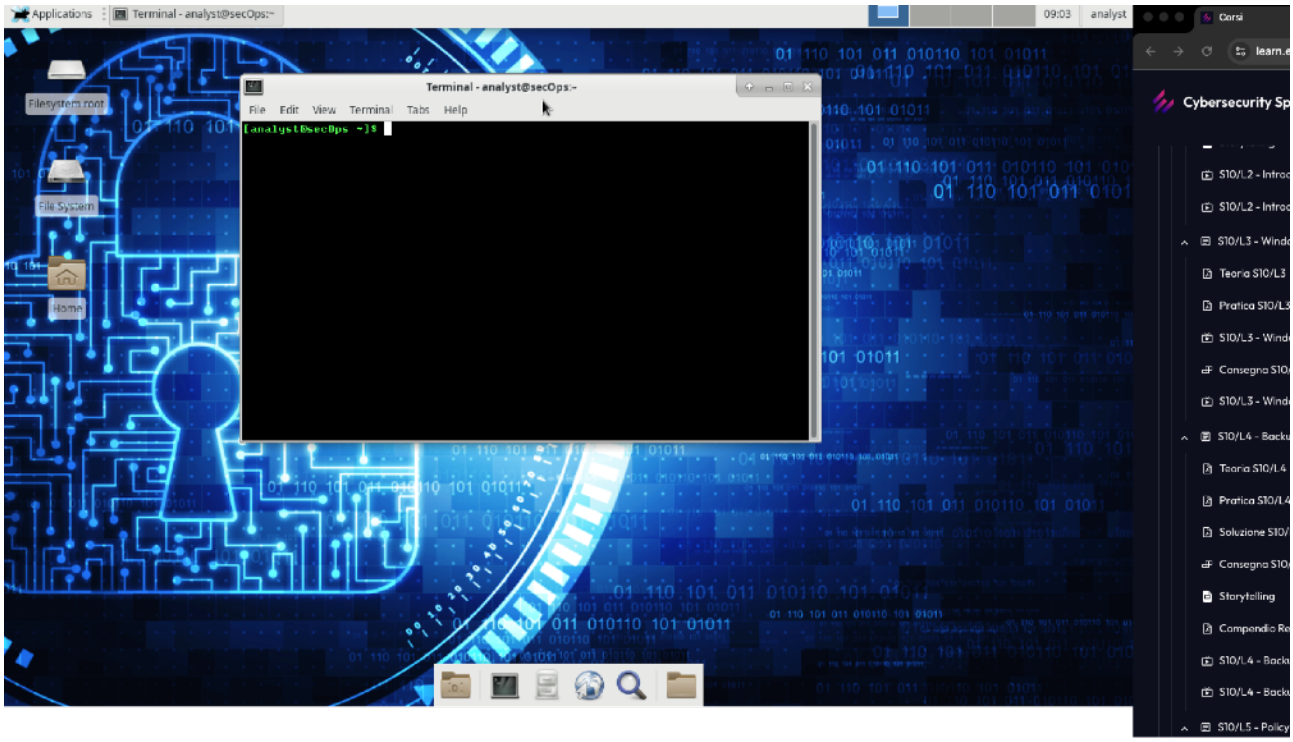
S11L2

Obiettivi
- Parte 1 Preparare gli Host per Catturare il Traffico
- Parte 2 Analizzare i Pacchetti usando Wireshark
- Parte 3 Visualizzare i Pacchetti usando tcpdump

Step1.

Avvio la macchina ed apro il terminale



Inserisco questo Codie “sudo lab.support.files/scripts/cyberops_topo.py” ed si avvia il CLI

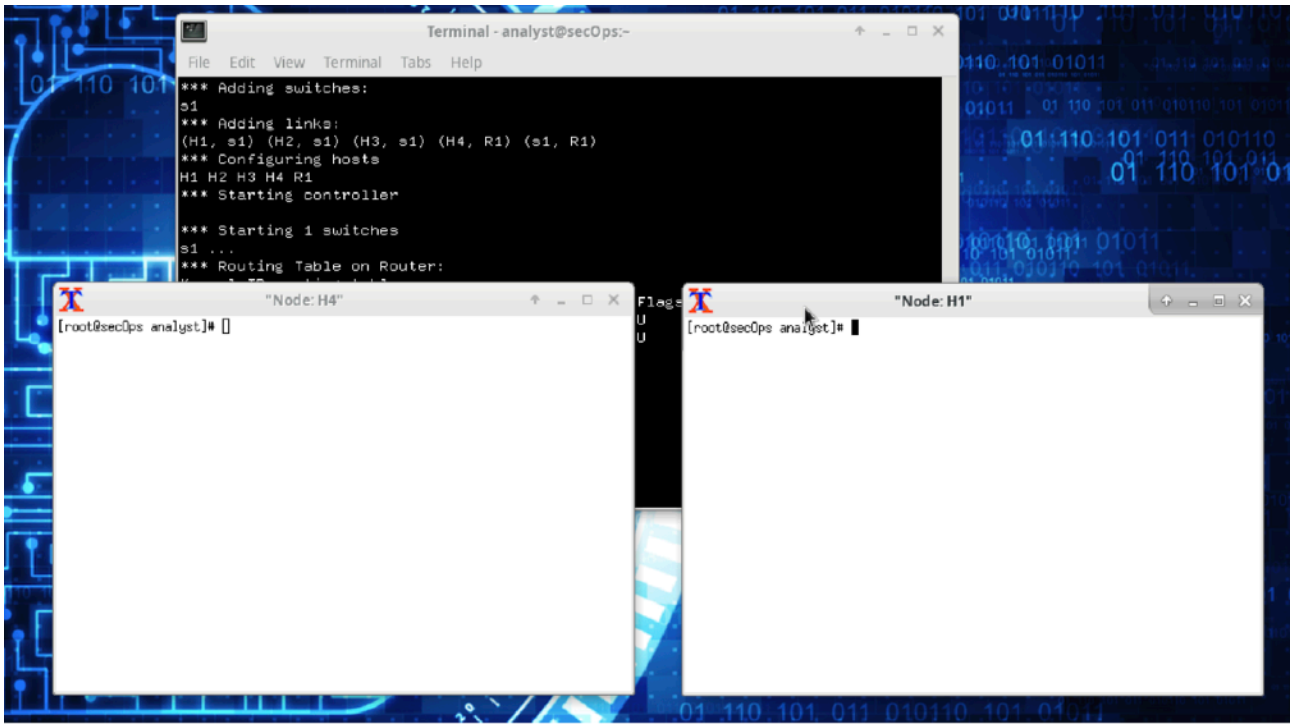
```
------    ------    ------

*** Add links
*** Creating network
*** Adding hosts:
H1 H2 H3 H4 R1
*** Adding switches:
s1
*** Adding links:
(H1, s1) (H2, s1) (H3, s1) (H4, R1) (s1, R1)
*** Configuring hosts
H1 H2 H3 H4 R1
*** Starting controller

*** Starting 1 switches
s1 ...
*** Routing Table on Router:
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
10.0.0.0        0.0.0.0         255.255.255.0   U     0      0        0 R1-eth1
172.16.0.0      0.0.0.0         255.240.0.0     U     0      0        0 R1-eth2

*** Starting CLI:
mininet>
```

Ora con i comandi xterm H1 e xterm H4 apro le altre due pagine



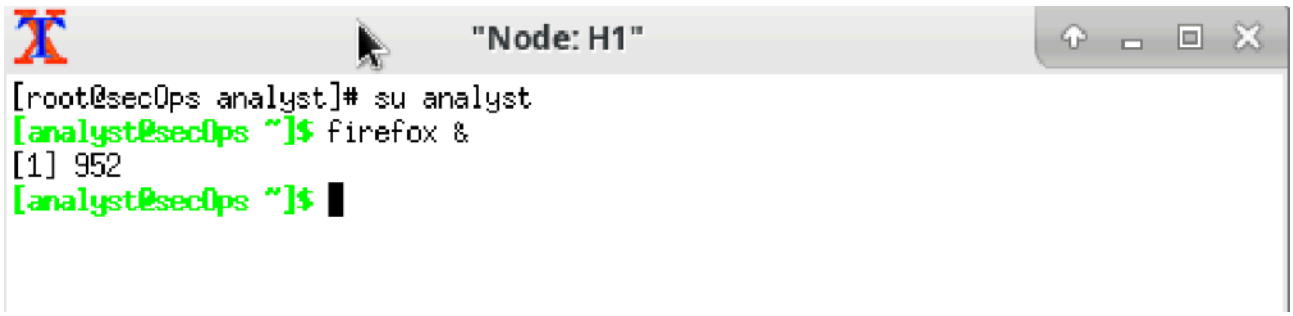
Su H4 inserisco /home/analyst/lab.support.files/scripts/reg_server_start.sh

---

`reg_server`: Si riferisce a un "registry server" (server di registro). Un registry server è un'applicazione che gestisce e memorizza i log, ovvero eventi registrati da altri sistemi, applicazioni o dispositivi.

`start`: Indica che la sua funzione è quella di avviare il servizio.

Su H1 invece inserisco il comando “su analyst” per cambiare utente per poi poter avviare firefox con “firefox &”



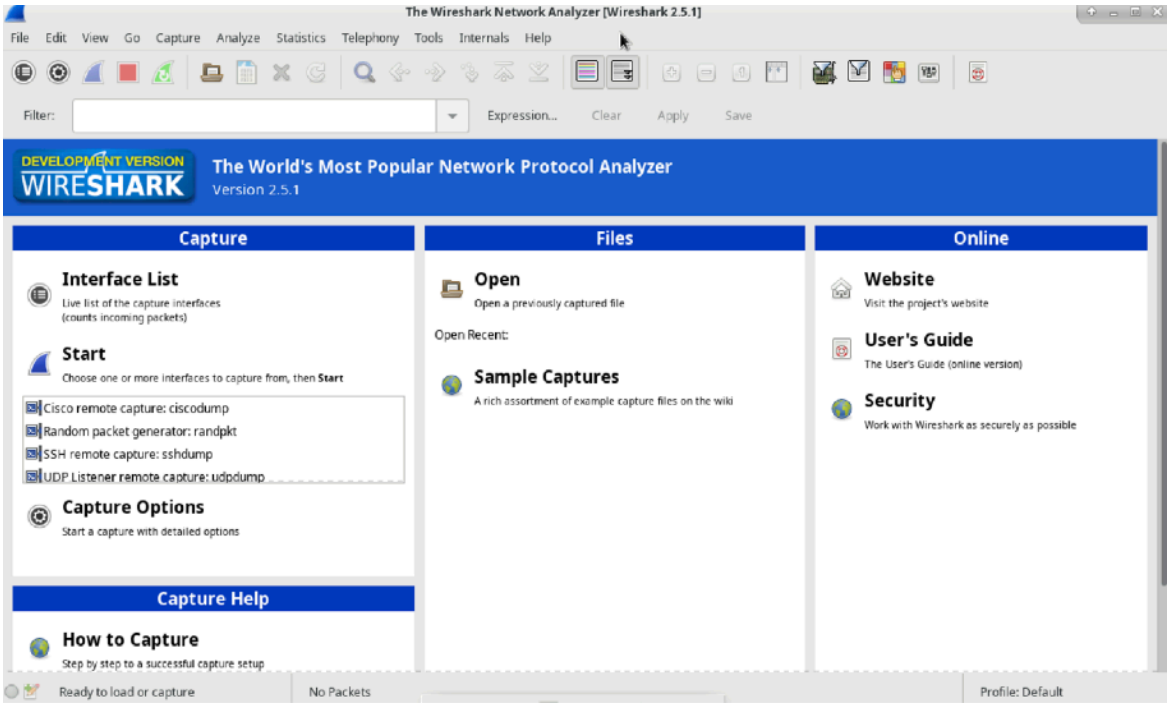
Ora inserisco il comando sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.pcap

```
[analyst@secOps ~]$ sudo tcpdump -i H1-eth0 -v -c 50 -w /home/analyst/capture.p
cap
[sudo] password for analyst:
tcpdump: listening on H1-eth0, link-type EN10MB (Ethernet), capture size 262144
bytes
Got 11
```

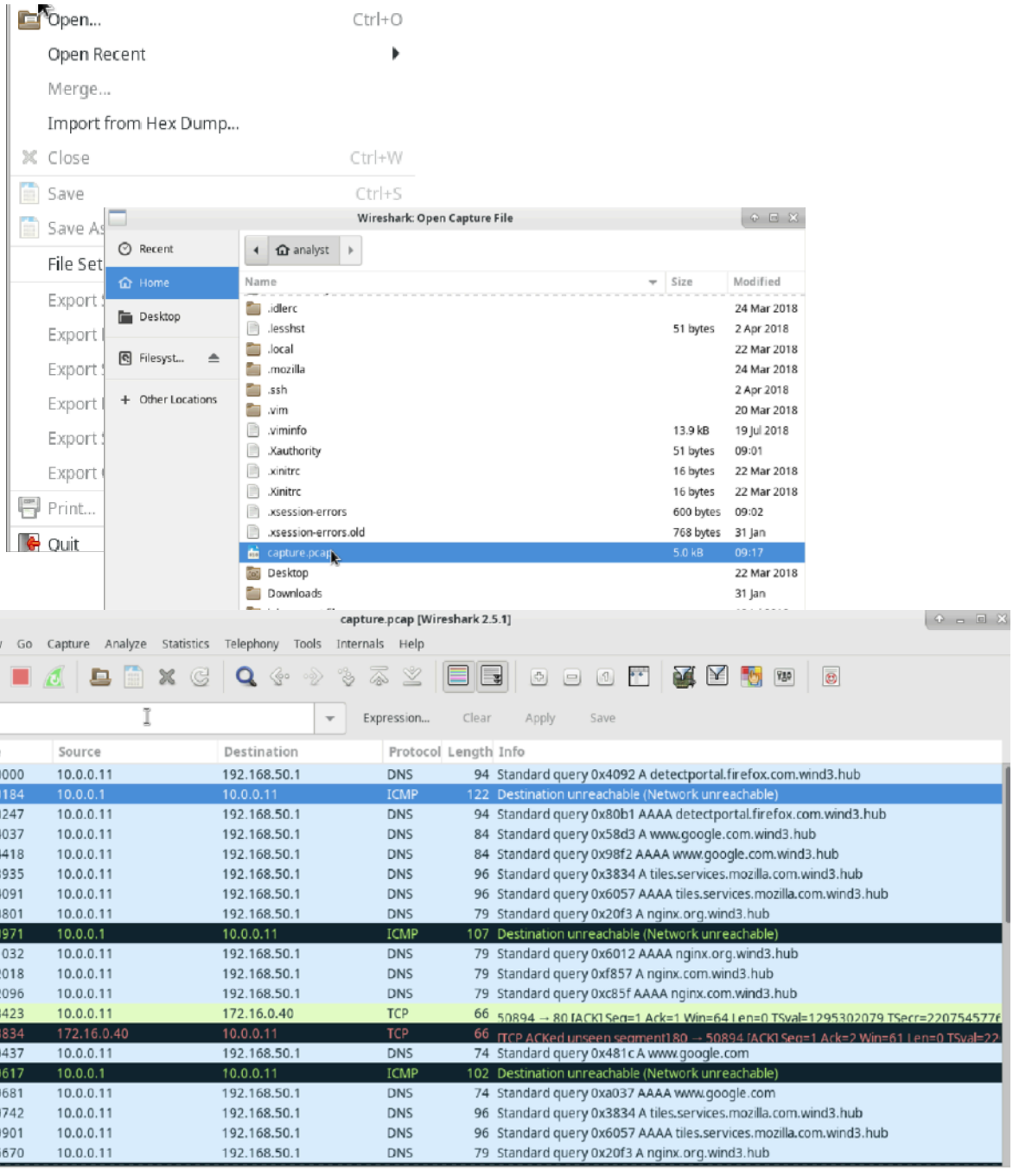
Dopo di che su firefox vado sul ip del H4 ovvero 172.16.0.40

Step2. Wireshark

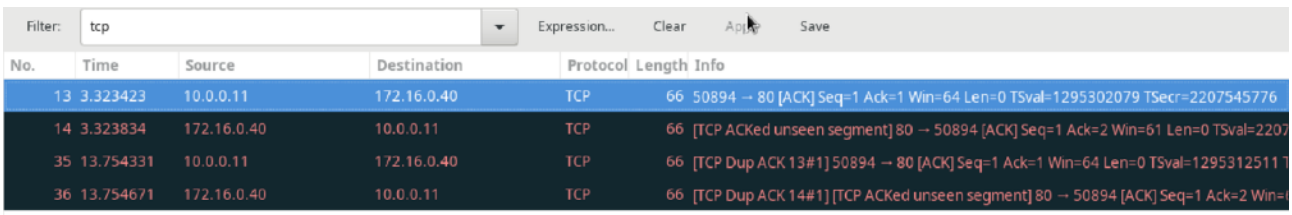
Su H1 avvio Wireshark con il comando “Wireshark-gtk &”



Ora vado su File > Open e selezione il file salvato



In fine applico il filtro tcp



Step3. Domande

Primo pacchetto:

1. Qual è il numero di porta TCP di origine?
   50894
2. Come classificheresti la porta di origine?
   Dynamic/Private/Ephemeral Ports (49152-65535)
3. Qual è il numero di porta TCP di destinazione?
   80
4. Come classificheresti la porta di destinazione?
   well-known (0-1023)
5. Quale flag è impostato?
   ACK
6. A quale valore è impostato il numero di sequenza relativo?
   1

Secondo pacchetto:

1. Quali sono i valori delle porte di origine e destinazione?
   80 origine 50894 destinazione
2. Quali flag sono impostati?
   ACK
3. A quali valori sono impostati i numeri relativi di sequenza e acknowledgment?
   SEQ=1 ACK=2

Terzo pacchetto:

1. Quale flag è impostato?
   ACK

Step4. Tcpdump

Cosa fa l'opzione -r?
Legge i pacchetti del file

Step5. Domande di riflessione

1.Ci sono centinaia di filtri disponibili in Wireshark. Una rete di grandi dimensioni potrebbe avere numerosi filtri e molti tipi diversi di traffico. Elenca tre filtri che potrebbero essere utili a un amministratore di rete.

1. Filtro per Indirizzo IP

`ip.addr == 192.168.1.10` (per vedere tutto il traffico che coinvolge 192.168.1.10)

`ip.src == 192.168.1.10` (per vedere solo il traffico in uscita)

`ip.dst == 192.168.1.10` (per vedere solo il traffico in entrata)

2. Filtro per Porta TCP/UDP

tcp.port == 80 (per visualizzare il traffico HTTP)
udp.port == 53 (per visualizzare le query DNS)
tcp.port == 22 or tcp.port == 23 (per visualizzare il traffico SSH o Telnet)

3. Filtro per Protocollo

`tcp` (visualizza solo i pacchetti TCP)

`icmp` (visualizza solo i pacchetti ICMP, spesso usati per i comandi ping)

`arp` (visualizza i pacchetti ARP per la risoluzione degli indirizzi IP in indirizzi MAC)

2.In quali altri modi Wireshark potrebbe essere utilizzato in una rete di produzione?

1. Risoluzione dei problemi di connettività

Wireshark permette di diagnosticare perché due host non riescono a comunicare. Analizzando i pacchetti, si possono identificare errori comuni come il mancato "three-way handshake" TCP, pacchetti ICMP che indicano che un host è irraggiungibile (`host unreachable`), o problemi di risoluzione DNS.

2. Analisi delle prestazioni

Gli amministratori di rete usano Wireshark per individuare i colli di bottiglia e le cause del rallentamento della rete. È possibile monitorare i tempi di risposta (RTT - Round-Trip Time), identificare pacchetti ritrasmessi che indicano problemi di congestione o perdita di pacchetti e analizzare il traffico generato da applicazioni specifiche per capire se consumano troppa banda.

3. Sicurezza e sorveglianza

Wireshark è un tool essenziale per la sicurezza. Può essere usato per:

- **Rilevare accessi non autorizzati:** Monitorando le connessioni e i tentativi di accesso a servizi sensibili.
- **Identificare attacchi:** Riconoscere schemi di traffico anomali che potrebbero indicare scansioni di porte, attacchi DoS (Denial of Service) o il tentativo di esfiltrazione di dati.
- **Analizzare malware:** Studiare il comportamento di un malware in un ambiente controllato, analizzando il traffico di rete che genera per comunicare con server C&C (Command and Control) o per diffondersi.

4. Debug di applicazioni e protocolli

Gli sviluppatori e gli ingegneri di rete usano Wireshark per il debug di nuove applicazioni e servizi. Permette di verificare che un'applicazione stia usando i protocolli e le porte corrette e che i dati siano formattati come previsto. È anche utile per comprendere a fondo il funzionamento interno dei protocolli di rete.