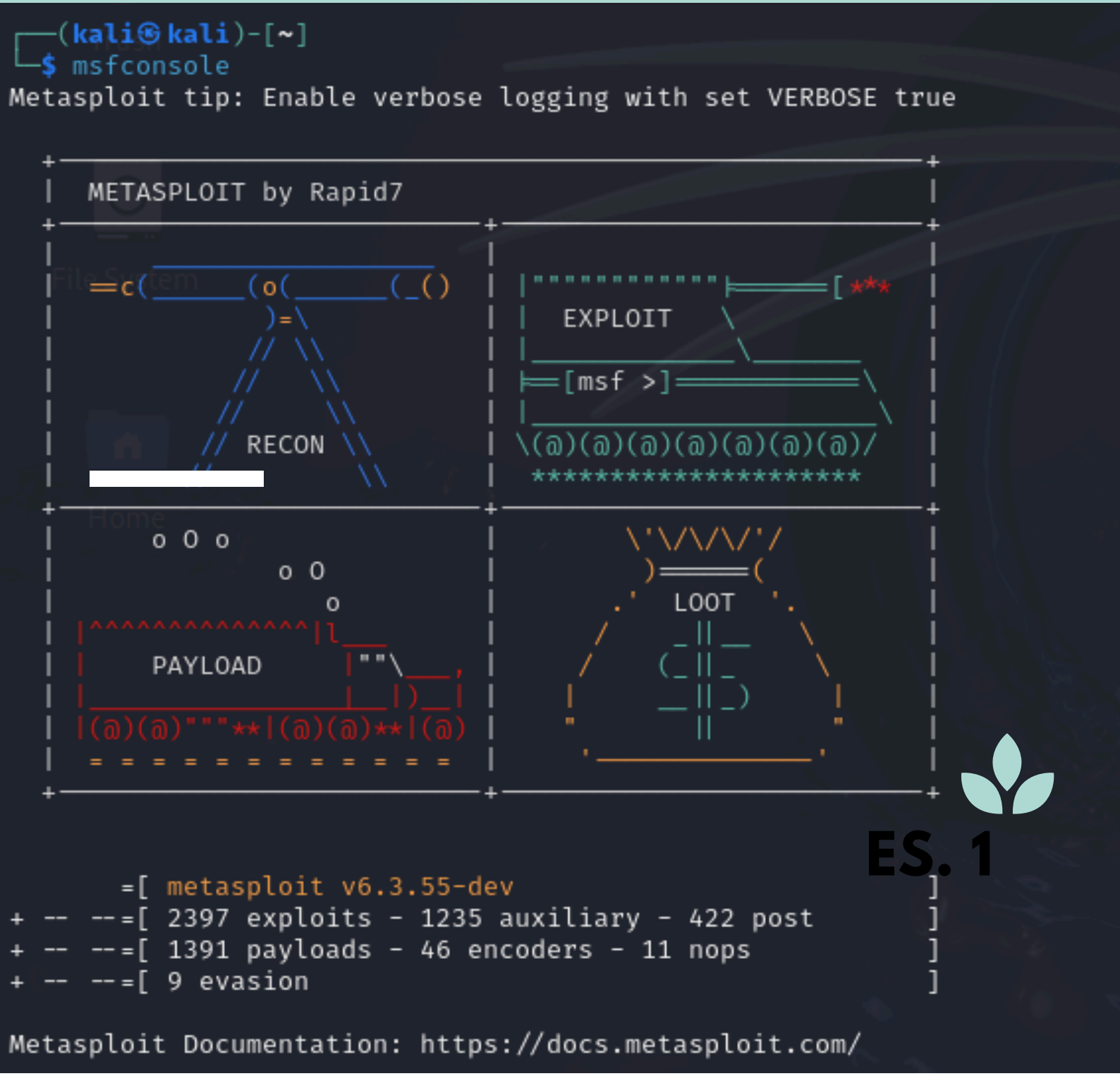
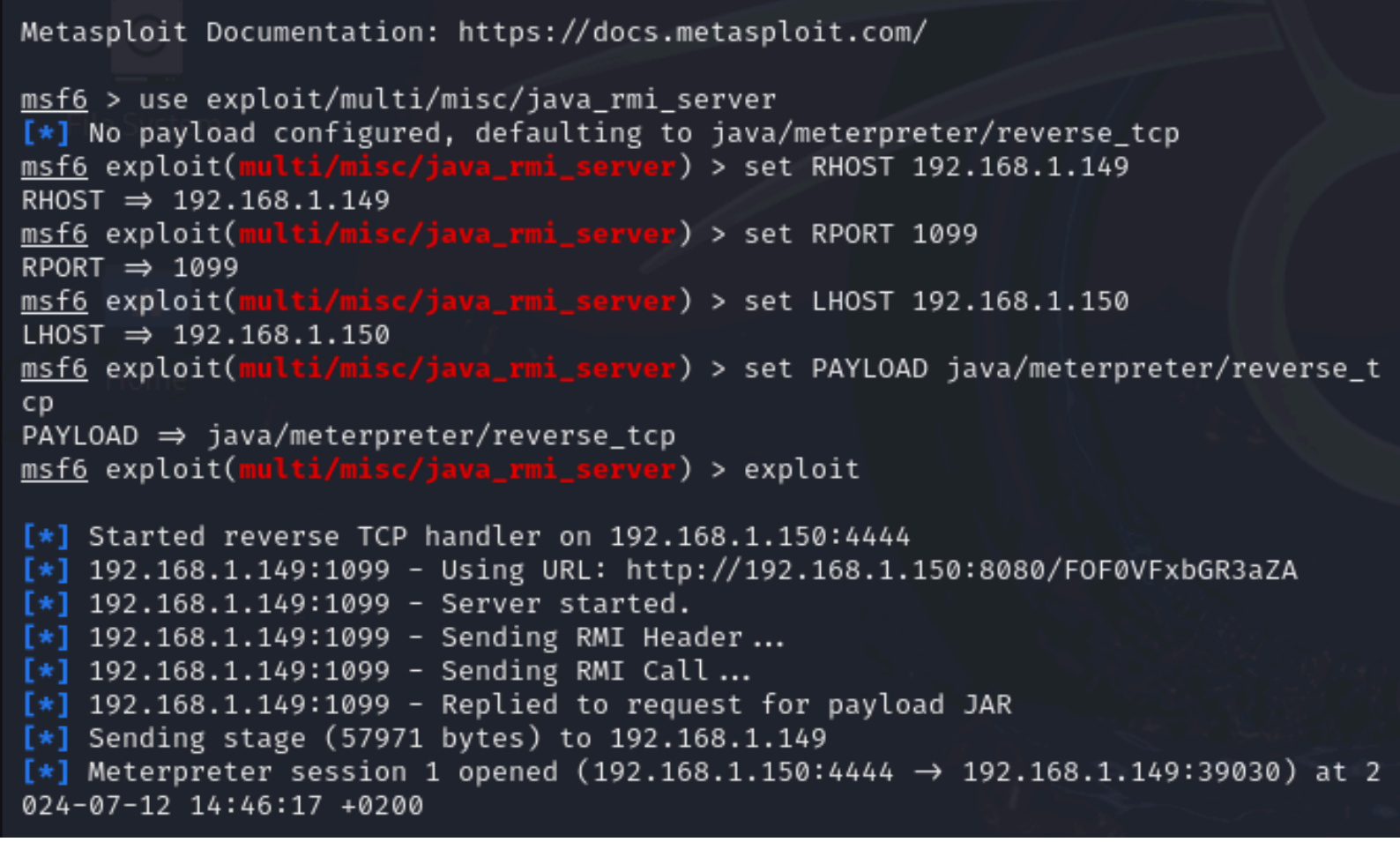
S7L5

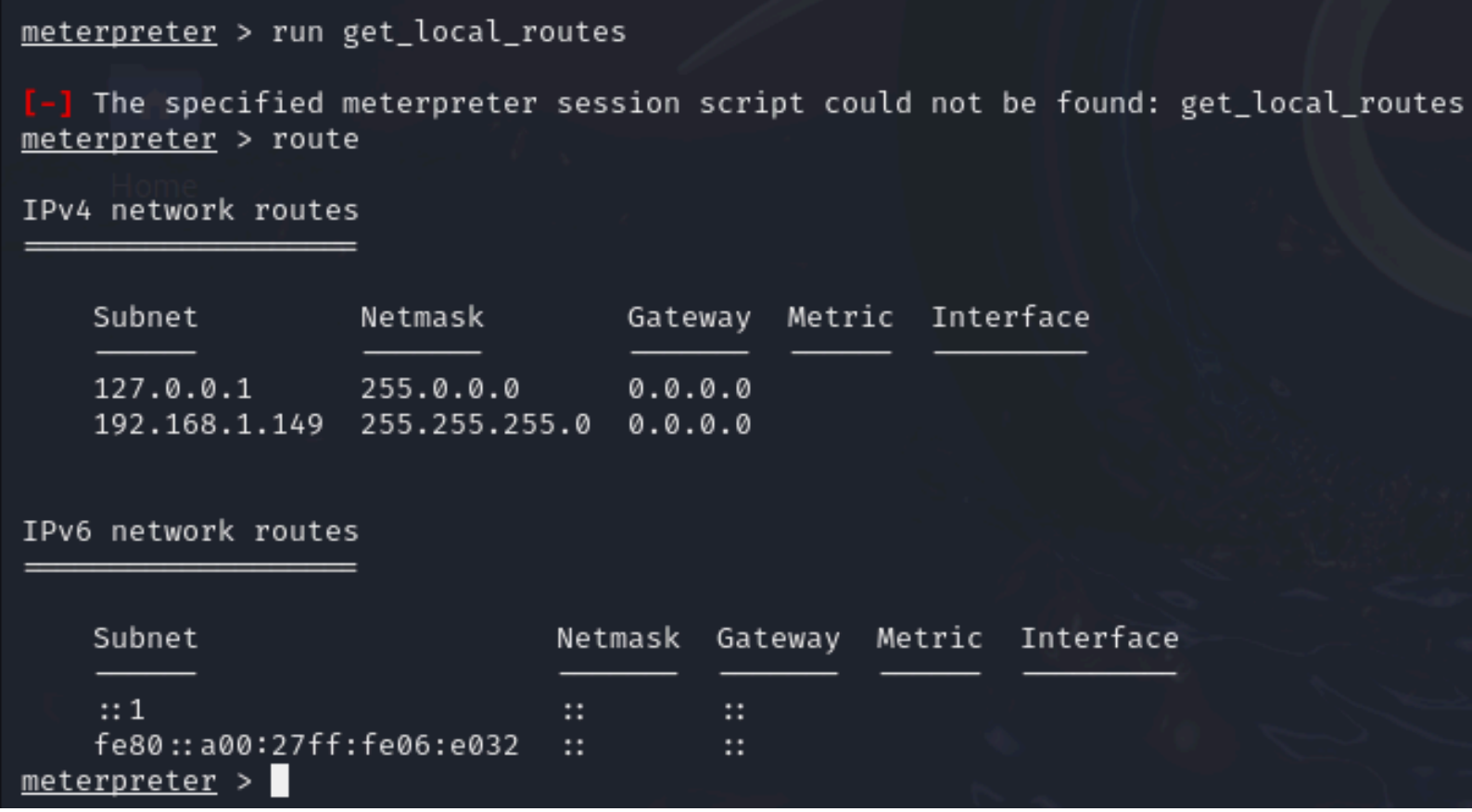
SARAH ORTIZ



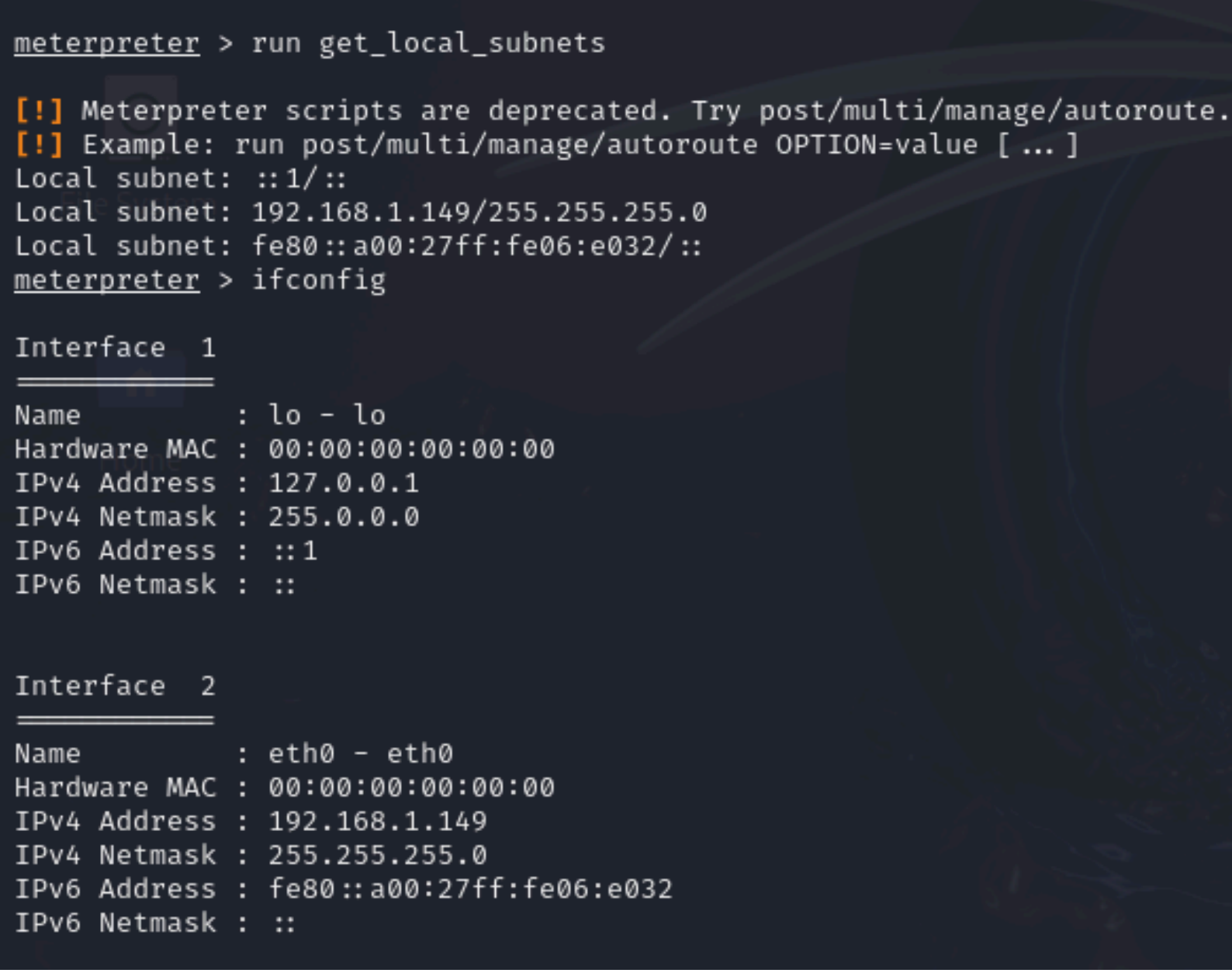


1. Utilizzeremo un modulo exploit di Metasploit per attaccare il servizio Java RMI
2. Configuriamo l'indirizzo IP di Metasploitable e KALI.
3. apriamo una sessione di Meterpreter utilizzando un payload Java

Una volta che l'exploit ha avuto successo, ottenerremo la sessione Meterpreter



Con il comando “run get_local_subnets” raccogliamo informazioni sulle sottoreti locali della macchina compromessa. Identifica tutte le interfacce di rete disponibili e raccoglie le informazioni sulle sottoreti a cui sono collegate



Con il comando “run get_local_routes” raccogliamo la tabella di routing della macchina compromessa. Fornisce una lista delle rotte di rete configurate, mostrando come il traffico di rete è instradato dalla macchina.