Universidad de Buenos Aires

Facultades de Ciencias Económicas

Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Aseguramiento de Equipos de red en ambientes Empresariales

Autor: Ing. Diego Rafael Forero Pulido

Tutor: Diego Alonso

Cohorte 2011

Declaración Jurada de Origen de los contenidos.

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual

FIRMADO

DIEGO RAFAEL FORERO

DNI: 94.773.947

Tabla de contenido

Nomina de Abreviaturas

AAA: Authentication**,** Authorization, Accounting

ARP: Address Resolution Protocol, Protocolo de la capa de enlace de datos responsable de la resolución de una Dirección IP a una Dirección MAC.

BID: Bridge ID: Numero de identificación de los Switches en la estructura de Spanning Tree Protocol, consistente de 8 Bytes de longitud. 2 bytes de Prioridad y 6 Bytes de la dirección MAC del Switch.

BPDU: Bridge Protocol Data Units, paquetes de datos del protocolo STP, para comunicación de Información de estado, conexión y notificaciones de los Switches.

CAM: Content Addressable Memory: Parte de la memoria usada en los Switches para almacenar la tabla de direcciones MAC Dinámicas.

CDP: Cisco Discovery Protocol. Protocolo propietario cisco desarrollado para el descubrimiento de dispositivos en capa de enlace de datos.

CLI: Command Line Interface, Interface de línea de comandos

CNA: Cisco Network Assistant: Programa de administración centralizada de equipos de red Cisco.

DTP: Dynamic Trunking Protocol: Protocolo propietario cisco desarrollado para realizar la negociación automática puertos Trunk entre dos Switches.

DoS: Denial of Service. Ataque informático, consistente en el agotamiento de recursos de conexión de un equipo o servicio.

GC: Global Catalog: Servicio usado por la infraestructura Active Domain Microsoft.

HTTP: Hypertext Transfer Protocol: Protocolo de aplicación, para intercambio y/o transferencia de Hipertexto.

HTTPS: Secure Hypertext Transfer Protocol: Protocolo de aplicación, para intercambio y/o transferencia de hipertexto a través de un canal cifrado.

IPS: Intrusion Prevention System. Equipo de seguridad.

LDAP: Ligthweigth Directory Access Protocol: Protocolo de aplicación, para acceso y mantenimiento de servicios de información sobre IP.

MAC: Media Access Control. Identificador de interfaces o dispositivos I/O de redes de datos.

MITM: Man In the Middle: Ataque Informático, consistente en la intercepción del tráfico generado y recibido por un equipo.

KRBS: Kerberos : Protocolo de Autenticación para redes de datos.

RPC: Remote Procedure Call: Método de invocación remota de un procedimiento o rutina.

SMB: Server Message Block, Protocolo de capa de red, principalmente usado para acceso compartido a recursos.

SNMP: Simple Network Managment Protocol: Protocolo para administración de equipos en redes IP.

STP: Spanning tree protocol: Protocolo de capa de enlace de datos, usado para evitar loops en capa 2.

SSH: Secure Shell. Protocolo de acceso seguro a interface de comandos.

VLAN: Virtual Local Area Network.

WAF: Web Application Firewall. Equipo de red.

Introducción

En la actualidad las empresas están empezando a darse cuenta de la importancia que tiene la seguridad de la información en el desarrollo de sus actividades productivas, el crecimiento de Internet como medio de alcanzar a nuevos clientes y nuevos tipos de negocio ha hecho que se tomen cada día mas medidas para proteger las redes empresariales de posibles ataques, desde la adopción de modelos de gestión de riesgo de la seguridad de la información, hasta el montaje de infraestructura tecnológica específicamente diseñada para proteger los activos informáticos de las empresas (Firewalls, IPSs, WAFs…).

Pero como sabemos, la implementación de seguridad de la información es un proceso que conlleva muchas capas y ninguna de ellas puede ser tomada a la ligera. Los equipos de red (capa 2) son el portal de entrada a las redes empresariales, muchas de las amenazas informáticas que se presentan en la actualidad pueden ser detectadas e incluso evitadas, si se aprovecharan las funcionalidades en seguridad que tienen estos equipos, todo esto sin incurrir en mayores gastos en infraestructura tecnológica.

Durante el desarrollo de mi carrera profesional en la implementación de Seguridad en redes de datos, he observado que la mayoría de las empresas que piensan en seguridad se centran en la adquisición de hardware o software específicamente diseñado para la protección de los datos, pero descuidan el aseguramiento de los equipos que ya se encuentran en funcionamiento; se tiene la concepción que los equipos como switches y routers no tienen mucho que aportar a la seguridad de la información y que sus funciones están únicamente ligadas a las tareas de networking; en consecuencia no es requerida la verificación de configuraciones y funcionalidades activas, esta idea no podría estar mas alejada de la realidad.

Este trabajo dará lineamientos, consejos, herramientas y organización para el aseguramiento de los equipos de red en ambientes empresariales.

Metodología de Trabajo…

Las tareas de aseguramiento de una red de datos requieren experiencia y un nivel de conocimiento técnico amplio, esto las puede convertir en tareas tediosas, de gran dificultad y en muchos casos abrumadoras. Para evitar estas situaciones, en este trabajo se propone dividir estas tareas en tres grandes grupos, descriptos brevemente a continuación:

1. **Identificación. "Que debemos proteger"**
   El primer problema que se enfrenta en el aseguramiento de red es (en su gran mayoría) el desconocimiento de lo que debemos asegurar. Es una práctica muy común de las empresas no tener un inventario actualizado de los equipos de red, ni de las versiones de Firmware en ejecución, los sets de funcionalidades, ni tampoco del tipo específico de tráfico que es generado por las aplicaciones usadas por el negocio. En la primera parte del trabajo, se mostraran herramientas y procedimientos para la identificación de equipos y de servicios en una red de datos con el fin de empezar las tareas de aseguramiento con un nivel de información adecuado.

2. **Análisis amenazas. "Contra que debemos protegernos"**
   Luego de la identificación descrita en el primer grupo de actividades, se debe identificar y analizar los riesgos y los diferentes tipos de ataques que se presentan a nivel de equipos de red. En esta parte del trabajo enumeraran y se mostrara como funcionan algunos de estos ataques, con el fin de entender su funcionamiento y en pasos siguientes tomar medidas para contrarrestarlos.

3. **Tratamiento. "Como nos protegemos"**
   Teniendo en cuenta los resultados de la etapa de Análisis, se deberán tomar medidas en lo que se refiere a configuración de equipos y diseño de red, con el fin de mitigar o eliminar el impacto de estas amenazas en la red de datos; esta parte del trabajo dará ejemplos de configuraciones y propondrá diseños de red que ayudaran a alcanzar la meta de proteger la red de datos sin llegar comprometer el normal funcionamiento de los equipos.

Etapas de Aseguramiento

Identificación.

Como se comento anteriormente uno de los principales problemas que enfrentan las empresas en las tareas de aseguramiento de las redes de datos, es el desconocimiento de los equipos que poseen, sus funcionalidades y los servicios que se prestan a nivel de red, esta situación se debe en gran parte a que los protocolos y servicios usados no son evaluados al momento de diseñar las redes, y no son documentados debidamente por personal de Desarrollo y/o Implementación de software.

También aporta a este problema, la falta de documentación de cambios en equipos y en configuraciones de red. Las tareas de documentación son una parte bastante tediosa en el mantenimiento de una red y asimismo no se les presta la suficiente atención, lo que lleva a tener información desactualizada en los momentos en donde se presentan problemas o se requieren hacer cambios que puedan afectar el normal funcionamiento de los equipos.

Uno de los objetivos principales de este trabajo es mostrar la verdadera importancia de las tareas de identificación, y su utilidad en todas las etapas. La primera etapa en el proceso de aseguramiento de una red debe ser siempre la de identificar aquello que deseamos proteger (servicios, información y equipos).

Como referencia durante el desarrollo del trabajo tomaremos como ejemplo una red de tamaño mediano, entre 1500 y 2000 usuarios, compuesta de aproximadamente 30 a 40 switches de Acceso/distribución y 2 switches de core, con acceso inalámbrico habilitado, sobre la cual se han realizado varios cambios pero no se han realizado tareas de identificación ni de actualización de documentación y tampoco se encuentran documentados los servicios que se prestan. Solo tenemos un diagrama de red de 2 años de Antigüedad. (Grafico 1). En esta situación, nosotros somos los encargados de actualizar la información de servicios y de equipos como primer paso para el aseguramiento de la red.

Esquema de Red

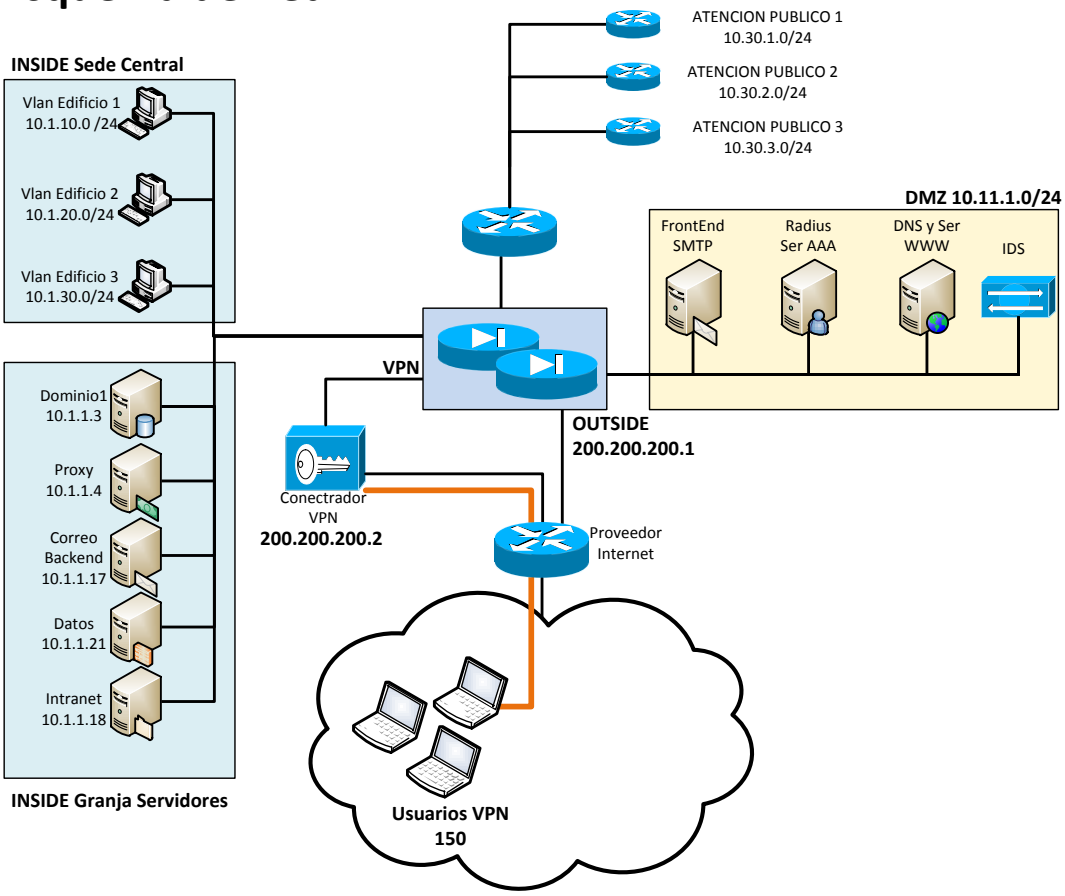

Grafico 1 (Información Inicial de la Red de Datos)

En la práctica, las tareas de identificación de servicios y equipos son encargadas en su gran mayoría a personal de Staff o Junior (Experiencia mínima) lo que agrava los problemas, ya que algunas de estas tareas a pesar de ser sencillas requieren de un nivel de conocimiento considerable para ser llevadas a cabo a buen término. Entre las herramientas que se pueden utilizar para conocer las direcciones IP, direcciones MAC como así también los nombres de los hosts, podemos encontrar:

Ping Scan (IP Angry Scan[1])

Es una herramienta libre, sencilla pero también una de las más útiles en las tareas de recopilación de información. Herramientas de este tipo no solo brindan información acerca de los equipos activos dentro de una subred también información básica acerca de puertos disponibles para comunicación, Direcciones MAC de los equipos (de aquí podemos inferir tipo de equipo y fabricante). En este caso usaremos la Herramienta IP Angry scan por su sencilla ejecución, no requiere instalación y es compatible con todas las versiones de Windows.

[1] http://www.angryip.org/w/About (Consultada el 10 de Junio de 2012)

En la red ejemplo se tomara posición en un equipo del segmento de red 10.1.1.0 y se realizara un ping scan a las direcciones del segmento 10.1.0.0/16 dadas en el grafico de red inicial (LAN de servidores) (Grafico 2). Si no se contara con información básica sobre la red, se deberían ejecutar los siguientes comandos en CMD de Windows para obtener información acerca del controlador de dominio, equipos DNS y relaciones del pc mediante conexiones activas.

ipconfig: Información de la dirección, Nombre y configuración de red del equipo, equipo DNS.

nslookup*:* información sobre dirección de los equipos, información acerca de servidores DNS.

arp –a: Información acerca de conexiones activas del equipo, puertos de origen y destino, nombres y direcciones Mac.

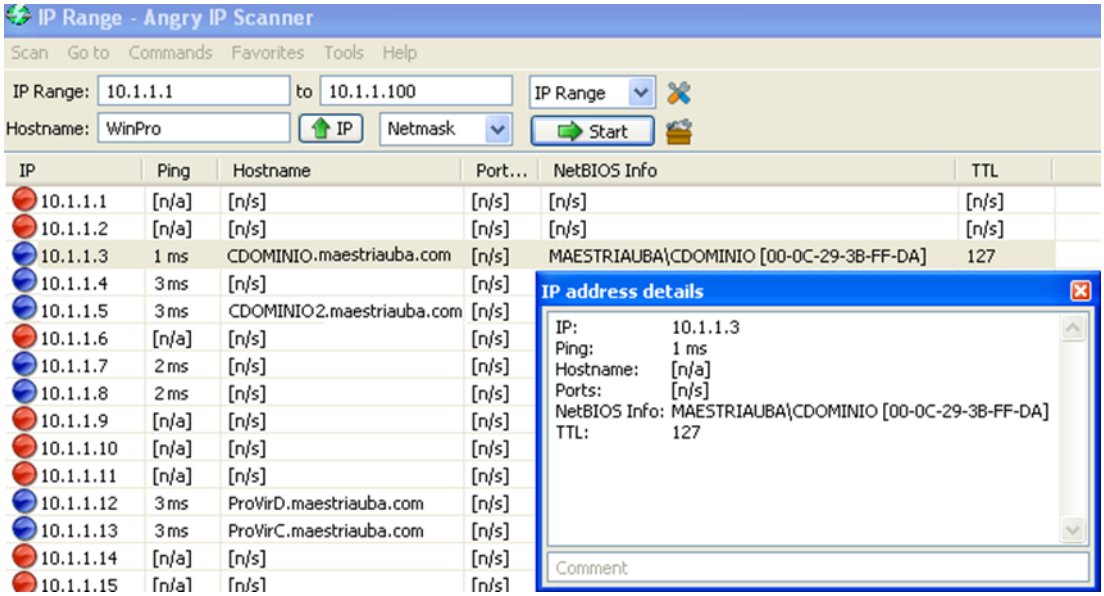

Grafico 2 Resultados Ping Scan

En el grafico 2, observamos la información obtenida del servidor 10.1.1.3, equipo con funciones de controlador del dominio maestriauba.com, con el nombre CDOMINIO. Mediante el control de los valores de TTL podemos saber el número de saltos en capa tres necesarios para alcanzar esta dirección, utilizando la dirección MAC y paginas como http://www.coffer.com/mac_find/ o http://www.macvendorlookup.com/ podemos saber el tipo de equipo y su fabricante, para este ejemplo la dirección 00-0C-29-3B-FF-DA pertenece a Vmware Incorporated.

Realizando un escaneo de todas las VLANs conocidas podremos tener un estimado bastante cercano a la realidad de la cantidad de usuarios presentes en la red.

Otras herramientas que pueden ser utilizadas son: NetScanner (Northwest Software), PingScan (PacketTrap Networks), Netdiscover (Backtrack)

Port Scan (Zenmap [2])

Zenmap es la interface grafica de la Nmap, inicialmente desarrollada para Linux por Gordon Lyon, con el fin de "consolidar el campo fragmentado de los analizadores de puertos de propósito especial en una herramienta gratuita potente y flexible"[3], Zenmap es ampliamente conocida y utilizada por principiantes, consultores de seguridad y hackers para obtener información de manera rápida y fácil. Nmap a pesar de ser muy sencillo en su estructura funcional, posee más de 100 opciones diferentes de generación de paquetes sonda, además de las combinatorias generadas por velocidad, tamaño de los paquetes y numero de equipos a verificar, entre otras. El diseño de la interface Zenmap tiene como objetivo facilitar las funciones de scan básicas e intermedias y simplificar la presentación de los resultados obtenidos. Siguiendo con el ejemplo, Zenmap puede ser usado para identificar que servicios están activos en equipos servidores y que puertos están disponibles para realizar conexiones en equipos de red, la información de respuesta a los paquetes sonda enviados por Nmap puede ser usada para identificar el tipo, fabricante y función del equipo escaneado. Para el ejemplo realizamos escaneo para los equipos encontrados mediante IP Angry.

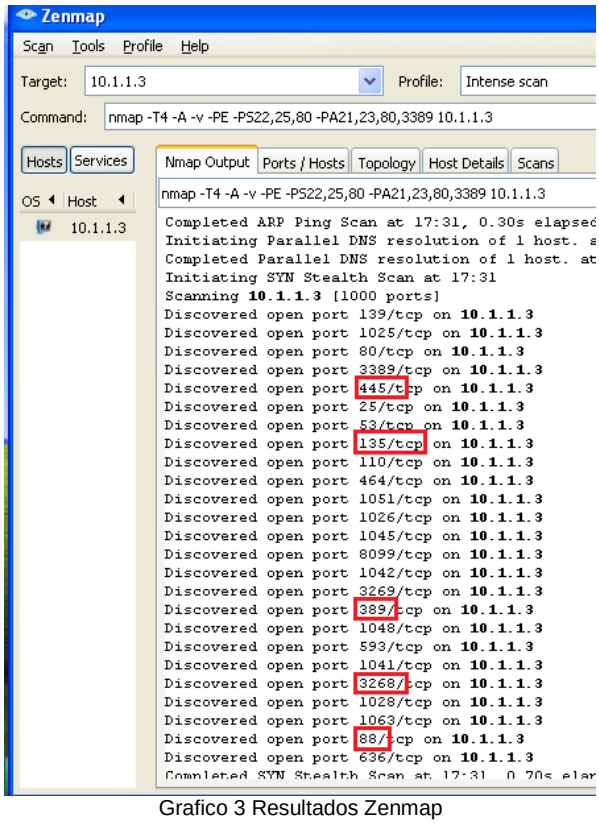

Grafico 3 Resultados Zenmap

Esta información en si misma no es muy significativa pero mediante su análisis detallado pueden ser determinados los servicios activos, procesos en ejecución en los equipos y posibles fallas de seguridad presentes.

En este caso (Grafico 3), encontramos los puertos 88 (Krbs), 135 (RCP), 445(SMB) 3268 (GC) y 389 (LDAP) como abiertos, Comparándolos con bases de referencia[4] se puede determinar que los puertos están relacionados con los servicios de replicación de Active Directory en un Controlador de Dominio.

Mas importante que saber que el equipo tiene X o Y puertos abiertos hemos descubierto que cumple funciones de controlador de dominio de la red[5].

[2] http://nmap.org/zenmap/ (Consulta el 2 de Junio de 2012)
[3] http://nmap.org/book/preface.html#preface-intro (Consulta el 2 de Junio de 2012)
[4] http://technet.microsoft.com/es-es/library/dd772723%28v=ws.10%29.aspx (consulta 10 de Junio de 2012)
[5] http://support.microsoft.com/kb/832017 (consulta 10 de Junio de 2012)

Scan Equipos de red (Cisco Network Assistant CNA)[6]

A pesar de no ser herramientas específicamente concebidas para la recolección de información sino para la administración de redes, programas como Cisco Network Assistant ofrecen muchas funcionalidades en el reconocimiento automático de equipos de capa 2 y capa 3.

Mediante la configuración de las credenciales de un equipo "Semilla" y perfiles de conexión, CNA busca información mediante protocolos como SNMP, ICMP, TELNET, HTTP, STP y CDP acerca de equipos de red conectados. Luego de encontrarlos, CNA usa las credenciales configuradas para leer información de estado, conexiones, y configuración y a partir de esta información continuar su búsqueda. El uso de esta herramienta en reconocimiento de Red presenta muchas ventajas como:

a) Se realizan búsquedas de equipos en múltiples protocolos de una manera rápida y sencilla, búsquedas que de otra manera requerirían tiempo y conocimiento técnico considerables.

b) La información recolectada es mostrada en una interface grafica sencilla y fácil de entender (Grafico 4).

c) Es una herramienta gratuita, fácil de instalar y manejar.

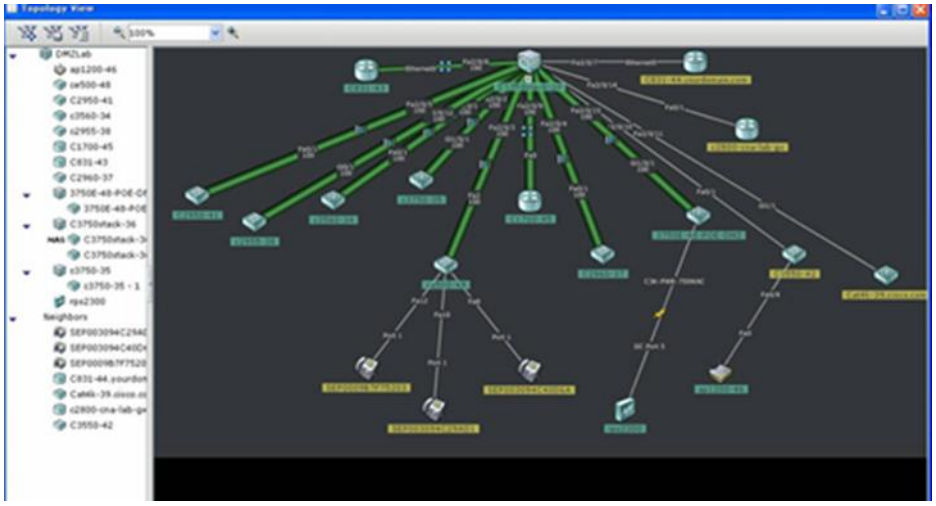

Grafico 4 Cisco Network Assistant [7]

Dentro de la información dada inicialmente para el aseguramiento de la red no se observa información alguna acerca de los equipos Switches que actualmente se encuentran brindando servicio, esta situación de fallas de documentación en equipos de capa 2 es muy común. En casos como este, las herramientas de Administración centralizada son de gran utilidad, ya que permiten a los administradores de red, identificar características como el uso

[6] http://www.cisco.com/en/US/products/ps5931/index.html (consulta 14 de Junio de 2012)
[7] Getting Started with Cisco Network Assistant, Cisco Systems, San Jose USA, 2009

de procesador y de memoria, roles, tipos de conexiones, estado de las conexiones de los equipos que prestan servicio en la red.

La mejor manera de comenzar seria la configuración de las credenciales del equipo central, (switchcore) en el CNA, este realizara las tareas de identificación de switches y routers conectados directamente. En caso de no contar con credenciales de acceso a todos los equipos encontrados podemos usar las credenciales default de acceso, es muy probable que si la red no ha sido documentada y se encuentra en un grado de descuido como en el que se observa en el grafico 1, los accesos sean los dados por el fabricante.

En páginas como *pcsupport.about.com*[8], encontramos los credenciales de usuario, contraseña y dirección de administración para modelos específicos de Switches y Routers. El reconocimiento de esta herramienta suele demorar de 2 a 3 minutos por cada equipo encontrado y ya que es una herramienta gratuita solo agregara hasta 40 equipos en la red, lo que para redes pequeñas y medianas es más que suficiente.

La información dada por este tipo de herramientas sirve como base para ampliar nuestro conocimiento sobre la red, pero si se desea realizar un mapa completo de equipos de red y sus relaciones, debemos realizar una inspección mas profunda, mediante las interfaces CLI de los equipos.

Otras herramientas: WhatsUp, NetBrain, OpenNms…

Actualizando el grafico de la red con la información recolectada con estas sencillas herramientas (Grafico 5), se evidencia fácilmente la cantidad de información que podemos extraer con unos cuantos programas gratuitos y un análisis detallado de la información que ellos nos brindan. Hasta este punto no hemos tenido acceso a equipos de red ni acceso directo a los servidores.

En color rojo se observa la información obtenida con las herramientas, mediante Ping scan determinamos un valor aproximado de los usuarios de la red activos en cada segmento de red y los saltos en capa tres que debe dar el trafico para alcanzar su destino, mediante Zenmap obtenemos información acerca de los servicios activos en los servidores de la granja, y podemos diferenciar direcciones usadas por equipos pc y las direcciones usadas por equipos de red como routers y switches, y finalmente mediante el uso de programas como CNA, se obtiene información acerca de equipos de red no referenciados, conexiones entre ellos, topología física de red, Velocidad de conexiones y estado de las mismas.

[8] http://pcsupport.about.com/od/cisco-default-passwords/cisco-default-passwords.htm Consulta el 14 de junio de 2012

En la siguiente etapa de la identificación de servicios se tendrá acceso directo a los equipos red y su configuración, pero es muy importante y un hecho digno de subrayar la cantidad de información que podemos obtener sin tener acceso directo a los equipos, únicamente con el uso de estas herramientas y sin mayor intervención por parte del Usuario.

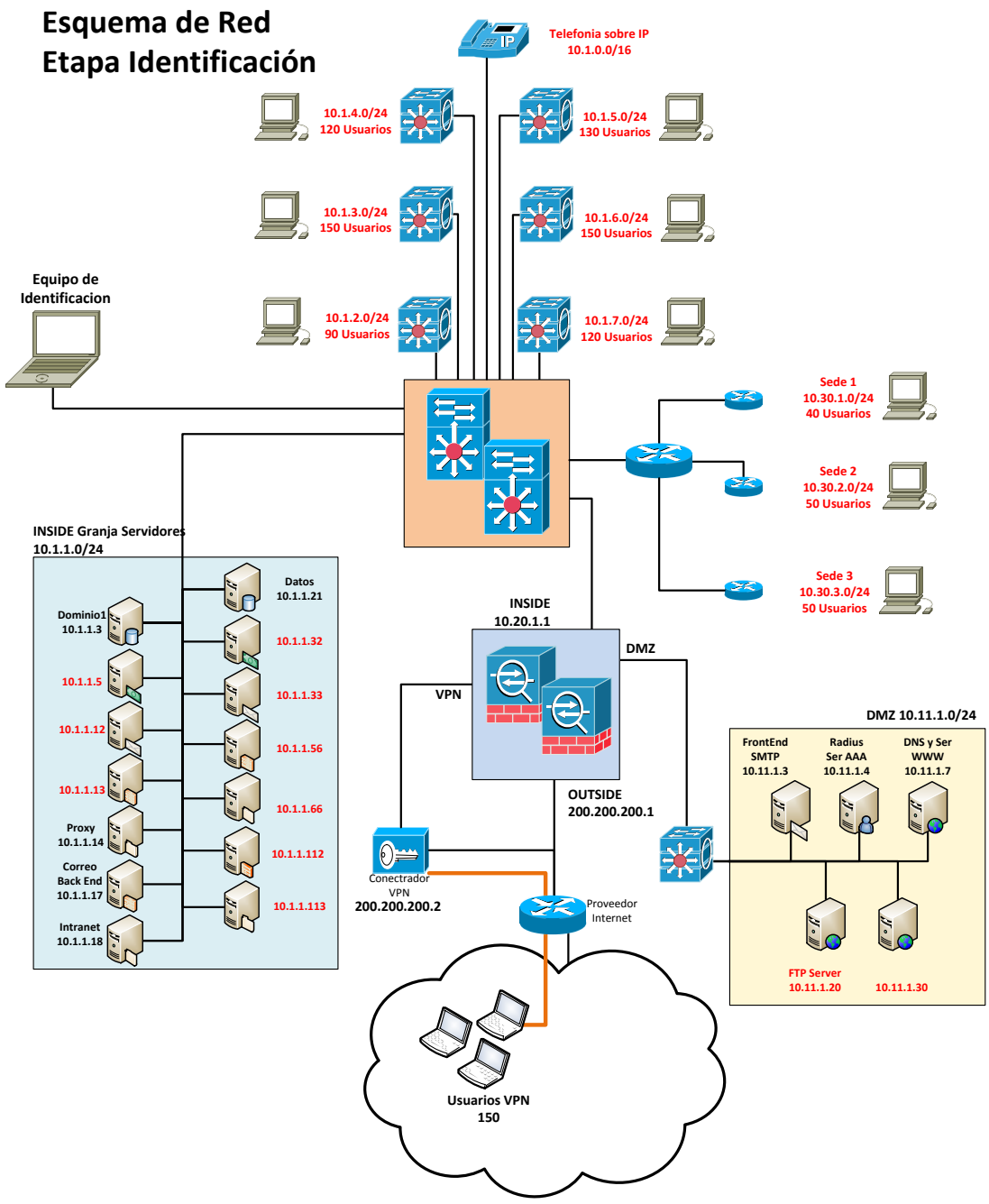

Grafico 5 Red de Datos 1° Etapa Identificación.

Verificación de Configuración y comandos CLI para equipos Cisco (Switches y Routers)

Información mas profunda y detallada acerca de los equipos de red requiere la revisión de las configuraciones y el estado de sus conexiones, estas tareas deben realizarse directamente en las consolas de administración.

Esta revisión requiere un nivel de conocimiento mas alto de los equipos y en algunos casos podrían llegar a afectar el desempeño de la red en producción, algunos de los comandos que se sugerirán en esta sección del trabajo pueden producir cargas de procesamiento en los equipos de red o modificaciones en la topología de STP, lo que hace que estas tareas necesiten de una atención mas alta que las descritas en la primera parte de Identificación.

Lo primero será verificar la configuración actual de los equipos mediante el comando s*how running-config,* para el caso de esta red asumiremos que la única configuración fuera lo común será la de HSRP junto con otro Switch de iguales características (BackupSwitchcore).

Conexiones Físicas.

Es muy Importante mantener documentado para cada equipo de red, con que equipos están conectados, en que puerto especifico y que parámetros posee esta conexión, esto con el fin de disminuir el tiempo de respuesta en el evento de fallas o caídas de servicio, cambios de configuración y modificación de parámetros de conexión.

show interface status

Switchcore# *Show interface status*

Port	Name	Status	VLAN	Duplex	Speed	Type
Gi1/1		connect	Trunk	a-full	a-100	10/100BaseTX
Gi1/2		connect	Trunk	a-full	a-100	10/100BaseTX
Gi1/3		connect	Trunk	a-full	a-100	10/100BaseTX
Gi1/4		connect	Trunk	a-full	a-100	10/100BaseTX
Gi1/5		connect	Trunk	a-full	a-100	10/100BaseTX
Gi1/6		connect	Trunk	a-full	a-100	10/100BaseTX
Gi1/7		connect	Trunk	a-full	a-100	10/100BaseTX
Gi1/8		connect	Trunk	a-full	a-100	10/100BaseTX

show ip interface brief

Switchcore# *show ip interface brief*

Interface	IP-Address	OK?	Method	Status	Protocol
VLAN1	10.1.1.1	YES	NVRAM	up	up
VLAN2	10.1.2.1	YES	NVRAM	up	up
VLAN3	10.1.3.1	YES	NVRAM	up	up
VLAN4	10.1.4.1	YES	NVRAM	up	up
VLAN5	10.1.5.1	YES	NVRAM	up	up
VLAN6	10.1.6.1	YES	NVRAM	up	up

La salida de estos comandos muestran que, los puertos Giga-Ethernet del 1 al 7 del Switchcore están actuando como puertos trunk comunicándose a otros Switches, el estado de los puertos es el de dynamic-desirable, (dúplex A-full, speed a-full) lo que en la practica quiere decir que, ante una nueva conexión, el Switch intentara negociar de manera dinámica el estado del puerto y tratara de establecer preferiblemente un puerto trunk, este comportamiento es muy poco deseable a nivel de seguridad ya que un puerto trunk, puede llevar información de cualquiera de las VLANs configuradas en el equipo , además de poder crear inestabilidad en el estado de la red, debido a cambios en el STP. También se observa que las interfaces de las VLANs usadas (default Gateway para cada subred) se encuentran configuradas en el equipo Switchcore, lo que muestra que los switches intermedios entre los usuarios de las 6 primeras VLANs y el core están configurados como switches capa 2, este punto es importante ya que demuestra la importancia que tiene en la red la correcta configuración del protocolo Spanning Tree.

La topología de Spanning tree es una de las características de los equipos de Capa 2 que menos atención recibe en el diseño e implementación de una red, esta situación se presenta en primera medida porque se da por sentado el correcto funcionamiento del protocolo STP para cualquier arquitectura de red, además el crecimiento de una red empresarial en muchas ocasiones no es planeado detalladamente, sino que responde necesidades de crecimiento rápido; la preocupación por mantener sin interrupciones el servicio impide que el personal responsable de la Administración de la red analice de una manera profunda los cambios realizados y el impacto que estos traerán en el desempeño de los equipos, esta falta de atención, ya sea por tiempos o por complejidad de las tareas genera muchos inconvenientes.

Show spanning tree y show spanning tree summary.

Switchcore#show spanning-tree

VLAN0001

Spanning tree enabled protocol ieee

Root ID Priority 16384

Address c8f9.f945.2ca3

Cost

Port 1 (Gigaethernet 1/1)

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

Bridge ID Priority 32768 (priority 32768 sys-id-ext 1)

Address 000f.2493.af80

Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec

```
        Aging Time 300
Interface       Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
GE 1/1          Root FWD 19        128.1    P2p
```

Switchcore# show spanning-tree summary

```
Extended system ID                 is enabled
Portfast Default                   is disabled
PortFast BPDU Guard Default  is disabled
Portfast BPDU Filter Default     is disabled
Loopguard Default                  is disabled
EtherChannel misconfig guard is enabled
UplinkFast                         is disabled
BackboneFast                       is disabled
Configured Pathcost method used is short
```

Este equipo aun siendo el Switchcore, no es el switch Root para el Spanning tree de la red, además la configuración de prioridad y de protección para la topología están en sus valores de fabrica (Default). La configuración de esta parte de la red será parte de la etapa de Aseguramiento.

Con fines de documentación para los pasos siguientes será necesario obtener información acerca de los puertos físicos en donde se encuentran conectados los demás equipos Switch y Servidores de aplicaciones, bases de datos, servidores web y demás… para esto puede consultar las tablas CAM de los switches, teniendo en cuenta que ya tenemos las direcciones MAC de los equipos gracias a la primera etapa de identificación. (CDOMINIO 000C.293B.FFDA)

Switchcore #show mac-address-table | include 000C.293B.FFDA

```
1      000C.293B.FFDA    DYNAMIC     GE1/15
```

Este comando solicita información acerca del puerto por el cual se conoció la dirección de MAC dada, el numero uno en la muestra la VLAN a la cual el puerto ha sido configurado.

CDP Cisco Discovery Protocol[9]

Cisco Discovery Protocol es un protocolo propietario de Cisco que funciona en la capa de enlace de datos, su tarea principal es brindar información de los equipos de red que estén conectados directamente a un equipo cisco.

El Protocolo funciona de la siguiente manera, por default cada 60 segundos envía trafico a la dirección MAC 0100.0CCC.CCCC con información acerca de sistema operativo, versión, dirección IP, la información recibida es guardada por en una tabla de Adyacencias o de "neighbors" junto con el tiempo que fue recibida, la información de un equipo especifico será borrada luego de 180 segundos de no recibir actualización. Este tipo de información es muy útil en la identificación de equipos y en la elaboración de un mapa de red detallado, pero representa un riesgo de seguridad ya que revela muchísima información acerca de los equipos de red, sus sistemas operativos y funcionalidades.

Para el caso de la red ejemplo, desde el Switchcore se ejecutaran los comandos, Show cdp neighbors y Show cdp neighbors detail para saber que equipos están conectados directamente al Switch, por cuales puertos, las direcciones de Administración y las versiones de sistema operativo de los equipos.

Switchcore#show cdp neighbors

Device ID	Local Intrfce	Holdtme	Capability	Platform	Port ID
Bckpcore	Gig 1/1	168	R S	4506	Gig 1/1
Edificio2	Gig 1/2	168	S	3750	Gig 1/0/1
Edificio3	Gig 1/3	168	S	3750	Gig 1/0/1
Edificio4	Gig 1/4	168	S	3750	Gig 1/0/1
Edificio5	Gig 1/5	168	S	3750	Gig 1/0/1
Edificio6	Gig 1/6	168	S	3750	Gig 1/0/1

Switchcore#show cdp neighbors detail

Device ID: Edificio2

Entry address(es): IP address: 10.1.2.253

Platform: cisco 3750, Capabilities: Switch

Interface: GigaEthernet 1/2, Port ID (outgoing port): GigaEthernet1/0/1

[9] http://www.cisco.com/en/US/tech/tk648/tk362/tk100/tsd_technology_support_sub-protocol_home.html consulta 27 de Junio de 2012

Holdtime : 156 sec

Version : Cisco Internetwork Operating System Software

IOS (tm) 3700 Software (C3750-ADVENTERPRISEK9-M), Version 12.3(26), RELEASE SOFTWARE (fc2)

Technical Support: http://www.cisco.com/techsupport

Copyright (c) 1986-2008 by cisco Systems, Inc.

Compiled Mon 17-Mar-08 17:42 by dchih

advertisement version: 2

VTP Management Domain: ''

Duplex: full

Verificando la información dada por los comandos se observa que es muy amplia, permitiendo modelar de una manera detallada la topología de la red y los servicios que sobre ella corren.

La utilidad de este tipo de protocolos de descubrimiento llevo a la IEEE al desarrollo del Estándar 802.1ab (LLDP Link Layer Discovery Protocol[10]) que permite realizar las mismas tareas de CDP en un ambiente de equipos de red de diversos vendedores.

Si realizamos la consulta de direcciones MAC de los equipos que conocemos y la analizamos junto con la información de CDP podemos llegar a un grafico de red como el siguiente.

[10] http://standards.ieee.org/getieee802/download/802.1AB-2005.pdf Consulta 27 de Julio de 2012

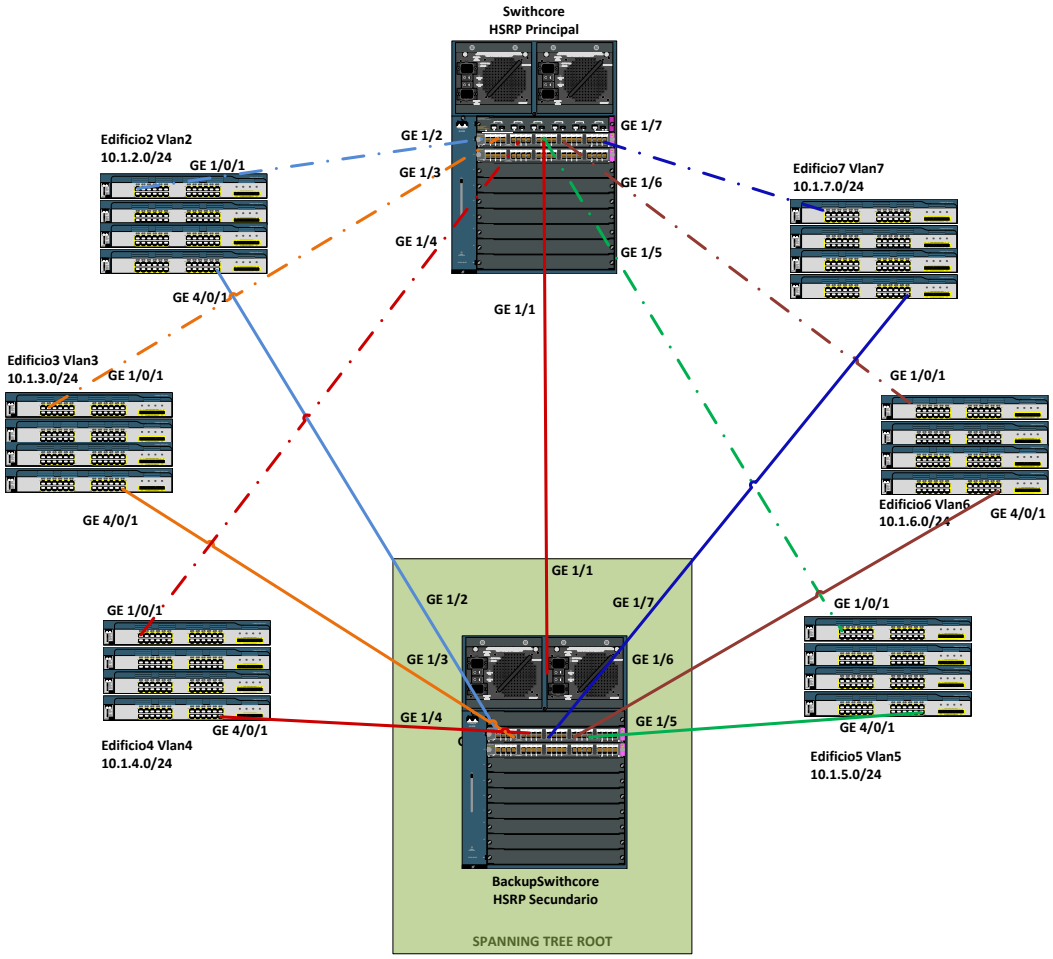

Grafico 6 Conexiones STP Switches.

Analizadores de protocolos

Los analizadores de protocolos son una de las herramientas más útiles en las tareas de identificación de servicios en una red de datos. Programas como WireShark permiten capturar, analizar y observar el flujo de datos además del contenido de los paquetes transmitidos en una red funcional.

Por estas características, un analizador de protocolos será la herramienta ideal en la identificación de comportamiento y requerimientos de las aplicaciones que se ejecutan en la red de datos. En muchas ocasiones no basta con un escaneo de puertos a los equipos servidores para conocer que servicios prestan, algunas aplicaciones solo abren sus puertos hasta que son requeridos (uso de puertos dinámicos) o abren sus puertos de servicio luego de una secuencia de solicitudes a otros puertos (Port Knocking).

La modelación completa de los servicios de una red, requiere el uso de estas herramientas. En este caso, se usara esta herramienta para modelar el comportamiento y necesidades del Controlador de dominio equipo con la dirección 10.1.1.3.

Para lograr analizar el tráfico de datos del controlador de dominio, se usara la configuración SPAN (switch port analyzer), para duplicar el tráfico del puerto conectado al controlador de dominio, a un puerto de nuestra selección.

Monitor session *1* **source** *FE0/1* **both**

Monitor session *1* **destination** *FE0/20*

Cuando se usa la funcionalidad SPAN es conveniente hacer las siguientes recomendaciones.

a) El Caudal de tráfico de puertos específicos puede ser muy alto, dependiendo de la configuración, de la memoria y capacidad de procesamiento, la configuración de SPAN, puede traer problemas de desempeño en el Switch.
b) Por consideraciones legales es necesario tener autorización para realizar análisis que involucre copia de tráfico de datos.
c) Debido al caudal de información que generan algunos equipos, es recomendable que el equipo en el que se recolectan los datos, tenga gran capacidad de procesamiento y memoria.

En el equipo Analizador se usara el programa Wireshark para realizar la captura. Ya que deseamos realizar un reconocimiento únicamente de los puertos y protocolos usados por el controlador de dominio, no necesitamos capturar los paquetes en su totalidad (de 576 y 1500 Bytes) configuraremos el equipo para capturar únicamente el encabezado de cada paquete (20 - 80 bytes), En el menú Capture > Options > Seleccionar - Limit Each packet to…. y colocar 80 Bytes, de esta manera, el tamaño del archivo de captura será mucho mas pequeño y fácil de manejar.

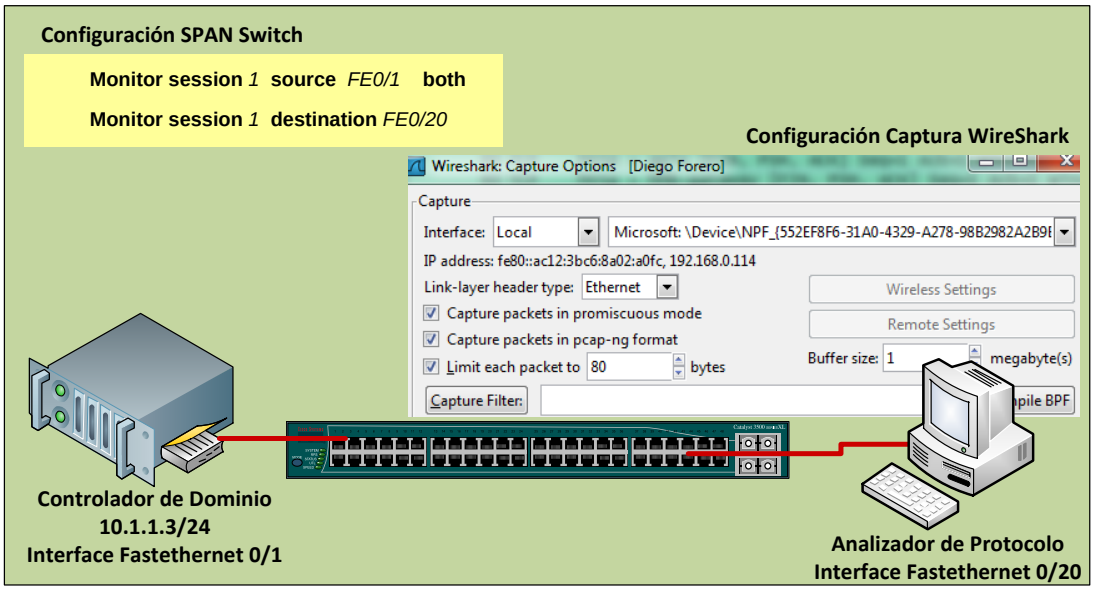

Grafico 7 Configuración Captura de trafico

Luego de realizar la captura, la información debe ser analizada para observar los requerimientos de puertos, servicios y anchos de banda tienen los equipos para cumplir con sus funciones.

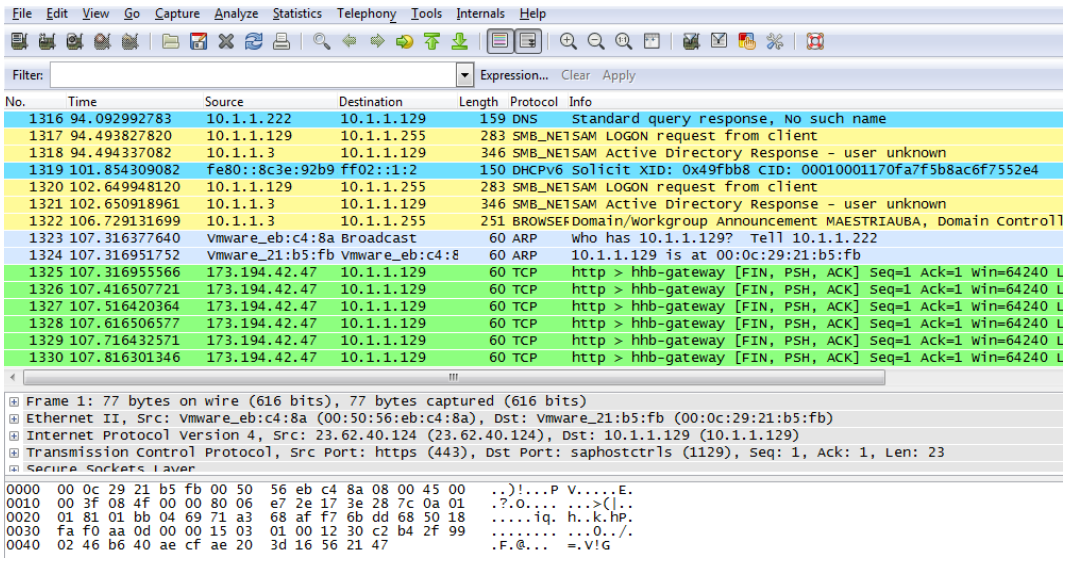

Grafico 8 Captura (Visualización Wireshark)

En esta captura (grafico 8) se observa el proceso de autenticación de un equipo miembro del dominio de dirección 10.1.1.129, contra el controlador del Dominio MAESTRIAUBA. De esta captura podemos detalla los puertos necesarios y los protocolos usados por los equipos de una red.

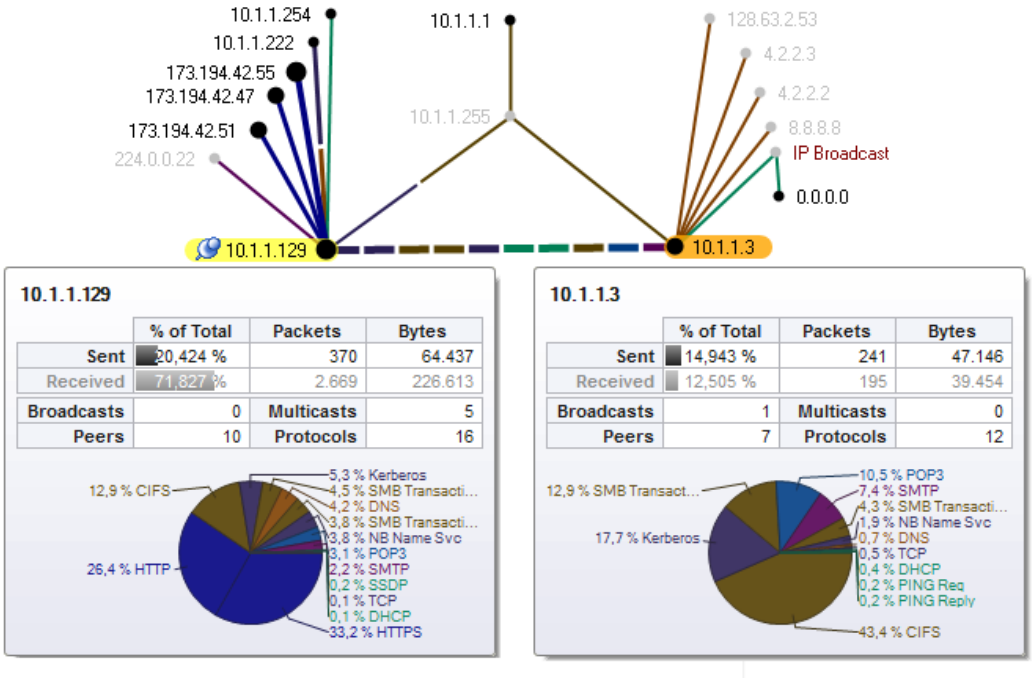

Grafico 9 Captura (Visualización Omnipeek)

Usando la misma captura de trafico pero utilizando el programa Omnipeek, podemos observar de una manera grafica y mucho mas sencilla el mismo

proceso de autenticación visto en el Grafico 8, adicionalmente se observan servicios comúnmente utilizados en una arquitectura de Active Directory, el tipo de protocolos usados, relaciones de conexión entre equipos, niveles de broadcast, cargas de trafico e incluso porcentajes de utilización.

Otros programas de análisis de protocolos de red: Wireshark(gratis), Capsa(gratis), CACE Pilot, Omnipeek.

Como se puede observar las tareas de identificación de servicios y activos de una red, requieren comparativamente poco esfuerzo pero brindan un caudal de información esencial para el mantenimiento, monitoreo y aseguramiento de una red de datos

Análisis Amenazas

Ahora que se tiene un mapa completo de la red y de los servicios que esta presta, la pregunta es ¿Contra qué se debe proteger a los equipos? En esta etapa se realizara una exploración de algunos tipos de ataques dirigidos a los switches, con el fin de entender de una manera profunda su funcionamiento. Esta información permitirá tomar medidas para mitigar o disminuir su efecto ante una posible ocurrencia

MAC-Flooding

MAC Flooding también conocido como CAM Overflow es un tipo de ataque usado para afectar el funcionamiento normal de un Switch. Fundamentalmente consiste en bombardear a un Switch con un número muy grande de direcciones MAC falsas, el switch registrara estas direcciones MAC en su tabla CAM (la tabla CAM es usada para seleccionar los puertos por donde será enviado el trafico que llega al Switch), después de cierto tiempo de recibir direcciones falsas, la tabla CAM llegara a su máximo de capacidad de almacenamiento, al llegar a esta situación el switch no podrá aprender mas direcciones MAC y no podrá tomar decisiones acerca de los puertos destinos del trafico, Dada esta situación critica el switch tratara de mantenerse en operación y empezara a enviar copia de todos los paquetes que llegan a él, por todos los puertos disponibles, de la misma manera que lo hace un HUB.

Luego de lograr este comportamiento en el Switch, un atacante no tendría que hacer más que abrir un Network Sniffer para tener acceso a todo el tráfico que se genera en su segmento de red.

Como podemos ver este sencillo ataque tiene gravísimas consecuencias en la seguridad de los datos, sin mencionar el aumento en el tráfico, el aumento en los tiempos de respuesta y la posible caída de la red, debido a la sobrecarga en el procesamiento de los equipos involucrados.

Programas como Dsniff para Windows son capaces de generar este tipo de tráfico. En este caso usaremos el programa macof para Linux para analizar el funcionamiento de este ataque.

En el grafico 10 se observa el estado normal de un switch su tabla de MAC dinámica y el número total de posiciones disponibles en la tabla CAM.S e ejecutan los comandos show *mac-address-table dynamic* y *show mac-address-table count* para observar el estado de la tabla CAM.

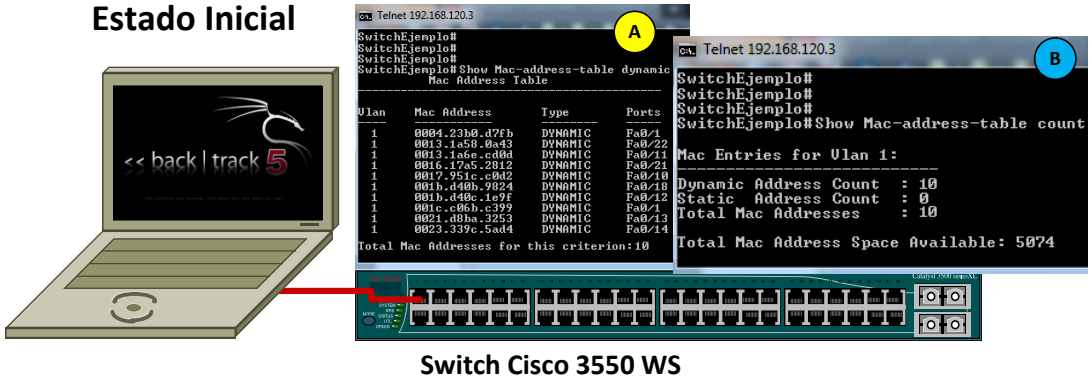

Grafico 10 MAC Address Table Funcionamiento normal.

Se observa que el switch ha aprendido dinámicamente solo 10 direcciones (grafico 10A) en la VLAN 1 tiene 5074 (grafico 10B) posiciones disponibles en su tabla CAM para aprender nuevas direcciones.

Ahora desde la Maquina conectada, se ejecutara el comando *macof,* este comando generara trafico TCP con direcciones origen y destinos falsa con direcciones MACs diferentes, esto hará que el Switch llene su tabla CAM y se comporte como un HUB.

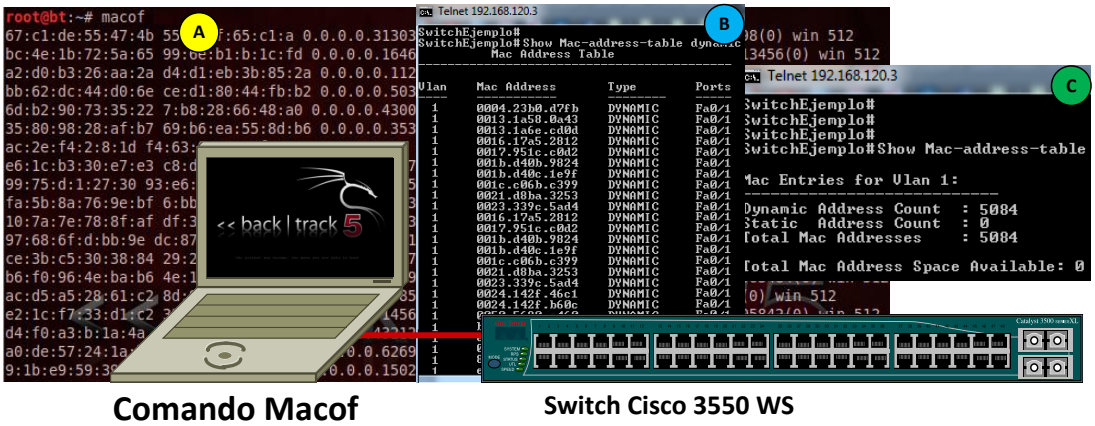

Grafico 11 Ataque MAC Overflow

Luego de tan solo 15 segundos se generaron alrededor de 35000 paquetes TCP con MACs diferentes el comando *macof* (grafico 11A), rebasando la capacidad de la tabla CAM del Switch, todas las direcciones aprendidas por el Switch llegaron por el Puerto Fa0/1 (grafico 11B) además, no hay disponibilidad de memoria en el Switch para aprender direcciones nuevas.

Luego de esto, lo único que tendría que hacer un Atacante para tener acceso a todo el tráfico de VLAN 1 seria abrir un Network Sniffer y empezar a escuchar.

VLAN Hopping[11]

Este ataque de VLAN hopping o salto entre VLANs consiste básicamente en hacer que el trafico generado en un puerto configurado en una VLAN especifica pase a otra VLAN, sin necesidad de que sea direccionado por un equipo en Capa 3. Este tipo de ataque se divide en dos tipologías, VLAN Hopping por Trunk falso y VLAN Hoping por Doble Tag

VLAN Hopping por Trunk Falso.

Esta división del ataque de VLAN hopping consiste en obtener un puerto trunk con un switch que pertenezca a una red objetivo, mediante la conexión de otro Switch extraño a la red o mediante la modificación y envío de paquetes DTP desde un computador atacante. Este ataque aprovecha de la configuración default de "*Dynamic Desirable"* de todos los puertos de los switches cisco, gracias a ella, el Switch Legitimo esperara paquetes DTP con la intención de negociar un Puerto Trunk, lo único que tendría que hacer un atacante es conectar un switch extraño configurado de la misma manera a uno de estos puertos para que se establezca un puerto Trunk, y luego de esto, en el Switch extraño se pueden configurar los puertos para tener acceso a cualquiera de las VLANs que el Switch legitimo tenga acceso.

Otra manera de lograrlo sin la necesidad de un Switch es mediante un programa como Yersinia, (Linux), este programa crea paquetes DTP con el fin de engañar al Switch haciéndolo pensar que en el puerto en donde se encuentra conectado el computador, esta un Switch tratando de negociar un puerto trunk. Para acceder a este programa en la distribución Backtrack click *en Backtrack>Priviledge Escalation>SpoofingAttacks>NetSpoofing>yersinia* y teclear *yersinia –G*

[11] Securing Networks with Cisco Routers and Switches Vol 1, Cisco, San Jose CA USA 2007 pp 47-49

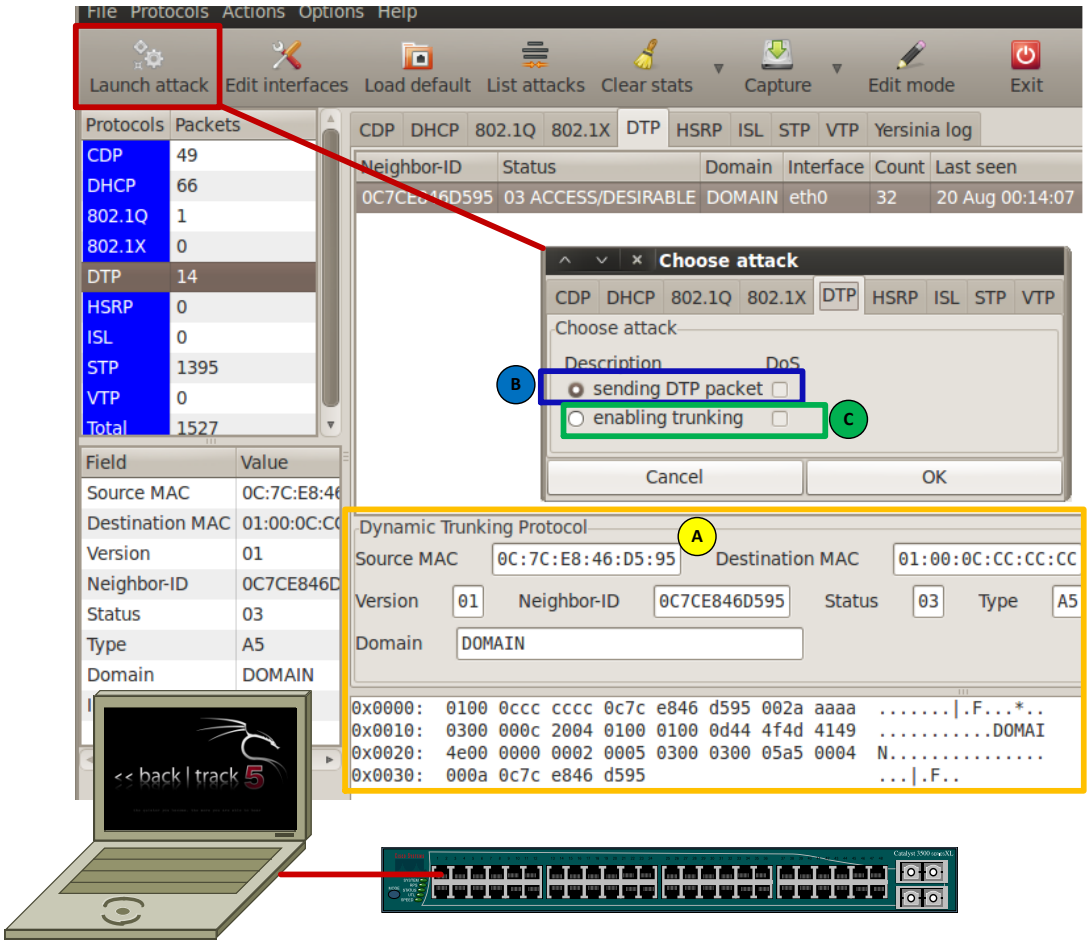

Grafico 12 VLAN hopping Trunk Falso

Los puertos Trunk se negocian automáticamente mediante el Dynamic Trunking Protocol (DTP), como se observa este programa permite crear paquetes con parámetros específicos seleccionados por el usuario (Grafico 12A), para lograr que el un puerto configurado dynamic desirable se convierta en un puerto trunk. Luego de configurar los parámetros correctos se envían paquetes DTP al Switch para que se inicie el proceso de negociación, en primera medida el atacante tratada de que el Switch lo reconozca como equipo de red (Grafico 12B) y luego intentara negociar un puerto trunk (Grafico 12C).

VLAN Hopping por Doble Tag[12] .

Otra manera de enviar tráfico de una VLAN a otra sin pasar por los controles de un equipo de Capa 3 es aprovechando una vulnerabilidad en el protocolo 802.1Q y la característica de VLAN Nativa.

Normalmente en un puerto Trunk todo el trafico esta marcado con la VLAN a la cual pertenece, pero en el tiempo en que se implemento el protocolo

[12] CCNA Security Official exam Guide, Michael Watkins, Cisco Press , Indianapolis USA 2008

802.1Q no todos los equipos de red tenían la capacidad de taguear trafico con esta información (Concentradores y Hubs), entonces para facilitar las tareas de implementación la IEEE incorporo la característica de VLAN Nativa, esta permite que el trafico de una VLAN especifica no requiera tag para ser comunicado entre los Switches en un puerto trunk, por default esta red es la VLAN1.

Si un atacante tiene acceso a un puerto de VLAN nativa y logra diseñar paquetes con un tag adicional que pertenezca a otra VLAN, estos paquetes podrán llegar a equipos no autorizados en redes bloqueadas.

Para demostrar este comportamiento, se usara nuevamente la herramienta yersinia para Backtrack 5 y la topología mostrada en el grafico 13

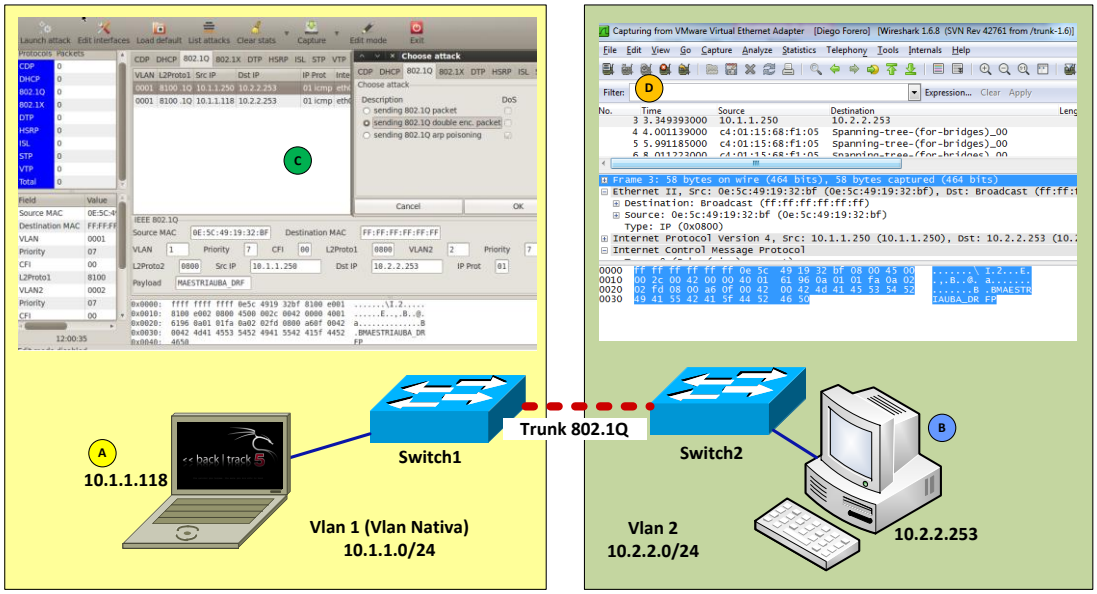

Grafico 13 VLAN Hopping por doble tag

El equipo de donde se realizará la prueba es el 10.1.1.118 (Grafico 13A) y esta conectado al Switch1 configurado en la VLAN 1 que es la VLAN Nativa por defecto, este equipo tratara de enviar trafico al equipo 10.2.2.253 de la VLAN2 (grafico 13B) conectado al Switch2.

Mediante el Programa Yersinia, creamos paquetes con destino 10.2.2.253 y doble tag, primer tag VLAN1(nativa) y segundo tag VLAN2 (Grafico 13c); al llegar el paquete al Switch1, se eliminara el primer tag y se enviara al Switch2, esto hace que el tag de VLAN2 quede activo, El Switch2 recibirá el paquete por el puerto trunk y lo procesará, asumiendo que el tag(VLAN2) del paquete es valido, ahora el Switch2 simplemente redirecciona el trafico a la VLAN marcada por el tag y entregará el paquete al equipo destino (Grafico 13D).

Se observa que el trafico generado en ningún momento necesito un equipo capa tres para su redirección a pesar de pertenecer a dos segmentos de red

totalmente diferentes, evadiendo así reglas de Inspección de protocolo y bloqueos por listas de acceso, también se observa que de la misma manera que podemos falsear el destino del paquete, podemos también falsear su origen, haciendo las tareas de detección de este tipo de ataque mucho mas complejas.

DHCP Starvation[13]

DHCP starvation es un vector de ataque relativamente simple y puede ser ejecutado de una manera sencilla, pero que puede tener un gran impacto en cualquier red de datos.

Primero observemos el funcionamiento del protocolo DHCP descrito en la RFC 2131[14](Grafico 14).

1. El cliente envía un mensaje DHCPDISCOVER en su segmento de red Físico, En caso que los servidores DHCP no se encuentren en el mismo segmento de red, Agentes BOOTP pueden pasar el mensaje a la red correcta.
2. Cada servidor puede responder con un mensaje DHCPOFFER que incluye direcciones de red disponibles para préstamo, el servidor de ser necesario puede transmitir el mensaje DHCPOFFER al cliente, utilizando el agente de re envío de BOOTP.
3. El cliente recibe uno o más mensajes DHCPOFFER de uno o más servidores, El cliente elige un servidor para solicitar la configuración de dirección, luego. el cliente difunde un mensaje DHCPREQUEST que debe incluye la opción 'Identificador de servidor' para indicar que servidor que ha seleccionado.
4. Los servidores reciben el DHCPREQUEST enviado por el cliente. Los servidores no seleccionados utilizan la información del DHCPREQUEST como notificación de que el cliente ha rechazado su oferta. El servidor seleccionado compromete la dirección y la enlaza a la MAC del cliente en su base de datos luego de esto, el servidor responde al cliente con un mensaje DHCPACK que contiene los parámetros de configuración IP.
5. El cliente recibe el mensaje DHCPACK con los parámetros de configuración requeridos. En este punto el cliente aplica la configuración y puede inicializar su conexión.
6. El cliente puede enviar un mensaje DHCPRELEASE al servidor para liberar su dirección.

El Ataque de DHCP Starvation consiste en la generación masiva de trafico DHCPREQUEST con direcciones MAC falsas, estas peticiones tienen

[13] Securing Networks with Cisco Routers and Switches Vol 1, Cisco, San Jose CA USA 2007 pp 55-57
[14] http://www.ietf.org/rfc/rfc2131.txt Consultada el 9 de noviembre de 2012

objetivo de agotar las direcciones disponibles para préstamo de un servidor DHCP.

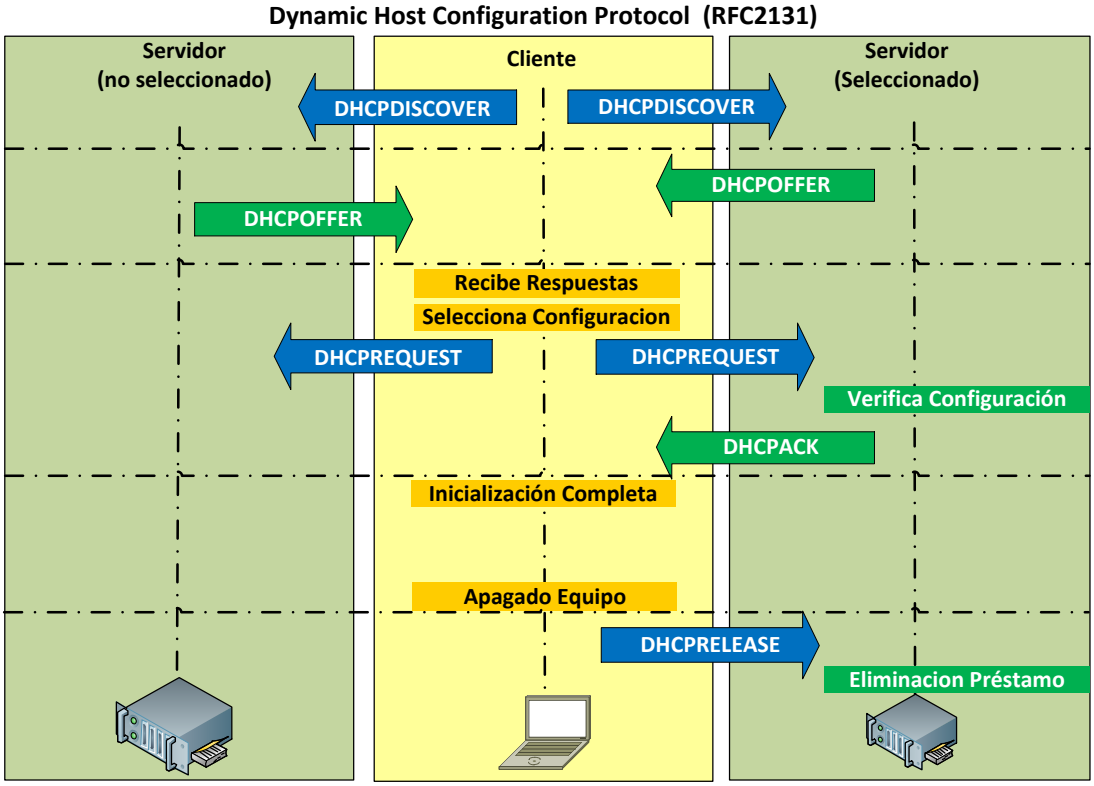

Grafico 14 Funcionamiento DHCP

Los servidores DHCP normalmente no generan muchos problemas y la función DHCP no es verificada a menos que se presenten problemas, lo que hace que sean que normalmente se mantienen desatendidos, estas características hacen del servicio DHCP un objetivo perfecto para la explotación de Vulnerabilidades.

El DHCP Starvation se usa normalmente como ataque de negación de servicio (DoS) ya que impide la conexión de nuevos equipos a la red y es usado como primer paso en un ataque elaborado de Man In the Middle. (MITM).

El comando dhcpstarv –I eth0 para Linux (Grafico 15A), ejecuta un programa que generara múltiples peticiones.

El servidor DHCP responde normalmente a las peticiones de dirección hasta que agota su pool de direcciones (Grafico 15B).

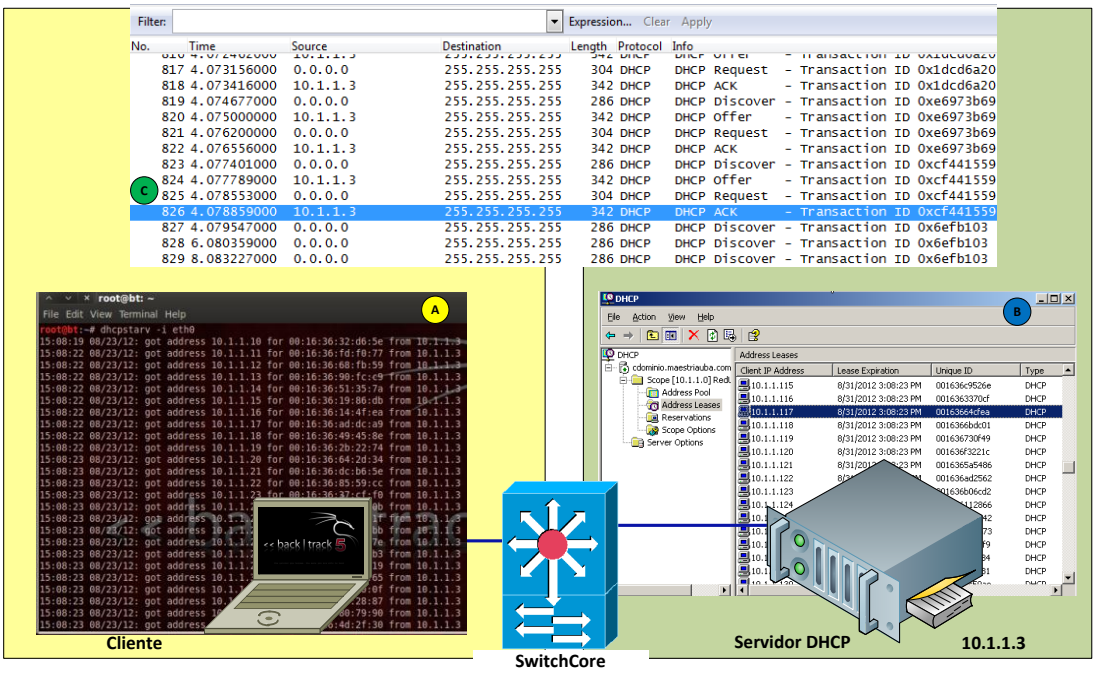

Grafico15 Ataque DHCP Starvation

Es de anotar que este ataque en particular solo necesito 4.07 segundos para agotar las 250 direcciones disponibles en el servidor. Luego de este tiempo el servidor simplemente dejo de responder a los dhcpdiscover (grafico 15C) y en consecuencia no habría direcciones disponibles para los nuevos clientes que deseen navegar, generando así una negación de servicio, o mas delicado aun, este segmento de red estaría disponible para que otro equipo asumiera las funciones de servidor DHCP.

Rogue DHCP Server[15]

El DHCP es uno de los servicios mas usados en las redes de datos, por su facilidad y versatilidad en el manejo de usuarios y direcciones IP, pero no siempre se es consiente de la verdadera importancia que tiene este servicio en una red. En su funcionamiento normal, un servidor DHCP provee la información necesaria a los clientes para poder navegar en una red de datos, información como dirección IP, puerta de enlace, direcciones para resolución DNS.. El ataque de Rogue DHCP server consiste en que sea el Atacante el que provea esta información al usuario con el fin de controlar sus conexiones y observar la información generada y recibida por este.

En si misma, la configuración de un servidor DHCP no representa un ataque a la red , pero ya que provee información esencial para la navegación de los usuarios es un punto vulnerable de la red que suele ser explotado como paso intermedio en un ataque mas sofisticado

[15] Securing Networks with Cisco Routers and Switches Vol 1, Cisco, San Jose CA USA 2007 pp 55-57

En el ataque anterior se demostró como evitar que un servidor DHCP realizara ofertas de direcciones IP en una red. Para la demostración de Rogue DHCP continuaremos desde este punto.

Normalmente los servidores DHCP se encuentran en el mismo segmento de red en donde se encuentran los clientes, ya que el trafico de DhcpDiscover es del tipo Broadcast, si esta situación no se presenta, es necesario configurar los Switches con el comando, *ip helper-address IP_Sev_DHCP,* mas allá de esto, el proceso de asignación de dirección por DHCP transcurre sin la intervención o monitoreo de ningún otro equipo.

Para el ejemplo se utilizara el programa Udhcpd que funcionará como servidor DHCP y el Sslstrip para redireccionar el tráfico del cliente una vez llegue al computador atacante.

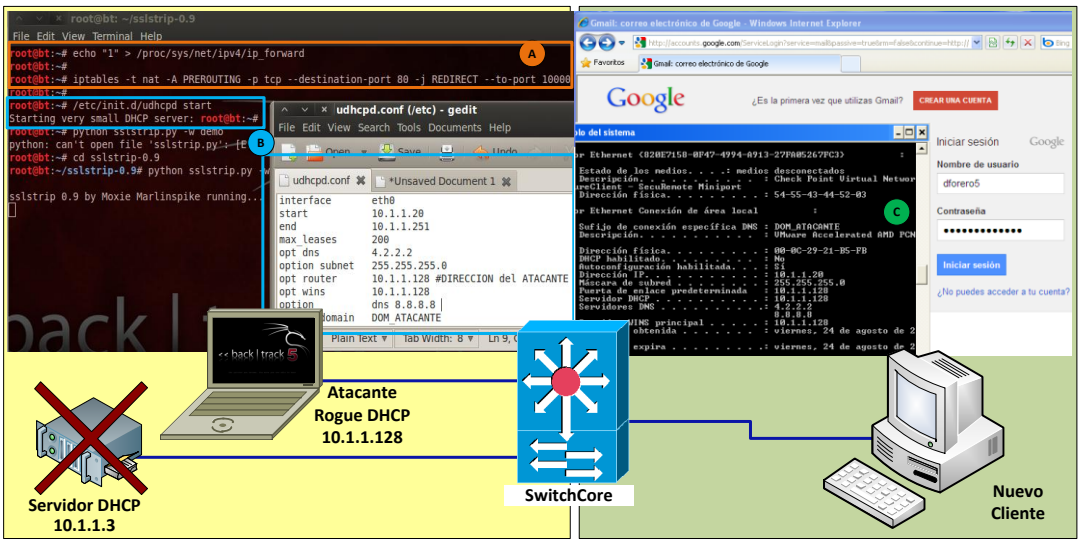

Grafico 16 Rogue DHCP

Antes de comenzar, es necesario prepara el re-direccionamiento del trafico de las posibles victimas, para esto se usara el programa Sslstrip[16], mediante los comandos (grafico 16A)

Echo "1" > /proc/sys/net/ipv4/ip_foward: activara la función de redireccionamiento.

Iptables –t nat A PREROUTING –p TCP –destination-port 80 –j REDIRECT –to port 10000: todo tráfico que llegue por puerto 80 será re-direccionado será redireccionado por el puerto 10000 (puerto a elección del Atacante).

Finalmente *python sslstrip.py –w demo*: iniciara el proceso sslstrip y guardara el contenido de la comunicación capturada en un archivo de texto plano llamado "demo".

[16] http://www.thoughtcrime.org/software/sslstrip/ Consulta el 25 de junio de 2012

Luego de esto se puede iniciar el servidor DHCP falso, este dará direcciones en donde la propia dirección del atacante será el Default Gateway, lo que permitirá que todo el trafico de las victimas pase por el atacante y se capture antes de ser re-direccionado (MITM).El inicio del servicio de DHCP y los parámetros del servidor DHCP son configurados en un archivo se observan en el grafico 16B.

Al conectarse un nuevo cliente a la red, no encontrara el servidor DHCP legítimo y tomara dirección de un servidor que responda al DhcpDiscover, como se observa en el grafico 16C, el equipo acepto la oferta de dirección del servidor Rogue 10.1.1.128, ahora, tanto la dirección de Default Gateway como los DNS configurados en el nuevo cliente se encuentran bajo el control del atacante. Gracias a la redirección de tráfico el cliente no nota ninguna diferencia en la navegación.

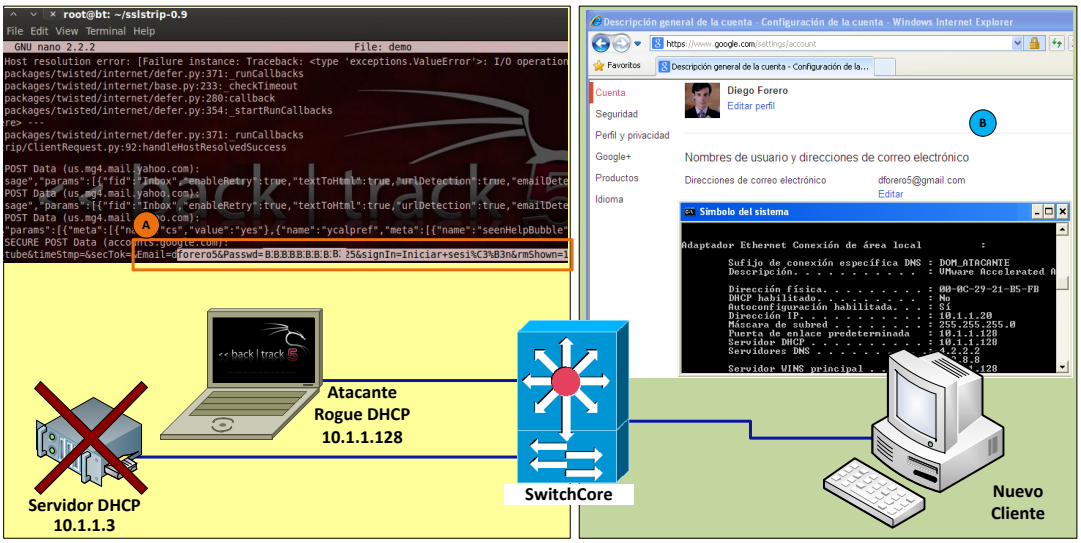

Grafico 17 Rogue DHCP Resultados

En el grafico 17 se observan los resultados del ataque completo, se observa que el trafico generado por el cliente esta pasando por el Computador del Atacante y se ha logrado capturar en el archivo “demo” la cuenta de correo y la contraseña (grafico 17A), esto sin afectar en absoluto la navegación normal de la Victima (grafico 17B). En este punto solo seria necesario que el Atacante abriera un Analizador de protocolos como Wireshark para observar y guardar todos los paquetes generados y recibidos por la Victima.

ARP Poisoning

Otra manera de lograr la redirección del tráfico es el ARP Poisoning, este ataque toma ventaja del Protocolo ARP (Address Resolution Protocol).

Cuando un equipo debe enviar tráfico a otro y los dos comparten el mismo segmento de red, los equipos no hacen uso de sus direcciones IP sino de

sus direcciones MAC, por lo que cada equipo debe mantener una tabla de referencia que relacione estos dos elementos, el protocolo ARP es el encargado obtener una dirección MAC a partir de una IP de la siguiente manera.

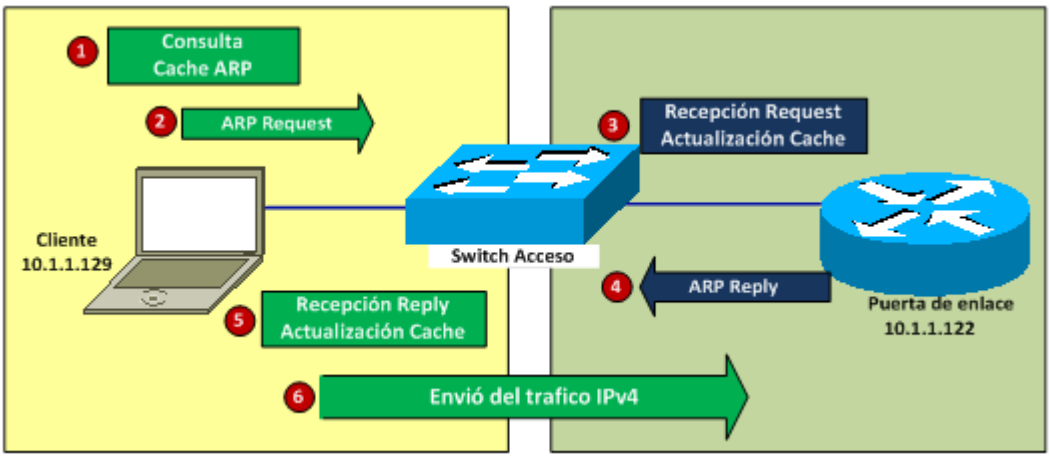

Grafico 18 Funcionamiento ARP

Cuando el cliente 10.1.1.129 tiene trafico para la dirección 10.1.1.122, primero consultará su Cache ARP para ver si tiene la MAC de esta IP, si esta MAC no se encuentra en el Cache ARP, el Cliente enviara en broadcast un ARP Request con su propia información de MAC e IP y la información de la IP Destino. Al recibir la petición ARP, el receptor actualiza su propio Cache ARP y responderá por trafico Unicast con un ARP Reply; el cliente al recibir esta respuesta actualiza su tabla ARP y empezara la comunicación.

Analizando el comportamiento de este protocolo se observa que la parte inicial de la comunicación entre partes se realiza mediante trafico Broadcast y además no hay un método de autenticar a los participantes en los procesos de resolución ARP.

Los ataques de ARP Poisoning aprovechan esta debilidad enviando paquetes ARP falsos a los equipos de una LAN; la recepción de estos paquetes ARP genera la actualización del Cache ARP con información falsa. Como se observa en el grafico 18, cuando el equipo cliente desee iniciar una comunicación con algún miembro de su LAN, el primer paso será consultar su Cache ARP, si esta información es falsa, se podría redireccionar el trafico a un equipo atacante y generar un ataque del tipo MITM.

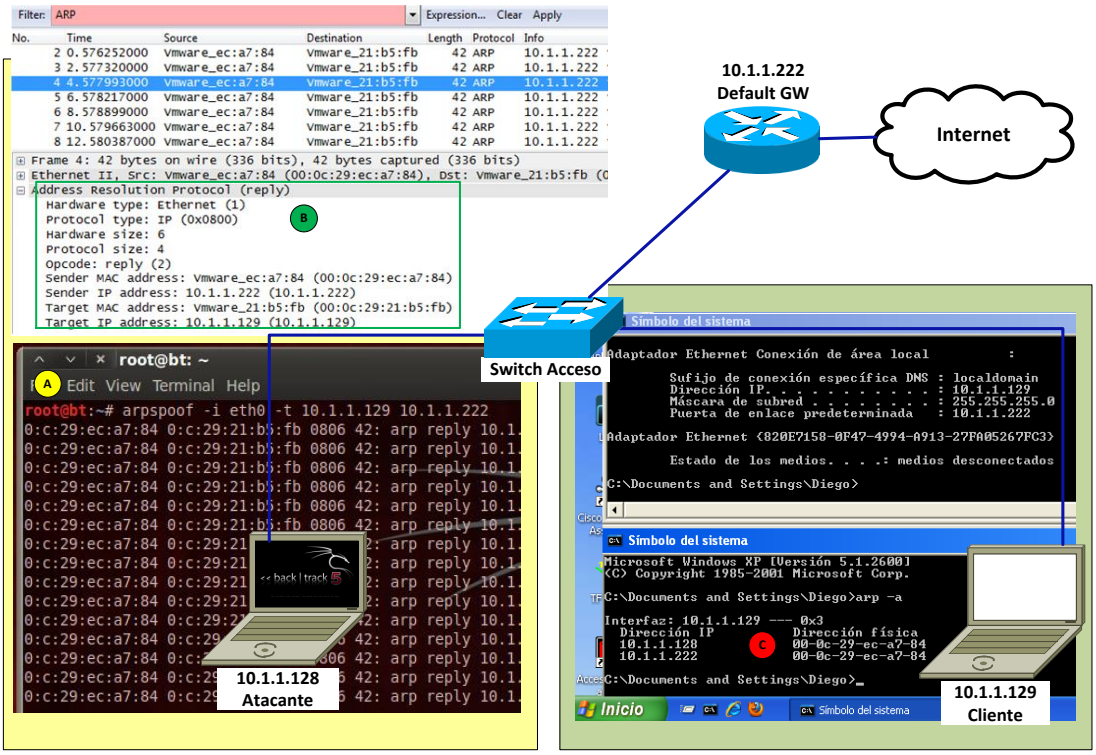

Grafico 19 Comando ARPspoof

Para ilustrar los efectos de este ataque se usara la arquitectura ilustrada en la grafico 19.

Desde el computador atacante conectado a la misma LAN del Cliente, se ejecutara el Comando *arpspoof –i eth0 –t 10.1.1.129 10.1.1.222*,(grafico 19A), este comando generara un flujo continuo de trafico ARP Reply con información falsa sobre la dirección del Default Gateway de la red. (grafico 169) dirigido al cliente de dirección 10.1.1.129.

Cuando el Cliente reciba los ARP Reply falsos, actualizara su Cache ARP, generando un enlace entre la dirección IP del Default Gateway de la red y la MAC del equipo Atacante. (grafico 19C).

Luego de esto, todo tráfico generado por el equipo cliente destinado a la dirección IP del Default Gateway será direccionado al equipo Atacante.

Nuevamente se usara el comando *Echo "1" > /proc/sys/net/ipv4/ip_foward:* para configurar y activar la función de redireccionamiento.

Iptables –t nat A PREROUTING –p TCP –destination-port 80 –j REDIRECT – to port 10000:

Luego se usara el comando *python sslstrip.py –w* para permitir las funciones de Proxy SSL en Backtrack y finalmente se activará un Analizador de protocolos para ver el trafico generado por el usuario con el comando

ethercap -Tq –i eth0

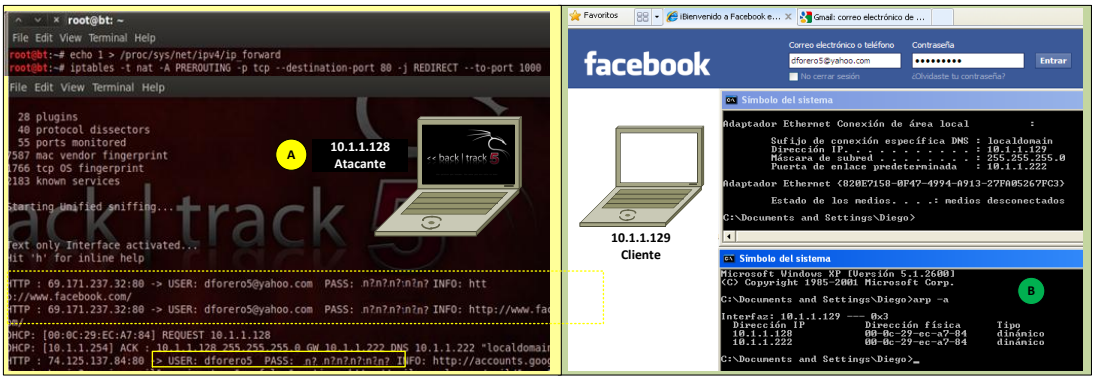

Grafico 20 ARP Poisoning Resultados

En el grafico 20 se observa el resultado del ataque, luego de envenenar el cache ARP del cliente, redireccionar el tráfico y funcionar como Proxy, el equipo atacante puede ver todas las peticiones generadas por el equipo de dirección 10.1.1.129. En el grafico 20A se pueden ver las peticiones realizadas los usuarios y las contraseñas usadas para el ingreso a las páginas, en este caso Facebook y Gmail, todo esto, sin afectar la navegación normal en el equipo de la victima. La única variación que se puede observar es la modificación del Cache ARP (grafico 20B)

Manipulación de Arquitectura STP

En los ataques de manipulación de STP el atacante busca modificar la estructura de Spanning tree de la red, esto lo puede lograr de dos maneras,

1) conectando un Switch extraño a la red o

2) manipulando paquetes generados desde un PC engañando a la red mediante generación de tráfico malicioso logrando así la adición de un Switch falso a la estructura de STP.

Luego de esto, el atacante tiene acceso a la información de la estructura STP y modificar los parámetros de configuración para forzar cambios de arquitectura o hasta para lograr que el switch falso conectado se convierta en el Root Bridge.

Controlar el Root Bridge en una red implica tener control sobre el equipo responsable de calcular la topología de STP a partir de los cambios que se presentan en los demás switches, el Root Bridge tiene acceso a una cantidad importante de información que en otros switches no se encuentra disponible.

Para ejecutar este tipo de ataque desde un PC, es necesaria la lectura y generación de trafico BPDU. En el protocolo STP los Switches se identifican mediante el Bridge ID (BID), El BID esta compuesto por dos partes, la

primera consiste en 16 bits configurables de Prioridad y la segunda son los 48 bits de la Dirección MAC del Switch, en el proceso de elección de Root Bridge, se observan los Valores de BID de todos los Switches conectados y el menor de ellos será elegido como el Root Bridge.

Teniendo en cuenta esta situación, lo único que tendría que hacer el atacante seria generar trafico BPDU con valores de BID bajos para ganar el rol de Root Bridge.

Es importante subrayar que los cambios en la arquitectura de STP pueden llegar a generar problemas de disponibilidad y acceso a los servicios, además, muchos de estos problemas no son fáciles de identificar y pueden llevar fallas en toda la red.

Para ilustrar el comportamiento de este ataque se usara la topología ilustrada en el grafico 21.

En el grafico 21A se observa que el Switch 1 es el Root Bridge de la red, con un BID 32768.C400.0D34.0000, el otro miembro del STP es el Switch2 con BID 32768.C401.0D34.0000, (Grafico 21B) en este caso los valores de prioridad son iguales, (32768, valor por defecto), pero la MAC del Switch1 es menor que la del Switch 2 lo que hace que en este caso el Switch1 sea elegido como Root Bridge.

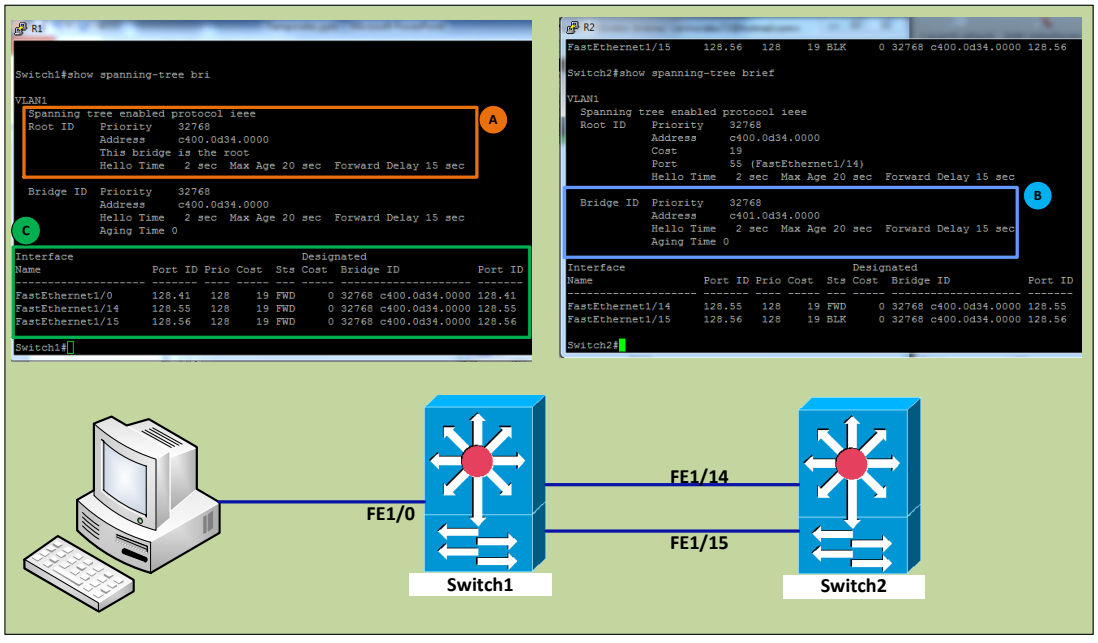

Grafico 21 Spanning Tree Protocol, Funcionamiento Normal.

En el grafico 21C se observan lo puertos que participan en los procesos de STP, entre estos puertos se encuentra el FastEthernet 1/0 que pertenece a un equipo de usuario, este puerto en este caso esta funcionando como puerto de acceso para un PC pero, nada en la configuración del Switch1 le impide en participar en la elección del Root Bridge.

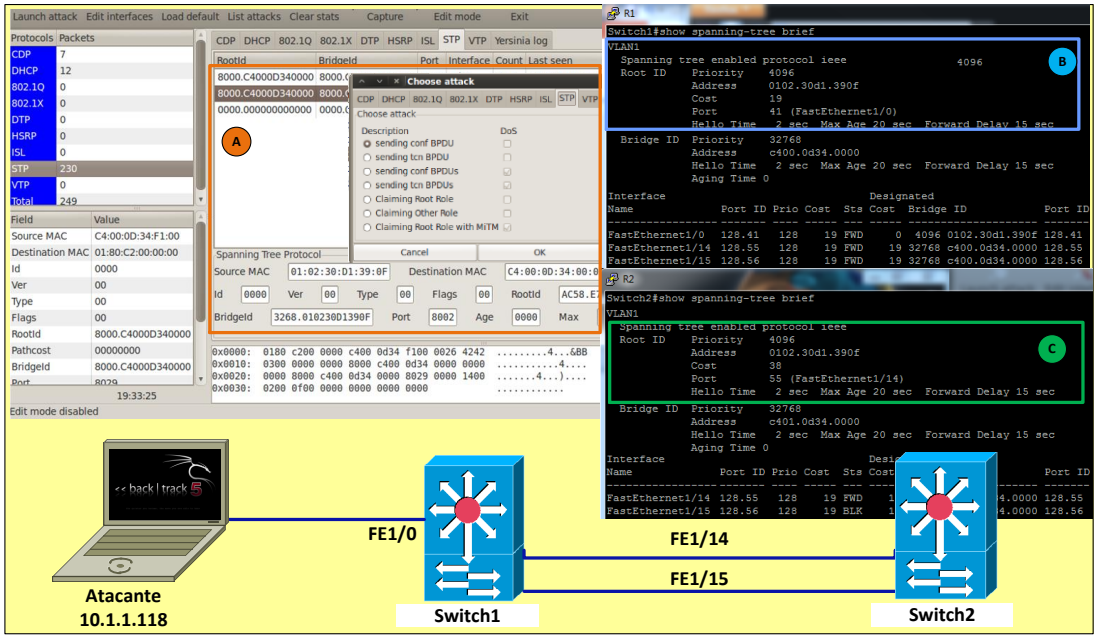

Grafico 22 Ataque de Manipulación STP

Nuevamente se usara la Herramienta Yersinia para Backtrack5, que permitirá diseñar paquetes STP con valores BID necesarios para modificar la arquitectura de STP.

Desde Backtrack 5 conectado ahora a la Interface FastEthernet 1/0 del Switch1 se genera el trafico BPDU Falso con BID 4096.0102.30D1.390F, (grafico 22A). La llegada de trafico BPDU por la interface FastEthernet 1/0 del Switch1, genera un cambio en la Topología STP, ya que un “nuevo equipo” de red ha sido conectado, esto genera una nueva elección de Root Bridge, la BID generada desde Backtrack es menor a la del Switch1, lo que hace el Switch falso sea elegido como Root Bridge de la red (grafico 22B). Dicho cambio será promocionado a todos los miembros del Spanning tree a través de Actualizaciones BPDU, (grafico 22C).

Ahora las decisiones de topología, rutas y actualizaciones en la red STP están controladas por el equipo atacante.

Es importante señalar que mediante el diseño de paquetes con la herramienta yersinia, nos es posible no solo manipular la prioridad de BID, sino también la MAC del equipo falso; en las configuraciones de STP normalmente se elige una prioridad pequeña para asegurar la elección de un Switch como Root Bridge, pero manipulando estos dos parámetros, a voluntad (en los switches no es posible modificar los valores de MAC) aseguraremos siempre que el atacante será elegido como Root Bridge de la red.

Tratamiento.

Luego de ver la facilidad con la que se puede extraer información acerca de los equipos y de la arquitectura de una red de datos, la variedad de los ataques disponibles y la facilidad de su ejecución, podemos tomar el siguiente paso en el aseguramiento de la red.

Continuando con el desarrollo del trabajo, se trabajara con los resultados obtenidos en la etapa de Identificación sobre la red ejemplo, gracias a esta etapa se cuenta con una arquitectura completa de la red, información de Servidores, Clientes, puertos de Conexión, Direcciones MACs. Versiones de Software, servicios activos y protocolos usados, esta información hará que las tareas de la etapa de tratamiento sean mucho más sencillas y efectivas.

Muchas de las medidas básicas de seguridad no son implementadas en las redes de datos, ya sea por desconocimiento de las mismas, por sobredimensionamiento de las tareas necesarias para su implementación o por simple descuido, sin embargo, como se verá a continuación, la aplicación de, estas medidas dificulta e incluso pueden llegar a bloquear totalmente muchos de los ataques y amenazas presentes en las redes de datos, mejorando de esta forma su desempeño y confiabilidad.

Aseguramiento de acceso administrativo.

El acceso administrativo a Switches y a Routers debe ser el primer punto a asegurar. Una de las primeras recomendaciones será la de crear una VLAN independiente en donde residan las direcciones de administración de los equipos de red, el acceso a este segmento de red puede ser restringido por medio de una ACL que permita solo el acceso desde direcciones de originen especificas (Segmento de red de Oficina de sistemas y Soporte técnico), como se observa en la etapa de identificación, el solo hecho que una dirección responda a ping brinda mucha información acerca de una red.

Configuración VTP

Para que las tareas de configuración de VLANs no deban hacerse en todos los equipos de una red se puede utilizar el protocolo VTP, que mediante una estructura de Servidor, Cliente, difunde la información acerca de las VLANs configuradas en una red, en el caso de la red de Ejemplo, se tomará el

Switch Core como Servidor de la estructura VTP y todos los demás equipos serán Clientes.

Configuración Servidor VTP

vtp versión 2
vtp domain *RED_EJEMPLO_VTP*
vtp mode server
vtp password clave_vtp_123
vlan 567 **name** ADMINISTRACION

Configuración Cliente VTP

vtp versión 2
vtp domain *RED_EJEMPLO_VTP*
vtp mode client
vtp password clave_vtp_123

En esta configuración se crea el Dominio VTP *RED_EJEMPLO_VTP* autenticado por la cadena *clave_vtp_123,* toda modificación en la base de datos de VLAN del equipo Servidor será replicada automáticamente a los demás miembros del dominio. Para el caso, la VLAN 567, que será usada para asignar direcciones de administración de los equipos de red.

Aseguramiento Puertos

Dadas las características de las conexiones de los switches a otros equipos, se pueden identificar tres tipos de conexiones a asegurar:

- De Switch a servidor, (Grafico 23C)
- De Switch a Switch (Grafico 23B) y
- De Switch a usuario Final, (Grafico 23A).

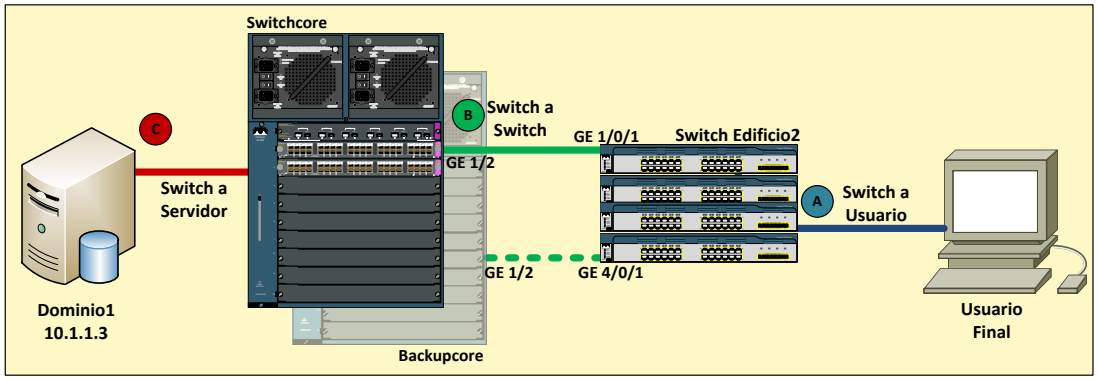

Grafico 20 Tipos de Puertos a asegurar.

Puertos de Usuario Final.

Como primer paso en las tareas de aseguramiento, se trataran los puertos conectados a los usuarios finales. Luego de la etapa de Identificación, es sencillo identificar los puertos destinados a usuarios finales; es para facilitar las tareas de Configuración es recomendable agrupar estos puertos en "Macros", este tipo de agrupaciones disminuyen los tiempos de configuración y facilitan la implementación de políticas de seguridad y de acceso en los equipos.

Macros de Puertos.[17]

Como se observa en el grafico 23B, los puertos conectados a los equipos Core y Switchcore y BackUpCore son los GE 1/0/1 y GE 4/0/1, los demás puertos están o estarán conectados a un equipo de usuario final. Para realizar la agrupación se usa el comando.

SwitchEdf2# **define interface-range** *P_ACCESO* gig1/0/2 –gig1/0/24, gig2/0/1 –gig2/0/24

En este caso, el Macro de nombre P_ACCESO agrupara los puertos desde el GigaEthernet 1/0/2 hasta el 2/0/24, del Switch Edificio2. Para ingresar a este macro y modificar la configuración de todos los puertos a la vez se usara el siguiente comando.

SwitchEdf2#**interface-range** *P_ACCESO.*

Port Security[18]

El primer tipo de ataque que se mostro en este trabajo fue el de MAC Flooding, para detener este tipo de ataques, existe un mecanismo llamado Port Security, mediante este grupo de comandos se puede configurar una dirección MAC fija , también se puede decidir si un puerto puede aprender direcciones nuevas o controlar el numero de direcciones MAC que se pueden aprender en un puerto; en caso de que exista una violación a estas políticas se puede instruir al equipo para que deshabilite el puerto, asilando rápidamente la amenaza..

Para el caso de los puertos de acceso de equipos de usuario final, no se recomienda realizar una configuración fija de dirección MAC en cada puerto, pero es una muy buena práctica la restricción del número de direcciones MAC que se aprenden. Para lograrlo, se usaran los siguientes comandos.

[17] CCNP SWITCH official certification guide, Pearson Education, Inc, David Hucaby, Indianapolis USA 2010 pp 51
[18] CCNP SWITCH official certification guide, Pearson Education, Inc, David Hucaby, Indianapolis USA 2010 pp 373 -376.

interface-range *P_ACCESO.*
switchport mode access
switchport port-security
switchport port-security maximun *10*
switchport port-security violation *shutdown*

La línea 1 accede al rango de puertos configurados como acceso, la línea 2 configura el puerto como puerto de acceso, condición inicial para el funcionamiento del Port Security, la línea 4 establece que el numero máximo de direcciones MAC que se podrán aprender en este puerto será de 10, en caso de que por el puerto se conozcan mas de 10 direcciones el puerto entrara en modo ErrDisable (desconexión por violación de seguridad).

En el evento de un ataque del tipo de MAC Flooding, el puerto se desactivara automáticamente cuando el equipo atacante envié la dirección MAC Numero 11.

En este caso el restablecimiento del puerto a su funcionamiento normal requiere la intervención del administrador de red, pero si esta situación no es la deseada y se requiere que el restablecimiento del puerto ante una violación sea un proceso automático, se puede configurar un temporizador que restablezca el estado normal del puerto.

errdisable detect cause *mac-limit*
errdisable recovery cause *mac-limit*
errdisable recovery interval *300*

Luego de 5 minutos (300 segundos) de la caída del puerto el servicio se restablecerá automáticamente.

BPDU Guard[19]

En el marco del STP, los switches necesitan intercambiar información entre ellos para funcionar correctamente. Los paquetes BPDU son los encargados de cumplir esta tarea. Los BPDU contienen información sobre el Switch desde el cual se transmiten y sus puertos, direcciones MAC, prioridad de puertos y costos. Mediante el intercambio y actualización de esta información el Protocolo Spanning tree, elige al Root Brigde, modifica rutas de acceso a sectores de la red, detecta novedades… entre otras.

Como se observo en el Análisis de amenazas, en la sección de manipulación de Arquitectura STP, los paquetes BPDUs tienen una importancia vital en el

[19] CCNP SWITCH official certification guide, Pearson Education, Inc, David Hucaby, Indianapolis USA 2010 pp 167 - 169.

correcto funcionamiento del STP y como consecuencia en toda la red de datos, lo que hace necesario proteger su funcionamiento.

BPDU guard es una característica de los switches que evita que por determinados puertos se reciba trafico BPDU, como se observo en el ataque VLAN hopping por trunk falso y en la Manipulación de Arquitectura STP, se puede "engañar" a un switch para que negocie un puerto Trunk, o haga participe de los procesos de STP a un equipo que no pertenece a la red.

La característica BPDU Guard bloquea los puertos no autorizados por donde se genere trafico BPDU. Este tipo de tráfico solo se debe generar en los puertos conectados a otros Switches.

interface-range *P_ACCESO.*
switchport portfast
spanning-tree bpduguard *enable*

Primero se accede a los puertos configurados como acceso mediante el macro, luego se configura la característica Portfast (disminución de los tiempos de conectividad) y por ultimo se habilita el BPDU Guard. Este comando es responsable de desactivar un puerto en caso de ver trafico BPDU. De la misma manera que en la violación por número de MACs aprendidas, el puerto puede recuperarse automáticamente después de un tiempo determinado, pero en este caso, no es recomendable habilitar esta opción.

DHCP Snooping[20]

La característica DHCP Snooping aplicada en los puertos de acceso limita el numero de peticiones DHCPREQUEST que pueden generarse desde un puerto conectado a un equipo de usuario final, además de bloquear el puerto si se presenta trafico del tipo DHCPOFFER o DHCPACK.

Un puerto en el cual esta conectado un equipo de trabajo, no debería poder realizar mas de una petición por dirección ip o responder a peticiones de dirección IP, Esta característica permite discriminar entre puertos en los cuales se confiara recibir respuestas de servidores DHCP y los que no. De esta manera se protege a la red de ataques del tipo DHCP Starvation.

La configuración necesaria para los DHCP snooping en los puertos de acceso es la siguiente.

Ip dhcp snooping
Ip dhcp snooping vlan *10*

[20] http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/12ew/configuration /guide/dhcp.pdf Consultada el 20 de Septiembre de 2012

interface-range *P_ACCESO.*
no ip dhcp snooping trust
ip dhcp snooping limit rate *15*

En el primer comando se habilita la función DHCP Snooping para todo el Switch, luego se habilita su uso en la VLAN deseada. Luego mediante el comando de Interface range, entramos a modo de configuración de los puertos de acceso del switch. Mediante el comando *no ip dhcp snooping trust,* hace que el switch no confíe en trafico DHCPOFFER o DHCPACK generado desde estos puertos (Evita el Rogue DHCP server) y finalmente *ip dhcp snooping limit rate 15* limita generación de paquetes DHCPREQUEST a 15 por segundo. (Evita el DHCP starvation).

Agregando las Configuraciones dadas tenemos el siguiente template para los puertos de acceso. (grafico 24)

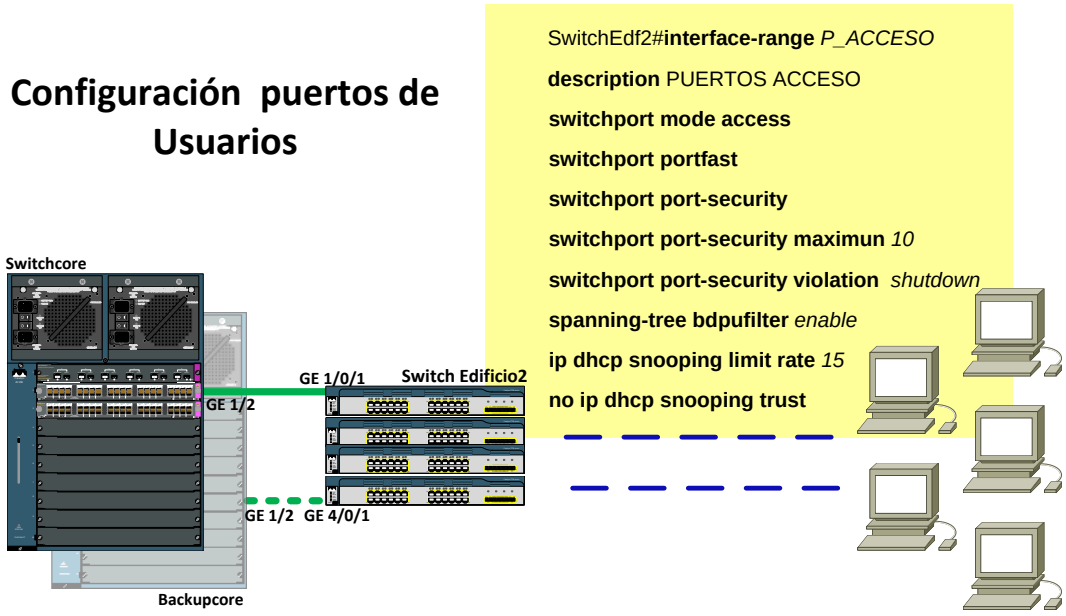

Grafico 24 Configuración Puertos Usuarios

Puertos Switch a Switch.

Los puertos de conexión entre los switches son la columna vertebral de la estructura de una red de datos en Capa 2, pero a pesar de esta situación, en la mayoría de las redes empresariales no son configurados de una manera segura y que garantice estabilidad y óptimo rendimiento. En esta sección del trabajo se propondrán configuraciones que mejoraran la seguridad de estas conexiones.

Configuración de Modo y velocidad estáticos

Es considerado como buena practica la configuración explicita del modo de funcionamiento de un puerto, ya sea tipo trunk o de acceso, durante el desarrollo de este trabajo se han visto los problemas que pueden ocasionar las configuraciones por defecto, uno de los problemas mas comunes que generan estos valores son las fallas producidas por los procesos de auto negociación.

Un puerto en modo AUTO, estará siempre dispuesto a negociar modo de conexión, Velocidad y tipo de conexión (Duplex o half Duplex) ante cualquier cambio de estado, estos procesos de negociación pueden llevar a los puertos a caídas inesperadas, estas caídas pueden conducir a fallas del servicio local por no disponibilidad de conexiones o falla total de la red en capa 2 por inestabilidad de la estructura STP.

Se recomienda siempre fijar mediante comandos, la velocidad y modo de conexión en los puertos configurados como Trunk, esta tarea se puede lograr con los siguientes comandos.

interface GigabitEthernet1/2

description Hacia SW_Edificio2

switchport mode trunk

switchport trunk encapsulation *dot1q*

speed *1000*

dúplex *full*

VLAN Nativa

Como se explico en el ataque de VLAN Hopping por doble tag, la característica de VLAN Nativa permite el transporte de tráfico no tagueado en un puerto trunk. Para evitar este tipo de ataques se recomienda no usar esta VLAN para tráfico de usuarios, o bien modificar su valor por defecto (VLAN1, este cambio se realiza con el siguiente comando.

interface GigabitEthernet1/2

switchport trunk native vlan *543*

A pesar de ser una característica creada la inclusión de dispositivos “legacy” en una red de datos, la VLAN nativa también es usada en protocolos como el de CDP para enviar y recibir paquetes entre equipos Cisco, para evitar problemas, el cambio de VLAN nativa debe realizarse en todos los equipos Switch de la red.

Otra opción es la de obligar a todos los switches de una red a taguear el trafico perteneciente a la VLAN nativa. Para esto se tendrá que introducir en todos los Switches de la red el siguiente comando.

vlan dot1q tag native

Protección STP

Muchos de los ataques mencionados anteriormente aprovechan las características de los switches para hacerlo creer que en uno de sus puertos esta conectado un equipo Falso, hacerlo negociar un puerto trunk o una nueva estructura de STP, este tipo de amenazas crean gran inestabilidad en las redes de datos además de ser difíciles de identificar.

Es muy importante planear, diseñar y proteger correctamente la estructura STP de una red con el fin de evitar problemas de disponibilidad, estabilidad y pérdidas de servicio.

Cuando pensamos en STP se le debe prestar gran atención a los tiempos de convergencia y al ajuste de los mismos a nuestra topología especifica, El comando *Diameter* especifica el diámetro de una red en capa 2, (numero de saltos de switches entre dos estaciones de trabajo cualquiera), retomando la información de la red mostrada en el grafico 5 podemos decir el diámetro de la red es de 3, entonces podemos realizar el siguiente ajuste.

spanning-tree vlan 1 root primary diameter 3

Al especificar el valor del diámetro de la red, el Switch automáticamente ajustara y seleccionara los tiempos de Hello, forward delay, y Maximum age. lo que se traduce en una reducción de los tiempos de convergencia ante cambios en la topología.

Root Guard

La función de equipo Root en una estructura STP es critica ya que define los caminos en capa 2 que tomaran los paquetes para llegar de un segmento de red a otro, por esta razón existen variados tipos de ataques que buscan usurpar este rol, la función Rootguard evita que un equipo conectado a un puerto especifico sea elegido como Root, solo podrán ser elegidos como Root Switch equipos conectados a puertos específicos con las características necesarias de capacidad de trasmisión y procesamiento para asumir estas tareas, esto fortalece el Diseño inicial del STP y evita inestabilidad en el evento de fallas o ataques.

En el caso de la red ejemplo tenemos.

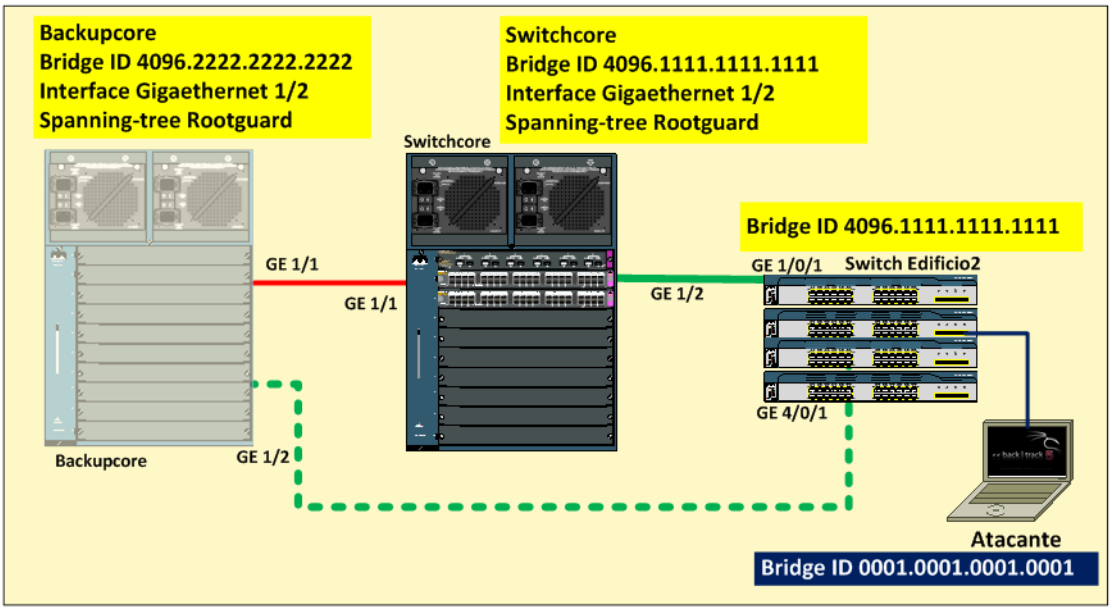

Grafico 25 Rootguard.

El Switchcore es el Root de la estructura STP gracias a su BID de 4096.1111.1111.1111, (Grafico 25) El stack de Switches Edificio2 esta conectado al Switchcore en el puerto GE1/2, y al BackUpCore en el puerto GE1/2, como se observo en los ataques de manipulación de STP, es bastante sencillo manipular paquetes BPDU y lograr ser elegido como Root Bridge. Normalmente el atacante necesitaría únicamente promocionarse con una BID inferior a la del Root actual para generar un nuevo proceso de elección, pero, gracias a que el Switchcore y el Backupcore tienen configurada la función Root guard descartaran todo trafico BPDU que venga por puertos no autorizados, en este caso el puerto GE1/2. En caso de fallas en el STP los Switchcore y BackUpCore recibirán ofertas BPDU para elección de Root únicamente por los puertos autorizados, sin importar que otros equipos (falsos o verdaderos) envíen BID Inferiores.

Vlan Pruning

Por defecto, todos los puertos configurados como Trunk están en la capacidad de transportar cualquier VLAN en la red, por esta razón los puertos trunk son uno de los objetivos preferidos de los atacantes. Una manera sencilla de mejorar el rendimiento y limitar los efectos que puede tener el compromiso de un Switch o de un puerto trunk es el de limitar las VLANs en cada Puerto Trunk.

Esto se puede lograr de dos maneras, mediante la configuración manual de las VLANs autorizadas o mediante el uso de una función del protocolo VTP configurado en el la primera sección de Tratamiento “Aseguramiento de acceso administrativo”.

Manualmente la configuración es la siguiente

interface GigabitEthernet1/2

switchport trunk allowed vlan *10, 20-30*

Esta configuración limitada al puerto GE1/2, solo permitirá el trasporte de las VLANs 10 y del rango de la VLAN 20 a la 30.

Repetir este proceso para cada puerto Trunk en la red y verificar la configuración para cada VLAN configurada puede requerir mucho tiempo y convertirse en una tarea tediosa.

Mediante la configuración inicial del dominio VTP, se puede lograr el mismo resultado de una manera automática mediante la función Pruning del Protocolo VTP.

vtp pruning

Este comando configurado en el Server del dominio VTP, deshabilita la transmisión en los puertos Trunk de VLANS que no sean usadas en los Switches de Acceso a usuarios, de una manera más sencilla, el puerto trunk solo permitirá la transmisión de tráfico de VLANs configuradas en los puertos de los switches de acceso. Esta configuración de restricción de tráfico de VLANs, contrarresta los tipos de ataque que involucran el Doble Tag de paquetes y ataques de negociación de Trunk falso.

Puertos de Servidores.

Los equipos servidores son uno de los puntos mas críticos de una red de datos, y esto hace que los puertos de conexión requieran consideraciones especiales en términos de privilegios de acceso y configuración, en esta sección del trabajo se mostraran algunas configuraciones que buscan mejorar la seguridad en esta parte de la red.

Port Security[21]

Los puertos conectados a equipos servidores son estáticos y normalmente no deberían tener que aprender otras MACs diferentes, la primera medida será la de fijar la dirección MAC de los servidores a puertos específicos, mediante los comandos:

interface gigaethernet 2/1
Description CONTROLADOR DOMINIO
switchport mode access
switchport port-security
switchport port-security maximun *1*

[21] CCNP SWITCH official certification guide, Pearson Education, Inc, David Hucaby, Indianapolis USA 2010 pp 373 -376.

switchport port-security mac-address *0000.1111.2222.3333*
switchport port-security violation *restrict*

Las cuatro primeras líneas acceden al puerto especifico, lo configuran como puerto de acceso y habilitan las funciones Port Security, luego se le instruye al Switch para que la única dirección que aprenda por el puerto sea la de 0000.1111.2222.3333, y luego, en caso de presentarse una violación, el Switch generara mensaje log y SNMP, se generara un contador de Violaciones para el puerto, se descartara el trafico con la MAC desconocida, pero el puerto seguirá operacional.

El ingreso manual de las Direcciones MAC en la configuración de los equipos puede ser una tarea tediosa y complicada. Para evitar el ingreso manual de estas direcciones se puede usar el comando, port-security mac-address sticky, que permite enlazar al puerto en el que se encuentra conectado un equipo la Dirección MAC aprendida dinámicamente por el switch

interface range gigaethernet 2/1 - 10
switchport port-security
switchport port-security mac-address sticky
exit
copy running start

Algunos ataques de Spoofing requieren la caída del puerto de conexión del equipo atacado, esto con el fin de asumir su dirección IP y su dirección MAC. Si se logra la caída un servidor y la MAC ha sido aprendida por un switch de manera dinámica, nada impide que después cierto tiempo un equipo atacante pueda reclamar la IP y la MAC del servidor como propias sin generar ningún tipo de aviso, advertencia o mal funcionamiento, esta configuración evita que el switch olvide el vinculo puerto/MAC/IP para las direcciones de los servidores.

Dhcp Snooping[22]

La configuración DHCP Snooping del lado del servidor DHCP, es la siguiente

interface gigaethernet 2/1
Description CONTROLADOR DOMINIO
ip dhcp snooping trust

Sumada a la configuración ya observada del lado del cliente, DHCP Snooping se convierte en una herramienta muy valiosa en la identificación de posibles ataques, ahora el switch solo permitirá la generación de paquetes DHCPOFFER desde el puerto Giga Ethernet 2/1 y además, ahora

[22] http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_58_se/command/reference/cli2.html#wp2808943 Consultada el 22 de septiembre de 2012

el switch guardara una tabla dinámica de las direcciones IPs asignadas por procesos DHCP, con estadísticas de numero de peticiones y valores de Puerto origen de la petición, MACs:

Switchcore# **show ip dhcp snooping binding**

MacAddress	IP Address	Lease (seconds)	Type	VLAN	Interface
0000.2222.3333	10.1.1.100	1600	dynamic	2	FastEtht2/10
0000.2222.4444	10.1.1.200	1600	dynamic	2	FastEtht2/11

Switch# **show ip dhcp snooping statistics**

Packets Forwarded	= 25
Packets Dropped	= 2
Packets Dropped From untrusted ports	= 2

Las tablas generadoras por la característica DHCP Snooping además de brindar información real del comportamiento de la red, ayudaran en la identificación y bloqueo de ataques como el de DHCP starvation y Rogue DHCP server.

Source Binding

Una vez configurado en su totalidad el DHCP snooping en los puertos de Servidor y Usuarios se puede configurar la característica Source Binding, esta característica esta diseñada para detectar y suprimir ataques del tipo de ARP Poisoning y Spoof de direcciones.

Source binding, permite que el switch pueda verificar la información de un paquete recibido en un puerto en contra de la información guardada en tabla de DHCP Snooping, si la información de MAC e IP no es la misma, el paquete será descartado. En sentido practico, un equipo solo podrá generar trafico con la MAC que realizo el DHCPREQUEST y la Dirección IP que le fue asignada por el servidor DHCP, cualquier otro tipo de trafico ni siquiera será procesado y será descartado automáticamente. Esta característica se habilita de la siguiente manera.

interface-range *P_ACCESO.*
ip verify source port-security

Esta característica es configurada en los puertos de acceso a usuarios finales, pero, ya que necesita la configuración completa de DHCP Snooping y que se relaciona tan profundamente con las funciones del servidor DHCP se ha colocado en la sección de aseguramiento de puertos de servidores.

VLAN privada[23]

Por defecto, el tráfico entre equipos en una misma VLAN es siempre permitido, pero en muchas ocasiones este comportamiento no es muy deseado, pensemos en una VLAN que preste servicios como DMZ, en esta red se encuentran comúnmente servidores FrontEnd de Correo, Servidores Web, Servidores de aplicaciones y Servidor FTP, todos equipos que no necesitan comunicarse entre si para cumplir con sus funciones normales, cada uno de ellos con diferentes vulnerabilidades y múltiples relaciones de confianza con equipos en red Interna, si alguno de ellos fuera comprometido por un atacante, no habría nada que impidiera que desde este equipo comprometido se realizara un ataque a otro equipo de la misma VLAN, buscando explotar sus relaciones de confianza.

Para ilustrar esta situación de una manera mas clara, veremos la DMZ de la Red Ejemplo.

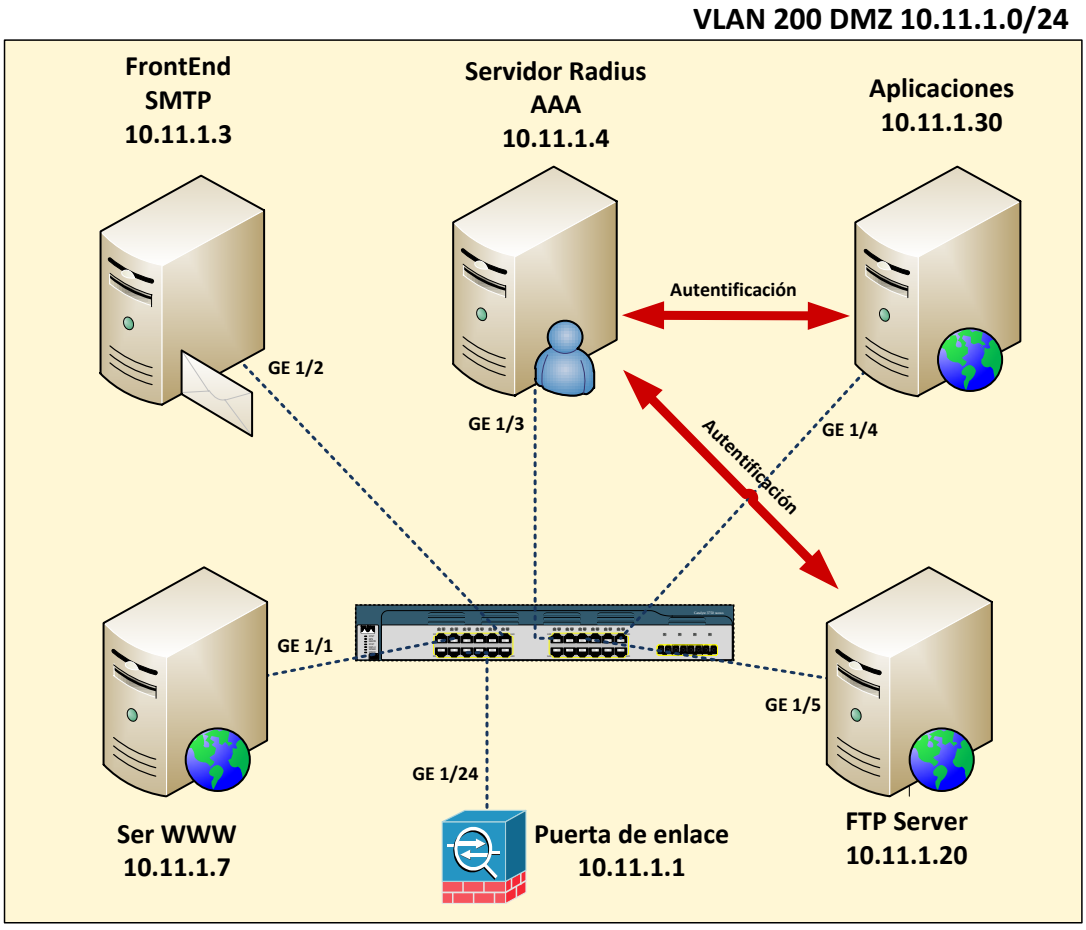

Grafico 26 Relación servidores DMZ.

En el grafico 26 se observa que el servidor de SMTP y el servidor Web, son independientes en su operación y requieren únicamente comunicación con la

[23] http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/pvlans.pdf Consultada el 24 de septiembre de 2012

puerta de enlace, también se tiene que los servidores de Aplicaciones y FTP adicional al acceso a la puerta de enlace requieren conexión con el Servidor RADIUS para realizar tareas de autentificación.

En ambientes de alta riesgo y exposición a amenazas como granjas de servidores y Redes DMZ se hace necesario aislar a los equipos de sus propios "vecinos" de red, esto con el fin de contener cualquier tipo de amenaza y limitar su impacto.

La configuración de VLAN privada permite realizar una asociación lógica de una VLAN "Primaria" con varias VLANs secundarias, equipos asociados con una VLAN secundaria podrán comunicarse con puertos de la VLAN primaria, (puerta de enlace por defecto, routers…) pero no podrá comunicarse con equipos que pertenezcan a otra VLAN secundaria.

En la practica se tendría que, cada equipo servidor estaría asociado a una VLAN secundaria, aislado los demás servidores de la misma VLAN primaria pero capaz de acceder a su puerta de enlace por defecto y a los servidores que compartan su VLAN secundaria

La configuración para la DMZ de la red ejemplo seria la siguiente:

Primero se crean las VLANS secundarias necesarias para el escenario en este caso se necesitaran 3 VLANs secundarias, 1 para el Servidor WWW, 1 para el servidor SMTP y otra para los servidores FTP, AAA y Aplicaciones.

```
vlan  21          ¡              !!!VLAN_WWW
private-vlan      Isolated
vlan  22          ¡              !!!VLAN_SMTP
private-vlan      Isolated
vlan  23          ¡              !!!VLAN_FTP AAA y Aplicaciones
private-vlan      community
```

Segundo, se crea la VLAN primaria y se asocia con las VLANs secundarias.

```
vlan  200         ¡              !!!VLAN Principal
private-vlan      primary
private-vlan  association     21, 22, 23
```

Tercero, se asocian los puertos a las VLANs secundarias en cada caso.

```
interface gigaethernet 1/1        ¡          !!Puerto Servidor WWW
switchport private-vlan host
switchport private-vlan host-association    200   21

interface gigaethernet 1/2        ¡          !!Puerto Servidor SMTP
switchport private-vlan host
switchport private-vlan host-association    200   22

interface range  gigaethernet 1/3 – 5       !!Puertos AAA, FTP y aplicaciones
```

switchport private-vlan *host*
switchport private-vlan host-association 200 23

En el comando *Switchport private vlan host association* el primer numero (200) representa la VLAN principal y el segundo (2x) representa la VLAN secundaria a la cual el puerto estará asociado..

Por ultimo, se configura el puerto de puerta de enlace, aquel al cual todos podrán tener acceso, (puerto promiscuo)

interface gigaethernet 1/24 ¡ **!!***Puerto Servidor WWW*
switchport private-vlan *promiscuous*
switchport private-vlan mapping 200 21,22,23

En el comando *Switchport private vlan mapping* se asocian las VLANs secundarias y la VLAN al puerto promiscuo, de esta manera cualquiera de ellas tendrá acceso irrestricto al mismo.

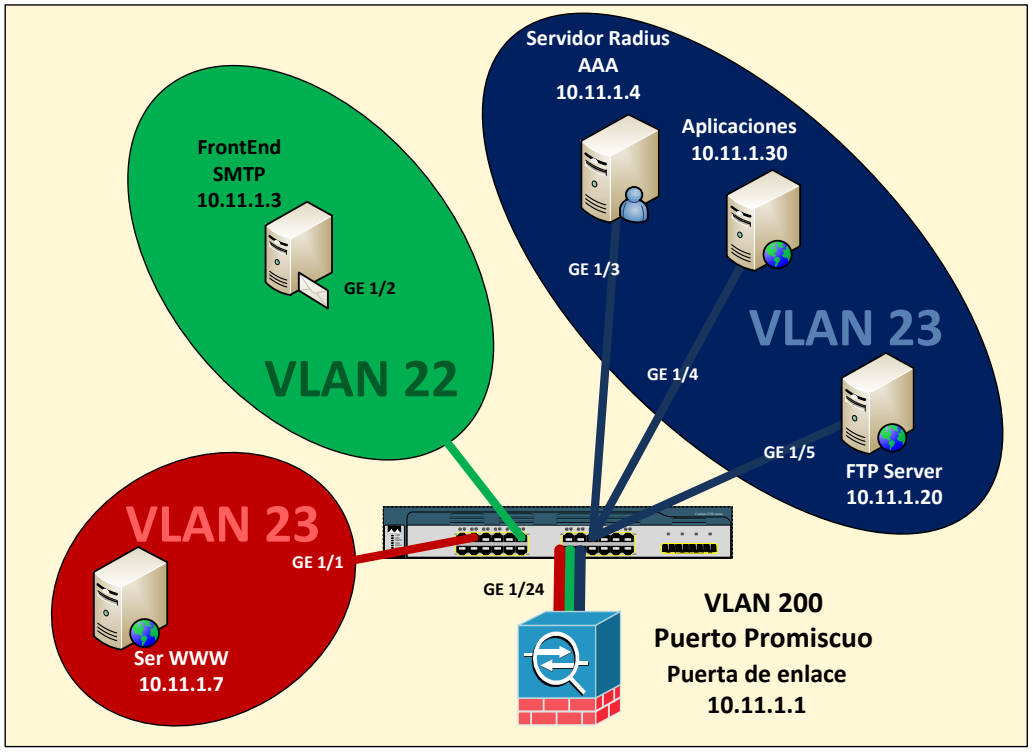

Grafico 27 configuración Private VLAN.

En el grafico 27, se muestra gráficamente el resultado de la configuración de Private VLAN, los equipos de Web y SMTP, se encuentran aislados, cada uno en una VLAN secundaria, y los equipos de AAA, Aplicaciones y FTP comparten otra VLAN secundaria, adicionalmente todos tienen acceso al

puerto GE1/24, configurado como puerto promiscuo, y en el cual se encuentra la puerta de enlace para la red 10.11.1.0/24.

Gracias a las tareas de Identificación, se logro obtener un mapa completo y detallado de los equipos de red y sus funciones en la red de datos, luego en la fase de Análisis de amenazas, se obtuvo un conocimiento mas profundo acerca de las diferentes amenazas que afectan a los equipos de red, de su comportamiento y posible impacto, y finalmente basados en la información recolectada en las dos primeras fases, se propusieron configuraciones especificas para contrarrestar las situaciones de riesgo.

Seguridad Router

Los equipos Routers son el Link de conexión entre dos o más segmentos de red, con distintas necesidades y muy diferentes características de seguridad, por esta razón los Equipos Routers son un punto esencial a asegurar.

ACLs para Acceso Remoto

Una manera sencilla de bloquear el acceso administrativo a los equipos es mediante ACLs en las líneas de acceso virtual, esta configuración solo permitirá acceso VTY HTTP y SNMP a los equipos desde direcciones de administración seleccionadas.

```
access-list 10 permit 10.1.1.129
ip http access-class 10
snmp-server community COMUNIDAD_SNMP rw 10
line vty 0 15
access-class 10 in
```

En este caso, se permitirá acceso administrativo por acceso remoto por los protocolos http, telnet, ssh y snmp únicamente a la dirección 10.1.1.129.

Ahora para asegurar el acceso administrativo se activara el uso de ssh y https, como sabemos, estos protocolos establecen un canal cifrado entre el equipo administrador y el equipo administrado, esto evitara captura de contraseñas por métodos como MAC Flooding, ARP Poisoning o MITM.

Para activar el uso de llaves de cifrado necesarias en los protocolos SSH y HTTPS los equipos deben primero generarlas, para esto usan el nombre del

equipo, dominio, hora y fecha en el proceso, por lo cual se recomienda configurar estos parámetros antes de la generación de las llaves.

```
hostname SWITCH_ED1
ip-domain-name maestria.uba
clock timezone ARG -3
clock set 12:12:12 Dec 21 2012
```

Luego generamos las llaves y limitamos las sesiones SSH a 20 minutos, y el número de intentos de autentificación a 5 en cada sesión (para bloquear Ataques por Fuerza bruta)

```
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 5
```

Ahora que las llaves de cifrado han sido creadas se bloquea el uso de protocolos http y telnet y se habilita el uso de HTTPS y SSH para conexiones de administración.

```
no ip http server
ip http secure server

line vty 0 15
transport input ssh
```

ARP Gratuitos

El ataque de ARP Poisoning se fundamenta en que los miembros de una red de datos aceptaran paquetes ARP gratuito (Generación de paquetes ARP_REPLY sin haberse hecho primero un ARP_REQUEST) una manera sencilla de controlar este tipo de comportamientos es descartar los ARP_REPLY no solicitados al llegar a la puerta de enlace predeterminada, esto se logra con el comando.

```
no ip gratuitous-arps
```

Esta característica debe ser manejada con cuidado ya que protocolos como HSRP utilizan ARP gratuitos para su funcionamiento normal, pero en caso de que las características de la red lo permitan, la función de recibir paquetes ARP gratuitos debe ser desactivada.

Context-Based Access Control[24]

Cuando hablamos de seguridad en un Router , lo primero que viene a la mente son las Listas de acceso o ACLs, pero en el caso de los routers cisco, existe una característica que permite limitar el acceso a recursos de una manera mas adaptable que simplemente la creación de una regla estática.

Context-Based Access Control o CBAC activamente inspecciona la actividad que sale a través de una interface seleccionada (interna) y basado en esta información CBAC decide que trafico se le permitirá la entrada en la interface de salida (externa). Esta característica no solo tiene en cuenta dirección de origen y destino, sino que hace una inspección dinámica de los protocolos usados y autorizados para permitir únicamente el ingreso de trafico respuesta, de manera análoga a como se comporta un Firewall de red.

Para aplicar esta configuración primero se debe definir la relación entre las redes que conecta el Router, en este caso se usara la relación Interna (red segura a proteger) y Externa (red insegura de la que debemos protegernos) (grafico 28)

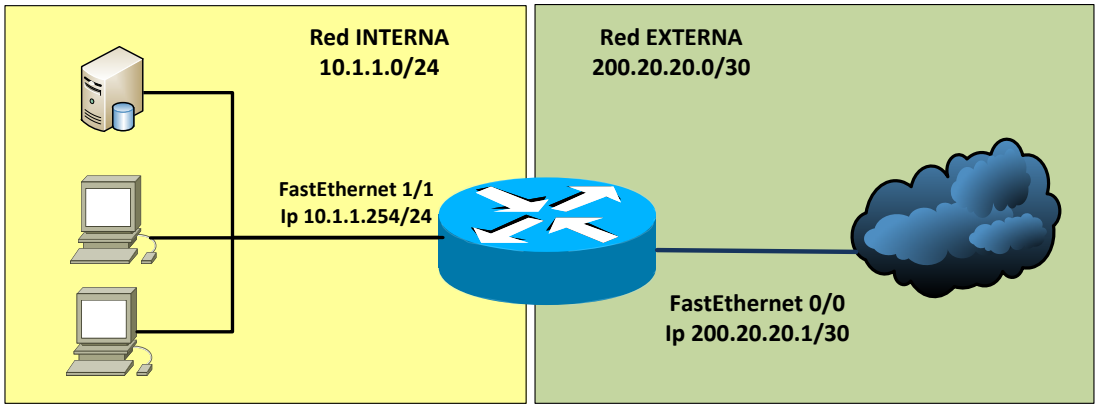

Grafico 28 Router CBAC inicial

Ahora que sabemos cual va a ser la red que se debe proteger, se debe elegir que tipo de tráfico será permitido usar, esto con el fin de configurar las reglas de inspección en el Router. Para el ejemplo se tomara que los usuarios de red interna necesitan los servicios de http, smpt y ftp en un conjunto de reglas de inspección de nombre *INSPEC_INTERNA,* los comandos son

ip inspect name *INSPEC_INTERNA* **ftp**
ip inspect name *INSPEC_INTERNA* **smtp**
ip inspect name *INSPEC_INTERNA* **http**

[24] http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094e8b.shtml consultada el 10 de noviembre de 2012

Luego de esto, se crea aplica una lista de acceso en la interface externa que solo permita el trafico esencial desde internet, para el ejemplo se tomara que se permitirán paquetes ICMP únicamente y se negara todo el resto del trafico.

ip access-list extended *ACL_EXTERNA*

10 permit icmp *any* **host** *200.20.20.1* **echo-reply**
20 permit icmp *any* **host** *200.20.20.1* **unreachable**
30 permit icmp *any* **host** *200.20.20.1* **administratively-prohibited**
40 permit icmp *any* **host** *200.20.20.1* **packet-too-big**
50 permit icmp *any* **host** *200.20.20.1* **echo**
60 permit icmp *any* **host** *200.20.20.1* **time-exceeded**
70 deny *any any*

Interface fastethernet 0/0
Ip access-group *ACL_EXTERNA* **in**

Ahora se debe aplicar la regla de INSPEC_INTERNA a la interface Interna, para que se verifique el trafico que entra a esta interface.

Interface fastethernet *1/1*
ip inspect *INSPEC_INTERNA* **in**

Luego de esto los usuarios de red interna, podrán generar trafico http, ftp y smtp destinado a la red externa, y el trafico respuesta será permitido dinámicamente por el router, mientras que el resto del trafico que llegue a la interface externa será descartado, todo esto mediante una sencilla configuración sin la necesidad de listas de acceso complicadas y extensas (grafico 29).

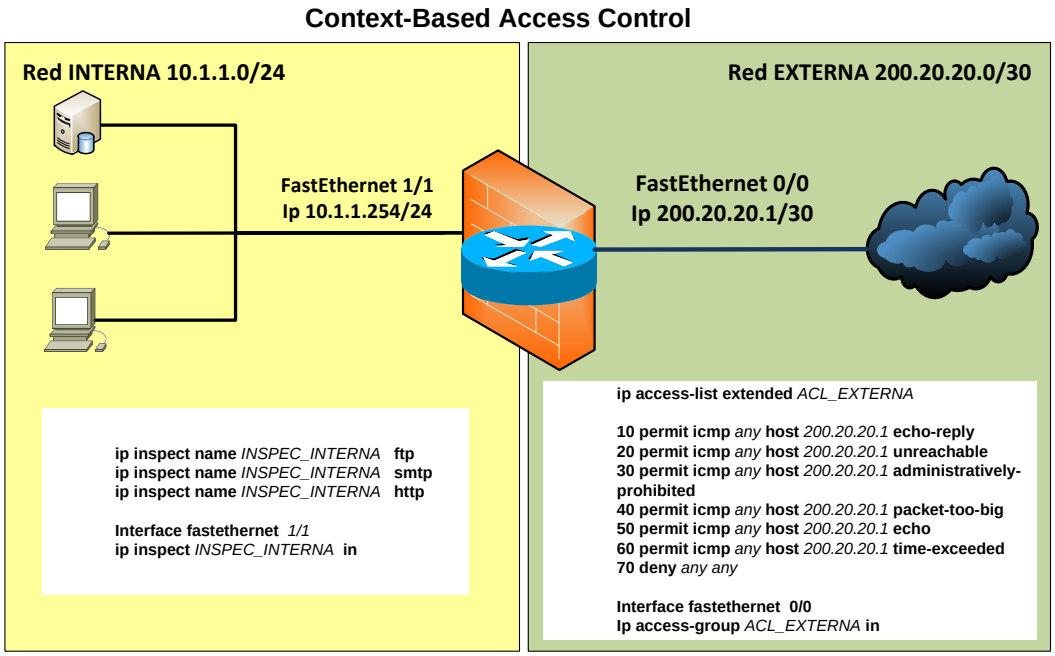

Grafico 29 Router CBAC Completo

Conclusiones

- En mi opinión, el punto más importante en las tareas de aseguramiento es el de la correcta identificación de protocolos, equipos y servicios prestados por una red de datos, este punto es la base sobre las cuales se sustentará todo el proceso de aseguramiento. A pesar de su aparente sencillez estas tareas no deben ser menospreciadas ya que su ejecución y el análisis de la información obtenida requieren un nivel de experticia elevado.

- Las consideraciones de seguridad deben estar presentes desde las primeras etapas de diseño de una red, el conocimiento de las verdaderas necesidades del negocio permitirán una selección adecuada de Equipos, topología de red y características a configurar

- La ejecución periódica de tareas de Identificación y reconocimiento por parte del personal encargado, no solo ayudan a mantener la información de la red actualizada, sino que también fortalecen los conocimientos técnicos y prácticos acerca de equipos, posibles amenazas y herramientas útiles.

- La información actualizada de una red de datos empresarial es esencial en la toma de decisiones en términos de seguridad, diseño y crecimiento, la capacitación y ejecución en tareas de relevamiento de información deben ser parte del calendario de actividades de los equipos de sistemas, no solo para efectos de aseguramiento sino para optimización, mejoramiento y diagnostico problemas.

- Demostraciones de diferentes tipos de ataques de red pueden ayudar a generar conciencia de la importancia del aseguramiento de las redes. En los niveles de gerencia ayudaran a dimensionar impacto y consecuencias de un ataque y en niveles técnicos mostraran los requerimientos tecnológicos y de conocimiento para generar y enfrentar estas amenazas.

- Tareas de Investigación y análisis de ataques de red realizados por el personal encargado, permitirán que en el evento que se presenten ataques, estos sean identificados rápidamente y sean tratados de una manera más efectiva, disminuyendo considerablemente su impacto.

- La documentación adecuada de las medidas de seguridad tomadas en una red de datos, disminuyen los problemas generados por cambios o rotación de personal, dentro de esta documentación debe

hacerse referencia a las amenazas especificas que se desea combatir, con el fin de enfocar los esfuerzos de capacitación y actualización el posible nuevo personal encargado de los equipos de red.

- El Aseguramiento de los equipos de red, mejora enormemente la capacidad de defensa de la red ante una amenaza con una inversión pequeña, en tiempos de capacitación, investigación y configuración.

- Antes de pensar en la adquisición de nuevos equipos y servicios de seguridad, es necesario conocer y evaluar el uso y características de los que ya se encuentran en funcionamiento, en muchas ocasiones la respuesta a un problema de seguridad no requiere la ampliación de la infraestructura, sino de su adaptación y optimización de las partes que ya la componen.

Fuentes

- Cisco Certified Network Administration
  Documentación y Entrenamiento para CCNA

- Cisco Certified Network Administration Security
  Documentación y Entrenamiento para CCNAS

- Cisco Certified Security Professional
  Documentación y Entrenamiento para CCSP

- Ethical Hacking Training
  Documentación de Certificación CEH v5

- Penetration Testing With Backtrack
  Documentación de certificación Offensive Security.

Bibliografía Específica.

[1]http://www.angryip.org/w/About (Consultada el 10 de Junio de 2012)

[2] http://nmap.org/zenmap/ (Consulta el 2 de Junio de 2012)

[3] http://nmap.org/book/preface.html#preface-intro (Consulta el 2 de Junio de 2012)

[4] http://technet.microsoft.com/es-es/library/dd772723%28v=ws.10%29.aspx (consulta 10 de Junio de 2012)

[5] http://support.microsoft.com/kb/832017 (consulta 10 de Junio de 2012)

[6] http://www.cisco.com/en/US/products/ps5931/index.html (consulta 14 de Junio de 2012)

[7] Getting Started with Cisco Network Assistant, Cisco Systems, San Jose USA, 2009.

[8] http://pcsupport.about.com/od/cisco-default-passwords/cisco-default-passwords.htm Consulta el 14 de junio

[9] http://www.cisco.com/en/US/tech/tk648/tk362/tk100/tsd_technology_support_sub-protocol_home.html consulta 27 de Junio de 2012

[10] http://standards.ieee.org/getieee802/download/802.1AB-2005.pdf Consulta 27 de Julio de 2012

[11] Securing Networks with Cisco Routers and Switches Vol 1, Cisco, San Jose CA USA 2007 pp 47-49

[12] CCNA Security Official exam Guide, Michael Watkins, Cisco Press , Indianapolis USA 2008

[13] Securing Networks with Cisco Routers and Switches Vol 1, Cisco, San Jose CA USA 2007 pp 55-57

[14] http://www.ietf.org/rfc/rfc2131.txt Consultada el 9 de noviembre de 2012

[15] Securing Networks with Cisco Routers and Switches Vol 1, Cisco, San Jose CA USA 2007 pp 55-57

[16] http://www.thoughtcrime.org/software/sslstrip/ Consulta el 25 de junio de 2012

[17] CCNP SWITCH official certification guide, Pearson Education, Inc, David Hucaby, Indianapolis USA 2010 pp 51

[18] CCNP SWITCH official certification guide, Pearson Education, Inc, David Hucaby, Indianapolis USA 2010 pp 373 -376.

[19] CCNP SWITCH official certification guide, Pearson Education, Inc, David Hucaby, Indianapolis USA 2010 pp 167 - 169.

[20]http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.1/12ew/configuration /guide/dhcp.pdf Consultada el 20 de Septiembre de 2012

[21] CCNP SWITCH official certification guide, Pearson Education, Inc, David Hucaby, Indianapolis USA 2010 pp 373 -376.

[22]http://www.cisco.com/en/US/docs/switches/lan/catalyst2960/software/release/12.2_58_se/command/reference/cli2.html#wp2808943 Consultada el 22 de septiembre de 2012

[23]http://www.cisco.com/en/US/docs/switches/lan/catalyst4500/12.2/31sg/configuration/guide/pvlans.pdf Consultada el 24 de septiembre de 2012

[24]http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a0080094e8b.shtml consultada el 10 de noviembre de 2012

Bibliografía General

- CCNA Security, Official Exam Certification Guide, Cisco Press, Michael Watkins, Kevin Wallace, Indianapolis USA 2008.

- CCNP TSHOOT Official certification Guide, Cisco Press, , Kevin Wallace, Indianapolis USA 2010.

- Securing Networks with Cisco Routers and Switches Vol 1, 2 y 3, Cisco Press 2007.

- Network Security Auditing, Chris Jackson, Cisco Press Indianapolis USA 2010.

- The Basics of Hacking and Penetration Testing, Patrick Engebretson, James Broad. Syngress Waltham MA USA 2011.

- Hacking exposed, Network Security, secrets and solutions. Second edition, Joel Scambray, Stuart McClure McGraw-Hill, 2001