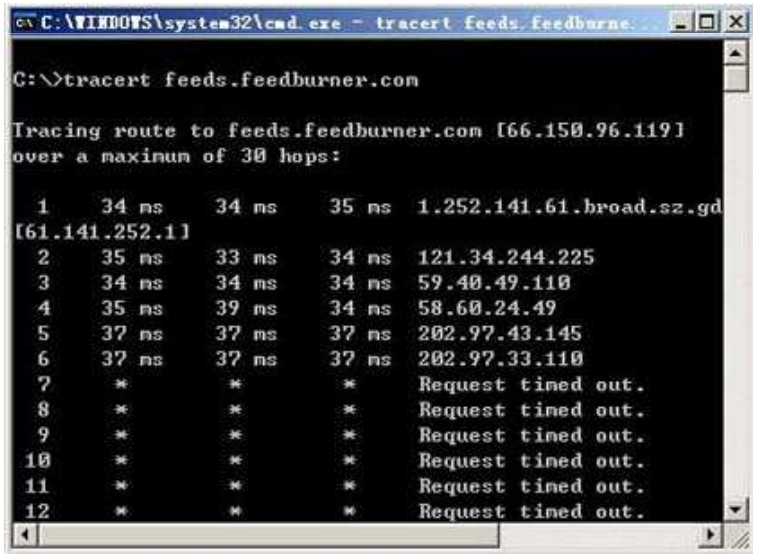
3- SCANNING

NETWORK MAPPING .

El proceso de **Network Mapping**, consiste en tratar de identificar la arquitectura (Topología) de la red a la cual vamos a realizarle las pruebas de seguridad y auditoria a nivel intrusivo.

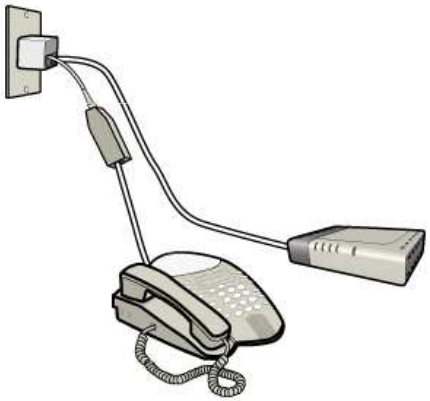


Network Mapping y Port Scanning

Luego del proceso de mapeo de la red, se puede proceder posteriormente a realizar procesos de Scanning. **¿¿¿¿¿Pero a que se le puede realizar procesos de Scanning????????**

AP Inalámbricos

Sistemas PBX



Módems

Redes TCP/IP

Ping-Sweep .

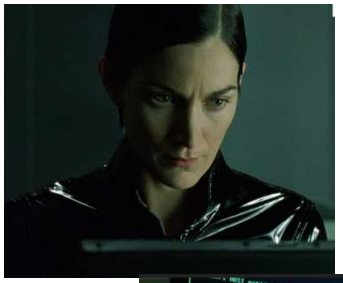
El proceso de **Ping Sweep,** consiste en poder identificar hosts que este vivos dentro de una red, con el propósito de que dichos Hosts, posteriormente se coinvierte en parte del conjunto de targets (Objetivos), o sistemas que se requieren evaluar y auditar. El proceso de Ping Sweep, se puede realizar de varias formas, como por ejemplo usando una de las tantas herramientas especializada en scanning, o realizando algún tipo de Script que invoque el comando ping de forma secuencial, según el numero de hosts de una subred.

```
root@kali:~# nmap -sP 192.168.153.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2014-05-21 15:46 EDT
Nmap scan report for 192.168.153.1
Host is up (0.00081s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.153.2
Host is up (0.00017s latency).
MAC Address: 00:50:56:EC:1D:56 (VMware)
Nmap scan report for 192.168.153.129
Host is up (0.00089s latency).
MAC Address: 00:0C:29:4D:88:55 (VMware)
Nmap scan report for 192.168.153.254
Host is up (0.00029s latency).
MAC Address: 00:50:56:F5:32:08 (VMware)
Nmap scan report for 192.168.153.130
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 1.84 seconds
root@kali:~#
```

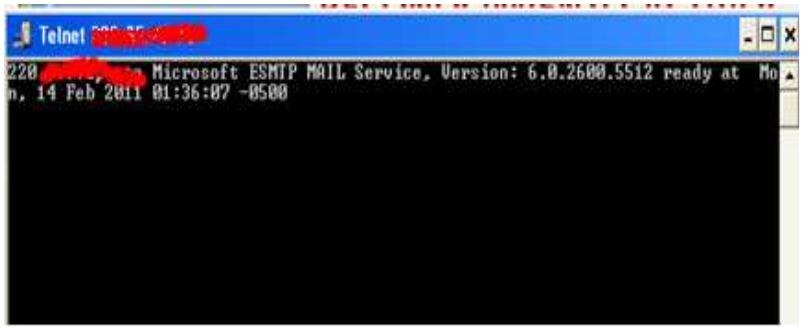
http://en.wikipedia.org/wiki/Ping_sweep

PORT SCANNING. -Características



"Es la segunda fase del Hacking Ético, y consiste en la identificación activa de objetivos de ataque o evaluación, mediante un proceso de escaneo de puertos, la identificación de servicios y sistemas operativos". Algunas de las características de la fase de Scanning son:

- ✓ **Identificación y Estado de Puertos.**
- ✓ **Identificar Servicios**
- ✓ **Identificar Sistema operativo.**
- ✓ **Hay contacto directo con el Objetivo**
- ✓ **Banner Grabbing "Captura de Banners"**



PORT SCANNING.

Scanning de Puertos: También identificada como la fase de exploración de puertos y vulnerabilidades, es una fase en la cual el atacante intenta descubrir que puertos están abiertos en el sistema objetivo, luego de que el atacante puede identificar el estado de los puertos, procede a identificar servicios asociados a estos puertos, para posteriormente lanzar un ***Scanning de vulnerabilidades***, con el fin de identificar posibles entradas en el sistema victima. Una exploración de puertos puede interpretarse como una etapa de Pre- ataque. Un proceso completo de Scanning involucra herramientas exploradoras de puertos, exploradores de vulnerabilidades, mapeadores de red y Dialers para identificar puertos de Módems en equipos remotos.

PORT SCANNING

¿En que consiste?

Escaneo de Puertos: El escaneo o exploración de puertos es una actividad que consiste en el envió de paquetes de red a un host (Router, IDS, Firewall, PC Escritorio, Portatil, Tablet, Servidor, Entre otros), con el objetivo de identificar el estado de los puertos TCP o UDP. Un puerto en una host tiene varios estados, entre los cuales se puede distinguir:

- ✓ ***Abierto***
- ✓ ***Cerrado***
- ✓ ***Filtrado***

PORT SCANNING.

Tipos generalizados de procesos de Scanning

- Scanning de Puertos
- Scanning de Vulnerabilidades
- Scanning de Red

PORT SCANNING.

Otras aplicabilidades del Scanning:

Todas las anteriores definiciones están orientadas a una exploración de puertos de un solo equipo, pero también hay otras clases de exploraciones, tales como: **Exploraciones de red, exploraciones de vulnerabilidades, exploraciones de módems**, entre otros. La exploración de red es un procedimiento para identificar host o maquinas activas en una red, **la exploración de módems**, consiste en la búsqueda de Módems que estén a la escucha de servicios de acceso remoto **(RAS),** los cuales son poco comunes en nuestros días, pero sin embargo hay aun servidores con estos servicios. Para la búsqueda de Módems, no se requiere de tarjeta de red, se debe de usar un Equipo con un Modem, y se le instala un programa especial para identificar equipos con módems a la escucha, llamados Dialers.

PORT SCANNING.

Fases básicas del proceso de Scanning

Entre las fases y/o actividades que aun auditor de seguridad del tipo Hacking Ético deberá de realizar en el procesos de scanning básico, son:

- ✓ **Arquitectura del Sistema evaluado.**
- ✓ **Direccionamiento IP de la red que se va a auditar**
- ✓ **Detectar sistemas vivos corriendo o ejecutando procesos en una red**
- ✓ **Descubrir que puertos están abiertos o tienen programas/servicios en ejecución.**
- ✓ **Descubrir huellas de sistemas operativos, o lo que se conoce como OS FingerPrinting**
- ✓ **Identificar Banners**
- ✓ **Aplicación de diversas técnicas de scanning**
- ✓ **Evasión**

PORT SCANNING.

Herramientas de Scanning (NMAP)

Son muchas las herramientas a nivel de Software para realizar procesos de auditorias de seguridad relacionadas con la fase de Scanning, sin embargo existe una herramienta que es muy completa, y altamente usada en el mundo de la seguridad informática, y las auditorias de seguridad.

NMAP (Nmap Security Scanner)

http://nmap.org/

PORT SCANNING.

Intercambio de 3 Vías

"Three Way Handshake"

Existen varias técnicas de escaneo de puertos, las cuales varían según las necesidades y habilidades del atacante. Antes de hablar de cada una de ellas, se debe de comprender lo que significa el intercambio en tres vías del protocolo TCP.

Se debe de tener presente que el protocolo TCP es un protocolo que trabaja en la capa de trasporte (Capa 4) del modelo de referencia OSI y es un protocolo orientado a conexiones, es decir que antes de comenzar a trasmitir información entre dos host, estos primero deben de sincronizarse y realizar de forma completa lo que se conoce como intercambio de tres vías

PORT SCANNING.

Intercambio de 3 Vías

"Three Way Handshake"

```
192.168.1.2:2342 ------------syn--------------->192.168.1.3:80
192.168.1.2:2342 <---------syn/ack------------192.168.1.3:80
192.168.1.2:2342-------------ack--------------->192.168.1.3:80
```

Conexión establecida

PORT SCANNING.

Bits de Control: Concepto FLAGS - Paquete TCP

- URG: Especifica a la máquina receptora la existencia de información urgente en el flujo de datos.
- ACK: Se corresponde con una respuesta de correcta recepción de un paquete anterior que se envió a otra máquina.
- PSH: Indica a la máquina receptora que debe pasar la información a la capa de aplicación (programas) lo más rápido posible.
- RST: Especifica el reinicio de la conexión entre la máquina receptora y la emisora.
- SYN: Se utiliza para la sincronización de números de secuencia entre máquinas.
- FIN: Indica que debe empezar el proceso de fin de conexión.

PORT SCANNING.

Técnicas de Exploración de Puertos

- TCP Connect Scan
- TCP SYN Scan
- TCP Xmas Tree Scan
- TCP Null scan
- UDP Scan
- Ping Scan

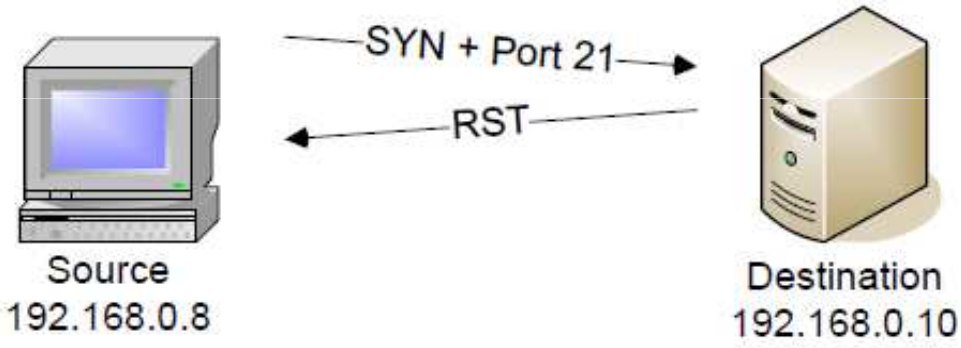
PORT SCANNING.

TCP Connect Scan: Es un proceso de exploración de puertos abierta, y necesita el intercambio de tres vías para poder realizar de forma completa la exploración de puertos. Se llama Connect Scan, ya que implementa una llamada al sistema de tipo Connect, para así saber de forma rápido el estado del puerto. Es un tipo de exploración de puertos ruidosa, es decir que es fácilmente identificada por los sistemas de filtrados de paquetes Firewall, o por los sistemas detectores de intrusos (IDS). ES una exploración de puertos segura, en lo referente a las respuestas de que los estados de los puertos, es recomendable para hacer auditorias internas a los sistemas, sin embargo no es recomendable hacerlo con host o maquinas ajenas, ya que puede considerarse como un delito.

```
192.168.1.2:2342 ------------syn-------------->192.168.1.3:80
192.168.1.2:2342 <---------syn/ack-----------192.168.1.3:80
192.168.1.2:2342-------------ack-------------->192.168.1.3:80
```

PORT SCANNING.

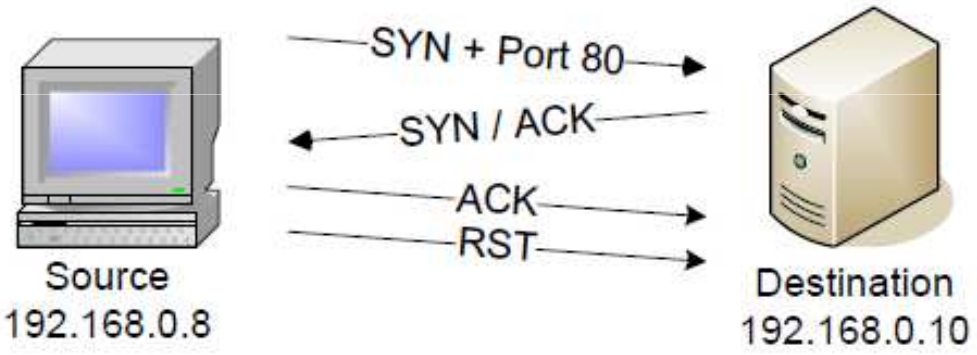
TCP Connect Scan: Grafica de cómo trabaja este tipo de Scanning para un puerto que esta **Cerrado (Closed)** en el equipo que se esta evaluando.




```
Source           Destination    Summary
-------------------------------------------------------------------------------
[192.168.0.8]    [192.168.0.10] TCP: D=21 S=41441 SYN SEQ=3365539736 LEN=0 WIN=5840
[192.168.0.10]   [192.168.0.8]  TCP: D=41441 S=21 RST ACK=3365539737 WIN=0
```

PORT SCANNING.

TCP Connect Scan: Grafica de cómo trabaja este tipo de scanning para un puerto que esta **Abierto (Open)** en el equipo que se esta evaluando.




```
Source           Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8]    [192.168.0.10]  TCP: D=80 S=49389 SYN SEQ=3362197786 LEN=0 WIN=5840
[192.168.0.10]   [192.168.0.8]   TCP: D=49389 S=80 SYN ACK=3362197787 SEQ=58695210 LEN=0
[192.168.0.8]    [192.168.0.10]  TCP: D=80 S=49389 ACK=58695211 WIN<<2=5840
[192.168.0.8]    [192.168.0.10]  TCP: D=80 S=49389 RST ACK=58695211 WIN<<2=5840
```

PORT SCANNING.

TCP SYN Scan: Es una técnica de exploración de puertos que envía de un host a otro únicamente paquetes de inicio de conexión de tipo SYN, por cada uno de los puertos que se quieren analizar, para poder determinar si estos están abiertos o no. Recibir como respuesta un paquete RST/ACK significa que no existe ningún servicio que escuche por este puerto. Por el contrario, si se recibe un paquete SYN/ACK, podemos afirmar la existencia de un servicio asociado a dicho puerto TCP. En este caso, se enviaría un paquete RST/ACK para no establecer conexión y no ser registrados por el sistema objetivo.
A diferencia del caso anterior (TCP connect scan), este tipo de exploración de puertos no es tan ruidosa, ya que no termina el proceso de intercambio en tres vías, y algunos Firewalls o IDS, no las registran.

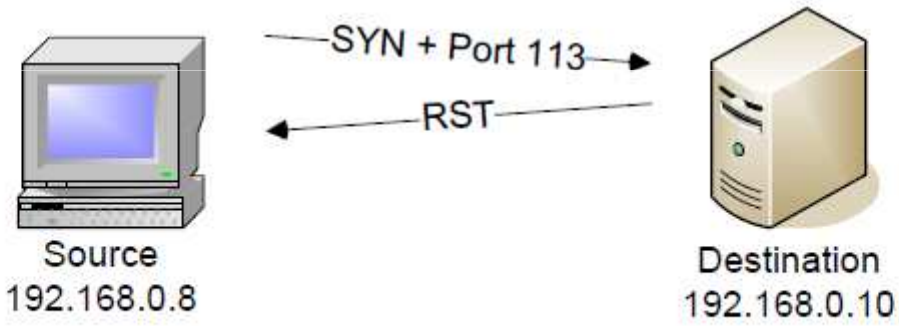
PORT SCANNING.

TCP SYN Scan Para saber si el puerto esta cerrado o no, el proceso de TCP SYN Scan debe de hacer lo siguiente: Supongamos la comunicación entre un host A y B

- **A envía a B una petición de conexión SYN**
- **B responde con una petición RST/ACK, lo que indica que el puerto esta cerrado**
- **B responde con una petición SYN/ACK lo que indica que el puerto esta abierto**
- **A responde con una petición RST para romper la conexión y no terminar el intercambio de tres vías.**

PORT SCANNING.

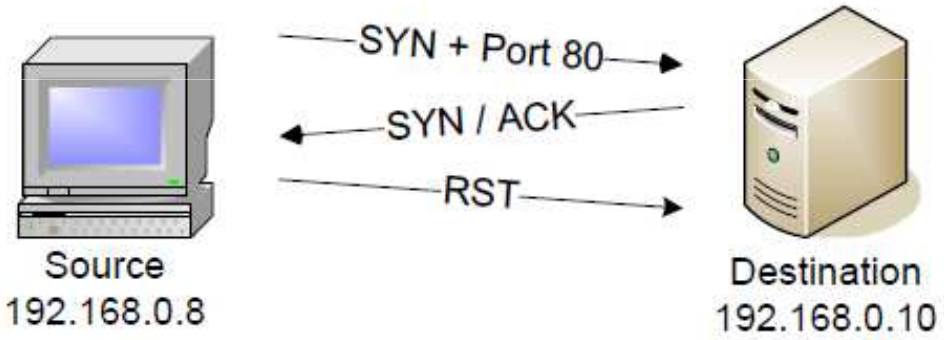
TCP SYN Scan: Grafica de cómo trabaja este tipo de scanning para un puerto que esta **Cerrado (Closed)** en el equipo que se esta evaluando.




```
Source          Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8]   [192.168.0.10]  TCP: D=113 S=57283 SYN SEQ=2360927338 LEN=0 WIN=3072
[192.168.0.10]  [192.168.0.8}   TCP: D=57283 S=113 RST ACK=2360927339 WIN=0
```

PORT SCANNING.

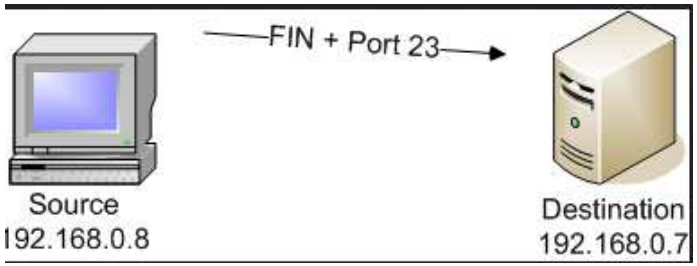
TCP SYN Scan: Grafica de cómo trabaja este tipo de scanning para un puerto que esta **Abierto (Open)** en el equipo que se esta evaluando.




```
Source          Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8]   [192.168.0.10]  TCP: D=80 S=57283 SYN SEQ=2360927338 LEN=0 WIN=3072
[192.168.0.10]  [192.168.0.8]   TCP: D=57283 S=80 SYN ACK=2360927339 SEQ=1622899389
[192.168.0.8]   [192.168.0.10]  TCP: D=80 S=57283 RST WIN=0
```

PORT SCANNING.

TCP FIN Scan: Es una técnica de exploración de puertos que consiste en enviar un paquete FIN a un puerto determinado, con lo cual deberíamos recibir un paquete de reset (RST) si dicho puerto esta cerrado. Esta técnica se aplica principalmente sobre implementaciones de pilas TCP/IP de sistemas Unix.
No es recomendable usar este tipo de exploración de puertos con Sistemas Microsoft, ya que la información que se devolverá será un poco confusa y poco valida. El FIN Scan esta pensado para trabajar únicamente con sistemas operacionales que tengan implementaciones de TCP/IP con respecto al documento RFC 793. El FIN Scan tiene como particularidad para identificar el estado de un puerto la manera en que reacciona el host victima con respecto a una petición de cierre de conexión en un puerto TCP.



PORT SCANNING.

TCP FIN Scan: Para saber si el puerto esta cerrado o no, el proceso de TCP FIN Scan debe de hacer lo siguiente:

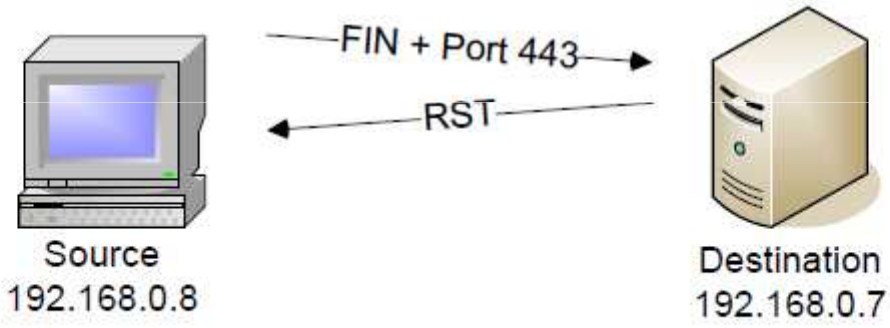
Supongamos la comunicación entre un host A y B

- El host A manda una petición FIN al host B
- Si Host B responde con una petición RST/ACK, el puerto esta cerrado
- Si host B no responde, posiblemente el puerto esta abierto.

Este tipo de exploración de puertos, es silenciosa y en muchas ocasiones no es
registrada por Firewall o IDS, así que puede ser usada por atacantes informáticos.

PORT SCANNING.

TCP FIN Scan: Grafica de cómo trabaja este tipo de scanning para un puerto que esta **Cerrado (Closed)** en el equipo que se esta evaluando.

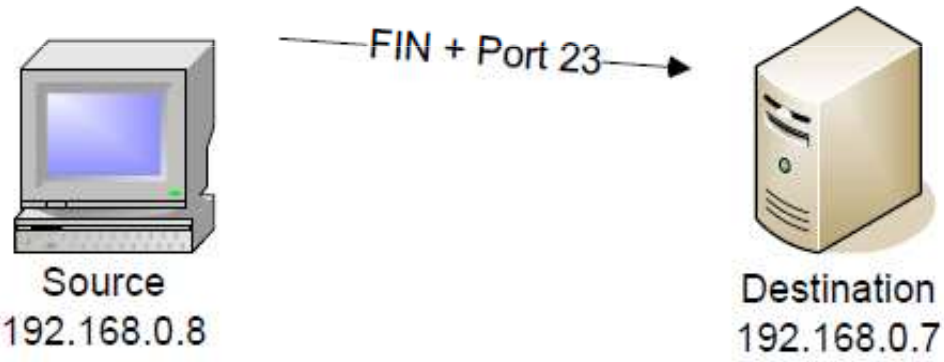



```
Source          Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8] [192.168.0.7] TCP: D=443 S=62178 FIN SEQ=3532094343 LEN=0 WIN=2048
[192.168.0.7] [192.168.0.8] TCP: D=62178 S=443 RST ACK=3532094343 WIN=0
```

PORT SCANNING.

TCP FIN Scan: Grafica de cómo trabaja este tipo de Scanning para un puerto que esta **Abierto (Open)** en el equipo que se esta evaluando.

If a port is open on a remote device, no response is received to the FIN scan:



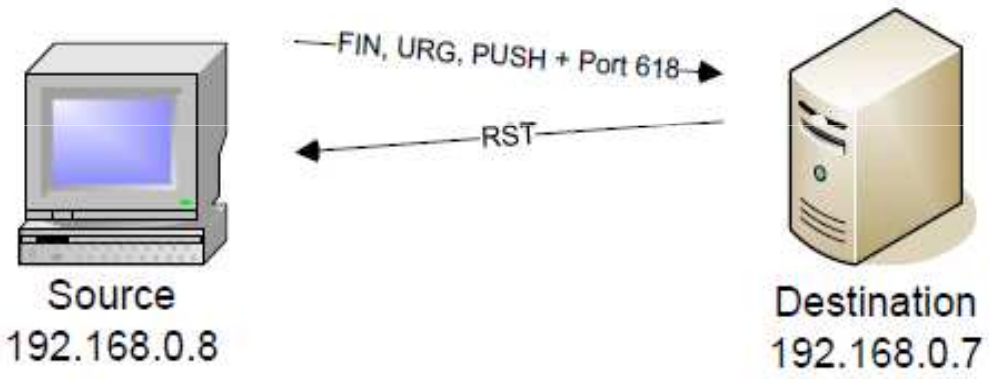

```
Source          Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8] [192.168.0.7] TCP: D=23 S=62178 FIN SEQ=3532094343 LEN=0 WIN=2048
```

PORT SCANNING.

TCP Xmas Tree Scan. Es una técnica de exploración de puertos parecida al FIN Scan, ya que también se obtiene como resultado un paquete de Reset (RST) si el puerto esta cerrado. Para el caso de este tipo de exploración de puertos, se envían paquetes o solicitudes del tipo FIN, URG y PUSH al host que se esta explorando. No es recomendable usar este tipo de exploración de puertos con Sistemas Microsoft, ya que la información que se devolverá será un poco confusa y poco valida. El Xmas Scan esta pensado para trabajar únicamente con sistemas operacionales que tengan implementaciones de TCP/IP con respecto al documento RFC 793. No es recomendable usar este tipo de exploración de puertos con Sistemas Microsoft, ya que la información que se devolverá será un poco confusa y poco valida. Este tipo de exploración es recomendable llevarlo a la practica en sistemas de tipo UNIX, LINUX y *.BSD

PORT SCANNING.

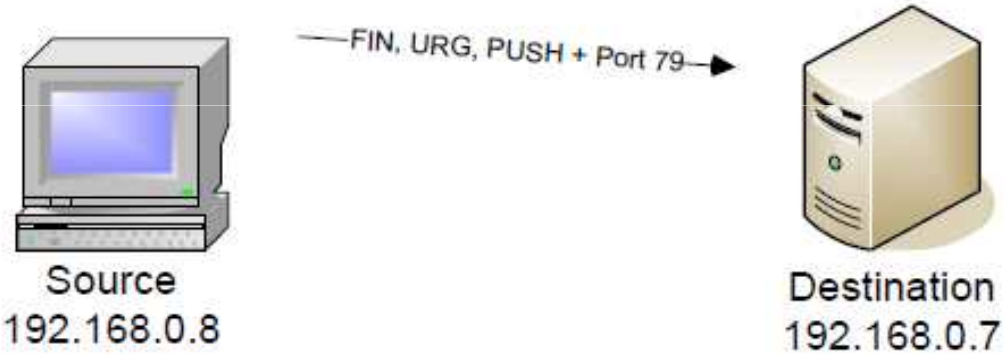
TCP Xmas Tree Scan: Grafica de cómo trabaja este tipo de Scanning para un puerto que esta **Cerrado (Closed)** en el equipo que se esta evaluando.




```
Source          Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8]   [192.168.0.7]   TCP: D=618 S=36793 FIN URG PUSH SEQ=3378228596 LEN=0 WIN=1024
[192.168.0.7]   [192.168.0.8]   TCP: D=36793 S=618 RST ACK=3378228596 WIN=0
```

PORT SCANNING.

TCP Xmas Tree Scan: Grafica de cómo trabaja este tipo de Scanning para un puerto que esta **Abierto (Open)** en el equipo que se esta evaluando.




```
Source          Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8] [192.168.0.7]   TCP: D=79 S=36793 FIN URG PUSH SEQ=3378228596 LEN=0 WIN=2048
```

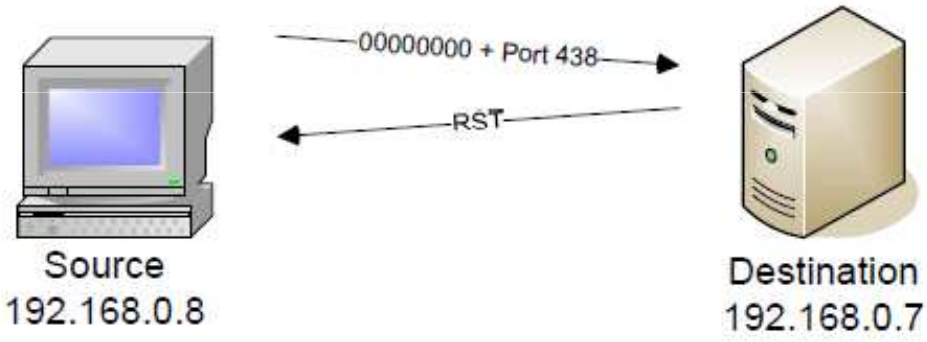
PORT SCANNING.

TCP Null scan: Este tipo de exploración pone a cero todos los Indicadores de la cabecera TCP, por lo tanto la exploración debería recibir como resultado un paquete de reset (RST) en los puertos no activos.

No es recomendable usar este tipo de exploración de puertos con Sistemas Microsoft, ya que la información que se devolverá será un poco confusa y poco valida. Este tipo de exploración es Recomendable llevarlo a la practica en sistemas de tipo UNIX, LINUX y *.BSD

PORT SCANNING.

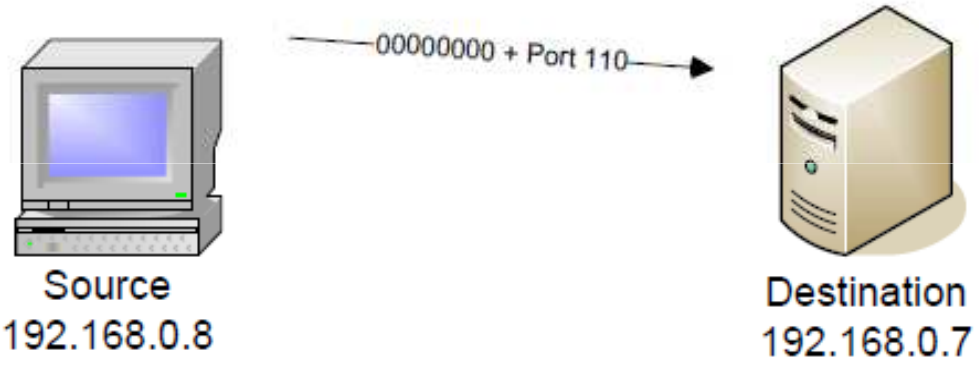
TCP NULL Scan: Grafica de cómo trabaja este tipo de Scanning para un puerto que esta **Cerrado (Closed)** en el equipo que se esta evaluando.




```
Source          Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8]   [192.168.0.7]   TCP: D=438 S=36860      WIN=4096
[192.168.0.7]   [192.168.0.8]   TCP: D=36860 S=438 RST ACK=2135565682 WIN=0
```

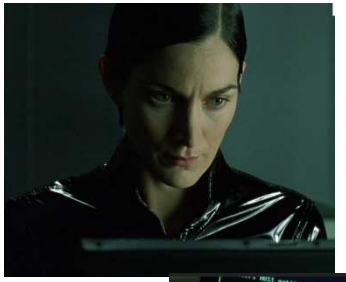
PORT SCANNING.

TCP NULL Scan: Grafica de cómo trabaja este tipo de Scanning para un puerto que esta Abierto (Open) en el equipo que se esta evaluando.




```
Source          Destination     Summary
-------------------------------------------------------------------------------
[192.168.0.8]   [192.168.0.7]   TCP: D=110 S=36860      WIN=1024
```

PORT SCANNING.



Otras Tools (Herramientas)

Algunas de las herramientas importantes en esta fase son las siguientes:

http://xprobe.sourceforge.net/

Xprobe2 active os fingerprinting tool

hping

McAfee SuperScan v3.0

http://www.mcafee.com/us/downloads/free-tools/superscan3.aspx

Unicornscan

http://www.unicornscan.org/

SCANNING.

Resumen de tipos de scanning soportados por Nmap

Nmap Scan	Command Syntax	Requires Privileged Access	Identifies TCP Ports	Identifies UDP Ports
TCP SYN Scan	-sS	YES	YES	NO
TCP connect() Scan	-sT	NO	YES	NO
FIN Scan	-sF	YES	YES	NO
Xmas Tree Scan	-sX	YES	YES	NO
Null Scan	-sN	YES	YES	NO
Ping Scan	-sP	NO	NO	NO
Version Detection	-sV	NO	NO	NO
UDP Scan	-sU	YES	NO	YES
IP Protocol Scan	-sO	YES	NO	NO
ACK Scan	-sA	YES	YES	NO
Window Scan	-sW	YES	YES	NO
RPC Scan	-sR	NO	NO	NO
List Scan	-sL	NO	NO	NO
Idlescan	-sI	YES	YES	NO
FTP Bounce Attack	-b	NO	YES	NO