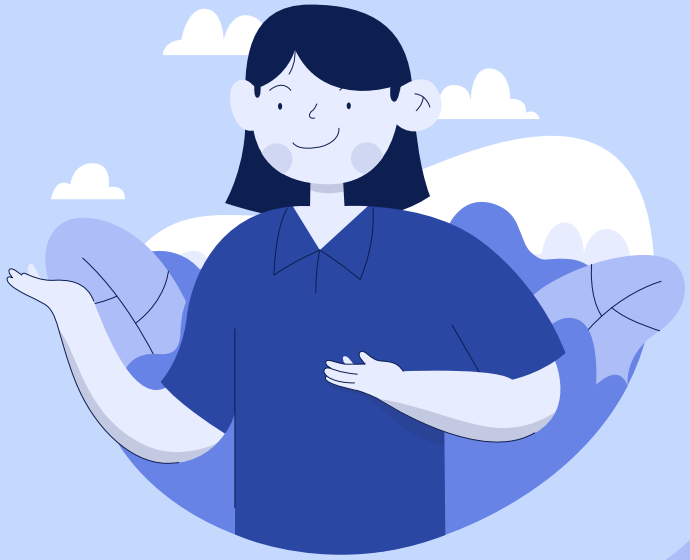
# Auxiliatura de LAB-273

Heidy Soliz Santos



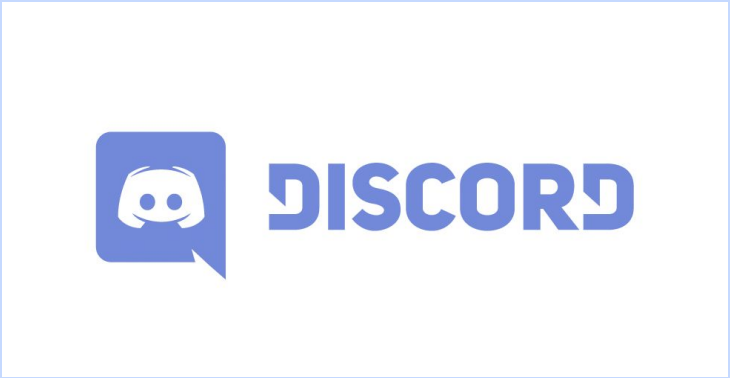
# Calificación

| | |
|---|---|
| **Modulo 1** | 2,5 |
| **Modulo 2** | 2,5 |
| **Modulo 3** | 2,5 |
| **Modulo 4** | 2,5 |
| **Total** | 10 |

# Participacion en clases

Grupos de 3 a 4 personas

# Plataforma Tecnológica a usar




# Horario

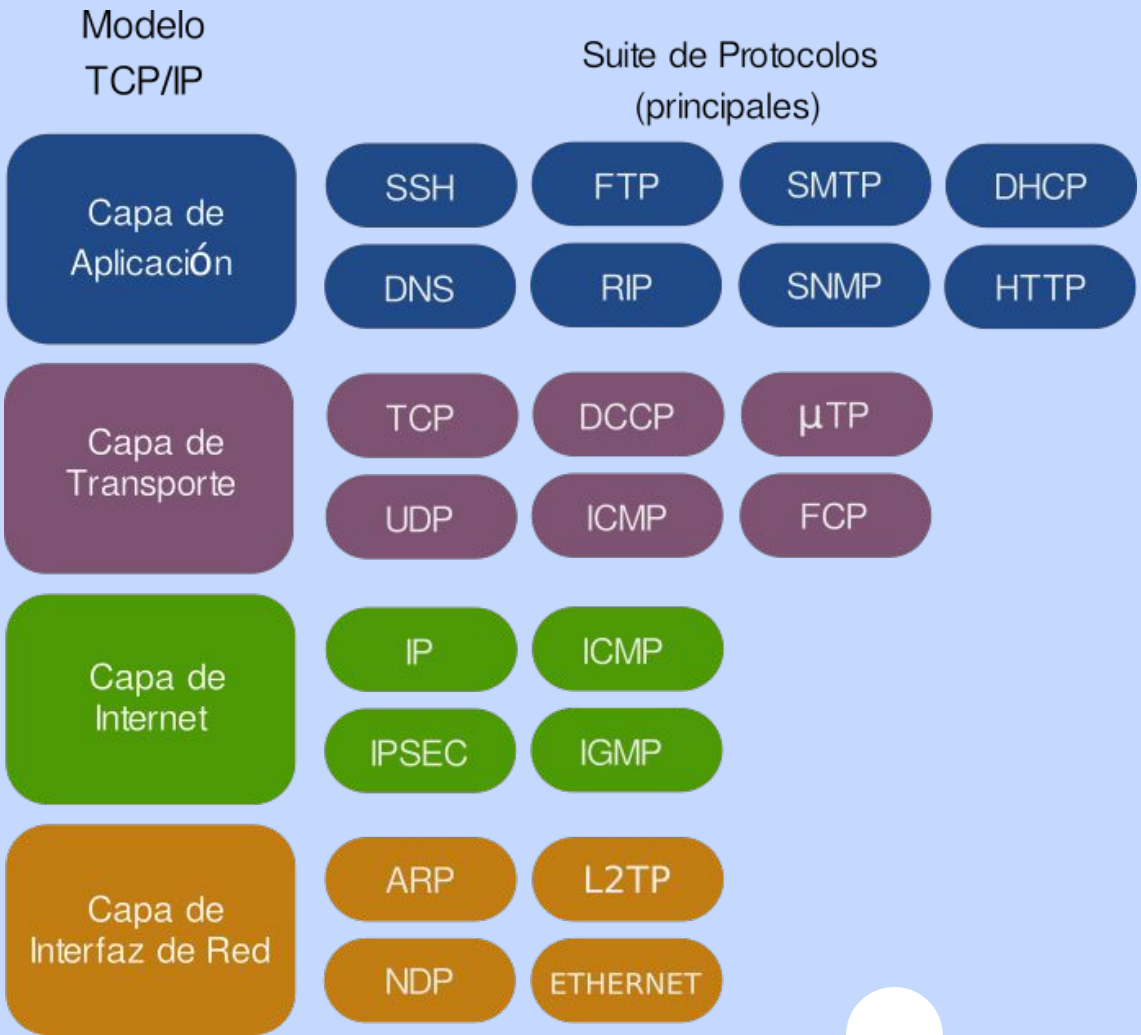
| |
|---|
| Sábados 18:00-20:00 |
| Sábados 10:00- 12:00 |
| Viernes 20:00- 22:00 |

# Instalación de Wireshark

```
sudo add-apt-repository ppa:wireshark-dev/stable
```

```
sudo apt-get update
```

```
sudo apt-get install wireshark
```


Modelo TCP/IP
Suite de Protocolos (principales)
Capa de Aplicación
SSH
FTP
SMTP
DHCP
DNS
RIP
SNMP
HTTP
Capa de Transporte
TCP
DCCP
µTP
UDP
ICMP
FCP
Capa de Internet
IP
ICMP
IPSEC
IGMP
Capa de Interfaz de Red
ARP
L2TP
NDP
ETHERNET

# FILTRADO DE WIRESHARK

- Podemos especificar el protocolo, por ejemplo:
  - ✓ tcp
  - ✓ ip
  - ✓ arp
  - ✓ icmp
- Podemos especificar un puerto o rango de puertos
  - ✓ tcp.port==53
  - ✓ tcp.port==80
  - ✓ tcp.port==25
  - ✓ tcp.port > 1025 and tcp.port < 2050
  - ✓ tcp.port > 2000 and tcp.port < 30000
- Podemos especificar un equipo o una red
  - ✓ ip.addr==192.168.130.111
  - ✓ ip.addr==192.168.130.0/24
- Podemos especificar una fuente o un destino (ip o tcp o udp)
  - ✓ ip.src==192.168.130.111
  - ✓ ip.dst==200.3.192.20
  - ✓ tcp.srcport==2024
  - ✓ tcp.srcport>1024 && tcp.srcport<65535
  - ✓ http
  - ✓ tcp.dstport==80

# Zenmap

sudo apt-get update

sudo apt-get install zenmap nmap

sudo zenmap

# Reto

1. Mostrar el puerto de origen y el puerto de destino de un paquete tcp
2. Crear un perfil que rastree el puerto 43 con destino a la ip 8.8.8.8