**Task 1.1:**

**Task 1.1 A**

**sniffer.py: Below is the python code to sniff icmp packet(print\_pkt is the callback function to be executed once the packet is sniffed)**

**#!/usr/bin/env python3**

**from scapy.all import \***

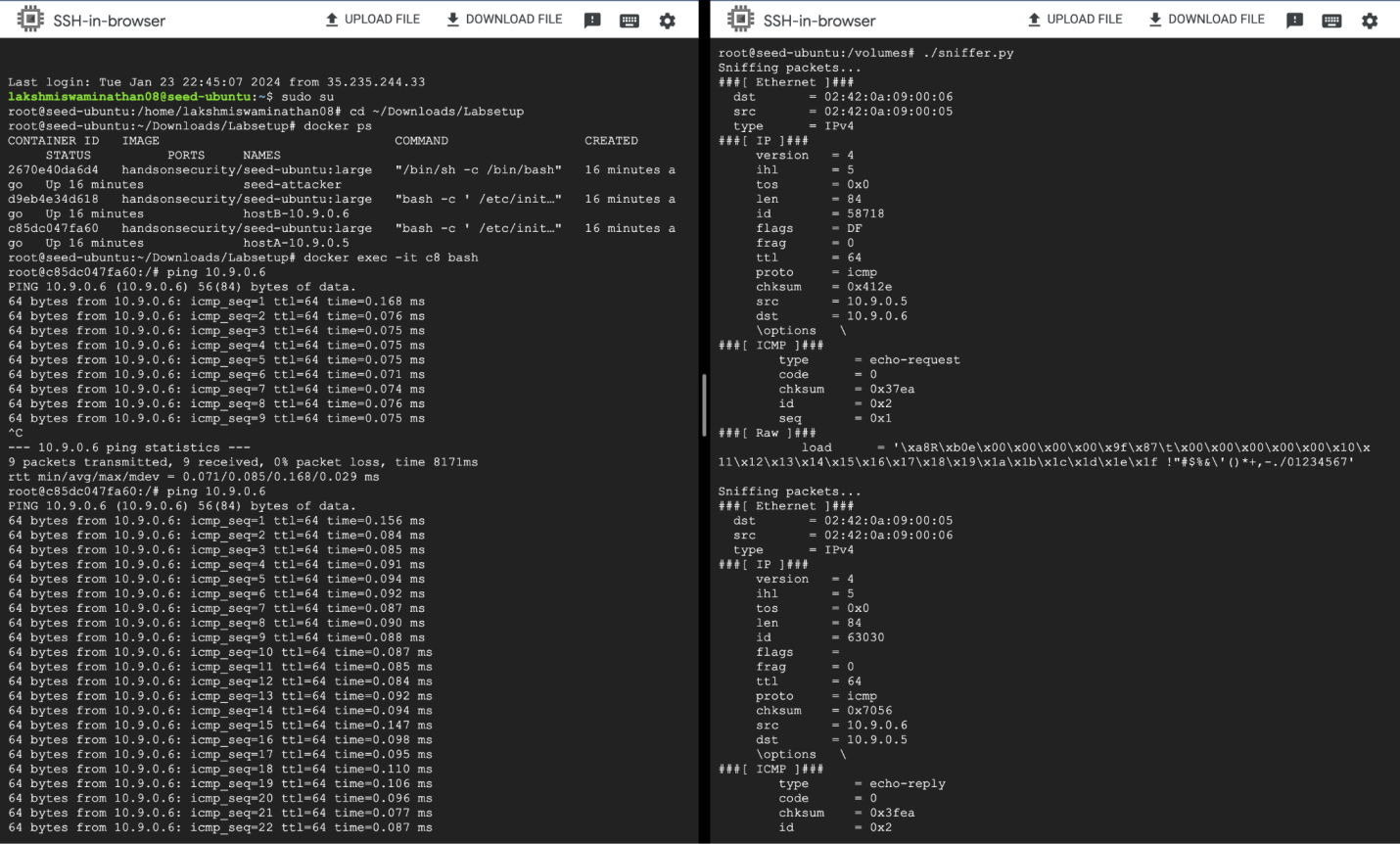
**def print\_pkt(pkt):**

**print('Sniffing packets...')**

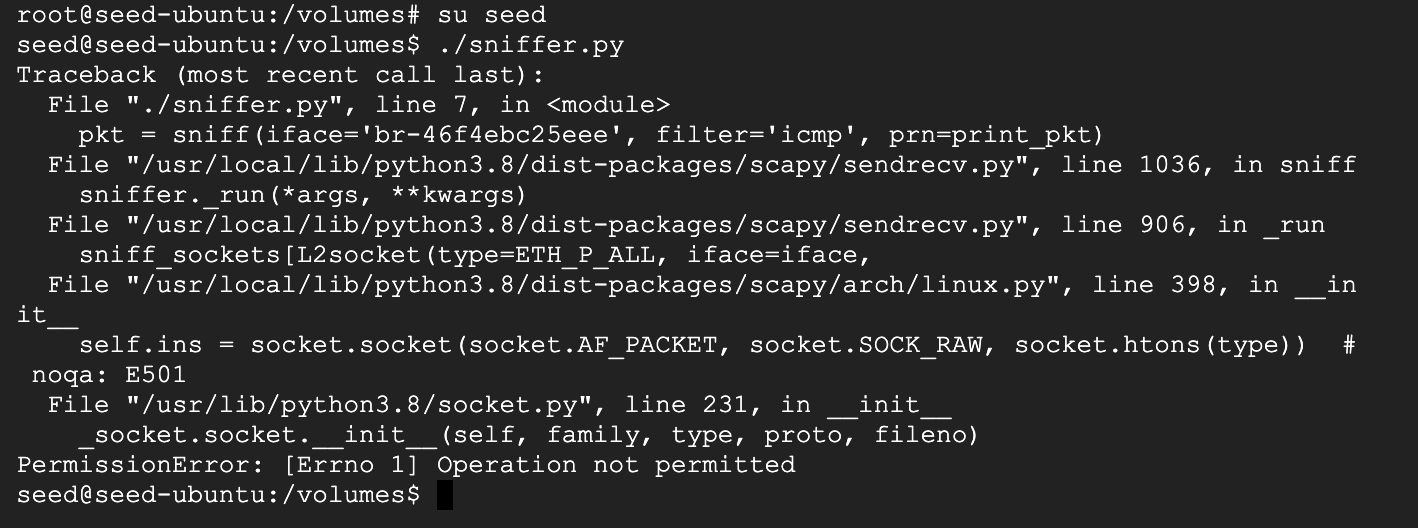
**pkt.show()**

**pkt = sniff(iface='br-46f4ebc25eee', filter='icmp', prn=print\_pkt)**

**sniffer\_execution\_with\_root\_privilege(Sniffing the icmp packet from host A)**

****

**sniffer\_execution\_without\_root\_privilege**

****

**Task 1.1 B**

**ICMP Filter: Below is the python logic to sniff icmp packet(print\_pkt is the callback function to be executed once the packet is sniffed)**

**sniffer.py**

**#!/usr/bin/env python3**

**from scapy.all import \***

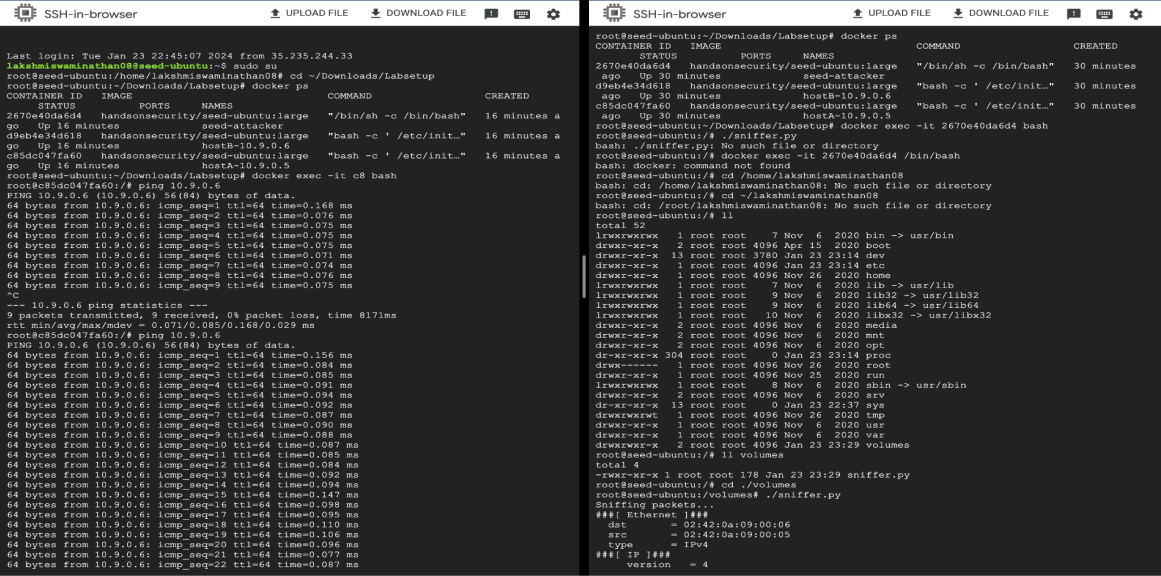
**def print\_pkt(pkt):**

**print('Sniffing packets...')**

**pkt.show()**

**pkt = sniff(iface='br-46f4ebc25eee', filter='icmp', prn=print\_pkt)**

**icmp\_filter execution:(sniffing the icmp packet from host A from attacker container)**

****

**subnet filter: Below is the python logic to sniff packets from or to go to a subnet 128.230.0.0/16(print\_pkt is the callback function to be executed once the packet is sniffed)**

**sniffer\_subnet.py**

**#!/usr/bin/env python3**

**from scapy.all import \***

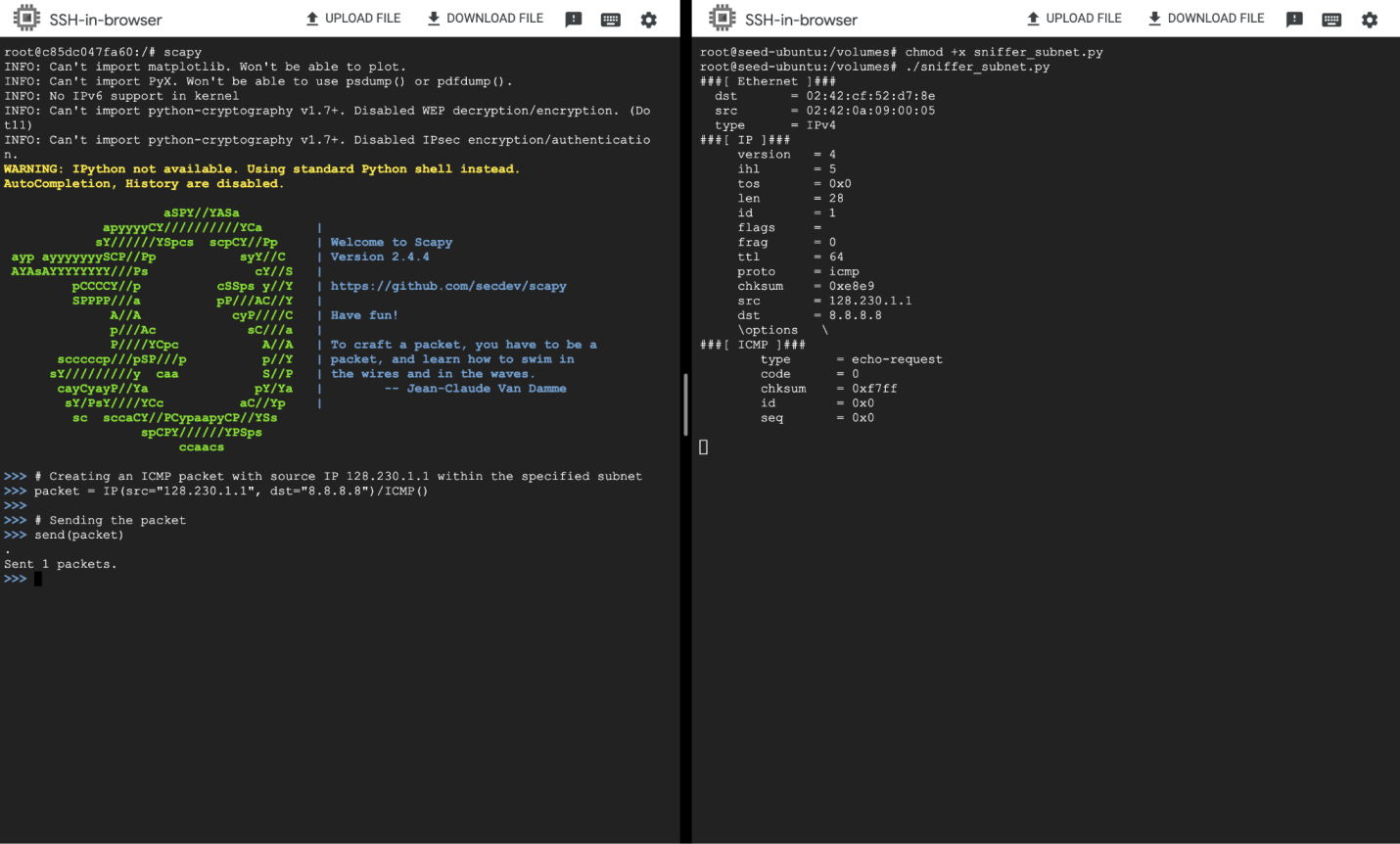
**def print\_pkt(pkt):**

**pkt.show()**

**# Capture packets from or to a particular subnet**

**pkt = sniff(iface='br-46f4ebc25eee', filter='net 128.230.0.0/16', prn=print\_pkt)**

**Subnet filter execution**

****

**TCP filter:**

**sniffer\_tcp.py: Below is the python logic to sniff tcp packets from IP-10.9.0.5 and destination port 23(print\_pkt is the callback function to be executed once the packet is sniffed)**

**#!/usr/bin/env python3**

**from scapy.all import \***

**def print\_pkt(pkt):**

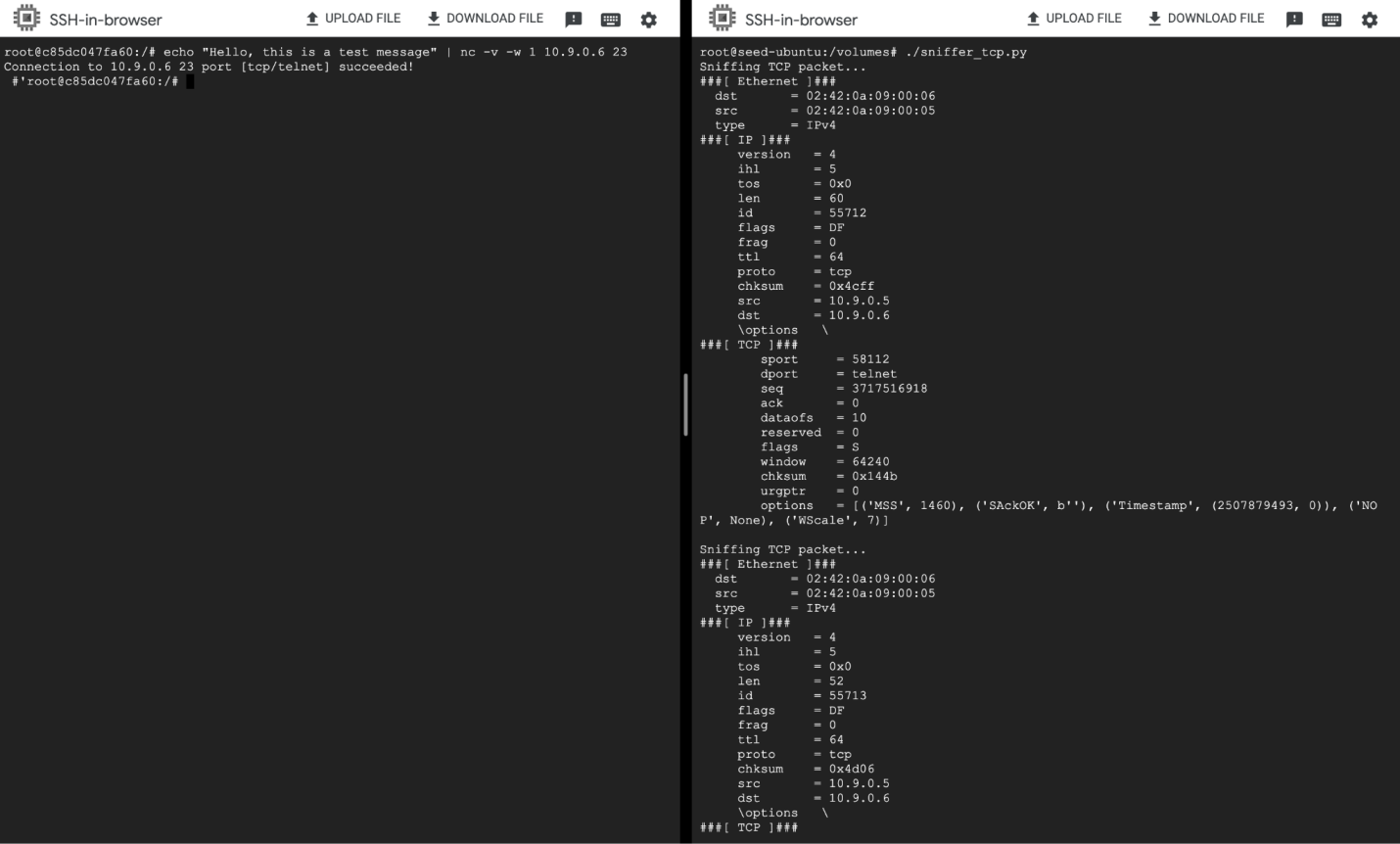
**print('Sniffing TCP packet...')**

**pkt.show()**

**# Capturing TCP packets from IP address 10.9.0.5(Host A) with destination port 23**

**pkt = sniff(iface='br-46f4ebc25eee', filter='tcp and host 10.9.0.5 and dst port 23', prn=print\_pkt)**

**TCP filter execution: Establishing tcp connection from host A to host B(IP address 10.9.0.6) with destination port 23**

****

**Task 1.2**

**icmp\_spoof.py: Below is the code to send out spoofed icmp packet**

**#!/usr/bin/python3**

**from scapy.all import \***

**print("SENDING SPOOFED ICMP PACKET.........")**

**ip = IP(src="1.2.3.4", dst="93.184.216.34")**

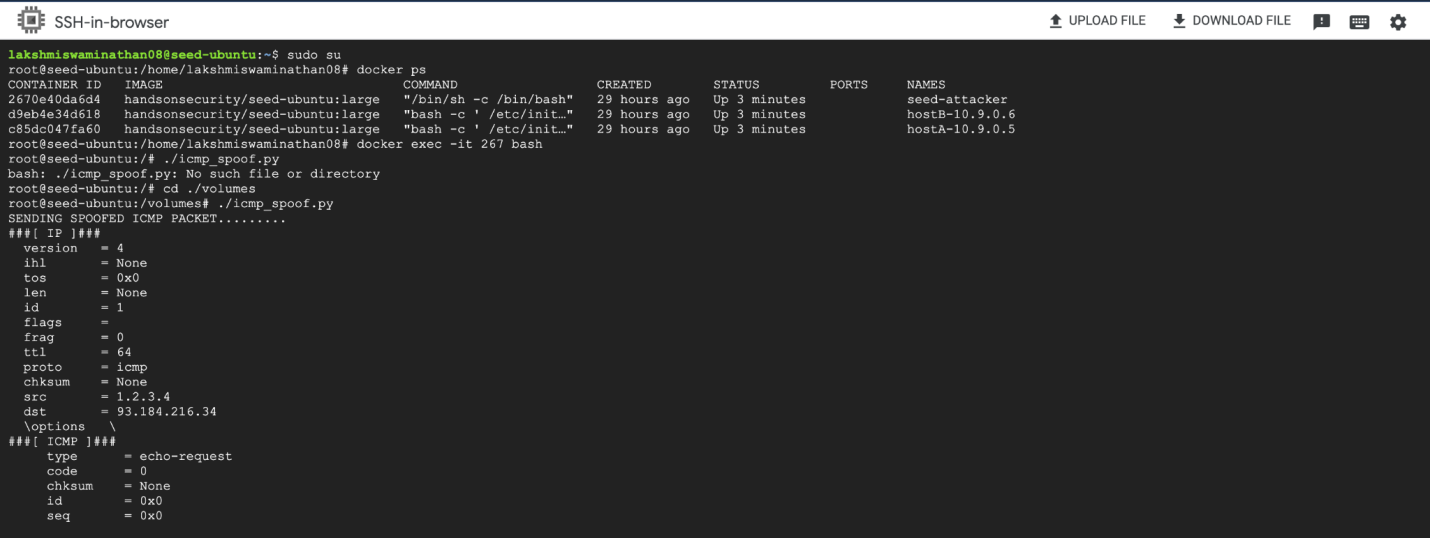
**icmp = ICMP()**

**pkt = ip/icmp**

**pkt.show()**

**send(pkt,verbose=0)**

**icmp spoofing execution:**

****

**Task 1.3**

**traceroute.py:**

**#!/usr/bin/env python3**

**from scapy.all import \***

**while True:**

**a = IP()**

**a.dst = sys.argv[1]**

**ttl = 3**

**a.ttl = ttl**

**b = ICMP()**

**p = a/b**

**resp = sr1(p, timeout=2, verbose=0)**

**if resp is None:**

**print("No reply")**

**elif resp[ICMP].type == 0 :**

**print("%d hops away: " % (a.ttl), resp[IP].src)**

**print("Done", resp[IP].src)**

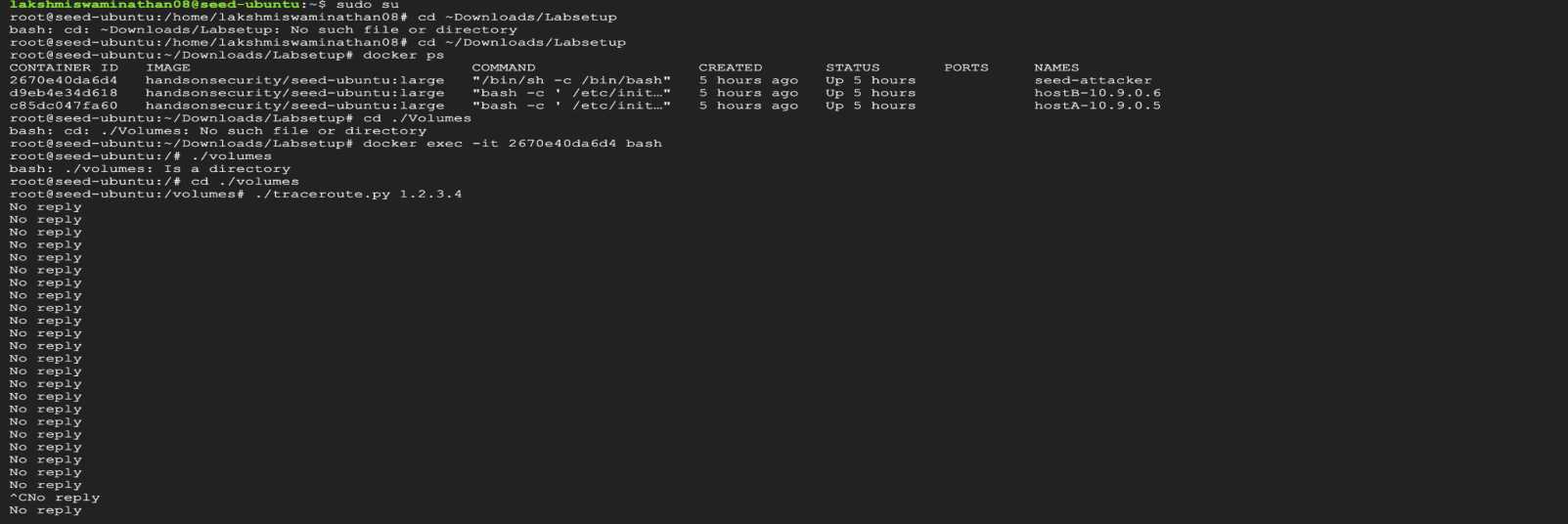
**else :**

**print("%d hops away: " % (a.ttl), resp[IP].src)**

**if ttl==30:**

**break**

**Traceroute execution:**

****

**Task 1.4**

**sniff\_spoof\_icmp.py: Below is the code to sniff and then spoof the icmp packet**

**#!/usr/bin/python3**

**from scapy.all import \***

**def spoof\_pkt(pkt):**

**if ICMP in pkt and pkt[ICMP].type == 8:**

**print("Original Packet.........")**

**print("Source IP : ", pkt[IP].src)**

**print("Destination IP :", pkt[IP].dst)**

**ip = IP(src=pkt[IP].dst, dst=pkt[IP].src, ihl=pkt[IP].ihl, ttl=50)**

**icmp = ICMP(type=0, id=pkt[ICMP].id, seq=pkt[ICMP].seq)**

**data = pkt[Raw].load**

**newpkt = ip/icmp/data**

**print("Spoofed Packet.........")**

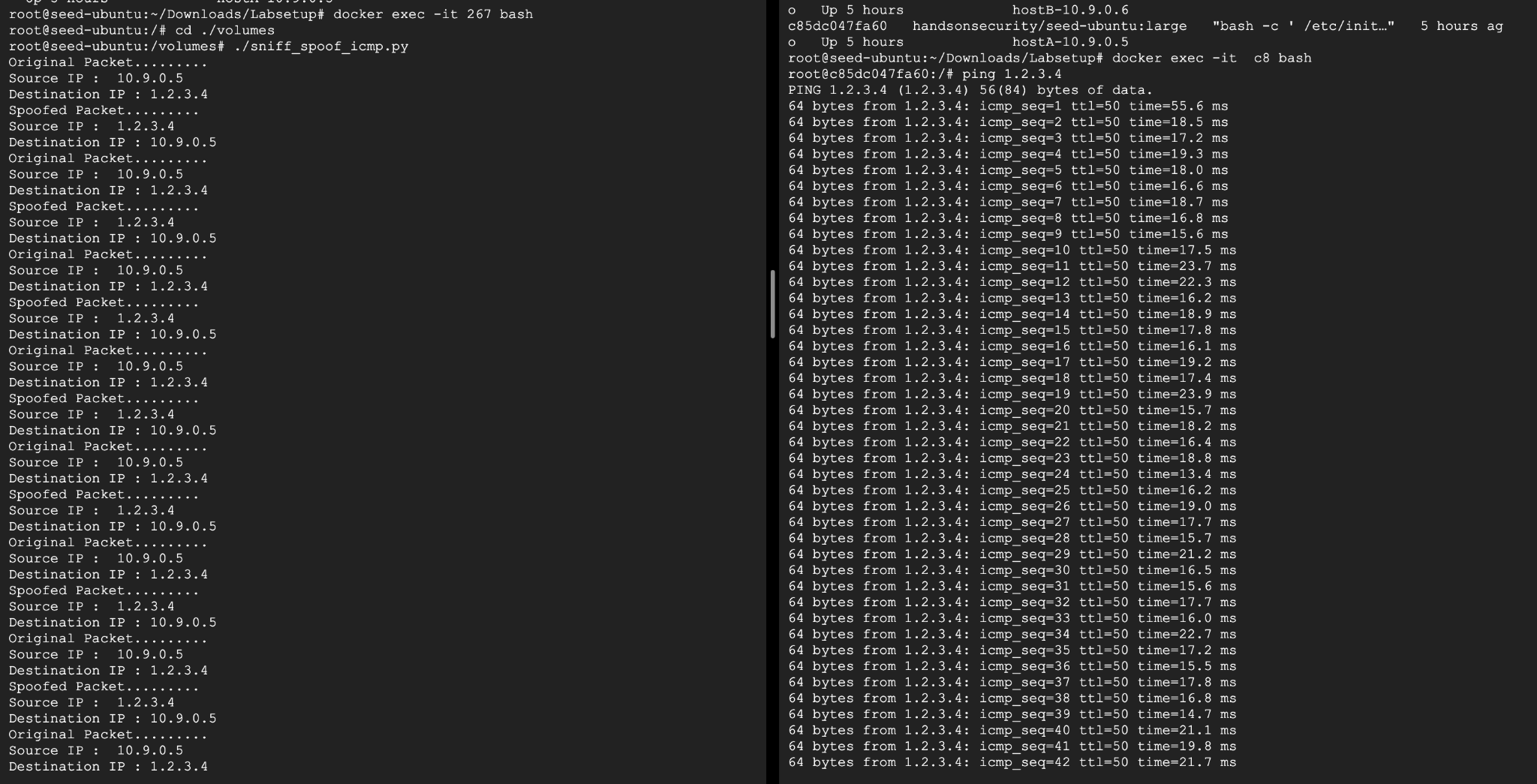
**print("Source IP : ", newpkt[IP].src)**

**print("Destination IP :", newpkt[IP].dst)**

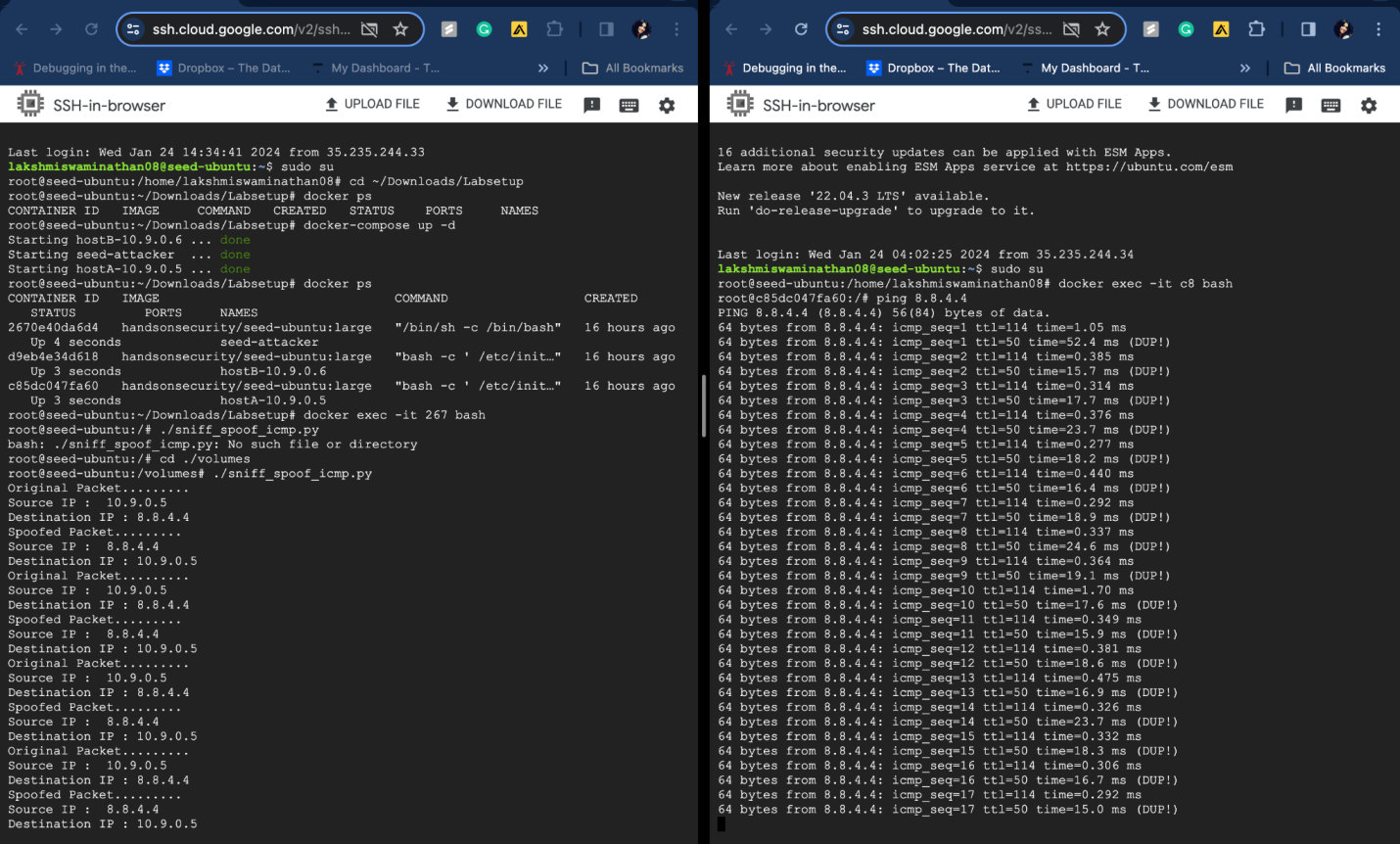
**send(newpkt,verbose=0)**

**pkt = sniff(iface='br-46f4ebc25eee', filter='icmp and src host 10.9.0.5',prn=spoof\_pkt)**

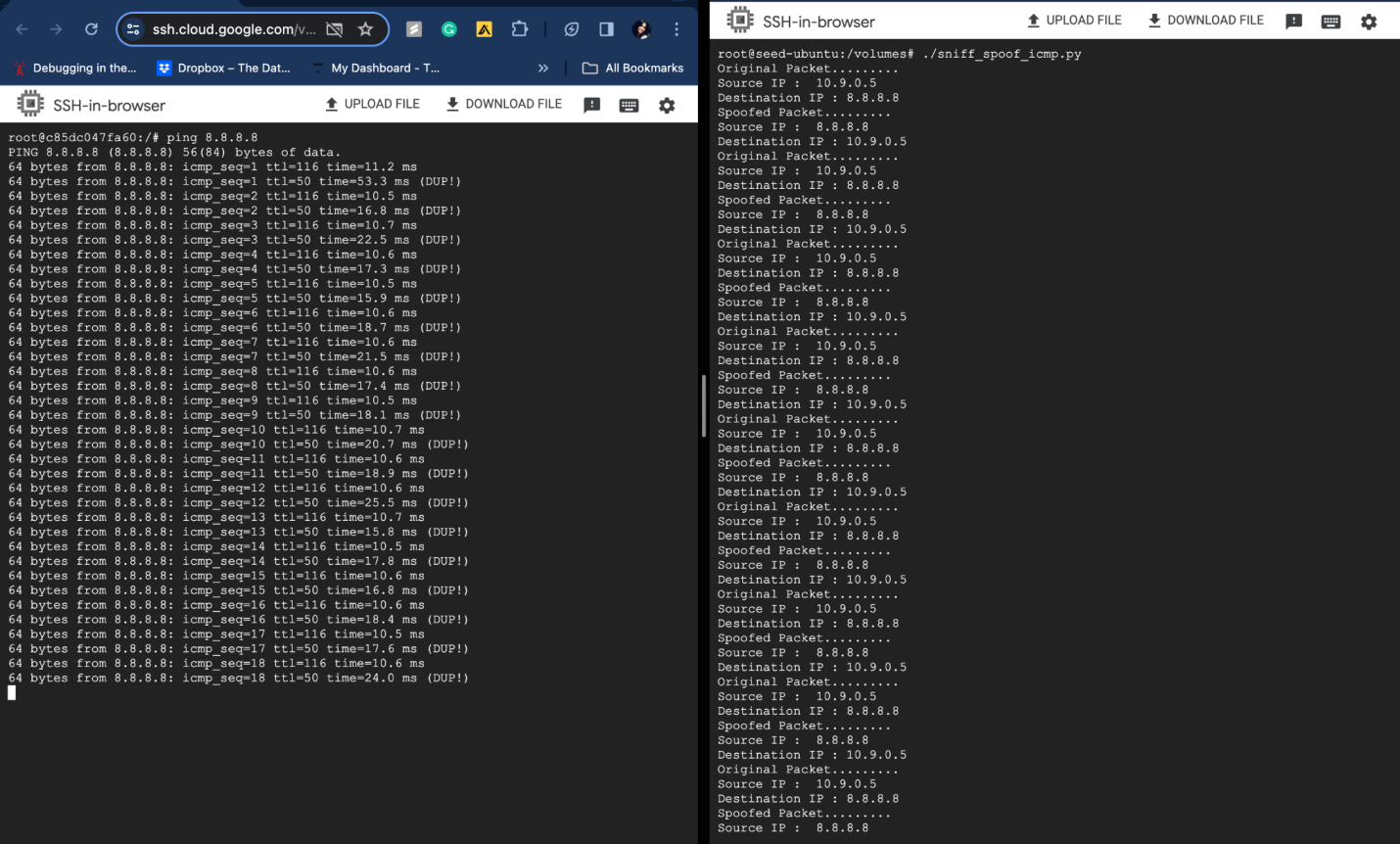
**Results of pinging 1.2.3.4(from host A) while running sniff\_spoof\_icmp.py from attacker container**

****

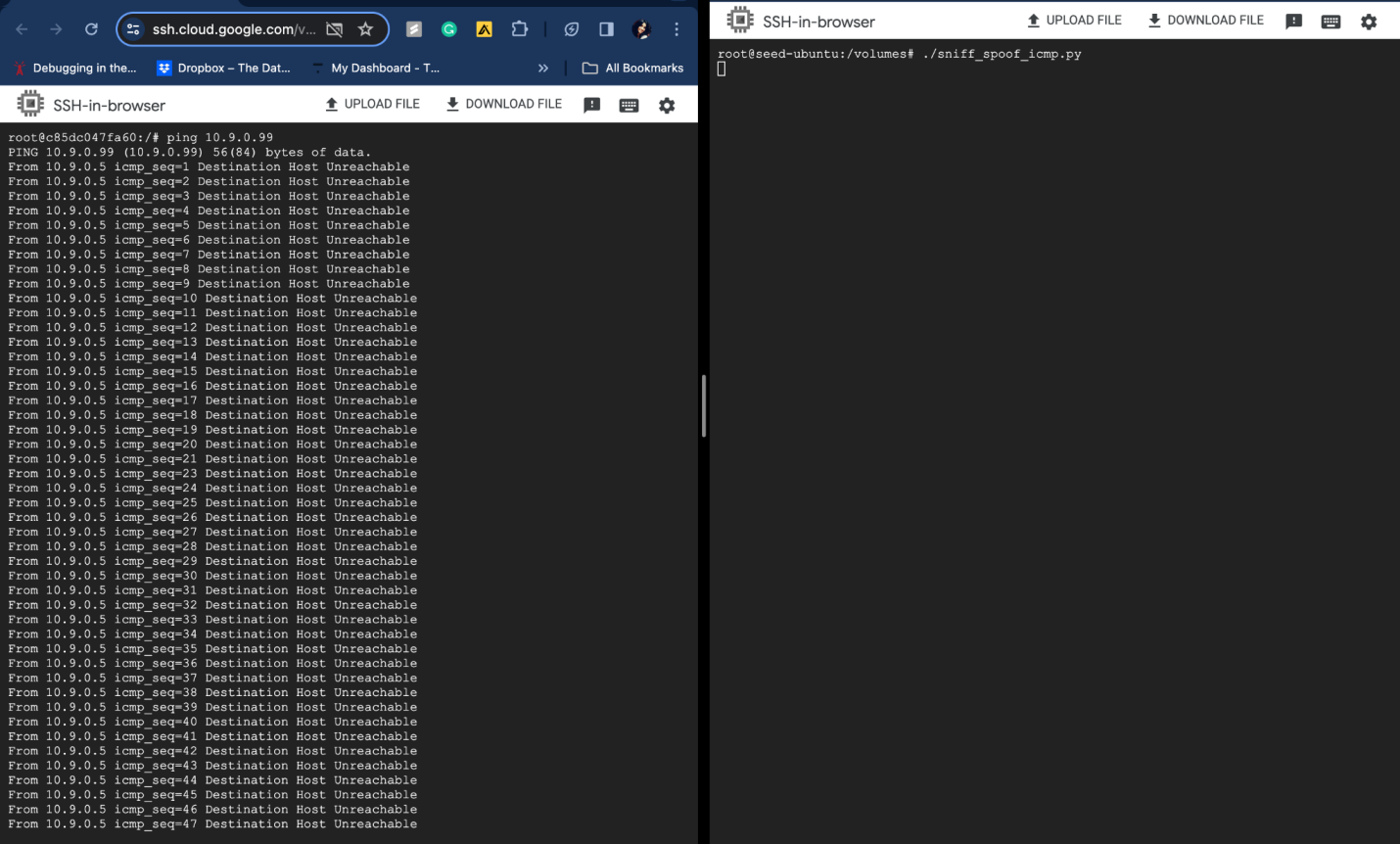
**Results of pinging 8.8.4.4(from host A) while running sniff\_spoof\_icmp.py from attacker container**

****

**Results of pinging 8.8.8.8(from host A) while running sniff\_spoof\_icmp.py from attacker container**

****

**Results of pinging 10.9.0.99(from host A) while running sniff\_spoof\_icmp.py from attacker container**

****