Step 2 - netstat -tna

franci		1000101	SP NOT	-10	
<pre>[wen.dong@ALMORG1915P-W01 networking_mon]\$ netstat -tna Active Internet connections (servers and established)</pre>					
			Local Address		State
tcp	0	-	127.0.0.1:32000	0.0.0.0:*	LISTEN
	0		0.0.0.0:33699	0.0.0.0:*	LISTEN
tcp	0		0.0.0.0:139	0.0.0.0:*	LISTEN
tcp	0		0.0.0.0:139	0.0.0.0:*	LISTEN
	0		0.0.0.0:8080	0.0.0.0:*	LISTEN
tcp	0		0.0.0.0:38545	0.0.0.0:*	LISTEN
tcp	0		0.0.0.0:38343	0.0.0.0:*	LISTEN
tcp	0		0.0.0.0:445	0.0.0.0:*	LISTEN
tcp	0		10.212.153.9:43978	10.210.208.10:49687	
tcp	0		10.212.153.9:43978	10.212.158.45:1521	
tcp	0		127.0.0.1:31000	127.0.0.1:32000	ESTABLISHED
tcp	0		10.212.153.9:8080	10.212.152.203:28270	TIME WAIT
tcp			127.0.0.1:32000	127.0.0.1:31000	ESTABLISHED
tcp	0		10.212.153.9:45346	10.212.158.45:1521	ESTABLISHED
tcp	0		10.212.153.9:45346	52.119.161.149:443	ESTABLISHED
tcp					
tcp	0		10.212.153.9:35162	52.119.172.239:443	TIME_WAIT ESTABLISHED
tcp	0		10.212.153.9:48914	10.210.208.10:445	
tcp	0		10.212.153.9:8080	10.212.154.119:57554	TIME_WAIT
tcp	0		10.212.153.9:22	172.27.1.3:22001	ESTABLISHED
tcp	0		10.212.153.9:37268	10.212.158.45:1521	ESTABLISHED
tcp	0		10.212.153.9:902	8.8.8.2:2049	ESTABLISHED
tcp	0		10.212.153.9:37730	10.212.158.45:1521	ESTABLISHED
tcp	0		10.212.153.9:8080	10.212.152.203:28198	TIME_WAIT
tcp	0			10.210.208.10:49666	ESTABLISHED
tcp	0		10.212.153.9:43704	52.94.212.197:443	ESTABLISHED
tcp	0		10.212.153.9:45644	10.212.158.45:1521	ESTABLISHED
tcp6	0		:::139	:::*	LISTEN
tcp6	0		:::111	:::*	LISTEN
tcp6	0		:::8081	:::*	LISTEN
tcp6	0		:::56469	:::*	LISTEN
tcp6	0		:::22	:::*	LISTEN
tcp6	0	0	:::445	*	LISTEN

Step 5. check tcp connections in this machine:

```
ubuntu@ip-172-31-13-112:~$ sudo netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address
                                            Foreign Address
                                                                     State
                                            0.0.0.0:*
           0
                  0 127.0.0.1:37333
tcp
                                                                     LISTEN
tcp
           0
                  0 127.0.0.53:53
                                            0.0.0.0:*
                                                                     LISTEN
tcp
           0
                  0 0.0.0.0:22
                                            0.0.0.0:*
                                                                     LISTEN
                384 172.31.13.112:22
tcp
           0
                                            18.237.140.160:48645
                                                                     ESTABLISHED
                  0 172.31.13.112:22
           0
                                            18.237.140.161:8092
                                                                     ESTABLISHED
tcp
                                                                     ESTABLISHED
                  0 172.31.13.112:22
                                            18.237.140.160:64106
           0
tcp
                                                                     LISTEN
           0
                  0 :::22
ubuntu@ip-172-31-13-112:~$
```

Step 6

```
ubuntu@ip-172-31-13-112:~$ telnet 172.31.13.112 23
Trying 172.31.13.112...
telnet: Unable to connect to remote host: Connection refused
ubuntu@ip-172-31-13-112:~$ ssh 172.31.13.112
The authenticity of host '172.31.13.112 (172.31.13.112)' can't be established.
ECDSA key fingerprint is SHA256:vnklu5jf31DYhFGL6ZAmyM/uSgpN4vNhkFlXA54jwuM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: yes
```

telnet failed due to netwox is attacking the default telnet port 23 on the server, which was overwhelmed thus unable to receive more connection.

Ssh succeeded because the SSH port 22 was OK, not being overwhelmed.

P2. Answer

telnet in step 1 succeeded, however it failed in step 3 because during the TCP connection establishment, it was reset by the response of spoofing.

P3. Answer

My youtube video suddenly got frozen, this was because the attack netwox 78 attacked my computer by resetting every request from my server.