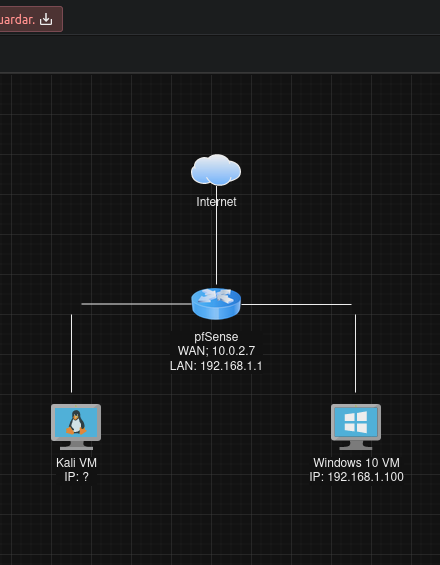
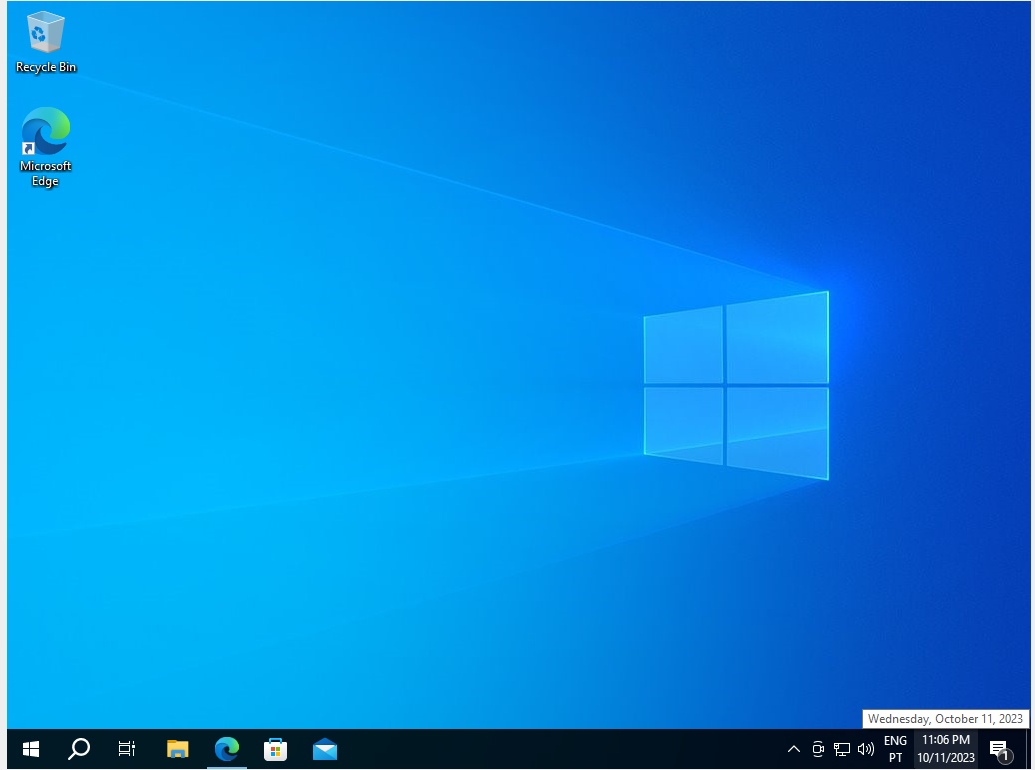
Rodrigo Brasil 10/2023

### **Part 1: Topology 1/2**

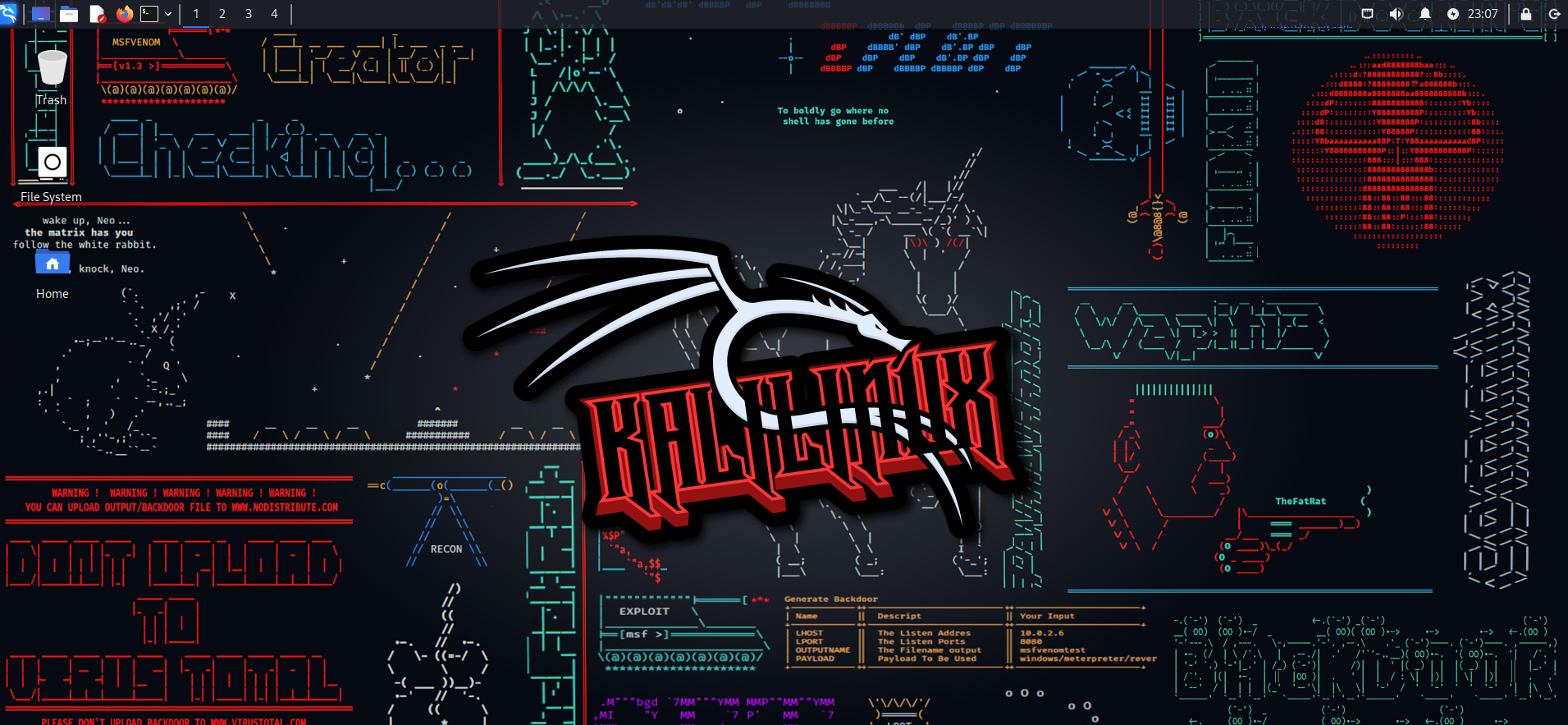


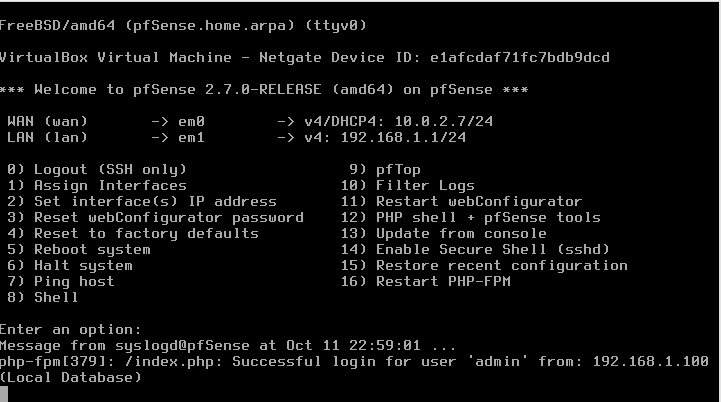
Initial Topology

### **Part 2: Staging**



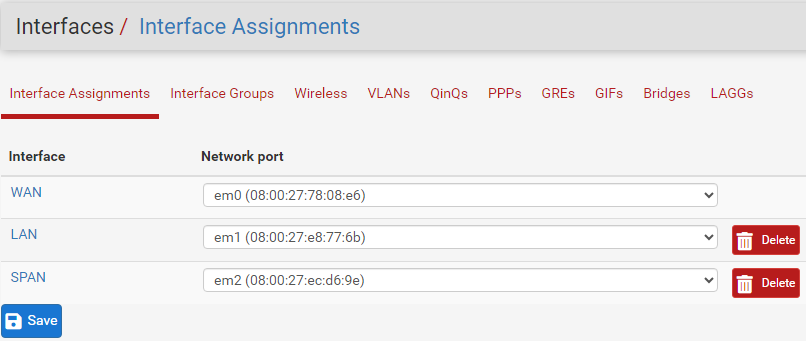
Windows 10 VM

Kali VM

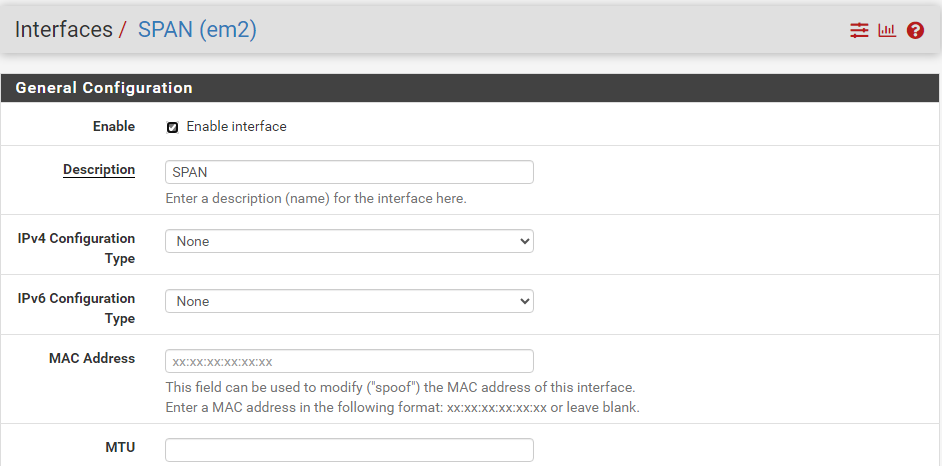


pfSense VM

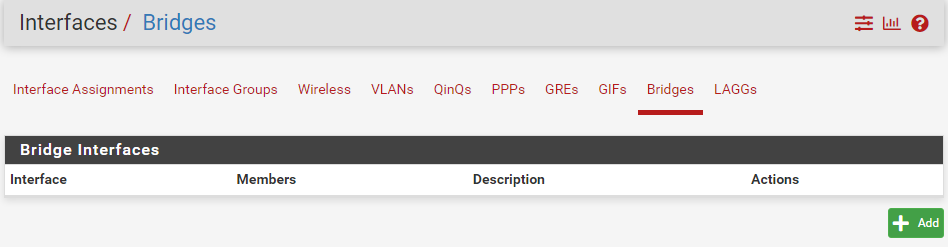
### **Part 3: Prepare a Span Port on pfSense**



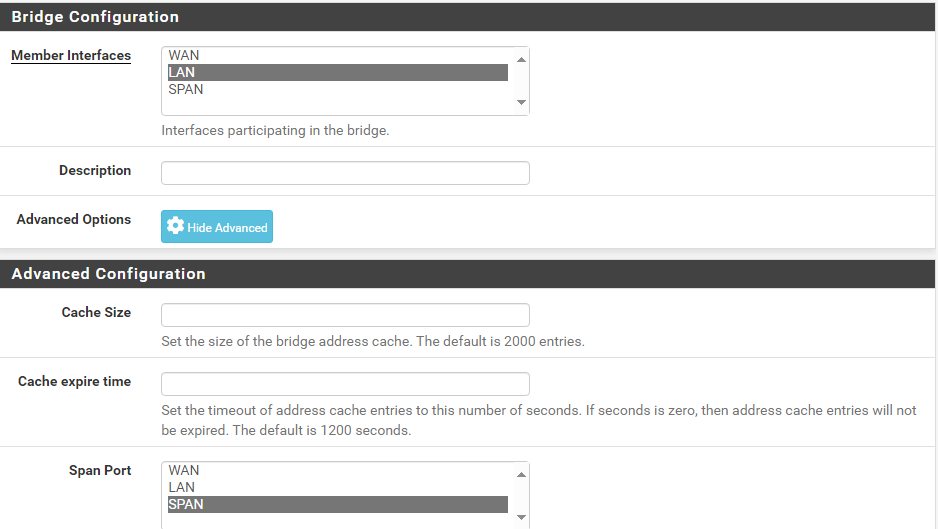
Log in pfSense and go to Interfaces / Assignments / Interface Assignments, click The green +Add button to add the another network interface.



Enable the check box and give it a name in the Description

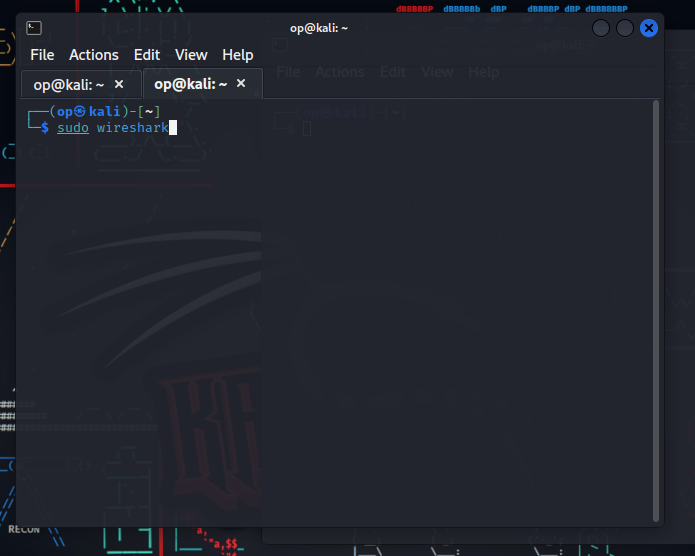


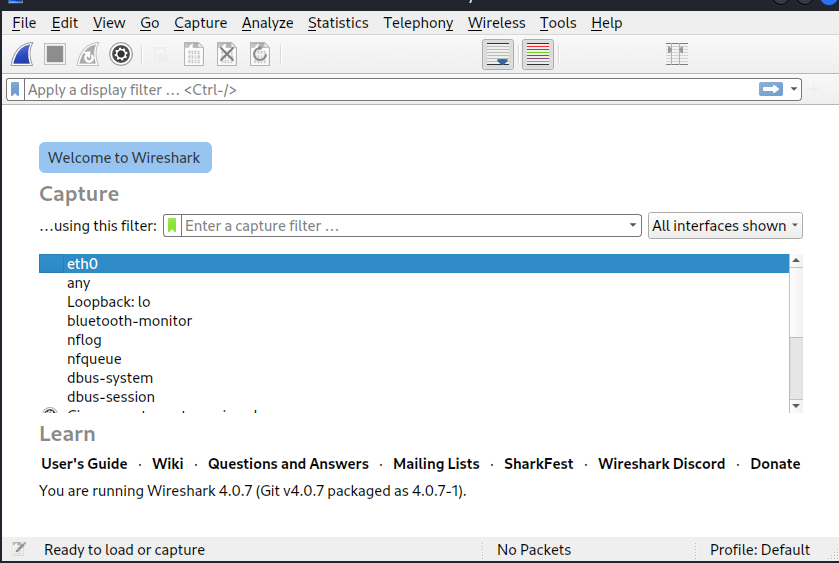
Head over to Interfaces / Assignments / Bridges and click the green +Add button to add a bridge.

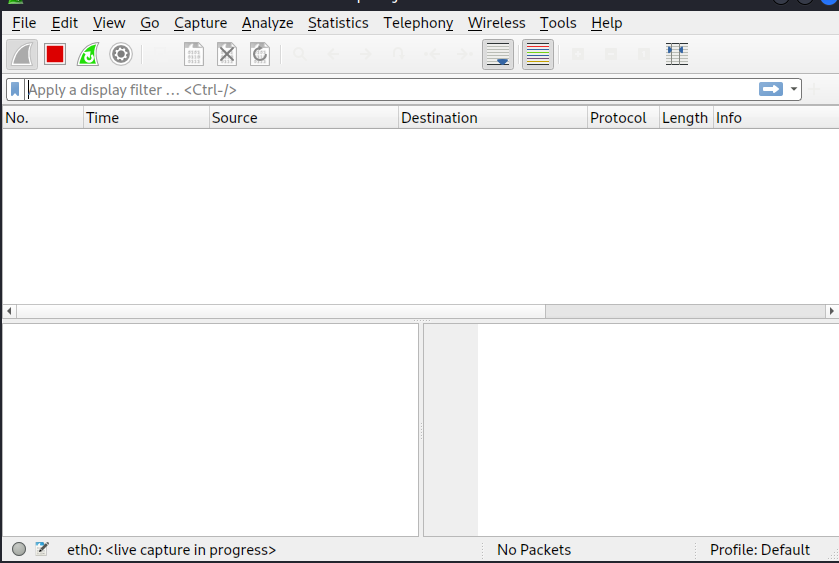


In the member interfaces select the LAN option and in Span Port select the SPAN option (if it is not there check if the “Enable Interface” check box on interface Assignments is enabled) and save.

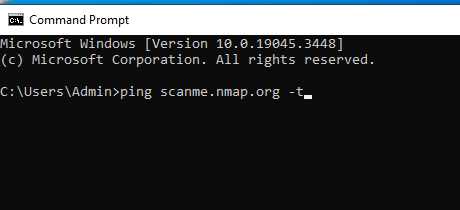
### **Part 4: Capture Packets with Kali**



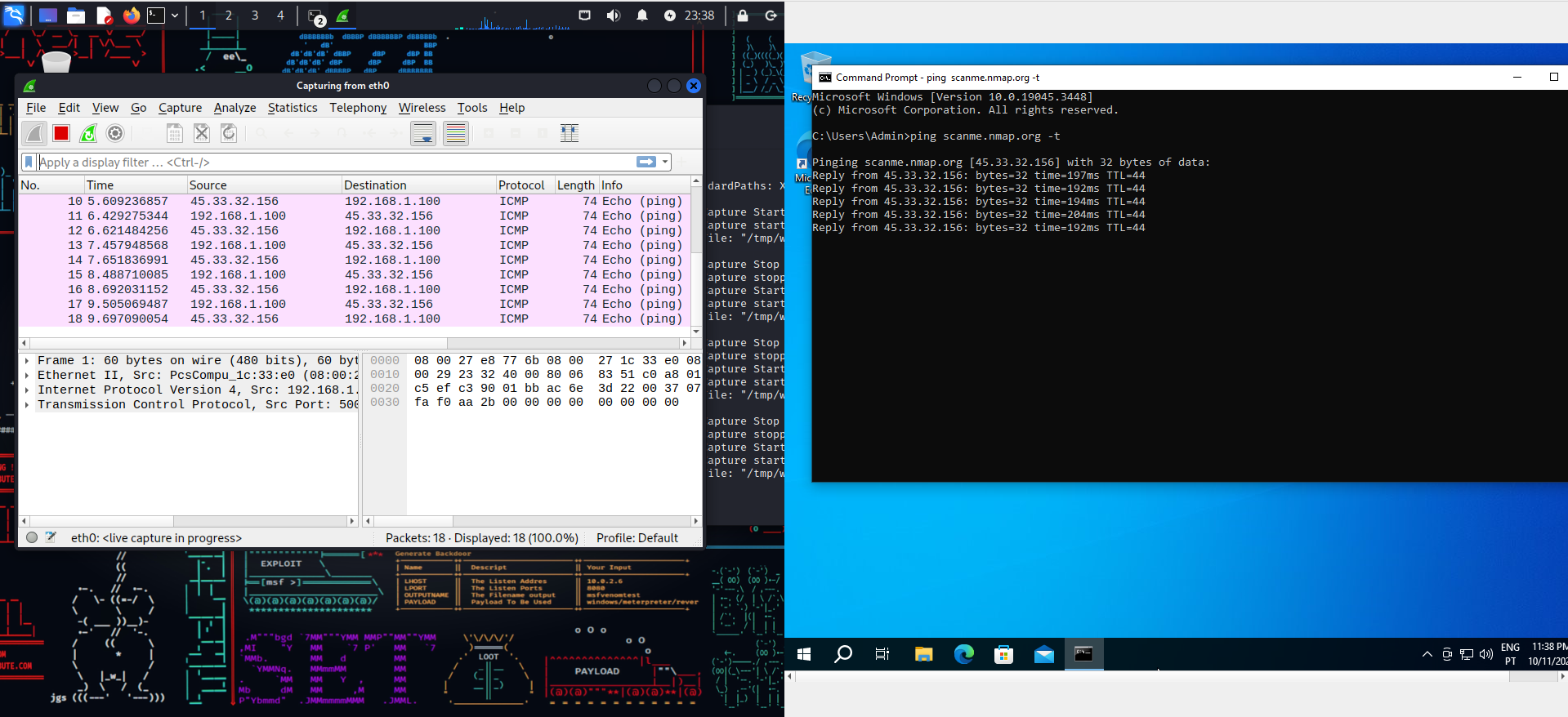




On Kali VM open a terminal and use the command *sudo wireshark* to start wireshark with root privileges. Open the network adapter that the SPAN port is connected to.(In this case is eth0)



on the Windows 10 VM simply open the command prompt and type the command *ping scanme.nmap.org -t* to send ping requests simultaneously to the domain.

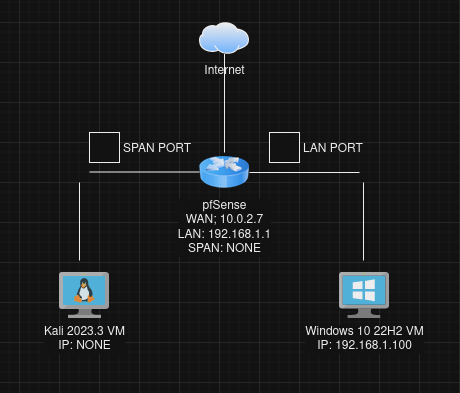
Kali VM Capturing the ping requests from Windows 10 VM

### **Part 5: Questions**

* On pfSense, navigate to the Dashboard, and locate the list of active interfaces
  + Does the interface you created have an IP address?
    - No, it does not.
* Disable all network devices on Kali *except* the span port connection
  + Does the traffic capture still work?
    - Yes.
  + Why might you want to disconnect a sniffing machine in this way?
    - So its own network traffic does not collide with the sniffed network
  + Does Kali have any IP addresses?
    - No it does not.
* If neither Kali nor pfSense have an IP address on the span port connecting them, how is traffic being sent from pfSense and reaching Kali?
  + - Because the span port on pfSense is used to mirror the traffic passing through it, and Kali is configured to capture and analyze this traffic using MAC addresses. IP addresses are not required, as the devices are working with Ethernet frames, not IP packets.

### 

### **Part 6: Topology 2/2**



Final Topology