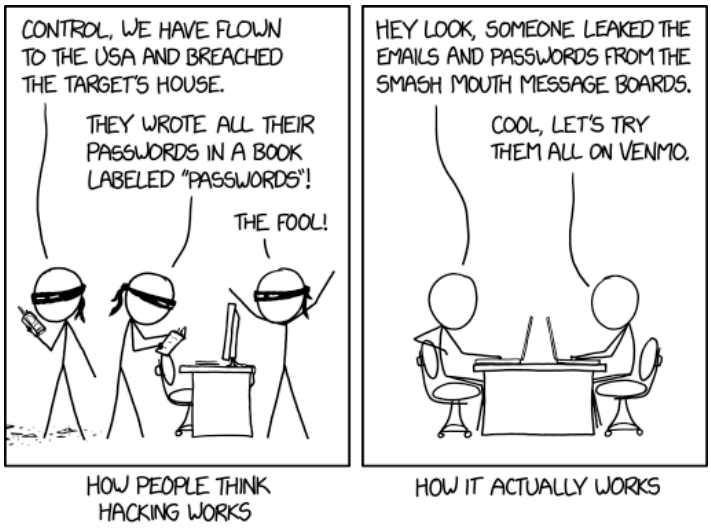
Taller 5: *PenTesting: Fundamentos de Análisis de Vulnerabilidades*

Para el desarrollo de este taller debe crear un informe en formato `.doc` o formato `.odt` en el cual debe colocar las respuestas a todas las preguntas **resaltadas en negritas** que encuentre en las siguientes Secciones. Al finalizar el taller envíe su respectivo informe al profesor. El informe debe incluir su nombre y número de cédula al principio.



1. Herramientas de UNIX: `nslookup` y `dig`

`Nslookup` y `dig` son dos herramientas básicas de UNIX que permiten realizar consultas a servidores DNS.

1.1. `nslookup`

La ejecución básica de `nslookup` tiene la siguiente forma:
`nslookup -query=`*`TIPO DOMINIO SERVIDOR`*

Las opciones mostradas son las siguientes:

-query=*TIPO* modifica el tipo de consulta DNS que se realiza, es decir el tipo de registro DNS solicitado. Por defecto se solicitan registros de tipo `A` (dirección IPv4).

DOMINIO nombre de dominio o dirección a revisar. Si se coloca una dirección IP en lugar de un nombre de dominio se realiza entonces una consulta de DNS reversa.

SERVIDOR servidor DNS a consultar.

Todos los parámetros indicados son opcionales. Si no se especifica el *DOMINIO* a verificar entonces `nslookup` entra a un modo de uso interactivo.

Ejecute los siguientes comandos `nslookup` y analice las salidas de cada uno.

1. `nslookup correo.ciens.ucv.ve`
2. `nslookup -query=MX correo.ciens.ucv.ve 8.8.8.8`
3. `nslookup -query=AAAA correo.ciens.ucv.ve 190.169.30.2`
4. `nslookup -query=PTR correo.ciens.ucv.ve`
5. `nslookup 190.169.94.200`

1.2. `Dig`

`Dig` es una alternativa a `nslookup` para hacer consultas a servidores DNS. **ejecute el comando "`dig correo.ciens.ucv.ve`" y contraste su salida con la correspondiente producida por `nslookup`.**

2. Análisis Web con `nikto`

El análisis de vulnerabilidades de un servidor Web con la herramienta `nikto` es muy sencillo. La ejecución del comando `nikto` toma la forma siguiente:

`nikto -Display` ***NIVEL*** `-host` ***URL:PUERTO*** `-id` ***USUARIO:CONTRASEÑA*** `-output` ***ARCHIVO***

Algunas de las opciones que puede recibir el comando son las siguientes:

-Display *NIVEL* donde *NIVEL* puede ser `1`, `2`, `3`, `4`, `D` ó `V`. Modifica el nivel de impresión de salida del comando.

-host *URL:PUERTO* especifíca la dirección IP o nombre de dominio y puerto del servidor a analizar.

-id *USUARIO:CONTRASEÑA* parámetros de identificación para el caso de que el servidor utilice autenticación básica de HTTP.

-output *ARCHIVO* guarda un reporte de las pruebas realizadas en el archivo especificado. El reporte puede tener formato `.csv`, `.html`, `.txt` o `.xml`.

Los parámetros `-Display`, `-id` y `-output` son opcionales.

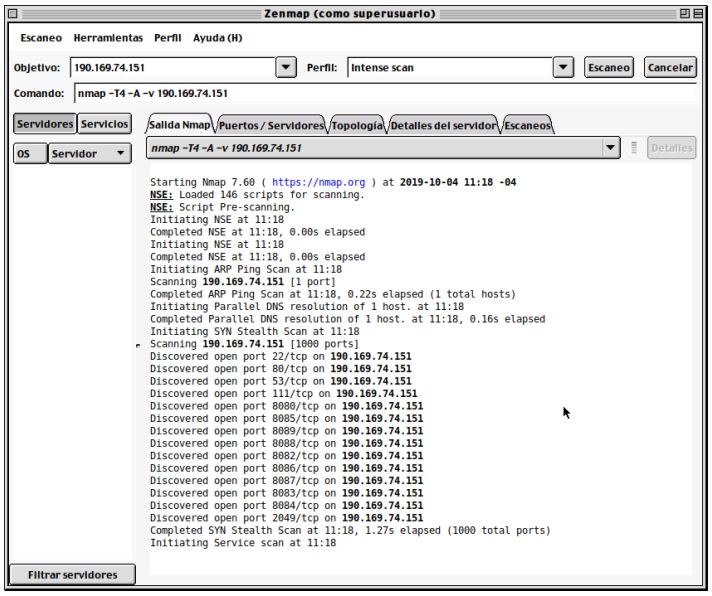
Ejecute `nikto` con el siguiente comando "`nikto -host http://190.169.74.151:9989 -output reporte.htm`". Una vez termine la ejecución del comando revise en la terminal cuantas pruebas realizó `nikto`, cuantas pruebas fallaron (reportaron error) y cuantos problemas identificó en el servidor. Revise el reporte generado por `nikto` y adjúntelo a su informe.

3. Exploración con `Zenmap`

`Zenmap` es una interfáz gráfica para el escaner de puertos `nmap`. Este escaner permite analizar un servidor a nivel de red para poder detectar información como la siguiente:

1. *Hosts* activos e inactivos en la red.
2. Puertos abiertos y/o filtrados en un *host* específico.
3. Versiones de software y sistemas operativos de los *hosts* escaneados.

La siguiente imagen muestra un ejemplo de la interfaz de `Zenmap`.



Ejecute `Zenmap` como usuario `root`. En la parte superior verá tres entradas de texto etiquetadas *Objetivo*, *Perfil* y *Comando* respectivamente. Coloque en el campo *Objetivo* la dirección IP "`190.169.74.1-254`". Escoja para el *Perfil* la opción `ping scan` y luego presione el botón etiquetado *Escaneo*. **Cuando el escaneo termine verifique en la salida cuales *hosts* están levantados actualmente**. El `ping scan` se utiliza para identificar *hosts* activos y consiste simplemente en el envío de mensajes `ping` para ver que *hosts* responden.

Para realizar la siguiente prueba, coloque en el campo *Objetivo* la dirección IP "`190.169.74.151`". Escoja para el *Perfil* la opción `Intense scan, all TCP ports` y luego presione el botón de *Escaneo*. **Cuando el escaneo termine**[1] **verifique en la salida cuales puertos abiertos tiene el *host* escaneado, que servicios se están ejecutando en cada puerto y cual es el sistema operativo del servidor. Utilice las pestañas identificadas como *Puertos/Servidores* y *Detalles del servidor* para obtener esta información**.

IMPORTANTE: No coloque otra dirección IP para este último escaneo. La única dirección autorizada para escanear en este taller es la dirección indicada.

[1] Puede realizar las demás actividades del taller mientras el escaneo se ejecuta. Este escaneo en particular toma aproximadamente 30 minutos en ejecutarse completo. El `Intense scan` basico sin el complemento de `all TCP ports` es considerablemente más rápido pero fallará en identificar servicios activos en puertos con valores altos.