetivo general

Realizar un análisis por medio de ataques controlados que permita determinar el nivel de seguridad actual de la red inalámbrica que tiene la ESPOL, detallando vulnerabilidades y posibles soluciones inherentes al medio.

1.4.2. Objetivo especifico

- Realizar un Diagrama Lógico de la red ESPOL.
- Realizar análisis de vulnerabilidades a elementos de red para conocer las amenazas potenciales.
- Probar y demostrar vulnerabilidades encontradas.
- Detallar soluciones a los problemas encontrados en los distintos ataques.
- Proporcionar una documentación del proyecto, proponiendo soluciones a vulnerabilidades encontradas en la red inalámbrica de la ESPOL.

1.5. Justificación

Las redes inalámbricas implementadas en la ESPOL, hasta el momento, no han sido sujetas a un estudio y análisis formal de riesgos y vulnerabilidades con sus respectivas medidas de seguridad implementadas, que permita garantizar un buen nivel de seguridad. Esto se debe a que en ocasiones los administradores descuidan esta parte de la red por facilidad o simplemente lo dejan en un segundo plano ya que no ven la importancia de tener un acceso inalámbrico seguro.

Por tal motivo, es probable que la información presente en estas redes inalámbricas no se encuentre debidamente protegida. De igual manera puede existir el acceso no autorizado de personas maliciosas poniendo en riesgo las contraseñas no cifradas, los documentos, credenciales de usuarios administrativos con su posterior escalamiento de privilegios, las calificaciones, los correos electrónicos, los roles de pago, o los documentos de bancos, entre otros. Toda esta información es altamente sensible y puede ser usada para fines no éticos trayendo consigo malas consecuencias en la Universidad. Lo que se busca es evitar el acceso no autorizado a la red y proteger su integridad, para brindar confiabilidad en las comunicaciones o en su defecto si actualmente está sucediendo frenar este acto peligroso y no ético.

Este análisis de seguridad estará basado en el funcionamiento del estándar IEEE 802.11, las tecnologías actuales, los tipos de seguridad disponibles, el protocolo de transporte TCP, los documentos RFC, las metodologías del Hacking ético en auditorias de seguridad como las presentadas por la certificación CEH, así como herramientas utilizadas por hackers reales como Foca, Ettercap, Wireshark, Nmap, AngryIP, Lanmap, Netstumbler, Aircrack Suite, Kismet, Jhon the Ripper, Nessus, entre otras. Todos estos

elementos nos ayudarán para este cometido, sin olvidar también contenido publicado en la Web como reportes y códigos para explotación de vulnerabilidades encontradas en dispositivos de red que pueden ser aprovechadas si estos no están actualizados debidamente.

Este proyecto busca analizar y dar soluciones al tema de seguridad inalámbrica en las redes de la ESPOL, detallar sus debilidades mediante ataques controlados y autorizados para las respectivas prácticas. De esta manera se puede tener una documentación de las falencias a nivel de seguridad y proponer soluciones para que estas sean atendidas.

CAPÍTULO 2

2. REDES INALÁMBRICAS, ESTANDAR IEEE 802.11

Las comunicaciones inalámbricas cuentan con varias implementaciones definidas a través del tiempo y estas son utilizadas de acuerdo a las necesidades del medio en que operan. También definen una estructura universal que debe ser adoptada por fabricantes de elementos de red para que sus productos sean interoperables con todos los que utilizan el estándar. En este capítulo se presentara la operación básica de una red inalámbrica con el estándar IEEE 802.11.

2.1. Conceptos y generalidades

El Estándar IEEE 802.11 se refiere a un conjunto de normas y protocolos destinados a proveer una conexión inalámbrica como alternativa a la red cableada proporcionando flexibilidad en el acceso. Creado por el IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) y el ETSI (Instituto Europeo de estándares de Telecomunicaciones), este estándar cuenta con varias versiones desde que fue aceptado y publicado en el año de 1997. Cada versión ha ido mejorando sus normas significativamente para alcanzar velocidades de transmisión más altas en función de las exigencias del medio actual. [1]

La publicación original, 802.11 Legacy, alcanza velocidades de 1 a 2 Mbps, con un protocolo de prevención de colisiones CSMA/CA; opera en la banda ISM de 2.4 GHz y especifica el uso de infrarrojo en capa física. Actualmente no hay implementaciones con este estándar. [2]

Luego apareció el estándar 802.11a, que opera en la banda de 5Ghz, poco usada en el medio. Alcanza una velocidad de transmisión de 54Mbps, pero necesita línea de vista puesto que su señal se atenúa

fácilmente y no es compatible con los estándares 802.11b y 802.11g. [1], [3]

El estándar 802.11b es la siguiente publicación; utiliza la banda de 2.4 a 2.5 GHz permitiendo que la señal no se degrade significativamente con la presencia de obstáculos pero sea susceptible a las interferencias. Su velocidad de transmisión máxima es de 11Mbps y utiliza el protocolo de prevención de colisiones CSMA/CA. [1], [3]

La posterior publicación, 802.11g, es compatible con el 802.11b; operan en la misma banda de frecuencia de 2.4 a 2.5 GHz y los mismos canales y son susceptibles a interferencias; mejora la velocidad de transferencia a 54 Mbps. Los equipos que operaban con el estándar 802.11b se adaptaron a 802.11g. [1], [3]

Finalmente, 802.11n permite duplicar las velocidades de transferencia del 802.11g, pueden utilizar las bandas de frecuencia 2.4 GHz y 5 GHz. [2], [3], [36]. En la tabla I se muestra un resumen de los estándares citados anteriormente.

Tabla I. Cuadro comparativo de estándares 802.11. [1], [2], [3], [36]

Estándar	Banda ISM	Velocidad (Mbps)	Capa Física	Año
802.11Legacy	2.4 GHz	1 – 2	IR	1997
802.11a	5 GHz	54	OFDM	1999
802.11b	2.4 GHz	11	DSSS	1999
802.11g	2.4 GHz	25–54	DSSS/OFDM	2003
802.11n	2.4/5 GHz	72 - 600	OFDM	2009

Según el Wiki de la Universidad Técnica Federico Santa María en su artículo *Estado del Arte 802.11*, el estándar más utilizado en el medio es 802.11b, debido a su máxima disponibilidad, seguido del 802.11g [38]. La red inalámbrica ESPOL cuenta con puntos de acceso operando en el estándar 802.11g, otorgando amplia compatibilidad con la mayoría de las tarjetas de red de computadoras personales y portátiles.

2.2. Arquitectura básica

Las especificaciones del estándar 802.11 comprenden reglas para la capa física y la capa de enlace de datos del modelo de referencia (OSI). La capa física se encarga de la transmisión y recepción de los datos a través de cuatro (4) tipos de modulación: FHSS (Salto de Frecuencia de Espectro Ensanchado), DSSS (Secuencia Directa de

Espectro Ensanchado), IR (Infrarrojos) y OFDM (Multiplexación por División de Frecuencias Ortogonales). [4]

La modulación FHSS permite 75 subcanales de 1 MHz cada uno, que permiten definir secuencias de saltos que no se superponen entre sí. Por otro lado la modulación DSSS permite un máximo de 3 canales de 20Mhz cada uno y genera la menor probabilidad de interferencias. La modulación OFDM consiste en la división de una portadora de datos de alta velocidad (20 MHz) en varias subportadoras de baja velocidad (300MHz) [4], [5].

2.3. Topología de red

Se puede definir dos (2) topologías de red en el estándar 802.11 que son *Conjunto Básico de Servicio (BSS)* y *Conjunto Extendido de Servicio (ESS).* [4].

2.3.1 Conjunto Básico de Servicio (BSS)

El Conjunto Básico de Servicio cuenta con dos modos de operación que son Conjunto Básico de Servicio Independiente

(IBSS) también llamado Ad-hoc e Infraestructura de Conjunto Básico de Servicios. [4]

Conjunto Básico de Servicios Independiente (IBSS) es el modo de operación Ad-hoc, consiste en la comunicación de dos o más estaciones entre sí *(Ver Figura 2.1)*, sin existir coordinación entre ellas. Cualquier estación que se encuentre dentro del área básica de servicio puede comunicarse con las demás de manera directa. Ese tipo de topología no es escalable y es utilizada para operaciones sencillas. [4], [7]

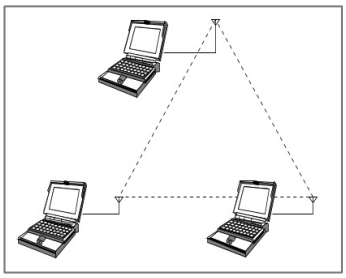


Figura 2.1. Redes Independientes. [4]

La Infraestructura de Conjunto Básico de Servicios cuenta con una entidad llamada Punto de Acceso el cual administra y coordina la comunicación entre las estaciones de trabajo *(Ver Figura 2.2)*; todos los nodos deben conectarse a este elemento para intercambiar información. En nuestro estudio el

punto de acceso ESPOL es al que los terminales se conectan para obtener servicios de red. [4], [7]

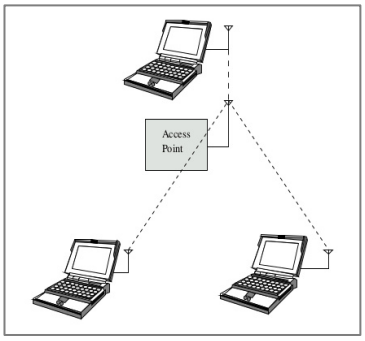


Figura 2.2. Figura Redes de Infraestructura. [4]

2.3.2 Conjunto Extendido de Servicios (ESS)

Esa estructura es un Sistema Distribuido escalable; permite enlazar varios BSS y proporciona conexión por celdas, es decir, la estación de trabajo puede movilizarse hacia otra área de cobertura con el mismo nombre sin perder conexión a la red. [4], [7]. La Figura 2.3 muestra una red formada por dos BSS, el Sistema de Distribución y la integración con la red cableada.

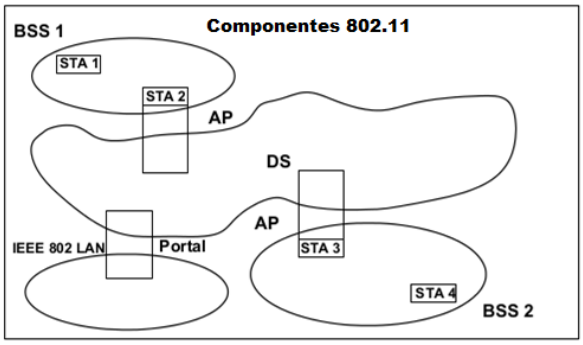


Figura 2.3. Conectando con otras redes 802 LAN [8]

La red inalámbrica ESPOL tiene varios puntos de acceso con el mismo ESSID distribuidos en diferentes lugares del campus. De esta manera los usuarios pueden moverse a través del campus sin perder la conexión a la red. El Sistema de Distribución conecta a los puntos de acceso ESPOL entre si y provee comunicación hacia la red cableada en donde se origina la conexión a Internet.

El estándar 802.11 especifica los servicios que el Sistema Distribuido debe brindar. Hay dos categorías de servicios: *Servicios de Estación (SS)* que son parte de la estación de trabajo y *Servicios del Sistema de Distribución (DSS)* que los provee el mismo Sistema de Distribución. Estos servicios son manejados por la subcapa de control de acceso al medio (MAC). [8]

Entre los Servicios de Estación tenemos Autenticación, Terminación o finalización de la autentificación, Confidencialidad de Datos, Entrega de MSDU, DFS, TPC, Sincronización de Temporizador de Capa Superior para Calidad de Servicio, Programación de Tráfico para Calidad de Servicio, Medición de Radio y DSE.[8] Entre los servicios del Sistema de Distribución tenemos el de Asociación, Desasociación, Reasociación, Distribución, Integración, Programación de Tráfico para Calidad de Servicio, DSE e Interfuncionamiento con el Sistema de Distribución. [8] Para este proyecto nos interesan los servicios de Autenticación, Terminación o finalización de la autentificación, Asociación, Desasociación y Reasociación.

La Autenticación es un servicio de estación que controla el acceso a la red, y autoriza el envío y recepción de trama. Sin esta autorización el terminal no puede asociarse al Punto de Acceso. Como métodos de autenticación tenemos el de *Sistema Abierto* en la cual el usuario tiene acceso libremente, la *Autenticación de Clave Compartida*, (FS) y Autenticación Simultanea de Iguales (SAE). Generalmente los más utilizados

son el de Sistema Abierto y el de Clave Compartida (WEP). [8], [9].

La asociación permite que el terminal se registre con el Punto de Acceso para que cuente con los recursos de red. Según José Roberto Vignoni en su publicación Redes Inalámbricas, “el sistema de distribución puede utilizar la información de estos registros para determinar que AP utilizar para alcanzar una dada estación móvil” [9].

La desasociación es una notificación por parte del Sistema de Distribución. Para terminar la asociación existente; la estación queda desvinculada de la red perdiendo todos los registros de movilidad en cada AP. [9]

La reasociación se da cuando es necesario cambiar de punto de acceso debido a las condiciones en la señal. Este servicio es invocado por parte de la estación. Según el documento del Estándar 802.11-2012 de la IEEE este proceso “mantiene al Sistema de Distribución informado del mapeo actual entre Punto de Acceso y estación a medida que la estación se mueve de un BSS a otro dentro de un ESS”. [8], [9]

2.4. Interferencia y atenuación

La señal proveniente de los puntos de acceso se ve perjudicada cuando se encuentra con ondas electromagnéticas de otras tecnologías operando en el mismo espectro de frecuencia como Bluetooth, teléfonos inalámbricos, hornos microondas. Ese factor externo es conocido como interferencia e influye negativamente al rendimiento. [10]

La modulación DSSS, cuenta con 14 canales de 22 MHz disponible, de los cuales solo 3 canales no se solapan entre sí. La tabla II muestra los canales disponibles con su respectiva frecuencia asociada. Los canales que no se superponen son el 1, 6 y 11 *(Ver Figura 2.4)*, es decir, tres redes pueden operar en estos canales sin interferir entre ellas. [11]

Tabla II. Canales de frecuencia DSSS PHY [8]

ID Canal	Frecuencia (MHz)
1	**2412**
2	2417
3	2422
4	2427
5	2432
6	**2437**
7	2442
8	2447
9	2452
10	2457
11	**2462**
12	2467
13	2472
14	2484

A medida que la señal de radio viaja por el ambiente esta va perdiendo su potencia debido a factores ambientales y obstáculos que atenúan la señal. [12]

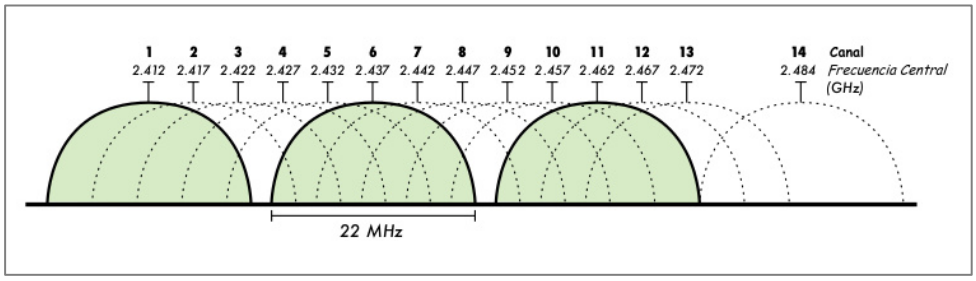


Figura 2.4. Canales sin solapamiento [11]

Existen varias implementaciones de puntos de acceso en los alrededores de la ESPOL, algunos formales y otros creados por usuarios sin ningún tipo de control por parte de administradores de red. Estas señales no autorizadas interfieren con la señal de la red ESPOL y entorpecen la conexión de usuarios.

2.5. Ventajas y desventajas

La mayor ventaja que tiene la implementación de una red inalámbrica en el caso de ESPOL, es que los estudiantes y docentes pueden tener acceso a Internet desde cualquier parte del campus sin necesidad de acudir a los laboratorios de computación, cuyos horarios pueden no ajustarse a los requerimientos de los usuarios.

Los usuarios deben escribir su nombre de usuario de correo electrónico y su contraseña como método de autenticación para contar con el servicio de Internet. Estas credenciales viajan por un medio inalámbrico siendo susceptibles a intercepciones.

2.6. Seguridad inalámbrica

Con el fin de proteger la información que viaja a través de ondas electromagnéticas se han adoptado varios métodos de seguridad

2.6.1. Redes abiertas

Una red abierta es el tipo de red más inseguro; la red está al alcance de cualquier usuario ya que al conectarse al punto de acceso no pasa por el proceso de autenticación y automáticamente cuenta con todos los servicios de red y por otro lado, los usuarios que se conectan a redes abiertas podrían ser víctimas de una red falsa creada maliciosamente para así captar contraseñas y cometer fraudes informáticos. Las redes abiertas cuentan con Filtrado de direcciones MAC, filtrado de direcciones IP y Ocultación del ESSID de la Red, por este tipo de seguridad se pueden romper fácilmente con programas espías. [13]

2.6.2. Cifrado WEP

La seguridad WEP (Privacidad Equivalente a la Cableada) fue el primer método de cifrado para el estándar IEEE 802.11. Panda Software S.L. en su artículo “Seguridad en redes Inalámbricas” asegura que “la seguridad ofrecida por WEP tiene como pilar central una clave secreta compartida por todos los comunicadores y que se emplea para cifrar los datos

enviados". Esta clave estática puede ser de 40 o 104 bits que se combinan con un Vector de inicialización (VI) de 24 bits, por lo que la clave WEP es de 64 o 128 bits. [13], [14]

No es un protocolo seguro ya que se basa en el algoritmo de cifrado RC4 que presenta vulnerabilidades en su implementación y la clave compartida se puede averiguar analizando una cantidad suficiente de paquetes capturados que contengan el mismo VI. [13], [14]

2.6.3. Cifrado WPA, WPA2

WPA (Acceso Protegido para Wi-Fi) fue creado para corregir las deficiencias del cifrado WEP. De acuerdo a Jhonatan Revelo y Edison Pazmiño en su Análisis de WPA/WPA2 Vs WEP, "en 2003 se propone el WPA y luego queda certificado como parte del estándar IEEE 802.11i con el nombre de WPA2 (en 2004)" [17]. La principal diferencia entre WPA y WPA2 es el método de cifrado que estas utilizan. [16], [19]

En WPA hay dos formas de asegurar la autenticación al acceso a la red inalámbrica: Una es por clave compartida

dinámica (WPA-PSK o WPA2-Personal) que puede utilizar una codificación TKIP/MIC para WPA o AES para WPA2 y otra por medio de un servidor de distribución de claves IEEE 802.1X (WPA2-Corporativo). [17]. En comparación con WEP, Joel Barrios Dueñas en su artículo *¿Que es WPA? ¿Por qué debería usarlo en lugar de WEP?,* indica que "WPA hace más difícil vulnerar las redes inalámbricas al incrementar los tamaños de las claves y Vectores de Inicialización" [18]. Actualmente algunos Puntos de Acceso soportan AES como método de cifrado para WPA, y TKIP para WPA2. [21]. En la tabla III se muestra en resumen el tipo de autenticación y cifrado que utiliza WPA.

Tabla III Diferentes modos de WPA y WPA2 [17]

Modo	WPA	WPA2
Corporativo	Autentificación: 802.1x/EAP	Autentificación: 802.1x/EAP
	Cifrado: TKIP / MIC	Cifrado: AES -CCMP
Personal	Autentificación: PSK	Autentificación: PSK
	Cifrado: TKIP / MIC	Cifrado: AES -CCMP

Cuando usamos un servidor de distribución de claves para el modo Corporativo, WPA puede usar Protocolos Extensibles de Autenticación (EAP). Entre ellos tenemos EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-LEAP. Este servidor de autenticación del

modo Corporativo utiliza RADIUS (Servidor de Autenticación Remota Telefónica de Usuario). Cuando se invoca al servidor RADIUS al momento de la autenticación, éste “comprueba la información utilizando esquemas de autenticación como PAP, CHAP o EAP”; si la autenticación es correcta el servidor asignará recursos de red como dirección IP, L2TP, entre otros. [18], [20]

Según el Centro de Tecnologías de la Información, la red ESPOL cuenta con un sistema de autenticación WPA que usa un servidor RADIUS para autenticar a sus usuarios y enlazarlos en la red.

2.6.4. Seguridad WPS

La Configuración Wi-Fi Protegida es un estándar promovido por Wi-Fi Alliance (http://www.wi-fi.org) para facilitar los mecanismos de configuración de una red. Este estándar provee un mecanismo rápido y fácil de registro del cliente con el Punto de Acceso. [23]

Existen dos métodos para utilizar WPS. El primero por medio del número de PIN del punto de acceso ubicado en su etiqueta, y el segundo mediante un botón que debe ser presionado tanto en el dispositivo del usuario como en el punto de acceso para lograr la conexión (conocido como el método PBC). Luego de la conexión inicial el dispositivo se conectará automáticamente. [22]

2.6.5. Simbología y búsqueda de redes

Es posible identificar los Puntos de Acceso y colocarlos en un mapa para el uso de otras personas; esta detección de redes en un lugar geográfico se lo conoce como *Wardriving (Vea un ejemplo de Wardriving en Anexo A)* [24], [25]

Una práctica similar es el *Warchalking* que tiene como finalidad encontrar puntos de acceso y luego mostrar una serie de símbolos que indican la presencia de esos puntos de acceso, el tipo de seguridad que tiene y el nombre del ESSID, de manera visible para las personas como se muestra en la figura 2.5. [24], [25]

Figura 2.5 Simbología utilizada en Warchalking [39]

2.7. Tecnologías actuales

La red inalámbrica de ESPOL está basada en la topología Conjunto Extendido de Servicio (ESS), que consiste en varios puntos de acceso ubicados en diferentes lugares geográficos enlazados entre sí por medio del Sistema de Distribución que en este caso es la red cableada. De esta manera los usuarios que se conectan pueden pasar de un área cubierta por un punto de acceso a otra área de otro punto de acceso sin perder la conectividad.

El tipo de seguridad que implementa es WPA con el protocolo EAP que permite manejar la autenticación por medio de un servidor RADIUS. Este tipo de autenticación tiene un alto nivel de seguridad ya que proviene de mecanismos de autenticación como si fuera una red cableada.

2.8. Tipos de ataque

Existen varios tipos de ataques que se pueden suscitar a una red inalámbrica. Los ataques activos llegan a producir cambios de la información y de situación de los recursos del sistema. Cuando una entidad pretende ser percibida como otra se conoce como enmascaramiento.

En algunos de los casos se produce la captura pasiva de datos y su retransmisión [31]. La modificación de mensajes podemos encontrarlo cuando una parte del mensaje se modifica a la espera de un resultado netamente diferente. Los ataques pasivos tienen un uso limitado de recursos que nos permitan acceder a la información almacenada o procesada en ese momento por el sistema.

La denegación de servicios tiene como fin impedir que el servicio siga ejecutando o a su vez este no tenga actividad.

2.9. Consecuencias de un bajo nivel de seguridad

La mala implementación de seguridad produce un impacto que puede ser leve o grave. Es necesario contar con un nivel de

seguridad que se ajuste a las necesidades de la organización sin dejar brechas que puedan ser aprovechadas por intrusos. Una red no asegurada debidamente es propensa al robo de información privada de los usuarios, robo de información propia de una organización, indisponibilidad del servicio informático, violación de la integridad de los equipos dentro de la red, entre otros. [35]

CAPÍTULO 3

3. METODOLOGÍA DE ATAQUE INALÁMBRICO

Como primer paso para intentar obtener un control total de la red inalámbrica se tuvo acceso a la red ESPOL como un usuario legítimo para contar con los servicios que proporcionan los Puntos de Acceso. Para esto empleamos herramientas profesionales que suelen utilizar los auditores de seguridad. Esta metodología está basada en la guía de estudio para la obtención de la Certificación de Hacking Ético (CEH)

3.1. Recopilación de información

Por medio de la recopilación de información se logró obtener datos importantes como el tipo de seguridad de la red inalámbrica, los datos con que los usuarios se identifican, ubicación de dispositivos, tipo de autenticación, administradores de red, entre otras.

3.1.1. Ingeniería social

Podemos definir a ingeniería social como un conjunto de técnicas psicológicas y habilidades sociales utilizadas conscientemente y en ocasiones de manera planificada para poder captar información a través terceros o mediante amistades que no saben el objetivo final de una conversación técnica.[43]

La ingeniería social no nos limita, podemos utilizar muchas herramientas expresivas y orales para poder captar información a través de preguntas o de una conversación donde esté involucrado nuestro tema objetivo. Según Mercé Molist en el portal de hackstory.net, “puede ser ingeniería

social el obtener de un profesor las preguntas de un examen o la clave de acceso de la caja fuerte un banco.” [43]

El gran objetivo de la ingeniería social es brindarnos información de manera técnica a través de terceras personas, y es ahí donde la ingeniería social tiene su llamado, para luego dejarla a un lado y seguir con el proceso del ataque.

Uno de los ingenieros sociales más famosos de los últimos tiempos es Kevin Mitnick [28]. Según su opinión, “*la ingeniería social se basa en estos cuatro principios: (1) todos queremos ayudar, (2) el primer movimiento es siempre de confianza hacia el otro, (3) no nos gusta decir No, (4) a todos nos gusta que nos alaben.”*

Estos cuatro principios nos ayudan a ver de una manera diferente como los demás piensas y como nosotros pensamos al momento de pedir información sobre temas de interés para un ataque provocado.

Esta técnica es muy usada para diferentes ramas como la investigación, acceso a privilegios que sean de riesgos para

los administradores, o para consultar de temas importantes que no todos manejen.

A la mayoría de las personas se les hace delicado decir que no cuando se pide información ya sea para investigación o para tareas dentro del ámbito universitario, de esta manera solo con el hecho de decirles que son “para investigaciones” están dispuestos a proporcionarnos información que nos pueden dar mucha ventaja para poder realizar el objetivo que tenemos en mano. En situaciones en las que los administradores no quieren proporcionar información, se puede nombrar a un superior en el rango diciendo que venimos de parte de él, algunos no toman las necesarias averiguaciones sino que al nombrarlo comienzan a decirnos los datos que necesitamos.

Puede sonar notorio pero tener un buen don de palabra nos puede llevar muy lejos y a su vez podremos obtener muchos beneficios a pocos costos, el dar admiración al alguien por la labor que cumple o dar algún obsequio o un tipo de alago nos ayudan a que la confianza fluctúe en la conversación, la que a su vez sin saber se les está sacando información referente al

objetivo que nos planteamos al momento de comenzar la conversación.

Según la versión 6 de la guía de estudio para la obtención de la certificación CEH, existen técnicas de ingeniería social basadas en computadora tales como archivos adjuntos en correos electrónicos, sitios web falsos y ventanas emergentes. Estas técnicas se conocen como “Phishing” y tienen como fin el robo de información haciéndose pasar por una fuente confiable que solicita nombres de usuarios, contraseñas o códigos de acceso. Estas técnicas se utilizan para el robo de identidad luego de obtener credenciales legítimas [44].Según Cristian Borghello en su informe de Ingeniería Social asegura que esta “continúa siendo una de las metodologías de ataque más utilizada por creadores de malware y usuarios con fines maliciosos debido al alto nivel de eficacia logrado engañando al usuario.” [29].

3.1.2. Ubicación geográfica de la red inalámbrica

La red ESPOL cuenta con un rango de cobertura que abarca la mayor parte del campus politécnico ya que sus servicios se

prestan a toda la comunidad politécnica. Sus Puntos de Acceso se encuentran distribuidos en varios rincones formando celdas de conexión muy amplias que permiten propagar la señal por casi todos los sectores. (Ver Anexo B1 y Anexo B2)

Por medio de la técnica del Wardriving logramos identificar aquellos puntos de acceso que no tienen el nombre de ESSID ESPOL, lo que en teoría no debería suceder ya que eso afecta al rendimiento de la red inalámbrica. En el Anexo C1 y Anexo C2 se muestran en color morado los puntos de acceso ESPOL y en color amarillo otros puntos de acceso diferentes.

3.1.3. Red a la que pertenece

La subred que provee acceso a los usuarios inalámbricamente es la 200.126.24.0 con máscara de red 255.255.252.0, que a su vez son proporcionadas por los puntos de acceso. Estos puntos de acceso se encuentran administrados dentro de la subred 192.168.50.0 con máscara de red 255.255.255.0. Los usuarios que se conectan a esta red inalámbrica ESPOL tienen acceso a los servidores de producción del CTI como el

SIDWeb, CTI, CES, Senescyt, Inventio, entre otras, todas estas en la subred 200.10.150.0 con máscara de red 255.255.255.0.

Esta red pública es administrada por el CTI, por medio del WLC (Controlador de red inalámbrica), luego se autentifica por medio de un portal web almacenada en un servidor RADIUS para poder asignar recursos de red.

3.1.4. Administradores de estas redes

La red de administración inalámbrica ESPOL es administrada y monitoreada por el CTI mediante una interfaz llamada “Controlador de Redes Inalámbricas” (WLC) de Cisco, y por otro lado gestiona su red de servidores de producción citados anteriormente.

El Centro de Servicios Informáticos (CSI) por su parte se encarga de propagar la red inalámbrica hacia todo el campus y dotándolo de conectividad a Internet.

3.2. Escaneo de puntos de acceso

Existen varias herramientas para identificar ondas electromagnéticas pertenecientes a puntos de acceso que se encuentran en el medio. **Aircrack-ng** es una de ellas y permite escanear el medio en busca de puntos de acceso, inyectar tráfico a un punto de acceso, y romper contraseñas de autenticación de puntos de acceso.

En este proyecto se utilizó un Sistema Operativo Linux para hacer uso de Aircrack-ng la cual nos permitió conocer el nombre del ESSID, el canal en el que operan, la potencia de la señal, tipo de seguridad y cifrado que presenta, cantidad de datos que recibe, clientes conectados, etc. De esta manera pudimos obtener información de los puntos de acceso.

3.2.1. Identificación de puntos de acceso inalámbrico

Se procedió a captar la señal de los accesos inalámbricos que están en el medio. Para lograr esto se contó con una tarjeta de red que permite capturar todo el tráfico que pasa por ella sin necesidad de asociarse a ningún punto de acceso.

La tarjeta de red fue configurada para operar en modo *Monitor* ya que de esta forma se logra escuchar todo el tráfico que pasa por ella [41]. Con la Suite de Aircrack se pudo crear una interfaz directamente en modo monitor a partir de nuestra tarjeta inalámbrica. Esto se realizó con el comando:

airmon-ng start wlan0

Donde *wlan0* es el nombre de la interfaz de red que el sistema le había asignado a nuestra tarjeta. Esto creó una interfaz llamada mon0 (Ver Figura 3.1).

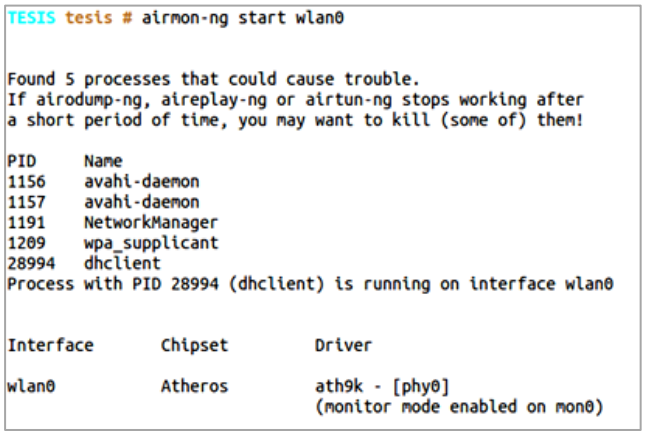


Figura 3.1 Creación de interfaz en modo monitor

Pudimos visualizar la creación de la nueva interfaz con el comando *ifconfig* que muestra información general de las interfaces de red del sistema. (*Ver Figura 3.2)*

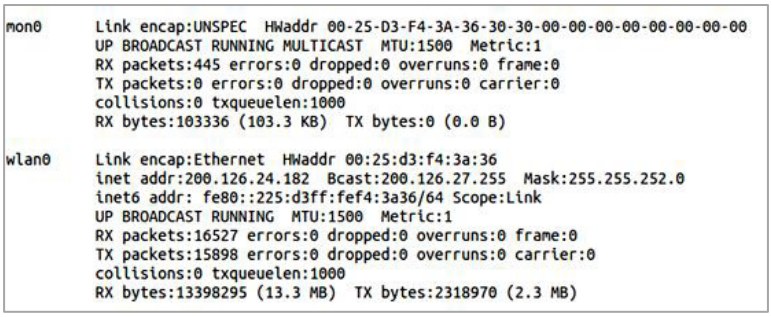
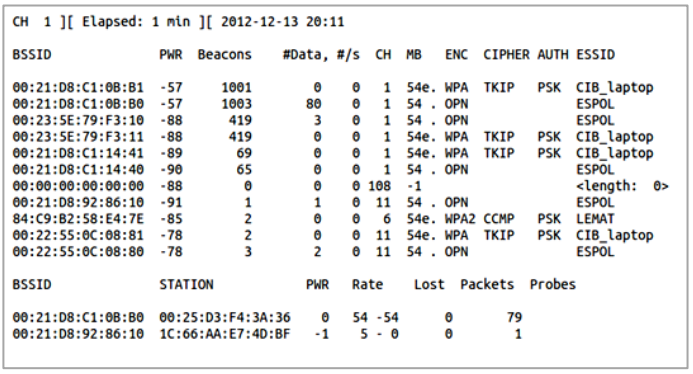


Figura 3.2 Interfaz mon0 creada a partir de wlan0

Se utilizó esta interfaz virtual para captar las ondas de los puntos de acceso a nuestro alrededor mediante el comando:

airodump-ng mon0

La tarjeta de red comenzó a escanear el ambiente en busca de señales inalámbricas dando como resultado lo que muestra la Figura 3.3.



```
CH  1 ][ Elapsed: 1 min ][ 2012-12-13 20:11

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:21:D8:C1:0B:B1  -57     1001        0    0   1  54e. WPA  TKIP   PSK  CIB_laptop
00:21:D8:C1:0B:B0  -57     1003       80    0   1  54 . OPN              ESPOL
00:23:5E:79:F3:10  -88      419        3    0   1  54 . OPN              ESPOL
00:23:5E:79:F3:11  -88      419        0    0   1  54e. WPA  TKIP   PSK  CIB_laptop
00:21:D8:C1:14:41  -89       69        0    0   1  54e. WPA  TKIP   PSK  CIB_laptop
00:21:D8:C1:14:40  -90       65        0    0   1  54 . OPN              ESPOL
00:00:00:00:00:00  -88        0        0    0 108  -1                    <length:  0>
00:21:D8:92:86:10  -91        1        1    0  11  54 . OPN              ESPOL
84:C9:B2:58:E4:7E  -85        2        0    0   6  54e. WPA2 CCMP   PSK  LEMAT
00:22:55:0C:08:81  -78        2        0    0  11  54e. WPA  TKIP   PSK  CIB_laptop
00:22:55:0C:08:80  -78        3        2    0  11  54 . OPN              ESPOL

BSSID              STATION            PWR   Rate    Lost  Packets  Probes

00:21:D8:C1:0B:B0  00:25:D3:F4:3A:36    0   54 -54      0       79
00:21:D8:92:86:10  1C:66:AA:E7:4D:BF   -1    5 - 0      0        1
```

Figura 3.3 Puntos de acceso disponibles en el medio

Se pudo apreciar que había cinco puntos de acceso con el ESSID ESPOL. Con herramientas normales de conexión Inalámbrica en Windows por ejemplo solo aparecería una sola vez la red ESPOL. Con este programa podemos ver todos los puntos de acceso con ese nombre así como identificar si se están enviando datos a sus clientes. El más cercano tiene una potencia de -57 dBm y el más lejano -91 dBm. Vemos que unos operan en el canal 1 y otros en el canal 11 del espectro de frecuencia. Esta diferencia de canales como se indicó anteriormente tiene la finalidad de evitar la interferencia entre los puntos de acceso.

3.2.2. Puntos de acceso ocultos

Según la documentación de Aircrack-ng disponible en la web, los puntos de acceso ocultos los podemos identificar mediante **<lenght: ?>** en la columna ESSID, donde "?" es un número que representa la cantidad de caracteres del SSID. Esta es una forma de darle seguridad a una red ya de esta manera es invisible para los usuarios y solamente acceden quienes conocen el nombre. [30]

Hay maneras de conocer el nombre de una red oculta con Aircrack-ng. En este caso hemos encontrado uno *(Ver Figura 3.3)* pero no fue objeto de estudio debido a que ya se había identificado la red a atacar que era ESPOL.

3.2.3. Tipo de seguridad presente

Según los datos de análisis de la salida del comando vimos que la red inalámbrica ESPOL a simple vista era abierta y no contaba con ningún tipo de seguridad ya que en la columna **ENC** aparecía como **OPN** (significa red abierta según la página web de Aircrack-ng Suite). Esto es engañoso ya que

realmente si cuenta con seguridad WPA-EAP mediante un servidor RADIUS. Nos pudimos dar cuenta de esto porque luego de conectarnos al punto de acceso y querer acceder a una página web se nos solicitó un nombre de usuario y contraseña para una autenticación. La herramienta Aircrack-ng no nos mostró el verdadero tipo de seguridad ya que esta sólo identifica puntos de acceso con seguridad WEP y WPA-PSK. [30]

3.2.4. Clientes conectados

En la parte de abajo de la salida del comando *(Ver Figura 3.3)* observamos también un listado de que clientes intentaron conectarse a que puntos de acceso. No necesariamente están conectados en ese momento. Intuyendo de que un cliente está conectado pudimos haber lanzado ataques de desautenticación al SSID del cliente, para obligarlo a volver a conectarse a la red. Esto podría ser aprovechado para que al conectarse nuevamente lo haga en un punto de acceso falso con el mismo nombre de ESPOL.

3.3. Penetración por la red inalámbrica

Una vez escaneados los puntos de acceso e identificado el objetivo de ataque se procedió a intentar entrar a la red con todos los servicios que esta otorga. De esta manera estaríamos conectados como si de un usuario legítimo se tratase suplantando su identidad. Para esto nos valimos de una técnica de ingeniería social que engaña al usuario proporcionándonos sus credenciales de conexión.

3.3.1. Red no protegida

En una red no protegida o red abierta no existe ninguna medida de seguridad para restringir el acceso a los usuarios. Estos pueden conectarse a la red e inmediatamente recibir todos los servicios que se proporcionan. La red ESPOL no es una red abierta por tanto no es el caso y no entró en nuestro estudio.

3.3.2. Red protegida

El ataque que realizamos en esta red protegida consistió en la creación de un Punto de Acceso falso que tuvo como ESSID

ESPOL. Se hizo esto para que cuando un cliente se conecte a este punto de acceso se le provea una dirección IP y al momento de hacer una petición HTTP esta sea reenviada a una página clonada de la interfaz web de autenticación del servidor RADIUS de ESPOL engañando de esta manera al usuario. Cuando la víctima escriba su nombre de usuario y contraseña y envíe los datos del formulario, capturaríamos esa información y así habríamos logrado conseguir credenciales válidas para acceder a la red.

Primeramente se configuró el servidor DHCP para proveer a los usuarios de direcciones IP cuando se conecten a nuestro punto de acceso. En este caso usamos el servidor llamado **dhcp3**. El archivo de configuración es */etc/dhcp3/dhcpd.conf* (Ver Anexo D).

Luego configuramos un servidor DNS para redireccionar al usuario a nuestro servidor local donde tendremos la interfaz web clonada. Para este efecto se usó la utilidad **dnsmasq.** En el archivo de configuración */etc/dnsmasq.conf* se ingresaron las líneas

interface=at0

address=/#/ 192.168.20.1

La interfaz **at0** es la del punto de acceso falso que cuando se creó más adelante tomó este nombre. La segunda línea de configuración significa que toda petición HTTP, cualquiera que sea, se vaya directamente a la dirección IP 192.168.20.1 que es la que se le configuro al punto de acceso falso en pasos posteriores ya que aquí se alojó la interfaz web clonada.

Se reinició el servidor DNS con */etc/init.d/dnsmasq restart.* Ahora como ya teníamos nuestra interfaz **mon0** creada anteriormente, se procedió a crear el AP falso con el nombre ESPOL y canal 11 (Ver Anexo E para ver una captura de la actividad del punto de acceso al iniciar).

airbase-ng -e ESPOL -c 11 -v mon0 &

Luego se levantó la interfaz y se le asignó dirección IP y puerta de enlace con los comandos:

ifconfig at0 up

ifconfig at0 192.168.20.1 netmask 255.255.255.0

route add -net 192.168.20.0 netmask 255.255.255.0 gw 192.168.20.1

Luego se activó el reenvío de paquetes entre la interfaz del AP y nuestra conexión a internet y activamos la traducción NAT del punto de acceso. Esto nos sirve en el caso que queramos que la víctima tenga acceso a internet por medio de nuestro AP. Para realizar esto se ejecutó el siguiente comando:

echo "1" > /proc/sys/net/ipv4/ip_forward

iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE

Luego creamos un enlace simbólico al proceso del servicio de DHCP para evitar errores al iniciar el servicio e iniciamos el servidor en la interfaz del punto de acceso (Ver Anexo F para observar una captura del inicio del servidor DHCP). Para esto se utilizaron los comandos

ln -s /var/run/dhcp3-server/dhcpd.pid /var/run/dhcpd.pid

dhcpd3 -d -f -cf /etc/dhcp3/dhcpd.conf at0 &

Luego se procedió a clonar la interfaz web de autenticación mediante una herramienta llamada SET (Kit de Herramientas de Ingeniería Social). Esta herramienta tiene muchas utilidades y entre una de ellas está la de clonar páginas web. La web del servidor de autenticación de la ESPOL para la red inalámbrica y la cual fue duplicada corresponde la dirección https://wifi.espol.edu.ec/fs/customwebauth/login.html .

Se inició la aplicación y se siguió los pasos mostrados por la misma herramienta en su interfaz para clonar una página web, llegando a lo que muestra la figura 3.4.

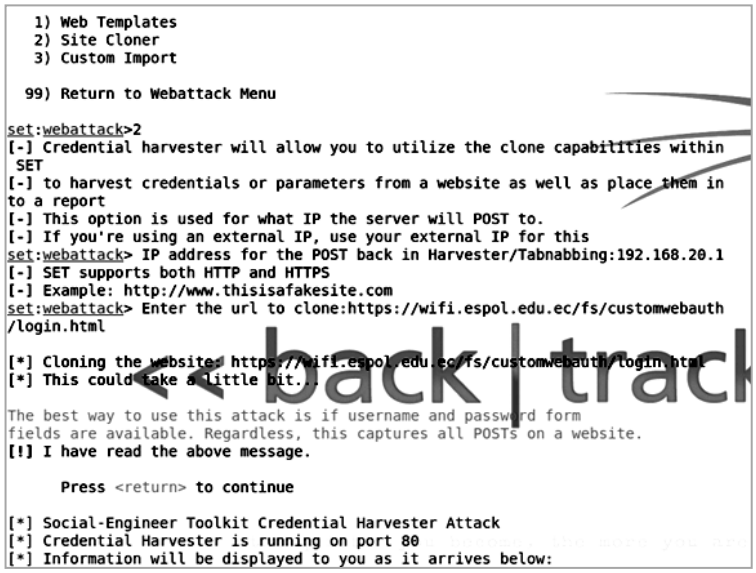


Figura 3.4 Interfaz para clonar páginas web. SET

Para esto se debió especificar la dirección IP con el cual se accede a la web clonada y la URL de la página a clonar. Luego de esto SET quedó a la espera de que un usuario ingrese sus datos y los envíe. La página en cuestión es mostrada en la Figura 3.5.

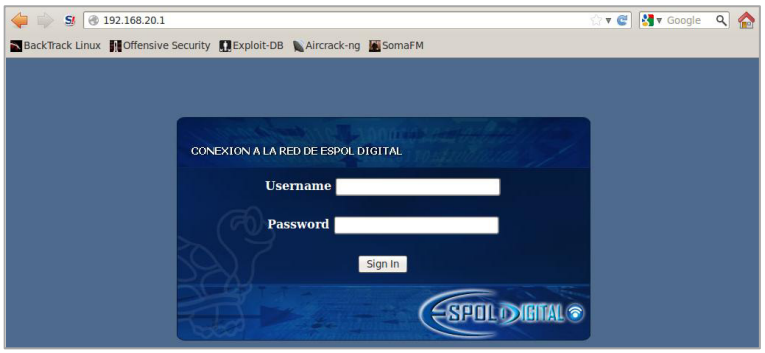


Figura 3.5 Interfaz web de autenticación clonada

Luego de algunos minutos ciertos usuarios se conectaron al AP falso e intentaron autenticarse en la web clonada pensando que era sitio oficial. Cuando esto sucedió SET capturó el nombre de usuario y contraseña mostrándolo en su interfaz tal y como se puede apreciar en la Figura 3.6. De esta manera ya tuvimos acceso a la red con credenciales válidas. (Ver Anexo G para observar otra credencial capturada)

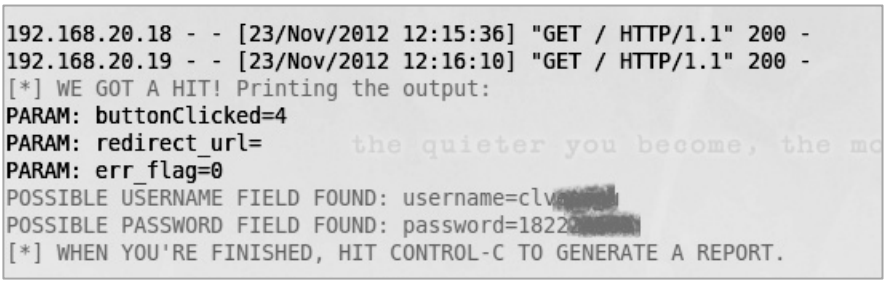


Figura 3.6 Captura de credenciales

CAPÍTULO 4

4. METODOLOGÍA DE ATAQUE DENTRO DE LA RED

En este capítulo se describe como se llevaron a cabo métodos de ataque dentro de la red interna, la cual se logró penetrar por medio de técnicas de ingeniería social. Se obtuvo información de los dispositivos de red como computadores personales y servidores DNS mediante un escaneo profundo de la red para luego lanzar vectores de ataque que midan el nivel de seguridad que presentan.

4.1. Escaneo de la red interna

Existen herramientas para explorar la red en busca de dispositivos conectados. Uno de ellas se llama *nmap* y su interfaz gráfica *Zenmap.* Según Gordon Lyon en su libro NMAP Network Scanning, “Nmap es una herramienta de código abierto usado para la exploración de la red y auditorias de seguridad”. [26]

Existen varias opciones al realizar un escaneo dependiendo de lo que se desee hallar.

- Obtener las direcciones IP de los hosts que están activos en la red para luego poder realizar un diagrama lógico de la red.
- Consultar que puertos se encuentran abiertos y los servicios que están en ejecución para luego investigar que vulnerabilidades se pueden explotar para dichos servicios.
- Identificar el sistema operativo que corresponden a cada uno de los hosts.
- Escanear un host especifico, luego de haberlo encontrado, en busca de vulnerabilidades ya reportadas por el fabricante y que no se han tomado las medidas necesarias para mitigarlas.

Con Zenmap se realizó un escaneo de la red *200.126.24.0/22* que es la que proporciona el punto de acceso cuando se establece la conexión. Por medio de varias opciones del comando nmap se encontró algunos datos de los hosts conectados en ella. La línea de comando utilizada fue:

nmap -sS -T4 -O -v 200.126.24.0/22

Donde la opción **–sS** permite hacer un escaneo de tipo **SYN** a los puertos, la opción **–O** permite averiguar el sistema operativo del host y las opciones **–T4** y **–v** permiten utilizar plantillas de tiempo y darle verbosidad al proceso de escaneo respectivamente. Estas opciones fueron tomadas de la ayuda del comando por medio de *nmap –h*.

El escaneo SYN es conocido como un escaneo sigiloso ya que envía paquetes SYN hacia los puertos del host como si fuera a comenzar una conexión real pero verdaderamente no se completa. Esto le da rapidez al escaneo y evita que el intento de conexión quede registrado en el objetivo. Al enviar un paquete SYN, si se recibe un paquete ACK/SYN entonces el puerto está abierto, si es un paquete RST entonces el puerto está cerrado, y si no se recibe respuesta alguna después de algunas retransmisiones o si se recibe un error de tipo ICMP no alcanzable entonces el puerto se encuentra filtrado [26].

4.1.1. Hosts activos

La Figura 4.1 muestra la lista de hosts activos que se encontraron durante el escaneo de la red. Aquí se puede apreciar que direcciones IP se encontraban conectadas en ese

momento. Estos resultados pueden cambiar dependiendo del momento en que se lleve a cabo el escaneo, ya que los clientes de la red inalámbrica luego se desconectan, pero los dispositivos que pertenecen a la administración de la red como enrutadores y servidores siempre estarán activos. (Para ver el resultado completo vea el Anexo H1 y H2).

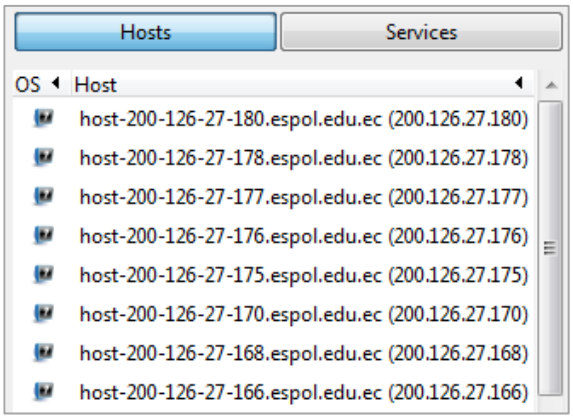


Figura 4.1. Host Activos Zenmap

4.1.2. Puertos y servicios

Entre los puertos y servicios que corren los hosts activos se pudo identificar aquellos que cuentan con servicios http, https, ftp y otros más. La figura 4.2 muestra ciertos servicios encontrados en algunos hosts. (Para ver el resultado completo vea el Anexo I)

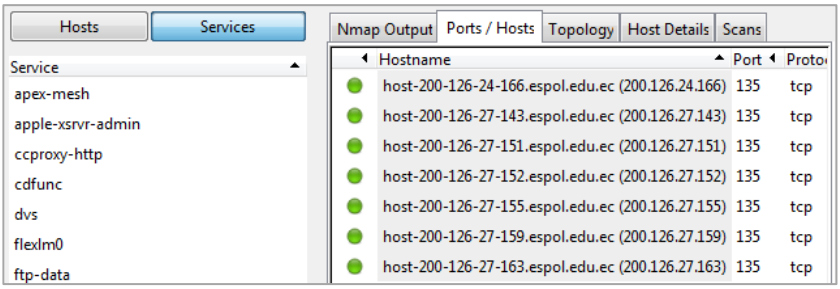


Figura 4.2. Puertos y servicios, Nmap

4.1.3. Identificación del sistema operativo de los hosts

En el escaneo realizado se detectó el tipo de sistema operativo que corre en los hosts con un cierto nivel de precisión cada uno. Esta información es muy útil para intuir y buscar las vulnerabilidades que pueden presentarse en ese sistema. La figura 4.3 muestra el sistema operativo detectado en un host y su nivel de precisión.

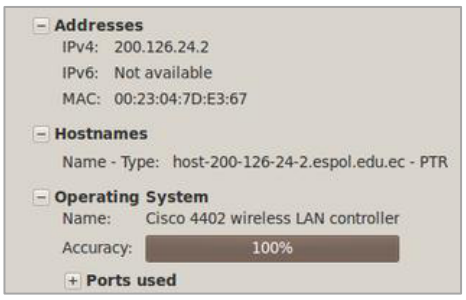


Figura 4.3. Detección de Sistema operativo, Zenmap

4.1.4. Identificación del dispositivo inalámbrico

Revisando los resultados del escaneo se observó que la herramienta Zenmap detecta *Cisco 4402 Wireless LAN Controller* como si fuera el sistema operativo del host 200.126.24.2, a pesar que no lo es. Se observó que este host contaba con puertos abiertos como el 22 que corresponde al servicio de SSH, el 443 que pertenece al protocolo HTTPS y el 16113 que es utilizado en este dispositivo Cisco por el protocolo de servicios de movilidad. (Ver estos resultados en Anexo J1 y Anexo J2). Con estos datos se puede intuir que todos los puntos de acceso de la ESPOL están administrados por este dispositivo que controla la red inalámbrica.

4.1.5. Diagrama de la red

Se realizó un diagrama lógico de la red mediante resultados obtenidos a través de un análisis de paquetes con Wireshark, para averiguar el servidor DHCP junto con la puerta de enlace y los servidores DNS, escaneos con *nmap* para hallar el controlador inalámbrico *WLC y* la herramienta *nslookup* para resolver nombres de dominio (Ver Anexo K y Anexo L para

consultar los resultados). La Figura 4.3 muestra el diagrama lógico que sólo pretende ser una guía general de la manera en que esta implementada la red inalámbrica.

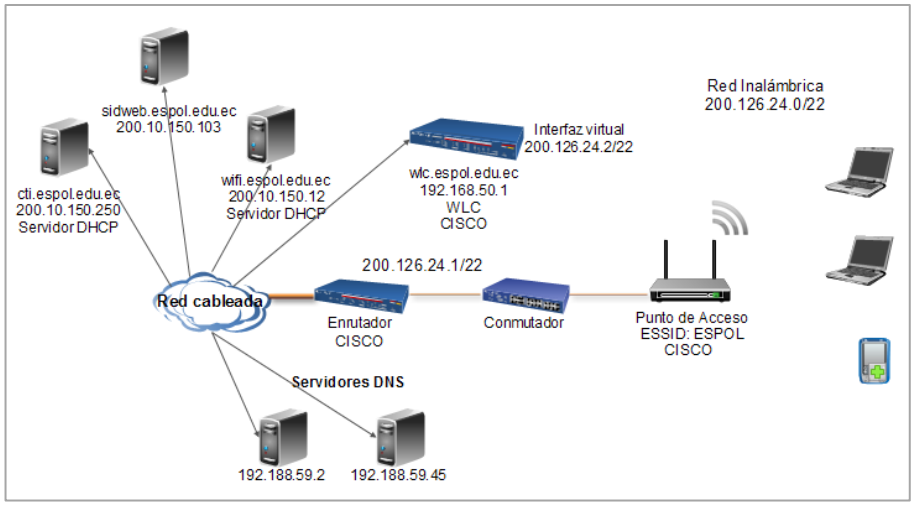


Figura 4.4. Diagrama de la red inalámbrica

4.1.6. Escaneo de vulnerabilidades

Una vez identificados los componentes de la red se procedió a realizar un escaneo de vulnerabilidades de los dispositivos de administración de la red mediante Nessus, el cual incorpora una larga base de datos de vulnerabilidades conocidas que pueden ser identificadas en las direcciones IP que se

especifiquen. Este programa se ejecutó usando un tipo de suscripción llamado HomeFeed[1].

Entre los terminales escaneados está la **puerta de enlace** que corresponde a la IP 200.126.24.1. Este host es de marca CISCO y no presentó ninguna vulnerabilidad conocida que pueda poner en riesgo el dispositivo y en consecuencia la red (Ver Figura 4.5).

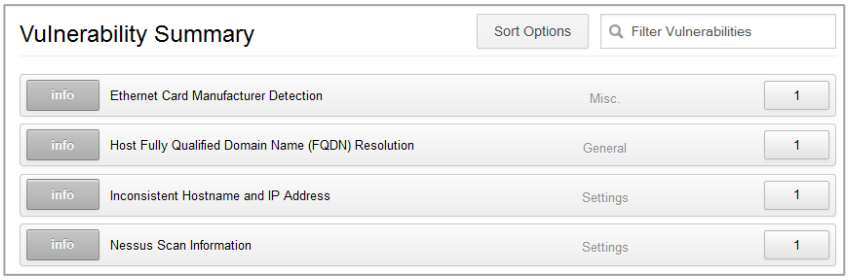


Figura 4.5. Reporte de vulnerabilidad del enrutador

El dispositivo **WLC de Cisco,** que controla los puntos de acceso, solamente accesible por SSH con la IP 200.126.24.2, también se sometió a un escaneo mostrando vulnerabilidades medias y bajas con respecto al protocolo SSL como muestra la Figura 4.5.

[1] La suscripción HomeFeed de Nessus es gratuita y está disponible para uso personal en ambientes pequeños para escaneos de hasta 16 direcciones IP.

Figura 4.6. Reporte de vulnerabilidad del WLC

El **host 200.10.150.12** que corresponde al servidor DHCP de la red inalámbrica y al host **wifi.espol.edu.ec** utilizado para la autenticación del usuario presentó vulnerabilidades medias y bajas a nivel de protocolo SSL y DHCP. En la Figura 4.7 se muestra el reporte.

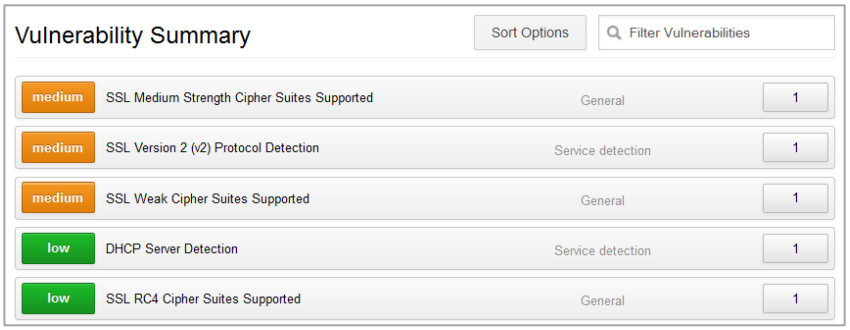


Figura 4.7. Reporte de vulnerabilidad del servidor DHCP

Los **servidores DNS** que corresponden a las IPs 192.188.59.2 y 192.188.59.45, presentaron vulnerabilidades medias respecto a sus servicios DNS como se muestra en la Figura 4.8.

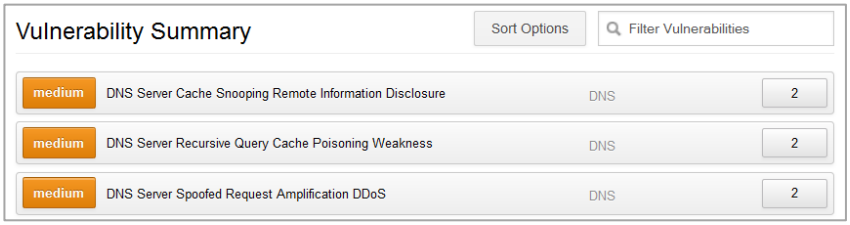


Figura 4.8. Reporte de vulnerabilidad de servidores DNS

Se realizó un escaneo de vulnerabilidades en dos los servidores de producción del que fueron el CTI y SIDWeb. Las figuras 4.9 y 4.10 muestran los resultados obtenidos respectivamente.

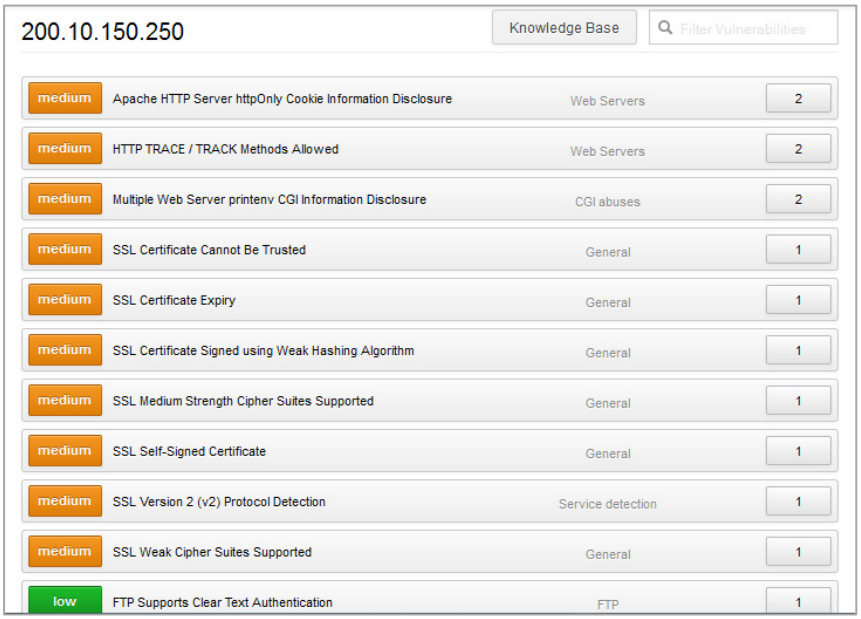


Figura 4.9. Reporte de vulnerabilidad de CTI

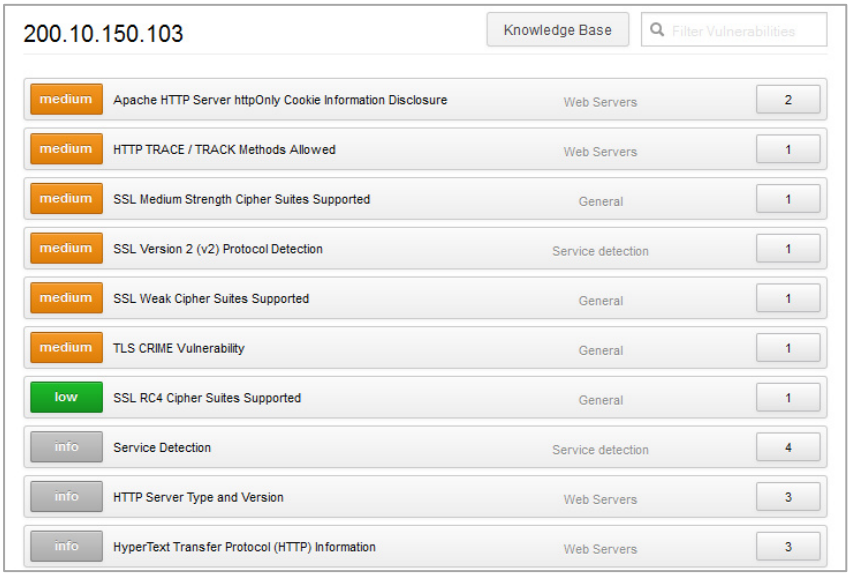


Figura 4.10. Reporte de vulnerabilidad de CTI

4.2. Ataque al dispositivo inalámbrico

El dispositivo que controla los puntos de acceso de manera centralizada es el llamado “Controlador de Redes Inalámbricas” de CISCO, como se vio en el subcapítulo anterior. Este elemento tiene una interfaz de administración tanto Web como SSH. Para ambos casos se probaron formas de ataque como ruptura de contraseña y explotación de vulnerabilidades según los resultados obtenidos anteriormente para analizar el nivel de seguridad que presenta. Si bien la dirección IP de este dispositivo es 200.126.24.2, este cuenta además con otra dirección IP accesible de igual forma desde la red inalámbrica. Esta es 192.168.50.1.

4.2.1. Ruptura de contraseñas de administración

Se hicieron pruebas de ruptura de contraseñas para el WLC con los valores predeterminados que son usuario admin y contraseña admin [46] sin lograr acceso. También se usaron herramientas conocidas como Hydra y Cisco Audtiting Tool en Backtrack para romper contraseñas por medio de ataques de fuerza bruta en la que con la ayuda de un diccionario, que no es más que un archivo que contiene una lista de posibles

contraseñas, se prueban cada una de ellas hasta coincidir con la verdadera. Estos ataques no tuvieron éxito.

4.2.2. Explotación de vulnerabilidades

En el WLC no se encontraron vulnerabilidades críticas que puedan ser explotadas con scripts o programas especializados publicados en Internet. Las vulnerabilidades encontradas fueron de nivel medio.

4.2.3. Ataques del tipo hombre en el medio

Los ataques de este tipo no fueron posibles ya que la interfaz de administración web, accesible con la IP 192.168.50.1, se encontraba en otra subred. Además la interfaz de administración SSH por medio de la red 200.126.24.0/22 no es utilizada para su gestión por lo que no se invirtió tiempo en este apartado.

4.3. Ataque a otros servidores

Si bien no existieron vulnerabilidades de alto nivel en el escaneo, se realizaron pruebas de seguridad mediante ataques de Denegación

de Servicio (DoS). Este ataque consiste en interrumpir un servicio de tal forma que no esté disponible para los usuarios [47]. En este caso se intentó colapsar el servicio web de algunos dominios dentro de la ESPOL resultando afectados los siguientes:

cti.espol.edu.ec

sidweb.espol.edu.ec

La herramienta que se utilizó se denomina *Slowloris (disponible en http://ha.ckers.org/slowloris/slowloris.pl)* que es un programa escrito en lenguaje Perl por Robert Hansen y consiste en inundar el servidor victima con conexiones HTTP hasta saturarlo y dejarlo fuera de servicio. El ataque tuvo éxito de manera que estas páginas web cesaron sus servicios durante el tiempo de duración que se permitió el ataque. El dominio *cti.espol.edu.ec* soportó alrededor de 1013 conexiones, y el dominio *sidweb.espol.edu.ec* alrededor de 1021 conexiones.

El comando que se utilizo fue el siguiente:

perl ./slowloris –dns dominio –options

donde la opción *dns* significa que se especificará el host de la víctima llamado *domain* que fue reemplazado en este caso por *cti.espol.edu.ec* y luego por *sidweb.espol.edu.ec*. La opción *options* es una opción propia del comando perl al ejecutar el script. La figura 4.11 y 4.12 muestra el proceso en la generación de conexiones al servicio Web tanto del CTI como del SIDWeb respectivamente.

Figura 4.11. Ataque DoS al CTI

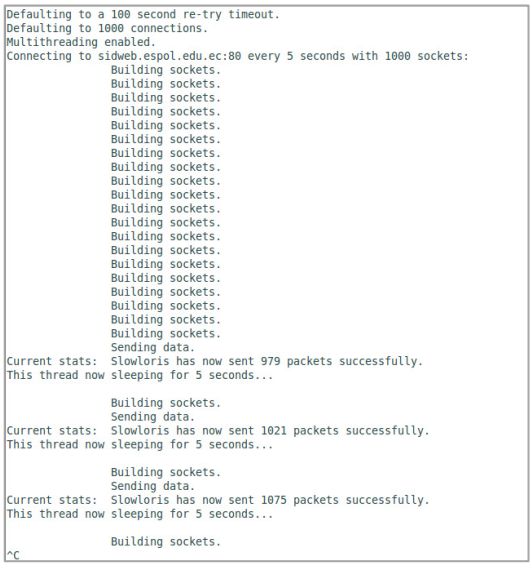


Figura 4.12. Ataque DoS al SIDWeb

La figura 4.13 y 4.14 muestra la conexión fallida al intentar entrar a la página del CTI y a la de SIDWeb respectivamente. Cabe destacar que si se cae el protocolo HTTP por ende también lo hará el protocolo HTTPS.

Figura 4.13. Sitio web cti.espol.edu.ec inaccesible

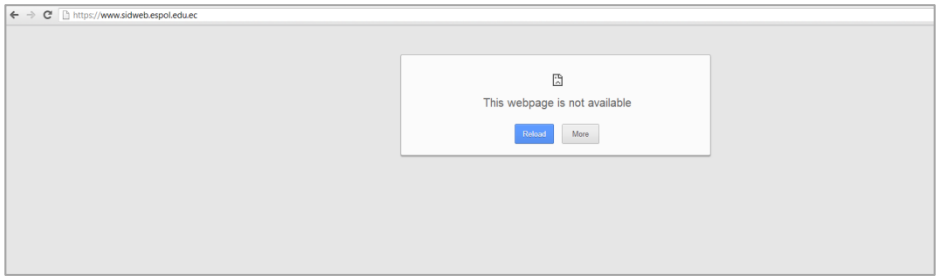


Figura 4.14. Sitio web cti.espol.edu.ec inaccesible

CAPÍTULO 5

5. ANÁLISIS EXPERIMENTAL DE VULNERABILIDADES

El análisis de los ataques que se han llevado a cabo, permite identificar el por qué son posibles dichos ataques y la manera en que estos funcionan explicando su mecanismo y los conceptos en los que están basados. Esto ayuda a entender el origen de las fallas de seguridad y a implementar medidas conscientes de mitigación para los administradores de red.

5.1. Información obtenida por Ingeniería Social

Hicimos algunas llamadas al CSI (Centro de Servicios de Información), donde obtuvimos información del servidor de autentificación de la red inalámbrica ESPOL, así también información sobre cuántos AP (Puntos de Acceso) tiene el Campus Prosperina en todas sus instalaciones.

Mediante la ingeniería social basada en computadora se logró engañar al usuario haciéndole creer que la página de autenticación a la red inalámbrica era la legítima. No se tuvo que hacer uso de correos electrónicos o mensajes de engaños ya que el mismo sistema de ESPOL nos permitió hacer creíble el engaño. Luego de que un usuario se conecta mediante un punto de acceso a la red ESPOL e intenta ingresar a una página de internet, inmediatamente es redirigido a una página autenticación donde debe escribir su usuario y contraseña. En nuestro ataque, cuando el usuario se conecta a nuestro punto de acceso falso ocurre exactamente lo mismo de tal manera que el usuario desconoce que en realidad el punto de acceso y la página de autenticación son falsos.

5.2. Redes inalámbricas sin protección de acceso administrativo

Existen redes inalámbricas que cuentan con puntos de acceso y dispositivos de control sin una contraseña de acceso administrativo hacia ellos. Muchas veces por descuido del personal dejan las contraseñas por defecto que vienen de fábrica dejando una gran brecha de seguridad en la administración de la red.

Se intentó acceder a los dispositivos de control utilizando la contraseña por omisión del mismo sin obtener resultados favorables, es decir los administradores han tomado las debidas precauciones cambiando inmediatamente el acceso por defecto.

5.3. Seguridad WEP

Según los resultados del escaneo de redes inalámbricas, la red ESPOL no cuenta con un tipo de seguridad WEP en sus puntos de acceso para la autenticación de los usuarios. Por esto no fue necesario utilizar herramientas de ruptura de contraseñas WEP como lo tiene el mismo Aircrack-ng Suite.

5.4. Contraseñas WPA, WPA2 no seguras

La seguridad WPA de la red inalámbrica ESPOL no es por medio de clave compartida, sino por un protocolo de autenticación extensible. En el caso de claves compartidas se puede llevar a cabo un ataque que consiste en capturar el paquete de saludo entre el usuario y el punto de acceso y averiguar la clave a través de un ataque de fuerza bruta con diccionario. En el caso de ESPOL que utiliza un protocolo de autenticación se necesita saber el nombre de usuario y luego hallar la contraseña por lo que se hace algo más complicado al ser dos parámetros a descubrir. Adicional a esto algunos servidores de autenticación tienen un número máximos de intentos erróneos luego del cual la cuenta se bloquea.

5.5. Seguridad WPS

Según en el blog de André Gasser en un apartado acerca de la seguridad WPS indica que para identificar si un punto de acceso cuenta con esta vulnerabilidad, basta con analizar paquetes con Wireshark. La figura 5.1 muestra en cuadros rojos lo que debe tomarse en cuenta para determinar si está configurada la seguridad WPS y por ende es vulnerable utilizando la herramienta Reaver de la que se habló en un capítulo anterior [42].La red ESPOL no cuenta

con seguridad WPS de acuerdo a los análisis de paquetes realizados con la herramienta Wireshark a los puntos de acceso.

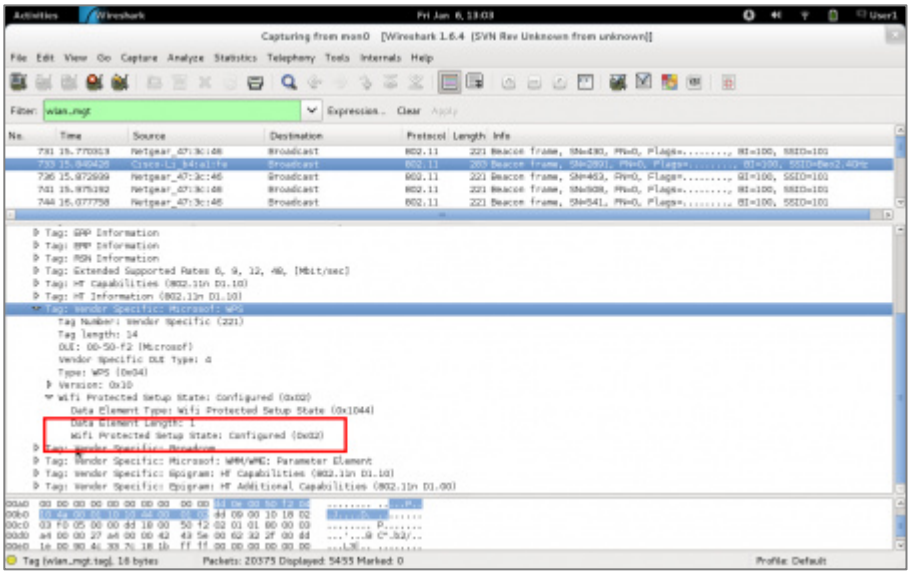


Figura 5.1. Análisis WPS con Wireshark [42]

5.6. Suplantación de identidad

Se suplantó la identidad de un punto de acceso legítimo y se logró que la víctima se conecte al dispositivo de esta forma obtener sus credenciales de acceso. Esto es posible debido a que las tarjetas de red funcionando en modo Gestionado al ver varios ESSID identifican al que tiene mayor potencia de señal de radio para conectarse [45].

Este tipo de ataque funciona cuando la víctima se encuentra cerca de nosotros y por ende recibirá mejor nuestra señal de radio.

Se suplantó también la interfaz Web de autenticación a la red para capturar las credenciales de la víctima. El proceso de conexión y autenticación mediante el punto de acceso falso es idéntico a como si se tratase de una conexión legitima. Es por esto que es muy difícil que la víctima pueda darse cuenta de lo que está ocurriendo y más aún si es un usuario que no conoce sobre redes.

5.7. Firmware de dispositivos inalámbricos desactualizado

En muchas ocasiones el software con el que cuentan los dispositivos de red presenta vulnerabilidades que son descubiertas y publicadas a través de Internet. Se intentó hallar algún fallo del software del dispositivo de administración pero no se encontró ninguno que pueda afectarlo. Cabe destacar que si el dispositivo estuviera desactualizado con alguna otra versión específica del firmware se hubiera logrado burlar el acceso administrativo. Por esto es importante que los administradores de red siempre mantengan actualizados los equipos y estén atentos a cualquier falla de seguridad que se presente por parte del fabricante.

5.8. Contraseñas de administración no seguras

Se intentó hallar la contraseña de administración del dispositivo de control inalámbrico mediante fuerza bruta. Estos ataques de diccionario son efectivos cuando las contraseñas son palabras fáciles de adivinar. Si la contraseña no es suficientemente segura entonces esta podría ser hallada mediante este tipo de ataque en cual se prueban todas las posibles contraseñas como si de un diccionario se tratase hasta que se da con la correcta. Esta técnica toma bastante tiempo dependiendo de la cantidad de palabras utilizadas y no se garantiza hallar la contraseña a menos que esta se encuentre dentro del diccionario.

5.9. Ataques DoS

Los ataques de denegación de servicios llevados a cabo en los servidores del CTI fueron exitosos debido a que el programa que intervino para este efecto llamado Slowloris compromete la capacidad de los servidores de manejar un número simultáneo de conexiones HTTP. Entre los servidores afectados por Slowloris están Apache 1.x y Apache 2.x, que si no cuentan con el módulo apropiado

para mitigar este ataque, son definitivamente vulnerables. Por medio de la herramienta *whatweb* desarrollada por *Andrew Horton* que permite identificar la tecnología utilizada en una página web dada ya sea con el URL o la dirección IP, se puede comprobar que la página del CTI y del SIDWeb utilizan el servidor web Apache 2.2.17, el cual es vulnerable a Slowloris.

Muchos de los servidores de producción del CTI cuentan con el servidor Apache, lo que los convierte muy probablemente en servidores completamente vulnerables al ataque de denegación de servicio realizado con esta herramienta.

CAPÍTULO 6

6. ANÁLISIS DE RESULTADOS Y MECANISMOS DE DEFENSA

Es necesario hacer un análisis de la información que se ha obtenido para de esta manera medir las consecuencias que conlleva el robo de información y la poca seguridad implementada. De acuerdo al grado de riesgo se presentan técnicas de mitigación para contrarrestar las falencias de seguridad y convertir la red inalámbrica en un lugar seguro para los usuarios.

6.1. Análisis de riesgos y vulnerabilidades reportados

Fácilmente los usuarios pudieron conectarse al punto de acceso falso con el nombre de ESPOL. A partir de aquí el usuario es completamente susceptible a muchos tipos de ataque ya que se encuentra conectado a una red que supuestamente brinda toda la confianza y garantías de seguridad sin conocer que realmente que se encuentra bajo el completo control de quien maliciosamente la creo. El usuario pudo ser engañado mediante páginas de Internet que él asume que son reales e ingresa contraseñas de sus cuentas o tarjetas de crédito por una compra u otro motivo.

Por medio de la página clonada, la herramienta SET reportó a dos estudiantes que ingresaron a ella proporcionándonos sus credenciales de autenticación. Este robo de información llega a ser crítico ya que el usuario y contraseña obtenida se manejan tanto en la cuenta del sistema académico como también SIDWeb y Mail de ESPOL. En muchas ocasiones las mismas contraseñas son utilizadas por el usuario para todo tipo de cuenta que poseen en Internet poniendo en riesgo el acceso a cuentas de correo y redes sociales como Hotmail, Gmail, Facebook, Twitter, entre otras. Por otro lado por un hacker malicioso puede llegar a cometer actos

ilícitos dentro en la red interna de ESPOL, utilizando la identidad del usuario así como hacer un uso inadecuado del internet para no ser descubierto.

Analizando los ataques de denegación de servicio, estos son muy calamitosos ya que al privar del servicio ofrecido por el SIDWeb y SIDWeb Beta conllevaría a que el sistema académico de la universidad se vea afectado ya que cesarían las actividades que los profesores realizan al igual que los estudiantes en el proceso de información, cursos, calificaciones, proyectos entre otras.

Debido a que el CTI también maneja otros servidores como Senescyt, GIS-CNE, CES, IAEN, etc, todos ellos con el Servidor Web Apache 2.x vulnerable a Slowloris, el efecto es aún peor ya que son utilizados por otras entidades privadas y gubernamentales que pagan por los servicios. El CTI también maneja el servidor NAGIOS que es un sistema de monitoreo de todos los servidores y utiliza de la misma forma la versión de Apache vulnerable. Hacer caer este servidor conllevaría a no poder monitorear los demás servidores vulnerables. Si los demás servidores son atacados junto con el NAGIOS, se perdería totalmente el control de los servicios web (El servidor NAGIOS fue atacado exitosamente en las pruebas).

Hay que tener en cuenta que muchos de los aplicativos de la universidad, no solo del CTI, son vulnerables a este ataque ya que utilizan el servidor Apache como la página de la FIEC, FIMCP, FEN, Blog de ESPOL, ESPOLTECH, etc.

6.2. Soluciones de seguridad frente a las vulnerabilidades encontradas

Detectar un punto de acceso falso es ya algo difícil de hacer y más para un usuario común. Existen sistemas de prevención de intrusos (IPS) tales como AirDefense o ZoneAlarm que tiene la capacidad de identificar aquellos puntos de acceso que se hacen pasar por legítimos. Cuando un atacante utiliza un punto de acceso falso, este tiene que utilizar herramientas para capturar los paquetes del usuario. Estos sistemas identifican el uso de estas herramientas. Algunos de estos sistemas también funcionan de tal manera que los puntos de acceso legítimos son detectados de acuerdo a algún identificador, y cuando se encuentra uno que no lo es, se lanza una alarma.

Para evitar ser víctima de páginas clonadas, por ejemplo la de ESPOL, el estudiante debe verificar que la página de autentificación se presente mediante el protocolo HTTPS con su debido certificado

digital. Por otro lado podría realizarse por parte de la institución un anuncio al estudiantado mediante un aviso de seguridad antes de ingresar sus credenciales, algo similar a lo que tiene las páginas Web de los Bancos como la del Banco del Pacífico [28] para que no sean víctimas de un robo de credenciales. Proporcionando este mensaje de Atención el estudiante podrá tener conocimiento que la página a la que va a ingresar sus credenciales cuente con las especificaciones descritas en el mensaje. (Ver figura 6.1)

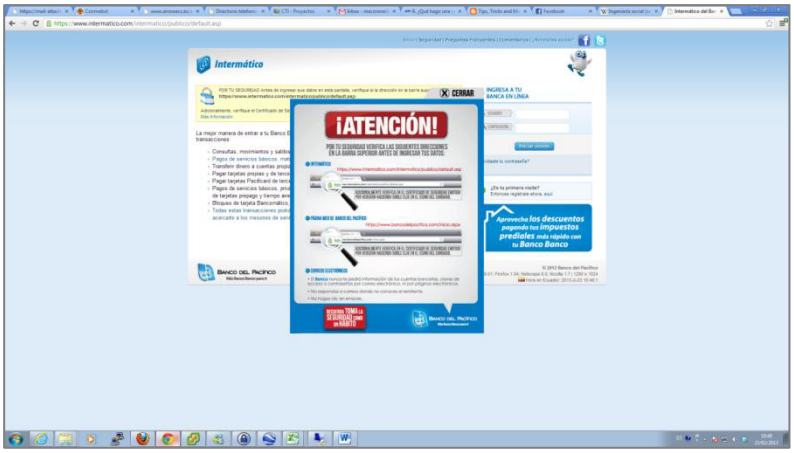


Figura 6.1. Página de ingreso a Intermático

Se entiende que las credenciales de acceso son únicas para cada usuario, sin embargo un usuario puede estar conectado con las mismas credenciales desde dos terminales diferentes. Por lo tanto se

debe implementar un sistema que solamente permita al usuario estar conectado desde un solo terminal.

Actualizar las versiones de los servidores Web afectados, especialmente Apache o activar los módulos disponibles para este servidor que bloquean específicamente el ataque de Slowloris.

Realizar una auditoría de seguridad minuciosa a todos los servidores para identificar otros problemas con los servicios web como por ejemplo ISS, actualizar software como Joomla, PHP, aplicar parches a huecos de seguridad potenciales previamente encontrados, entre otras, que pueden ser objetivos de ataque.

6.3. Ventajas y desventajas de las soluciones propuestas

Se debe tener cuidado con las políticas destinadas a detectar puntos de acceso falsos ya que de no ser así se pueden encontrar casos de falsos positivos o también que el sistema logre ser engañado fácilmente.

Una mala costumbre de los usuarios es no leer las advertencias que se presentan en pantalla, ya sea por tener conocimiento de tales

anuncios y no darle importancia, o por pensar que no existe la posibilidad de que lleguen a ser producto de un fraude. A esto se suma que los usuarios a veces no cuentan con tiempo suficiente para detenerse a leer, o simplemente se olvidan de verificar en caso de ya saber.

En cuanto a la autenticación, el hecho de sólo permitir a un usuario conectarse desde una sola terminal y no tener dos o más sesiones activas al mismo tiempo, puede traer incomodidad porque es probable que olviden cerrar su sesión en cierta máquina, y necesiten iniciarla en una diferente.

Para llevar a cabo las actualizaciones necesarias es indispensable realizar un plan de migración para así afectar lo menos posible a los usuarios y a los sistemas en producción.

CAPÍTULO 7

7. HERRAMIENTAS DE CONTROL, AUDITORÍA Y POLÍTICAS EN REDES WAN

Este capítulo es un poco apartado del desarrollo específico de este estudio y pretende ser una descripción general de herramientas de auditoría y políticas de seguridad que se deben tener en cuenta para mantener una red de trabajo confiable tanto para el acceso hacia ella como para los servicios que esta presta.

Es importante mantener las redes aseguradas y monitoreadas para cualquier eventualidad que se presente que ponga en riesgo la integridad de la misma. Por este motivo existen herramientas que ayudan a cumplir este objetivo y así garantizar en cierta medida que la red se encuentra protegida de acciones maliciosas. Por otro lado deben existir políticas en cuanto a la administración y operación de la red ya que esta es una parte muy importante en cuanto a la seguridad de los datos.

7.1. Seguridad de acceso inalámbrico a datos

La red inalámbrica dentro del campus nos provee de herramientas necesarias para nuestro desenvolvimiento diario a nivel académico tanto para el estudiantado como para profesores, por lo que es responsabilidad de ellos ser muy cuidadosos al momento de acceder a los servicios por medio de sus credenciales.

Es muy sencillo configurar un punto de acceso inalámbrico y más aún que un usuario se conecte a ella. Esta práctica es muy peligrosa porque el usuario está expuesto a revelar sus credenciales de acceso por medio de engaños de los que tal vez jamás se dé cuenta. Por este motivo la responsabilidad de acceder arbitrariamente a una red inalámbrica cualquiera y además sin tomar las debidas

precauciones y verificaciones pertinentes, cae directamente sobre el usuario. Por esto, acceder inalámbricamente a una red debe contar con las garantías necesarias que asegure el uso de la misma como conocer de antemano el punto de acceso, verificar que los servicios sean legítimos y estar pendiente a cualquier anomalía que jamás se haya presentado.

Es indispensable saber que el administrador de la red inalámbrica es responsable de los datos que los usuarios manejan dando confiabilidad a cada usuario, pero esto tampoco ayuda si alguien realiza algún tipo de ataque en el que pueda robar información importante, por lo que el usuario tiene que estar consciente de la seguridad de cada página en la que ingresa credenciales o datos importantes ya que esto es de única responsabilidad de cada usuario.

Es muy importante que la información que viaja por la red, tenerla muy bien organizada para de esta manera no exista problemas tanto de administración como de algún ataque hacia segmentos de la red.
Es muy importante restringir el ingreso a los datos, ya sea por usuarios independientes al ingreso de información específica para

saber quién y cuando fueron accedidos los datos o en su defecto quien los edita.

Todos los usuarios tienen la responsabilidad de hacer saber al centro de servicios de información CSI si existe en algún momento algún tipo de ataque o intruso que quiera perjudicar la integridad de la red o en su caso de los usuarios.

7.2. Seguridad en la configuración de puntos de acceso

Los puntos de acceso deben estar bien configurados de tal manera que no se vea comprometida la red. Entre buenas prácticas de configuración están la de asignar una contraseña de administración larga y difícil de adivinar, cambiar todas las contraseñas que vienen por defecto, restringir el acceso administrativo desde afuera es decir del lado de los usuarios, utilizar un buen cifrado de datos, desactivar el acceso WPS que es altamente vulnerable, utilizar un firmware actualizado recomendado por el fabricante para evitar huecos de seguridad, tener respaldo de la configuración del punto de acceso, etc.

7.3. Seguridad en el cifrado de información

Los datos que viajan por una red inalámbrica por el hecho de estar expuestos a todo cuanto le llegue su cobertura, deben tener un cifrado fuerte que enmascare la información para que no pueda ser leída fácilmente por un atacante. De acuerdo a capítulos anteriores de este estudio se habló de seguridad WEP, WPA y WPA2, los cuales cuentan con diferente tipo de cifrado siendo los más robustos y altamente recomendados los de WPA y WPA2.

7.4. Herramientas para auditorias

Existen muchas herramientas que nos pueden ayudar con la auditoria de la red inalámbrica brindándonos datos estadísticos, monitoreo y funciones que nos permiten sacar a la luz las malas configuraciones de los dispositivos y servicios con el fin de mejorar la seguridad en la red inalámbrica.

Las alternativas son muchas y la mayoría se las puede encontrar en distribuciones Linux especializadas para este efecto como Backtrack, WifiSlax, Wifiway que son las más conocidas. Estas distribuciones incorporan una infinidad de herramientas de auditoría de redes inalámbricas y cableadas, entre las que se pueden citar la suite de

Aircrack, Airoscript, GOYscript, BrutusHack, StringGenerator, Airlin, Wash, Reaver, CockiesMoster, AirSSL, Metasploit, Nessus, y muchas más.

También es parte de las auditorias tener organizado los puntos de acceso y saber la ubicación exacta de ellos, además de controlar el acceso a la red. Se debe incluir también la generación de estadísticas sobre cuáles son los Puntos de Acceso a los cuales los usuarios ingresan con más regularidad. Mediante esto se ayuda al administrador de red a buscar soluciones para que exista una mayor disponibilidad y mejor alcance en los sectores que generan más tráfico de red por los estudiantes. De igual manera controlar y verificar el contenido de las transacciones irregulares que los usuarios realicen.

7.5. Políticas de administración y operación

Se deben realizar políticas de administración y operación implementadas por el directorio para sus operadores y para usuarios que ayudara a regular y controlar los puntos de acceso, así como también el uso adecuado de la red. Deben existir leyes de penalización para estudiantes que se encuentren ingresando a sectores donde está prohibido para ellos, de igual manera si se está

tratando de ingresar a información clasificada únicamente para administradores. Estas políticas pueden ser definidas en diferentes categorías, así como también tienen que ser enfocadas a los estudiantes para su mejor funcionamiento.

Podemos definir algunas que nos parecen adecuadas:

1. Tener correctamente Identificadas la ubicación de cada punto de Acceso dentro del campus.

2. Llevar registro de mantenimiento cada cierto tiempo a cada punto de acceso así como también de datos estadísticos de cuantos alumnos ingresa promedio por semestre.

3. Todo punto de acceso que se quiera instalar debe ser aprobado por la entidad administradora de red del campus.

4. Llevar un monitoreo constante para detectar los puntos de acceso no autorizados presentes en el campus.

5. Informar al estudiantado sobre las políticas y manejo de la red inalámbrica dentro del campus.

6. Señalizar adecuadamente los lugares donde se encuentran cada punto de acceso para que el estudiante tenga conocimiento donde poder ubicarse para receptar mejor la señal.

7. Resolución de problemas referentes al daño o no funcionamiento de cada punto de acceso en el caso de que sea necesario.

Los estudiantes tienen que tener conocimiento del buen uso de la red inalámbrica, saber de las leyes que están implementadas y en el caso que no estén hay q implementarlas ya que si esto no se resuelve, el uso de la red no estará beneficiando a la institución.

CONCLUSIONES

1. A pesar de que no se abarcó todo lo referente a la seguridad de la red por cuestión de tiempo y esfuerzo, debido a que se debe analizar muchos puntos de todos los diferentes dispositivos para encontrar vulnerabilidades; se pudo demostrar que la red inalámbrica no es segura para los usuarios. De acuerdo a nuestras pruebas faltan medidas de seguridad para evitar los puntos de acceso falsos, y que el acceso que esta red provee hacia los servidores internos da paso a vulnerar los servicios que la universidad provee a los usuarios en general debido a una falta de seguridad en este caso de los servidores web.

2. Por otro lado más allá de la seguridad que necesita la infraestructura física y lógica de una red, el usuario juega un papel extremadamente importante ya que él es la brecha más peligrosa de seguridad en una organización. La

cultura de los usuarios con respecto a la seguridad de los sistemas debe ser una prioridad ante las demás medidas que se tomen. Generalmente esto no es tomado en cuenta por los administradores de red ni por los mismos usuarios, aun cuando ya conocen su responsabilidad.

3. Los mecanismos de defensa que consideramos factibles a implementar en primera instancia por el nivel de riesgo de los problemas que mitigan son: en primer lugar actualizar o parchar los servidores Apache y otros comprometidos como pueden ser dhttpd o GoAhead Webserver para evitar los ataques de denegación de servicio mediante Slowloris; luego solicitar un certificado digital confiable y mantenerlo actualizado para que sea implementado en la página Web de autenticación Wifi así como otros servidores que lo necesiten; y finalmente, concienciar a los usuarios sobre la verificación de este certificado al momento de iniciar sesión. Adicionalmente, se debe hacer un estudio para implementar un sistema de prevención de intrusos que detecte puntos de acceso falsos y un sistema de autenticación que no permita dos sesiones simultáneamente activas para un mismo usuario.

RECOMENDACIONES

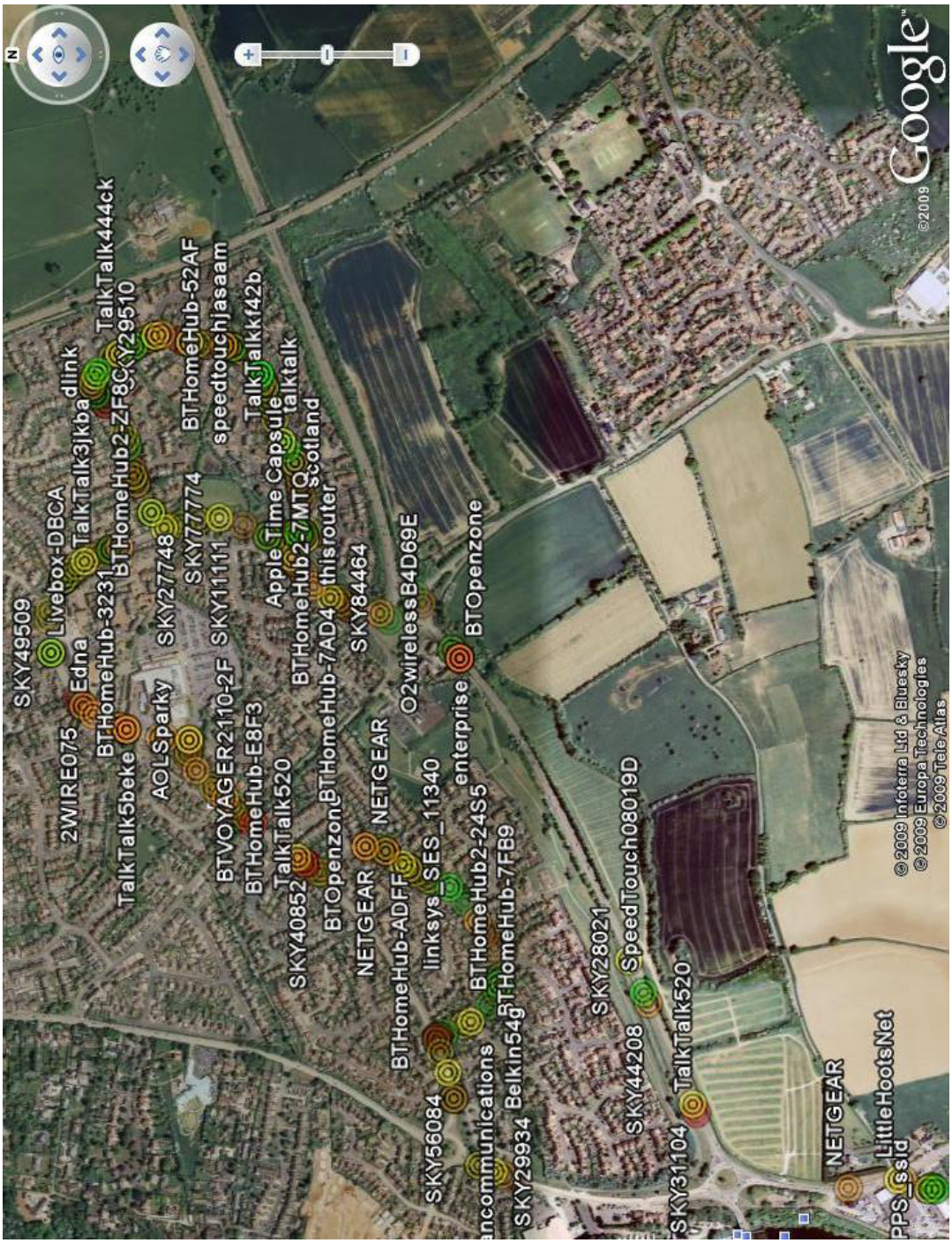
1. Las redes inalámbricas que no son reconocidas por la ESPOL deberían ser retiradas o justificar su existencia con las debidas políticas de seguridad y estudios previos porque además de generar interferencia con la señal de la red ESPOL, abren una brecha de seguridad con la red interna, más aun si esta no tiene autenticación alguna.

2. Se debe evitar en lo más posible que la red inalámbrica ESPOL tenga acceso a interfaces de administración de dispositivos como por ejemplo el Controlador de LAN Inalámbrica ya que los usuarios de esta red solo deberían tener acceso hacia Internet o a servicios como SIDWeb, Académico en línea, correo, etc.

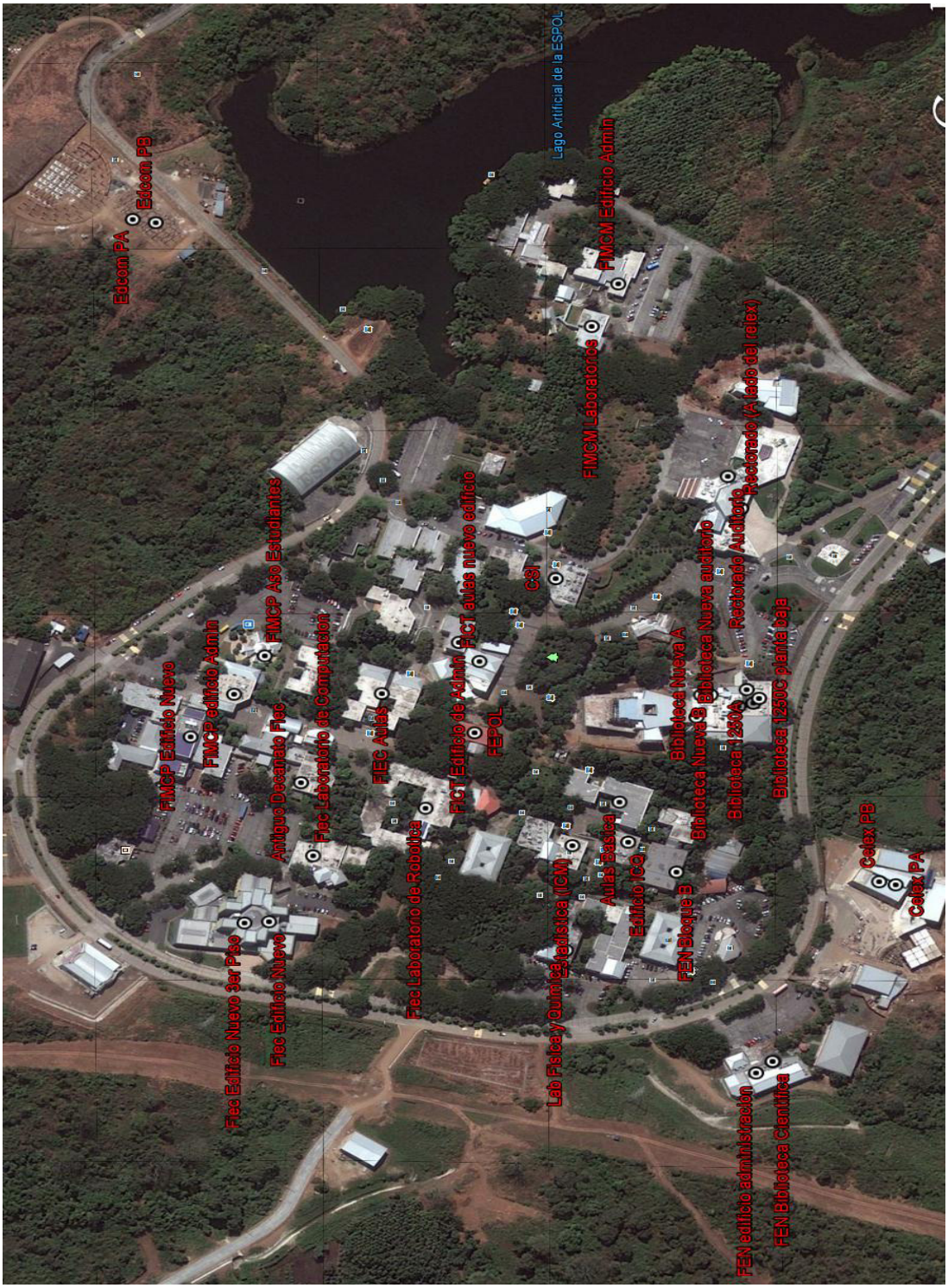
3. Se debe actualizar las políticas de seguridad determinando contraseñas de acceso diferentes para correo, SIDWeb y Académico en línea u obligar al estudiante cambiar de contraseña una vez otorgado su usuario para estos servicios. Esto incentivaría a los usuarios a hacer consciencia sobre lo importante de cada contraseña. Una buena práctica seria también que las contraseñas de estos servicios tengan un tiempo de expiración de manera que se obliga al usuario a renovarla frecuentemente.

4. Se recomienda monitorear constantemente la actividad de la red más de cerca en busca de actividad extraña como uso de herramientas espías en la red, trafico excesivo, intento de acceso a servidores y todo trafico anormal que sea potencialmente peligroso, tomando acciones de acuerdo a la política de seguridad implementada.

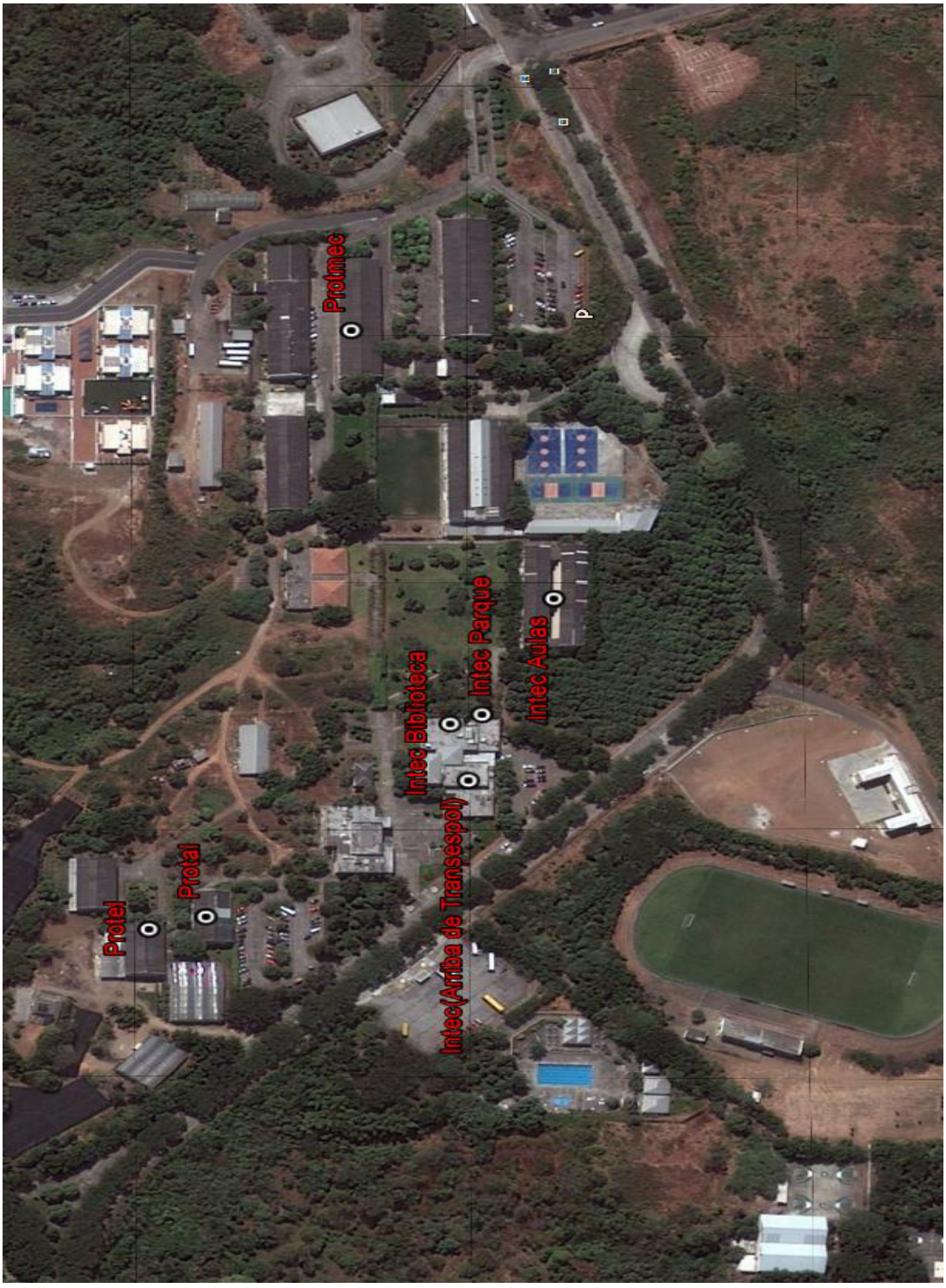
ANEXO A. EJEMPLO DE WARDRIVING [37]



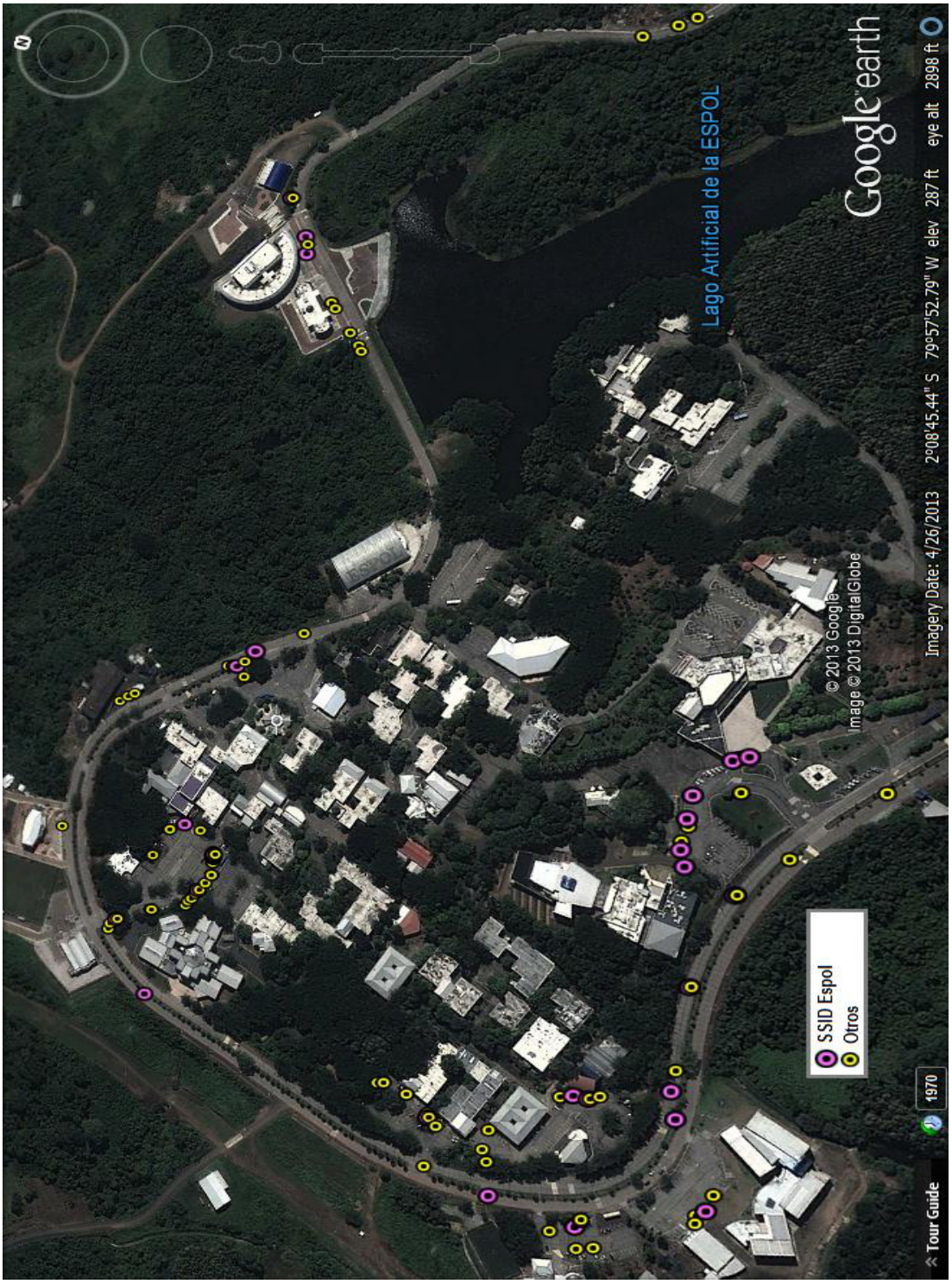
ANEXO B1. UBICACIÓN DE PUNTOS DE ACCESO EN ESPOL



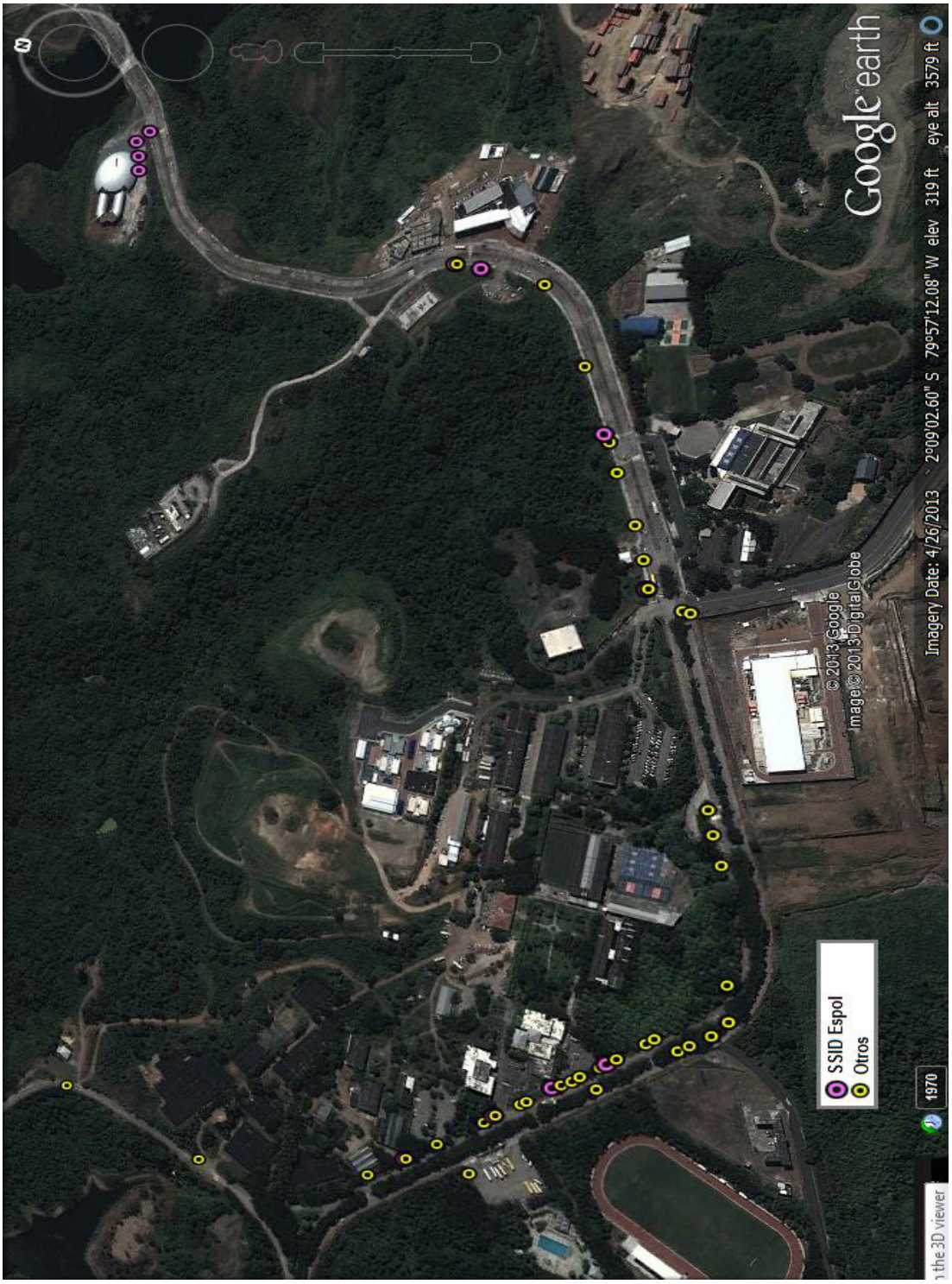
ANEXO B2. UBICACIÓN DE PUNTOS DE ACCESO EN ESPOL



ANEXO C1. RESULTADO DE WARDRIVING ESPOL (1)



ANEXO C2. RESULTADO DE WARDRIVING ESPOL (2)



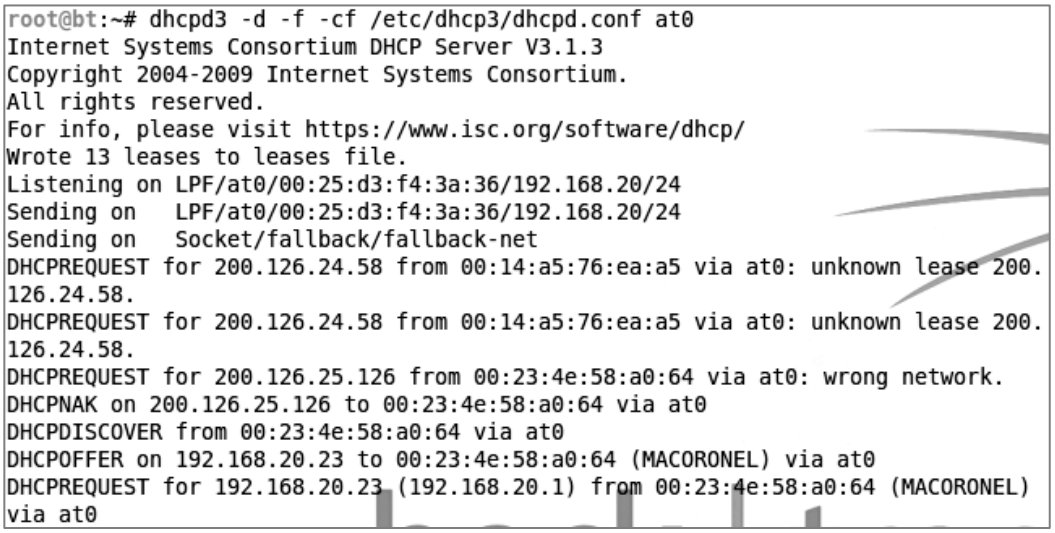
ANEXO D. ARCHIVO */etc/dhcp3/dhcpd.conf*

```
ddns-update-style none;
option domain-name-servers 192.168.20.1;
default-lease-time 60;
max-lease-time 72;
authoritative;
log-facility local7;
subnet 192.168.0.0 netmask 255.255.255.0 {
range 192.168.20.10 192.168.20.100;
option routers 192.168.20.1;
option domain-name-servers 192.168.20.1;
}
```

ANEXO E. ACTIVIDAD DEL PUNTO DE ACCESO FALSO

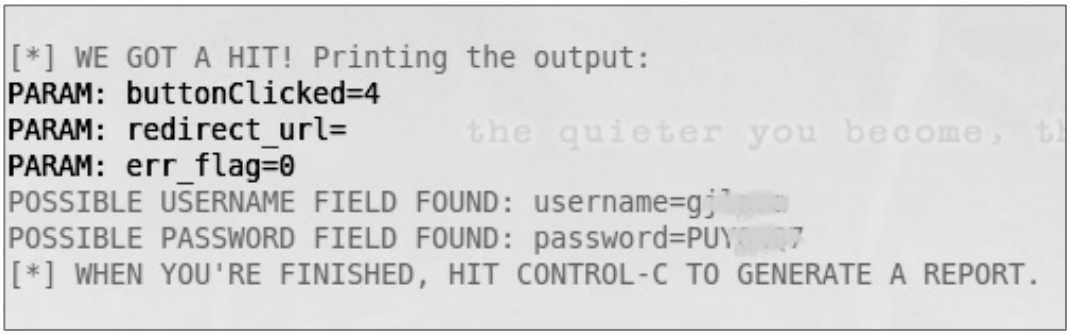
```
root@bt:~# airbase-ng -e ESPOL -c 11 -v mon0
11:56:59  Created tap interface at0
11:56:59  Trying to set MTU on at0 to 1500
11:56:59  Trying to set MTU on mon0 to 1800
11:56:59  Access Point with BSSID 00:25:D3:F4:3A:36 started.
11:57:02  Got directed probe request from 40:5F:BE:87:73:1D - "ESPOL"
11:57:04  Got directed probe request from 4C:0F:6E:2B:D3:24 - "ESPOL"
11:57:04  Got broadcast probe request from 5C:E8:EB:CB:97:A6
11:57:04  Got broadcast probe request from 5C:E8:EB:CB:97:A6
11:57:11  Got directed probe request from D4:87:D8:02:71:8B - "ESPOL"
11:57:14  Got broadcast probe request from CC:52:AF:56:E4:09
11:57:14  Got broadcast probe request from CC:52:AF:56:E4:09
11:57:14  Got broadcast probe request from CC:52:AF:56:E4:09
11:57:14  Got broadcast probe request from CC:52:AF:56:E4:09
11:57:14  Got directed probe request from 4C:0F:6E:2B:D3:24 - "ESPOL"
11:57:14  Got directed probe request from 4C:0F:6E:2B:D3:24 - "ESPOL"
```

ANEXO F. ACTIVIDAD DEL SERVICIO DHCP

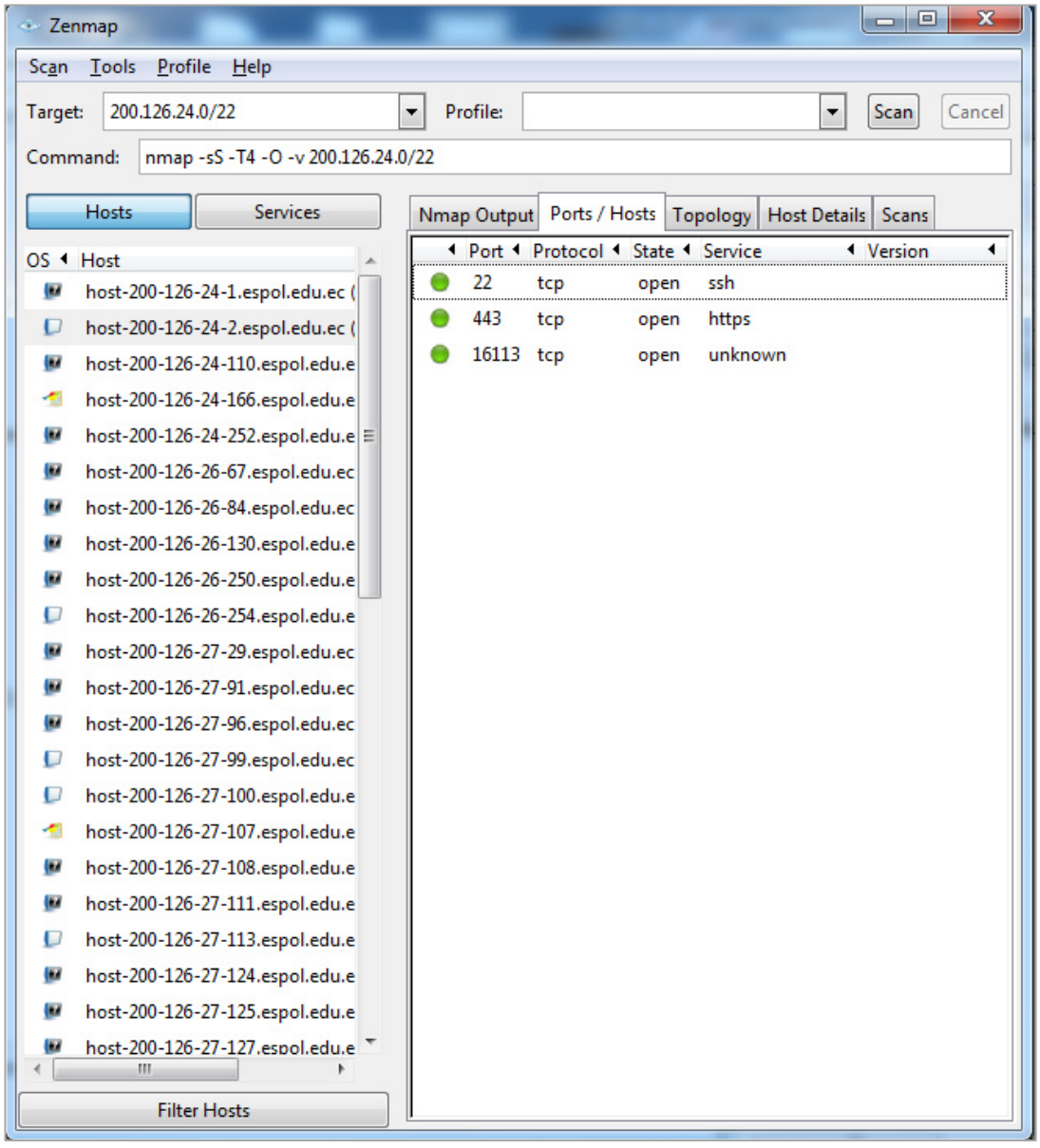


```
root@bt:~# dhcpd3 -d -f -cf /etc/dhcp3/dhcpd.conf at0
Internet Systems Consortium DHCP Server V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/
Wrote 13 leases to leases file.
Listening on LPF/at0/00:25:d3:f4:3a:36/192.168.20/24
Sending on   LPF/at0/00:25:d3:f4:3a:36/192.168.20/24
Sending on   Socket/fallback/fallback-net
DHCPREQUEST for 200.126.24.58 from 00:14:a5:76:ea:a5 via at0: unknown lease 200.
126.24.58.
DHCPREQUEST for 200.126.24.58 from 00:14:a5:76:ea:a5 via at0: unknown lease 200.
126.24.58.
DHCPREQUEST for 200.126.25.126 from 00:23:4e:58:a0:64 via at0: wrong network.
DHCPNAK on 200.126.25.126 to 00:23:4e:58:a0:64 via at0
DHCPDISCOVER from 00:23:4e:58:a0:64 via at0
DHCPOFFER on 192.168.20.23 to 00:23:4e:58:a0:64 (MACORONEL) via at0
DHCPREQUEST for 192.168.20.23 (192.168.20.1) from 00:23:4e:58:a0:64 (MACORONEL)
via at0
```

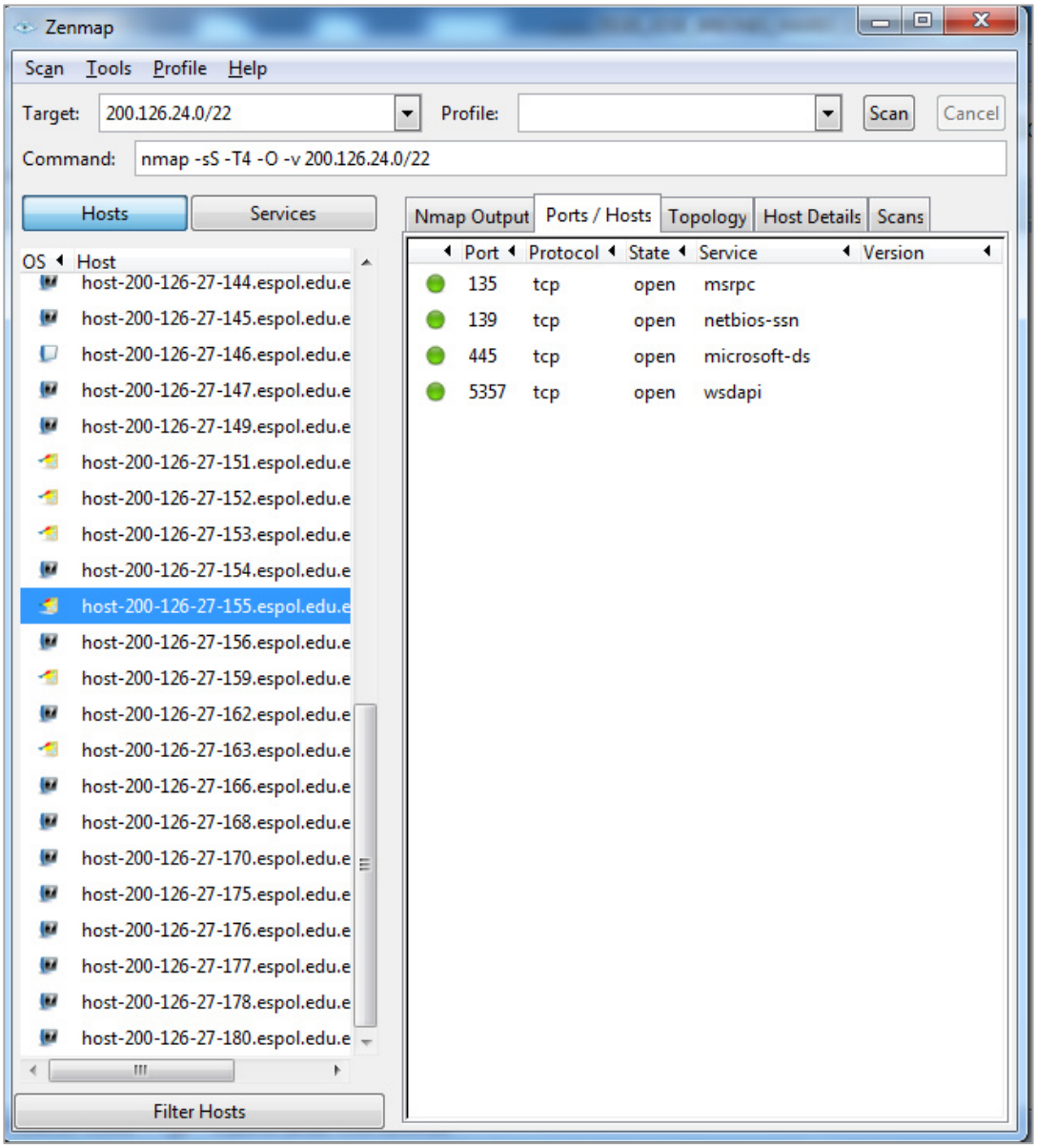
ANEXO G. CREDENCIALES CAPTURADAS POR SET



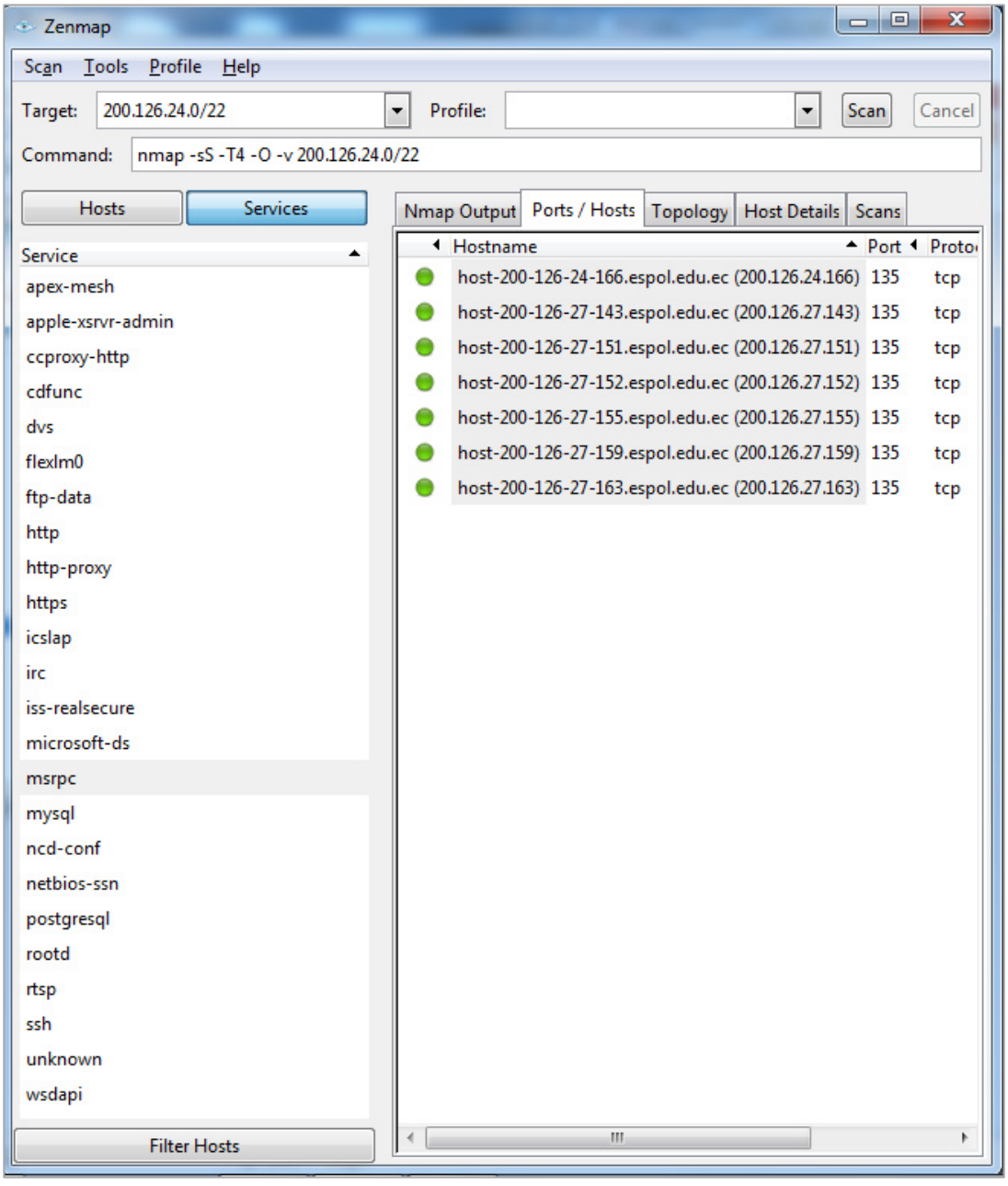
ANEXO H1. ESCANEO DE LA RED 200.126.24.0 (1)



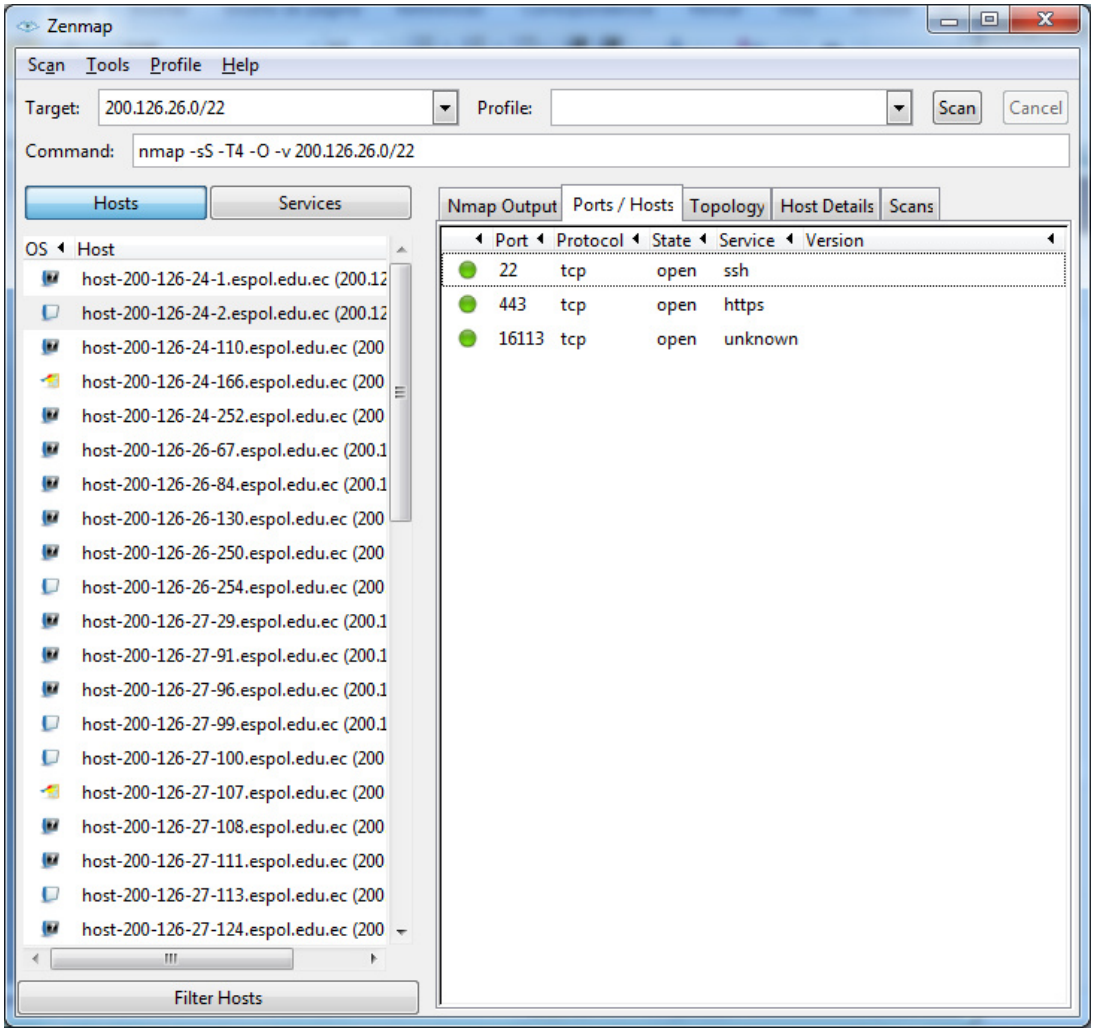
ANEXO H2. ESCANEO DE LA RED 200.126.24.0 (2)



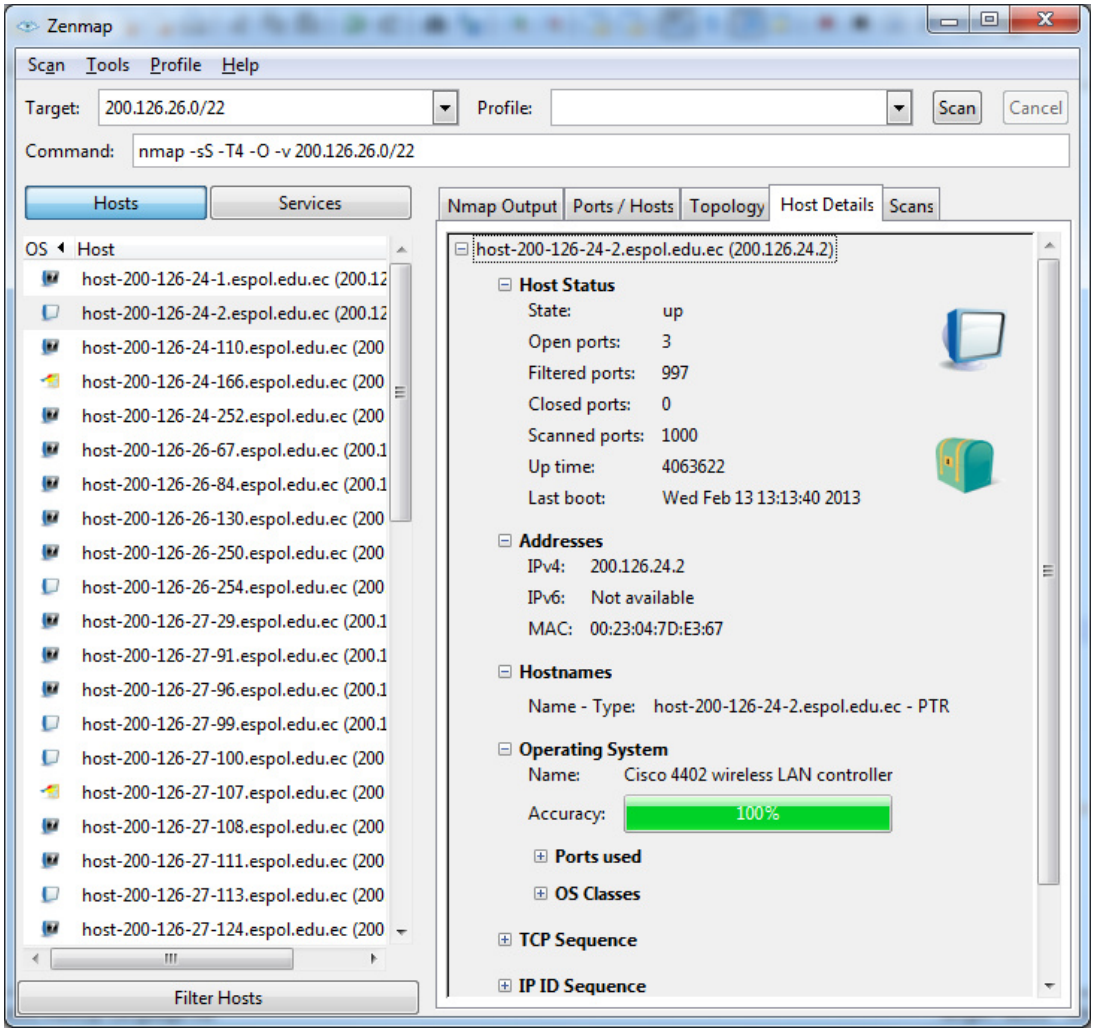
ANEXO I. ESCANEO DE LA RED 200.126.24.0 (3)



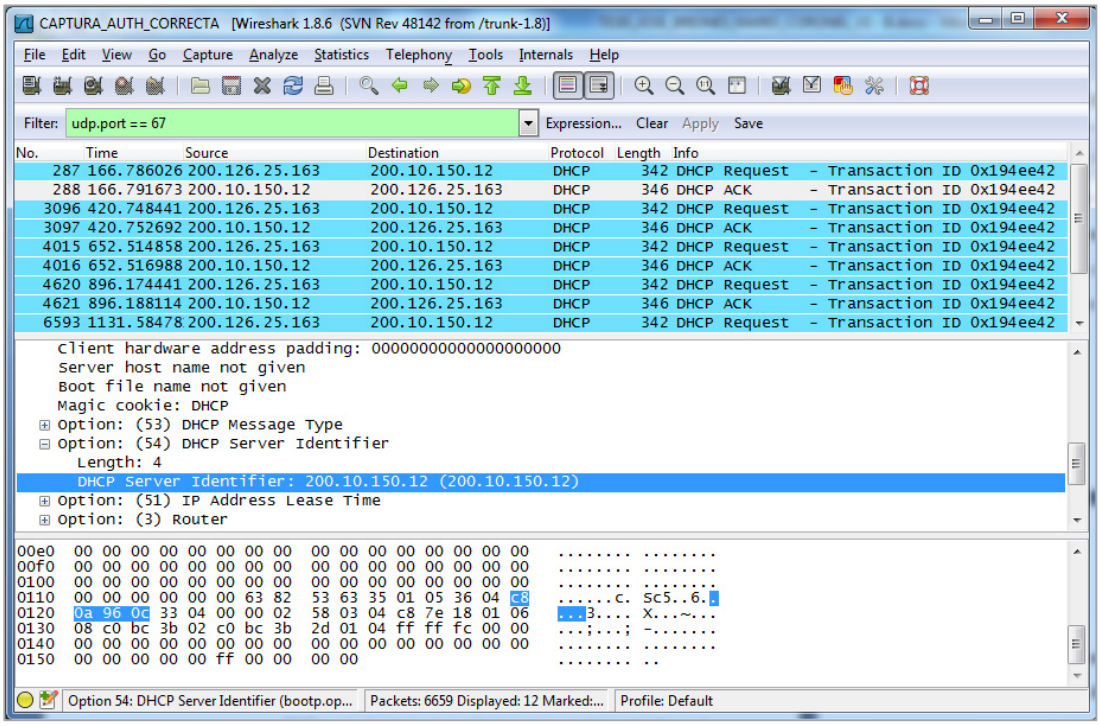
ANEXO J1. Escaneo del WLC (1)



ANEXO J2. ESCANEO DEL WLC (2)



ANEXO K. DIRECCIÓN IP DEL SERVIDOR DHCP



ANEXO L. DIRECCIONES IP Y NOMBRES DE DOMINIO

```
root@bt:~# ping wifi.espol.edu.ec
PING wifi.espol.edu.ec (200.10.150.12) 56(84) bytes of data.
64 bytes from 200.10.150.12: icmp_seq=1 ttl=64 time=1.36 ms
64 bytes from 200.10.150.12: icmp_seq=2 ttl=64 time=2.18 ms
^C
--- wifi.espol.edu.ec ping statistics ---
4 packets transmitted, 2 received, 50% packet loss, time 3012ms
rtt min/avg/max/mdev = 1.363/1.776/2.189/0.413 ms
root@bt:~# nslookup wifi.espol.edu.ec
Server:         192.188.59.45
Address:        192.188.59.45#53

Name:   wifi.espol.edu.ec
Address: 200.10.150.12

root@bt:~# nslookup espol.edu.ec
Server:         192.188.59.2
Address:        192.188.59.2#53

Name:   espol.edu.ec
Address: 192.188.59.33

root@bt:~# nslookup sidweb.espol.edu.ec
Server:         192.188.59.2
Address:        192.188.59.2#53

Name:   sidweb.espol.edu.ec
Address: 200.10.150.103

root@bt:~# nslookup 192.188.59.45
Server:         192.188.59.2
Address:        192.188.59.2#53

45.59.188.192.in-addr.arpa      name = ulises.espol.edu.ec.

root@bt:~# nslookup 192.188.59.2
Server:         192.188.59.2
Address:        192.188.59.2#53

2.59.188.192.in-addr.arpa       name = goliat.espol.edu.ec.
```

BIBLIOGRAFIA

[1] Lic. Héctor de Jesús Carlos Pérez, Karla Rocío Galván Salazar. “Redes Inalámbricas 802.11n el Nuevo Estándar”, *Consciencia Tecnológica No. 32,* Julio-Diciembre 2006

[2] “IEEE 802.11”, Visto en Diciembre 2012. Ultima modificación Febrero del 2013. Disponible: http://es.wikipedia.org/wiki/IEEE_802.11

[3] Andrea Fernanda Medina Andradre, Oscar Iván Castro Calderón. “Principales Estándares 802.11”, (en línea). Disponible: http://ieeestandards.galeon.com/aficiones1573579.html

[4] Javier Cañas R., “Introducción a las Redes Inalámbricas”, 13 de marzo del 2003

[5] Luis Alejandro Iturri Hinojosa, “Multiplexación Por División De Frecuencia Ortogonal”. Publicado Febrero 2011 en http://www.aiturrih.com

[6] Pablo Brenner. “A Technical Tutorial on the IEEE 802.11 Protocol”. Julio de 1996

[7] Ing. Pablo Jara Werchau, Ing. Patricia Nazar. “Estándar IEEE 802.11 X de las WLAN”, *Editorial de la Universidad Tecnológica Nacional.* Publicado en el año 2010 en http://www.edutecne.utn.edu.ar

[8] IEEE Computer Society. “IEEE Standard for Information Technology — Telecommunications and information exchange between systems. Local

and metropolitan area networks— Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". IEEE Std 802.11TM-2012. Elaborado el 29 de Marzo del 2012.

[9] Ing. José Roberto Vignoni, "Redes Inalámbricas". Elaborado en el 2008

[10] "Interferencias en Transmisiones Wifi", *Internet y Computadoras.* Diciembre 2010. Disponible en: http://www.amimefunciono.com.ar/

[11] Ermanno, Rob, "Introducción a las Redes Wifi", *Materiales de Entrenamiento para Instructores de Redes Inalámbricas".* Publicado en Junio del 2010

[12] Gerson Depablos. "Perdidas de señal en Wifi. Interferencias y obstáculos". Publicado en Junio del 2010. Disponible en: http://conocimientoswifi.blogspot.com/2010/06/perdidas-de-senal-en-wifi.html

[13] Panda Software International, S.L. "Seguridad en redes inalámbricas". Elaborado el 2005.

[14] Guillaume Lehembre, "Seguridad Wi-Fi – WEP, WPA y WP2" -hakin9 No 1/2006. Disponible en: http://www.hsc.fr/ressources/articles/hakin9_wifi/

[15] *Redes inalámbricas en los países en Desarrollo*. Tercera Edición

[16] "WI-FI Protected Access". Modificado en Septiembre de 2012. Disponible en: http://es.wikipedia.org/wiki/Wi-Fi_Protected_Access

[17] Jhonatan Revelo - Edison Pazmiño, “Análisis de WPA/WPA2 Vs WEP”, *Maestría en Gerencia de Redes y Telecomunicaciones.* Febrero 2008.

[18] Joel Barrios Dueñas, “¿Que es WPA? ¿Por qué debería usarlo en lugar de WEP?”. Artículo publicado en Abril del 2007 con licencia CreativeCommons Reconocimiento 2.5. Disponible en: www.alcancelibre.org. Enlace permanente: http://www.alcancelibre.org/article.php/20070404112747533

[19] Frank H. Katz, “WPA vs. WPA2: Is WPA2 Really an Improvement on WPA?”.*Armstrong Atlantic State University - Department of Information, Computing, and Engineering*. Publicado en 4th Annual Computer Security Conference, Abril 15-16, 2010.

[20] “RADIUS”. *Wikipedia La enciclopedia libre*. Modificado en Febrero del 2013. Disponible en: http://es.wikipedia.org/wiki/RADIUS

[21] “WEP, WPA, WPA2, TKIP, AES, CCMP, EAP.”. Artículos publicado en Febrero del 2010. Disponible en: https://learningnetwork.cisco.com/thread/11207

[22] Wi-Fi Alliance. “Wi-Fi CERTIFIED Wi-Fi Protected Setup”. Diciembre 2010

[23] Sacha Fuentes, “WPS, tu red inalámbrica segura”. Publicado en Junio 2008. Disponible en: http://www.xataka.com/otros/wps-tu-red-inalambrica-segura

[24] J. Campiño, R. Daza. “WARDRIVING: ¿EL PRELUDIO A UN ATAQUE INALÁMBRICO?”Paper de proyecto de curso COMBA I+D. Universidad Santiago de Cali. Noviembre 2004

[25] Xavier Caballé. “Seguridad de las redes inalámbricas: Wardriving y Warchalking”. Artículo de Hispasec.com. Publicado en Noviembre del 2002. Disponible en:http://unaaldia.hispasec.com/2002/11/seguridad-de-las-redes-inalambricas.html

[26] Gordon “Fyodor” Lyon. ”NMAP Network Scanning” en *Nmap Reference Guide*. Disponible en http://nmap.org/book/man.html#man-description

[27] Intermático: Sistema de transacciones proporcionada por el Banco del Pacífico para uso de sus clientes.

[28] “Kevin Mitnick”. *Wikipedia La enciclopedia libre.* Ultima modificación Febrero 2013. Disponible en: http://es.wikipedia.org/wiki/Kevin_Mitnick

[29] Cristian Borghello, “El arma infalible: la Ingeniería Social”, Publicado Abril 2009. Disponible en:http://www.eset-la.com/centro-amenazas/articulo/arma-infalible-ingenieria-social/1515

[30] Airodump-ng. “Aircrack-ng Main Documentation”. Última modificación en mayo del 2012. Disponible en: http://www.aircrack-ng.org/documentation.html

[31] Virtudes Miguel Calcaño, Anny Nolberto Armengo, Dilannia Yinet Taveras Núñez, Sixta María Hernández Hinojosa, Alex Rafael Polanco Bobadilla, “Tipos de Ataques de Red”, *Curso Seguridad en Redes y*

Telecomunicaciones – Universidad Autónoma de Santo Domingo. Disponible en: *http://www.slideshare.net/alexpolanco1/tipos-de-ataques-en-la-red-alex-anny-dilannia-sixta-y-virtudes* . Publicado Abril 2012

[32] Aetsu, "Asaltando redes Wi-Fi, WEP/WPA", *Licencia CreativeCommons 3.0.* Publicado en Marzo del 2011 , disponible en: http://laleyendadetux.blogspot.com/2011/03/asaltando-redes-wifi-cifrado-wep-wpa.html

[33] Diego Espitia, "Capturar Contraseña de WPA/WPA2 con REAVER", publicado en Enero del 2012. Disponible en: http://diegosamuel.blogspot.com/2012/01/capturar-contrasena-de-wpawpa2-con.html

[34] Zion3R , "[Ataque DoS Wireless] Denegación de Servicio a una Red Wi-fi". Publicado en Marzo del 2012. Disponible en: http://www.blackploit.com/2012/03/ataque-dos-wireless-denegacion-de.html

[35] "Seguridad informática, consecuencias", Publicado en marzo del 2012. Disponible en: http://aplicacionesgraficaschinampas.blogspot.com/2012/03/seguridad-informatica-consecuencias.html

[36] Albert Batiste Troyano, "Protocolos de encaminamiento en redes inalámbricas mesh: un estudio teórico y experimental", *UNIVERSITAT OBERTA DE CATALUNYA*. Publicado en Junio del 2011.

[37] “Wardriving with Kismet Newcore and BackTrack 4”.Publicado en Junio del 2009. Disponible en http://blog.securityactive.co.uk/2009/07/17/wardriving-with-kismet-newcore-and-backtrack-4/

[38] “Estado del arte 802.11”, *Universidad Técnica Federico Santa María*. Modificado en junio del 2012. Disponible en: http://wiki.inf.utfsm.cl/index.php?title=Estado_del_arte_802.11

[39] “Wardriving con Windows Mobile (I de IV)”. Articulo de un blog publicado en Octubre del 2009. Disponible en: http://www.elladodelmal.com/2009/10/wardriving-con-windows-mobile-i-de-iv.html

[40] “Análisis de Tráfico “, Wikipedia Modificado 21 de junio del 2012. Disponible en: http://es.wikipedia.org/wiki/An%C3%A1lisis_de_tr%C3%A1fico

[41] “Wireless Networking in the Developing World”, Segunda edición. Diciembre del 2007.

[42] André Gasser, “How to Check if Wi-Fi Protected Setup (WPS) is Enabled”. Publicado en Enero del 2012. Disponible en: http://blog.andregasser.net/?p=243

[43] HackHistory “Ingeniería Social” 12 de Abril 2012 Disponible en: http://hackstory.net/Ingenier%C3%ADa_social

[44] Kimberly Graves . “Certified Ethical Hacker STUDY GUIDE” Version 6. 2010. pp. 50-53

[45] Hao Han, Bo Sheng, Chiu C. Tan, Qun Li, Sanglu Lu. “A Timing-Based Scheme for Rogue AP Detection”. Vol. 22, No. 11, Noviembre 2011. p. 1

[46] CISCO, “Cisco Wireless LAN Controller Configuration Guide”, Release 3.2. Capitulo 4. Disponible en: www.cisco.com

[47] Kimberly Graves, “Certified Ethical Hacker Study Guide”, Version 6, p. 174

[48] RSnake, “Slowloris HTTP DOS”. Disponible en: http://ha.ckers.org/

[49] Wilberto Vega Rivera, “Política de Uso y Seguridad de la Red Inalámbrica”, Universidad de Puerto Rico en Banyon, Oficina de Sistemas de Información. Redactado en Mayo del 2007. Disponible en: http://www.uprb.edu/politicas/PolItica_Uso_Seguridad_Red-Inalabrica.pdf

[50] Sanson, “Manual Basico WifiSlax3”. Publicado en seguridadwireless.net. Año de publicación: 2013

[51] CISCO, “Quick Start Guide: Cisco 4400 Series Wireless LAN Controllers”. Disponible en la página web : http://www.cisco.com/en/US/docs/wireless/controller/4400/quick/guide/ctrlv32.html