ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría En Seguridad Informática Aplicada

"DESARROLLO DE UN PLAN DE PRUEBAS DE VULNERABILIDAD A LA RED DE DATOS DE UNA EMPRESA PÚBLICA DE DISTRIBUCIÓN ELÉCTRICA CNEL EP"

TESIS DE GRADO

Previa a la obtención del Grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

JOSÉ LUIS PACHECO DELGADO

Guayaquil – Ecuador

AÑO: 2015

AGRADECIMIENTO

A mis padres, Elizabeth y Luis Felipe, por demostrar que todos los objetivos son alcanzables, sin importar lo imposible que parezcan, lo grande que sea y lo distante que estén.

A mis hermanos por ser luchadores por la vida y no dejarse vencer por lo obstáculos presentados.

A mi mejor amigo por ser fuente de inspiración de muchas metas alcanzadas y su apoyo innegable en la vida.

A mis tíos por su hospitalidad incondicional en cada fase de mi vida.

DEDICATORIA

A mis hijos Saskia, Said y Shelia por ser la fuente de inspiración y la fuerza que se requiere para buscar días mejores. A mi esposa Evelyn por brindarme su amor, entrega, compañía y alegría en los retos de cada día.

TRIBUNAL DE GRADUACIÓN

DIRECTOR MSIA

DIRECTOR TESIS

MG. LENIN FREIRE C

MIEMBRO PRINCIPAL

MG. ALBERT ESPINAL S.

DEDICACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral"

(Reglamento de Graduación de la ESPOL).

JOSE LUIS PACHECO DELGADO

RESUMEN

La empresa de distribución eléctrica CNEL EP, está formada por 10 Unidades de Negocio (UN), un Data Center y la Oficina Central, quien coordina la gestión administrativa y genera políticas corporativas.

Cada UN es la encargada de administrar y controlar su red LAN, WAN y WLAN, además el esquema de red de enrutamiento y seguridad perimetral aplicada en el Data Center es el mismo que se utiliza en cada UN.

La administración del tráfico de datos generado por la red LAN, WAN y WLAN es controlado por los routers y firewall, configurados en un esquema redundante, donde se aplican las políticas de seguridad impartidas por la Oficina Central.

A pesar de ello, algunas UN han reportado diferentes problemas de seguridad, tales como:

- No existe una política de cambio de clave para la red WLAN, la misma que se ha mantenido por más de un año sin cambio y muchas personas ajenas a CNEL EP la conocen y tiene acceso a la red corporativa sin control.
- No existe control de acceso al medio, cualquier computador o dispositivo móvil que se conecte a la red de datos, puede usar los servicios sin control de CNEL EP.
- No existe una política de seguridad para evitar la denegación de servicios, para controlar el tráfico de datos generado desde el interior de la red LAN y WLAN, lo que ha permitido que en varias UN los equipos de comunicaciones como switchs, routers y firewall fallen por saturación de memoria y procesador, provocando el bloqueo de todos los servicios, causando problema en todas las áreas administrativas y de atención al cliente por minutos e incluso horas.
- No existen herramientas especializadas para identificar los dispositivos que provoca la denegación de servicios en la red de datos. Actualmente esta tarea es manual, como desconexiones de enlaces de datos, que afectan a varias áreas de trabajo como pisos o unos bloques de pisos. Después de aplicar este mismo procedimiento dentro de cada área de trabajo, se pudo identificar a switch de accesos y AP que se encontraban en mal estado; así como también se pudo identificar y bloquear teléfonos móviles como los causantes de estos incidentes.

- No existe un reglamento específico y detallado aplicado para la desvinculación del personal técnico que trabaja en el área de tecnología. Algunas aplicaciones y servicios dejaron de funcionar casi inmediatamente después de la separación de dicho personal. Para superar el incidente se tuvo que realizar tareas manuales, como: bloquear usuarios, cambiar claves, y revisar códigos fuentes de aplicaciones para identificar el origen del problema. (inventario de usuarios por sistemas)
- No existe un control de la seguridad de la información cada vez que se presenta un incidente.

ÍNDICE GENERAL

RESUMEN…… vi

ÍNDICE GENERAL……..... ix

ABREVIATURAS Y SIMBOLOGÍA…… xiii

ÍNDICE DE FIGURAS…… xiv

ÍNDICE DE TABLAS…… xix

INTRODUCCIÓN……... xx

CAPÍTULO 1: GENERALIDADES…… 1

1.1. Antecedentes……..... 1

1.2. Descripción del problema…….. 5

1.3. Solución propuesta……..... 7

1.4. Objetivo General…….. 9

1.5. Objetivos específicos…… 9

1.6. Metodología…….. 9

CAPÍTULO 2: MARCO TEÓRICO…… 38

2.1. Diagrama de red de datos corporativo…… 38

2.2. Características técnicas de los equipos de comunicaciones……... 39

2.3. Servicio de autenticación de usuarios…….……..…….…... 42

2.4. Servicio de autenticación del control de acceso al medio……..... 44

CAPÍTULO 3: LEVANTAMIENTO DE INFORMACIÓN……..…….…… 48

3.1. Zonas de seguridad perimetral…….…….…..... 48

3.2. Políticas de calidad de servicio…….……..……..…… 51

3.3. Políticas de control de acceso…….……..……..……. 56

3.4. Políticas de uso de Internet…….……... 59

3.5. Política desvinculación de personal…….…..... 61

CAPÍTULO 4: ANÁLISIS Y DIEÑO DE LAS PRUEBAS DE VULNERABILIDAD 67

4.1. Diseñar la matriz de riesgo……. 67

4.2. Definir herramientas de penetración informática……..... 77

4.3. Diseñar políticas de desvinculación del personal……. 78

4.4. Definir tipos de autenticación en la red de datos……... 79

4.5. Definir mecanismos de bloqueos en la red de datos…….…… 86

4.6. Definir QoS para garantizar la disponibilidad de los servicios…… 91

4.7. Definir políticas de control de acceso…….……..……..…… 94

4.8. Definir políticas para evitar ataques de Denegación de Servicios……100

CAPÍTULO 5: DESARROLLO DE LAS PRUEBAS DE VULNERABILIDAD….. 111

5.1. Desarrollar pruebas de vulnerabilidad……..... 111

5.2. Medir el riesgo y calcular el impacto…….…….…….… 122

5.3. Medir los tiempos de repuesta para bloquear a usuarios……..…128

5.4. Evaluar la infraestructura de red y medidas defensivas……. 133

5.5. Identificar el mejor esquema de red que se debe implementar……..…….. 132

5.6. Desarrollar el esquema de alertas tempranas…….…..... 144

CAPÍTULO 6: ANÁLISIS DE RESULTADOS…….…….… 150

6.1. Evaluar las amenazas mitigadas…….…….…….……..150

6.2. Analizar los riesgos mantenidos…….…….…….. 158

6.3. Evaluar el impacto administrativo las nuevas políticas de seguridad……159

6.4. Rediseñar el esquema de red corporativo…….…….163

CONCLUSIONES Y RECOMENDACIONES...……. 165

BIBLIOGRAFÍA……..…….……... 169

ANEXO I: VULNERABILIDADES DETECADAS CON NESSUS…….. 172

ANEXO II: INFORME TÉCNICO DE ESCANEO DE VULNERABILIDADES REALIZADAS A LOS SERVIDORES FINANCIERO, NÓMINA Y DIRECTORIO ACTIVO UTILIZADOS EN CNEL EP…….. 174

ANEXO III: AUTORIZACION PARA DESARROLLAR TEMA DE TESIS …… 175

ABREVIATURAS Y SIMBOLOGÍA

CNEL EP	Empresa Eléctrica Pública Estratégica Corporación Nacional de Electricidad CNEL EP
CNT	Proveedor de Servicio de Internet estatal
FW	Firewall
GSI	Gerencia de Seguridad de la Información
GTI	Gerencia de Tecnología de la Información
LAN	Red de Área Local
ISP	Proveedor de Servicio de Internet
RADIUS	Servidor de Usuario de Acceso Telefónico de Autenticación Remota
SO	Sistema Operativo
SW	Switch de acceso
TELCONET	Proveedor de Servicio de Internet privado
UN	Unidad de Negocio
WAN	Red de Área Amplia
WLAN	Red de Área Local Inalámbrica

INDICE DE FIGURAS

Figura 1.1: Diagrama de red de datos de una UN de CNEL EP……. 3

Figura 1.2: Comando nslookup ejecutando en entorno CLI…… 14

Figura 1.3: Consulta who-is en la página www.nic.ec…… 15

Figura 1.4: Interface gráfica del ping sweep…….. 18

Figura 1.5: NMAP buscando puertos y SO…… 23

Figura 1.6: Vulnerabilidades encontradas por *nessus*..…….. 25

Figura 1.7: Metasploit en modo consola…… .26

Figura 1.8: Entorno del comando msfconsole …….. 31

Figura 1.9: Tabla ARP con un computador Windows…….. 33

Figura 1.10: WireShark captura de paquetes……... 35

Figura 2.1: Diagrama de red de CNEL EP UN Los Ríos…… 39

Figura 2.2: Esquema de trabajo del 802.1x…….. 47

Figura 3.1: Zonas definidas en el firewall…… 49

Figura 3.2: Firewall en alta disponibilidad, una IP virtual protocolo VRRP.. 52

Figura 3.3: Protección de seguridad embebidas en el firewall……..…… 54

Figura 3.4: QoS aplicado por CNT en Agencias y Subestaciones…….. 56

Figura 3.5: Mensaje de página bloqueada por el Firewall……. 61

Figura 3.6: Gestión de baja de usuario definido por la GSI……. 66

Figura 4.1: Mapa de riesgo…… 77

Figura 4.2: Sistema de autenticación 802.1x…… 80

Figura 4.3: Servidor pfSense con las interfaces LAN y WAN…… 82

Figura 4.4: Módulo *FreeRADIUS* en pfSense…….. 82

Figura 4.5: Parámetros *NAS* en el FreeRADIUS…….. 83

Figura 4.6: Listado de todos los *NAS* en *FreeRADIUS*……83

Figura 4.7: Puerto de autenticación y de cuenta en *FreeRADIUS*..... 84

Figura 4.8: Habilita autenticación texto plano de MAC – *FreeRADIUS*…… 84

Figura 4.9: Autenticación EAP en FreeRADIUS…….…… 85

Figura 4.10: Aplicando puerto seguro ´por MAC…….. .87

Figura 4.11: Aplicando puerto seguro por ARP…… 88

Figura 4.12: Diagrama de red autenticar 802.1x……..… 89

Figura 4.13: Diagrama de red para configurar defensa IP……. 90

Figura 4.14: Diagrama de red para configurar supresión de tráfico……. 90

Figura 4.15: Diagrama de red previene ataques de falsos DHC…… 91

Figura 4.16: Sin aplicar QoS en puerto 0/0/6 ……..……..….. 93

Figura 4.17: Velocidad del puerto 0/0/6 previa al QoS……. 93

Figura 4.18: Aplicando QoS restringiendo la velocidad a 1Mbps……..…. 94

Figura 4.19: Velocidad medida después de QoS a 1Mbps……. 95

Figura 4.20: Esquema de autenticación en la red NAC……. 98

Figura 4.21: Firewall activando protección de seguridad……. 101

Figura 4.22: Activando protección contra ataques SYN FLOOD…… 102

Figura 4.23: Protección contra ataque UDP Flood X zona…….…… 102

Figura 4.24: Protección contra ataque ICMP Flood X zona……. 103

Figura 4.25: Protección contra ataque ARP Flood..…….…….. 104

Figura 4.26: Protección contra ataque SIP Flood..…….…….. 104

Figura 4.27: Protección contra ataque HTTP Flood ……..……..105

Figura 4.28: Protección de conexiones por inundación de paquetes…….. 106

Figura 4.29: Protección de detección de puertos……..... 106

Figura 4.30: Protección contra paquetes mal formados…… 108

Figura 4.31: Protección contra paquetes especiales…….. 108

Figura 4.32: Protección contra listas negras…… 109

Figura 4.33: Lista blanca analizadas en SYN, HTTP y SIP..…… 110

Figura 4.34: Activa la protección IP-MAC Binding, asocia IP con MAC……102

Figura 5.1: Entornos virtuales con herramientas de pruebas..... 111

Figura 5.2: Esquema de red para hacer pruebas de vulnerabilidad……. 113

Figura 5.3: *nmap* listando puertos y SO del firewall…….. 114

Figura 5.4: Vulnerabilidades firewall detectadas X *nessus*…… 114

Figura 5.5: *nmap* listando puertos y SO del SW CORE……..115

Figura 5.6: *nessus* vulnerabilidades del SW CORE…… 115

Figura 5.7: *nessus* vulnerabilidades del Prepago…… 116

Figura 5.8: *nmap* puertos y SO del Prepago…… 116

Figura 5.9: *nmap* puertos y SO del Servidor Comercial…….…….... 117

Figura 5.10: *nessus* vulnerabilidades del SRV Comercial…… 118

Figura 5.11: *nmap* puertos y SO del Servidor Financiero…… .118

Figura 5.12: *nessus* vulnerabilidades del srv Financiero……... 119

Figura 5.13: *nmap* puertos y SO del Servidor Nómina…..……. 119

Figura 5.14: *nessus* vulnerabilidades del SRV Nómina…….. 120

Figura 5.15: *nmap* puertos y SO del Directorio Activo……...…..... 120

Figura 5.16: *nessus* vulnerabilidades del Directorio Activo…..... 121

Figura 5.17: Bloqueo de un usuario en el Directorio Activo……132

Figura 5.18: Bloqueo lógico de interface de red……132

Figura 5.19: *nmap* muestra puerto filtrado en el firewall…… 133

Figura 5.20: *nessus* no muestra vulnerabilidades en el firewall…… 133

Figura 5.21: *Telnet* deshabilitado en el firewall…….134

Figura 5.22: *nmap* solo muestra el puerto 80 en el SW CORE…… 134

Figura 5.23: *nessus* no detecta vulnerabilidades en el SW CORE…… 135

Figura 5.24:*telnet* desactivado en el SW CORE…… 135

Figura 5.25: *nmap* puertos filtrados SRV Comercial Prepago..... 136

Figura 5.26: *nessus* no detecta vulnerabilidad del Prepago……..… 136

Figura 5.27: *nessus* no detecta vulnerabilidad SRV Comercial……... 137

Figura 5.28: *nmap* muestra puertos filtrados del SRV Comercial…… 138

Figura 5.29: *nessus* vulnerabilidad mantenida en el SRV Financiero…….. 139

Figura 5.30: *nmap* estado de los puertos del SRV Financiero……. 140

Figura 5.32: *nmap* estado de los puertos del SRV Directorio Activo…… 141

Figura 5.33: Nuevo esquema de red en la UN…….. 142

Figura 5.34: Enlaces redundantes en Agencias y Subestaciones…… 143

Figura 5.35: WhatsUpGold Ipswitch adquirido por CNEL EP……148

Figura 5.36: Alerta de correo electrónico generado por WhatsUpGold….. 149

Figura 6.1: Nuevo esquema de red corporativo CNEL EP…… 164

ÍNDICE DE TABLAS

Tabla 1: Características técnicas del router…..……...…… 40

Tabla 2: Características técnicas del switch de CORE……. 40

Tabla 3: Características técnicas del switch de acceso……..……... 41

Tabla 4: Características técnica del firewall…..…… 48

Tabla 5: Identificación del riesgo…… 75

Tabla 6: Estimación de riesgo…… 76

Tabla 7: Activos definidos en la matriz de riesgo..... 113

Tabla 8: Vulnerabilidades encontradas por nessus en Prepago…… 117

Tabla 9: Vulnerabilidades detectadas en activos de UN Los Ríos…….... 122

Tabla 10: Evaluación de la matriz de riesgo……..…… 129

Tabla 11: Tiempo empleado para bloquear un empleado en CNEL EP… 131

Tabla 12: Costo por implementar política de control de acceso……. 160

Tabla 13: Costo por implementar políticas de seguridad……..… 162

INTRODUCCIÓN

La implementación de la infraestructura de networking en el año 2013, fue un avance significativo que permite trabajar a todas las UN bajo un mismo esquema de red. Pero los problemas particulares de cada UN no son tratados corporativamente sino como casos aislados, proponiendo soluciones a mediano plazo, que hasta la fecha se han quedado en proyectos.

Con el ánimo de ser proactivo y adelantándome a los procesos que en su momento tratará la Gerencia Seguridad de la Información, se desarrolla un plan de pruebas de vulnerabilidades a los principales activos de la Unidad de Negocios Los Ríos, con el objetivo mantener la disponibilidad y confidencialidad de la información; y de garantizar que solo los dispositivos de CNEL EP puedan usar la red de datos.

La prueba de penetración o *pentesting* es la metodología utilizada, donde en la fase de escaneo se identifican las vulnerabilidades de seguridad de estos activos, que reflejan en menor o mayor medida problemas similares que

pueden presentarse en otras UN. Las herramientas utilizadas en esta fase son: nmap, nessus, nikto y metasploit.

La solución a los problemas presentados consiste en proponer la implementación de políticas y controles. Políticas como desvinculación de personal, control de acceso y denegación de servicios. Y controles como tipos de autenticación, mecanismos de bloqueo y calidad de servicios. A través de los switch y firewall ya instalados en las UN se puedo implementar parte de la solución.

En los switch: Permite implementar la política del control de acceso, activando la autenticación de dispositivos conectados a la red con un servidor RADIUS. Además controles como: Mecanismos de bloqueo con: puerto seguro y configuración de defensa contra ataques IP; calidad de servicio garantizando ancho de banda por puertos. En el firewall: Permite implementar la política de denegación de servicios, activando la protección contra ataques o flooding.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

La empresa de distribución eléctrica CNEL EP, está formada por 10 Unidades de Negocio (UN), un Data Center Corporativo y la Oficina Central quien coordina la gestión administrativa y genera políticas corporativas.

En cada UN existe un administrador de la red LAN, WAN y WLAN, supervisa la disponibilidad de los servicios locales y remotos, además monitorea los enlaces de datos activos y pasivos que brindan los Proveedores de Servicios de Internet ISP - CNT y TELCONET – hacia

las agencias, subestaciones, otras UN, el Data Center. Este esquema de red es el mismo en todas las UN.

Existen alrededor de 300 equipos informáticos en la UN Los Ríos, por lo que es necesario segmentar la red de datos en dominios de colisión o broadcast más pequeños, separados por VLAN's, Cada área de trabajos que puede estar agrupadas en pisos, edificios o departamentos tiene asociada una VLAN's. También existen VLAN's asociadas a servicios tales como: sistema de Radio Comunicaciones de 2 Vías, red WLAN corporativa con el mismo SSID, Sistema de Video Vigilancia Inteligente (IVS), etc.

La red perimetral está formada por un switch SW de CORE, conectado a un router - firewall y están conectados a los dos Proveedores de Servicios de Internet (ISP). Aguas abajo dentro de la red LAN se configuran las VLAN's para cada oficina y aguas arriba se conectan con las agencias, las subestaciones y otras UN.

Los servidores locales permanecen en la vlan 1 y los demás servicios de en la UN están configurados en diferentes vlan's.

El router – firewall trabaja con alta disponibilidad con el protocolo HSRP, tiene servicios integrados de seguridad contra ataques, VPN, NAT, QinQ, filtrado de contenido, router estático y dinámico, etc.

El switch de core, con funcionalidades de router permite realizar Vlan's, enlaces trunk, con servicios de autenticación local AAA y radius

Debido a la falta de una política de adquisición de equipos de infraestructura de tecnología, existen switches de accesos de diversas marcas y funcionalidades, algunas muy básicas que no permiten ser administrados y limitando algunos servicios corporativos.

La red WLAN es corporativa, su administración está centralizada en el Data Center y en todas las UN los Access Point son instalados con enlaces trunk desde los switch de acceso, razón por la cual está limitado su uso en varias áreas por no tener switch con estas características.

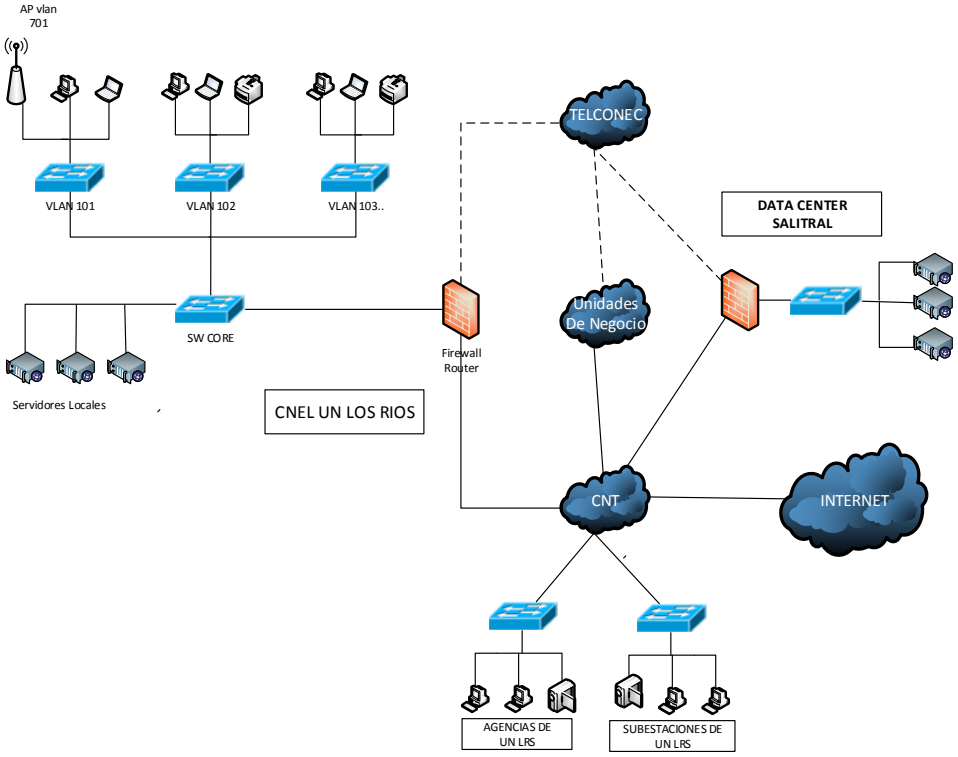


Figura 1.1: Diagrama de red de datos de una UN de CNEL EP

Los servidores locales son equipos HP Proliant con redundancia en discos y fuentes de poder, pero también existen computadoras de escritorios con funcionalidades de servidores, debido a la carencia de recursos se mantienen hasta la actualidad. Los servidores locales tienen los siguientes roles:

- Servidor HP Proliant de máquinas virtuales, con Sistema Operativo SO Windows 2008 Server R2, contiene las siguientes máquinas virtuales: servidor DHCP, servidor WSUS, servidor antivirus, servidor de aplicaciones de lectura de medidores sistema comerciales y otras relacionadas.
- Servidor HP Proliant del Sistema de Información Georeferencial GIS, con SO Windows 2008 Server R2.
- Servidor en computador de escritorio, sistema comercial Prepago. Con SO Windows XP
- Servidor de aplicaciones: reporteador Web del sistema comercial, sistema anterior financiero y de bodega; servidor proxy. Instalado en un computador de escritorio con Windows 2008 Server R2.
- Servidor HP Proliant con sistema de nómina anterior, SO CentOs 5.0
- Servidor de telefonía IP Elastix, SO CentOs 5.0
- Servidor en computador de escritorio, sistema de Radio Comunicaciones 2 Vías, SO Windows 8

La seguridad perimetral está gestiona por un firewall, donde tiene implementadas políticas de restricciones por rangos de IP, calificadas en tres niveles: gerenciales, masivos y recaudadores.

- El nivel gerencial es aplicado al gerente y sus directores, donde tiene acceso sin restricción excepto hacia las páginas consideradas como maliciosas informados por la Oficina Central.
- El nivel masivo está aplicado hacia el resto del personal, donde tienen bloqueadas las páginas con contenido de video o streaming, redes sociales, pornografía y los blacklist anteriores.
- El nivel recaudadores está aplicado hacia el personal que trabaja en las cajas de recaudación, donde se requiere el acceso sólo hacia las páginas de trabajo diario, de gestión documental, sistema financiero, correos electrónicos gratuitos y los principales medios de comunicación para estar informados.

El firewall además gestiona el acceso hacia la DMZ o NAT, controla los clientes VPN y gestiona el ancho de banda en la red LAN y WAN.

1.2. Descripción del problema

Como se había comentado anteriormente, la Oficina Central es la encargada de emitir las políticas de seguridad aplicadas en cada UN, pero solo las políticas están orientada a la capa tres del modelo OSI, descuidando la capa dos, y que una de sus subcapas es el control de

acceso al medio, es decir, el control de los equipos que acceden a la red LAN y WLAN de CNEL EP.

Debido a estos antecedentes se ha reportado en varias UN en diferentes fechas problemas de seguridad, tales como:

- No existe una política de cambio de clave para la red WLAN, la misma que se ha mantenido por más de un año sin cambio y muchas personas ajenas a CNEL EP la conocen y tiene acceso a la red corporativa sin control.
- No existe control de acceso al medio, cualquier computador o dispositivo móvil que se conecte a la red de datos, puede usar los servicios sin control de CNEL EP.
- No existe una política de seguridad para evitar la denegación de servicios, para controlar el tráfico de datos generado desde el interior de la red LAN y WLAN, lo que ha permitido que en varias UN los equipos de comunicaciones como switchs, routers y firewall fallen por saturación de memoria y procesador, provocando el bloqueo de todos los servicios, causando problema en todas las áreas administrativas y de atención al cliente por minutos e incluso horas.
- No existen herramientas especializadas para identificar los dispositivos que provoca la denegación de servicios en la red de datos. Actualmente esta tarea es manual, como desconexiones de

enlaces de datos, que afectan a varias áreas de trabajo como pisos o unos bloques de pisos. Después de aplicar este mismo procedimiento dentro de cada área de trabajo, se pudo identificar a switch de accesos y AP que se encontraban en mal estado; así como también se pudo identificar y bloquear teléfonos móviles como los causantes de estos incidentes.

- No existe un reglamento específico y detallado aplicado para la desvinculación del personal técnico que trabaja en el área de tecnología. Algunas aplicaciones y servicios dejaron de funcionar casi inmediatamente después de la separación de dicho personal. Para superar el incidente se tuvo que realizar tareas manuales, como: bloquear usuarios, cambiar claves, y revisar códigos fuentes de aplicaciones para identificar el origen del problema. (inventario de usuarios por sistemas)
- No existe un control de la seguridad de la información cada vez que se presenta un incidente.

1.3. Solución propuesta

Debido a los incidentes reportados por algunas UN, se hace necesario evaluar la red de datos, realizando varias pruebas de vulnerabilidad en una UN, descubrir los riesgos, evitar ataques, analizar los resultados, evaluar las alternativas de solución y recomendar sus implementaciones. Se detalla las políticas que se implementarán para

los siguientes ataques y/o escenarios para mitigar las amenazas y minimizar los riesgos:

- Ataque por ingeniería social.- Se pretende conseguir la clave de acceso de la red WLAN, y nombres de usuarios utilizados en el directorio activo. (concientización)
- Ataques de diccionario.- Se puede aplicar para conseguir la claves de acceso de los usuarios del directorio activo; claves de acceso a los usuarios de telefonía IP.
- Ataques por sniffer.- Se puede enviar correos electrónicos falsos, donde soliciten ingresar a servicios utilizados en la Intranet para conseguir autenticación, usuarios y claves de accesos.
- Ataques hombre en medio.- Se puede conseguir información crítica de aplicaciones realizando ataques de hombre en medio, redireccionando el tráfico de un computador a otro.
- Ataques por denegación de servicios.- Se puede utilizar aplicaciones para generar tráfico de red dentro de la red y dejar inutilizados los servicios que presta la CNEL durante un periodo de tiempo indefinido.
- Política de despido del personal.- Debido a la falta de políticas aplicado al personal despedido intempestivamente, pueden tomar represaría en contra de CNEL borrando la información contenida en

su computador, alteración de datos en base de datos, bloquear usuarios y servicios críticos que administraba.

- Políticas de control de acceso al medio, aplicado al personal de de CNEL EP y funcionarios externos.
- Políticas de acceso hacia los servidores locales, servidores en el Data e Internet.

1.4. Objetivo general

Desarrollar pruebas de vulnerabilidad de la Red de datos de una empresa pública de distribución eléctrica CNEL EP

1.5. Objetivos específicos

- Realizar test de vulnerabilidad aplicado a la infraestructura de una Unidad de Negocio de CNEL EP.
- Definir acciones correctivas que deberán implementarse como resultado de las pruebas realizada para mantener la disponibilidad y confidencialidad.
- Administrar el control de acceso al medio, para garantizar que los equipos terminales como computadoras y dispositivos móviles registrados por la corporación sean los únicos que puedan usar la red de datos de CNEL EP.

1.6. Metodología

Está basada en las fases del pentesting, donde las primeras fases son coincidentes, pero a las dos últimas son diferentes dependiendo si el consultor es cracker o ético

- Reconocimiento o footprinting.
- Exploración o escaneo y enumeración
- Obtener acceso
- Mantener el acceso
- Borrar huellas

El tipo de hacking ético es “interno”, debido que todas las pruebas se realizan desde la red interna y no desde la Internet.

La modalidad de las pruebas realizadas, de acuerdo a la cantidad de información proporcionada por CNEL EP UN Los Ríos, que es completa se denomina “white box hacking” o transparente.

1.6.1. Reconocimiento o footprinting.

Es la primera fase de ejecución y consiste en descubrir la mayor cantidad de información de CNEL EP UN Los Ríos.

Debido a la relación de dependencia con CNEL EP, la información disponible para ser analizada es total, y resulta de los años de trabajos en el área de tecnología.

Con este precedente la interacción es directa, el reconocimiento de los datos es activo, es decir, se realizará barridos de ping, conexiones a puertos de aplicativos, uso de ingeniería social, mapeos de red, etc., desde plataformas de sistemas operativos con Windows y Linux.

Debido a la cantidad de herramientas informáticas existentes en el mercado, no se las tiene disponibles por los limitados presupuestos destinados a la seguridad de la información, por lo que usaremos las siguientes:

- Footprinting con Google: Por ser el buscador más usado nos permite hacer búsquedas rápidas y acertadas, combinando operadores
- Resolviendo nombres con nslookup
- Obteniendo información de directorios Who-is
- Usando herramientas todo en uno

1.6.1.1. Footprinting con Google

Hoy por hoy existen muchos navegadores en Internet, pero Google se ha convertido en el buscador preferido y más usado, que permite combinar operadores de búsqueda y otros signos de puntuación para obtener resultados más rápidos, específicos y precisos.

Puntuación y símbolos:

- + (símbolo más) Permite incluir en su búsquedas las palabras separadas por el signo más **+CNEL EP**
- - (símbolo menos) Permite excluir en su búsqueda la palabra que se antepone al signo menos infraestructura **-edificio**
- “” (comillas dobles) Permite buscar un texto literalmente **“poema del mío cid”**
- * (asterisco) Utilizado en una posición como comodín o desconocido **quien con lobo * aunque * aprende**
- @ (arroba) Para buscar usuarios en redes sociales **@mashirafael**
- **| (pipe)** concatenar un operador con otro

Operadores de búsqueda: Son palabras que pueden ser añadidos para restringir los resultados

- site: Busca un sitio en particular en Internet **site:cnel.gob.ec**
- link: Busca páginas contenidos en un enlace en particular **link:wwwmipaginapuntocompuntoec**
- or: Busca una o varias palabras. Ejemplo **amenazas or vulnerabilidad**

- ext: Busca archivos por una extensión definida, por ejemplo **ext:avi | ext:mp3 | ext:wav**
- info: Busca información adicional de un sitio web **info: wwwmipaginapuntocompuntoec**
- intitle: Busca una palabra en el título de la página
- inurl: Busca una palabra en la URL de la página **inurl:login**

1.6.1.2. Resolviendo nombres con nslookup

Una vez conocido el sitio web, podemos saber la dirección IP a través de las consultas DNS, donde posiblemente no encontremos una sola dirección IP sino un rango IP

Este comando permite utilizar algunas opciones, como son: tipo de consulta y enumerar direcciones de dominio.

Tipo de consulta:

set type = [NS] [MX][ALL] NS servicio de nombres, MX servicio de correo y ALL todos

Enumerar direcciones de dominio

ls[-a | -d] dominio –a nombre canónicos y alias, -d todos los registros DNS

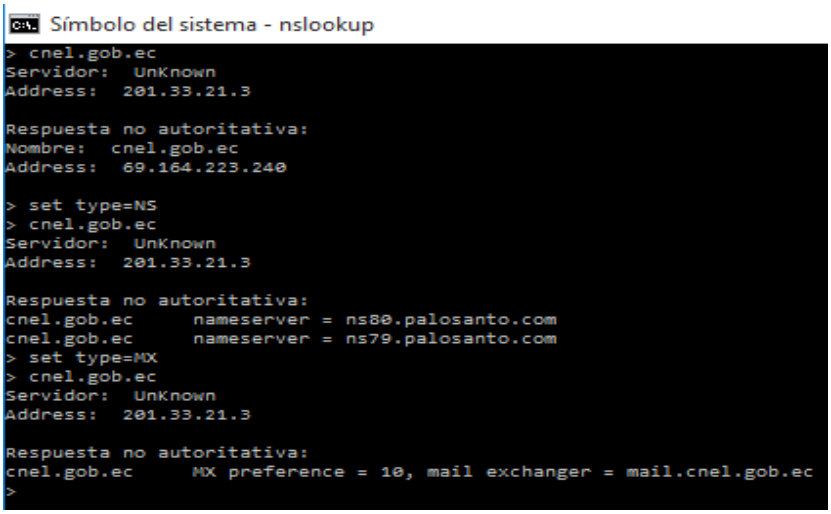


Figura 1.2: Comando nslookup en entorno CLI

En el ejemplo nos da información valiosa, como por ejemplo que el servidor con el dominio cnel.gob.ec tiene una IP versión 4 clase A; está alojado en palosanto.com y tiene un servidor de correo con el subdominio mail.cnel.gob.ec

1.6.1.3. Obteniendo de direcciones Who-is

El Who-is es un protocolo que permite realizar consultas en una base de datos que contiene información del propietario y dirección IP.

Existen algunos sitios web que llevan los registros a nivel regional, como son: AfriNIC (África), ARIN (América Anglosajona), LACNIC (Latino América), APNIC (Asia

Pacífico), RIPE NCC (Centro de Coordinación de redes Europeas), NIC (Países Ecuador, Perú, Colombia, República Dominicana, etc.

Esta información no necesita autorización y da información valiosa sobre la organización, por ejemplo consultando en la página nic.ec sobre cnel.gob.ec, nos da el resultado de la página

En la consulta aparece información real, como son: representante legal, nombre de la empresa, dirección en calles, teléfonos, contacto técnico, etc., que trabajan en la institución, que se presta para hacer ataques de ingeniería social.

Figura 1.3: Consulta who-is en la página www.nic.ec

1.6.1.4. Herramientas de reconocimiento

Hasta ahora los recursos aislados como *Google*, comandos *nslookup* y los *Who-is* permiten avanzar lentamente, pero se requiere una herramienta que permita hacer todo esto en el menor tiempo y mucho más con el objetivo de generar reportes.

Traceroute visual

Además de saber la dirección IP, es necesario saber si el servidor está administrado por la empresa o alojado en un hosting externo. Es necesario para saber si en caso de tener acceso remoto, estamos vulnerando la seguridad de un tercero.

La herramienta nos permite determinar la ubicación geográfica de los saltos del paquete, las direcciones IP, dominios hasta llegar al destino final.

Existen herramientas gratuitas y pagadas.

1.6.2. Exploración o escaneo y enumeración.

Ya en la fase previa se recabó información sobre nuestro objetivo. Si es un hacking externo tenemos identificado el rango de IP públicas y si es hacking interno, se tiene identificada los

segmentos de redes que van hacer auditadas. Se procede a identificar los “host” vivos dentro de los segmentos de red, detección de sistemas operativos, los puertos abiertos y las aplicaciones asociadas a los puertos, para su posterior análisis si los servicios detectados son susceptibles a enumeración, para saber si los host tienen vulnerabilidades potenciales de explotar.

Para ello se utilizará algunas herramientas con extremo cuidado, para evitar ser detectados y bloquear IP a través de una lista de control de acceso ACL generada por sistemas.

- Ping sweepers
- TCP ping
- NMAP
- NESSUS
- METASPLOIT

Todas estas herramientas son gratuitas y en el Internet existe mucha información disponible sobre su uso

1.6.2.1. Ping sweepers

Para identificar los host activos usamos esta herramienta que genera un barrido de ping enviando protocolo *ICMP* solicitudes de eco (*echo request*). Un inconveniente de esta herramienta es que muchos firewalls bloquean las

solicitudes de ping para ser detectados y evitar ataques de denegación de servicios distribuidos DoS basados en *echos-request*.

Se puede personalizar las pruebas de ping entre diferentes host para evitar ser detectados por los IPS

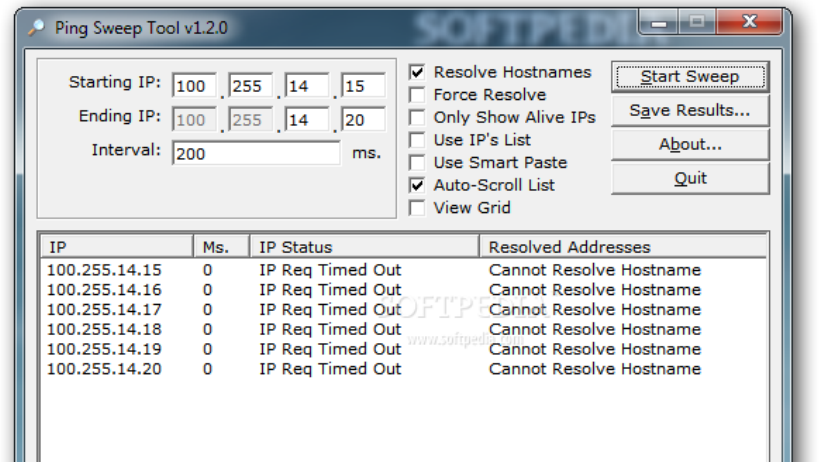


Figura 1.4: Interfaz gráfica de ping sweep

1.6.2.2. TCP ping

Si está bloqueado el ping, podemos utilizar TCP ping.

Ambas herramientas *ping sweepers* y *TCP ping* sólo realizan escaneo de host activos, pero las herramientas de escaneo de puerto detectado los puertos abiertos en cada host activo encontrado y su aplicación asociada.

Esta herramienta no utiliza el protocolo *ICMP* sino *TCP*, realiza conexiones a uno o varios puertos conocidos del

equipo remoto esperando una repuesta, si responde es porque está activo.

1.6.2.3. Estados de los puertos

Es necesario saber cuáles son los estados de los puertos para comprender mejor las herramientas mencionadas.

- Abierto.- La aplicación está disponible y escuchando.
- Cerrado.- Es lo contrario de abierto, no tiene asociado una aplicación o servicio que responda
- Filtrado.- No puede ser accesado y determinar si está abierto o cerrado porque existe un equipo intermedio – router o firewall - que filtra los paquetes.
- No – filtrado.- Es un puerto accesible, que no se puede determinar si está abierto o cerrado. Esta técnica es conocida como escaneo ACK
- Abierto | filtrado.- No se puede saber si está abierto o filtrado, porque el puerto abierto a veces no responde.
- Cerrado | filtrado.- El escáner de puertos no puede saber si está cerrado o filtrado.

1.6.2.4. Técnicas de escaneo

Basado en la técnica de TCP “apretón de mano de 3 vías” o llamado three-way handshake, utilizado para el

inicio de una conexión, tal como se describe a continuación entre el computado A y B

- **A** envía un sincronismo *SYN* a **B**
- **B** responde sincronismo + acuse de recibo *SYN+ACK*
- **A** responde con el acuse de recibo *ACK* a **B**

Escaneo SYN o Hald-Open (medio abierto)

Esta técnica se basa en hacer los dos primeros pasos sin completar la conexión, es decir, sin enviar el acuse de recibo quedando en estado embriónica.

Es obvio que si recibo un SYN + ACK, el puerto está abierto, si recibo un RST está cerrado, caso contrario está filtrado.

Esta técnica es muy buena, porque las conexiones embriónicas se mantienen en memoria, sin ser registradas en los logs, pasando desapercibidos por los administradores.

Escaneo Full o Connect-Scan

También utiliza paquetes TCP y si se completa la conexión. Posiblemente si se registre en los logs y sea detectados por los IPS

Escaneo UDP

Se envían tramas UDP a los puertos remotos esperando una repuesta. Si llega una trama UDP el puerto está abierto, si llega un *ICMP port-unreachable* está cerrado, si llega *ICMP* del tipo 3 códigos 1, 9, 10 ó 13 está filtrado.

Escaneo especiales (si RTS está abierto)

Basado en el protocolo TCP, se trabaja con los estados de las banderas de la cabecera para saber si está abierto o cerrado.

- Null scan (flags off)
- FIN scan (FIN on)
- XMas scan (FIN + URG + PSH)

Cuando un puerto está cerrado al recibir un segmento que no contenga la bandera RST responderá con un reset de acuerdo al RFC 793, en caso que no se reciba repuesta se coloca como abierto | cerrado.

Windows y otros sistemas operativos siempre devuelve un RST, para evitar falsos positivos se recomienda complementar con otra herramienta.

Escaneo ACK (si RTS no-filtrado)

Se lo utiliza para saber si existe un firewall de por medio y no para saber si un puerto está abierto o cerrado. Si se envía un ACK y recibe un RST el puerto no está filtrado, caso contrario está filtrado.

1.6.2.5. Nmap

Es quizás el software de escaneo de puertos más completo debido a su versatilidad, se pueden aplicar las técnicas descritas anteriormente. Esta herramienta de escaneo de redes permite identificar a todos los dispositivos remotos, activos, sistemas operativos, existencias de filtros, firewall.

Algunas de las características más representativas son:

- Escaneo de puertos
- Escaneo de servicios
- Escáner de vulnerabilidades
- Escaneo de redes
- Escaneo por scripts

Es una herramienta de línea de comandos donde se indica cuál será el objetivo y la sintaxis es:

nmap [tipo(s) de escaneo] [opciones]{red|host objetivo}

Opciones:

-*sn* : Búsqueda por ping

-*sS* : Búsqueda por syn/half scan

-*sT* : tcp/connect scan

-*sA* : ack scan

-*sN* : null scan

-*sU* : Búsqueda por paquetes udp

-*sF* : Búsqueda por bandera *fin*

-*sX* : Búsqueda por bandera *xmas*

-*sV* : Detecta los servicios abiertos, que versión tiene

-*O* : detección de sistema operativo

-*T<0-5>*: Es un temporizador de tiempo, donde el valor más alto es más rápido

-*v* : salida detallada

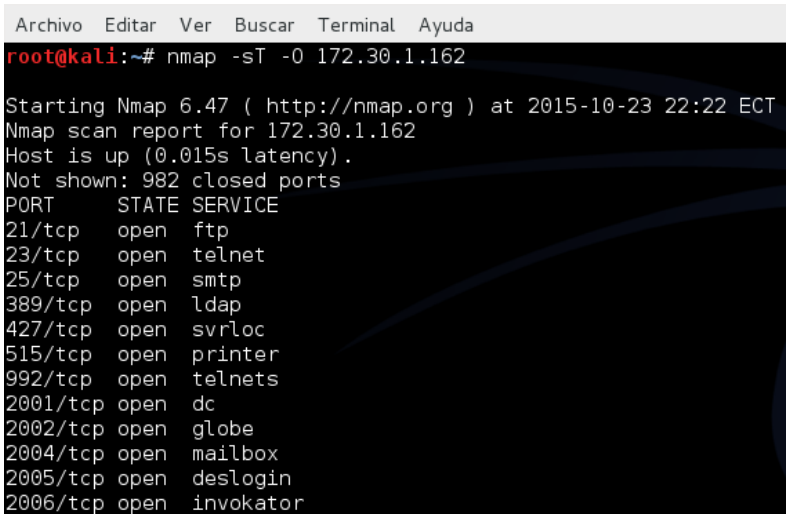


Figura 1.5: *nmap* buscando puertos y SO

1.6.2.6. Nessus

Es una herramienta que identifica las vulnerabilidades de los servicios abiertos identificados por NMAP, ejecutando plugins que verificar si la vulnerabilidad existe o no en un determinado equipo.

Esta herramienta tiene una gran base de datos de vulnerabilidades, cuenta versiones gratuitas llamada Home que permite escanear hasta 32 IPs y comerciales que no tiene límite en el números de IPs

Primero se deben de crear las políticas, que será acorde al SO y aplicaciones utilizadas.

Segundo hace el escaneo de los equipos ingresando las direcciones IP seleccionando las políticas.

Se generan las vulnerabilidades calificadas en: críticas, alto, medio, bajo e informativo.

Las vulnerabilidades son clasificadas de acuerdo al nivel de riesgo: bajo, mediano y alto.

- Riesgo Alto: Estas vulnerabilidades son críticas, que pueden ser explotadas fácilmente, pudiendo tomar el

control total del equipo o comprometer la seguridad de la empresa. Su corrección es inmediata

- Riesgo mediano: Son vulnerabilidades severas que requieren mayor grado de complejidad para ser explotadas, que no necesariamente se tendría el mismo nivel de acceso. Su corrección puede ser a corto plazo.
- Riesgo bajo: Son vulnerabilidades moderadas, que podría brindar información para su posterior ataque. No tienen un nivel urgencia alto

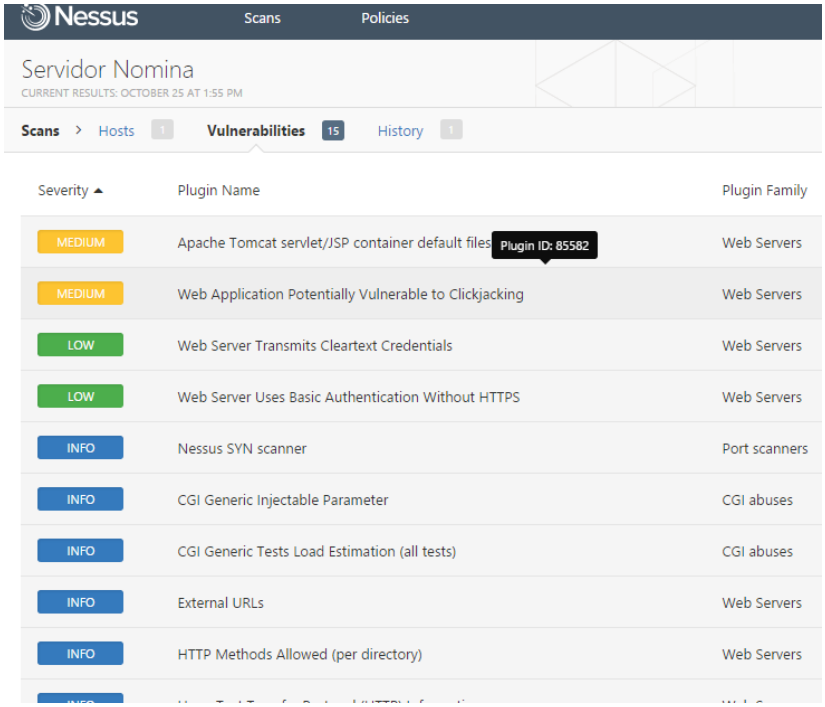


Figura 1.6: Vulnerabilidades encontradas *nessus*

1.6.2.7. Metasploit

Una vez identificados los equipos activos, sus servicios o puertos utilizados y vulnerabilidades, el paso siguiente es explotarla con la herramienta Metasploit. Pero no siempre estas vulnerabilidades se las puede explotar debido a otras medidas de control que no fueron consideradas, otra capa de seguridad o distintas variables. En caso que se pueda explotar la vulnerabilidad, podrá comprobarse y dimensionarse el daño dentro de la empresa.

Metasploit es una herramienta ideal que tiene una base de datos de exploits que pueden aprovecharse.

Tiene una interfaz gráfica y de línea de comandos donde se podrá hacer pruebas de las vulnerabilidades.

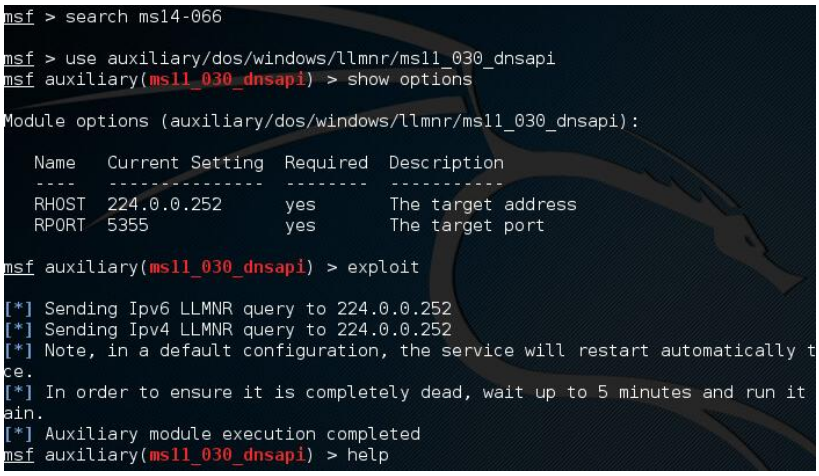


Figura 1.7: Metasploit en modo consola

1.6.2.8. Enumeración

En este punto, debemos de obtener la mayor cantidad de información que sea posible de lo que consideramos nuestro objetivo tipo, como datos de un administrador, que puede ser: nombres de usuarios, grupos, recursos compartidos, recursos de NetBios, nombre del equipo, servicios de red, etc.

A continuación se detalla los protocolos más populares para enumerar:

- Netbios
- DNS
- LDAP
- SNMP

Debido que el 85% de los SO instalados son Windows, este protocolo viene embebido por defecto, por lo que es susceptible de enumeración o explotación, según la versión del SO instalado.

Utiliza los puertos 137 TCP, 138 UDP, 139 UDP y 445 TCP.

Las sesiones nulas se las crearon inicialmente para poder compartir archivos e impresoras y autenticación entre procesos, valiéndose de una debilidad de los

protocolos SMB/CIFS usados en sistemas Windows y Linux – Samba, que permitían enumerar listas de usuarios, listas de grupos, máquinas que se encontraban conectadas y hasta SID.

Claro está que esto fue válidos para los sistemas XP y 2000. Los SO Windows 2003 no permite enumeración y Windows 7 se puede bloquear pero no cuentas de usuarios o grupos

El comando net use \\nombrePC\IPC$ “” /u:”” permite abrir conexiones nulas.

El comando net permite ver, actualizar o realizar cambios. Para visualizar dominios, grupos de trabajo, computadoras o recursos compartidos utilicemos net view [\\NombreEquipo] [/domain[:NombreDeDominio]]

Una vez establecida las conexiones nulas, obtenemos información adicional del protocolo NetBios con el comando nbtstat que recupera los nombres de los servicios.

Existen herramientas que permiten recuperar usuarios y grupos de Windows tales como sid2user y dumpuser que

trabajan en modo comando y las herramientas GetAcct, Hyena y DumpSec en forma gráfica.

1.6.3. Obtención de acceso

Una vez encontrados los dispositivos, sistema operativo, puertos abiertos, aplicaciones usadas, vulnerabilidades, enumerar los usuarios, nombres de máquinas, grupos, etc., se debe de ejecutar el ataque con herramientas de explotación tales como:

- Metasploit
- Immunity Canvas
- Core Impact Pro

Tanto Immunity Canvas como Core Impact son versiones pagadas que cuestan desde $995 y $40,000 aproximadamente, mientras que Metasploit tiene la versión gratuita y pagada; por ese motivo vamos a elegir Metasploit

1.6.3.1. Metasploit Framework

Es un proyecto de seguridad de código abierto que brinda información acerca de las vulnerabilidades y ayuda en la ejecución en el test de penetración.

El Metasploit Framework MSF desarrolla y ejecuta exploit contra un dispositivo de red, compuesto por librerías, módulos, interfaces y un sistema de archivos.

Las interfaces para la versión Framework son: msfcli, msfconsole y Artimage. En las versiones pagadas tienen interfaces Web.

Los módulos son de seis tipos: auxiliares, codificadores, explación, generadores de no operación, cargadores y post explotación:

- Auxiliares (auxiliary).- Proveen funcionalidades para ejecutar tareas en un equipo remoto.
- Codificadores (encoders).- Encargado de cargar y descargar los payloads que se ejecutan en un exploits.
- Explotación (exploits).- Explota un vulnerabilidad, que a diferencia de los auxiliares utilizan una cargar
- Generadores de no-operación (nops).- Se utilizan para garantizar la correcta cargar de los payloads detro del MSF
- Cargas (payloads).- Son programas que se cargan al host remoto después de haber ejecutado exitosamente un exploit.

- Post explotación (post).- Se usan para ganar mayor acceso.

Puede correr bajo las plataformas Linux (embebido en Kali Linux) y Microsoft. El comando msfconsole permite cargar

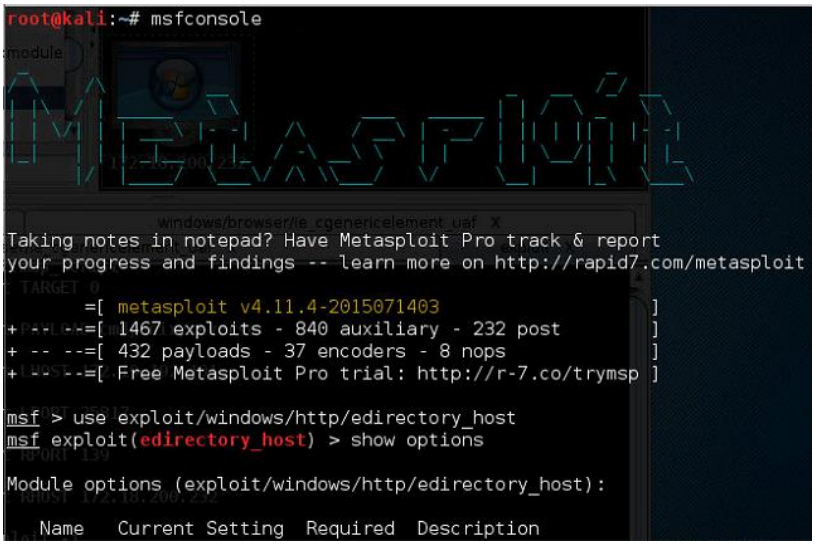


Figura 1.8: Entorno del comando msfconsole

Dentro de los comandos más usados están: search, use, info, set, run y exploits

- search: Utilizado para hacer búsquedas que pueden ser por nombre o ruta del término indicado, por códigos cve, osvbd, bid
- use: Utilizado para escoger un módulo ingresando la ruta completa, por ejemplo para cargar una

vulnerabilidad en Windows XP utilice: use windows/smb/ms08_067_netapi

- info: Proporciona información del módulo cargado
- set: Permite ingresar información adicional para ejecutar el módulo cargado. Nos podemos ayudar del comando show options que nos dice los parámetros que deben ser ingresados con el comando set. Por ejemplo para ingresar la IP remota del Windows XP que se desea hackear ingresamos el comando set RHOST seguido de la IP
- run o exploits: Comandos utilizados para ejecutar un auxiliar o un exploit respectivamente

1.6.3.2. Ataques de claves mediante sniffer

La forma tradicional para ingresar a un sistema consiste a través de las credenciales. Pero ello realizaremos el ataque a las credenciales mediante el método de sniffer.

El sniffer o husmeador es un software que le permite capturar todos los paquetes de red LAN o WLAN, colocando la tarjeta de red en modo “promiscuo”.

La captura de paquetes se la puede hacer en una topología tipo bus, implementada en un HUB o una red wireless, usando los dos métodos:

- Inundando el switch (mac flooding).- Si se envía paquetes tras paquetes al switch que se vea obligado a: borrar todas su tabla MAC comportándose como HUB o simplemente no soporte el ataque y se produzca una denegación de servicio.
- Engaño a los dispositivos finales (ataque hombre en el medio).- Debido a la debilidad del protocolo ARP (Adress Resolution Protocol) que permite buscar en una tabla la direccione MAC una dirección IP, es posible suplantar las tramas Ethernet que tienen en sus cabeceras direcciones MAC origen y destino, y no direcciones IP. Así se envían paquetes ARP request como broadcase para conseguir paquetes ARP reply

Mediante estos mecanismos se puede capturar hashes de Windows (credenciales codificadas), usuario o clave de aplicaciones Web que estén en texto planos. Lógicamente estos paquetes de red deben ser analizados con otro programa complementarios.

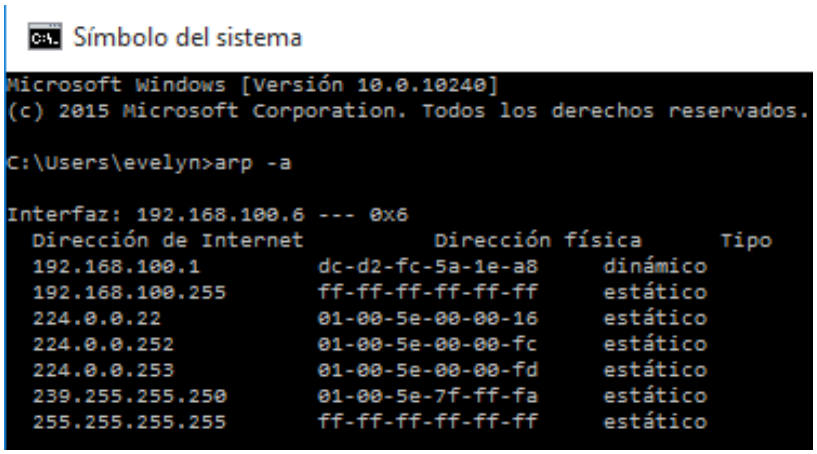


Figura 1.9: Tabla APR en un computador Windows

Existen dos programas open source muy buenos, el uno es WireShark para análisis de paquetes de red, generar estadísticas y el otro para Etthercat para realizar ataques hombre en el medio.

Wireshark

Es un analizador de protocolos, que tiene la funcionalidad de tcdump pero en modo gráfico con muchas opciones de filtrado y organización. Actualmente se lo utiliza para reconstruir sesiones, solucionar problemas de redes.

Además es un software libre, se ejecuta sobre plataformas Windows, Unix y compatibles Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Android y Mac OSX

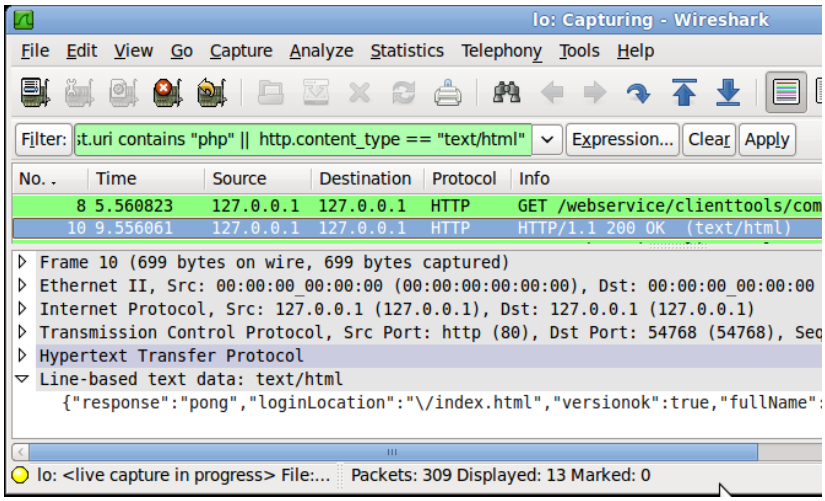


Figura 1.10: WireShark captura de paquetes

1.6.4. Mantener el acceso

Después de haber conseguido el acceso al sistema, evitará ser detectado por el personal de informática, por lo que usará recursos propios y los recursos de sistemas, para mantenerse con un perfil bajo, explorar el sistema atacado que será usado como plataforma o equipo para lanzar desde ese sitio nuevos ataques informáticos para escanear y explotar a otros sistemas informáticos que pretende atacar. En esta fase se quiere mantener indetectable, invisible, procede a eliminar cualquier evidencia de su penetración y hace uso de técnicas como:

- Puertas traseras para facilitar el acceso
- Troyanos para obtener o transferir información
- Rookit para obtener acceso al sistema operativo

- Keyloggers (capturar pulsaciones del teclado), botnets, etc.

Puertas traseras NetCat

Es una herramienta que permite mantener abrir un puerto TCP/UDP en el HOST quedando a la escucha, para que mantenga comunicación desde un equipo remoto ligado a otro puerto UDP/TCP. A continuación se lista los parámetros más usados con nc:

-l: abre puerto para ser escuchado

-p: puerto de escucha

-k: mantiene el puerto abierto después de haber recibido una conexión

-u: abre un puerto UDP en vez de TCP utilizado por defecto

-v: detalla información por de la conexión

-t: compatible con sesiones telnet

Ejemplo, se ejecuta en el host de la víctima el comando para escuchar por el puerto 80 y desde el remoto escuchar por el puerto 25

nc ip_attaker 80 | *cmd.exe* | *nc ip_attaker 25*

1.6.5. Borrar huellas

El atacante no quiere ser detectado, borra el rastro de su actividad ilícita por dos razones, para mantener el acceso y para evitar ser detectado.

También utilizará técnicas para no ser detectados, utilizada herramienta como la esteganografía y el tunneling.

- Esteganografía: Utiliza archivos multimedia como imágenes, videos y audios para camuflar o esconder archivos en formatos TXT, EXE, etc.
- Tunneling: Permite encapsular un protocolo de red sobre otro. Las VPN son ejemplos de túneles.

CAPÍTULO 2

MARCO TEÓRICO

2.1. Diagrama de red de datos corporativo.

Cada Unidad de Negocio de CNEL EP tiene implementado el mismo esquema de red WAN y LAN hasta la configuración del switch de core.

La red WAN está formada por dos firewall en modo activo – pasivo. La red LAN está formada por un switch CORE donde se conectan los switches de acceso y access points de los usuarios finales.

La red WAN de CNEL EP está implementada por dos proveedores de servicio público ISP en modo activo – pasivo. El proveedor activo es CNT, brinda el servicio de Internet y además el de datos que permite la comunicación desde la oficina principal en cada UN hacia sus agencias

y a las otras UN de CNEL EP incluido el Data Center. El segundo proveedor pasivo es TELCONET, que sólo brinda el servicio de datos que permite la comunicación desde la oficina principal de cada UN hasta sólo el Data Center.

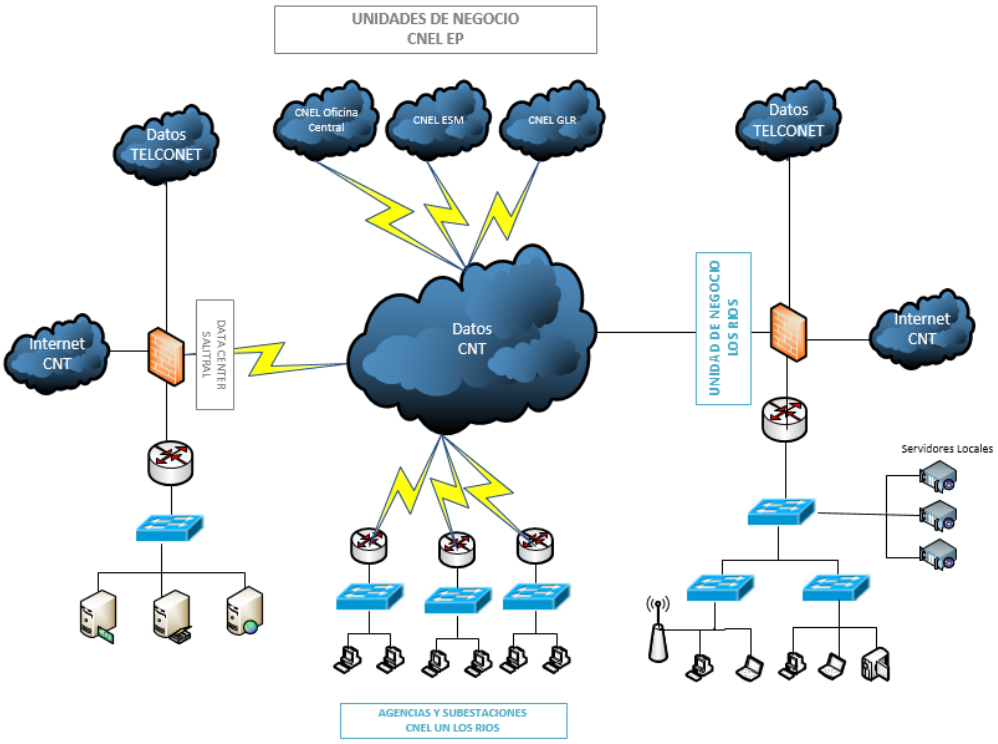


Figura 2.1: Diagrama de red de CNEL EP UN Los Ríos

2.2. Características técnicas de los equipos de comunicaciones.

La infraestructura de red en cada UN de CNEL EP está implementada principalmente por equipos de la marca Huawei, como adquisición resultó de un concurso en una licitación realizada en el 2012 para adquirir equipamiento de infraestructura de red corporativa como son: router, firewall, switch de core, switch de accesos y access point. Cabe

mencionar que existen equipos de red otra marca que no han sido homologadas, la misma que no será motivo de análisis en esta tesis. Estos equipos están clasificados según su categoría:

- Router implementado con un equipo UTM
- Switch de CORE
- Switch de acceso
- Access Point modelo

2.2.1. Router

Tabla 1: Características técnicas del router

Característica Técnica	**Descripción**
Modo de trabajo	Router, Transparente, Compuesto
Interconexión de red	Soporta dot1q VLAN
	Soporta enrutamiento estático
	Soporta enrutamiento dinámico RIP, OSPF, BGP
	Balanceo de carga
Mantenimiento y disponibilidad	VRRP (virtual router redundancy protocol)
	VGMP (virtual group management protocol)
	HRP (Huawei redundancy protocol)
SNMP	v1, v2c, v3

2.2.2. Switch CORE

Tabla 2: Características técnicas del switch de CORE

Características Técnicas	**Descripción**
Puertos	24GE TX + 4 GE Combo + 2x10GE
Capacidad	88Gbps
Forwarding	65.47 Mpps

VLAN's	4096
	Soporta interfaces basado en VLANs, MAC, IP, protocolo, políticas, QinQ y voz
MAC	Tabla 32K
	Desactivación aprendizaje basado de MAC en VLAN
	Soporta TRUNK, LACP y múltiples tipos de balanceo
Router unicast IPv4	Statics router
	Dynamic router protocol: RIP, OSPFv2, ISIS, BGP
QoS	Soporta clasificador de tráfico
	Soporta política de tráfico
	Soporta organizador de tráfico
	Soporta PQ, WRR, DWRR
	Soporta 256k ACL
Características de seguridad	Dispositivo de seguridad 802.x
	Detección dinámica ARP
	Guarda la IP origen
	Envenenamiento de MAC
	Puerto aislado
	Espiar DHCP
	Reenvío forzado de MAC

2.2.3. Switch Acceso

Utilizado en las agencias y subestaciones.

Tabla 3: Características técnicas del switch de acceso

Características Técnicas	**Descripción**
Puertos	48 FE + 4GE FX
Capacidad	17.6Gbps
Forwarding	13.1 Mpps
VLAN's	4096
MAC	8k
	Soporta interfaces basado en VLANs, MAC, IP
Router unicast IPv4	Statics router
QoS	Soporta clasificador de tráfico

	Clasificación basado en MAC
Características de seguridad	Detección dinámica ARP
	Guarda la IP origen
	Envenenamiento de MAC
	Puerto aislado

2.3. Servicio de autenticación de usuarios

La autenticación de acuerdo a varias definiciones es un proceso por el que una entidad, denominada como un usuario o computador, prueba su identidad ante otra que puede ser un servidor de aplicaciones.

Existen tres categorías para la verificación de los métodos de verificación:

- Sistemas basado en lo que usted conoce: una clave
- Sistemas basado en lo que usted tiene: una tarjeta, un token, smartcard (certificados digitales), coordendas, etc.
- Sistemas basado en lo que usted es: una huella, la retina del ojo, facial, etc.
- Una combinación de los anteriores.

Las computadoras utilizadas por los usuarios finales de CNEL EP utilizan como sistema operativo Microsoft Windows, quien de manera nativa sólo soporta dos tipos de autenticación: claves y smartcards, actualmente sólo se utiliza claves.

Hay un servidor de directorio activo alojado en el Data Center que sirve para autenticar las claves de los usuarios, implementado principalmente para validar el ingreso de las sesiones de inicio de Windows en cada computador, y escasamente vinculado a varias aplicaciones corporativas.

Todas las aplicaciones desarrolladas y adquiridas por CNEL EP utilizan un solo método de autenticación, que es basado en lo que usted conoce, la clave. Excepto el software de gestión documental implementado por la Vice Presidencia de la República, utiliza el sistema de autenticación basado en lo usted tiene, un token, que sólo está dirigido el uso a los directores gerentes de las UN.

La mayoría de los aplicativos utilizados por las diferentes UN no están integrados al directorio activo corporativo, siendo los más vulnerables los aplicativos web por transmitir sus credenciales en texto plano.

Los aplicativos web utilizados en todas las UN en orden de uso son los siguientes:

- Sistema de Nómina
- Sistema Financiero
- Sistema de Reclamos Comerciales
- Sistema de seguimiento de auditoria interna.
- Sistema de localización de nuevos servicios comerciales

Estas aplicaciones guardan las credenciales en sus bases de datos, sin ningún control o estandarización de su validación, donde lo más probable que las credenciales viajen directamente a través de la red en texto plano, vulnerables a su captura.

Estos sistemas mencionados anteriormente serán analizados posteriormente para su análisis y descubrir las debilidades, como explotar sus vulnerabilidades y una propuesta de solución.

2.4. Servicio de autenticación del control acceso al medio

Con la finalidad de mejorar la seguridad de la información, se requiere que las computadoras de los empleados de CNEL EP sean los únicos que puedan utilizar los servicios de red dentro de la Unidad de Negocio, caso contrario se les negará el acceso a cualquier recurso de la red.

La mejor forma para controlar el acceso a la red es validando la dirección MAC de cada dispositivo a la red implementada a través de los switch de acceso.

Los switch de acceso tienen características de seguridad, que permite autenticar la dirección MAC en forma local o remota. Debido que la cantidad de computadores que existen en cada UN es variables desde varios cientos hasta miles, no es práctico mantener el registro de cada dirección MAC en todos los switch de acceso de cada una de las UN,

sino que lo más práctico es almacenarlo en una base de datos, para después posteriormente consultarlo remotamente y en caso de existir la MAC consultada, permitir autenticar el equipo, caso contrario negarle el acceso. Este proceso de autenticación si existe y fue definido por la IEEE en junio del 2001, denominado el protocolo de autenticación 802.1x

Claro está que el control de autenticación deberá de realizarse en la subcapa 2 del modelo OSI llamada control de acceso al medio MAC, el protocolo de autenticación IEEE 802.1X, que fue diseñado originalmente para redes cableadas, posee mecanismos de autenticación, distribución y autorización de credenciales o claves, también añade controles de acceso para todos los usuarios que deseen consumir los recursos de la red. La arquitectura está compuesta por tres entidades funcionales:

- El solicitante que se une a la red
- El autenticador - por lo general es un switch localizado en medio del solicitante y el servidor de autenticación- hace el control de acceso.
- El servidor de autenticación quien ejecuta la validación del solicitante y procede a realizar la autorización.

El IEEE 802.1x está basado en el Protocolo Autenticación Extensible (EAP), que se usa para transportar la información de identificación del usuario.

El EAP se basa en un controlador de acceso (switch o Access Point) llamado autenticador, que permite o niega el acceso de red al solicitante, proveniente de un servidor de autenticación.

El servidor de autenticación Servidor de Acceso a la Red (NAS) generalmente llamado RADIUS está definido como el que aprueba la identidad de los usuarios y aprueba el acceso de acuerdo a sus credenciales.

Voy a explicar de una fácil el funcionamiento del IESS 802.1x, incluyendo alias las tres entidades funcionales: solicitante=*PC*, controlador de acceso=*SW* y servidor de autenticación=*RADIUS*.

- Cuando el *PC* desea conectarse a la red, el *SW* recibe la petición y envía una solicitud de autenticación.
- El *PC* envía una repuesta al *SW,* quien lo enruta al *RADIUS.*
- El *RADIUS* envía un "challenge" al *SW,* quien lo transmite al *PC*
- El *challenge* es un método para establecer la identificación.
- El *PC* responde al challenge.
- Si la identidad es correcta, entonces el *RADIUS* envía la aprobación al *SW*, quien tiene acceso a la red o parte de ella.
- Si la identidad no es correcta, entonces el RADIUS envía la negación al SW, y niega al PC el acceso a la red

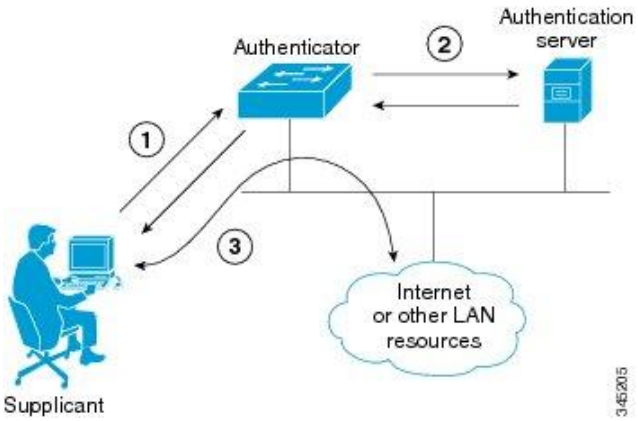


Figura 2.2: Esquema de trabajo del 802.1X

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

3.1. Zonas de seguridad perimetral.

La seguridad perimetral lo realiza el firewall Huawei en un esquema de alta disponibilidad, donde utilizan una puerta de enlace redundante a través del protocolo Virtual Router Redundancia Protocolo (VRRP)

Tabla 4: Características técnicas del firewall

Característica técnica	**Valor**
Control de política	Loose control policy
	Strict control policy
Clasificación de tecnología	Packet filter firewall: ACL, Blacklist, ASPF
	Proxy firewall
	State Inspection Firewall
NAT	NAT, NAT server
Defensa de Ataques	DoS attacks: syn flood, icmp flood, udp botnet, cc attack botnet
	Scanning

	Spoofing
Firewall virtual	
VPN	Protocolo IPSec

El firewall controla todo el tráfico de datos que circula en la UN, desde el generado en la oficina principal dirigido hacia las agencias, subestaciones y otras UN hasta el solicitado y devuelto por el Internet. También controla el ancho de banda y se protege contra los ataques más comunes en nuestro medio.

La administración de la seguridad está aplicada por IP o rango de dirección IP, que pueden contener filtrado: IPS, antivirus, web, mail, ftp y de aplicaciones.

Estas direcciones IP están asociadas a una zonas en el firewall, que a su vez corresponde a las interfaces de donde se origina el tráfico de red.

Cada zona tiene un nombre con un número que calificada el nivel de seguridad, donde el número 1 representa a la zona más insegura y 100 a la zona más segura.

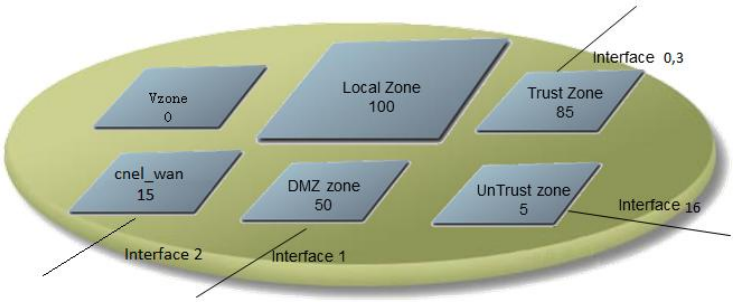


Figura 3.1: Zonas definidas en el firewall

Las zonas definidas en CNEL EP, son las siguientes:

- Zona local o el mismo firewall, tiene la máxima seguridad, con el número 100
- La red LAN o zona trust tiene asignada el nivel de seguridad 85, y es tráfico que circula por las interfaces 0 y 16
- La red DMZ con el nivel de seguridad 50 no está defina en esta red
- La red WAN llamada cnel_wan es la Intranet, tiene asignada un nivel de seguridad 15, circula el tráfico de las agencias, subestaciones y otras UN.
- La red de Internet o zona unTrust tiene un nivel de seguridad 5

Debido al flujo de datos que existen entre las zonas trust y untrust, donde se evidencia una traducción de IP privada a pública y viceversa, ya sea producto de la navegación desde la red de LAN, por publicar un servicio al Internet o simplemente por ingresar por una conexión VPN, donde se aplica nateo, el servicio de NAT está habilitado.

El tráfico de datos es controla con políticas de seguridad de entradas o salidas entre dos zonas, definida con el nombre de la zona más segura seguida la zona menos segura, aplicado a una IP o segmento de red, donde se permite o bloquea el tráfico, con opciones de filtrado: IPS, antivirus, dirección WEB, correo o aplicaciones.

La Oficina Central gestiona las políticas corporativas que deberán aplicarse en todas las UN, siendo la Gerencia de Seguridad de la Información GSI quien define grupos de listas de sitios web calificados como: spam, video streaming, sitios inseguros, pornografía, redes sociales, entidades financieras, noticias, medios de comunicación, entidades oficiales, servidores de correos públicos, permitidas, bloqueadas, permitidas, banco, deportes, gobierno, varios, cultura, hacker, etc.

La idea es calificar a estos listados como listas blancas o negras según sea el usuario que lo utilice, calificado como uno de los tres perfiles creados:

- Perfil gerencia: Tiene todas las páginas y servicios desbloqueados, exceptuando la lista de sitios definidos en el listado hacker.
- Perfil masivo: Tiene más restricciones que el perfil gerencia, se califica como listas negras a las definidas como listas de: redes sociales, video streaming, pornografía, antivirus virus, bloqueadas, spam y youtube.
- Perfil recaudador: Bloqueado lo anterior y sólo puede ingresar a las páginas definidas en las listas: permitidas, banco, deportes, gobierno, varios, cultura, ti,

En la figura siguiente se detalla el esquema de red definido por la Oficina Central que es aplicado a todas las UN, donde está el firewall está configurado en alta disponibilidad implementado con el protocolo VRRP, quien comunica con los dos proveedores de datos ISP y el switch de CORE, además administra la conexión de Internet.

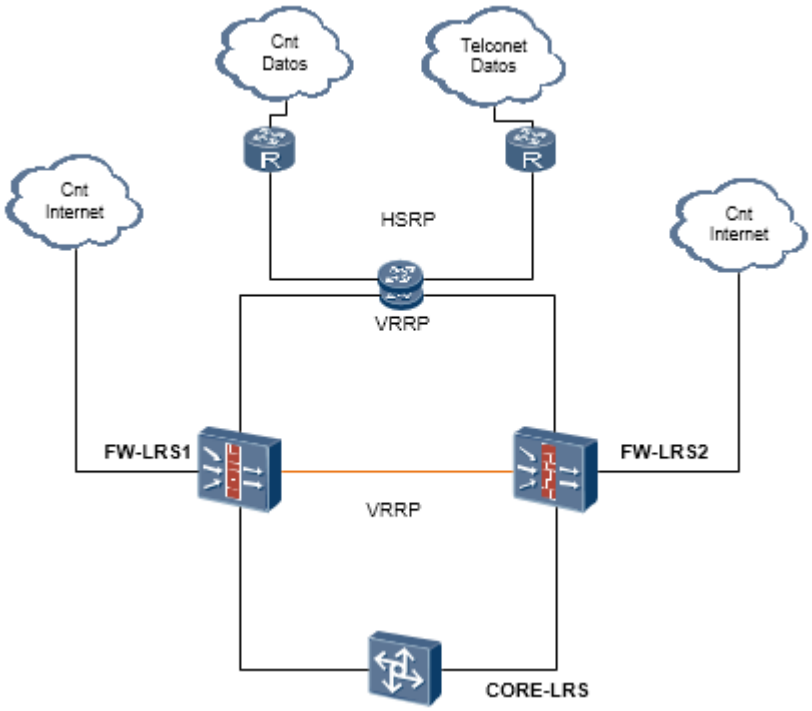


Figura 3.2: Firewall en alta disponibilidad con IP virtual protocolo VRRP

Este esquema de red tiene un pequeño error en su implementación, todas las conexiones que provienen desde los ISP llegan al switch de CORE y no al firewall, como debería ser. Se explica brevemente estos errores.

- La conexión de datos provenientes de CNT llega al switch de CORE para conectarse al firewall. Ambos puertos sin configuración de VLAN's.
- La conexión de datos proveniente de TELCONET llega al switch de CORE para conectarse al firewall. Ambos puertos sin configuración de VLAN's.
- La conexión de Internet proveniente de CNT llega al switch de CORE VLAN's 501 para conectarse al firewall VLAN's 501

El firewall tiene opciones de protección de seguridad integradas tal como se muestra en la figura 3.3, que actualmente no se encuentran activadas, donde existen cuatro grupos:

- Defensa de Ataque
- BlackList Lista negra de direcciones IPv4 que serán bloqueadas
- WhileList: Lista blanca
- IP-MAC Binding: Cuando se necesita asociar una dirección MAC con una IP

Defensa de Ataques

Previene ataques procesando paquetes de datos, generando una alerta o bloquearlos. La defensa de ataques evita las clásicas inundaciones clasificados por su tipo de tráfico y de aplicaciones; además controla el

procedimiento de scanner de puertos, malformaciones de paquetes y control especial de paquetes.

El tipo tráfico, se pueden evitar: syn flood, udp flood, icmp flood, arp flood. A nivel de aplicaciones puede proteger ataques dirigidos a: sip flood, http flood, connection flood.

Figura 3.3: Protección de seguridad embebida en el firewall

3.2. Política de calidad de servicio

La Oficina Central no ha generado políticas de Calidad de Servicio QoS, pero indirectamente cada UN ha implementado este servicio con CNT.

La calidad de servicio se define como el rendimiento promedio de una red de datos, que permite a las aplicaciones, usuarios, o de garantizar

un cierto nivel de rendimiento para un flujo de datos con diferentes prioridades.

La QoS hace referencia a la Clase de Servicio (CoS) como al Tipo de Servicio (ToS), cuyo objetivo es conseguir el ancho de banda y latencia necesaria para una determinada aplicación.

Actualmente a través del proyecto de video vigilancia se han instalado cámaras de seguridad en las oficinas de los edificios principales, agencias y subestaciones de cada UN de CNEL EP.

El tráfico generado por las cámaras de video vigilancia es transmitido a través de los enlaces de datos, para finalmente quedar almacenado en los servidores locales de cada UN. Por lo que es necesario garantizar un ancho de banda mínimo para datos generado por la gestión administrativa de las agencias y subestaciones y del ancho de banda, destinarlo para transmitir video de las cámaras de video vigilancia.

La QoS está implementada por CNT, quien configura sus equipos la distribución del ancho de banda en la siguiente proporción:

- Se garantiza el 40% del CIR[1] para datos con salida por la Vlan's 1
- Se garantiza el 60% del CIR para video con salida por la Vlan's 90

[1] Wikipedia, "Commited Information Rate", https://es.wikipedia.org/wiki/Frame_Relay

Los switch de acceso de CNEL EP se configura los puertos VLAN's para las cámaras y los computadores. Además se configura el puerto TRUNK entre los switch de CNEL y CNT.

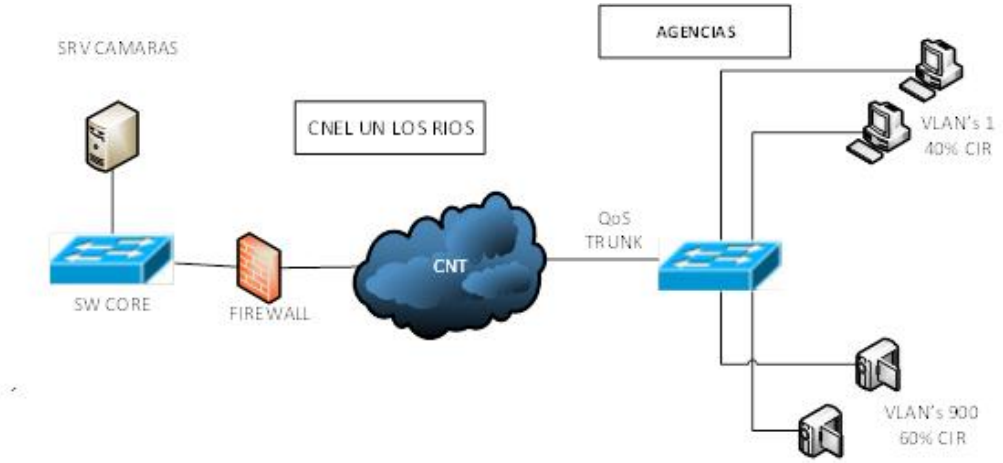


Figura 3.4: Qos aplicados por CNT en Agencias y Subestaciones

3.3. Política de control de acceso.

Actualmente existe una política de control de acceso definida en el "*Manual de políticas de seguridad de la información*" redactada por la Gerencia de Seguridad de Información, aprobada y publicada el 27 de julio 2015. En este manual se ha definido la "*Política para control y gestión de accesos: autenticación y manejo de contraseñas*", que está orientado autenticar el acceso a los sistemas de información, pero no abarca la autenticación de los dispositivos finales conectados a la infraestructura de red de CNEL EP.

A continuación se hace una breve descripción de esta política agrupada en:

- Principios de Control.- El acceso a los Sistemas de Información requerirá siempre de autenticación, basado en algo conocido (usuario y clave), sin utilizar token o certificados digitales.
- Gestión de Identificadores.- Los usuarios creados son normalizados, autorizados, individuales no grupales, auditables y responsables de todas las actividades. Se descartan usuarios anónimos
- Gestión de contraseñas.- Son responsables de accesos a servicios y de los accesos que se produzcan, no serán visibles, almacenadas, recordadas o enviar por correo.
- Recomendaciones para uso de contraseñas.- Se definen parámetros como: periodos máximos de rotación, caducidad, reutilización, longitud mínima, complejidad y semántica.
- Responsabilidad de contraseña.- El acceso y uso de los sistemas de información, base de datos y procesos de negocio, está sujeto a normas legales y reglamentarias. La información no podrá comercializar
- Gestión de inicio de sesión.- Los errores de la validación de entrada no debe evidenciar la información errónea. Se define límites de intentos fallidos, tiempos de espera y se recomienda cifrar en cuanto sea posible la autenticación.

- Auditoría de control.- Revisión de los derechos de accesos asignados, derechos de accesos privilegiados, permisos de accesos a usuarios que hubiese sufrido modificación en su responsabilidad.

Debido a la falta de autenticación de los dispositivos finales conectados a la infraestructura de red, algunos administradores han tomado algunas iniciativas para mitigar la inseguridad de las siguientes formas:

- En algunas UN como en Milagro, Los Ríos y Guayas – Los Ríos existe restricciones en la asignación de la dirección IP por el servidor DHCP, asignando la IP previo a la reserva manual de la dirección MAC, pero eso no impide que un atacante pueda conectarse a la red ingresando manualmente la dirección IP.
- Los switch de accesos no tienen activada la funcionalidad de *puerto seguro* o su equivalencia, que evita que cualquier computadora pueda conectarse a cualquier puerto de red de cualquier switch.
- Los switch de acceso no controla los posibles ataques generados por el protocolo ARP.

3.4. Política del uso de Internet

No existe un polítca de uso de Internet vigente, pero en el *Manual de políticas de seguridad de la información,* generado por la Gerencia de Seguridad de Información en su 4ta versión, que se encuentra en fase de aprobación por la Gerencia General para su posterior publicación en

la Intranet corporativa y ejecución inmediata, en el capítulo 16 se ha definido la *Política para el uso de Internet*, que en su parte pertinente dice lo siguiente:

3.4.1. Uso de Internet

Al conectarse a Internet, el equipo asignado al usuario y por consiguiente la red puede exponerse a algún ataque de los denominados hackers o de los virus que pueden descargarse junto con los archivos o programas que se bajan de Internet. Aun cuando se han implementado herramientas de seguridad que intentan minimizar estos riesgos, se debe evitar convertirse en un punto vulnerable para la red Corporativa e informar al personal de soporte en los casos que se detecten comportamientos extraños. Evite conectarse a sitios indebidos que no son de trabajo

El Internet es asignado de acuerdo a perfiles de acceso definidos y asignados por la Gerencia de Tecnología de la Información

3.4.2. Perfiles de navegación.

- Perfil 1: Acceso de Internet sin restricciones, con excepciones de bloqueo de categorías como pornografía, violencia y listas negras. Aplicado a Gerente General,

Gerentes Corporativos, Asesores de Gerencia, Coordinadores, Directores, personal de Marketing y Comunicación.

- Perfil 2: Acceso de Internet igual que perfil 1, pero bloqueado las categorías: deportes, militar, redes sociales, lotería, recreación, religión, sexual, inmobiliario y del hogar, trabajo, viajes, moda, enfoque social, humanidad, transporte&vehículos, stream&media, vida, compras, finanzas, comida-alcohol y tabaco, clubes&sociedades, vulgar, juegos de azar, drogas ilegales, sitios web código maliciosos, crimen, arma, fraude, aborto, suicidio, incitación al odio, culto. Pertenecen a éste grupo: Usuarios en general de las diferentes áreas de la Corporación que ingresan a la red corporativa.
- Perfil 3: Los usuarios tienen acceso únicamente a páginas gubernamentales, bancos, páginas de noticias. Pertenecen a éste grupo: Personal del Contact Center y áreas de Recaudación de las Unidades de Negocio de la Corporación.
- Perfil 4: Usuarios con requerimientos especiales. Se analizará cada caso de acuerdo al requerimiento

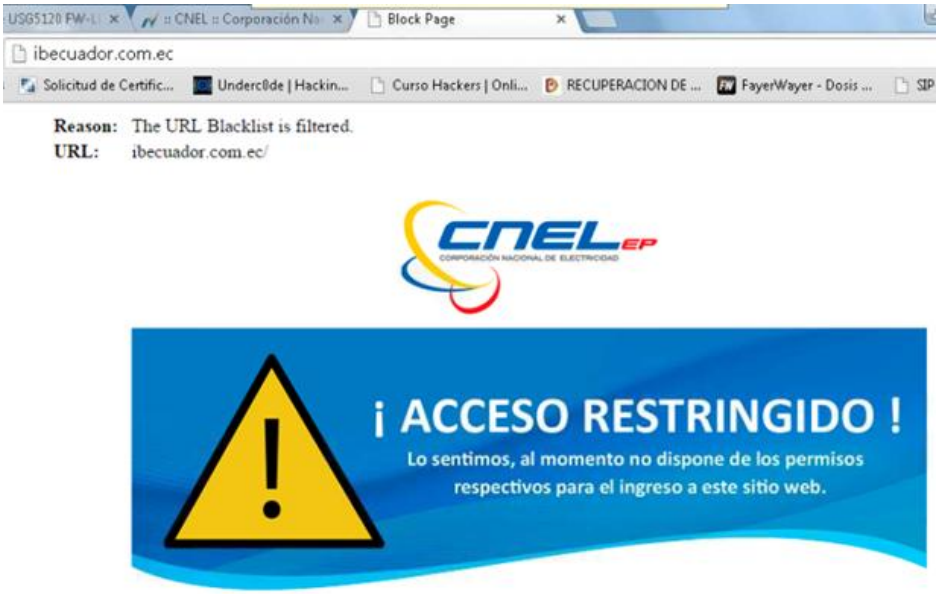


Figura 3.5: Mensaje de página bloqueada por el firewall

3.4.3. Consideraciones Generales

- En horas laborables, está permitido acceder a Internet solo cuando sea estrictamente necesario y por requerimiento de información para sus funciones dentro de CNEL EP. Si necesita realizar una investigación o bajar información de interés particular, se lo podría hacer siempre y cuando no sea en horas laborables, es decir a partir de las 17h30 y solo si se encuentra autorizado.

- Todos los accesos a Internet, serán solicitados por los canales de acceso provistos por la Corporación, en caso de necesitar una conexión a Internet con condiciones especiales o alterna, ésta debe ser notificada por el

Gerente o Director del Área y aprobada por la Gerencia de Seguridad de la Información.

- Todos los sitios y descargas serán susceptibles de supervisión y/o bloqueo por parte de la Corporación si se consideran perjudiciales y/o improductivos para el negocio.
- Toda la información redactada, transmitida y/o recibida haciendo uso de los sistemas informáticos propiedad de CNEL EP y/o del servicio de Internet corporativo se considerarán, de pendiendo del caso, como información interna o confidencial de la corporación y se reconocen como parte de sus datos oficiales. Por lo tanto, de ser requerido, podrá revelarse únicamente por exigencias legales a terceros autorizados.
- El equipamiento, los servicios y la tecnología utilizados para acceder a Internet pertenecen a CNEL EP y la empresa podrá supervisar el tráfico (metadata) generado mediante las conexiones hacia Internet.

3.4.4. Prohibiciones

- Acceder a Internet para asuntos personales, actividades políticas, negocios privados, o simplemente para cualquier

otra actividad que no esté relacionada con las funciones relativas a su cargo y no se encuentren autorizadas.

- Publicar o difundir información confidencial de los Sistemas de CNEL EP a través de Internet.
- El envío o la publicación de información difamatoria sobre la Corporación, sus productos o servicios, trabajadores y/o clientes
- La introducción de software malicioso en la red de la empresa y/o la realización de actividades que pongan en peligro la seguridad de los sistemas de comunicación electrónica de la empresa
- Utilizar Internet para visitar sitios o descargar texto, imágenes, videos que contengan material pornográfico, racista o político o promueva la violencia, odio o cualquier actividad ilegal.
- No se permitirá el acceso a redes sociales, ni chat en ningún horario de trabajo a menos que el usuario esté autorizado.
- Instalación y uso de programas de tipo *peer-to-peer* para el intercambio de archivos en Internet
- Descargar cualquier tipo de programas o software de Internet e instalarlos en las computadoras de CNEL EP sin previa autorización.

- Acceso a sitios reconocidos como inseguros, los cuales se ponga en riesgo los principales valores de la información como son la integridad y confidencialidad.
- El uso de los ordenadores para cometer cualquier tipo de fraude como descargar, copiar y/o distribuir de forma ilegal material con derechos de autor (música, películas, libros, programas, etc.).
- El robo, el uso o la revelación de las contraseñas de otra persona sin la autorización previa.
- No está permitido el uso de programas que bloqueen o eviten las restricciones de seguridad para Internet establecidas en la Corporación.
- No está permitido acceder vía Internet a emisoras de radio ni de televisión (TV) por motivos recreacionales.
- La presentación de opiniones personales sin autorización en sitios web como si representaran a la corporación.

3.5. Política desvinculación de personal.

Se ha buscado en la Intranet corporativa, toda la documentación relacionada a la *desvinculación de personal*, y sobre el procedimiento que debe ejecutar tecnología con la información y usuarios creados del personal desvinculado. Pero la Gerencia de Desarrollo Corporativo

(GDC), en sus documentos publicados no incluye ningún procedimiento en los documentos como son:

- Reglamento de retiro voluntario, aprobado 27 de marzo del 2015
- Normas Internas de la Administración del talento humano, aprobado el 2 de mayo del 2014
- Procedimiento de desvinculación, aprobado el 29 de diciembre 2011

La Gerencia de Tecnología de la Información, generó el siguiente procedimiento:

- Procedimiento para la gestión de los bienes informáticos, aprobado el 5 de mayo del 2015

La Gerencia de la Seguridad de la Información, generó los siguientes documentos:

- Procedimiento de control y gestión de usuarios: altas, bajas, manejo de privilegios, aprobado el 3 de septiembre del 2015

Este procedimiento está enfocado en usuarios, en dos esquemas de altas y bajas, ejecutados a través de formularios.

Donde se debe de seguir los siguientes pasos para dar de baja a un usuario:

- Solicitud de baja de usuario: El responsable es el Jefe de Área/usuario
- Baja de usuario: Responsable es TI, Dirección de Soporte
- Registro: Responsable es TI, Dirección de Soporte

En ninguno de los documentos generados por la GTI y GSI no encuentran detalla información relacionada a:

- El tiempo mínimo que debe de emplearse en bloquear al usuario, computadoras, sistemas, etc.
- El tratamiento que debe de ejecutarse sobre la información generada, como: documentos personales almacenados en el computador asignado, correos electrónicos, documentos oficiales almacenados en el Quipux.

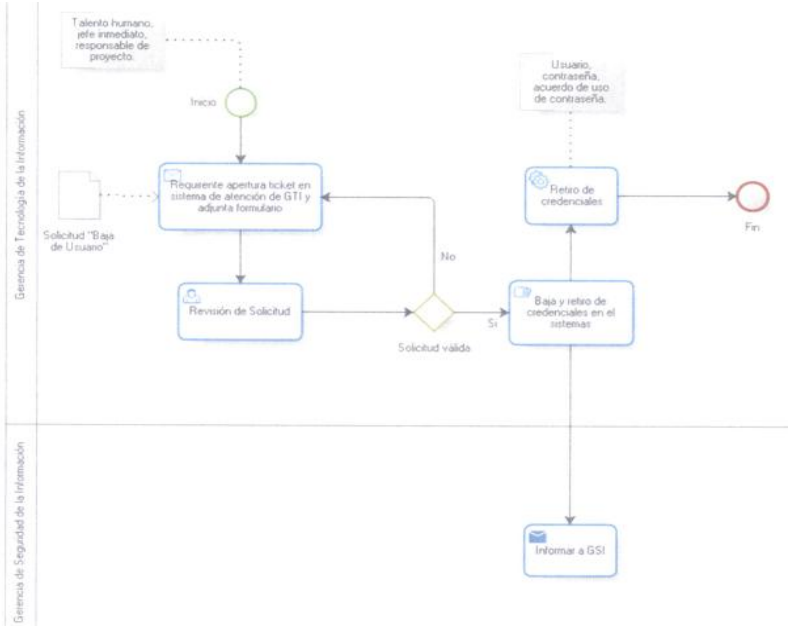


Figura 3.6: Gestión de baja de usuario definido por la GSI

CAPÍTULO 4

ANÁLISIS Y DISEÑO DE LAS PRUEBAS DE VULNERABILIDAD

4.1. Diseñar la matriz de riesgo.

El riesgo es la probabilidad que ocurra una amenaza que explota una vulnerabilidad de un activo informático, causando un impacto, comprometiendo la confidencialidad, integridad y/o disponibilidad.

El acuerdo ministerial 166, donde se define el ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN EGSI, donde CNEL EP es una de las instituciones miembros, acata los acuerdos generados como el

Artículo 7: En su esencia dice que cada entidad debe evaluar, diseñar e implementar un plan de manejo de riesgos de su institución, en base a la norma ISO 27005 Gestión del Riesgo en la Seguridad de la Información

La norma define las directrices para elaborar el proceso de análisis de riesgo, con los los siguientes subprocesos:

- Establecimiento del contexto.- Definir alcances y los limites de la gestión de riesgo
- Evaluación del riesgo.- Análisis del riesgo consiste en identificación del riesgo (activos, controles, vulnerabilidades, consecuencia), estimación del riesgo (metodología para la estimación de riesgo, evaluación de consecuencias, evaluación de la probabilidad de incidentes) y evaluación de riesgo.
- Tratamiento de riesgo.- Reducción del riesgo, retención del riesgo, evitación del riesgo y transferencia del riesgo.
- Aceptación del riesgo.- Son todos los activos con riesgo aceptable y justificado, que no son considerados como criterios normales de aceptación de riesgo de la organización.
- Comunicación de riesgo.- Intercambiar o compartir la información acerca del riesgo entre personas que toman la decisión y otras partes interesadas.

- Monitorización y revisión de riesgo.- Los riesgos no son estáticos, son cambiantes y debemos de monitorearlos constantemente por entidades externas.

4.1.1. Establecimiento del contexto

CNEL EP es una de las principales empresas de servicios de distribución eléctrica en el Ecuador, con la mayor cobertura y número de clientes del país.

Cualquier UN puede sufrir un ataque a la infraestructura de tecnología de la información, que pueda comprometer los servicios de toda CNEL EP.

Por lo que es necesario medir el riesgo que puede representar la violación de la seguridad de la UN Los Ríos, y evaluar cómo afecta a la gestión de las otras UN.

Esta evaluación deberá de hacerse por lo menos una vez al año para cumplir con lo dispuesto por el acuerdo ministerial 166, Esquema gubernamental de seguridad de la información EGSI

4.1.2. Valoración del riesgo en la seguridad de la Información

El riesgo se lo puede estimar como la concurrencia que se presenta después que ocurra un evento indeseado con su probabilidad que pase.

La valoración del riesgo calcula el valor del activo, identifica amenazas basadas en vulnerabilidades, aplica los controles para mitigar el impacto, estima sus efectos y determina las consecuencias, finalmente prioriza los riesgos.

Las siguientes actividades constan en la valoración del riesgo:

- Análisis de riesgo: Identificación del riesgo y estimación del riesgo
- Evaluación del riesgo

4.1.2.1. Identificación del riesgo

Como su nombre lo dice, el objetivo es determinar qué podría pasar para que se produzca una falla permisible, para llegar a entender los factores de esta pérdida.

Activos

Los activos seleccionados para definir el análisis de riesgo son considerados como críticos dentro de la gestión administrativa y comercial de la UN. La falla parcial o total de uno de estos servicios, ocasionaría problemas serios en la gestión administrativa, desde paralización de los trámites financiero hasta pérdidas económicas.

Los activos son propiedad de la UN Los Ríos, y el departamento de tecnología de la UN es la responsable de su producción, uso y seguridad; y algunas UN se tiene entornos de desarrollo y mantenimiento. Los activos primarios son:

- Facturación y recaudación
- Pago de nómina y proveedores.

Los activos secundarios son:

- Firewall: Equipo que administra la seguridad de la UN
- Switch de CORE: Equipo de alta velocidad instalado en el edificio principal
- Servidor de reportería comercial: Computador de escritorio, con funcionalidad de servidor válido para la solo para UN, que tiene publicado al Internet una aplicación Web utilizada exclusivamente por los contratistas.
- Servidor Comercial prepago: Computador de escritorio, con tarjetas generadoras de códigos de seguridad utilizados en la facturación de energía prepagada, además recauda el valor facturado localmente.

- Servidor Comercial: Servidor que mantiene el sistema comercial, con los procesos de: altas de cliente, facturación, recaudación, medidores solo de la UN.
- Servidor Financiero: Servidor que aloja el aplicativo financiero de toda la CNEL EP, corren los procesos de: presupuesto, tesorería, contabilidad, activos fijos y bodega.
- Servidor de Nómina: Servidor que aloja el aplicativo RR.HH de toda la CNEL EP, con los procesos de: talento humano,
- Servidor Directorio Activo: Servidor réplica del Directorio Activo principal, alojado en el Data Center.

Identificación de amenazas

Las amenazas son potenciales causales de daños a los activos tales como información, procesos y sistemas. Las amenazas pueden ser provocadas o accidentales, y su origen puede ser humana o natural.

Identificación de controles

El objetivo del control es garantizar que las operaciones reales coincidan con las operaciones planificadas. Se identificarán los controles existentes y los planificados.

Se debe de verificar que los controles existentes funcionen correctamente y en caso de implementarlos en el futuro se deberán de planificarlos igual que aquellos ya implementados.

Identificación de las vulnerabilidades

Se deberán de identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos de la empresa.

Identificación de las consecuencias

Se deberán de identificar las consecuencias que puedan tener cuando se pierde la confidencialidad, integridad y disponibilidad de los activos

A continuación se detalla un cuadro de los activos, sus amenazas, controles, vulnerabilidades y sus consecuencias.

4.1.2.2. Estimación del riesgo

Metodología para la estimación del riesgo

Puede ser cualitativa o cuantitativa, o una combinación de ellas, dependiendo de las circunstancias.

- Estimación cualitativa: Es la más fácil de implementar, utiliza una escala de atributos calificativos para describir la longitud de las resultados potenciales, por ejemplo alta, media y baja; y la probabilidad de que ocurran dichas consecuencias.
- La estimación cuantitativa: A diferencia de la estimación cualitativa, las consecuencias y la probabilidad se valen de una escala con valores numéricos

Evaluación de las consecuencias

Evaluar el impacto en el negocio que puede resultar de incidentes posibles o reales, teniendo en cuenta las consecuencias por la pérdida de confidencialidad, integridad o disponibilidad de los activos.

Evaluación de la probabilidad de incidentes

Tabla 5: Identificación del riesgo

Activo	Nro	Identificación de Amenaza	Identificación de Controles	Identificación vulnerabilidades	Evaluación de Consecuencias
Servidor Comercial	1	Falla en la comunicación de datos	UPS, enlaces redundantes	Línea de comunicación sin protección	Pérdida de la disponibilidad
	2	Abuso de derechos	Diccionario de datos y Backup de respaldos	Falta de ambiente de pruebas	Pérdida de la integridad
	3	Estafa de clientes	Confirmar datos personales en oficinas de CNEL	Falta de acuerdos de confidencialidad con contratistas.	Pérdida de la confidencialidad
Servidor Comercial Prepago	4	Pérdida de suministro de energía	UPS	Funcionamiento no confiable del UPS	Pérdida de la disponibilidad
	5	Daño del disco duro	Backup de datos	Incumplimiento en el mantenimiento	Pérdida de la integridad
	6	Apropiación de contraseñas de usuarios privilegiados	Software cliente sólo instalado en una máquina validada por el servidor su IP	Contraseñas sin política de cambios	Pérdida de la confidencialidad
Servidor Financiero	7	Saturación del sistemas	Servidor real con mejore rendimiento CPU y memoria. UPS	Entorno virtualizado con poca asignación de recursos	Pérdida de la disponibilidad
	8	Falla en la base de datos	Sistema redundante de discos duros RAID, backup de cintas	Falta del procedimieno formal para la supervisión del registro	Pérdida de la integridad
	9	Escucha subrética	Adquirir switch de accesos que permitan implementar seguridades	Tráfico sensible sin proteción	Pérdida de la confidencialidad
Servidor Nómina	10	Falla en el equipo de telecomunicaciones	VirtualHost	Falta de balanceo de carga	Pérdida de la disponibilidad
	11	Falta de mecanismos de auditoría	Documentos que justifican incrementos en los rubros o de personal	Procesamiento ilegal de los datos	Pérdida de la integridad
	12	Espionaje remoto	Procesos críticos validar IP+usuarios	Arquitectura insegura de la red	Pérdida de la confidencialidad
Servidor Directorio Activo	13	Falla en el equipo de telecomunicaciones	Réplica de servidores por zonas	Falta de balanceo de carga	Pérdida de la disponibilidad
	14	Ataque por ingeniería social	Bloquear los puertos de administración en el firewall y usuarios por entidades	Autenticación basada en "algo que el usuario sabe"	Pérdida de la confidencialidad
Firewall	15	Falla del equipo de comunicaciones	Configuración activo, pasivo. Protocolo HRSP	Punto único de falla	Pérdida de la disponibilidad
Switch CORE	16	Tráfico sensible sin protección	Configuración redundante del stack	Escucha subreticia	Pérdida de la disponibilidad

Después de identificar los escenarios de incidentes, es necesario evaluar la probabilidad de cada escenario y estimar la ocurrencia del impacto, utilizando técnicas cualquiera de las dos estimaciones cualitativas o cuantitativas.

Nivel de estimación del riesgo

Se deberían estimar el nivel de riesgo para todos los contextos de incidente adecuados

- La metodología para la estimación del riesgo se hace con valores numéricos con una escala del 1 al 5.
- La evaluación de las consecuencias se las mide en valor monetario, con escala desde menor de $10,000 hasta mayor que el patrimonio.
- La probabilidad de los incidentes se hace en el tiempo, con valores desde un mes hasta 5 años.

Tabla 6: Estimación de riesgo

Probabilidad	Impacto
1 Por lo menos 1 caso en 5 años	1 Menos de $10,000
2 Por lo menos 1 caso cada 3 años	2 Mayor de $10,000 y menor de $50,000
3 Por lo menos 1 vez al año	3 Mayor de $100,000 y menor de $500,000
4 Por lo menos 2 veces al año	4 Mayor de $1,000,000 y menor de $5,000,000
5 Por lo menos 1 vez al mes	5 Mayor que el patrimonio

También se define la matriz de calor, donde relaciona el impacto con la probabilidad.

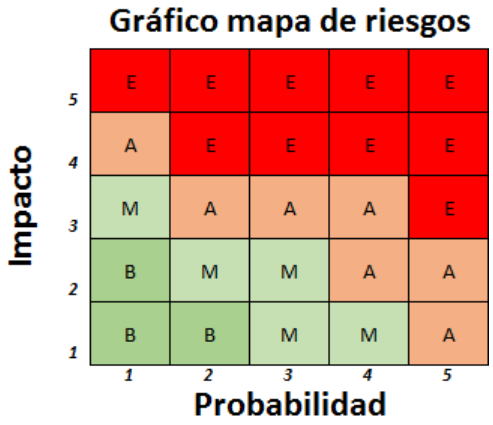


Figura 4.1: Mapa de riesgo

4.2. Definir herramientas de penetración informática.

Para realizar todas las pruebas de penetración, utilizaremos un computador de escritorio, con funcionalidad de servidor de máquinas virtuales instalado el VmWare ESXi 6.0, con tres máquinas virtuales. Una de las máquinas virtuales es Kali Linux versión 6.0, donde se aplican las herramientas informáticas open source de mayor uso, tales como:

- NMAP.- Mapeador de redes, herramienta de exploración de redes y de sondeo de seguridad – puertos.
- NESSUS.- Programa de escaneo de vulnerabilidades de diversos sistemas operativos.
- NIKTO.- Programa escáner de servidores web, que se encarga de realizar distintos tipos de acciones como: malas configuraciones y vulnerabilidades en el servidor, archivos de instalación por defecto,

listado de estructura de versión, test de vulnerabilidades XSS, ataque de fuerza bruta.

- METASPLOIT.- Es un proyecto de seguridad de código abierto que brindar información acerca de las vulnerabilidades y ayuda en la ejecución en el test de penetración
- NETCAT.- Es una herramienta que permite mantener abrir un puerto TCP/UDP en el HOST quedando a la escucha, para que mantenga comunicación desde un equipo remoto ligado a otro puerto UDP/TCP

4.3. Diseñar política de desvinculación del personal.

Para tener una reacción inmediata en el bloqueo de todos los servicios asociados de una persona, que se encuentra en proceso de desvinculación, es necesario realizar cambios en la *Política para control y gestión de acceso* del *Manual de políticas de seguridad de la información* redefinida más adelante en el capítulo 4.7

Por lo que se procede a mejorar el *Procedimiento de control y gestión de usuarios: altas, bajas, manejo de privilegios* añadiendo las siguientes tareas en altas y bajas.

Altas

- Cada usuario creado en un Sistema de Información deberá de estar relacionado con un equipo terminal, identificado con información

única la combinación de: dirección MAC, puerto físico de un switch o lógico de un AP y dirección IPv4.

Bajas

- Tiempo de baja usuario. El responsable de asignación de recursos de TI procederá a bloquear en el mismo día: todos los Sistemas de Información, todos los equipos de comunicación, dirección IP, dirección MAC, puerto físico del switch o puerto lógico del AP.
- Respaldo de la información.- El responsable de asignación de recursos de TI procederá a realizar el respaldo de toda la información que hubiese generado el trabajador, en un tiempo no mayor a 5 días laborables, entregables en DVD y servidor de respaldo, que se almacenará hasta un máximo de 5 años. Este respaldo comprende: documentos personal almacenados en el equipo terminal, correos electrónicos, documentos oficinales, etc. Una copia de todo lo respaldado será entregado al trabajador desvinculado

4.4. Definir tipos de autenticación en la red de datos.

Todos los equipos terminales como computadoras desktop, computadoras portátiles o dispositivos móviles que se conecten a la red de datos de CNEL EP UN Los Ríos, deberán estar autenticados, con la finalidad de evitar que equipos informáticos que no sean de propiedad

de CNEL EP puedan ingresar a la red de datos y potencialmente convertirse en una amenaza latente.

Para solucionar el problema de autenticación de la red ethernet IEEE 802 LAN/WAN, ha definido el reenvío de paquetes con el protocolo 8021.1x. El protocolo es ampliamente usado como un mecanismo de control en las interfaces LAN para solucionar problemas de autenticación y seguridad ethernet. El 8021.1x es un protocolo de control de acceso de red basado en puerto. El sistema 8021.1x tiene una típica estructura cliente/servidor que incluyen tres entidades: cliente, dispositivo y servidor.

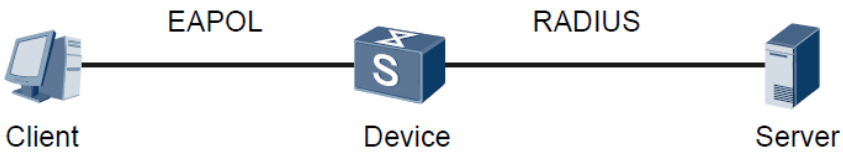


Figura 4.2: Sistema de autenticación 802.1x

- Cliente: Es una entidad en el segmento LAN, que está autenticado por un dispositivo en el otro extremo del enlace. El cliente usualmente es un terminal de usuario. Un usuario inicia la autenticación 802.1x iniciando el software cliente.
- Dispositivo: Es una entidad en el segmento LAN, que autentica al cliente conectado. El dispositivo por lo general es un dispositivo de red que soporta el protocolo 802.1x y proporciona una interface físico o lógico para el acceso LAN al cliente.

- Servidor: Es una entidad que ofrece autenticación para el dispositivo. El servidor suele ser un servidor de acceso telefónico de autenticación de servicio de usuario remoto (RADIUS) para la implementación de la autenticación, autorización y contabilidad (AAA)

La implementación del servidor *radius* se lo hace es a través del módulo *freeradius*[2], añadido del software pfSense, que es una distribución de Linux Debían muy estable, con las siguientes características:

- Módulos incluidos soportan LDAP, MySQL, PostgreSQL, Oracle y otras BBDD
- Soporta todos los tipos de autenticación EAP, PEAP y EAP-TTLS

El pfSense por ser un firewall que requiere como mínimo dos tarjetas de red. Una tarjeta de red configurada para el segmento WAN y otra tarjeta de red para el segmento LAN. Debido que el servidor RADIUS debe de comunicarse con el switch de CORE, ambos deben de tener el mismo segmento de red, es decir la dirección IP es 172.19.192.11/25

La interface WAN se la utilizará para tener acceso hacia el resto de la red, incluida Internet, por ahora no la vamos a utilizar, debido que no es motivo de estudio y se le asignará la dirección IP 192.168.1.100/24 con puerta de enlace IP 192.168.1.1

[2] Freeradius: Es un servidor RADIUS de alto rendimiento de software abierto más popular que soporta

El pfSense de forma predeterminada no incluye el módulo freeRadius, deberá de agregarlo manualmente para posteriormente configurarlo.

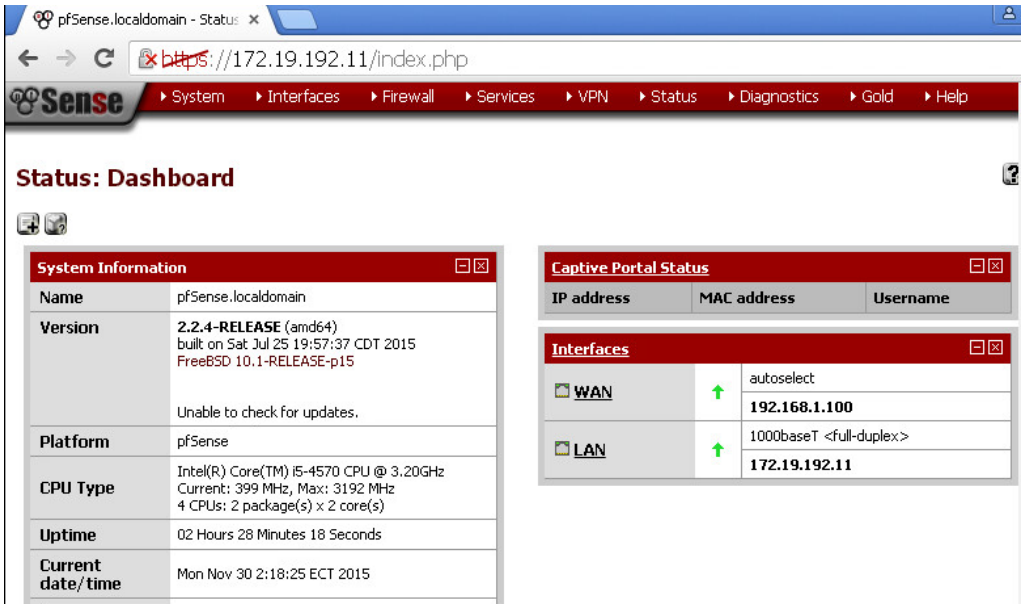


Figura 4.3: Servidor pfSense con las interface LAN y WAN

Figura 4.4: Módulo *FreeRADIUS vs 2* en el *pfSense*

Una vez añadido el módulo del *freeradius* en el servidor *pfSense*, se procede a configura el dispositivo que realizarán el Servidor de Acceso a la Red (NAS) o punto de entrada, que en este caso representa el switch de CORE. Los principales parámetros a configurar son: dirección

IP, la clave compartida preferentemente debe ser larga y el número máximo de conexiones.

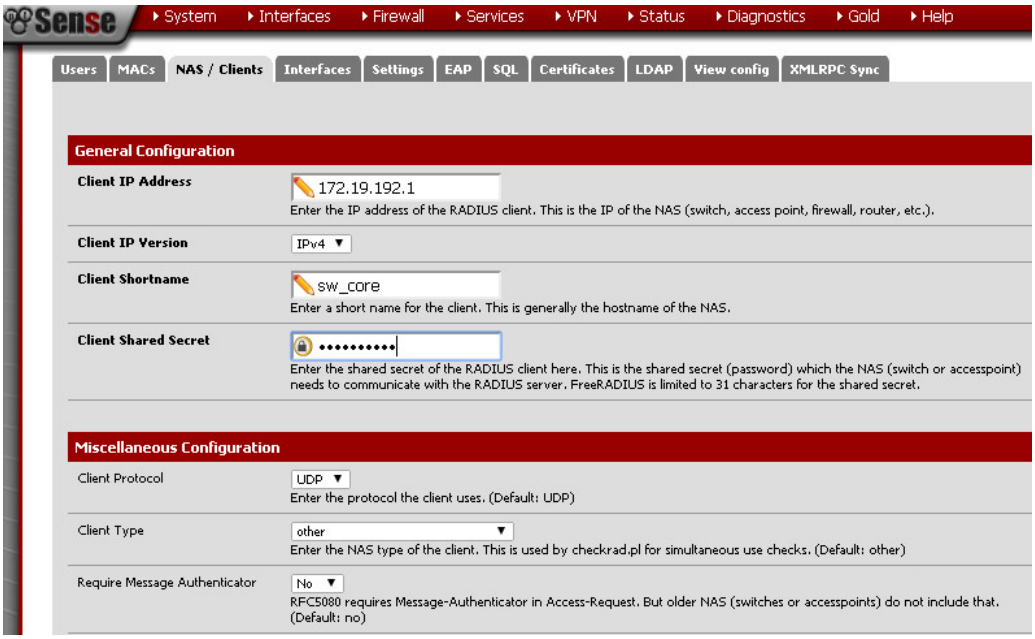


Figura 4.5: Parámetros *NAS* en el *freeradius*

Se configura todos los clientes NAS que tiene CNEL EP, entre ellos están los puntos los Access Point

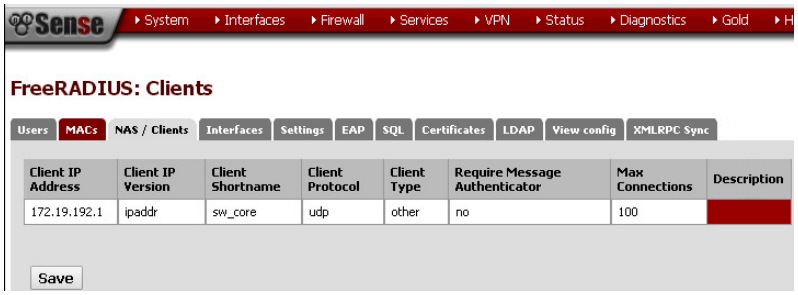


Figura 4.6: Lista de todos los NAS en freeRadius

En la página de Interfaces se configura los puertos que utilizan el servidor de autenticación puerto 1812 y el puerto para la cuenta 1813

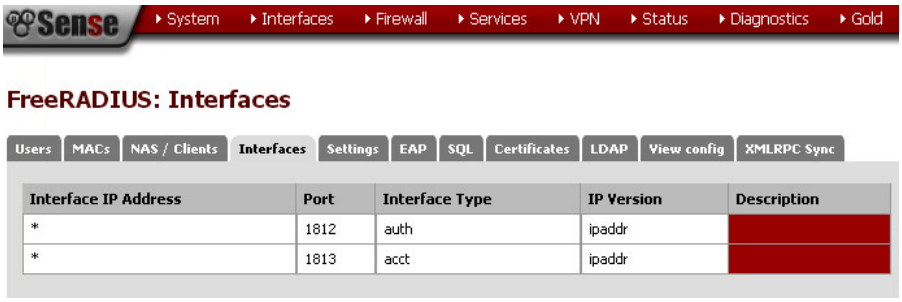


Figura 4.7: Puerto de autenticación y cuenta del cliente NAS freeRadius

En la página Setting se configura principalmente la habilitación de la autenticación por dirección MAC por texto plano que son los últimos de esta sección

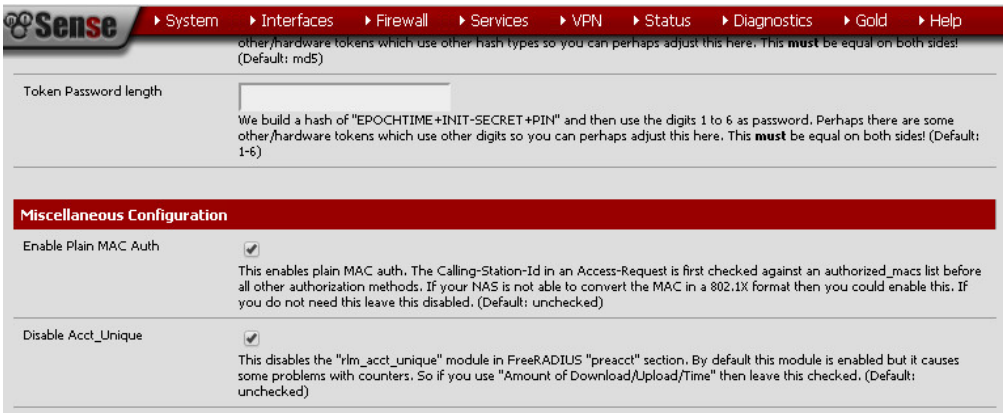


Figura 4.8: Habilitar autenticación texto plano de MAC – FreeRADIUS

Quizá uno de los principales parámetros de configuración del FreeRADIUS, es la Extensible Autenticación Protocolo (EAP), que es un framework de autenticación usado habitualmente en redes WLAN, aunque puede ser usado en redes cableadas. Es una estructura de

soporte, no es un mecanismo específico de autenticación. Suministra algunas características comunes y negociaciones para los elementos de autenticación optados. Estos mecanismos son llamados métodos EAP, de los cuales se conocen actualmente unos 40. Los definidos por los RFC de la IETF incluyen EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-IKEv2, EAP-SIM, EPA-AKA.

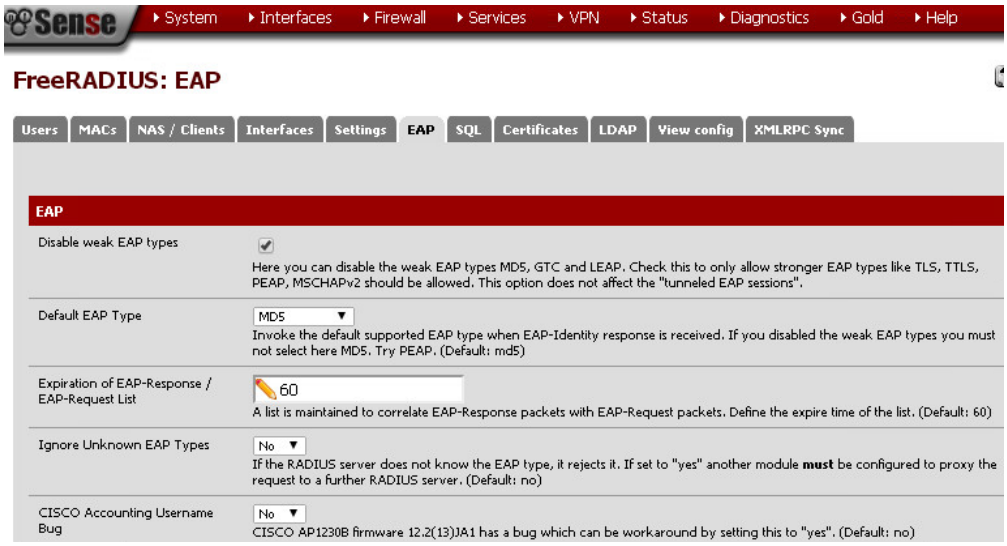


Figura 4.9: Autenticación EAP en FreeRadius

Finalmente las direcciones MAC de los dispositivos finales, se registran en la base de datos MySql, debido a la gran cantidad de equipos que actualmente existen.

Cabe mencionar que existen dos modos de autenticación del protocolo 802.1x, el modo realy que permite enviar el usuario y clave; y el modo termination que solo envía la MAC como usuario y como clave. Este

segundo modo de autenticación es ideal para validar terminales que no permite interactuar, como son impresoras y teléfonos IP.

Esta protección se puede realizar en el edificio principal de la UN, debido que en los switch de las agencias no soporta la funcionalidad 802.1x. Por lo que en el switch de CORE se habilitarán en los puertos que conectan los switch de accesos la funcionalidad del 802.1x

4.5. Definir mecanismos de bloqueos en la red de datos

Los mecanismos de bloqueos en la red se los puede controlar a nivel de la capa 2 y capa 3, implementados con los switch de accesos y el firewall

4.5.1. Bloqueos en capa 2

Todos los bloqueos en el switch son aplicables en los edificios principales, pero en las agencias y subestaciones están limitadas algunas características (de puerto seguro, NA, pero si se puede habilitar en los switch del edificio principal.

Existen varios mecanismos de seguridad que se pueden implementar:

- Puerto seguros
- Control de acceso a la red NAC
- Espiar DHCP

- Configuración de ataques de Defensa de IP
- Supresión de tráfico
- Descubrimiento del vecino espía.

4.5.1.1. Puerto seguros

Se configura cada interfaz de red del switch de acceso, que proteja contra ataques, se implementa medidas de seguridad por MAC o ARP

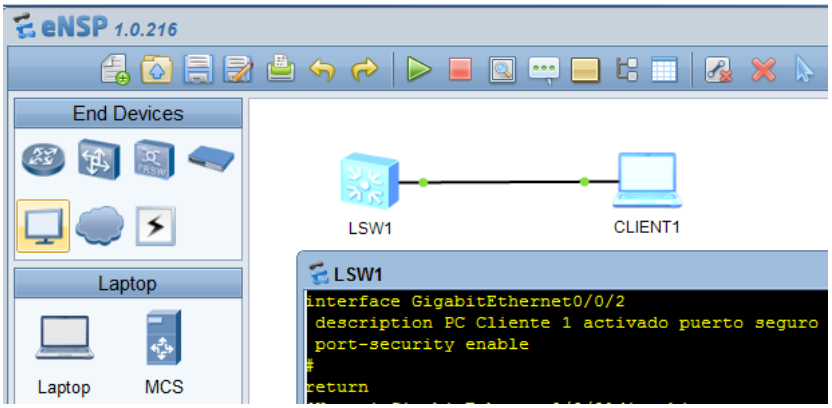


Figura 4.10: Aplicando puerto seguro por MAC

- Protección por MAC.- Garantiza conexiones no deseadas en una interfaz de red, restringiendo el número máximo de direcciones MAC que ese puerto puede soportar, en forma predeterminada es 1. Esta política será utilizada para todas las estaciones de trabajos. Opcionalmente se puede configurar el comportamiento de realizará una vez que detecte que

se ha cambiado la MAC, que puede ser *protect, restrict* o *shutdown,* por defecto utiliza *restrict*

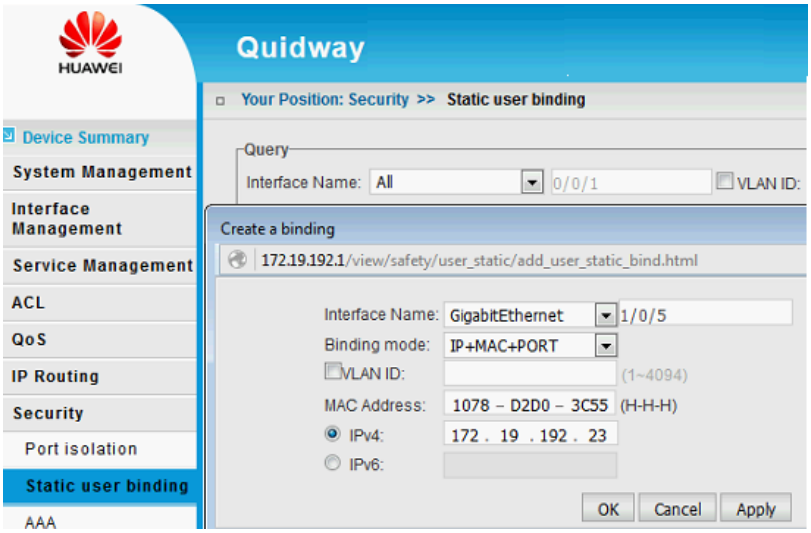


Figura 4.11: Aplicando puerto seguro por ARP

- Mapeo ARP.- Evita que la tabla ARP se desborde y el switch se comporte como HUB debido a un ataque hombre en medio. Política destinada a las conexiones de servidores, donde asegura que ese puerto se conecta un servidor con una dirección MAC y una IP

4.5.1.2. Control de acceso a la red NAC

En los switch de acceso puede implementar el principio de funcionamiento y la configuración del control de acceso a la red NAC.

Los computadores pueden accesar a la red usando la autenticación 802.1x. La autenticación del servicio es un

servidor RADIUS que está implementado con el programa freeradius embebido en pfSense.

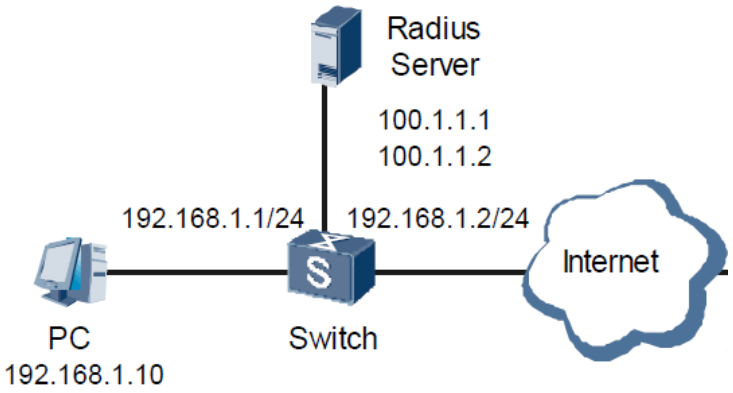


Figura 4.12: Diagrama de red autenticar 802.1x

4.5.1.3. Configuración de ataques de Defensa de IP

Se utiliza para proteger que la dirección IP y MAC de un dispositivo de red conectado en una interfaz de red, no pueda ser falsificada por otro dispositivo en la red, para que posteriormente envíe información a un tercero, como un servidor. Este escenario es ideal para configurarlo para las computadoras destinadas para asuntos puntuales, por ejemplo: Puntos de recaudación, realizar pagos por parte de tesorería.

4.5.1.4. Supresión de tráfico.

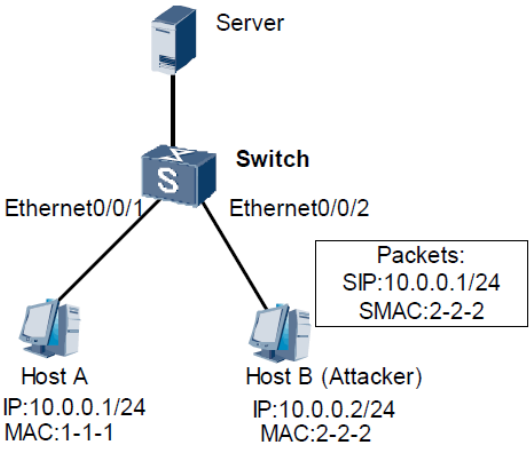


Figura 4.13: Diagrama de red para configura defensa IP

Con la finalidad de limitar o suprimir el tráfico generado por paquetes broadcast, paquetes desconocidos multicast y unicast se lo puede limitar. Este escenario es ideal para evitar congestiones en enlaces de datos con otros edificios o switch de accesos

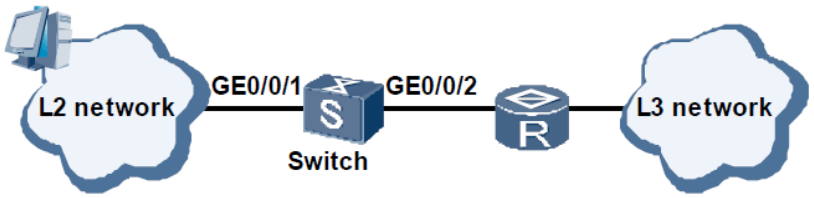


Figura 4.14: Diagrama de red de supresión de tráfico

4.5.1.5. DHCP defensa

Evita la prevención de ataques al servidor DHCP, configurando la interfaz donde se encuentra el servidor y

activa la función de alarma para los paquetes de respuesta DHCP descartados

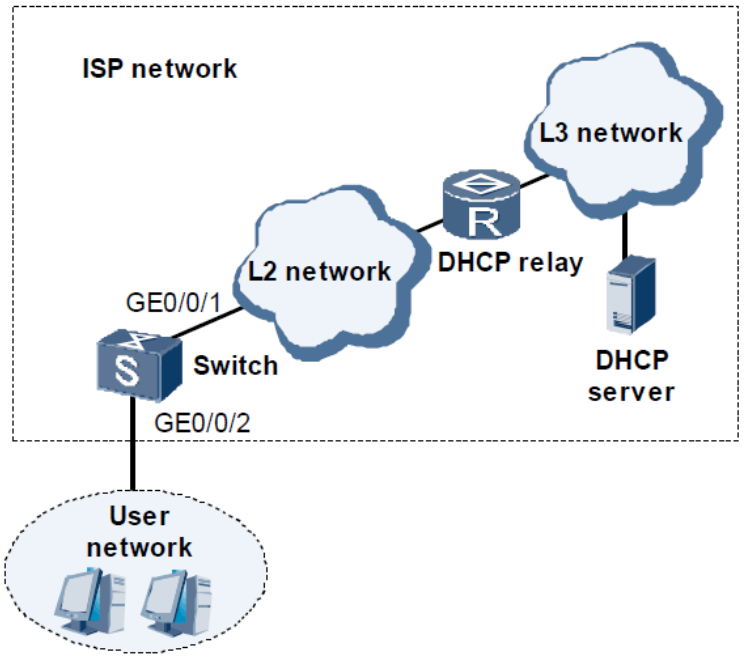


Figura 4.14: Diagrama de red previene ataques de falso DHCP

4.5.2. Bloqueo de capa 3

El firewall de Huawei es el encargado de realizar todos los bloqueos a nivel de capa tres en adelante y de ser posible de capa siete, en el caso de CNEL EP, los equipos soportan algunas aplicaciones. Por lo el firewall bloquea lo siguiente:

- Direcciones IPv4
- Direcciones URL
- Aplicaciones

4.6. Diseñar QoS para garantizar la disponibilidad de los servicios.

La QoS se la administra en la capa 2 del modelo OSI, utilizando los switch de acceso que se encuentran instalados en las oficinas principales, agencias y subestaciones de la UN Los Ríos.

El tráfico que circula en la red, es de datos y video. Se aplicará la QoS a los switch de acceso de las agencias y subestaciones, para controlar la velocidad de salida en los puertos donde están conectadas las cámaras de video vigilancia, limitando su ancho de banda, para evitar saturar del enlace de datos.

Se hace el análisis del tráfico requerido por la red de datos y las cámaras de video vigilancia, y se concluye que se requiere las siguientes tasas:

- 1Mbps por cada cámara.
- 2Mbps para datos

En este tipo de switch de acceso se puede limitar solo la velocidad de salida. Por lo que es necesario estar familiarizado con la siguiente terminología:

- Tasa de Información Comprometidas (CIR) o ancho de banda.
- Tasa de Exceso de Información (EIR): Es la velocidad adicional al inicial
- Tasa de Información Máxima (PIR): Que es la velocidad máxima que una interface puede transmitir

Además se asigna la Vlan's 900 para video y la Vlan's 1 para datos, y se realizan los siguientes cambios:

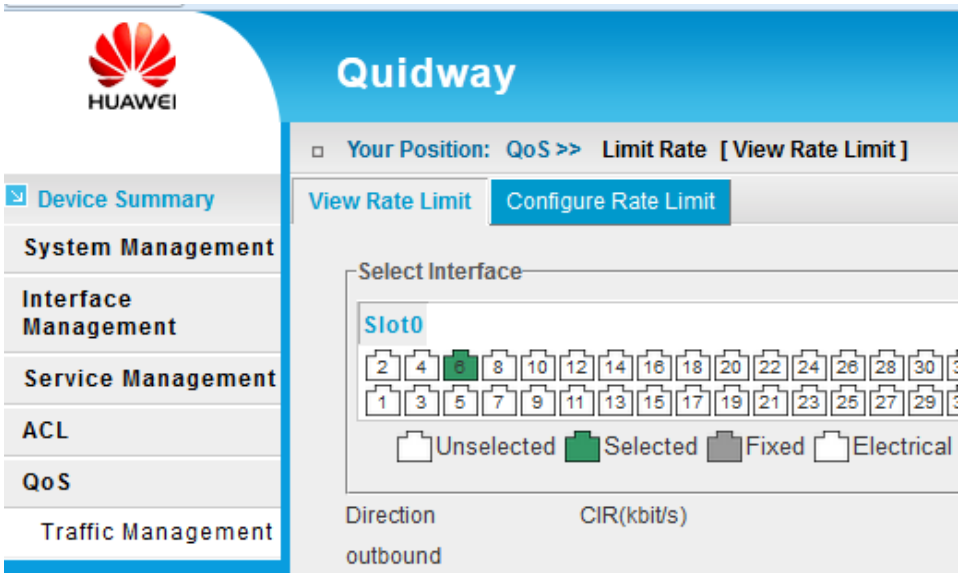


Figura 4.16: Sin aplicar QoS en puerto 0/0/6

- Solicitar a CNT eliminar la configuración del puerto TRUNK que permite pasar las Vlans 1 y 900 en una sola interfaces.

Figura 4.17: Velocidad de puerto 0/0/6 previa a la QoS

- Solicitar a CNT separar las dos Vlan's en dos interfaces de red, una para la Vlan's 1 y otra para la Vlan's 900
- Conectar la interface ethernet de CNT configurada como Vlan's 1 a un puerto del switch de CNEL EP configurado con Vlan's 1, aplicado Qos, con velocidad limitada de salida a 2 Mbps.

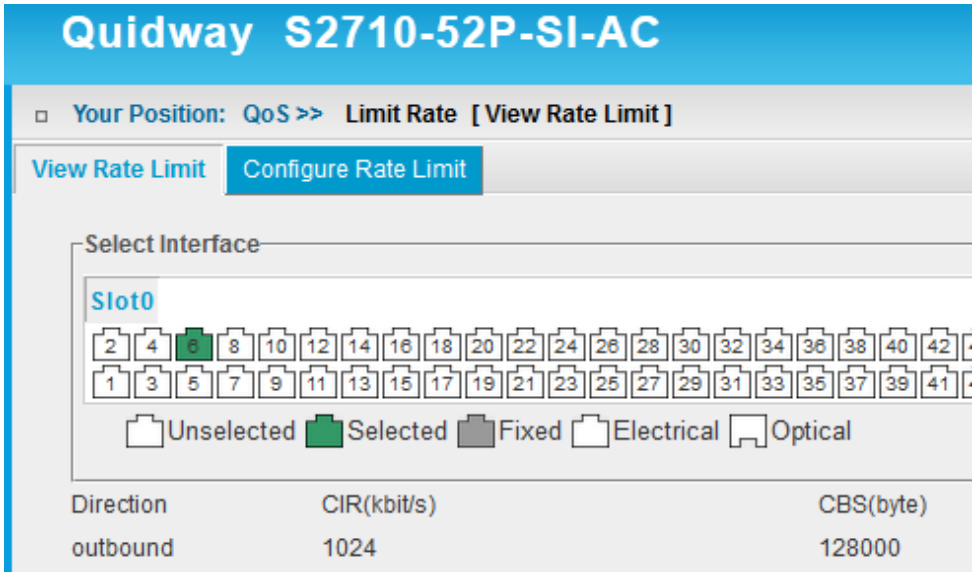


Figura 4.18: Aplicado QoS restringiendo la velocidad de salida a 1Mbps

Conectar la interface Ethernet de CNT configurado como Vlan's 900 a un puerto del switch de CNEL EP configurado con Vlan's 900, a una velocidad igual a la cantidad de las cámaras de video vigilancia en Mbps.

Se hacen los cambios en el puerto 0/0/6 y se verifica la velocidad de transmisión.

4.7. Diseñar políticas de control de acceso.

Con el desarrollo y el aumento de las aplicaciones corporativas, los usuarios tienen mayor necesidad y dependencia en la red. Esto crea un incremento en el riesgo de la seguridad. Una red segura, confiable, con mayor capacidad de conmutación y calidad de servicio, es la mayor preocupación del usuario usuarios de la empresa, y las instalaciones de red deben son la base para la seguridad de las redes empresariales.

Figura 4.19: Velocidad después del QoS a 1Mbps

En la actualidad la comodidad de una red, representa amenazas para los activos de la empresa. Los problemas clásicos que se presentan en la Intranet por parte de los usuarios finales son:

- Usuarios no autorizados ingresan a la red
- Usuarios autorizados abusan de la Intranet
- Equipos terminales no tienen los parches actualizados

- Los empleados instalan software no autorizado
- Los empleados acceden a páginas web irrelevante para la empresa
- Los empleados se saltan los controles del firewall
- El antivirus no siempre está actualizado o instalado

Los dispositivos de seguridad actuales no pueden proteger eficazmente la red, ya que no son capaces de:

- Evaluar la seguridad de los equipos finales.
- Prevenir usar terminales autorizadas que abusan de los recursos
- Prevenir ataques maliciosos

La tecnología del Control de Adminisión de la Red (NAC) sirve para garantizar la seguridad de los servicios de comunicación de la red. En el marco de seguridad NAC, la seguridad de la red interna se considera desde la perspectiva del terminal de usuario, la aplicación de control de seguridad sobre los usuarios de acceso, y garantizar la seguridad de extremo a extremo.

En base a lo expuesto se recomienda definir el Control de Admisión de Red (NAC) como un marco de seguridad de extremo a extremo, diseñado bajo el siguiente esquema de red, definiendo las siguientes entidades:

NAC Terminal

Funciona como el cliente NAC e interactúa con los dispositivos de acceso de red para autenticar a los usuarios de acceso. Si se utiliza la autenticación 802.1x, los usuarios deben instalar el software de cliente

Dispositivo de acceso a la red

Autentica y autoriza acceso a los usuarios. Por lo general funciona con un servidor de Autenticación, Autorización y Contabilidad (AAA) para evitar el acceso no autorizado de terminales, reducir al mínimo las amenazas presentadas por terminales inseguros, evitar las solicitudes de acceso no autorizados desde los terminales autorizados, y proteger los recursos básicos.

Servidor de control de acceso.

Controla la salud del terminal y gestiona terminales basados en políticas específicas. Gestiona los comportamientos de los usuarios y cheques por violaciones de reglas para prevenir ataques maliciosos de terminales

Por los antecedentes presentados, esta política deberá de incluirse en el *Manual de políticas de seguridad de la información* elaborado por la Gerencia de la Seguridad de la Información, reformando la *Política para control y gestión de acceso: autenticación y manejo de contraseñas* quedado de la siguiente manera:

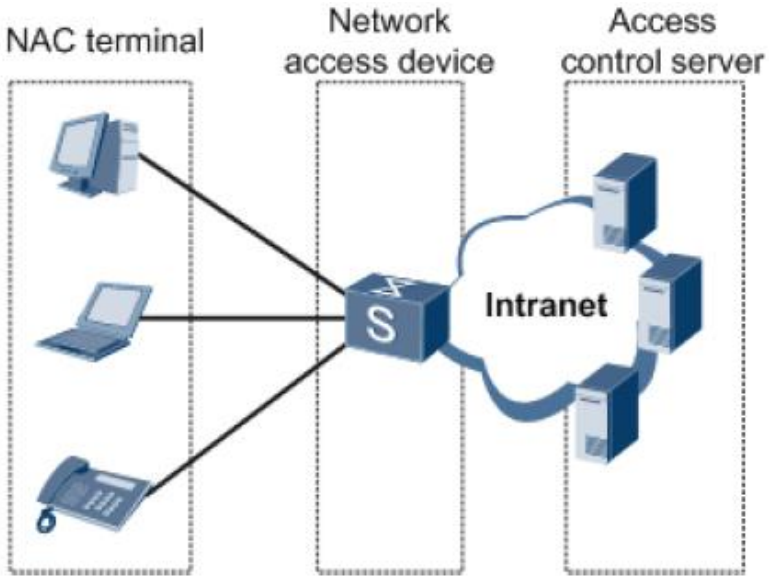


Figura 4.20: Esquema de autenticación en la red NAC

4.7.1. Control de acceso

Principio de control

- Todo equipo terminal interno o externo de la corporación que requiera conectarse a la infraestructura tecnológica de CNEL EP, deberá de verificarse que cumplan con el modelo de seguridad de control de acceso, antes de que estos tengan acceso a la red.
- El modelo de seguridad del control de acceso es NAC que utiliza la infraestructura de red para forzar las políticas de seguridad
- Los clientes son usuarios o computadoras
- Al momento de realizar la conexión con la red, los clientes presentan sus credenciales, que una vez validada, se define el nivel apropiado de acceso dentro de la red.

- Los clientes no compatibles serán aislados en una red cuarentena, para ser provistos de componentes que permitan conectarse y acceder a la red de forma normal
- Los clientes utilizan un agente NAP (Network Access Protection), que recolecta credenciales y genera una lista de declaraciones al equipo que evalúa declaraciones de la salud
- El equipo que evalúa la declaración de salud, envía a un servidor de políticas de red para validar al cliente
- El servidor de políticas de red evalúo las declaraciones de salud en función del modelo de seguridad definido devuelve el estado de validación de salud.
- El equipo evalúa los resultados de todas las validaciones y envía el perfil de acceso correspondiente al dispositivo de acceso para permitir el acceso del cliente a la red de datos.
- Los clientes no compatibles que están en la red cuarentena, serán re-evaluados posteriormente a la revisión de los requerimientos faltantes para garantizar el acceso a la red.
- Que la única fuente de autenticación para todos los sistemas de información son los usuarios definidos en el Directorio Activo corporativo.
- El método de autenticación usados en los sistemas de información masivas, están basado en algo conocido, la clave

- El método de autenticación usados en los sistemas de información especiales, están basado en algo conocido más algo poseído (certificado digital emitido por una entidad certificadora, contenida en un dispositivo usb tipo token)

4.8. Definir políticas para evitar ataques de Denegación de Servicios.

- El estándar ISO 27001 tiene un especial enfoque la preservación de la confidencialidad, integridad y disponibilidad de la información.
- El objetivo es “garantizar la disponibilidad de los servicios informáticos prestados en cada de las UN”.
- Se recomienda aplicar como mejores prácticas, la protección contra ataques por inundación de paquetes.
- Todos los terminales que se conecte a la infraestructura de la red tecnológica de CNEL EP de forma directa, que se detecte que genere tráfico inusual con el objetivo de saturar la red de datos, será identificado y bloqueado de forma automática hasta que el software calificado como ataque sea bloqueado o desinstalado.

La implementación de esta política se la realizará con los firewall instalado en cada UN, activando la opción *protección de seguridad*

A continuación se procede a explicar la activación y protección en forma detallada

4.8.1. Defensa de ataques

La protección contra ataques por inundación está configurada para descartar los paquetes y generar alarma, y la interface que se elegirá es la expuesta al Internet VLAN 501 que tiene asociada la IP pública

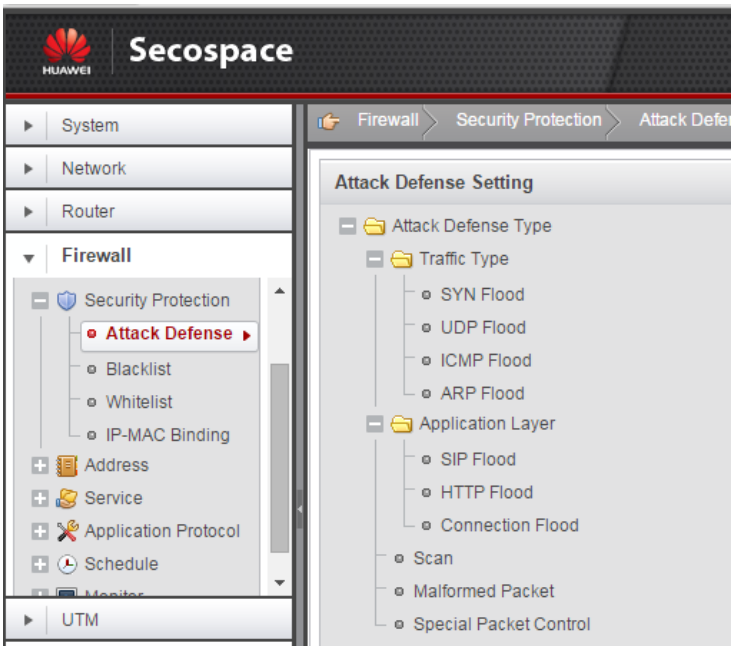


Figura 4.21: Firewall activando protección de seguridad

4.8.1.1. SYN FLOOD

El ataque consiste en enviar una gran cantidad de paquetes SYS TCP que causa masivas conexiones incompletas TCP ocupando recursos.

Se configura la opción de detección basada en la detección de fuente, es decir el firewall comprueba si la

dirección IP fuente existe, si no existe el paquete es descartado; caso contrario es enviado a una lista blanca,

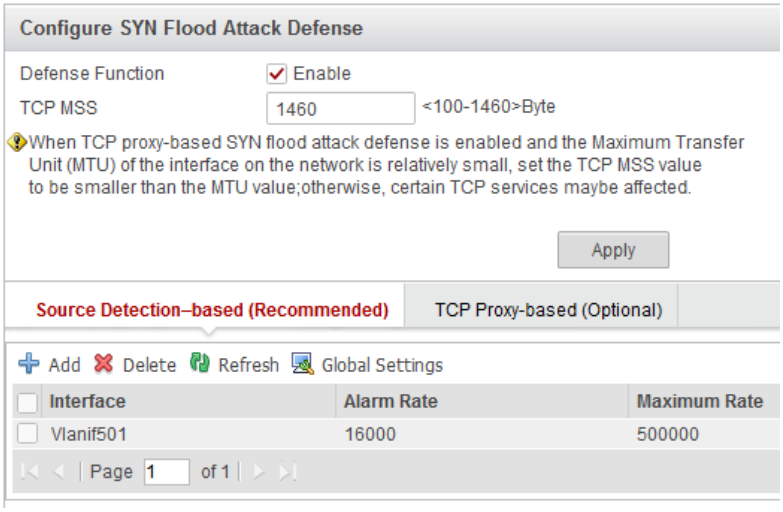


Figura 4.22: Activando protección contra *SYN FLOOD*

4.8.1.2. UDP FLOOD

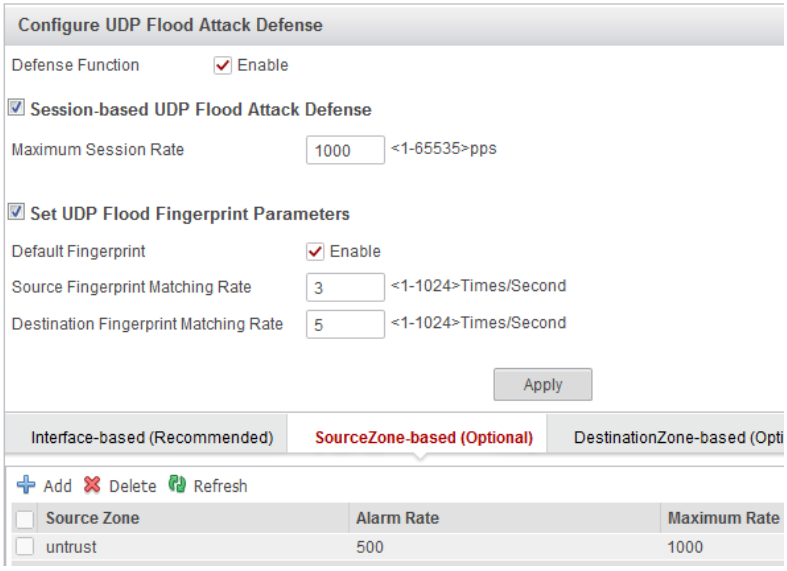


Figura 4.23: Protección con ataques *UDP Flood* X zona

El atacante envía gran cantidad de paquetes UDP al firewall que ocupan ancho de banda, como resultado se satura y no puede seguir brindando el servicio externo.

La defensa se basa en limitar el número de paquetes por interfaces, zonas de seguridad o sesiones.

4.8.1.3. ICM FLOOD

Envía gran cantidad de paquetes ICMP para ocupar ancho de banda en el servidor, como resultado el servidor no brinda los servicios externos. Para evitar el ataque se limita la cantidad de paquetes ICMP que pueden circular por interfaces, zonas o sesiones.

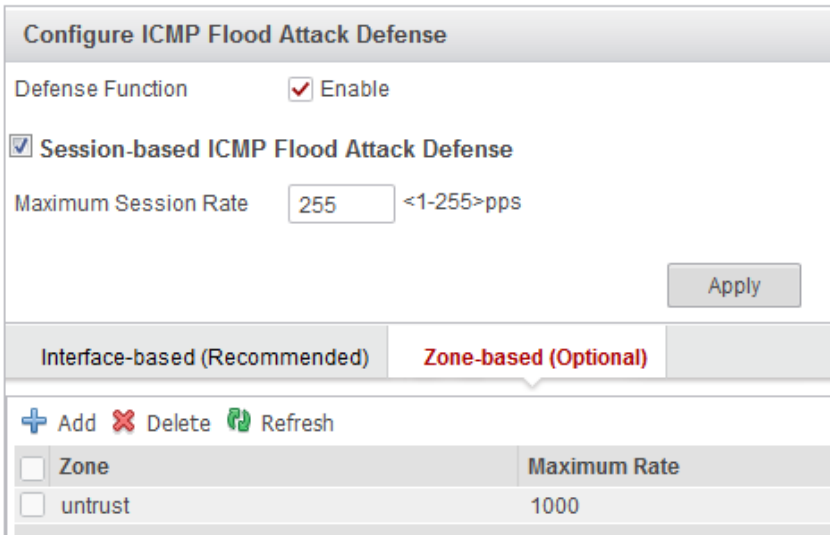


Figura 4.24: Protección con ataques ICMP Flood X zona

4.8.1.4. ARP FLOOD

Puesto que hay diferentes tipos de paquetes broadcast y ARP, los paquetes ARP son usualmente utilizados para evitar ataques. El firewall puede defenderse de los ataques de inundación ARP mediante el control del umbral de los paquetes ARP recibidos por interfaces

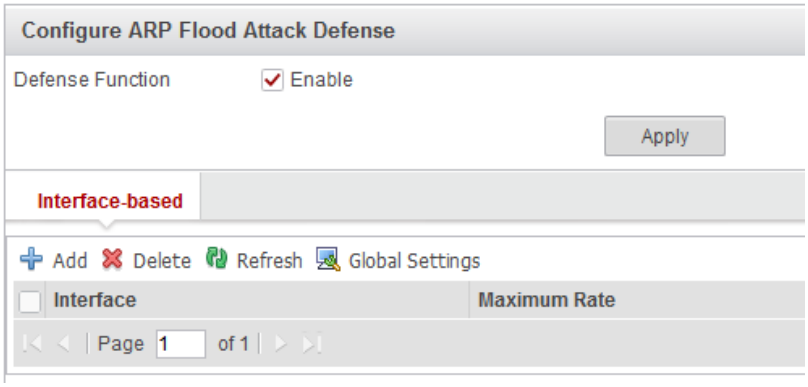


Figura 4.25: Protección con ataques ARP Flood

4.8.1.5. SIP FLOOD

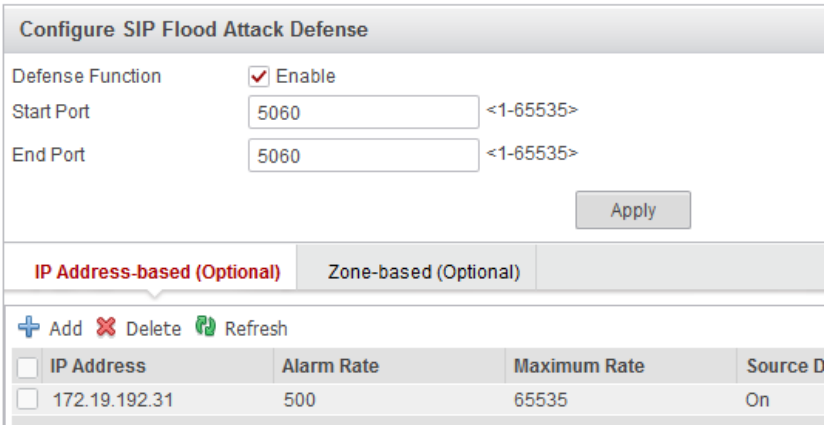


Figura 4.26: Protección con ataques SIP Flood

Un ataque consiste en enviar una gran cantidad de paquetes SIP en un periodo muy corto de tiempo, agotando los recursos del servidor y o ancho de banda. La defensa consiste en limitar la tasa de paquetes SIP basado en direcciones IP o zonas de seguridad

4.8.1.6. HTTP FLOOD

Consiste en enviar una gran cantidad de paquetes HTTP al servidor a través del servidor directamente o a través de una bots. Como resultado, los recursos del servidor se consumen, y el servidor no puede responder a las solicitudes normales. Para defenderse de estos ataques el firewall controla la velocidad de los paquetes HTTP por interfaces

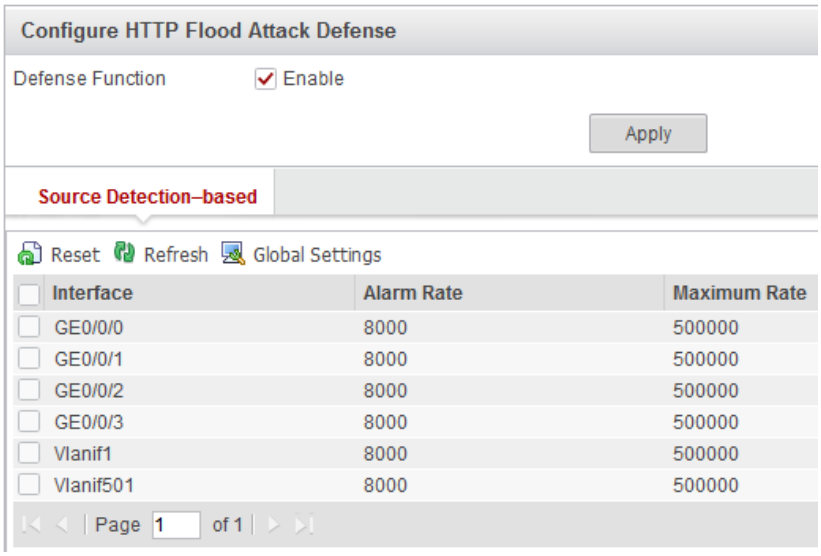


Figura 4.27: Protección con ataques HTTP Flood

4.8.1.7. Conexiones flood

El ataque consiste en crear conexiones completas TCP sin subsecuencias de paquetes, consumiendo los recursos del atacado. Las conexiones TCP completas sin transmisiones de paquetes se considera como una conexión anormal, y la defensa consiste en limitar el número de conexiones anormales.

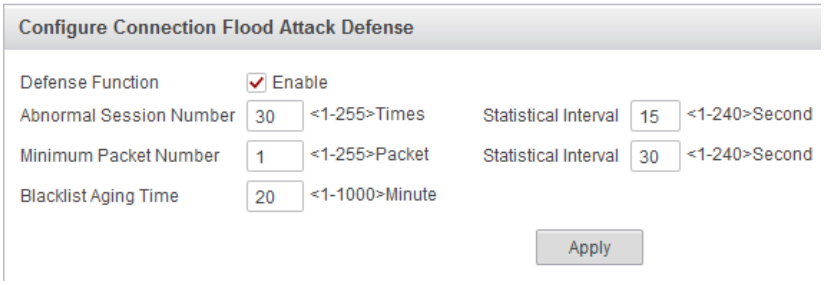


Figura 4.28: Protección por inundación de paquetes

4.8.1.8. SCAN

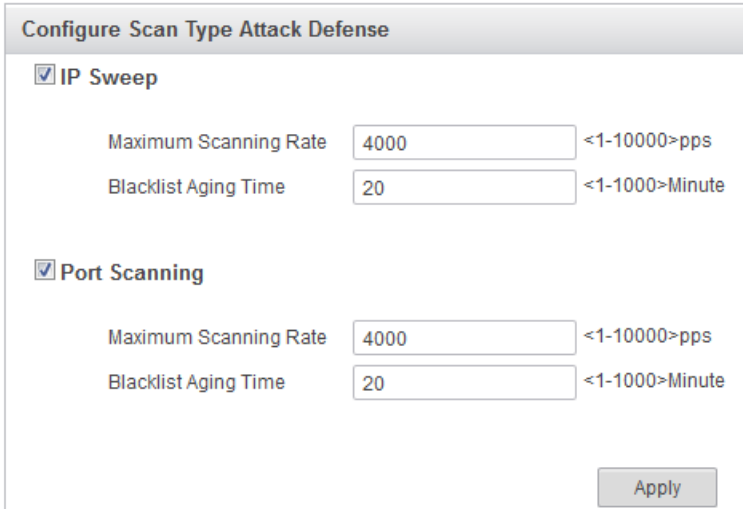


Figura 4.29: Protección de detección de puertos

Este ataque principalmente incluye escaneo de direcciones IP y puertos. En un ataque de barrido a una dirección IP el atacante envía paquetes IP TCP, UDP, ICMP para verificar si hay cambios y encontrar hosts y redes existentes. De esta manera, los objetivos potenciales de ataque pueden ser detectados con precisión. El escaneo de puertos TCP y UDP quiere decir que el atacante puede detectar sistema operativo y servicios potencialmente atacados. Mediante la exploración, el atacante más o menos puede aprender los tipos de los servicios que ofrece el sistema y las posibles vulnerabilidades de seguridad, para prepararse para una mayor intrusión en el sistema de destino.

4.8.1.9. Malformaciones de paquetes

En un atacante de paquetes mal formados, el atacante envía paquetes IP defectuosos al sistema destino. El sistema destino puedo encontrar errores o bloquear los paquetes si así lo determina. Este tipo de ataques incluye PING de la muerte y ataque de fragmentación

Figura 4.30: Protección contra paquetes mal formados

4.8.1.10. Configuración de paquetes especiales

Es un ataque especial de paquetes, el atacante utiliza paquetes legítimos para sondear las redes o detectar datos. Los paquetes utilizados son los paquetes de aplicaciones legítimas, pero rara vez se utilizan en las redes

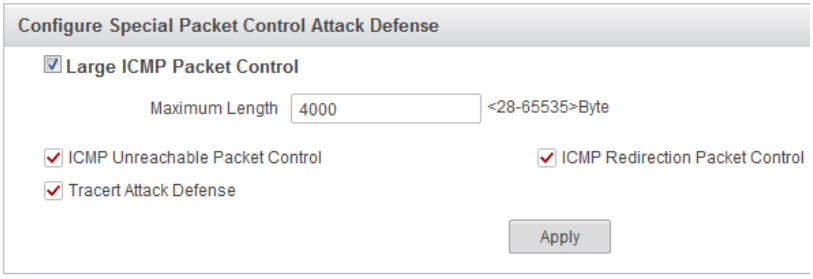


Figura 4.31: Protección de paquetes especiales

4.8.2. BlackList

Después de habilitar esta función, al percibir un intento de ataque por parte del usuario con una dirección IP específica, de acuerdo con el comportamiento de los paquetes, el sistema añade automáticamente la dirección IP a la lista negra y filtra los paquetes enviados desde esta dirección IP para proteger la red.

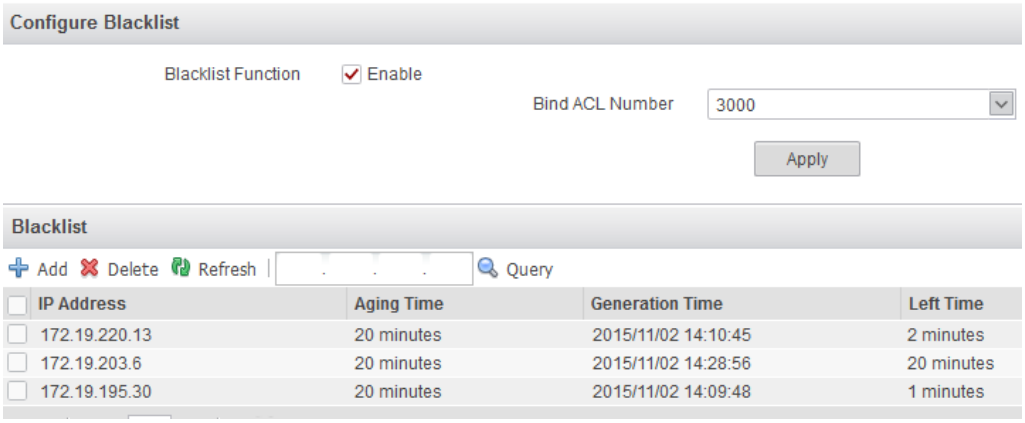


Figura 4.32: Protección contra listas negras.

Las direcciones IP calificadas en listas negras tienen un tiempo de 20min de envejecimiento que permanece bloqueo, que después de eso se liberan automáticamente. Se configura una ACL asociada a la acción que va a realizar, para el ejemplo se incluye la 3000 que tiene la política 5 que bloquea todo el tráfico

4.8.3. WhileList

.

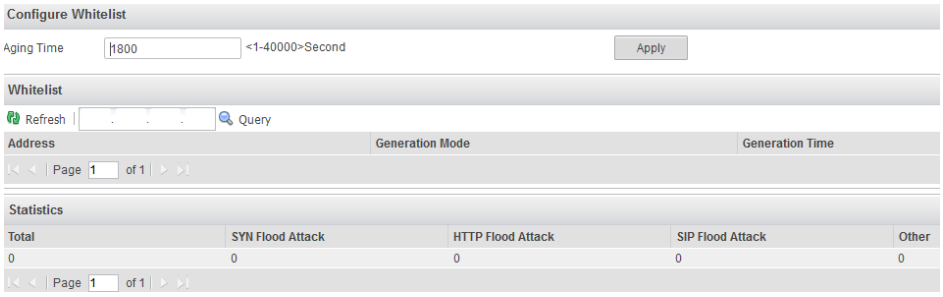


Figura 4.33: Lista blanca analizadas en SYN, HTTP y SIP

Es utilizada en la defensa de los ataques de inundaciones: SYN, HTTP, SIP. Después de recibir un ataque de paquetes y se verifica el origen la legitimidad de la dirección IP. Si la dirección

IP es legítima, se añade a la WhileList, caso contrario se descarta

4.8.4. IP-MAC Binding

La dirección MAC está asociada una dirección IP, si se recibe una IP con otra dirección MAC el paquete es descartado. Cuando un paquete es enviado a una dirección IP se forza el envío a la dirección MAC registrada, ver figura

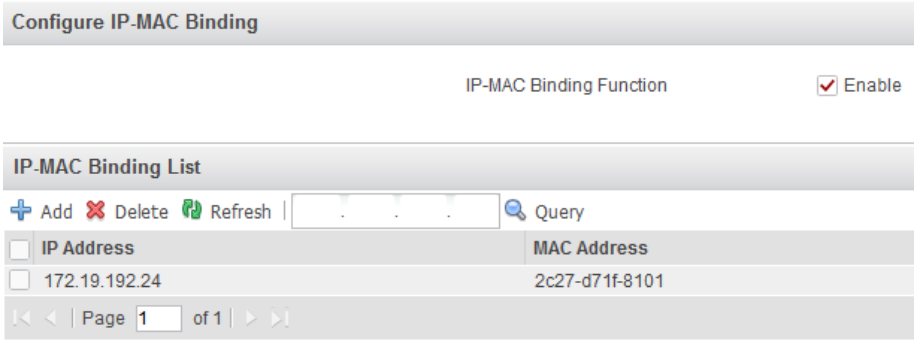


Figura 4.34: protección IP-MAC Binding, asocia IP con MAC

CAPÍTULO 5

DESARROLLO DE LAS PRUEBAS DE VULNERABILIDAD

5.1. Desarrollar pruebas de vulnerabilidad.

Debido al rol desempeñado en la jefatura de tecnología de la UN Los Ríos, la experiencia alcanzada por los años de trabajo y el conocimiento adquirido de toda la organización, se considera que el tipo de hacking que se va a realizar es del tipo caja blanca.

Las pruebas se realiza desde un computador de escritorio ubicado en el edificio principal de la UN Los Ríos, conectado a un switch de acceso, en cascada con el switch de CORE, cuyo puerto está configurado con la VLAN's 105.

Este computador tiene funcionalidades de servidor de máquinas virtuales, con el sistema operativo ESXi VMWare ESXi 6.0.0, 3029758 que contiene las siguientes máquinas virtuales:

- Kali Linux: Incluye programa de auditoría y seguridad informática.
- pfSense: Distribución de FreeBSD para uso de firewall y router.
- Windows XP: Máquina de prueba de las herramientas de Kali Liux.

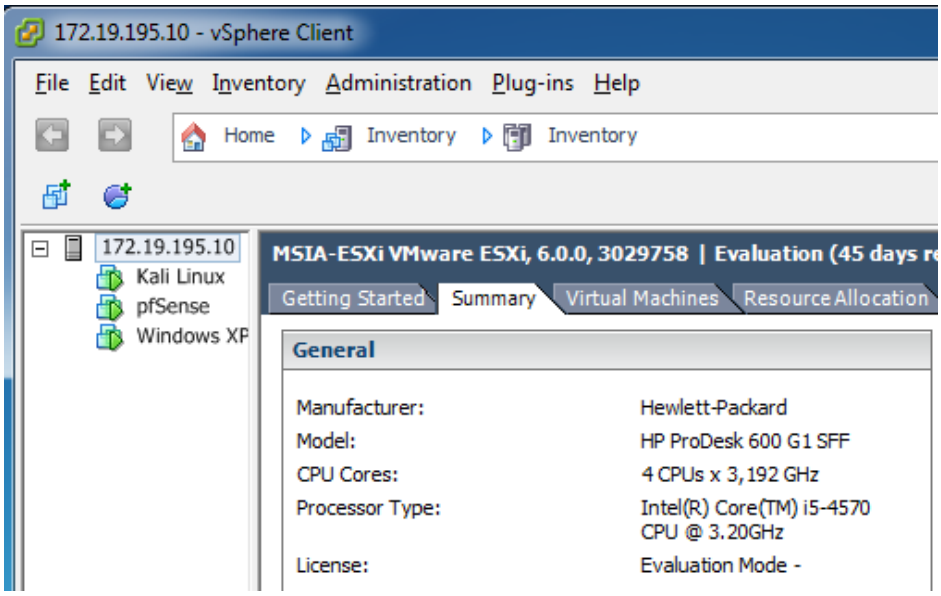


Figura 5.1: Entornos virtuales con herramientas de pruebas

A continuación se detalla los resultados encontrados por fase del pentesting.

5.1.1. Fase de reconocimiento o Footprint

Después de definir la matriz de riesgo se ha definido los activos más importantes de la UN Los Ríos, y se detalla las direcciones IP.

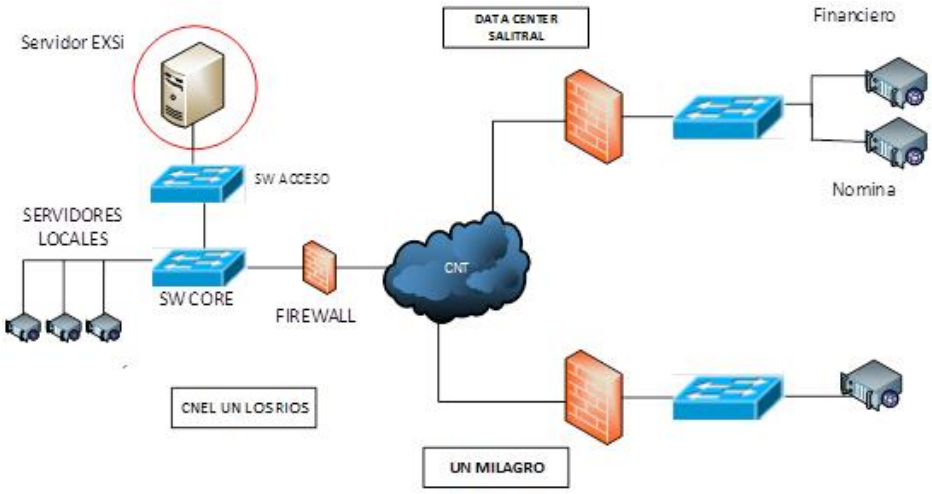


Figura 5.2: Esquema de red de pruebas de vulnerabilidad

Tabla 7: Activos definidos en la matriz de riesgo

Nro	Activo
1	Firewall UN
2	Switch de CORE UN
3	Servidor Comercial prepago UN
4	Servidor Comercial UN
5	Servidor Financiero CNEL EP
6	Servidor Nómina CNEL EP
7	Servidor Directorio Activo

5.1.2. Fase de escaneo y enumeración.

- *nmap*: determinar los puertos abiertos, los programas asociados a esos puertos, sistema operativo
- *nexpose nessus*: Buscar las vulnerabilidades asociados a las aplicaciones asociadas a las aplicaciones de los puertos abiertos
- *nkito*: Busca vulnerabilidades sql injection en aplicaciones web.

5.1.2.1. Firewall:

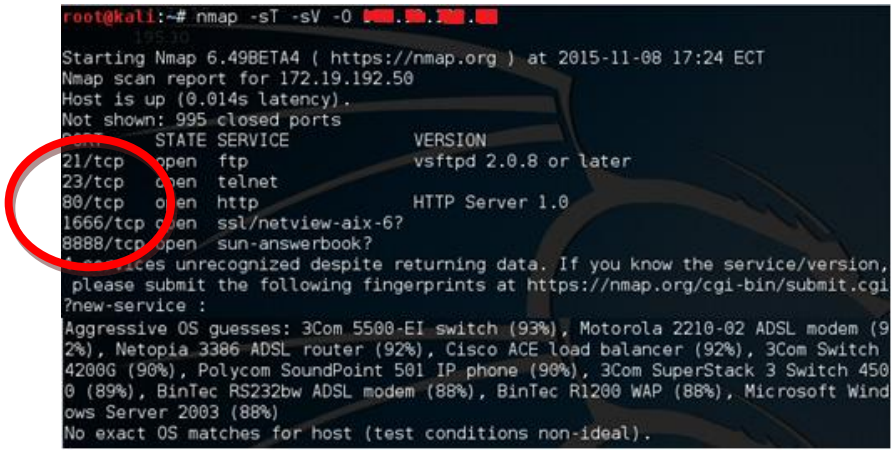
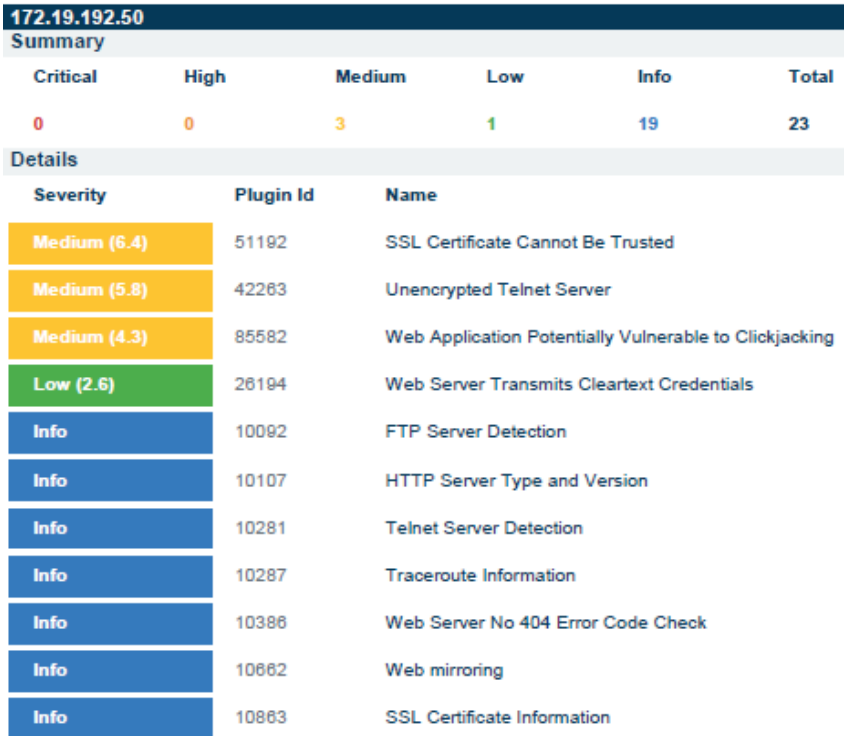


Figura 5.3: *nmap* listando puertos y SO del firewall



172.19.192.50

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	1	19	23

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.8)	42263	Unencrypted Telnet Server
Medium (4.3)	85582	Web Application Potentially Vulnerable to Clickjacking
Low (2.6)	26194	Web Server Transmits Cleartext Credentials
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	10386	Web Server No 404 Error Code Check
Info	10662	Web mirroring
Info	10863	SSL Certificate Information

Figura 5.4: Vulnerabilidades firewall detectadas X *nessus*

5.1.2.2. SWITCH DE CORE:

Figura 5.5: *nmap* listado de puertos y SO del SW CORE

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	9	10

Details

Severity	Plugin Id	Name
Medium (5.8)	42263	Unencrypted Telnet Server
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information

Figura 5.6: *nessus* vulnerabilidades del SW CORE

5.1.2.3. Servidor comercial prepago de la UN

Summary

Critical	High	Medium	Low	Info	Total
1	0	6	1	25	33

Details

Severity	Plugin Id	Name
Critical (10.0)	73182	Microsoft Windows XP Unsupported Installation Detection
Medium (5.8)	42263	Unencrypted Telnet Server
Medium (5.8)	50686	IP Forwarding Enabled
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-th Weakness
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10281	Telnet Server Detection
Info	10287	Traceroute Information
Info	10342	VNC Software Detection
Info	10394	Microsoft Windows SMB Log In Possible

Figura 5.7: *nessus* vulnerabilidades del Prepago

```
root@kali:~# nmap -sT -sV -O [redacted]

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-08 18:27 ECT
Nmap scan report for 172.19.192.23
Host is up (0.00032s latency).
Not shown: 992 closed ports
PORT     STATE SERVICE       VERSION
23/tcp   open  telnet        Microsoft Windows XP telnetd
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows 98 netbios-ssn
211/tcp  open  914c-g?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
3389/tcp open  ms-wbt-server Microsoft Terminal Service
5800/tcp open  vnc-http      RealVNC E4
5900/tcp open  vnc           RealVNC Enterprise (protocol 4.1)
Device type: general purpose
Running: Microsoft Windows XP|2003
OS CPE: cpe:/o:microsoft:windows_xp cpe:/o:microsoft:windows_server_2003
OS details: Microsoft Windows XP SP2 or SP3, or Windows Server 2003, Microsoft W
indows XP SP2 or Windows Server 2003 SP2
```

Figura 5.8: *nmap* puertos y SO del Prepago

Tabla 8: Vulnerabilidades encontradas por nessus en Prepago

Vulnerabilidad	Nivel Riesgo	Explotable	Observaciones
Sin soporte por el Vendedor	Alto	No	Microsoft Windows XP no tiene soporte

5.1.2.4. Servidor Comercial

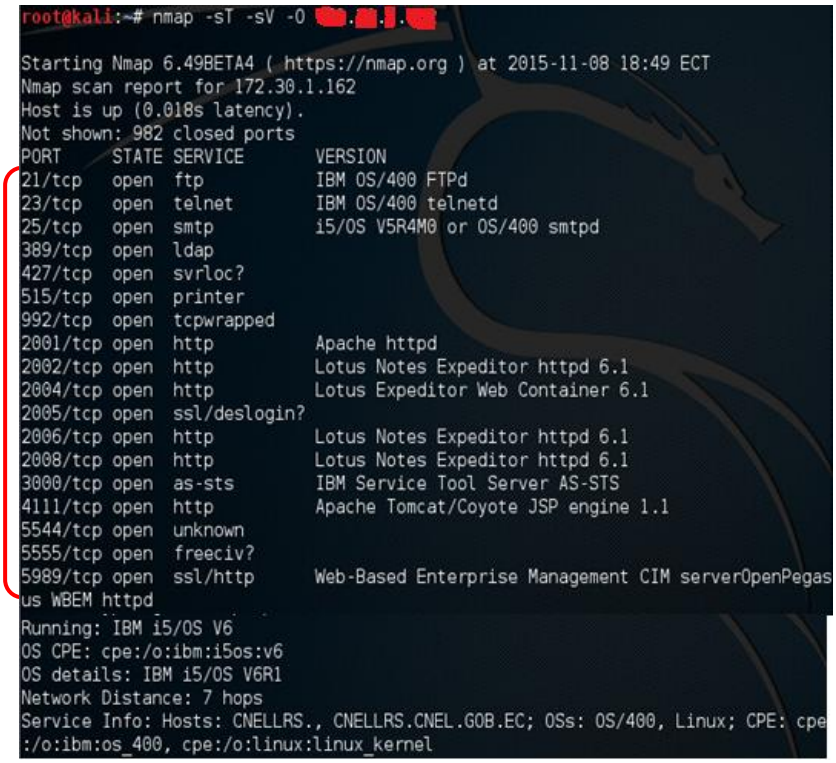


Figura 5.9: *nmap* puertos y SO del Servidor Comercial

El *nmap* no puede determinar el sistema operativo del servidor Comercial, pero sí los puertos que se encuentran abiertos.

Summary

Critical	High	Medium	Low	Info	Total
0	0	12	0	25	37

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.0)	10722	LDAP NULL BASE Search Access
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	81606	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)
Medium (4.3)	26928	SSL Weak Cipher Suites Supported
Medium (4.3)	42873	SSL Medium Strength Cipher Suites Supported
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	83738	SSL/TLS EXPORT_DHE <= 512-bit Export Cipher Suites Supported (Logjam)
Medium (4.3)	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Info	10092	FTP Server Detection
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure

Figura 5.10: *nessus* vulnerabilidades del SRV Comercial

5.1.2.5. Servidor Financiero de CNEL EP

```
root@kali:~# nmap -sT -sV -O [redacted]

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-08 19:01 ECT
Nmap scan report for cgweb-app.cnel.gob.ec (172.30.1.41)
Host is up (0.0092s latency).
Not shown: 984 closed ports
PORT      STATE SERVICE       VERSION
80/tcp    open  http          Microsoft IIS httpd 7.5
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows 98 netbios-ssn
445/tcp   open  microsoft-ds  (primary domain: CORPCNEL)
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2012
1801/tcp  open  msmq?
2103/tcp  open  msrpc         Microsoft Windows RPC
2105/tcp  open  msrpc         Microsoft Windows RPC
2107/tcp  open  msrpc         Microsoft Windows RPC
2383/tcp  open  ms-olap4?
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
8080/tcp  open  http          Microsoft IIS httpd 7.5
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49161/tcp open  msrpc         Microsoft Windows RPC
Running: Microsoft Windows Vista
OS CPE: cpe:/o:microsoft:windows_vista::- cpe:/o:microsoft:windows_vista::spl
OS details: Microsoft Windows Vista SP0 - SP1
```

Figura 5.11: *nmap* puertos y SO del Servidor Financiero

Summary

Critical	High	Medium	Low	Info	Total
0	0	12	2	39	53

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	20007	SSL Version 2 and 3 Protocol Detection
Medium (5.0)	45411	SSL Certificate with Wrong Hostname
Medium (5.0)	57608	SMB Signing Required
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Medium (4.3)	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
Medium (4.3)	85582	Web Application Potentially Vulnerable to Clickjacking
Medium (4.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Low	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure

Figura 5.12: *nessus* vulnerabilidades del SRV Financiero

5.1.2.6. Servidor Nómina de CNEL EP

```
root@kali:~# nmap -sT -sV -O [redacted]

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-08 18:57 ECT
Nmap scan report for 172.30.1.193
Host is up (0.0097s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 5.3 (protocol 2.0)
80/tcp open  http    Apache httpd 2.2.15
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.32
Network Distance: 7 hops
Service Info: Host: n0.polux.cnel
```

Figura 5.13: *nmap* puertos y SO del Servidor Nómina

Summary

Critical	High	Medium	Low	Info	Total
0	0	2	2	12	16

Details

Severity	Plugin Id	Name
Medium (6.8)	12085	Apache Tomcat servlet/JSP container default files
Medium (4.3)	85582	Web Application Potentially Vulnerable to Clickjacking
Low (2.6)	26194	Web Server Transmits Cleartext Credentials
Low (2.6)	34850	Web Server Uses Basic Authentication Without HTTPS
Info	10662	Web mirroring
Info	11032	Web Server Directory Enumeration
Info	11219	Nessus SYN scanner
Info	20108	Web Server / Application favicon.ico Vendor Fingerprinting
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	33817	CGI Generic Tests Load Estimation (all tests)
Info	39470	CGI Generic Tests Timeout
Info	42057	Web Server Allows Password Auto-Completion
Info	43111	HTTP Methods Allowed (per directory)
Info	47830	CGI Generic Injectable Parameter

Figura 5.14: *nessus* vulnerabilidades del SRV Nómina

5.1.2.7. Directorio Activo

```
root@kali:~# nmap -sT -sV -O [redacted]

Starting Nmap 6.49BETA4 ( https://nmap.org ) at 2015-11-08 20:20 ECT
Nmap scan report for 172.18.200.232
Host is up (0.0094s latency).
Not shown: 984 filtered ports
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Microsoft DNS 6.1.7601
88/tcp    open  kerberos-sec  Windows 2003 Kerberos (server time: 2015-11-09 01:
20:33Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn?
389/tcp   open  ldap?
445/tcp   open  microsoft-ds  (primary domain: CORPCNEL)
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap
3269/tcp  open  tcpwrapped
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49157/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49159/tcp open  msrpc         Microsoft Windows RPC
Running: Microsoft Windows 2008|Phone|Vista|7
OS CPE: cpe:/o:microsoft:windows_server_2008::beta3 cpe:/o:microsoft:windows_ser
ver_2008 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_vista::- cpe:/o:micro
soft:windows_vista::sp1 cpe:/o:microsoft:windows_7
OS details: Microsoft Windows Server 2008 or 2008 Beta 3, Windows Server 2008 R2
, Microsoft Windows Phone 7.5 or 8.0, Microsoft Windows Vista SP0 or SP1, Window
s Server 2008 SP1, or Windows 7, Microsoft Windows Vista SP2, Windows 7 SP1, or
Windows Server 2008
Service Info: Host: MLGSRV-CD02; OS: Windows; CPE: cpe:/o:microsoft:windows, cpe
:/o:microsoft:windows_server_2003
```

Figura 5.15: *nmap* puertos y SO del Directorio Activo

Summary

Critical	High	Medium	Low	Info	Total
0	0	7	1	35	43

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (6.4)	57582	SSL Self-Signed Certificate
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
Medium (5.0)	12217	DNS Server Cache Snooping Remote Information Disclosure
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Medium (4.3)	58453	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
Medium (4.3)	65821	SSL RC4 Cipher Suites Supported (Bar Mitzvah)
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10863	SSL Certificate Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	10940	Windows Terminal Services Enabled
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection

Figura 5.16: *nessus* vulnerabilidades del Directorio Activo

En el anexo 1 se puede resumir todas las pruebas realizadas a todos los activos, el sistema operativo, el nombre del equipo, los puertos abiertos clasificados como TCP o UDP, la versión de las aplicaciones abiertas, el tipo de riesgo, si son explotables o no y algunas observaciones.

Tabla 9: Vulnerabilidades en los activos de la UN Los Ríos

Nombre	Plataforma del Sistema Operativo detectada	Vulnerabilidades			
		Críticas	Altas	Medias	Baja
Servidor Comercial	IBM i5/OS V6	0	0	12	0
Servidor RR.HH	Linux 2.6.3	0	0	1	2
Servidor Financiero	Windows 2008 Server	0	0	15	2
Servidor Directorio Activo	Windows 2008 Server	0	0	7	1
Sistema comercial prepago	Windows XP	1	0	2	0
Firewall	VRP Version 5.30				
Switch de CORE	Quidway V200R001C00PC300				
	TOTAL	1	0	37	5

5.2. Medir el riesgo y calcular el impacto generado.

Para medir el riesgo se deberían comparar los niveles de riesgo frente a los criterios para la evaluación del riesgo y sus criterios de aceptación.

Las decisiones como la evaluación del riesgo, se basan en el nivel aceptable de riesgo. Sin embargo hay que considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo. La agrupación de variados riesgos bajos o medios puede dar como resultado riesgos globales mucho más altos y es necesario tratarlos según corresponda.

La evaluación del riesgo se obtiene mediante el análisis del riesgo para la toma de decisiones sobre acciones futuras.

Al final se obtiene un listado de riesgos con prioridad de acuerdo con los criterios de evaluación del riesgo, con proporción a los escenarios de incidente que llevan a tales riesgos y se evalúa las consecuencias

como son la pérdida de la disponibilidad, confidencialidad y la integridad.

5.2.1. Servidor Comercial

Pérdida de la disponibilidad

Se genera cuando el único proveedor de servicio ISP de los enlaces de datos y de Internet se cae la comunicación en el Data Center, los procesos de recaudación se paralizaba tanto en las ventanillas de CNEL EP como en el sistema financiero, llegando a producir hasta una pérdida económica de hasta un día de recaudación.

Pérdida de la integridad

Debido a la deficiencia del sistema comercial fue necesario desarrollar aplicaciones que genere reportes para los organismos de control, donde es necesario tener acceso directo con la base de datos, creando tablas y procedimientos almacenados. Por la falta de un ambiente de prueba, se cometieron “errores” de buena fe, borrando gran parte la información de los clientes.

Pérdida de la confidencialidad

Debido al cambio de la matriz productiva promovida por el gobierno nacional, que fomenta la adquisición de las cocinas de inducción eléctrica, algunas empresas vendedoras de electrodomésticos “consiguieron” copias de la base de datos de

los clientes de CNEL EP y del MIES, para chantajear a las personas que cobran el bono de desarrollo humano BDH, obligándolas a firmar documentos, certificando que han adquirido la cocina.

5.2.2. Servidor Comercial Prepago

Pérdida de la disponibilidad

El UPS instalado en el data center local de la UN, suministra energía no solo al área de servidores, sino a equipos de otras áreas de trabajo, pero debido al crecimiento de la infraestructura de tecnología, este UPS no soporta la carga actual, dejando de funcionar después de media hora de uso ininterrumpido.

Pérdida de la integridad

Debido que la aplicación fue desarrollada en Windows XP para generar códigos de seguridad a través de hardware adicional, el servidor instalado en un computador de escritorio no cuenta con un sistema redundante de almacenamiento como son los RAID

Pérdida de la confidencialidad.

La recaudación prepago funciona con un software en modo cliente – servidor. En el servidor debe de ejecutarse manualmente el programa y el cliente corre en cualquier

computador que se encuentre instalado el programa. Debido a la falta de autenticación con certificados digitales, las claves de acceso de los clientes y servidor son transmitidas en texto plano.

5.2.3. Servidor Financiero

Pérdida de la disponibilidad

Debido al uso concurrente de la aplicación web en todas las UN y por agregar los módulos de activos fijos y bodega, los recursos asignados al servidor virtual no son suficientes, generando problemas de cumplimiento ante los organismos de control.

Pérdida de la integridad

La información almacenada en la base de datos, puede sufrir alteraciones en el almacenamiento de la data generado por pequeños bajones de voltaje indetectables por el UPS, que no logran ser corregidos por el sistema de archivo. Estas inconsistencias en la data almacenada generan alertas en logs de la base de datos, que deben ser supervisados periódicamente por personal técnico para su inmediata corrección.

Pérdida de la confidencialidad

La aplicación WEB se ejecuta sobre el puerto http y no https, permitiendo capturar fácilmente las credenciales de los

administradores del tráfico en la red de datos, pudiendo causar una pérdida total de la información, alteración o simplemente una copia ilegal de la información para usos no identificados, que pudiera causar un daño moral y/o económica sin precedentes.

5.2.4. Servidor Nómina

Pérdida de la disponibilidad

Debido a los procesos de ejecución del cálculo de la nómina del rol de pago, generada en dos periodos mensuales, realizada concurrente en todas las UN, el servidor experimentaba una saturación en su rendimiento, causando la indisponibilidad del servicio, generando retrasos en el procesamiento de la información y por consiguiente retraso en la entrega de la información, causando multas ante organismos de control como el IESS

Pérdida de la integridad

Debido a la limitación del recurso humano en UN pequeñas, una misma persona puede estar asociada con varios roles, entre ellos administrador de base de datos, programador y jefe de la sección, sin que exista un control de cambios y una auditoría de los datos, se presta para manipular la información y alterar los roles de pago para su beneficio personal.

Pérdida de la confidencialidad

Debido que la aplicación web transmite las credenciales en texto plano y el acceso remoto utiliza certificados vulnerables, fácilmente se pueden capturar las credenciales en la red de datos con la finalidad de manipular el servidor, hacer copias de programas fuentes, base de datos o simplemente hacer réplicas para usos no definidos con potenciales daños hacia la institución.

5.2.5. Servidor Directorio Activo

Pérdida de la disponibilidad

Debido a la cantidad de usuarios que tienen que logonearse diariamente contra el servidor del directorio Activo, el servidor no podría atender oportunamente los requerimientos de cada usuario, generando largos periodos de tiempo de espera.

Pérdida de la confidencialidad

Debido que el eslabón más débil de la cadena de seguridad no son los equipos ni los programas informáticos, sino que son las personas, y aprovechando la vulnerabilidad del tipo de autenticación de los usuarios, basado en “algo que el usuario sabe” que es la clave, fácilmente se puede utilizar cualquier terminal para conseguir acceso a la administración del servidor del directorio activo y utilizar el listado de los usuarios como

fuente de información para probar estos usuarios en futuros ataques a otros sistemas de CNEL EP.

5.2.6. Firewall

Pérdida de la disponibilidad

Debido que existe un único firewall en la UN, existe la probabilidad que pueda fallar y dejar de operar toda la UN por no tener contingencia, causando serios problemas administrativos, operacionales y financieros.

5.2.7. Switch de CORE

Pérdida de la disponibilidad

Son las mismas consideraciones que el firewall, si se tiene un punto de falla, se requiere tener contingencia, debido que el riesgo y el impacto son altos.

Esta matriz de riesgo, se generó basado a la encuesta realizada al equipo de tecnología de la UN Los Ríos, donde se promedió las opiniones de los cuatro técnicos.

5.3. Medir los tiempos de repuesta para bloquear a usuarios.

El análisis de este ítem tiene como objetivo calcular el tiempo mínimo que requiere un técnico, para bloquear completamente a una persona de CNEL EP, todos los accesos a todos los sistemas de información,

incluyendo los equipos terminales como computadoras o dispositivos móviles.

Tabla 10: Evaluación de la matriz de riesgo

Nro	Riesgo Inherente		Riesgo Residual		Riesgo Residual Deseado	
	Probabilidad	Impacto	Probabilidad	Impacto	Probabilidad	Impacto
1	4	3	2	2		
2	2	1	1	1		
3	5	2	1	1		
4	4	1	3	1		
5	2	3	2	3	1	1
6	2	1	1	1		
7	4	1	2	1		
8	3	3	1	1		
9	2	4	1	1		
10	5	2	4	1	1	1
11	2	1	1	1		
12	2	2	1	1		
13	4	1	2	1		
14	3	1	1	1		
15	2	3	1	1		
16	2	3	1	1		

Considerando que no existe un usuario único válido para todos los Sistemas de Información, y que se han creados usuarios sin control no homologados por cada aplicativo, se debe de proceder a bloquear manualmente cada usuario creado en cada sistemas asociado a una persona que se desea bloquear. La mayoría de los usuarios se bloquean remotamente a través del mismo sistemas de información, pero existen sistemas que no permiten hacer esta acción remotamente, debido que el proceso de alta, modificación o eliminación debe de hacerse en directamente en el dispositivos físicos, como es el caso de

las huellas dactilares, registradas en los relojes biométricos instalados en cada agencia.

Para calcular el tiempo de bloqueo, se toma como ejemplo un caso real presentado en la UN Los Ríos, donde la gerencia solicitó anular todos los accesos a un trabajador que se desempeñaba como programador en el área de tecnología con privilegios de administrador, debido que su contrato se da por terminado de forma unilateralmente por mantener diferencias de criterio con el administrador.

En esa tarde se procedió a bloquear todos los usuarios relacionados con el trabajador, incluido las huellas dactilares, y se cambió las claves en los servidores que el administraba.

El problema se detectó al siguiente día, dos aplicaciones dejaron de funcionar inmediatamente después de bloquear los usuarios del programador. Se revisó el código fuente de las dos aplicaciones y se encontró, que la causa del problema se debía, que había usado una de los usuarios bloqueados, que servía para autenticarse con la base de datos desde la aplicación. Se soluciona el problema después de una semana, se volvió a compilar las aplicaciones y se soluciona el inconveniente.

Debido este antecedente es necesario tomar consideraciones especiales en la desvinculación del personal de tecnología, creando

políticas en la GTI o GSI que permitan implementar procedimiento de controles más afectivo y evitar contratiempos.

Tabla 11: Tiempo empleado para bloquear un empleado de CNEL EP.

Nro	Sistema de Información	Tiempo (min)
1	Bloqueo del usuario del Directorio Activo	5
2	Bloqueo del usuario del Correo Electrónico	5
3	Bloqueo de usuario del reloj biométrico	5
4	Bloqueo de la IP asignada al computador	20
5	Bloqueo del puerto de red asociado al computador	30
6	Cambio de clave administrador en servidores locales	10
7	Cambio de clave del usuario utilizado en aplicaciones	2,400
TOTAL		2,475

Debido a la experiencia adquirida, se propusieron cambios en el desarrollo de aplicaciones de la UN, donde las credenciales utilizadas para logonearse son las definidas en el directorio activo y el acceso hacia la base de datos depende del perfil del usuario asociado al Sistema de Información. Cabe aclarar que no todos los sistemas de información soportan este esquema de trabajo y se ha optado por utilizar los mismos usuarios creados por los sistemas de información ya creados.

El bloqueo en el directorio activo y el switch son procesos manuales. Para bloquear un usuario en el switch de acceso o un Access Point, se debe de identificar la localidad Edificio Agencia o Subestación, el switch y puerto.

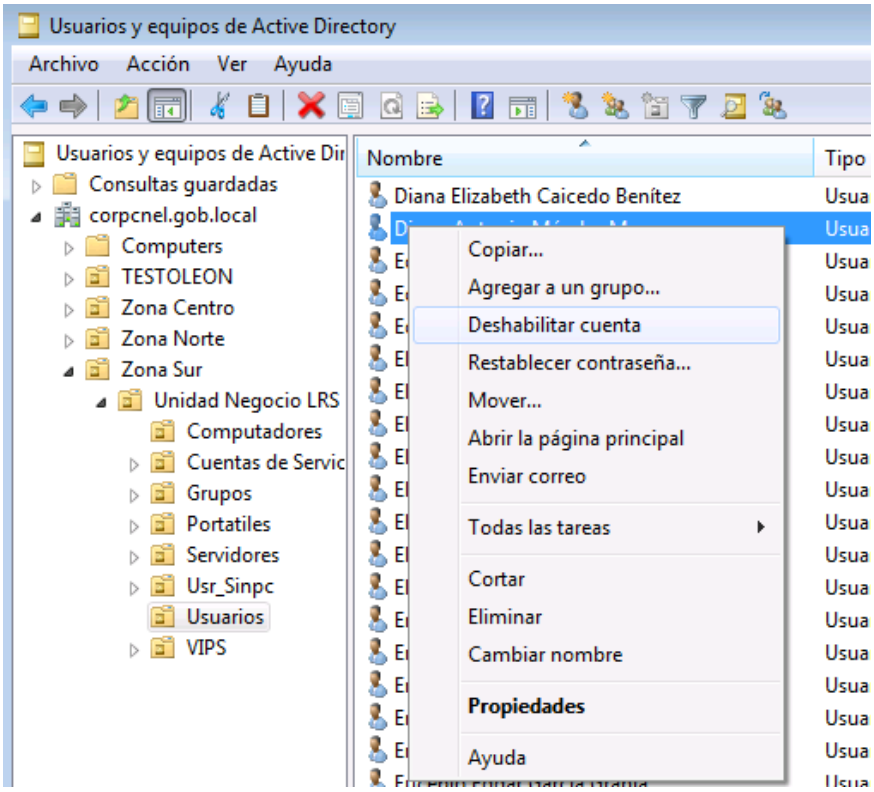


Figura 5.17: Bloqueo de un usuario en el Directorio Activo

Figura 5.18: Bloqueo lógico de interface de red

5.4. Evaluar la infraestructura de red y medidas defensivas.

Una vez corregidas las vulnerabilidades detectadas inicialmente, se vuelve a ejecutar los test para verificar que hayan sido mitigadas.

5.4.1. Firewall

Debido que a las vulnerabilidades encontradas en los puertos ftp, telnet y web, se procedió a deshabilitar estos servicios, tal como se muestra en las pruebas elaboradas por el *nmap* y *nessus*

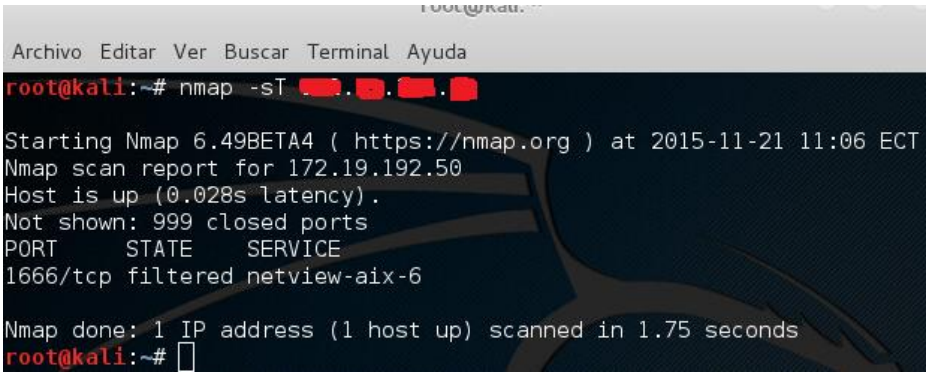


Figura 5.19: *nmap* muestra el puerto filtrado en el Firewall

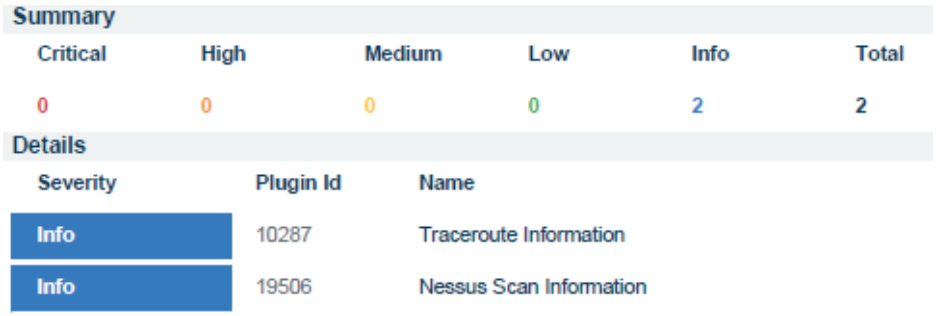


Figura 5.20: *nessus* no muestra vulnerabilidades en el Firewall

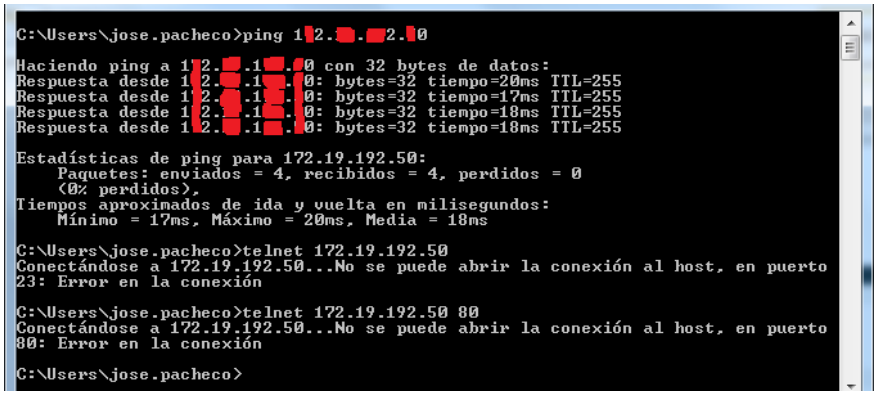


Figura 5.21: *Telnet* deshabilitado en el Firewall

5.4.2. Switch de CORE

El servicio http se considera seguro debido que genera patrones de códigos al azar. El servicio *telnet* tal como se muestra en la siguiente figura, se mantiene los accesos *consola* y el *http*

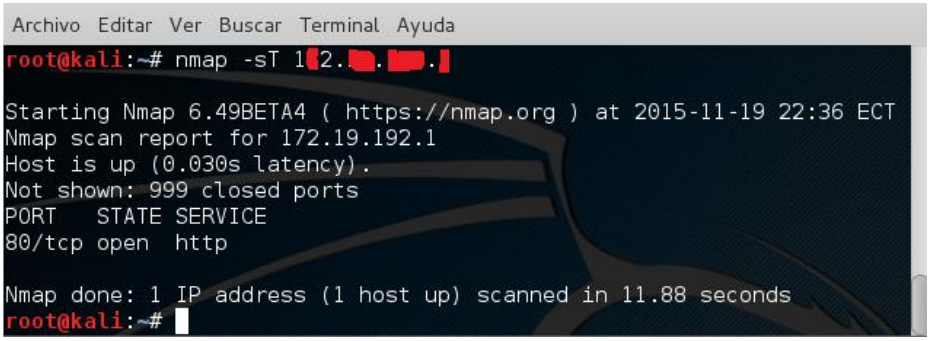


Figura 5.22: *nmap* solo muestra el puerto 80 en el SW CORE

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	9	9

Details

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	19506	Nessus Scan Information
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	45590	Common Platform Enumeration (CPE)

Figura 5.23: *nessus* no detecta vulnerabilidades en el SW CORE

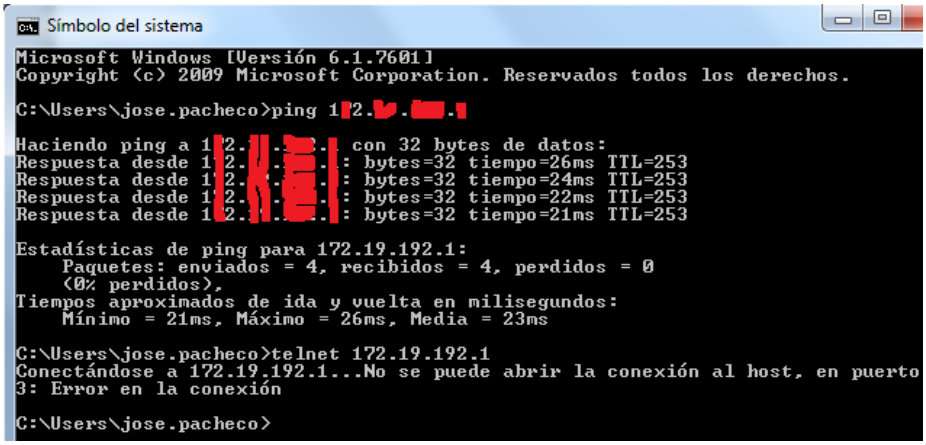


Figura 5.24: *telnet* desactivado el servicio en el SW CORE

5.4.3. Servidor comercial prepago

El servidor comercial prepago, es un computador de escritorio con sistema operativo Windows XP que actualmente no tiene soporte del fabricante.

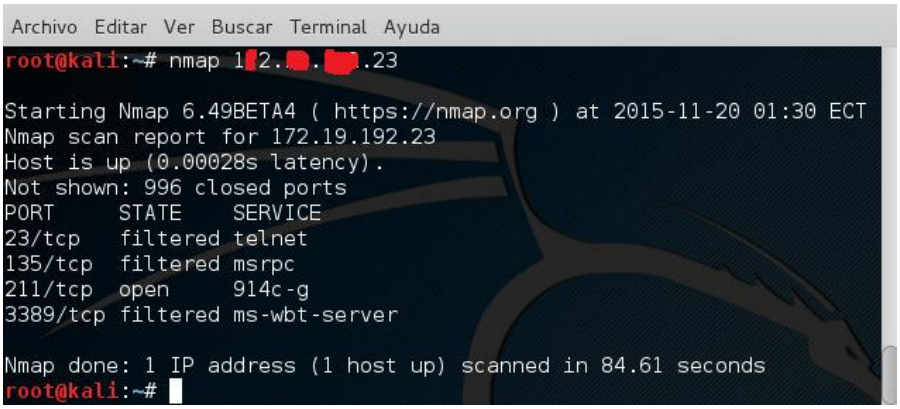
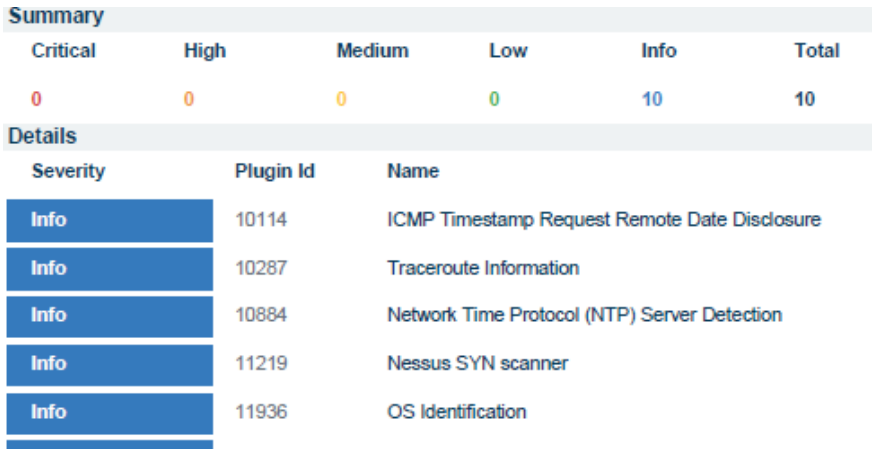


Figura 5.25: *nmap* puertos filtrados del SRV Comercial Prepago

Se corrigieron los problemas detectados en la fase anterior, modificando el registro del sistema manualmente y parchando el sistema operativo.

Se activó el cortafuego de Windows y se agregó la excepción del puerto 211. El resto de los puertos se los filtran en el firewall de la UN.



Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	10	10

Details

Severity	Plugin Id	Name
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification

Figura 5.26: *nessus* no detecta vulnerabilidades del Prepago

5.4.4. Servidor comercial

El "*Sistema Informático Comercial"* (SICO), desarrollado sobre el servidor IBM Power 700 con sistema operativo AS400, solo requiere abrir el puerto TCP 23 para ejecutar la aplicación como usuario final, tanto los internos de CNEL EP que está disponible en la Intranet, como los externos contratista disponible en el Internet. Los otros puertos son filtrados en el firewall, y estarán abiertos solo para las direcciones IP de la Intranet con origen del personal técnico de CNEL EP que realiza gestión administrativa o para el personal externo contratado para dar mantenimiento especializado remoto como son lo partner autorizados de IBM

En la figura se puede observar que todos los puertos se encuentran filtrados, excepto el puerto TCP 23. En la prueba realizada por el *nessus* refleja que se ha mitigado las vulnerabilidades clasificadas como medianas y bajas.

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	13	13

Details

Severity	Plugin Id	Name
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10287	Traceroute Information
Info	11153	Service Detection (HELP Request)
Info	11219	Nessus SYN scanner

Figura 5.27: *nessus* no detecta vulnerabilidades del Comercial

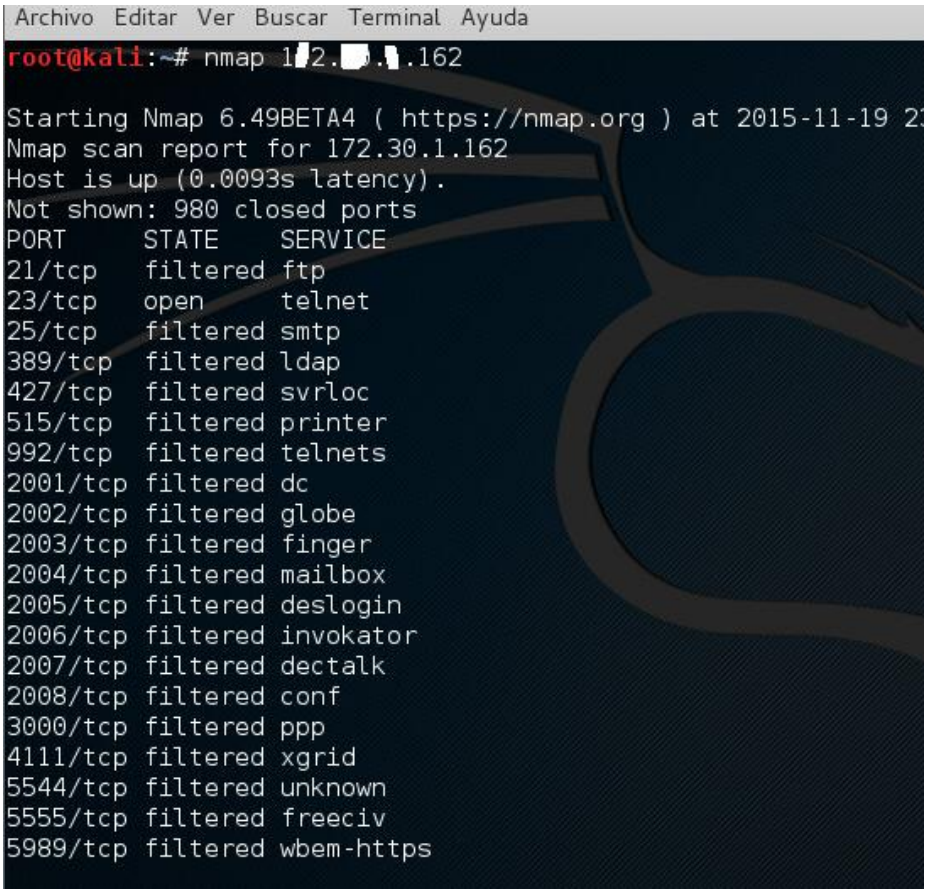


Figura 5.28: *nmap* muestra puertos filtrados del SRV Comercial

5.4.5. Servidor financiero

Debido que el servidor financiero se encuentra en el Data Center corporativo y la responsabilidad del mantenimiento y soporte de segundo nivel depende de la GTI, se solicitó a través de correo electrónico al personal técnico de la Oficina Central que proceda a corregir las vulnerabilidades detectadas en el anterior test de vulnerabilidades. Esta test fue supervisado por la GSI y corroboró lo indicado, tal como se muestra en el correo electrónico generado con fecha anexo 3. Ahora que se corrió nuevamente el

test se evidencia que se ha corregido todas las vulnerabilidades medianas y bajas, exceptuando una mediana a través de filtrado en el firewall, tal como se muestra en el mapeador de puertos *nmap*. Los puertos que no son necesarios para su ejecución son filtrados en el servidor y solo se habilitado el puerto 80 para los usuarios finales

Summary

Critical	High	Medium	Low	Info	Total
0	0	1	0	25	26

Details

Severity	Plugin Id	Name
Medium (4.3)	85582	Web Application Potentially Vulnerable to Clickjacking
Info	10107	HTTP Server Type and Version
Info	10114	ICMP Timestamp Request Remote Date Disclosure
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10674	Microsoft SQL Server UDP Query Remote Version Disclosure
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11422	Web Server Unconfigured - Default Install Page Present
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	22964	Service Detection

Figura 5.29: *nessus* vulnerabilidad mantenida en SRV Financiero

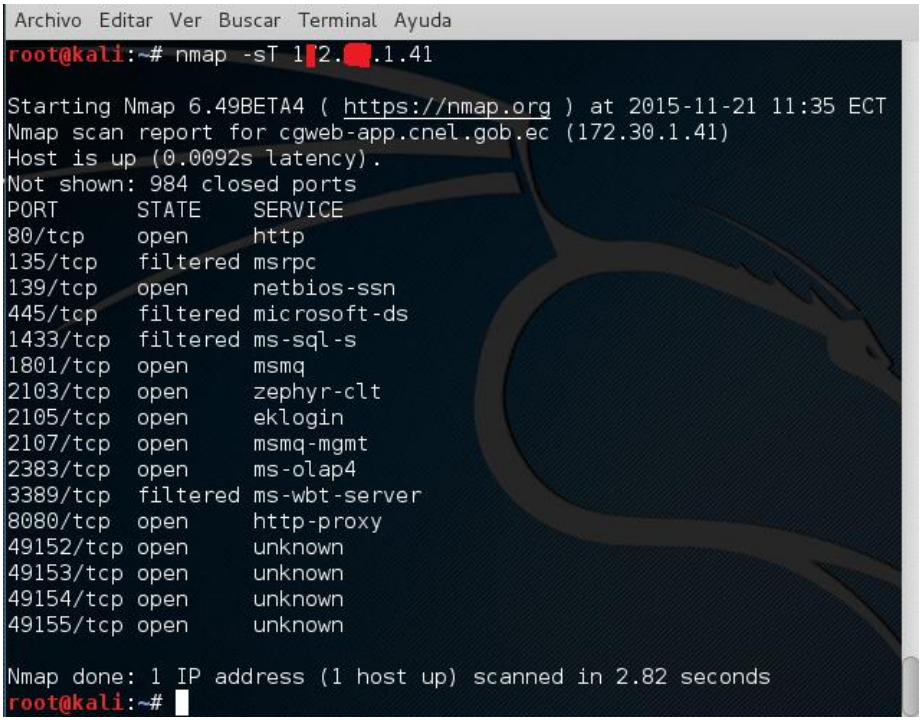


Figura 5.30: *nmap* estado de puertos del SVR Financiero

5.4.6. Servidor nómina

Tal como se explicó en el servidor de nómina, se solicitó al personal técnico de la Oficina Central que proceda a corregir las vulnerabilidades detectadas en el anterior test de vulnerabilidades. Ahora que se corrió nuevamente el test se evidencia que se no se han corregido las vulnerabilidades medianas y bajas; esto representa un problema potencial que será tratado en la siguiente sección.

5.4.7. Servidor directorio activo

Este servidor, al igual que los servidores Financiero y de Nómina, no se encuentran en la UN Los Ríos, por lo que la solución de las

vulnerabilidades corresponde a un técnico encargado de replicar el Directorio Activo para tres UN. De lo revisado se ha corregido todas las vulnerabilidades de riesgo medio y bajo. El tratamiento de las vulnerabilidades se las realizó directamente en el servidor réplica, por lo que los puertos se mantienen abiertos.

Las vulnerabilidades fueron mitigadas en su totalidad, el servidor réplica del Directorio Activo que atienden las peticiones de los usuarios de las UN Milagro, Machala y Los Ríos se ha solucionado complemente.

Summary

Critical	High	Medium	Low	Info	Total
0	0	0	0	25	25

Details

Severity	Plugin Id	Name
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10736	DCE Services Enumeration
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
Info	10884	Network Time Protocol (NTP) Server Detection
Info	11002	DNS Server Detection
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information

Figura 5.32: *nmap* puertos del SRV Directorio Activo

5.5. Identificar el mejor esquema de red que se debe de implementar.

Debido al crecimiento de las UN, la administración del parque informático se vuelve cada vez inmanejable, por lo que se asigna personal de tecnología para realizar procesos de control manuales como: actualizar parches del sistema operativo, validar y actualizar la base de datos del antivirus Kaspersky, controlar el acceso a la red de terminales autorizadas para consumir recursos de la Intranet o el Internet.

Se implementa el NAC (Network Admission Control) que es un framework de dispositivo final, donde deben de existir en cada UN los siguientes servidores: WSUS, antivirus Kaspesrky, RADIUS, etc. Además debe de existir redundancia en los enlaces de datos de las agencias y subestaciones de cada UN

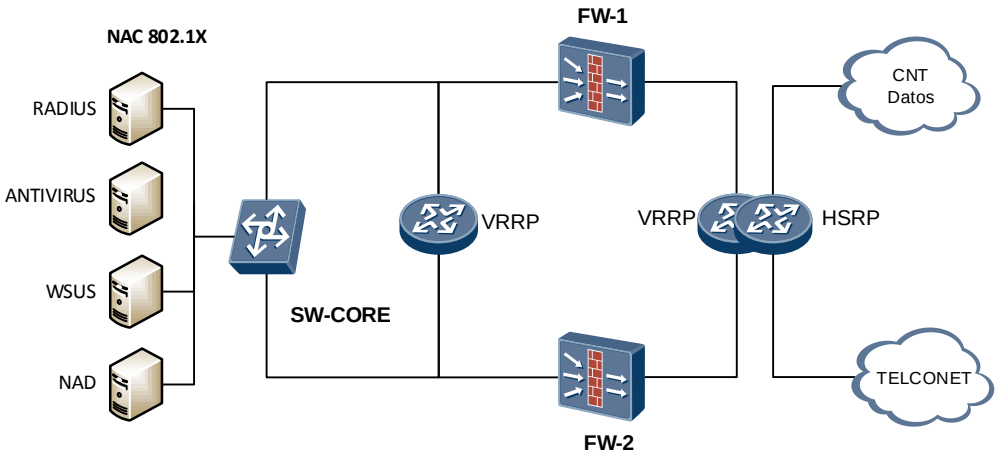


Figura 5.33: Nuevo esquema de red en la UN

Este nuevo esquema de seguridad disminuye el riesgo de suplantación de identidad, mejora la confidencialidad de la información al autenticar terminales que sean de CNEL EP y los usuarios consten en el directorio

activo previamente validado. También mejorará la disponibilidad de la información, al garantizar que las terminales pasen el antivirus sin detectar programas maliciosos y a su vez tengan la última actualización del sistema operativo. Si los terminales pasan los controles, entonces tiene acceso a la red de datos, caso contrario se queda aislado en una zona restringida, hasta que se actualicen las deficiencias detectadas.

De acuerdo al cronograma de trabajo planificado por la GTI, el próximo año se implementará este esquema de red corporativo, donde cada terminal se le instalará un software cliente que valida su contenido contra un servidor de dispositivo de acceso a la red NAC, que posteriormente continua con la autenticación 802.1x con el servidor RADIUS.

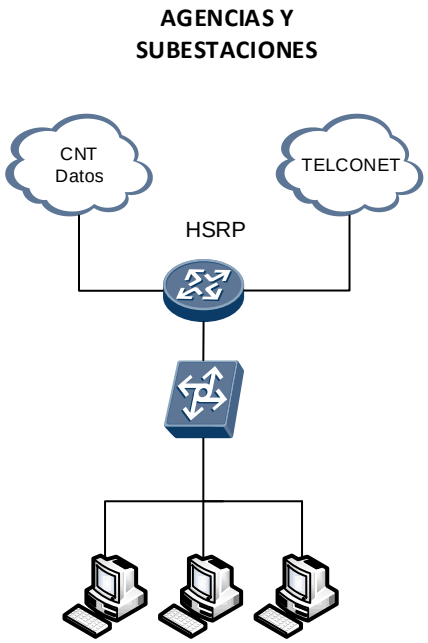


Figura 5.34: Enlaces redundantes en Agencias y Subestaciones

5.6. Desarrollar el sistemas de alertas tempranas

La red WAN de CNEL EP está formada por sus oficinas distribuidas en los edificios principales, agencias, subestaciones y otras UN, quienes consumen servicios instalados en el data center local de cada UN y servicios remotos instalados en el Data Center Corporativo. Los servicios consumidos tienen una creciente demanda de uso, y al estar alojados remotamente desde el punto de vista de las oficinas, es necesario garantizar la disponibilidad de la información definidos por la GSI en los acuerdos de niveles de servicios (SLA). Para ello es necesario monitorear toda la cadena de elementos activos que intervienen desde el servidor alojado en el data center, pasando por los proveedores de servicios, hasta llegar el dispositivo del usuario final alojado en la oficina, para que, en caso que exista un problema de comunicación de datos, pueda determinar cuál es el elemento de falla, genere una alerta, lo envíe al técnico responsable y solucione el problema en el menor tiempo posible.

Los elementos activos que se monitorean, pueden ser parámetros de rendimiento de un equipo tales como: porcentaje de uso del procesador, memoria y disco duro; puede ser elementos de red como: direcciones IP, interfaces de redes, velocidad de transmisión de datos de entrada y salida; puede ser servidores como: aplicaciones asociadas a los protocolos de red abiertos TPC/UDP, base de datos, etc.

Existen múltiples herramientas informáticas que cumplen con este propósito, que en su esencia, utilizan el Protocolo Simple de Administración de Red SNMP. Entre los principales programas tenemos: PRTG Network Monitor, ManageEngine OpManager, WhatUp Gold, Nagios.

WhatsUp Gold es una herramienta informática que permite realizar monitoreo unificado de redes, servidores y aplicaciones, cuenta con varios productos:

- WhatUpGold Ipswitch: Monitoreo unificado de disponibilidad de redes y servidores
- Application Performance Monitor Ipswitch: Busca y soluciona problemas de aplicaciones
- Flow monitor de Ipswitch: Visibilidad del tráfico de red y del uso de ancho de banda
- WhatsVirtual de Ipswitch: Administre la salud, la disponibilidad y el rendimiento de los entornos virtuales.
- WhatsConnected de Ipswitch: Automatiza el descubrimiento de redes y la asignación de dependencias
- WhatsConfigured de Ipswitch: Hace más eficiente la configuración y la gestión de cambio.

WhatUsGold Ipswitch es la aplicación adquirida por CNEL EP, monitorea las redes cableadas e inalámbricas, servidores físicos y

virtuales, aplicaciones empaquetadas y del cliente en un entorno de TI de proveedores múltiples.

- Descubre su red: Descubrimiento de capa 2 y 3, identifica los dispositivos de su red, como enrutadores, conmutadores, servidores y más.
- Crea mapas de su red: Genera automáticamente mapas de red de niveles 2 y 3 de la infraestructura central.
- Monitorea la red: Monitorea continuamente la disponibilidad de los enrutadores, conmutadores y firewall.
- Alertas inteligentes: Suministra alertas en tiempo real de e-mail, mensajes de textos.
- Genera informes de red: Brinda un entorno de generación de reportes fácil de personalizar.

El WhatsUpGold Ipswitch se encuentra instalado en el Data Center, desde donde se monitoreo los enlaces de datos y servidores instalados en cada UN, detallados de la siguiente manera:

- Se monitorean los enlaces de datos contratados con los ISP, a través de las direcciones IP de los routers en estado activos y pasivos instalados en el Data Center y en los edificios principales, agencias y subestaciones de las UN.
- Se monitorea la seguridad perimetral de los equipos de CNEL EP, a través de las direcciones IP de los firewall de en estado activo y

pasivo, más el swith de CORE con todas sus interfaces, que se encuentren instalados en el Data Center y en todas las UN.

- Se monitorea todos los servidores instalados en el Data Center y en las UN, a través de las direcciones IP.

Las alertas son notificaciones de correos electrónicos, dirigidas para los técnicos responsables de cada UN, que informan la afectación de un servicio. Por ejemplo, se monitorea los router que conectan los edificios principales, agencias y subestaciones, verificando si el enlace de datos se encuentra caído o levantado. En otros casos informa que ha sobrepasado el umbral de un componente relacionado al rendimiento del equipo, como por ejemplo, porcentaje muy alto del consumo del procesador, memoria o disco duro. Y por último informa sobre posible ataque de DoS monitoreando de las interfaces de red del switch de CORE, generando alertas cuando sobrepasando el umbral definido como máximo throughput

Estos son los pasos que debemos de realizar:

- Preparar los dispositivos a ser identificados y especificar las claves que se manipularán con el protocolo SNMT v1,2c
- Descubra los dispositivos y genere un mapa de red
- Configura y asigna acciones al monitoreo.
- Explora y personaliza reportes.

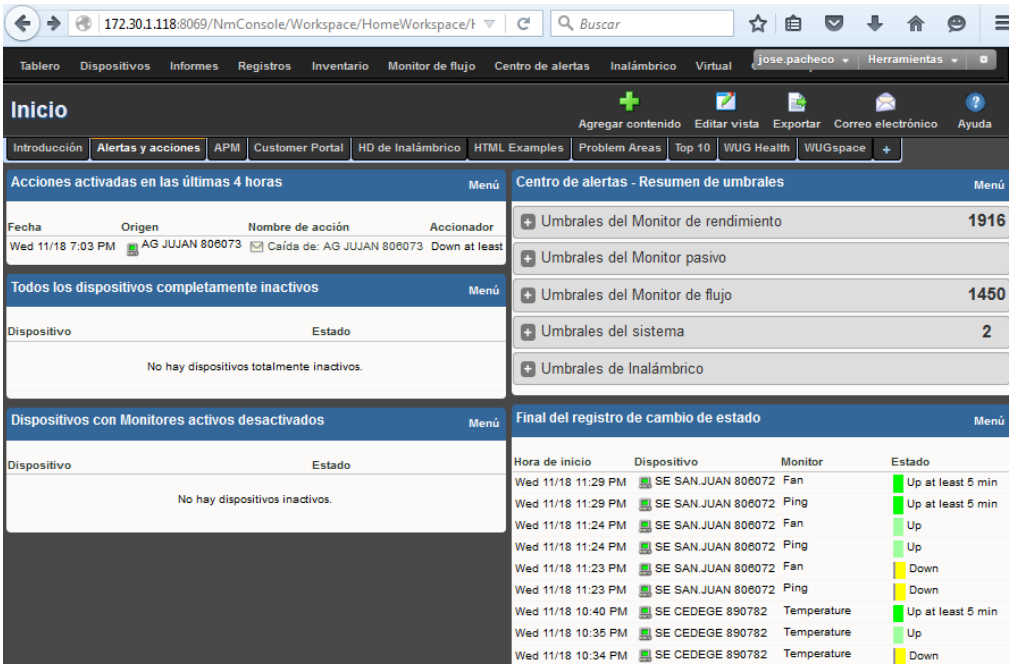


Figura 5.35: WhatsUpGold Ipswitch adquirido por CNEL EP

Por ejemplo, llega una alerta de correo electrónico, indicando que router de la localidad “Subestación Terminal Terrestre” lleva más de dos minutos en estado *down*. El contenido del correo se lo parametriza, indicando el código del equipo, en este caso es el código que CNT lo puede identificar llamado piloto, además fecha y hora, tal como se muestra en la siguiente figura.

Las alertas de correo electrónico provocadas por caídas del enlace o saturación del equipo, no podrá ser recibida por el técnico, debido que la red donde reside el técnico está incomunicada. Por este motivo la alerta debe ser por SMS

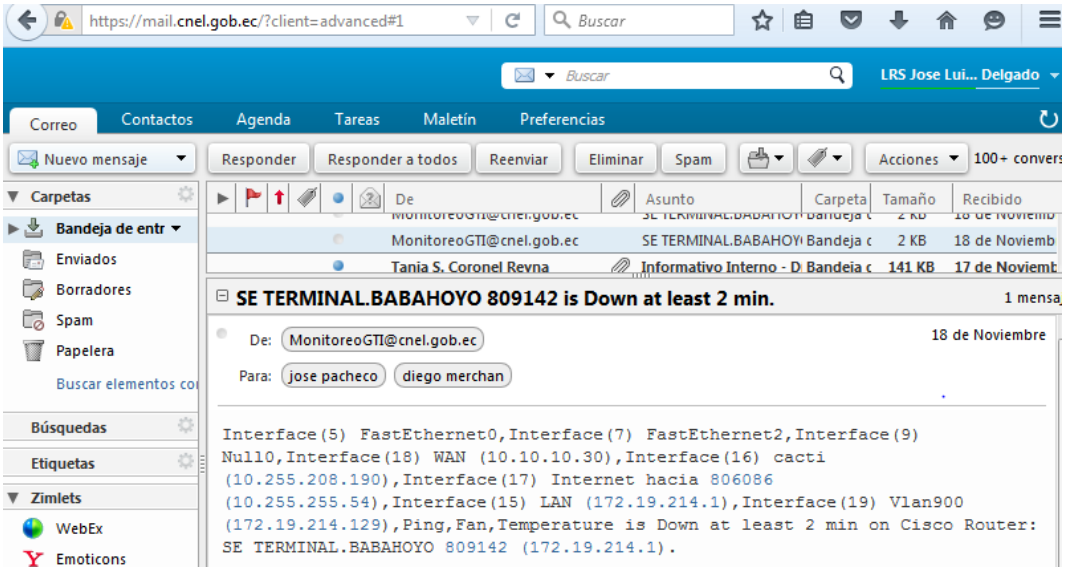


Figura 5.36: Alerta correo generado por WhatsUpGold

CAPÍTULO 6

ANÁLISIS DE RESULTADOS.

6.1. Evaluar las amenazas mitigadas.

El nivel de los riesgos se reducirá con la aplicación de controles, de modo que el riesgo residual se pueda revaluar como admisible. Se analizan todos los activos y se evalúa las consecuencias mitigadas.

6.1.1. Servidor Comercial

Mitigar la pérdida de la disponibilidad:

Actualmente se ha implementado enlaces redundantes de datos en el Data Center, disminuyendo notablemente el riesgo de la indisponibilidad del servicio.

Mitigar la pérdida de la integridad

Debido que es un servicio crítico para la UN, todos los días se generan respaldos de seguridad, realizados por una persona partir de las 20:00, que genera un respaldo de la data variable y además ejecuta procesos de cierre y facturación. Los fines de semanas y fin de mes se realizan respaldos totales de toda la base de datos. Los discos de respaldos están codificados y clasificados por fecha y tipos de respaldos.

En caso de existir fallos en la integridad de la data, se recupera los datos restaurando la información almacenada por el take backup de esa fecha.

Además para evitar corromper la data por accidente debido que no existe un servidor de producción, se mejora el conocimiento de la estructura de la base de datos, socializando el diccionario de datos y se genera una prohibición para actualizar cualquier dato de cualquier tabla. Este proceso lo realizará la empresa proveedora del servicio.

También se levantó un ambiente de pruebas, que todavía está en fase de revisión y aprobación.

Mitigar la pérdida de la confidencialidad.

Debido a denuncias verbales presentadas por usuarios finales que posteriormente fueron presentadas en la fiscalía, se asume que alguna empresa comercializadora del producto “cocinas de inducción” había conseguido de alguna manera no definida todavía, información confidencial de los clientes activos que registran sus consumos en la distribuidora, con el propósito de “vender” su producto, presionando a un sector de la población considera vulnerable, que si no adquiere el producto, se les quitará ciertos beneficios que reciben por parte del gobierno. Por este motivo para proteger la confidencialidad de la información de estos clientes, en caso de solicitar una cocina de inducción, no podrán adquirirlas directamente, sino hasta que CNEL EP verifique y actualice sus datos.

6.1.2. Servidor Comercial Prepago

Pérdida de la disponibilidad

La recaudación del sistema comercial, se lo hace a través de las ventanillas de la UN y también del sistema financiero. En las oficinas del edificio principal que es donde realiza la mayor recaudación, existía problemas de energía, debido que el UPS no soportaba la carga instalada de los pisos del data center local y de recaudación y atención al cliente. Pero debido a la remodelación del edificio, se solucionó el problema de carga del

UPS, porque se aisló el piso de recaudación y atención al cliente, y se dotó de UPS locales.

Pérdida de la integridad

A pesar de implementar sistemas de respaldos de tape backup, es necesario contar con un nuevo computador, que tenga instalado el hardware generado de códigos. Este proyecto está considerado a implementarse el siguiente año a partir del mes de abril

Pérdida de la confidencialidad

La aplicación cliente no puede ejecutarse en cualquier computador, debido que el servidor prepago controla y valida las direcciones IP de los clientes, previamente al registro y las licencias adquiridas y autorizadas, que por sólo está activa en un solo computador a pesar que se han adquirido tres.

También se ha protegido la suplantación del servidor prepago, configurando en el switch de core la protección ARP= IP+MAC+PUERTO. En el cliente se ha configurado el puerto seguro y el segmento de red sólo es válido en la VLANs de recaudación.

6.1.3. Servidor Financiero

Pérdida de la disponibilidad

Debido a problemas presentados de rendimiento en el servidor financiero se identificó que los recursos asignados de procesador y memoria eran insuficientes, por lo que se decidió cambiar de un ambiente virtual a un ambiente real, con contingencia de energía UPS, mitigando significativamente el riesgo y el impacto.

Pérdida de la integridad

Debido al cambio de un ambiente virtual a un ambiente real, se pudo implementar la redundancia en el almacenamiento RAID, que permite corregir cualquier problema de almacenamiento, estimando un crecimiento de almacenamiento de la data por varios años. Además se programa un plan de respaldos y recuperación de información basada en los backup por fechas, con capacidad de reconstrucción añadiendo las transacciones generadas en los días respaldados.

Pérdida de la confidencialidad

Para evitar capturar las credenciales de la aplicación WEB a través de ataques de hombre en medio, se habilitó en los switch de acceso la característica de puerto seguro, que impide configurar la tarjeta de red de un computador en modo promiscuo, con capacidad de hacer ataques al switch por envenenamiento ARP.

6.1.4. Servidor Nómina

Pérdida de la disponibilidad

Debido a problemas de rendimientos en el servidor de nómina, se determinó que los procesos de cierre de meses generado por cada UN consumían los recursos del servidor, y debido a la concurrencia de los procesos, no era factible satisfacer en un solo servidor. Se procedió a crear servidores réplicas para evitar la saturación del mismo, pero se debía de solucionar el problema utilizar la misma dirección IP para más de un servidor.

Riesgo residual deseado

Se crea una configuración en el servidor Apache llamada *VirtualHost* que utiliza la dirección IP del servidor de nómina, y éste a su vez redirecciona el tráfico hacia los otros servidores, evitando la congestión del rendimiento y disminuyendo el riesgo

Pérdida de la integridad

Existió un caso que el Administrador de la Base de Datos (DBA) de nómina se aumentó el sueldo, y fue detectado varios meses después. Se evidenció la falla en el control para detectar la ejecución de estos procesos ilegales. Se mitiga esta vulnerabilidad buscando los documentos de soportes que justifiquen el incremento, en que caso de no existir, se procede a

realizar el descuento más la aplicación del reglamento interno que puede llegar hasta la destitución del cargo.

Pérdida de la confidencialidad

Las credenciales de los usuarios privilegiados pueden ser capturadas en la red de datos, debido que viajan como textos planos. Pero se mitiga este problema validando la dirección IP como origen para realizar actualizaciones del programa. Para ejecutar procesos críticos se valida el usuario y la dirección IP de origen.

6.1.5. Servidor Directorio Activo

Pérdida de la disponibilidad

Las computadoras de las 10 UN no se validarán directamente al servidor del Directorio Activo DA que está en el Data Center, sino que dependiendo de la localización de cada UN, su autenticarán lo derivarán a uno de los tres servidores réplicas del DA, y éstos replicarán cualquier cambio en el principal.

Además se garantiza el ancho de banda desde la UN hasta el servidor réplica del DA y viceversa, para evitar saturación del enlace de datos.

Pérdida de la confidencialidad

Se mitiga la confidencialidad restringiendo la administración de los usuarios por UN y la administración de la consola filtrado por IP en el firewall

Para evitar que cualquier administrador de consola del directorio activo pueda modificar los usuarios de otras UN, se restringe el ámbito de administración solo a los usuarios de una UN.

Además la consola solo lo puede ejecutar en dirección IP específicas, debido al filtrado realizado por el firewall, que restringe los puertos de administración

6.1.6. Firewall

Pérdida de la disponibilidad

Al trabajar en modo redundante, con otro router firewall en estado activo pasivo, con el mismo Gateway con con el protocolo Virtual Router Redundancia Protocol (VRRP) se reduce el riesgo prácticamente a la mitad.

6.1.7. Switch de CORE

Pérdida de la disponibilidad

Se tienen dos switch configurados en stack que tiene los siguientes beneficios: Permite escalar el tamaño, gestión unificada y proporciona redundancia en las comunicaciones.

6.2. Analizar los riegos mantenidos.

6.2.1. Mantener vulnerabilidades detectadas por *nessus*

De los siete activos evaluados, todos las vulnerabilidades detectadas por *NESSUS* fueron mitigados exceptuando algunas en el servidor de Nómina, que mantiene archivos de ejemplo de la configuración predeterminada y algunos link internos tampoco fueron corregidos o eliminados. Esto se debe que la compañía que da el soporte de segundo nivel tiene un contrato de mantenimiento vigente, pero que se encuentra en fase de implementación de algunas mejoras, programadas a realizarse hasta abril del año 2016.

Pero para mitigar los link internos detectados por el scanner de vulnerabilidades *nessus* se ha implementado bloqueos en el firewall, que impiden que los usuarios finales puedan accesar a los archivos contenidos en la ruta http://172.30.1.193/examples, http://172.30.1.193/sample

6.2.2. Vulnerabilidades mantenidas de la matriz de riesgo

De los siete activos analizados, el servidor comercial prepago no se pudo mitigar en este año la pérdida de la integridad.

Como se sabe es un computador de escritorio que no permite mantener redundancia en el almacenamiento, debido al SO y corre el riesgo de dañarse el disco duro que se encuentra en el límite de su vida útil. La solución es cambiar el computador íntegro, a ejecutarse a partir del mes de abril del próximo año.

6.3. Evaluar el impacto administrativo las nuevas políticas de seguridad.

Se ha definido tres políticas de seguridad que está en análisis de aprobación, gestionada por la Gerencia de la Seguridad de la Información. En caso de aplicarse estas políticas, CNEL EP tendrá que adquirir equipamiento, reformar reglamentos y gestionar un programa de capacitación. Las políticas creadas son las siguientes:

- Diseñar políticas de control de acceso
- Definir políticas para evitar ataques de Denegación de Servicios
- Política de desvinculación de personal

6.3.1. Políticas de control de acceso

Se propone autenticar todos los terminales como son computadores desktop, computadores portátiles y dispositivos móviles a través de un servidor RADIUS, y los switch de accesos deben soportar esta funcionalidad, por lo que se deben de adquirir para cubrir déficit y reemplazar los instalados en las

agencias y subestaciones que no soportan este tipo de autenticación.

Además se propone cambiar la autenticación desde “algo que el usuario sabe” una clave, combinada con “algo que el usuario tiene” un token, con certificados digitales que se van autenticar en servidores regionales.

Este reto representa cambiar varios sistemas de información que validan las credenciales con autenticación tradicional, sumado con el token. Los sistemas más fáciles de cambiar son las aplicaciones WEB

Tabla 12: Costo para implementar política de control de acceso

Equipo	Cantidad	Costo	Subtotal
Switch de acceso Quidway	450	$900	$405,000
Token con certificados digitales	2,000	$66	$ 132,000
Recodificar autenticación de Sistemas de Información WEB	20	$20,000	$ 400,000
Servidores de autenticación zonales	3	$10,000	$30,000
		TOTAL	$967,000

6.3.2. Políticas para evitar ataques de Denegación de Servicios

Cuando se activó las protecciones contra ataques flooding en el firewall, se hicieron evidentes que existen software maliciosos instalados en computadoras y dispositivos móviles, que no pudieron ser detectados debido que varios factores:

- El antivirus corporativo no detecta todos los software maliciosos instalado en los terminales de CNEL EP, porque no está programado para detectar comportamientos
- No existe un software cliente instalado en los dispositivos móviles personales que determine las aplicaciones maliciosas instaladas.

El firewall procedió a bloquear inmediatamente la dirección IP de los equipos que generan ataques de DoS, durante periodos de tiempos de 20 min, hasta que se elimine el software malicioso instalado en cada terminal. En el caso de los terminales de CNEL EP, se procedió a re-instalar el SO y en caso de los dispositivo móvil personales se sugirió restablecer su configuración de fábrica.

El impacto es administrativo tiene un costo de mano de obra, focalizada para re-instalar el sistema operativo y programas en general de todas las computadoras detectadas con programas que generan ataques DoS, que fue un promedio del 10%, de las 3,000 terminales que existen CNEL EP, y asignando un técnico pueda instalar 2 computadoras diariamente se requiere a 1,500 técnicos, que trabajan 22 días mensuales, representa el sueldo de 69 personas, a un sueldo de $1,000.

El costo de esta implementación representa $69,000

6.3.3. Política de desvinculación de personal

Debido que es la implementación del reglamento definido por la GSI, las desvinculaciones del personal está asociada a la función de bloqueos lógicos de todos los sistemas de información, que se los realiza a través del bloqueo de la cuenta del directorio activo, bloque del token en el servidor de certificados digitales y bloqueo del puerto físico en switch de acceso o lógico en Access point.

Es necesario dar una capacitación integral de las nuevas herramientas del firewall y configuración de los switch de CORE y acceso, con la finalidad de implementar el nuevo esquema de red, por lo que en el plan de capacitación anual, se requiere por lo menos a dos técnicos por cada UN, durante dos semanas, para recibir 80 horas de clases, con la finalidad de obtener una certificación.

Considerando $80 diarios de viáticos por persona, más el local y el instructor, se estima que se incurre en un gasto aproximado de $27,000

Tabla 13: Costo por implementar políticas seguridad

Nro.	Política	Costo
1	Política de control de acceso	$967,000
2	Política para evitar ataques de DoS	$69,000

3	Política desvinculación de personal	$27,000
	TOTAL	$1,063,000

6.4. Rediseñar el esquema de red corporativo.

Debido que los principales servicios de red que utiliza cada UN se encuentran centralizados en el Data Center Corporativo y en los edificios principales, es necesario garantizar la disponibilidad de la información desde cualquier oficina de CNEL EP, por lo que es necesario implementar enlaces redundantes en las agencias y subestaciones que actualmente no lo tienen.

Como consecuencia de la seguridad de las redes de computadoras, el Control de Acceso a la Red NAC tiene varios servidores, que debido a la alta disponibilidad varios de ellos estarán en los data center de las UN, tales como: RADIUS, servidor antivirus, servidor WSUS, servidor DHCP, servidor de autenticación WEB, servidores de Políticas de seguridad. Otros servidores que forman parte de la solución seguirán alojados en el Data Center Corporativo como son: Directorio Activo.

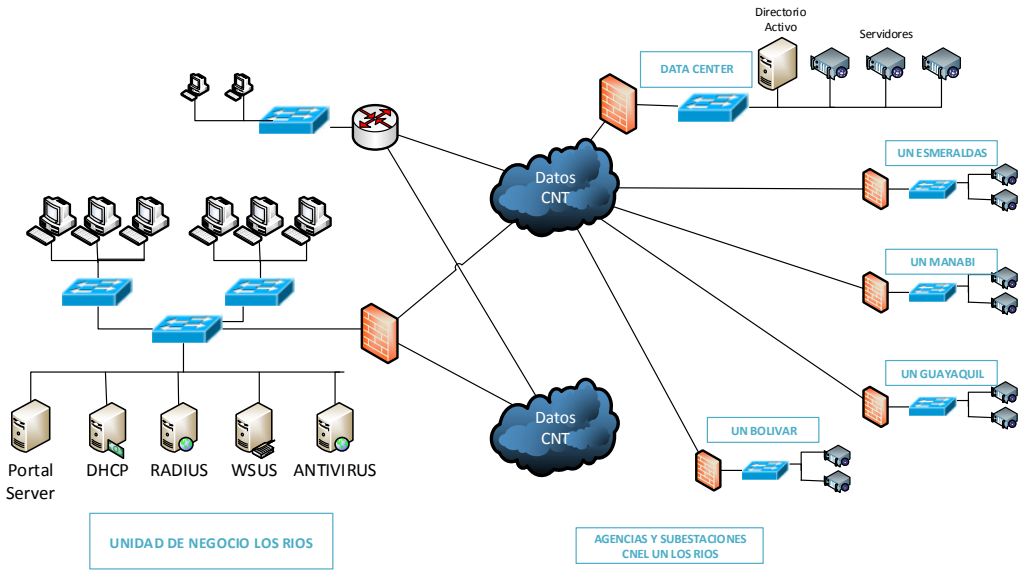


Figura 6.1: Esquema de red corporativo CNEL EP

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Se realizó el test de vulnerabilidad a los siete activos de la UN Los Ríos considerados como principales, encontrando una vulnerabilidad crítica, 37 medianas y cinco bajas.
2. Todas las vulnerabilidades críticas, medianas y bajas fueron mitigadas exceptuando una mediana, programada su mitigación el próximo año a través de un programa de mantenimiento realizada por la contratista que administra el servidor financiero.
3. Las vulnerabilidades críticas fueron mitigadas haciendo cambios en el registro del sistema y parchando el sistema operativo Windows.

4. Las otras vulnerabilidades se mitigaron, bloqueando los puertos en el firewall, permitiendo solo los puertos indispensables para los servicios que requiere cada activo.
5. Para mejorar la disponibilidad de la información, se evita ataques de denegación de servicios, activando características de protección de seguridad en el firewall como: Attack Defense, blacklist, whitelist, IP-MAC Binding
6. Para mejorar la disponibilidad de la información se activó características en el switch, que realiza la supresión de tráfico y QoS limitando la velocidad de salida por VLAN's
7. Para mejorar la confidencialidad de la información se activaron características en el switch como puerto seguro por MAC y ARP, que evitar ataques de hombre en medio
8. El control de acceso a la red NAC, define el protocolo 802.1x con servidor de autenticación en la red, implementado con un servidor FreeRADIUS.
9. Se propone implementar NAC como un enfoque de seguridad integral, instalando servidores locales para garantizar la disponibilidad del servicio y el DA en el data center corporativo.
10. El ataque de ingeniería social enfocado para conseguir la clave de la red WLAN corporativo, queda mitigada por la autenticación en la red

con FreeRADIUS, donde todos los terminales están registrados sus direcciones MAC

11. Se propone como política de control de acceso que la autenticación en los sistemas de autenticación esté basado en *algo conocido* + *algo poseído*. El *algo conocido* es la clave definida en el DA y el *algo poseído* es el token con certificados digitales.
12. La matriz de riesgo calculada para los siete activos considera principalmente la disponibilidad, y en menor medida la integridad y confidencialidad de la información. Con los controles aplicados, el riesgo inherente se reduce hasta un riesgo residual, y sólo dos activos se vuelve aplicar controles adicionales y planes a futuro para bajar el riesgo residual deseado.
13. El impacto administrativo por la aplicación de las nuevas políticas tiene un costo económico valorado en $1,063,000

RECOMENDACIONES

1. La mayoría de las implementaciones de seguridad realizadas en los switches y firewalls, no se las realizaba en las UN por falta de conocimiento, por lo que es necesario realizar un plan de capacitación para explotar al máximo las funcionalidades de la infraestructura adquirida.

2. Realizar este plan de pruebas en todas las UN por lo menos una vez al año, para mitigar las vulnerabilidades y cumplir con lo dispuesto por el acuerdo ministerial 166 “Esquema Gubernamental de Seguridad de la Información EGSI”.

BIBLIOGRAFÍA

[1] Astudillo, Karina. “Hacking Ético 101. Cómo hackear profesionalmente en 21 días o menos!”, 2013

[2] Tory, Carlos. “Hacking Ético”, mayo del 2008.

[3] CNEL EP, “Estructura Organizacional de CNEL: Estatus Orgánico de la Gestión Organizacional por Procesos, página 13 www.cnel.gob.ec

[4] CNEL EP, “Normativa Interna de la Administración de Talento Humano de la Empresa Eléctrica Pública Estratégica Corporación Nacional de Electricidad, CNEL EP”, 2 de mayo del 2,014

[5] CNEL EP, “Manual de políticas de seguridad de la información”, 14 de septiembre del 2015

[6] CNEL EP, Procedimiento – Desvinculación, 29 de diciembre del 2,011

[7] CNEL EP, “Procedimiento de control y gestión de usuarios: altos, bajos, manejo de privilegios”, 3 de septiembre del 2015

[8] Secretaría Nacional de la Administración Pública, Acuerdo ministerial 166 “Esquema gubernamental de seguridad de la información EGSI”, 25 de septiembre del 2013

[9] Huawei Technologies Co, “Quidway S2700-52P-EI Ethernet Switch V100R006C00”, 15 de julio del 2011.

[10] Lehembre, Guillaume. “Seguridad Wi-Fi – WEB, WAP y WAP2” http://www.haking9.org, fecha de consulta 10 de agosto del 2015

[11] Caballero, Alonso. “Hacking con Kali Linux” http://www.reydes.com/d/?q=node/2 , versión 2.1, octubre del 2013

[12] Instituto Tecnológico y Estudios Superiores de Monterrey, “RADIUS”, septiembre del 2017

[13] Barrios, Joel, “Configuración de Freedradius con MySQL™/MariaDB™ en CentOs” http://www.alcancelibre.org/staticpages/index.php/como-freeradius-mysql-centos, fecha de consulta 10 de agosto del 2015

[14] Gómez, Ángel. “ISO 27005 Gestión del Riesgo Informático” http://es.scribd.com/doc/149691797/Iso-27005-Gestion-Del-Riesgo-Informatico#scribd, fecha de consulta 10 de agosto del 2015

ANEXOS

Resultado de las vulnerabilidades detectados con NESSUS

				Puertos Abiertos						
ID	HOSTNAME	Descripción	Sistema Operativo	TCP	UDP	Aplicación - Versión	Vulnerabilidades detectadas	Niveles de Riegos	Explotables?	Observaciones
1	WIN-V90062A5A1A	Servidor Financiero	Windows 2008 Server	80		Microsoft IIS httpd 7.5	CVSS2	Mediano		
				135		Microsoft Windows RPF	n/a			
				139		Microsoft Windows 98 netbios-ssn	n/a			
				445		(primario dominio: CORCNEL)	n/a			
				1433		Microsoft SQL Server 2012	CVE-2013-2566, CVE-2015-2808 CVE-2004-2761, CVE-2014-3566	Mediano	Si	SSL Certificados digitales
				1801		msm	n/a			
				2103		Microsoft Windows RPC zephyr-clt	n/a			
				2105		Microsoft Windows RPC eklogin	n/a			
				2107		Microsoft Windows RPC msmq-mgmt	n/a			
				2383		ms-olap4	n/a			
				3389		Microsoft Terminal Service	CVE-2005-1794	Mediano	Si	Escritorio Remoto, tiene un certificado por defecto
				8080		Microsoft IIS httpd 7.5	n/a			
				49152		Microsoft Windows RPC	n/a			
				49153		Microsoft Windows RPC	n/a			
				49154		Microsoft Windows RPC	n/a			
				49155		Microsoft Windows RPC	n/a			
2	n/a	Servidor RR.HH	Linux 2.6.3	22		OpenSSH 5.3 (protocol 2.0)	n/a			
				80		Apache httpd 2.2.15	n/a			
3	MLGSRV_CD02	Servidor Directorio Activo	Windows 2008 Server	53		Microsoft DNS 6.1.7601	n/a			
				58		Windows 2003 Kerberos	n/a			
				135		Microsoft Windows RPF	n/a			
				139		Microsoft Windows 98 netbios-ssn	n/a			
				389		ldap	n/a			
				445		(primario dominio: CORCNEL)	n/a			
				464		tcpwrapped	n/a			
				593		Microsoft Windows RPC over HTTP 1.0	n/a			
				636		tcpwrapped	n/a			
				3268		ldap	n/a			
				3269		tcpwrapped	n/a			
				3389		Microsoft Terminal Service	CVE-2005-1794 CVE-2013-2566, CVE-2015-2808	Mediano	Si	
				49154		Microsoft Windows RPC	n/a			
				49155		Microsoft Windows RPC	n/a			
				49157		Microsoft Windows RPC over HTTP 1.0	n/a			
				49159		Microsoft Windows RPC	n/a			

Resultado de las vulnerabilidades detectados con NESSUS

				Puertos Abiertos						
ID	HOSTNAME	Descripción	Sistema Operativo	TCP	UDP	Aplicación - Versión	Vulnerabilidades detectadas	Niveles de Riegos	Explotables?	Observaciones
4	FW-LRS1	Firewall	VRP Version 5.30	21		vsftpd 2.0.8 or later				
				23		telnet		Mediano		Telnet envia texto plano
				80		HTTP Server 1.0				
				1666		ssl/netview-aix-6?		Mediano		Certificado SSL no autenticado
				1888		sun_answerbook?				Web Application vulnerable
5	SW-CORE LRS	Switch de CORE	Quidway V200R001C00PC300	23				Mediano		Telnet envía texto plano
				80		Huawei S5700-series switch httpd				
6	CNELLRS	Servidor Comercial	IBM i5/OS V6	21		IBM OS/400 FTPd	n/a			
				23		IBM OS/400 telnetd	n/a			
				25		i5/OS V5R4M0 or OS/400 smtdp	n/a			
				389		ldap	n/a			
				427		lsvrloc	n/a			
				515		printer	n/a			
				992		tcpwrapped	n/a			
				2001		Apache httpd	n/a			
				2002		Lotus Notes Expeditor httpd 6.1	n/a			
				2004		Lotus Expeditor Web Container 6.1	n/a			
				2005		ssl/deslogin?	CVE-2004-2761, CVE-2004-2761 CVE-2013-2566, CVE-2015-2808 CVE-2015-4000, CVE-2015-0204 CVE-2015-0204	Mediano	SI	Certificados digitales
				2006		Lotus Notes Expeditor httpd 6.1	n/a			
				2008		Lotus Notes Expeditor httpd 6.1	n/a			
				3000		IBM Service Tool Server AS-STS	n/a			
				4111		Apache Tomcat/Coyote JSP engine 1.1	n/a			
				5544		unknown	n/a			
				5555		freeciv	n/a			
				5989		Web-Based Enterprise Management CIM	n/a			
8	PREPAGO	Sistema comercial prepago	Windows XP	23		Microsoft Windows XP telnetd	n/a			
				135		Microsoft Windows RPC	n/a			
					137	Microsoft Windows NetBios				
				139		Microsoft Windows 98 netbios-ssn	n/a			
				211		914c-g	n/a			
				445		Microsoft Windwos XP microsoft-ds	CVE-1999-0519, CVE-1999-0520	Alto		Sessiones nulas
							CVE-1999-0519, CVE-1999-0520 CVE-2002-1117	Mediano		
				3389		Microsoft Terminal Service	CVE-1999-0511	Alto		Escritorio remoto subceptible ataque Main in the Medium
							CVE-2005-1794	Mediano	Si	
				5800		RealVNC E4	n/a			
				5900		RealVNC Enterprise (protocol 4.1)	n/a			

Zimbra: **jose.pacheco@cnel.gob.ec**

Informe técnico de las pruebas de vulnerabilidad aplicado a 3 servidores

De : Jose L. Pacheco Delgado <jose.pacheco@cnel.gob.ec>
mié, 04 de nov de 2015 17:45
1 ficheros adjuntos

Asunto : Informe técnico de las pruebas de vulnerabilidad aplicado a 3 servidores

Para : Oscar A��azco <oscar.anazco@cnel.gob.ec>

Estimado Oscar

Adjunto los archivos generados de las pruebas de vulnerabilidad aplicado a los servidores: Financiero, Nomina y Directorio Activo

Saludos

Ing. Jose Luis Pacheco Delgado
JEFE DE TECNOLOGIA (E)
CNEL LRS
EMPRESA ELÉCTRICA PÚBLICA ESTRATÉGICA CNEL EP
Dirección: 9 de Noviembre y General Barona, edif. Principal 5to. piso
Teléfono: +593 5 2730089 ext. 808
Edificio Principal / Babahoyo - Ecuador
www.cnel.gob.ec
CNEL
Síguenos en redes sociales:
facebook.com/cr twitter.com/CNEL_I youtube/cnel

pentesting.rar
360 KB

Documento Nro. CNEL – LRS –CCM – 20 - 17
Babahoyo, 4 noviembre 2015

PARA : Sr. Ing. Milton Esteban Serrano Blacio
GERENTE DE SEGURIDAD DE LA INFORMACION

ASUNTO : Informe técnico de escaneo de vulnerabilidades realizadas a los servidores Financiero, Nómina y Directorio Activo utilizados en CNEL EP

Las pruebas de vulnerabilidad fueron realizaron el 4 de noviembre 2015, a tres servidores de CNEL EP, supervisado por un técnico delegado por la Gerencia de Seguridad de la Información, basado en las fases del pentesting o hacking ético:

- Reconocimiento o footprinting.
- Exploración o escaneo y numeración
- Obtener acceso
- Mantener el acceso y
- Borrar huellas

Reconocimiento
Esta fase se ha obviado debido a la experiencia que tengo laborando en la Gerencia de Tecnologías de la Información, y se ha seleccionado a los tres servidores debido a su relevancia, por ser servicios utilizados en todas las UN y la explotación de una vulnerabilidad existente, causaría un impacto directo en la gestión administrativa de CNEL EP.

Exploración o escaneo
Para esta fase utilizamos varias herramientas:

- NMAP para averiguar los puertos abiertos, las aplicaciones asociadas a esos puertos y el sistema operativo.
- NESSUS verifica las vulnerabilidades presentadas en los puertos abiertos detectados con NMAP
- NIKTO es un escáner de aplicativos web que detecta archivos peligrosos, software desactualizado, entre otros.

Obtener acceso
No aplica, debido que es un ambiente de prueba, solo se identifican el test de vulnerabilidad encontradas, calificadas como informativas, bajas, medias, altas y críticas. La fase de explotación no será aplicada, salvo el caso que lo exprese por escrito la GTI o GSI.

Tabla: Resumen de las vulnerabilidades encontradas en 3 servidores

Sistema	Crítica	Alta	Media	Baja	Informativa
Financiero	0	0	12	2	39
Recursos Humanos	0	0	2	2	12
Directorio Activo	0	0	7	1	35

Conclusiones

- No se detectaron riesgos altos: Estas vulnerabilidades críticas pueden ser explotadas perjudicando el funcionamiento normal de las actividades de la empresa, pudiendo tomar el control total de los sistemas y su información. Tienen un nivel de criticidad alta.
- 21 riesgos medianos. Son vulnerabilidades que requieren atención pero no suponen un riesgo inminente para los sistemas; sin embargo existe el riesgo que puedan ser explotadas. Su criticidad es media.
- 5 riesgos bajos: Son vulnerabilidades moderadas, que podrían brindar información para su posterior ataque. Su criticidad es baja.
- 86 vulnerabilidades Informativas con las cuales la herramienta me informa de posibles riesgos para los sistemas y que se pueden corregir con ciertas configuraciones de los sistemas.

Recomendaciones

Se recomienda realizar el test de vulnerabilidades con un periodo no mayor a seis meses, como buenas prácticas del "ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACION EGSI" registrado en el acuerdo ministerial Nro. 166.

En base al punto anterior, las vulnerabilidades con riesgo mediano se las puede mitigar con acciones de bloqueo en firewall a todas las UN y permitiendo el acceso a esos puertos sólo al personal técnico autorizado.

Se adjunta cuadro de los puertos y vulnerabilidad encontradas por servidores, más un detalle de cada una de las vulnerabilidades.

Atentamente

Ing. José Luis Pacheco
JEFE DE TECNOLOGÍA - ENCARGADO
CNEL UN LOS RIOS

Ing. Oscar Añazco
TÉCNICO DE SISTEMAS
GERENCIA SEGURIDAD INFORMACION

Memorando Nro. CNEL-CORP-TIC-2015-0134-M

Guayaquil, 21 de agosto de 2015

PARA: Sr. Ing. José Luis Pacheco Delgado
Administrador de Base de Datos - ESM

ASUNTO: Autorización para desarrollar tema de tesis "DESARROLLO DE PRUEBAS DE VULNERABILIDAD A LA RED DE DATOS DE UNA EMPRESA PÚBLICA DE DISTRIBUCIÓN ELÉCTRICA CNEL EP.

De mi consideración:

La Gerencia de Tecnología de CNEL EP autoriza al estudiante de la ESPOL - MSIA.,José Luis Pacheco Delgado a desarrollar el tema de tesis "DESARROLLO DE PRUEBAS DE VULNERABILIDAD A LA RED DE DATOS DE UNA EMPRESA PÚBLICA DE DISTRIBUCIÓN ELÉCTRICA CNEL EP"

Con sentimientos de distinguida consideración.

Atentamente,

Ing. Luis Antonio Gomez Schwass
GERENTE DE TECNOLOGÍA DE LA INFORMACIÓN

easr