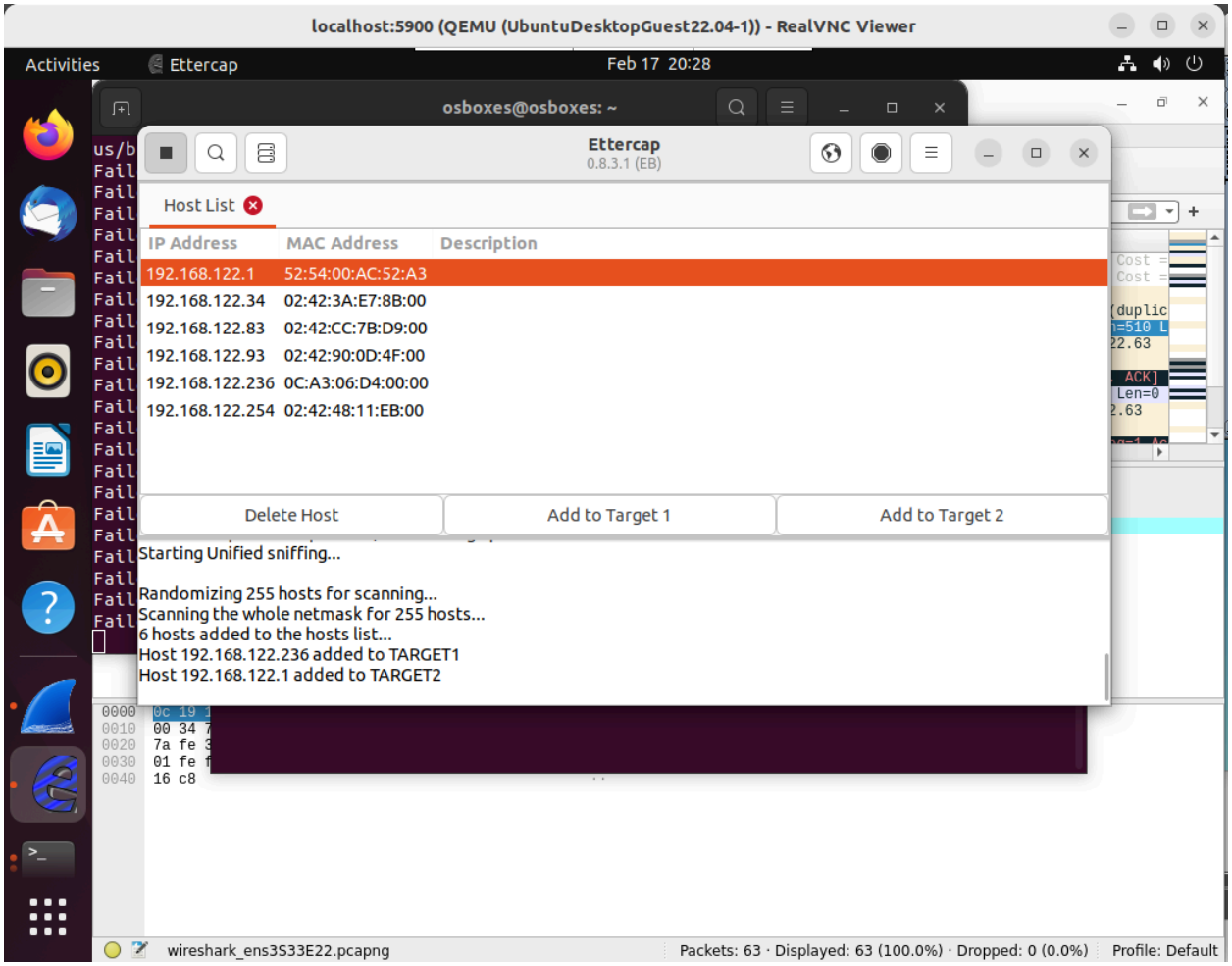
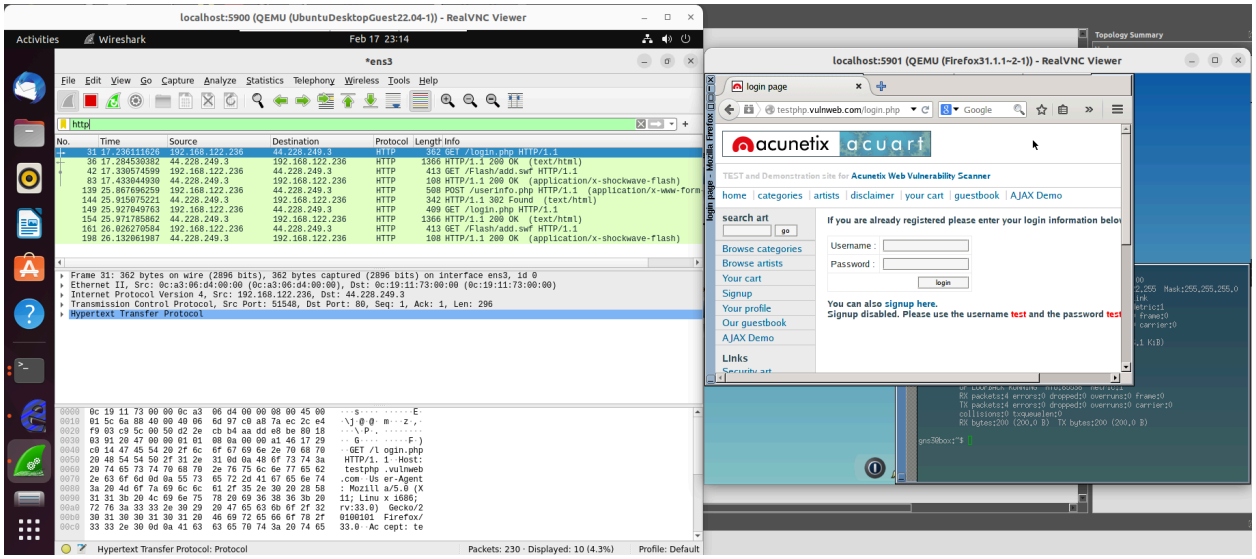
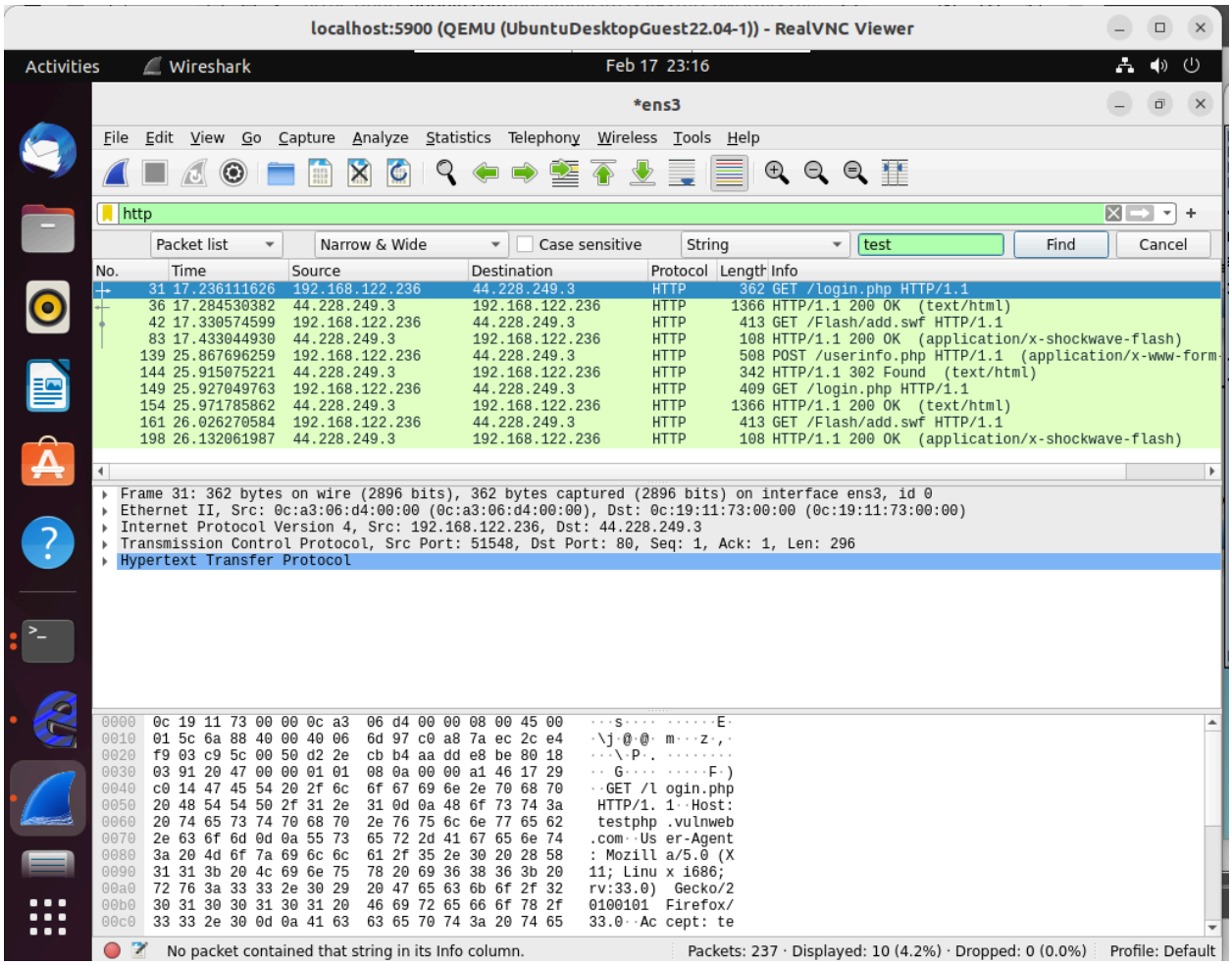
Setting Firefox VM and NAT node as targets



Poison attack between Firefox VM and the internet gateway. Picked up contents through Wireshark packet capture.



Filter “String” and input username or password in the search.



The ARP poisoning is sending ARP replies to both the Firefox VM and the NAT node. This tricks both systems into thinking they are sending packets to the “right” MAC address when they are actually being intercepted by the Ubuntu VM. In the Firefox VM, we go onto an HTTP website which is unencrypted. The Ubuntu VM is able to intercept the HTTP request which Wireshark is able to display. Through Wireshark, it is possible to see the packet details which include the username and password. This issue definitely poses a risk in enterprise settings as it is a breach in confidentiality. Credential theft can be extremely damaging, especially in the sense of admin logins. Intercepted traffic can also potentially be modified which creates a loss of data integrity as well.