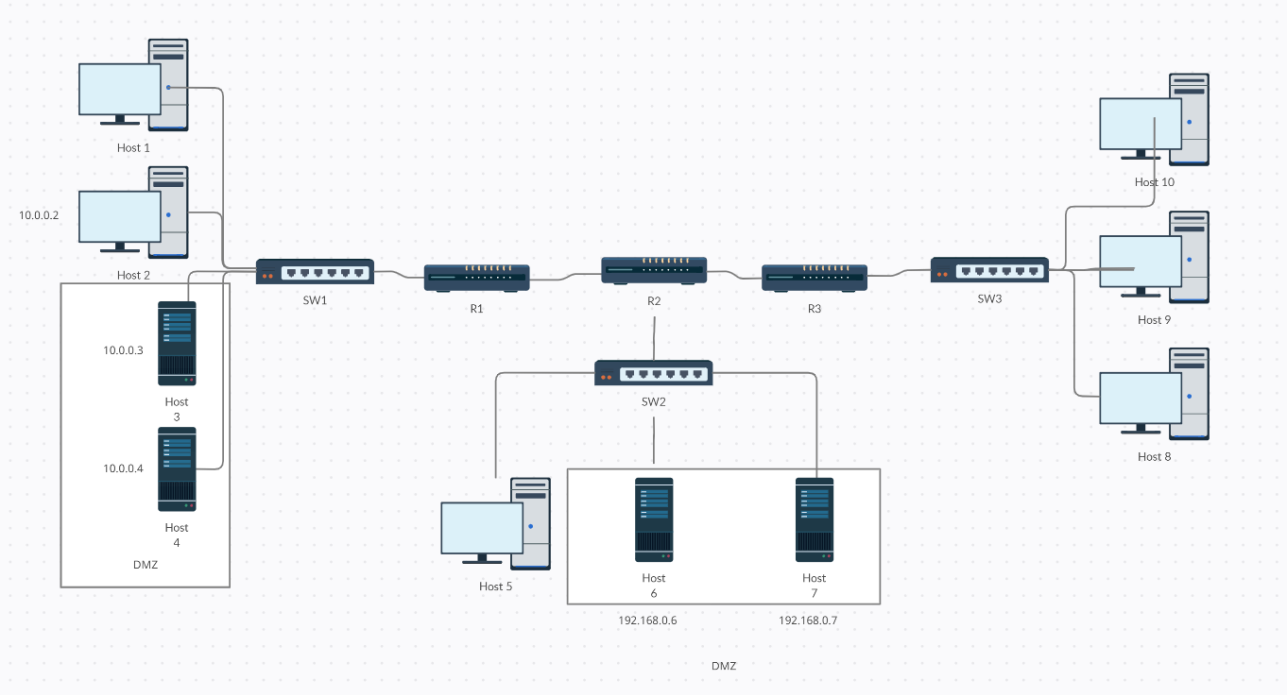
GRUPPO A – Progetto Cybersecurity

Sia data la seguente topologia di rete:



Implementare l'architettura in mininet rispettando i seguenti vincoli:

1. Garantire comunicazione tra tutti i dispositivi implementando le opportune tabelle di routing sui router R1, R2 ed R3.
2. All'interno della DMZ 1, l'host H3 deve poter essere raggiungibile solo dalla rete composta dagli host H8, H9, H10 mentre l'host H4 solo dagli host H5, H6 e H7
3. Implementare un server HTTP sull'host H6 che metta a disposizione una pagina web generica
4. Aprire sull'host H7 le seguenti porte: 502, 43 e 25
5. Verificare la raggiungibilità di tutti gli host presenti in rete

Successivamente, eseguire i seguenti File python:

a. Eseguire su host H3 codice python server.py
b. Eseguire su host H2 il codice python client.py
c. Eseguire su host H1 il codice python attacco1.py
d. Eseguire su host H6 il codice python attacco2.py
e. Eseguire su host H9 il codice python attacco3.py
f. Eseguire su host H10 il codice python attacco4.py

A seguito di una analisi del traffico di rete, implementare le opportune misure di sicurezza (ids/ips/firewall).

Cosa consegnare:

1) File di configurazione della topologia di rete iniziale
2) File word con la discussione delle minacce identificate tramite analisi del traffico di rete
3) File di configurazione della nuova topologia di rete che include la soluzione identificata e descrizione della scelta su file word

NOTA: I file di attacco sono volutamente criptati. Per poter eseguire i file è necessario installare sourcedefender:
pip3 install sourcedefender