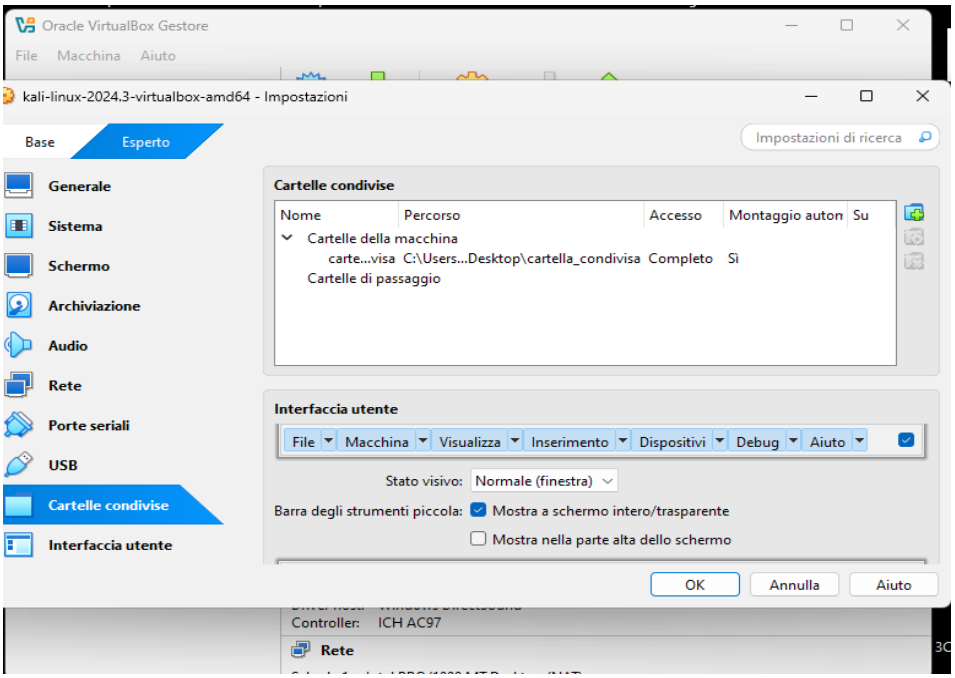
Threat Intelligence & IOC

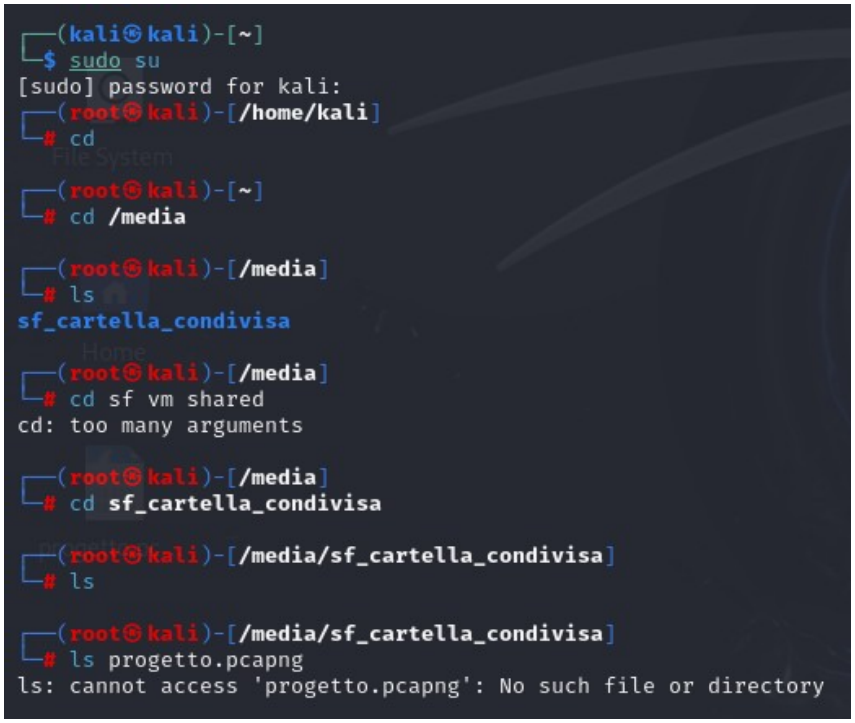
L’esercizio di oggi ci chiedeva di analizzare un file e rispondere ai seguenti quesiti:

1. Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso.
2. In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati.
3. Consigliate un’azione per ridurre gli impatti dell’attacco attuale ed eventualmente un simile attacco futuro.

Ho aperto la macchina virtuale Kali e ho condiviso una cartella in modo far visualizzare il progetto aperto precedentemente su Wireshark.



Successivamente ho aperto il root sul terminale di Kali e ho operato.



Non sono riuscito a visualizzare il progetto dentro la cartella e a continuare l’esercizio.