

Experto Universitario en Ethical Hacking

Módulo 1:

Diseño de redes seguras

Unidad 3:

Redes informáticas – Potenciales Riesgos



Presentación

En esta tercer Unidad del curso, nos introducimos en la comprensión de la temática correspondiente a lo que hay que tener en cuenta con respecto a los potenciales ataques.

Comprender los servicios que se utilizan y a la vez, como esos mismos servicios son vulnerables.

También se verán varios laboratorios, que dejarán en claro, la importancia tanto de comprender cómo de utilizar los servicios de Red.



Objetivos

Que los participantes logren...

- Conocer los conceptos generales de las redes de comunicación, los protocolos, los diferentes dispositivos y sus funciones.
- Aprender a planear, diseñar, estructurar e implementar una infraestructura de red informática de manera segura, protegiéndola de potenciales amenazas.



Bloques temáticos

1. Amenazas y ataques.
2. Servicios de Red.
3. Potenciales Ataques (LAB).

Amenazas y Ataques



Las amenazas a la seguridad de la información atentan contra su confidencialidad, integridad y disponibilidad.

Existen amenazas relacionadas con fallas humanas, con ataques malintencionados o con catástrofes naturales.

Mediante la materialización de una amenaza podría ocurrir el acceso, modificación o eliminación de información no autorizada; la interrupción de un servicio o el procesamiento de un sistema; daños físicos o robo del equipamiento y medios de almacenamiento de información.

Los protocolos de comunicación utilizados carecen de elementos relacionados con la seguridad o han sido implementados tiempo después de su creación.

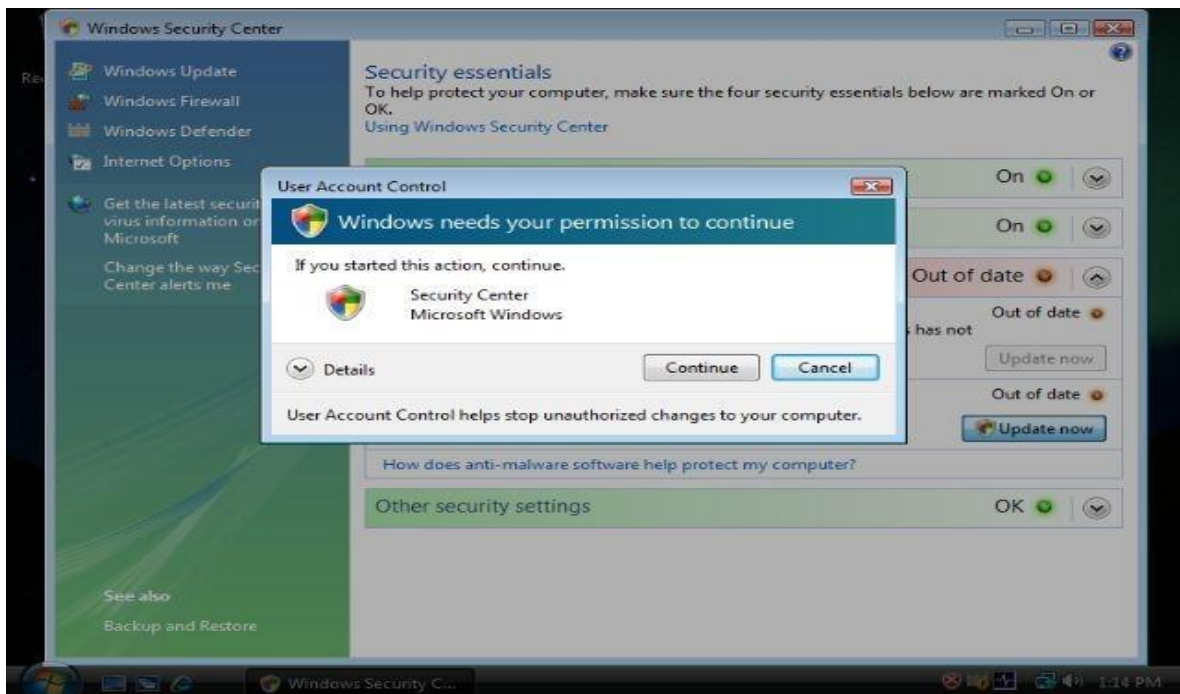
Nos encontraremos con:

- **Agujeros de seguridad en sistemas operativos**
- **Agujeros de seguridad en aplicaciones**
- **Errores en las configuraciones de los sistemas**

- Usuarios que carecen de información

Expliquemos los más relevantes:

Agujeros de seguridad (vulnerabilidades) en sistemas operativos



CONSECUENCIA: no se necesitó demasiado tiempo para que apareciera un *script* de Visual Basic haciéndonos pasar por el usuario que desactiva el UAC, agregara un ejecutable en la sección de Inicio de Windows, y reiniciará el sistema.

Sitios como **Exploit-DB** o **Security Focus**, informan los distintos agujeros (vulnerabilidades) que pueden tener los sistemas operativos.

Para la forma de mitigación, se necesita siempre estar al tanto de las actualizaciones y parchear los sistemas operativos, de esa forma uno no estaría expuesto, al menos con la vulnerabilidad declarada.

Una recomendación para comprender la importancia, es instalar un sistema operativo en una máquina virtual y llevar a cabo estadísticas de cada vez que se necesite actualizar, de esa manera entenderemos que no es una vez por mes, sino mucho más de lo que uno imagina.

Agujeros de seguridad (vulnerabilidades) en aplicaciones

Primero observemos estas Estadísticas de los Sistemas y aplicaciones más vulnerables

Top 50 Products By Total Number Of "Distinct" Vulnerabilities in 2019

Go to year: [1999](#) [2000](#) [2001](#) [2002](#) [2003](#) [2004](#) [2005](#) [2006](#) [2007](#) [2008](#) [2009](#) [2010](#) [2011](#) [2012](#) [2013](#)

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Android	Google	OS	414
2	Debian Linux	Debian	OS	360
3	Windows Server 2016	Microsoft	OS	357
4	Windows 10	Microsoft	OS	357
5	Windows Server 2019	Microsoft	OS	351
6	Acrobat Dc	Adobe	Application	342
7	Acrobat Reader Dc	Adobe	Application	342
8	Cpanel	Cpanel	Application	321
9	Windows 7	Microsoft	OS	250
10	Windows Server 2008	Microsoft	OS	248
11	Windows Server 2012	Microsoft	OS	246
12	Windows 8.1	Microsoft	OS	242
13	Windows Rt 8.1	Microsoft	OS	235
14	Ubuntu Linux	Canonical	OS	190
15	Fedora	Fedoraproject	OS	184
16	Chrome	Google	Application	177
17	Linux Kernel	Linux	OS	170
18	Iphone Os	Apple	OS	156
19	Leap	Opensuse	OS	146
20	Sd 625 Firmware	Qualcomm	OS	145

Fuente: <https://www.cvedetails.com/top-50-products.php?year=2019>

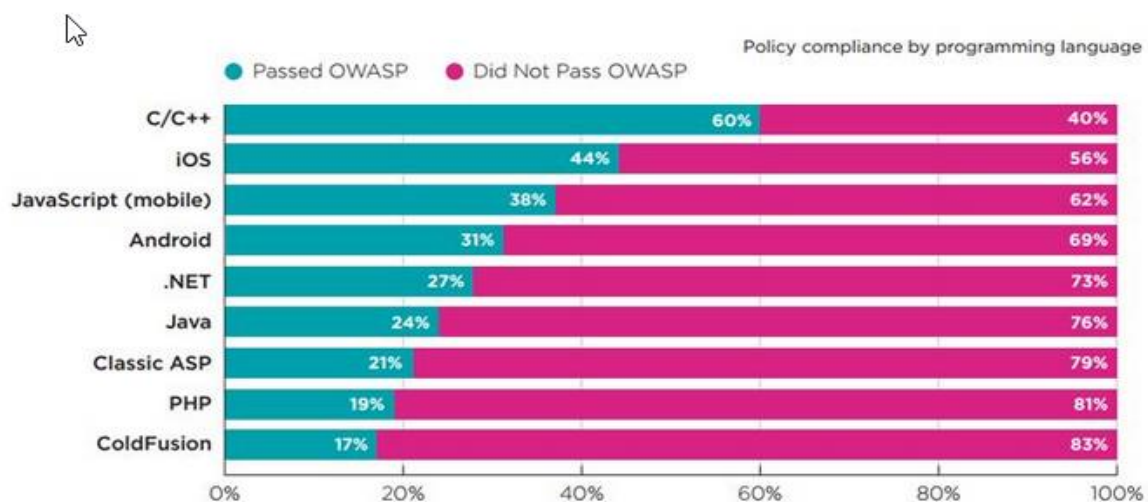
En estos casos, mantenerse informado sobre cómo las aplicaciones más conocidas es un punto positivo, para estar enterado de cuándo actualizar.

Se recomienda realizar un relevamiento completo de las aplicaciones que uno tiene, y a partir de ahí, chequear y analizar si existe la posibilidad de actualizarlas.



Estadísticas de los lenguajes de programación más vulnerables

Estos son los errores más buscados por los atacantes, ya que son errores propios de programación y la vulnerabilidad encontrada puede llegar a ser tomar control completo de un sistema o aplicación.

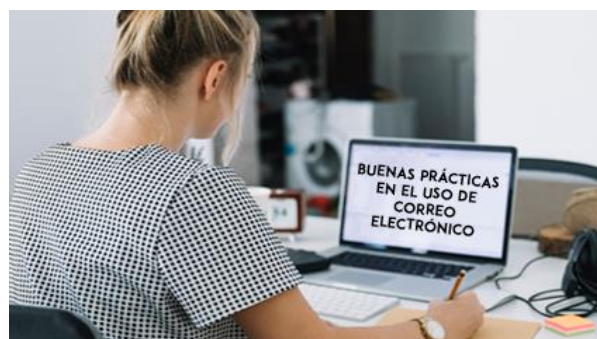


Usuarios sin conocimientos suficientes (concientización necesaria)

La medida de concientización, es la más importante de todas, lo mismo que aplicar procesos que eviten la fuga de información.



Así como evitar que se realicen prácticas indebidas, por ejemplo, el uso de USB no permitido, o abrir mails desconocidos o clickear a todo lo que salga, sin antes revisar o analizar.



Lo que uno se debe preguntar, de qué sirve aplicar políticas de seguridad si los usuarios no cumplen con los requisitos de conocimientos necesarios.

Una manera sencilla, en la concientización es enseñar al menos, 3 parámetros claves:

- 1- analizar si los mails tienen un destinatario directo, si no se distingue, estamos ante una campaña de envío masivo.
- 2- la historia central, generalmente es un mensaje alarmante o que llama la atención, donde requiere la intervención de la víctima.
- 3- lo que pide, generalmente propósito económico, contacto bancario, todo lo que pueda ir directo a una estafa, es síntoma.

Debido a su complejidad, se recolectan datos que le dan al atacante las pautas para tener éxito, las más habituales son:

- **Identificación del sistema operativo:**

Los ataques difieren mucho según el sistema operativo que esté instalado en el ordenador

- **Escaneo de protocolos, puertos y servicios:**

Los servicios: Son los programas que carga el propio sistema operativo para poder funcionar, servicio de impresión, actualizaciones automáticas, servicios de chat...

Los puertos son las vías que utiliza el ordenador para comunicarse, 21 es el del FTP, 995 el del correo seguro...

Protocolos: Son los diferentes lenguajes establecidos que utiliza el ordenador para comunicarse

De este modo si se escanea todo este entorno el atacante se hace una idea de cómo poder realizar el ataque.

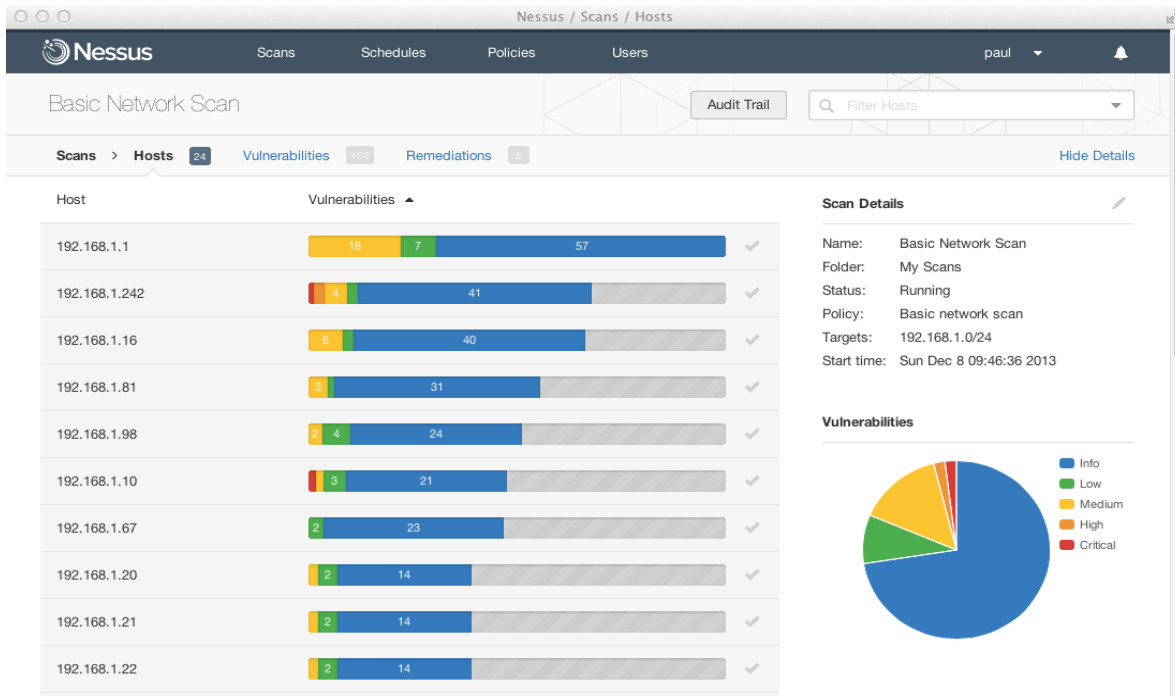
Escaneo de vulnerabilidades.

Del sistema operativo

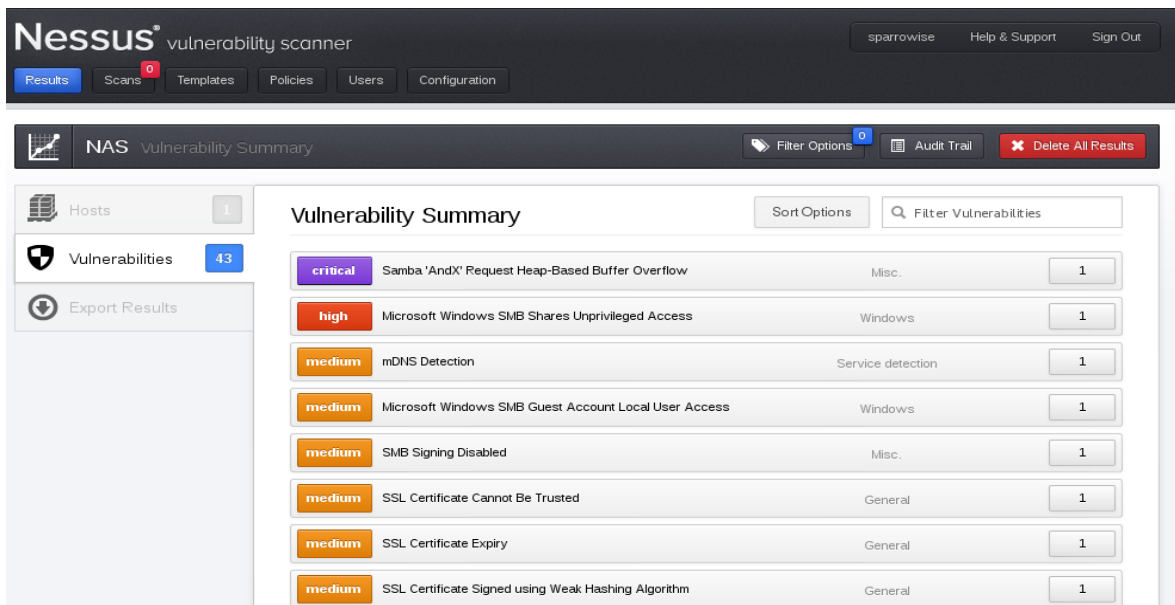
De los programas instalados

Estos 3 parámetros, son los que realizará un atacante para poder detectar cualquier posibilidad de intrusión, si observamos y comprendimos todo lo leído hasta ahora, se sabrá que la solución es mantener una línea de políticas y procesos adecuados para asegurar todos los entornos.

Un buen scanner de vulnerabilidades para empezar: “NESSUS”



Ejemplo de captura de resultados





Try Nessus Professional Free for 7 Days

Nessus® is the most comprehensive vulnerability scanner on the market today. Nessus Professional will help automate the vulnerability scanning process, save time in your compliance cycles, and allow you to engage your IT team.

	Nessus Evaluation	Nessus
Designed For	Commercial organizations wanting to evaluate Nessus Professional	Single Users, Commercial Use
Real-time Vulnerability Updates	✓	✓

Register

Please register to evaluate Nessus. An activation code will be emailed to the address you provide.

First Name*

Last Name*

Fuente oficial para descargarlo: www.tenable.com

The screenshot shows the OpenVAS website with a navigation bar containing 'OpenVAS', 'About OpenVAS', 'Try out OpenVAS', and 'Support'. A large green button with a white arrow and the text 'Download OpenVAS' is prominent. To the right, a diagram illustrates the OpenVAS architecture, including components like OpenVAS GUI, OpenVAS Security Analytics, OpenVAS Security Alerts, OpenVAS Scanner, OpenVAS Manager, OpenVAS Administration, and OpenVAS Results. A cartoon character is shown pointing towards the architecture diagram.

The world's most advanced Open Source
vulnerability scanner and manager

Otro scanner recomendado - Fuente oficial para descargarlo:

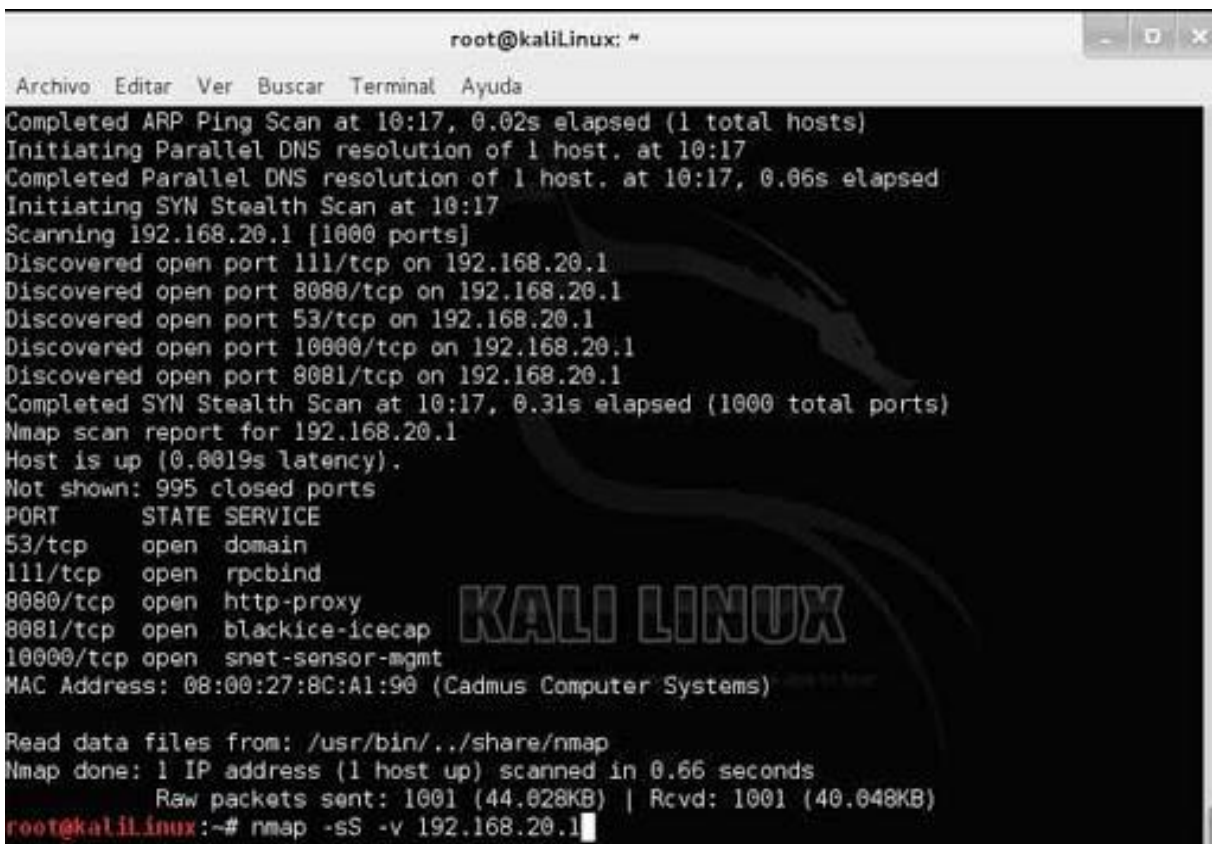
www.openvas.org

Que podemos encontrarnos:

- **Identificación vulnerabilidades en Versiones de Aplicación y Sistemas Operativos**
- **Gestión de Parches (Patch Management)**
- **Identificar Vulnerabilidades Tecnológicas y Humanas**
- **Configuraciones por Defecto (Password Default)**
- **Vulnerabilidades Técnicas y Funcionales**

(En otro módulo se verán en detalle estos temas)

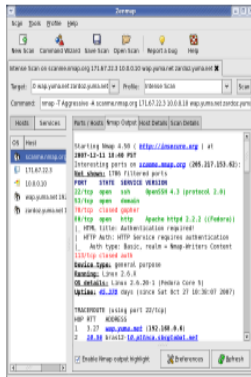
Ejemplo de un escaneo de un sistema operativo con el programa NMAP



```
root@kaliLinux: #
Archivo Editar Ver Buscar Terminal Ayuda
Completed ARP Ping Scan at 10:17, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:17
Completed Parallel DNS resolution of 1 host. at 10:17, 0.06s elapsed
Initiating SYN Stealth Scan at 10:17
Scanning 192.168.20.1 [1000 ports]
Discovered open port 111/tcp on 192.168.20.1
Discovered open port 8080/tcp on 192.168.20.1
Discovered open port 53/tcp on 192.168.20.1
Discovered open port 10000/tcp on 192.168.20.1
Discovered open port 8081/tcp on 192.168.20.1
Completed SYN Stealth Scan at 10:17, 0.31s elapsed (1000 total ports)
Nmap scan report for 192.168.20.1
Host is up (0.0019s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
111/tcp   open  rpcbind
8080/tcp  open  http-proxy
8081/tcp  open  blackice-icecap
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:8C:A1:90 (Cadmus Computer Systems)

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.048KB)
root@kaliLinux:~# nmap -sS -v 192.168.20.1
```

Microsoft Windows binaries



Please read the [Windows section](#) of the Install Guide for limitations and installation instructions for the Windows version of the Zenmap GUI or the much smaller command-line zip file version. We support Nmap on Windows 7 and newer, as well as **must run Nmap on earlier Windows releases.**

Note: The version of Npcap included in our installers may not always be the latest version. If you experience problems or just release.

The Nmap executable Windows installer can handle Npcap installation, registry performance tweaks, and decompressing the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

Latest **stable** release self-installer: [nmap-7.91-setup.exe](#)

Latest Npcap release self-installer: [npcap-1.10.exe](#)

We have written [post-install usage instructions](#). Please [notify us](#) if you encounter any problems or have suggestions for the in

For those who prefer the command-line zip files ([Installation Instructions](#); [Usage Instructions](#)), they are still available. The Zenmap graphical interface is *not* in window. Or you can download and install a superior command shell such as those included with the free [Cygwin system](#). Also, you need to run the [Npcap](#) and included in the zip file. The main advantage is that these zip files are a fraction of the size of the executable installer:

Latest **stable** command-line zipfile: [nmap-7.91-win32.zip](#)

Scanner de puertos y servicios recomendado - Fuente oficial para descargarlo: [**www.nmap.org**](http://www.nmap.org)

A través de estos Scanners, es posible detectar vulnerabilidades, fallas en sistemas y aplicaciones, malas configuraciones y posibilidad de detectar intrusiones.

En conclusión existen multitud de tipos de técnicas de ataques de red aunque existen cuatro tipos básicos:

- **Ataques de denegación de servicio**
- **Ataques contra la autenticación**
- **Ataques de modificación y daño a la integridad**
- **Ataques aprovechando deficiencias de seguridad**

Ejercicio Número 1 Unidad 3



Buscar en Internet alguna noticia de un incidente (ataque) informático (no importa el tipo de técnica de ataque) y hacer un análisis personal de cómo PIENSAN que sucedió y cómo habría que evitarlo de acuerdo a sus puntos de vista o conocimientos (postear en el foro).

El mismo queda para que TODOS lean los trabajos de sus compañeros.

TIPS: sitios recomendados para encontrar noticias

<http://hackmageddon.com>

<https://www.zdnet.com/blog/security/>

<https://www.redpacketsecurity.com/>

Por favor, en caso de que los links no funcionen, avisar al instructor, ya que es muy común que se cambien, den de baja o se actualice la misma URL.

HACKMAGEDDON
Information Security Timelines and Statistics

ABOUT SUBMIT AN ATTACK CYBER ATTACKS TIMELINE CYBER ATTACKS STATISTICS

Latest Posts

Cloud Cyber Attacks Timeline Security

Cloud-Native Threats in 2020
December 30, 2020 Paolo Passeri 0

Among the various things that I have done in 2020, there is the collection of the main cyber attacks that have exploited cloud services in the kill chain. I have built a personal (and obviously incomplete) list using publicly available information. The complete timeline is available at the end of the post, while some statistics are summarized in the following charts...

1-15 December 2020 Cyber Attacks Timeline
December 28, 2020 0

November 2020 Cyber Attacks Statistics
December 23, 2020 0

16-30 November 2020 Cyber Attacks Timeline
December 22, 2020 0

1-15 November 2020 Cyber Attacks Timeline
December 9, 2020 0

October 2020 Cyber Attacks Statistics
December 3, 2020 0

Servicios de Red

Dentro de una red, podremos encontrar o agregar servicios relacionados con la seguridad, la protección de datos y la configuración de la red.

Estos servicios nos permiten realizar diferentes tareas.

NAT – PAT – ARP – DNS – DHCP

A continuación analizaremos de forma resumida los mismos, ya que son imprescindibles para lograr establecer una conexión entre equipos.

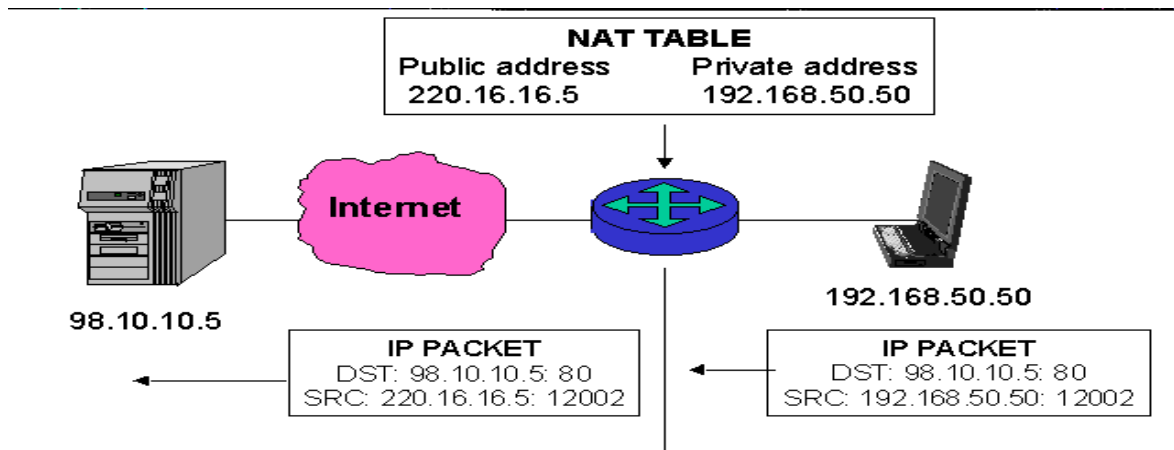
NAT (Network Address Translation)

Es un mecanismo utilizado por routers **IP** para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

El tipo más simple de **NAT** proporciona una traducción una-a-una de las direcciones **IP**.

La mayoría de los **NAT** asignan varias máquinas (hosts) privadas a una dirección **IP** expuesta públicamente.

En conclusión, cada equipo conectado a cada red, se identifica hacia otras redes, con una única **IP PÚBLICA**, teniendo nuestra identificación pública de nuestro **NAT**.



En este ejemplo, vemos que la **IP** 192.168.50.50 (Privada) se identificara en Internet con la **IP** 220.16.16.5 (Publica).

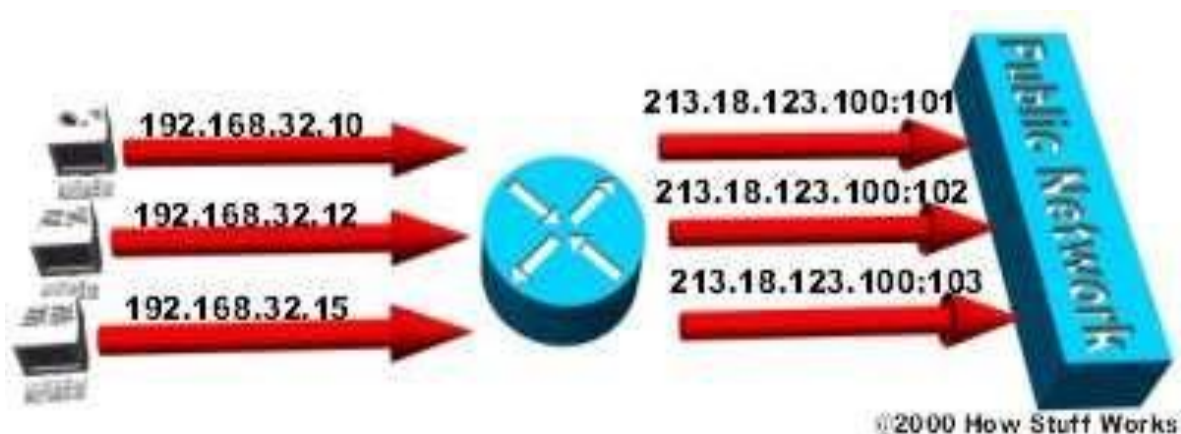
También notamos que quiere llegar a un objetivo **IP** 98.10.10.5 (Privada), el cual recibirá la notificación de la **IP PUBLICA NAT** (220.16.16.5) correspondiente a la **IP Origen PRIVADA**.

PAT (Port Address Translation)

Es una variante del **NAT**, aquí incorpora asignación dinámica de puertos en cada comunicación entre la red privada y la red pública.

Trabaja en capa 4 (TRANSPORTE) del modelo **OSI**, el **NAT** trabaja en capa 3 (**RED**), ya que solo gestiona direccionamiento **IP**.

Aquí vemos como traduce 3 direcciones **IP** privadas a 1 única **IP** pública, asignando a cada privada un puerto específico.



Otro ejemplo de PAT

Tenemos 3 computadoras y cada una tiene un servicio diferente:

Equipo A: 10.10.10.1 FTP o sea usa el puerto 21

Equipo B: 10.10.10.2 HTTP o sea usa el puerto 80

Equipo C: 10.10.10.3 TELNET o sea usa el puerto 23

Y como nuestro router tiene una sola **IP** Pública (200.10.90.17), lo que hará el mismo es asignarle un puerto a cada servicio e **IP**.



10.10.10.1:21 ----- 200.10.90.17:5001

10.10.10.2:80 ----- 200.10.90.17:5002

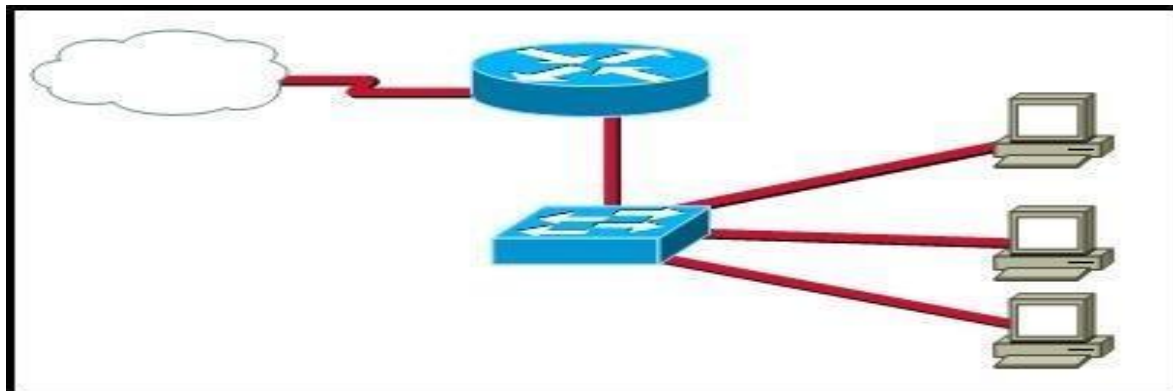
10.10.10.3:23 ----- 200.10.90.17:5003

De esta manera presentará a los equipos al exterior.

Ejercicio Número 2 Unidad 3



Completar con direccionamiento y puertos, utilizando el protocolo PAT (subirlo al foro, no mandar por mail)

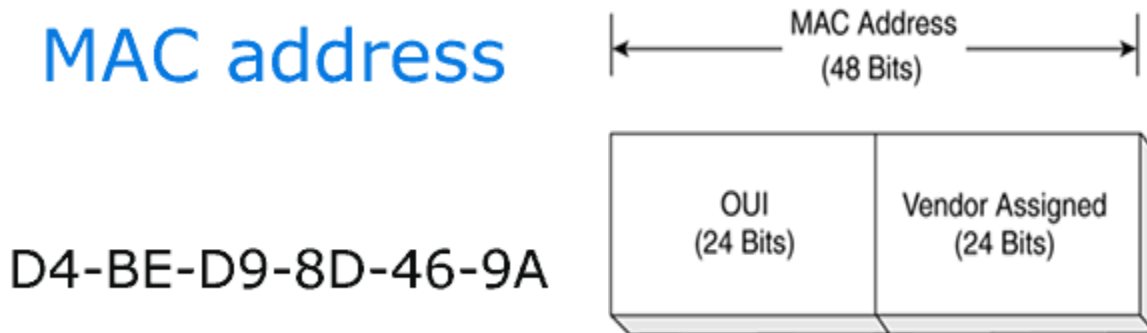


Se solicita: IPs origen, IPs destino, puerto origen, puerto destino, de cada una de las PCs.

Por otro lado, a nivel WAN, se pide una IP pública y el puerto identificador para cada servicio.

ARP (Address Resolution Protocol)

Antes sepamos que es una **Mac Address**: es un identificador único de 48 bits para identificar la totalidad de dispositivos de red como por ejemplo tarjetas de red Ethernet, tarjetas de red Wireless o inalámbricas, Switch de red, Routers, impresoras, etc.



Las direcciones MAC son identificadores únicos a nivel mundial para cada dispositivo y por lo tanto es imposible encontrar 2 tarjetas de red o 2 dispositivos de red que tengan la misma Mac Address.

La totalidad de fabricantes en el momento de fabricar el hardware, como por ejemplo una tarjeta de red Wireless, graban la Mac Address en formato binario en una memoria ROM del dispositivo que están fabricando.

Como la memoria ROM es solo de lectura es totalmente imposible modificarla y por lo tanto esto implica que la Mac address o identificador de un dispositivo nunca se podría modificar.

Más adelante veremos que es posible hacer creer a otras personas o a integrantes de la red que nuestra MAC Address es otra diferente a la real (posibilidad de cambiar la MAC).

El motivo por el cual es posible modificar la MAC de la tarjeta de red de nuestra PC es simple.

Cuando se arranca nuestro ordenador la tarjeta de red copia la dirección MAC a nuestra memoria RAM.

Una vez copiada la Mac Address a la memoria RAM la totalidad de veces que se requiere de la Mac Address se usará la Mac Address almacenada en la memoria RAM.

Por lo tanto si queremos cambiar nuestra Mac Address tan solo tenemos que modificar la Mac Address almacenada en nuestra memoria RAM .

Es un protocolo de la capa de enlace de datos responsable de encontrar la dirección hardware (MAC) que corresponde a una determinada dirección IP de un dispositivo de red.

En Ethernet, la capa de enlace trabaja con direcciones físicas.

El protocolo ARP se encarga de traducir las direcciones IP a direcciones MAC (direcciones físicas). Para realizar esta conversión, el nivel de enlace utiliza las tablas ARP, cada interfaz tiene tanto una dirección IP como una dirección física MAC.

```
C:\Users\Laboratorio-01>arp -a

Interfaz: 192.168.56.1 --- 0x15
Dirección de Internet      Dirección física      Tipo
192.168.56.255             ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático

Interfaz: 10.166.26.1 --- 0x18
Dirección de Internet      Dirección física      Tipo
10.204.128.9               02-00-0a-cc-80-09    dinámico
10.204.160.10              02-00-0a-cc-a0-0a    dinámico
10.244.10.16               02-00-0a-f4-0a-10    dinámico
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático

Interfaz: 192.168.1.33 --- 0x1d
Dirección de Internet      Dirección física      Tipo
192.168.1.1                c8-b4-22-71-12-50    dinámico
192.168.1.255              ff-ff-ff-ff-ff-ff    estático
224.0.0.22                 01-00-5e-00-00-16    estático
224.0.0.251                01-00-5e-00-00-fb    estático
224.0.0.252                01-00-5e-00-00-fc    estático
239.255.255.250            01-00-5e-7f-ff-fa    estático
255.255.255.255            ff-ff-ff-ff-ff-ff    estático
```

Aquí vemos las MAC aprendidas por una PC, usando el comando ARP -A

DNS (Domain Name Service)

Cada equipo conectado directamente a Internet tiene al menos una **dirección IP** específica. Sin embargo, los usuarios no desean trabajar con direcciones numéricas, como por ejemplo 194.153.205.26, sino con un nombre de dominio o más específicamente, con direcciones (llamadas direcciones **FQDN**) como por ejemplo es.kioskea.net.

Es posible asociar nombres en lenguaje normal con direcciones numéricas gracias al sistema llamado **DNS** (Sistema de Nombres de Dominio).

Esta correlación entre las direcciones **IP** y el nombre de dominio asociado se llama resolución de nombres de dominio (o resolución de direcciones).

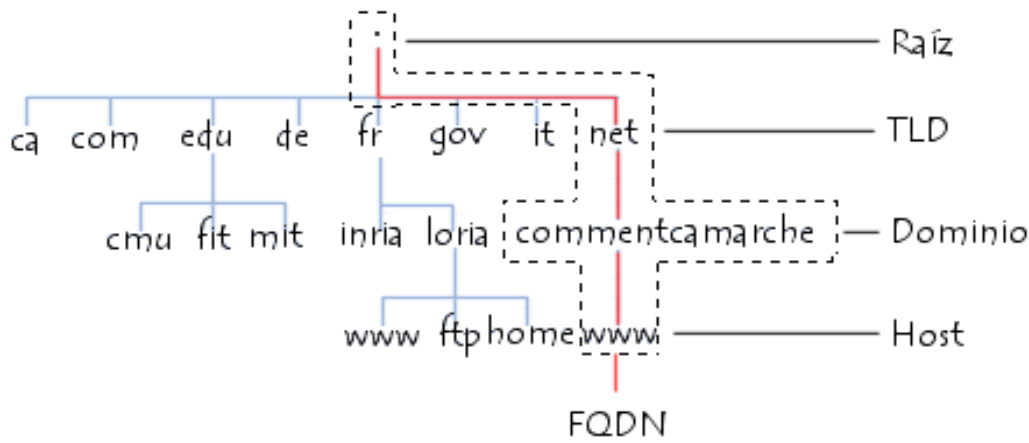
Introducción al Sistema de Nombres de Dominio:

Este sistema ofrece:

- Un espacio de nombre jerárquico que permite garantizar la singularidad de un nombre en una estructura arbórea.
- Un sistema de servidores de distribución que permite que el espacio de nombre esté disponible.
- Un sistema de cliente que permite "resolver" nombres de dominio, es decir, interrogar a los servidores para encontrar la dirección **IP** que corresponde a un nombre.

Espacio de nombre:

La estructura del sistema **DNS** se basa en una estructura de arbórea en donde se definen los dominios de nivel superior (llamados **TLD**, Dominios de Nivel Superior); esta estructura está conectada a un nodo raíz representado por un punto.



Cada nodo del árbol se llama nombre de dominio y tiene una etiqueta con una longitud máxima de 63 caracteres.

Por lo tanto, todos los nombres de dominio conforman una estructura arbórea inversa en donde cada nodo está separado del siguiente nodo por un punto (".").

El extremo de la bifurcación se denomina host, y corresponde a un equipo o entidad en la red. El nombre del ordenador que se provee debe ser único en el dominio respectivo, o de ser necesario, en el sub-dominio. Por ejemplo, el dominio del servidor Web por lo general lleva el nombre www.

La palabra "dominio" corresponde formalmente al sufijo de un nombre de dominio, es decir, la recopilación de las etiquetas de nodo de la estructura arbórea, con excepción del ordenador.

El nombre absoluto está relacionado con todas las etiquetas de nodo de una estructura arbórea, separadas por puntos y que termina con un punto final que se denomina la dirección **FQDN** (Nombre de Dominio totalmente calificado). La profundidad máxima de una estructura arbórea es 127 niveles y la longitud máxima para un nombre **FQDN** es 255 caracteres. La dirección **FQDN** permite ubicar de manera única un equipo en la red de redes. Por lo tanto, es.kioskea.net. es una dirección **FQDN**.

Servidores de nombres de dominio:

Los equipos llamados servidores de nombres de dominio permiten establecer la relación entre los nombres de dominio y las direcciones **IP** de los equipos de una red.

Cada dominio cuenta con un servidor de nombre de dominio, llamado servidor de nombre de dominio principal, así como también un servidor de nombre de dominio secundario, que puede encargarse del servidor de nombre de dominio principal en caso de falta de disponibilidad.

Cada servidor de nombre de dominio está especificado en el servidor de nombre de dominio en el nivel superior inmediato, lo que significa que la autoridad sobre los dominios puede delegarse implícitamente. El sistema de nombre es una arquitectura distribuida, en donde cada entidad es responsable de la administración de su nombre de dominio. Por lo tanto, no existe organización alguna que sea responsable de la administración de todos los nombres de dominio.

Los servidores relacionados con los dominios de nivel superior (**TLD**) se llaman "servidores de dominio de nivel superior". Son 13, están distribuidos por todo el mundo y sus nombres van desde "a.root-servers.net" hasta "m.root-servers.net".

Resolución de nombres de dominio:

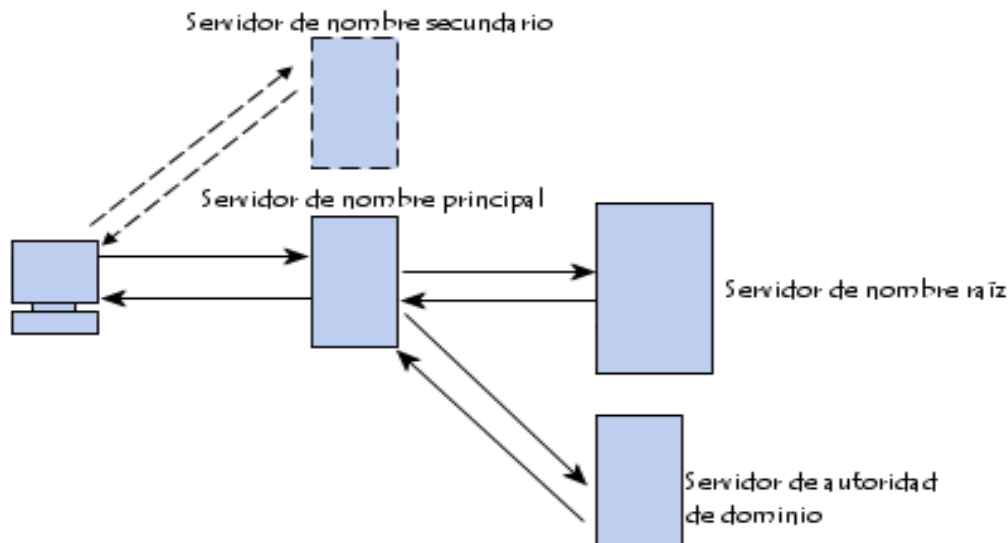
El mecanismo que consiste en encontrar la dirección IP relacionada al nombre de un ordenador se conoce como "resolución del nombre de dominio". La aplicación que permite realizar esta operación (por lo general, integrada en el sistema operativo se llama "resolución".

Cuando una aplicación desea conectarse con un host conocido a través de su nombre de dominio (por ejemplo, "es.kioskea.net"), ésta interroga al servidor de nombre de dominio definido en la configuración de su red. De hecho, todos los equipos conectados a la red tienen en su configuración las direcciones **IP** de ambos servidores de nombre de dominio del proveedor de servicios.

Entonces se envía una solicitud al primer servidor de nombre de dominio (llamado el "servidor de nombre de dominio principal"). Si este servidor de nombre de dominio tiene el registro en su caché, lo envía a la aplicación; de lo contrario, interroga a un servidor de nivel superior (en nuestro caso un servidor relacionado con el **TLD** ".net").

El servidor de nombre de nivel superior envía una lista de servidores de nombres de dominio con autoridad sobre el dominio (en este caso, las direcciones **IP** de los servidores de nombres de dominio principal y secundario para comofunciona.net).

Entonces el servidor de nombres de dominio principal con autoridad sobre el dominio será interrogado y devolverá el registro correspondiente al dominio del servidor (en nuestro caso www).



Tipos de registros:

Un **DNS** es una base de datos distribuida que contiene registros que se conocen como RR (Registros de Recursos), relacionados con nombres de dominio. La siguiente información sólo es útil para las personas responsables de la administración de un dominio, dado que el funcionamiento de los servidores de nombre de dominio es completamente transparente para los usuarios.

Ya que el sistema de memoria caché permite que el sistema **DNS** sea distribuido, los registros para cada dominio tienen una duración de vida que se conoce como **TTL** (Tiempo de vida). Esto permite que los servidores intermediarios conozcan la fecha de caducidad de la información y por lo tanto que sepan si es necesario verificarla o no.

Por lo general, un registro de **DNS** contiene la siguiente información:

Nombre de dominio (**FQDN**) TTL Tipo Clase RData

es.kioskea.net 3600 A IN 163.5.255.85

- Nombre de dominio: El nombre de dominio debe ser un nombre **FQDN**, es decir, debe terminar con un punto. En caso de que falte el punto, el nombre de dominio es relativo, es decir, el nombre de dominio principal incluirá un sufijo en el dominio introducido;
- Tipo: Un valor sobre 16 bits que define el tipo de recurso descrito por el registro. El tipo de recurso puede ser uno de los siguientes:

A: este es un tipo de base que hace coincidir el nombre canónico con la dirección **IP**. Además, pueden existir varios registros **A** relacionados con diferentes equipos de la red (servidores).

CNAME (Nombre Canónico): Permite definir un alias para el nombre canónico. Es particularmente útil para suministrar nombres alternativos relacionados con diferentes servicios en el mismo equipo.

HINFO: Este es un campo solamente descriptivo que permite la descripción en particular del hardware del ordenador (CPU) y del sistema operativo (OS). Generalmente se recomienda no completarlo para evitar suministrar información que pueda ser útil a piratas informáticos.

MX (Mail Exchange): es el servidor de correo electrónico. Cuando un usuario envía un correo electrónico a una dirección (user@domain), el servidor de correo saliente interroga al servidor de nombre de dominio con autoridad sobre el dominio para obtener el registro **MX**. Pueden existir varios registros **MX** por dominio, para así suministrar una repetición en caso de fallas en el servidor principal de correo electrónico. De este modo, el registro **MX** permite definir una prioridad con un valor entre 0 y 65,535:

- **NS:** es el servidor de nombres de dominio con autoridad sobre el dominio.
- **PTR:** es un puntero hacia otra parte del espacio de nombres del dominio.
- **SOA** (Start Of Authority (Inicio de autoridad)): el campo **SOA** permite la descripción del servidor de nombre de dominio con autoridad en la zona, así como la dirección de correo electrónico del contacto técnico (en donde el carácter "@" es reemplazado por un punto).
- **Clase:** la clase puede ser **IN** (relacionada a protocolos de Internet, y por lo tanto, éste es el sistema que utilizaremos en nuestro caso), o **CH** (para el sistema caótico);
- **RDATA:** estos son los datos relacionados con el registro.

Aquí se encuentra la información esperada según el tipo de registro:

- **A:** la dirección **IP** de 32 bits;
- **CNAME:** el nombre de dominio;
- **MX:** la prioridad de 16 bits, seguida del nombre del ordenador;
- **NS:** el nombre del ordenador; **PTR:** el nombre de dominio
- **PTR:** el nombre de dominio;
- **SOA:** varios campos.

Dominios de nivel superior:

Existen dos categorías de TLD (Dominios de Nivel Superior):

- Los dominios que se conocen como "genéricos", llamados gTLD (TLD genérico). Los gTLD son nombres de dominio de nivel superior genéricos que ofrecen una clasificación

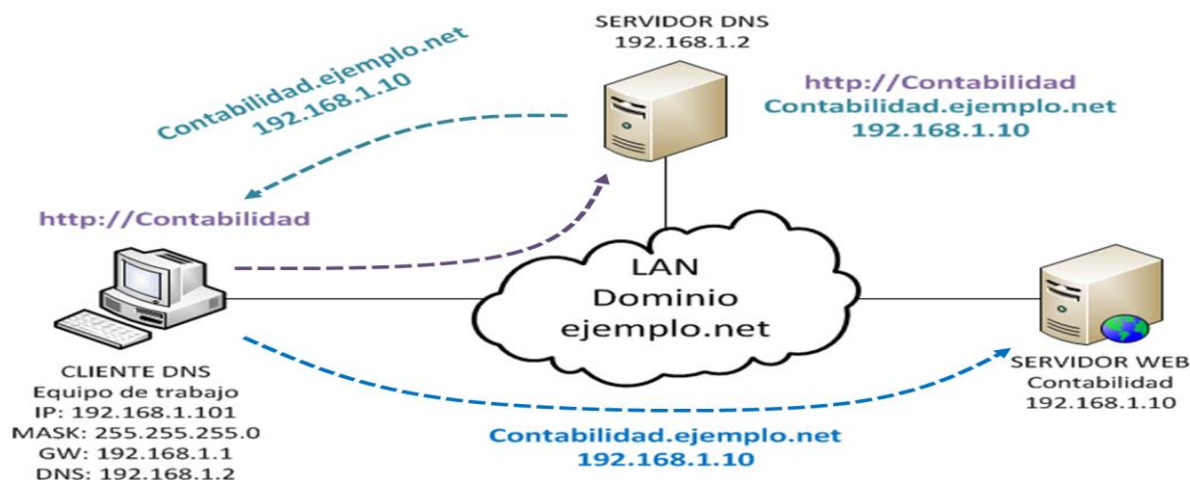
de acuerdo con el sector de la actividad. Entonces cada gTLD tiene sus propias reglas de acceso:

- gTLD historial:
 - .arpa relacionado con equipos pertenecientes a la red original;
 - .com inicialmente relacionado con empresas con fines comerciales. Sin embargo, este TLD se convirtió en el "TLD predeterminado" y hasta personas reales pueden adquirir dominios con esta extensión.
 - .edu relacionado con las organizaciones educativas;
 - .gov relacionado con las organizaciones gubernamentales;
 - .int relacionado con las organizaciones internacionales;
 - .edu relacionado con las organizaciones militares;
 - .net inicialmente relacionado con las organizaciones que administran redes. Con el transcurso de los años este TLD se ha convertido en un TLD común, y hasta personas reales pueden adquirir dominios con esta extensión.
 - .org está normalmente relacionado con organizaciones sin fines de lucro.
- nuevos gTLD presentado en noviembre de 2000 por ICANN:
 - .aero relacionado con la industria aeronáutica;
 - .biz (negocios) relacionado con empresas comerciales;
 - .museum relacionada con los museos;
 - .name relacionada con el nombre de personas reales o imaginarias;
 - .info relacionado con organizaciones que manejan información;
 - .coop relacionado con cooperativas;
 - .pro relacionado con profesiones liberales.
- gTLD especial:
 - .arpa relacionado con las infraestructuras para la administración de redes. El arpa gTLD también sirve para la resolución inversa de equipos en red y permite hallar el nombre relacionado con una dirección IP.
- Los dominios que se conocen como "nacionales", se llaman ccTLD (código de país TLD). El ccTLD está relacionado con los diferentes países y sus nombres se refieren a las abreviaturas del nombre del país definidas en la norma ISO 3166.

A continuación, algunos ejemplos de la lista de ccTLD.

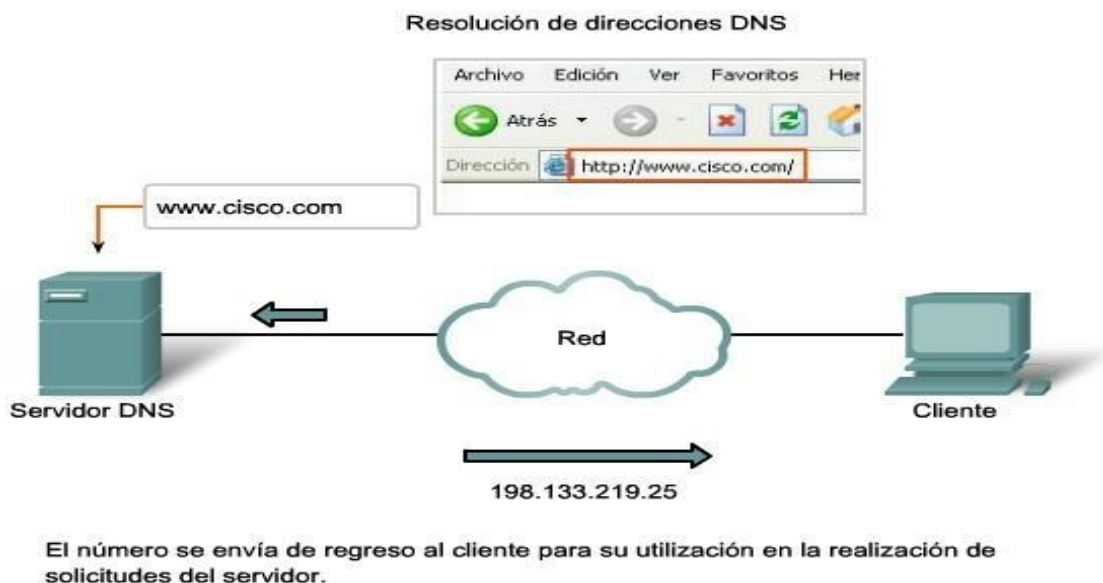
CÓDIGO: AR (Argentina), CO (Colombia), ES (España), HK (Hong Kong), NZ (Nueva Zelanda), UK (Reino Unido), ZA (Sudáfrica).

Si un equipo quiere comunicarse con otro llamado "CONTABILIDAD", la comunicación de red, se realizaría mediante IP, pero antes deberá averiguar cuál es la misma, utilizando la resolución de nombres.



Teniendo un servidor DNS, esa consulta la haría él mismo, buscaría en su zona si está ese equipo relacionado con una IP, y al encontrarlo, enviaría esa información al equipo que realizó la consulta.

En INTERNET, es constante la consulta con servidores DNS (ROOT HINTS), los cuales contienen la información necesaria para encontrar un dominio.



RECORDAR:

La información proporcionada por un servidor DNS se presenta en diferentes categorías llamadas registros.

A: son los registros principales, relaciona un nombre con una dirección IP

PTR: el inverso de A, relaciona una dirección IP con un nombre

NS: identifica a los servidores DNS del dominio consultado

MX: identifica a los servidores de correo electrónico correspondientes del dominio consultado, son utilizados por los servidores SMTP que posean correos electrónicos destinados a usuarios dentro de nuestro dominio.

Ejercicio Número 3 Unidad 3



Utilizar y probar el comando “**nslookup**”, usar como guía el **help** del mismo comando.

Buscar 3 direcciones **IP** y resolverlas a través del mismo comando.

Para los que no conocen este comando, tienen un Link TIP:

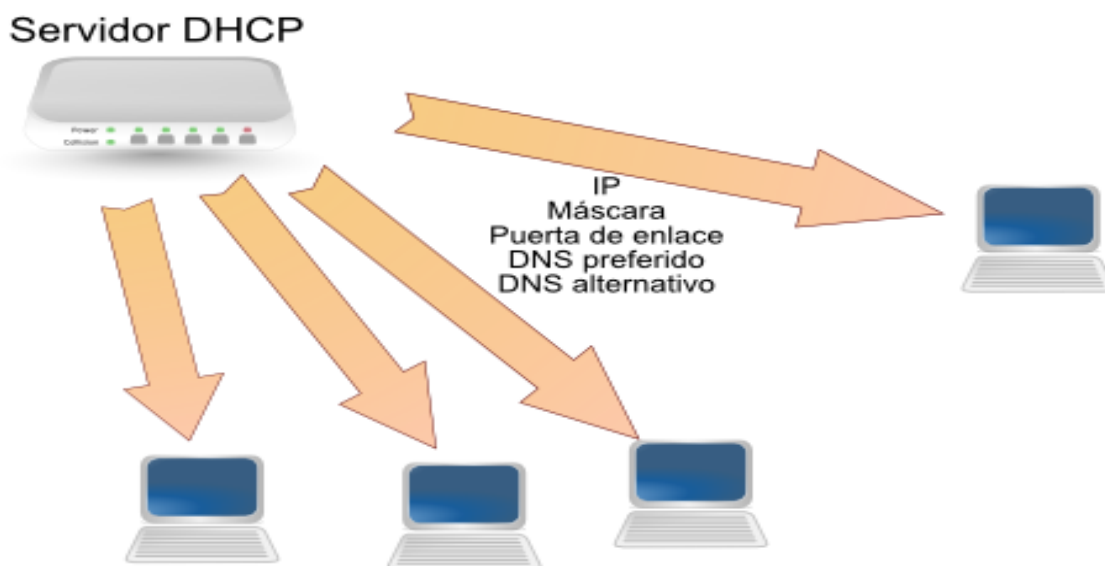
<https://norfipc.com/redes/como-usar-comando-nslookup-windows.html>

Recordar que es un comando propio del sistema operativo, hay cientos de comandos y puede resultar tedioso buscar información por muchos lados, por eso en esta práctica intentamos

estimular al alumno a realizar estos ejercicios, que son parte del conocimiento básico que uno debe tener y exponemos links de ayuda recomendados.

DHCP (Dynamic Host Configuration Protocol)

Se encarga de proveer las configuraciones necesarias de conectividad a los dispositivos (compatibles con este servicio) que se conectan a la red de una manera automática, simple y rápida.



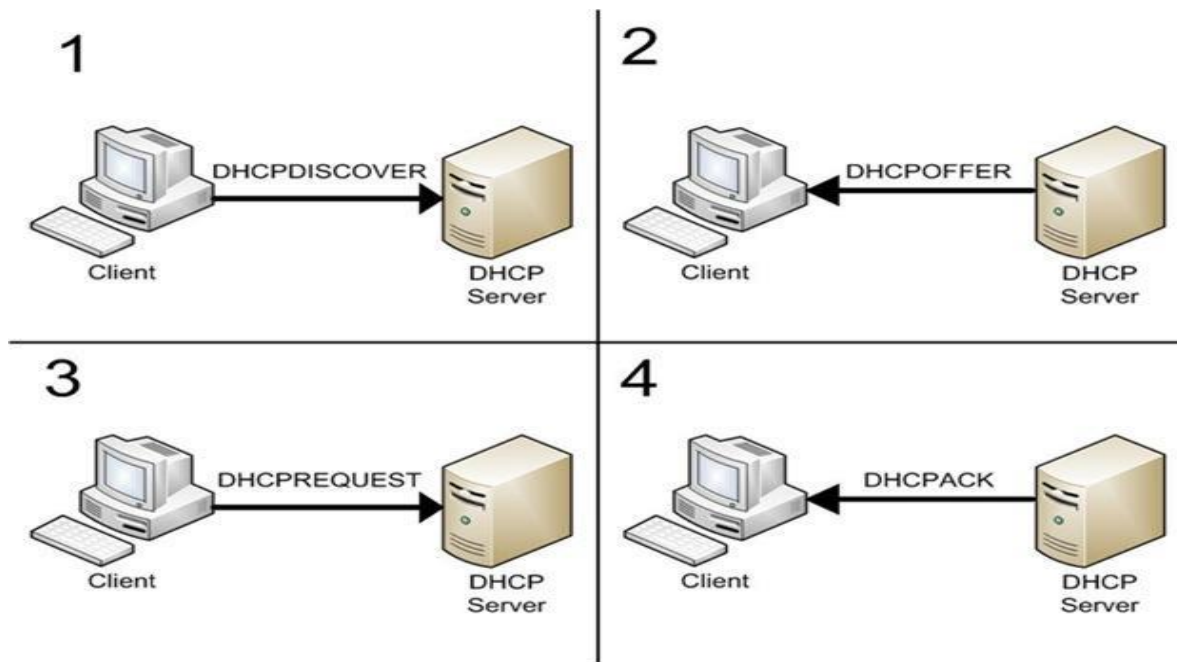
Gracias a este servicio, no es necesario configurar un dispositivo en forma manual, el solo hecho de conectarlo a la red, tomaría un direccionamiento automático de acuerdo a como lo configuramos.

Los pasos serían los siguientes:

- Se conecta un dispositivo en una boca de red o por WIFI.
- El dispositivo enviará paquetes de broadcast llamado **DHCPDISCOVER** buscando la existencia de un servidor **DHCP**.
- El servidor de **DHCP**, al recibir esa solicitud, reservara de su address pool, una dirección asignada a la **MAC** del dispositivo solicitante, enviándole una respuesta con un paquete unicast llamado **DHCPOFFER**, indicando un resumen del segmento de red.
- Este paquete será recibido únicamente por el dispositivo solicitante.

Cuando el dispositivo lo reciba, enviará un **DHCPREQUEST**, que simboliza el pedido oficial de obtención de su dirección IP y la conexión a la red.

El servidor lo recibe, asigna la IP reservada anteriormente, y envía un **DHCPACK**, notificando la aceptación del servidor, junto con la lista completa de opciones de configuración asignadas al cliente, más un tiempo de la duración de la reserva (**lease**).



Ejercicio Número 4 Unidad 3



Explicar el proceso de DHCP en este dibujo, y especificar cómo sería el direccionamiento IP que ofrecería a los dispositivos (la máscara es 255.255.255.0 o podría ser la 255.255.0.0)

AYUDA: hay un servicio que todavía no se enseñó que permitiría el uso de dos segmentos de red diferentes a través de un SW, ¿cuál es?

Laboratorio teórico: Potenciales ataques

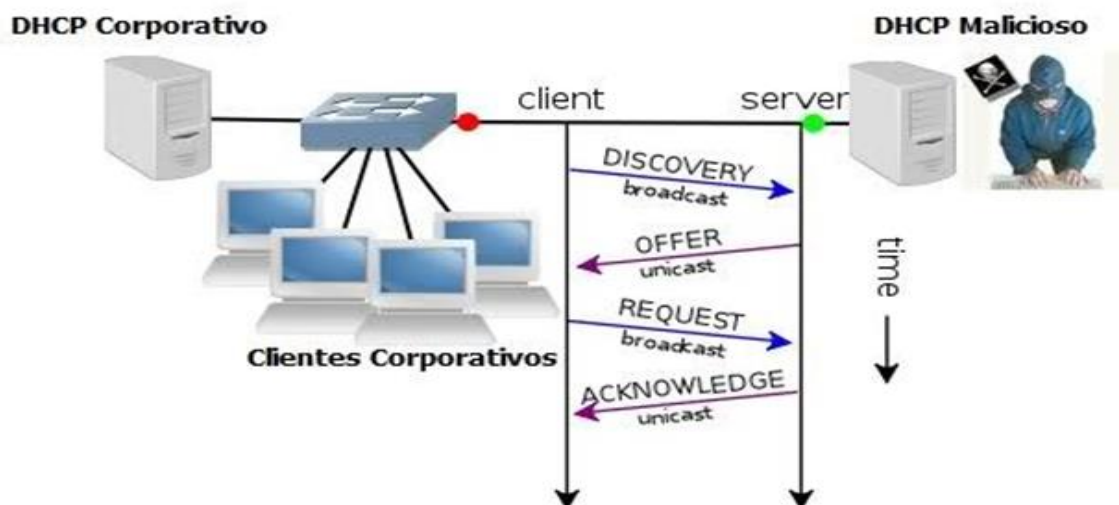


Estos son los nombres de algunos ataques más conocidos (a **DHCP**):

DHCP STARVATION

Es un ataque que consiste en inundar con peticiones **DHCP REQUEST** al servidor **DHCP**, con direcciones **MAC** falseadas y con el objetivo de agotar su espacio de direcciones asignables. El objetivo es que el servidor **DHCP** no sea capaz de responder a otros clientes.

DHCP SPOOFING



Consiste en suplantar al servidor de **DHCP** de una red y modificar los parámetros de red que reciben los equipos conectados al renovar o solicitar una nueva **IP**.

DHCP ROGUE SERVER

Un **DHCP** rogue server es un servidor que se encuentra en la red fuera del control del administrador de la misma para hacer ataques de tipo **MITM** modificando los parámetros de red que reciben los equipos de la red. Tiene el inconveniente de que no puede asegurarse que reciba la configuración los equipos del servidor atacante al existir un atacante legítimo en la red.

DHCP ACK INJECTION ATTACK

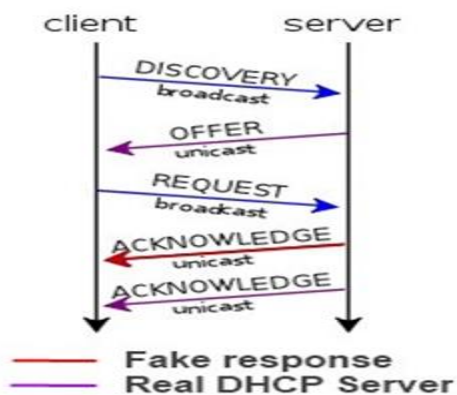
Tipo de ataque que mejora la utilización de un **DHCP** rogue server para hacer **DHCP** spoofing ya que se asegura de que los equipos reciban la configuración del servidor atacante.

Dado que toda la comunicación **DHCP** se realiza enviando los paquetes a la dirección **MAC** de broadcast FF:FF:FF:FF:FF:FF todos los clientes reciben los paquetes **DHCP**. Así que existe la posibilidad de que un atacante monitoree los intercambios **DHCP** y en un determinado punto de la comunicación envíe un paquete especialmente formado para modificar su comportamiento.

Uno de los puntos donde nos interesaría intervenir es cuando el servidor reconoce con un **DHCP ACK** la configuración del cliente. Primero se tiene que escuchar toda la comunicación poniendo atención en el paquete **REQUEST** donde el cliente solicita la **IP Gateway** de aquellos datos que anteriormente le ha ofrecido el servidor **DHCP**.

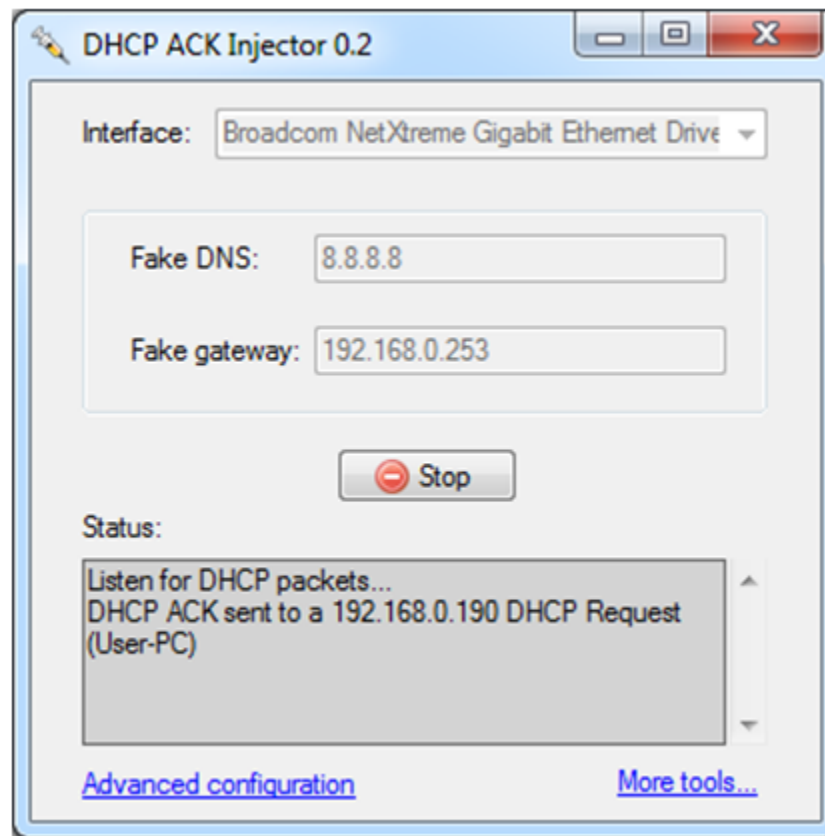
Una vez recibido el **REQUEST** el atacante responde con un **ACK** como lo haría el servidor **DHCP** real pero estableciendo la configuración de red modificada.

En el siguiente esquema se muestra el ataque:



Existe una herramienta denominada **DHCP ACK Injector** que es capaz de realizar este tipo de ataques. Entre sus parámetros configurables está:

- El servidor de que se le da al cliente
- La puerta de enlace que se le suministra al cliente.
- La dirección **MAC** del servidor **DHCP**
- La dirección **IP** del servidor



DHCP EXHAUSTION ATTACK

Ataque consistente en realizar peticiones **DHCP REQUEST** al servidor hasta que deja de recibir respuesta del servidor porque este ha agotado su pool de direcciones disponibles. Es un ataque de tipo denegación de servicio, ya que cualquier otro equipo que haga petición de concesión o renovación de **DHCP** no va a obtener respuesta del servidor.



De acuerdo a lo aprendido en las últimas 3 unidades, hacer un entregable, explicando cuáles podrían ser potenciales formas de mitigar los ataques en cada servicio o protocolo, por ejemplo, un ataque a un servidor DHCP.

Especificar diciendo nombre del ataque y servicio o protocolo atacado

Al menos seleccionar 2 ataques de todo lo que vimos, relacionados con lo aprendido

A continuación se brinda un aporte, pero la idea es que lo hagan con sus palabras:

VACL (Vlan Access List)

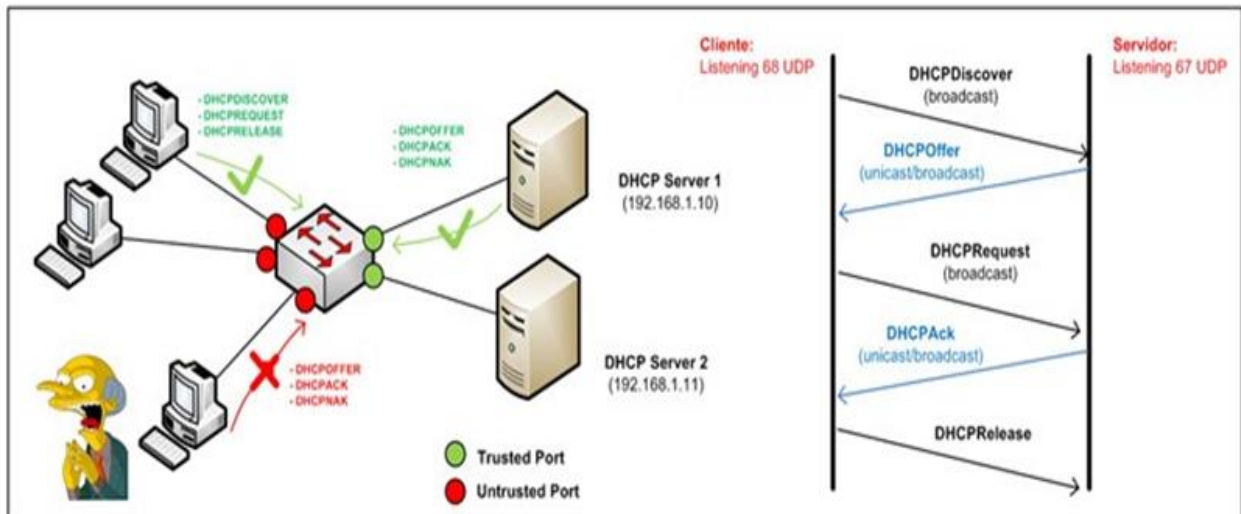
VACLs proporcionan control de acceso a todos los paquetes que se incluyen dentro de la **VLAN** permite filtrar paquetes a determinados puertos.

Habría que bloquear el tráfico proveniente del puerto 67 para aquellos puertos del switch destinados al usuario final. El problema de esta contramedida es que podría evadirse fácilmente si se falsifica la **MAC** e **IP** de los paquetes (y que en el caso de **DHCP Ack Injector** es posible)

DHCP snooping

Provee una protección más fiable.

La idea de esta funcionalidad es diferenciar entre dos tipos de puertos en un entorno conmutado: por una lado puertos confiables (trusted port) y, por otro, puertos no confiables (untrusted host).



Los primeros no tendrán restricciones de cara al tipo de mensajes **DHCP** que puedan recibir, puesto que serán aquellos conectados a un entorno controlado (en este caso a los servidores **DHCP**). Sin embargo, los segundos únicamente podrán enviar aquellos paquetes que en condiciones normales un cliente necesita enviar para conseguir su configuración **DHCP** (**DHCPDiscover**, **DHCPRequest**, **DHCPRelease**).

Los untrusted port por tanto serán configurados en aquellos puertos conectados a los usuarios finales y en el caso de que dicho puerto reciba un paquete suplantado **DHCPoffer**, un **DHCPack**, o **DHCPNack** (este es el caso de **DHCP Ack Injector**), serán bloqueados.

Cómo presentar los ejercicios de la unidad

Hay dos tipos de ejercicios, los de la unidad y los que se exponen como obligatorios (que son los finales de cada módulo)

La idea está en que cada uno pueda desarrollar todos los ejercicios y expresarlos en un archivo .doc o .pdf y lo suba al correspondiente foro que estará habilitado.

En el mismo, el formato del archivo será apellido_UnidadX.doc (donde apellido será el de cada uno y la "X" el número de la unidad de los ejercicios)

Esto significa que en un solo archivo deberán estar todos los ejercicios, así centralizamos lo de cada uno.

Es muy **IMPORTANTE** que realicen todos los ejercicios, ya que al ser un curso a distancia, es una herramienta para saber si hubo una buena comprensión de la unidad.

Luego, los mismos serán revisados por el instructor dentro de los 5 días de haberlo subido, por eso es importante que lo hagan pronto, para que no se les sume ejercicios de otras unidades.

Pueden ser revisados por todos los demás alumnos e instructor para dar puntos de vista, ayuda o guía.

Los ejercicios de esta unidad no llevan calificación

Los únicos ejercicios que tienen puntuación son los finales, que se realizan cada 4 unidades, pero más adelante se hablará de esto.



Bibliografía utilizada y sugerida

Harrington, J.(2006) Manual práctico de seguridad de redes. Editorial Anaya Multimedia. México

Hush J.(2020) Redes Informáticas Para Principiantes: La Guía Completa de la Tecnología Inalámbrica, La Seguridad de Redes, Arquitectura de Las Computadoras Y Los Sistemas de Comunicación. Editorial Charlie Creative Lab. España

Dorsel, R.(2020) Hacking for Beginners: Mastery Guide to Learn and Practice the Basics of Computer and Cyber Security. Editorial Charlie Creative Lab. EEUU

Trew, P.(2020) Kali Linux Hacking: A Complete Guide to Learn the Fundamentals of Hacking, Cyber Security, and Penetration Testing. Editorial Charlie Creative Lab. EEUU

Knox, J.(2020) Computer Hacking. Editorial Charlie Creative Lab. EEUU

Link complementarios:

<http://www.slideshare.net/mamuga/tipos-de-ataques-y-vulnerabilidades-en-una-red>

¿Cómo funciona ARP?:

<https://www.youtube.com/watch?v=DoQcznhxbhw>

En caso de que los links que se exponen no funcionen, por favor avisar al instructor (es normal que un sitio pueda cambiar su URL, dominio o variables, lo cual como la unidad se prepara a principio de año podría suceder que se haya modificado)