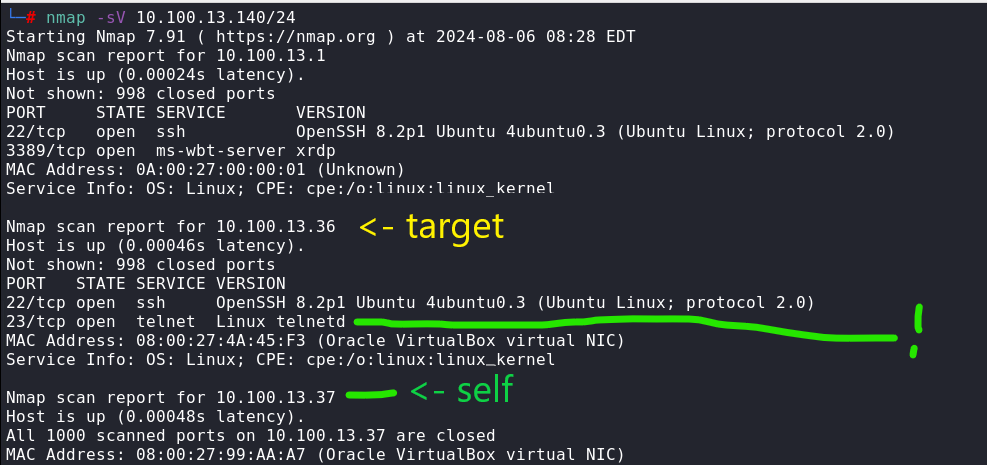
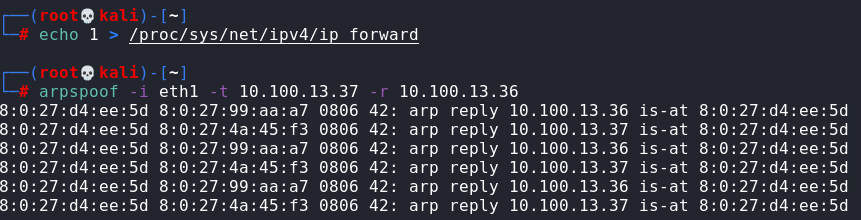
Starting scenario: 10.100.13.140/24 is the subnet we’re interested in. Our own attacking system is on this subnet. Let’s gather some info first.

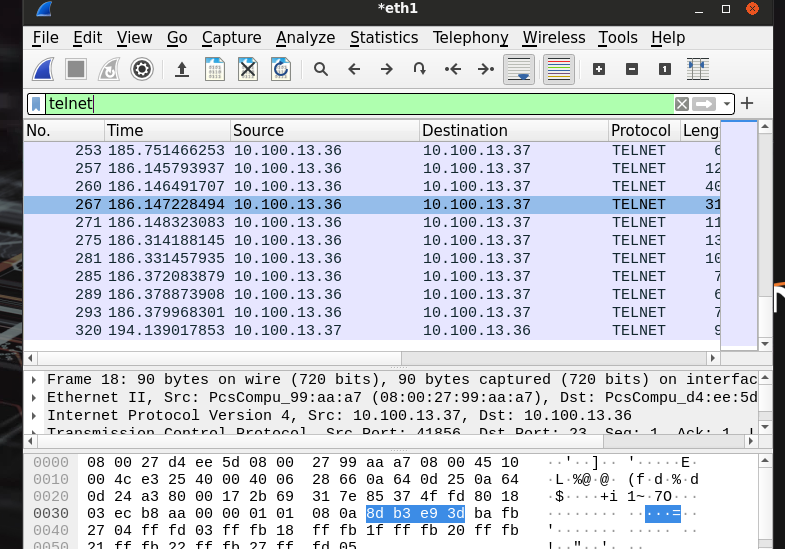
Port 23 looks interesting with telnetd on it



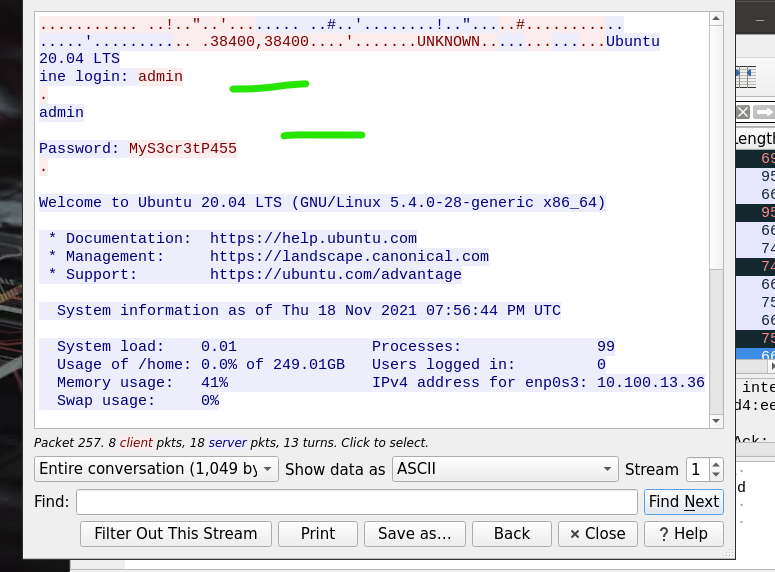
Set up packet forwarding and begin an arp spoof to become man in the middle



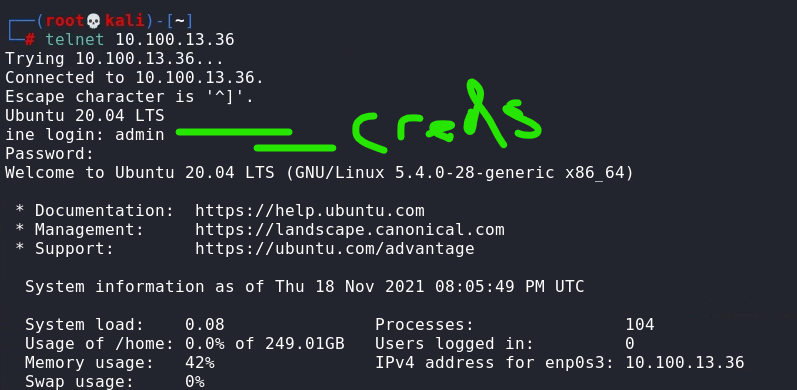
Start wireshark, then filter for telnet



Follow tcp channel and we find plaintext credentials. This is what is meant by plaintext comms being unsecure…



telnet into the target with the swiped credentials



That’s access…