Proyecto 3

Christofer Fabián Chávez Carazas
Universidad Nacional de San Agustín
Seguridad Computacional

11 de julio de 2017

1. Parte 1

En esta parte nos pide escanear el servidor scanme.nmap.org en busca de varias propiedades y puertos abiertos dentro de la página. Se pide responder a las siguientes preguntas:

1. **Comando completo:**
   sudo nmap -sS -A -r -d -d -T4 scanme.nmap.org > log
2. **IP del sitio escaneado:**
   45.33.32.156
3. **Sistema Operativo del servidor:**
   Linux 3.8 (86 %), Linux 3.11 - 4.1 (85 %)
4. **Puertos abiertos:**

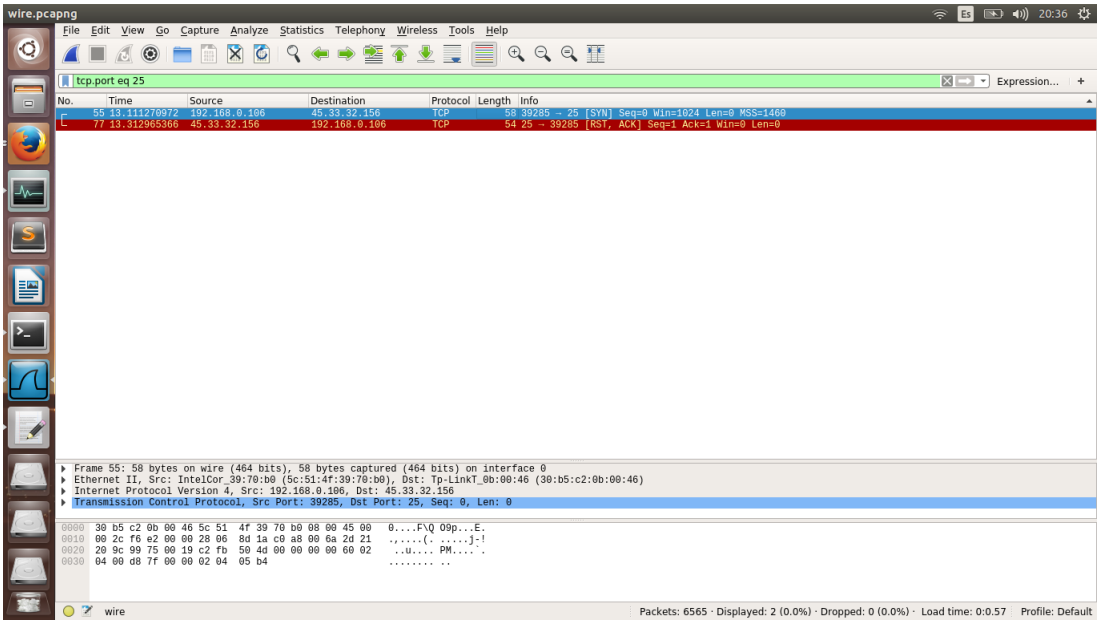
```
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 ac:00:a0:1a:82:ff:cc:55:99:dc:67:2b:34:97:6b:75 (DSA)
|   2048 20:3d:2d:44:62:2a:b0:5a:9d:b5:b3:05:14:c2:a6:b2 (RSA)
|_  256 96:02:bb:5e:57:54:1c:4e:45:2f:56:4c:4a:24:b2:57 (ECDSA)
80/tcp    open  http       Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Go ahead and ScanMe!
31337/tcp open  tcpwrapped
```

5. **Versión del SSH:**
   OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
6. **Versión del servidor:**
   Apache httpd 2.4.7

2. Parte 2

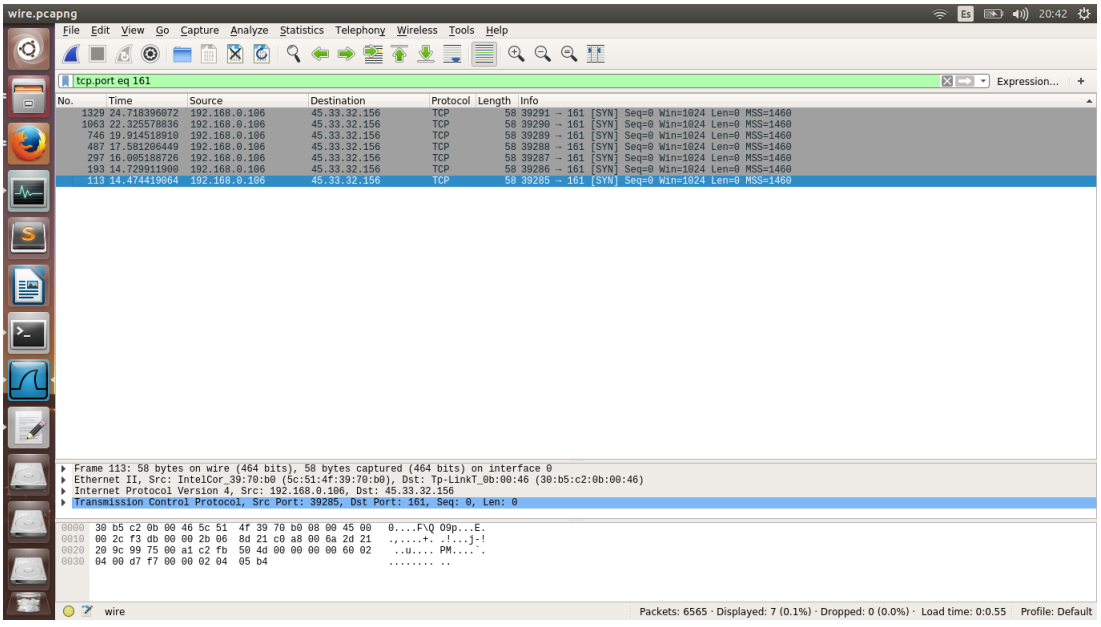
En esta parte se nos pide hacer un monitoreo del tráfico del comando nmap con Wireshark. Se pide contestar las siguientes preguntas:

1. **Que significa que un puerto esté cerrado:**



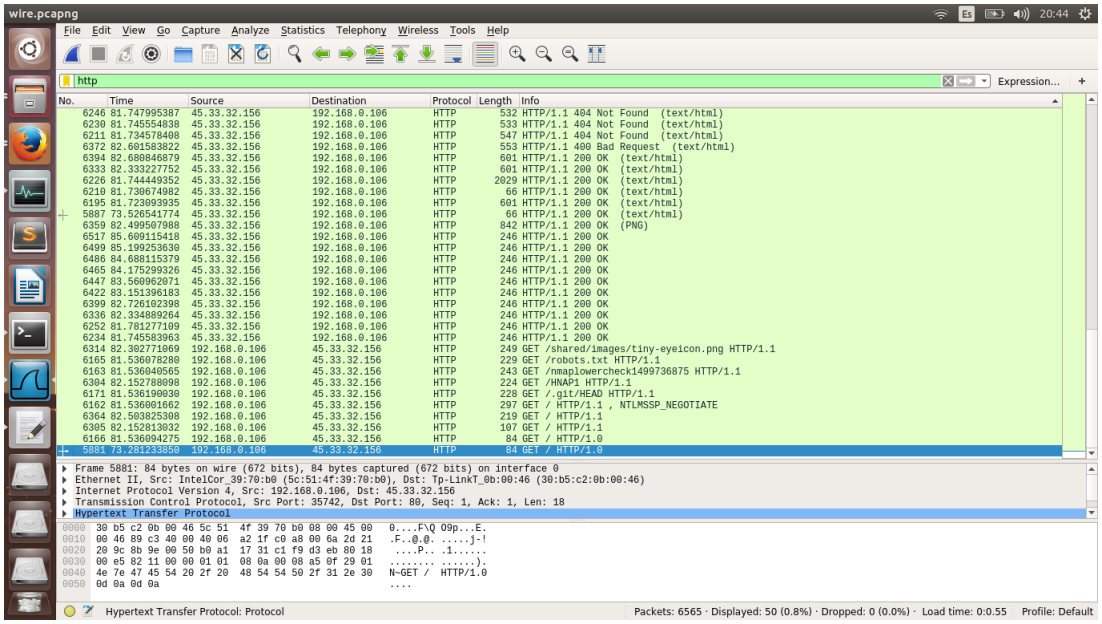
En la figura se muestra el paquete de envio y el paquete de retorno en color rojo. El paquete de retorno es del tipo [RST,ACK]

2. **Que significa que un puerto esté filtrado:**

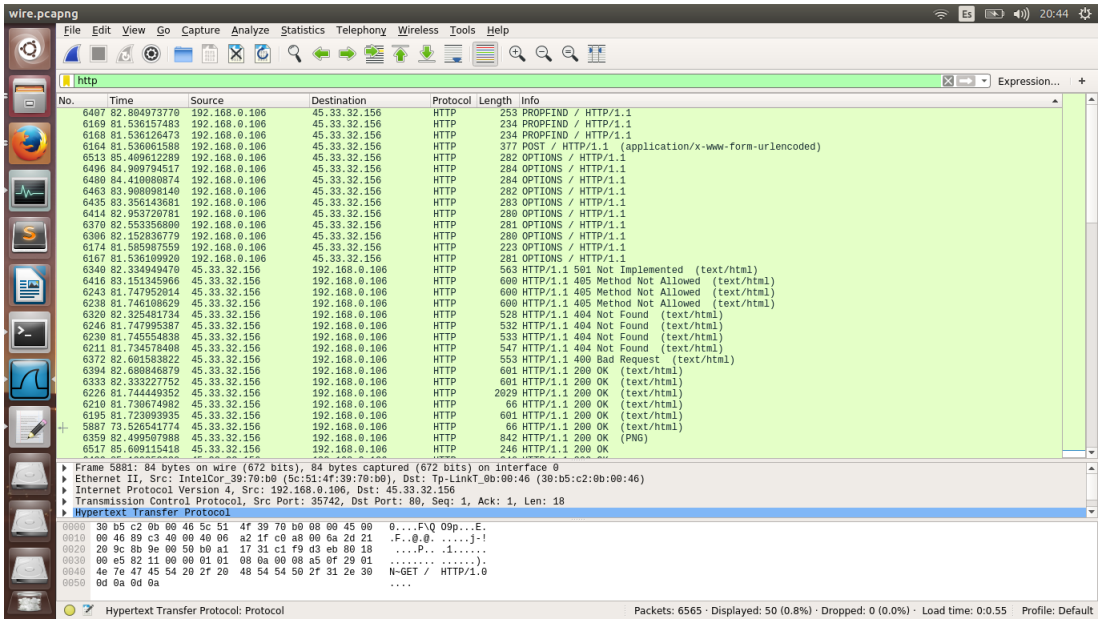


En la figura se muestran varios paquetes de envio, pero ninguno de regreso.

3. **Además del HTTP GET, que otras peticiones http envía nmap:**



En la figura se muestra las peticiones GET



En la figura se muestra las peticiones PROPFIND, POST y OPTIONS.

3. Parte 3

En esta parte se nos pide revisar un archivo con información de paquetes de una red. Se pide encontrar lo siguiente:

- **5 direcciones IP de páginas web a las cuales haya entrado el dispositivo 10.30.22.101**
  grep '10.30.22.101.*80:' trace.txt
  23.74.61.15
  184.25.56.67
  74.125.239.103
  66.235.138.194
  17.178.96.59.80

- **Encontrar la IP de destino y fuente de un escaneo de puertos, e indicar el rango**
  grep '[0-9]*[0-9]*[0-9]*[0-9]*161 > ' trace.txt
  Destino: 10.30.5.234.161
  Fuente: 10.30.1.65.55483
  Rango: 1 - 65389

- **Encontrar la IP de destino y fuente de un ataque DoS, e indicar cuántos paquetes han sido enviados**
  grep 'Flags [S].* length 0' trace.txt
  10.30.12.152
  10.30.17.255
  grep '10.30.12.152.[0-9]* > 10.30.17.255.80: Flags [S].* length 0' trace.txt — wc -l
  26076