Pratica W19D4

Traccia:

EPICODE

Esercizio
Threat Intelligence & IOC

Traccia:

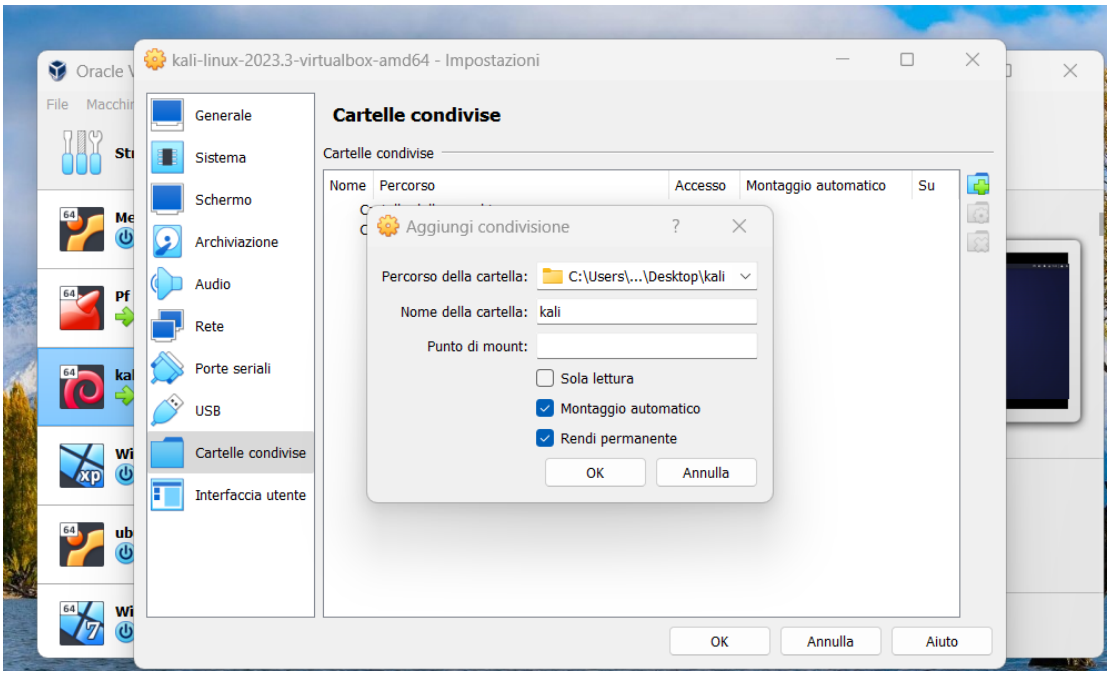
Durante la lezione teorica, abbiamo visto la **Threat Intelligence** e gli indicatori di compromissione.
Abbiamo visto che gli IOC sono evidenze o eventi di un attacco in corso, oppure già avvenuto.

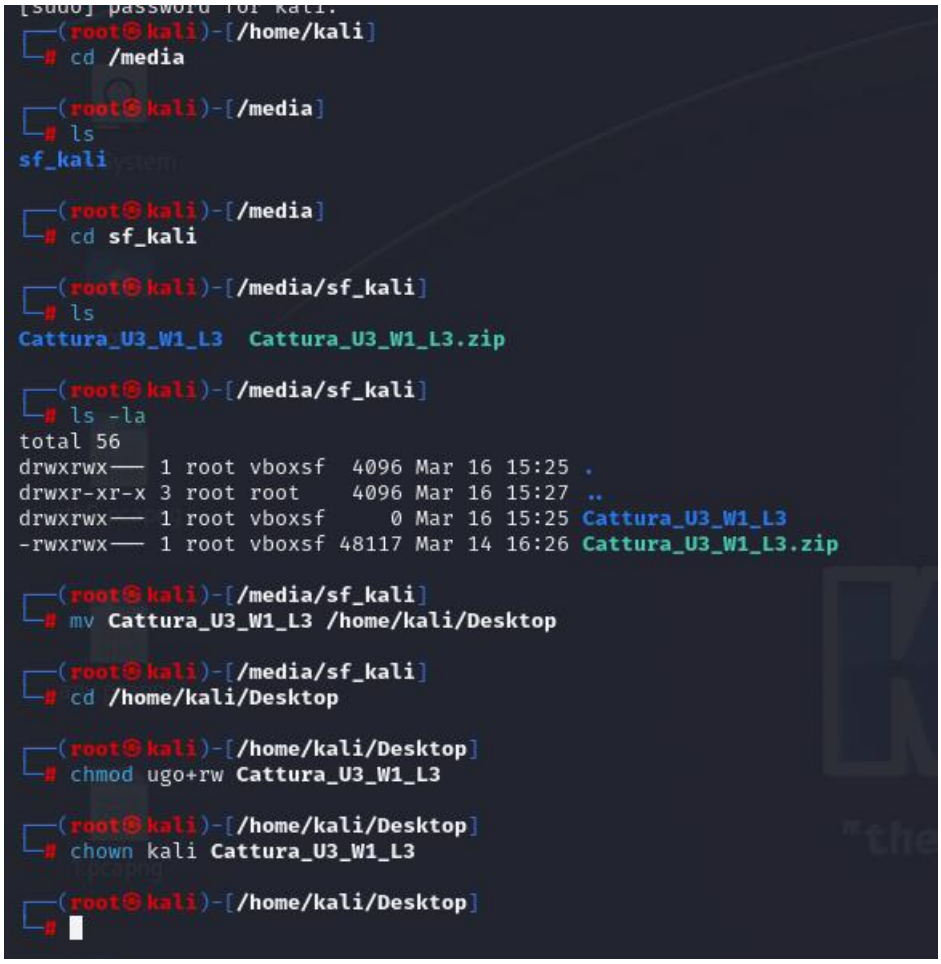
Per l'esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark.
Analizzate la cattura attentamente e rispondere ai seguenti quesiti:

- Identificare eventuali IOC, ovvero evidenze di **attacchi in corso**
- In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
- Consigliate un'azione per ridurre gli impatti dell'attacco

Cattura_U3_W1_L3.pcapng

Soluzione:





Riusciamo ad identificare un traffico di rete sospetto grazie alle numerose richieste TCP, un possibile vettore di attacco può essere una scansione sul nostro dispositivo da parte dell'IP 192.168.200.100. La possibile soluzione può essere la protezione delle porte tramite policy Firewall.