**Challenge Lab 1 Report**

1. **Challenge questions Description:**

Describe any suspicious activity or outlying data points by using screenshot.

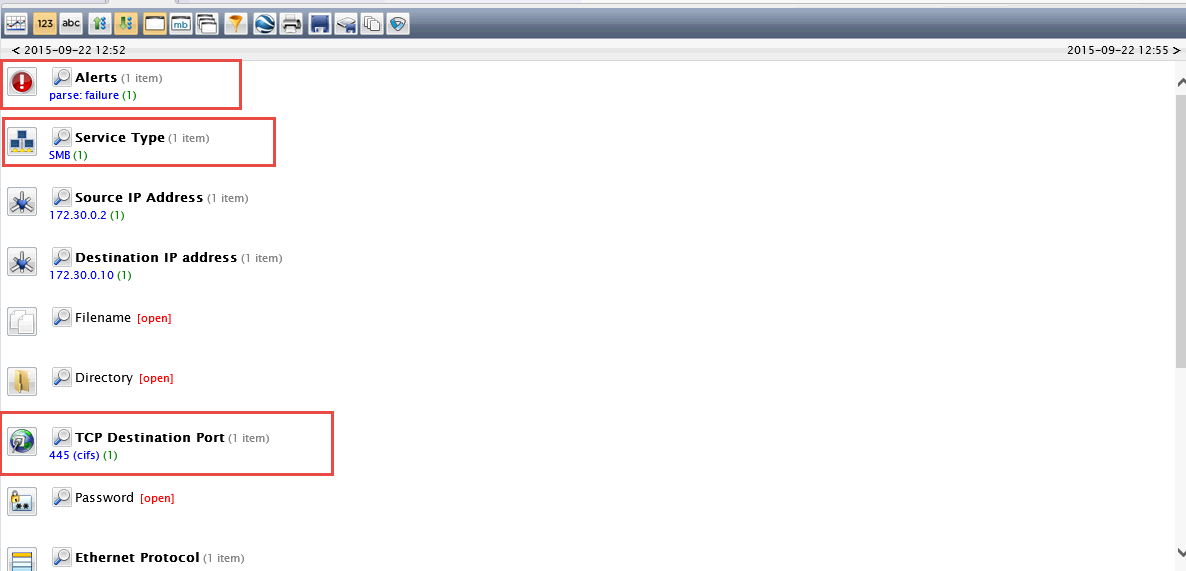
1. **Tools used in this report:**

In this report, we use the following three tools to analyze the potential existing threats

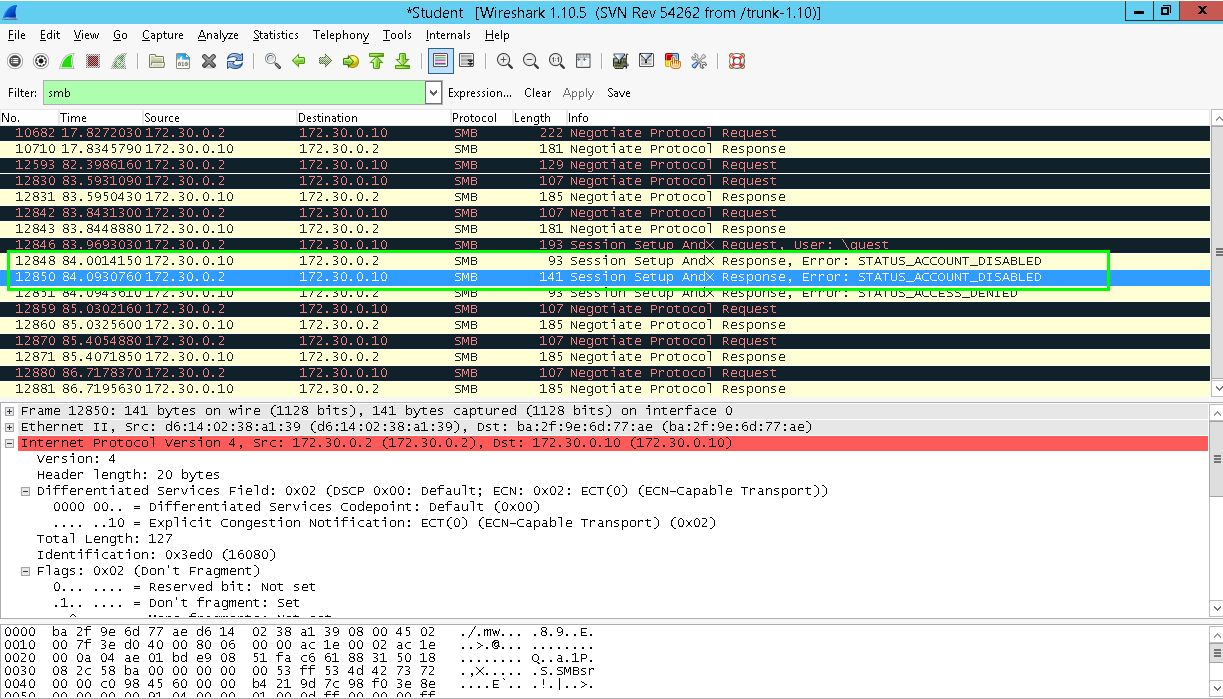
* Wireshark -> Capture all the packets over the script communication of Zenmap.
* Zenmap -> Run many scripts to generate network traffic.
* NetWitness Investigator -> Visualize the result of Wireshark.

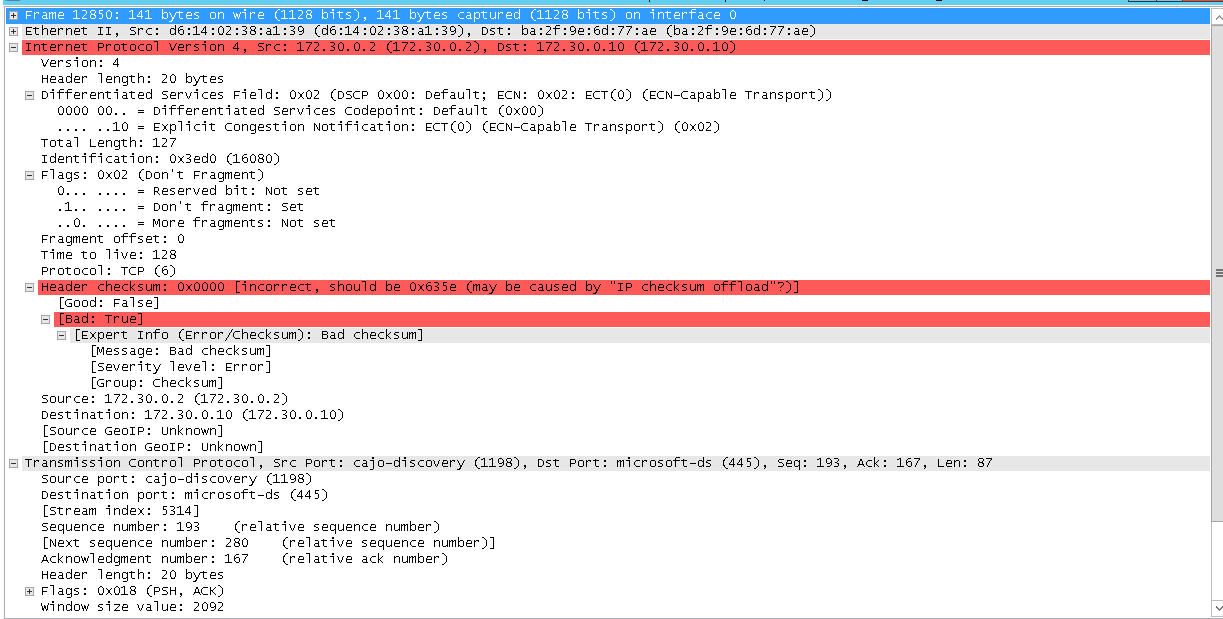
1. **Analysis Report**
2. **Packets transmission error**

When I use Wireshark on Vworkstation to capture the network work traffic of student interface, I found that there are two packets were failed to transmit correctly.



By viewing the Alert information we can see that this alter are generated by SMB services which are responsible for the communication among printers, sharing access file …etc. It uses SMB services (port 445) to communicate between two IP addresses – 172.30.0.2(Source) and 172.30.0.10(Destination). But if we want to know details we need to go back Wireshark.



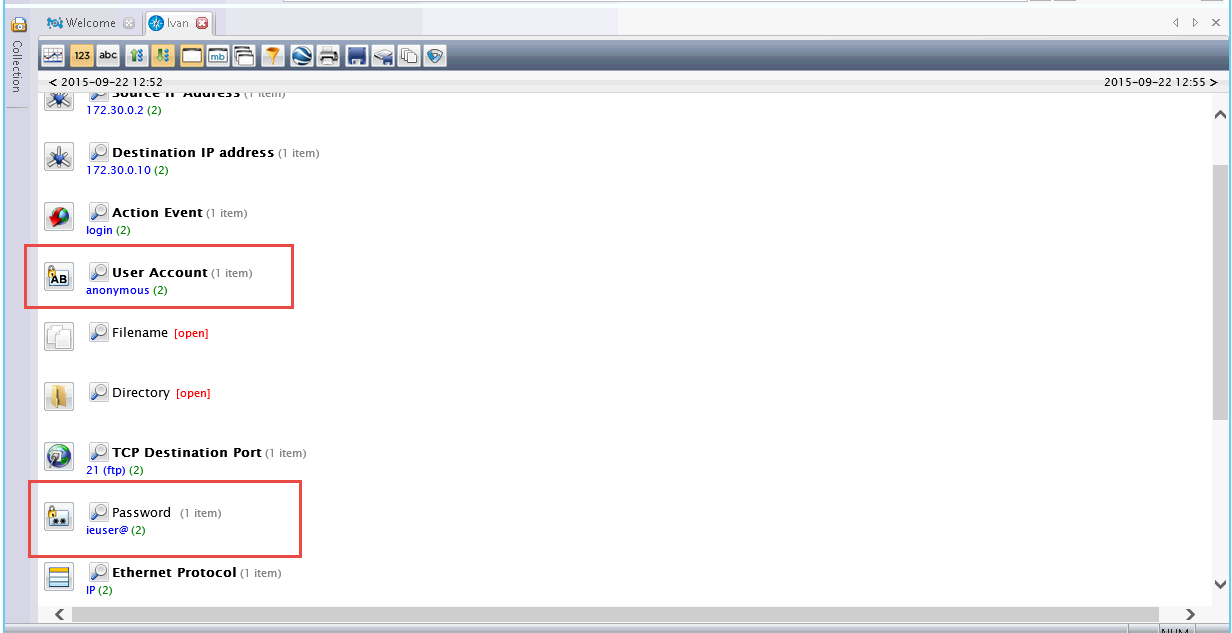


With the drill down information, I know that the error caused by incorrect packet header checksum and it was sent through SMB services. And the possible reason might be the effect of IP checksum offload. It may be the reason why NetWitness Investigator generates an alert.

In addition, we also found that there are tremendous data transmission activities happened between source IP 172.30.0.2(source) and 172.30.0.10(Destination). Therefore, it indicates that there should be some suspicious activities that are ongoing.

1. **Clear Password transmission**

According to the report of NetWitness Investigator, I found that when the Nmap scripts start, the wireshark captured a clear-text password as follows.



So, through this picture, we know that the password transmitted as clear text and login as anonymous when IP 172.30.0.2 (source) communicate with IP 172.30.0.10 (Destination). Therefore, there is a risk to disclose the password to attacker and some attackers could make a man-in-middle attack or do some other harmful things.