**TNE lab 1**

Some contextual configs of the systems:

*[****Note****: password of both systems is:* ***user****]*

|  |  |  |
| --- | --- | --- |
| Machine name | Ubunto 1 | Ubunto 2 |
| Server/Client | Server | Client |
| Interface being used | ens33 | ens33 |
| IP allocated | 192.168.54.128 | 192.168.54.129 |
| Port to send/forward | 23 | 80 |
| Port to recieve | 80 | 2323 |

(all the data is here + in copy)

1. What command is needed on the tunnel server to accept tunneled messages on port 80 and send them to port 23 on the local host? Include the IP addresses that you used.

sudo hts –F 192.168.54.128:23 80

1. What command is needed on the tunnel client to tunnel messages to and from port 2323 to and from port 80?

sudo htc –F 2323 192.168.54.128:80

1. What did Wireshark interpret the tunnelled traffic as?

TCP

1. How did the tunnelling software attempt to hide the traffic?

It tried to hide it as http traffic (port 80)

1. How might tunnelling of this kind be used to subvert security policy?

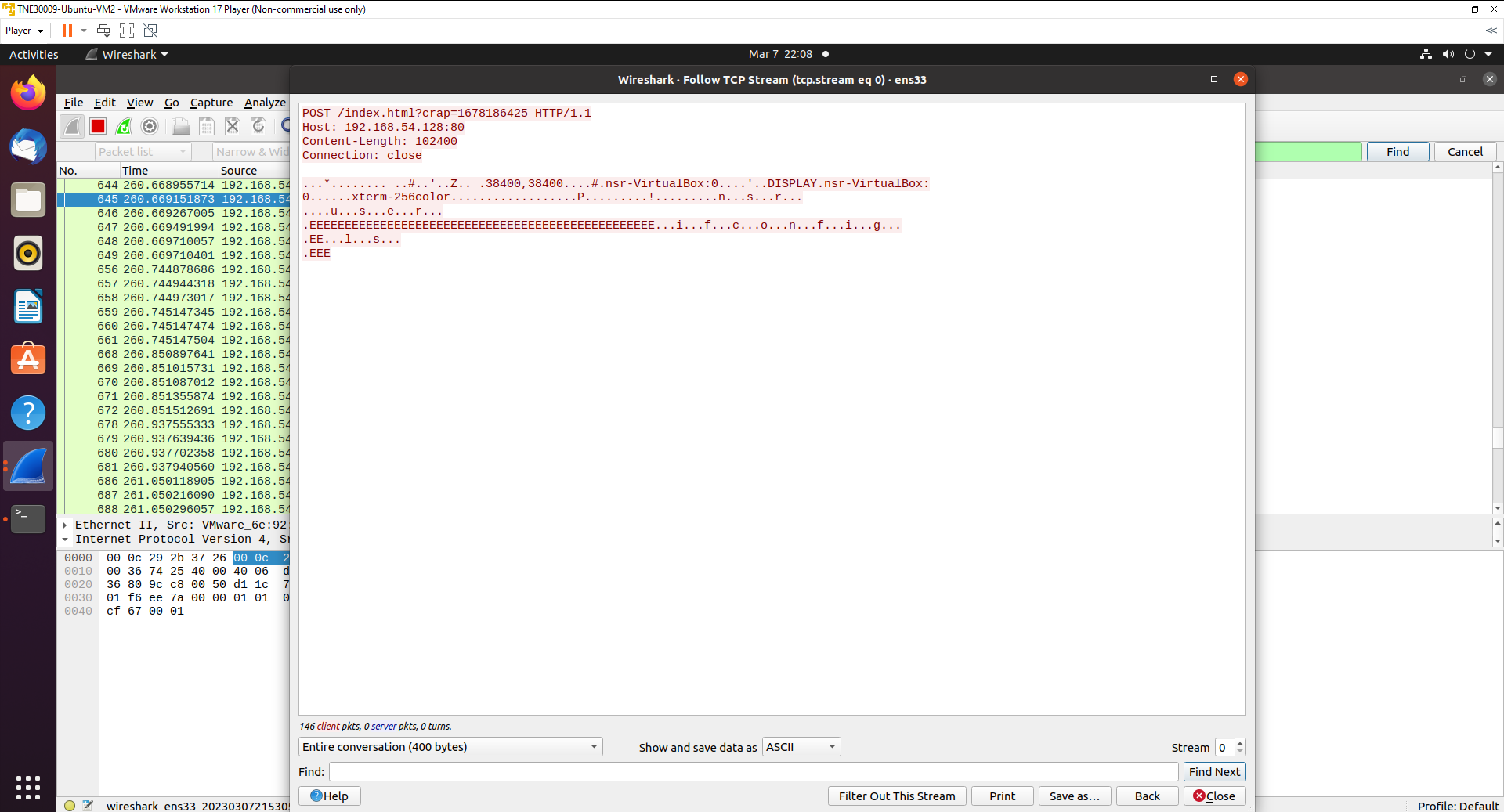
It may be used to pass fragmented data of malware which individually will not get triggered by the policy, ----but can be resolved using firewall that deep-inspects packet traffic

~~Also, it can be used to send information from server computer to client computer covertly if ssh or smth else was used to properly hide it~~

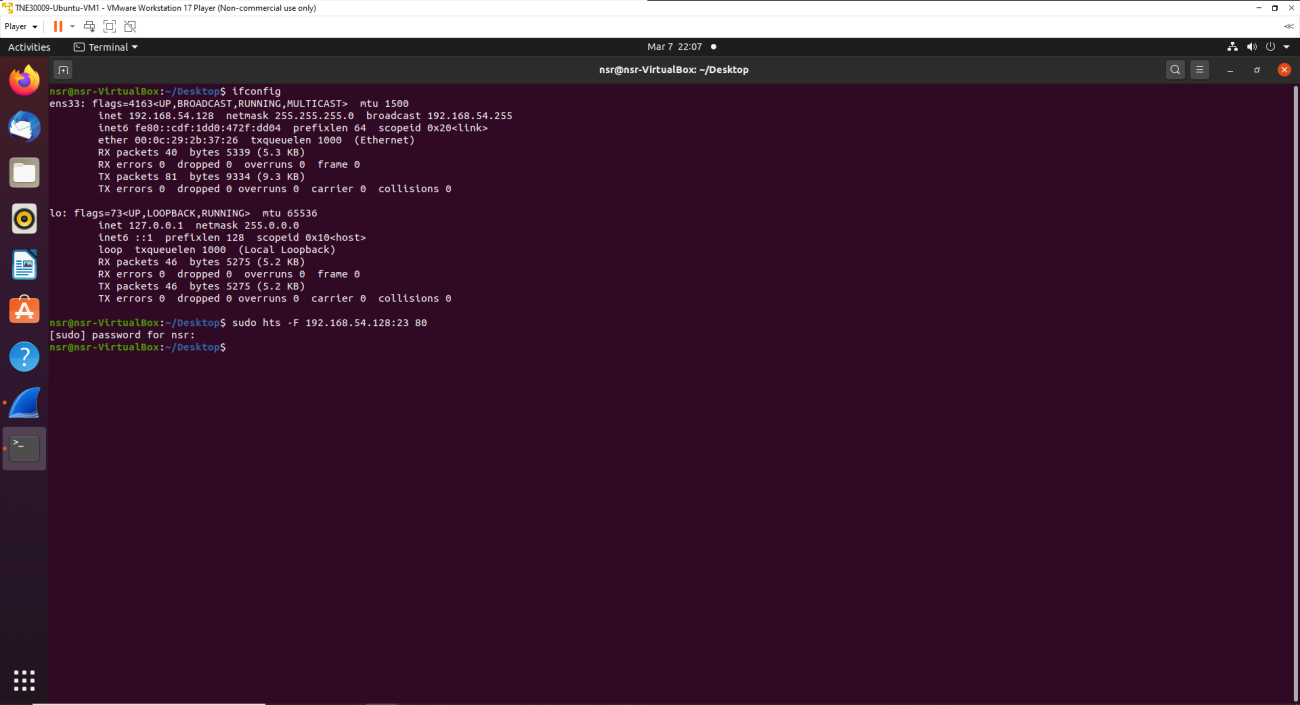
+ covert channel so can hide stuff from firewall as well and thus bypass all the protection feature!

*Including screen dumps of the cmd promts and stuff here just in case*

Wireshark:



Server:



Client:

