# Challenge Lab 1 Report

## 1. Challenge questions Description:

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

## 2. Tools used in this report:

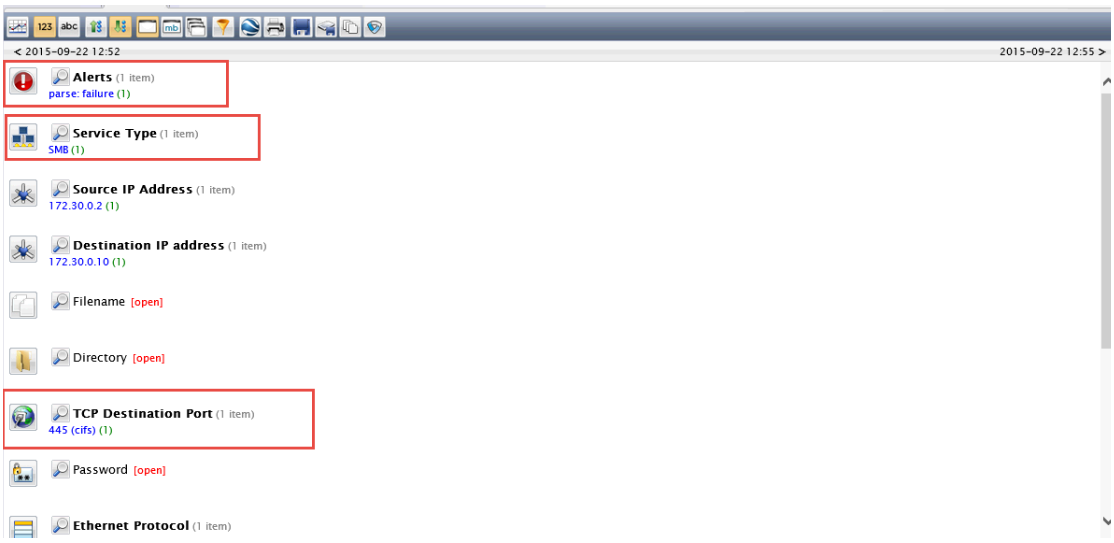
In this report, we use the following three tools to analyze the potential existing threats

- 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.

## 3. Analysis Report

### 3.1 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.



< 2015-09-22 12:52 2015-09-22 12:55 >

Alerts (1 item)
parse: failure (1)

Service Type (1 item)
SMB (1)

Source IP Address (1 item)
172.30.0.2 (1)

Destination IP address (1 item)
172.30.0.10 (1)

Filename [open]

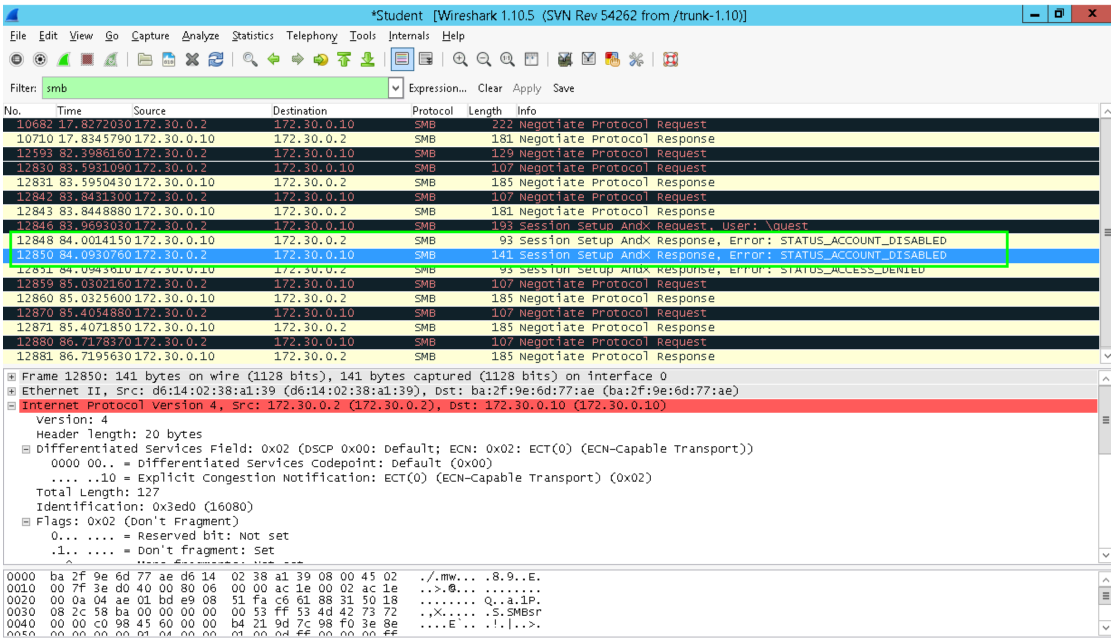
Directory [open]

TCP Destination Port (1 item)
445 (cifs) (1)

Password [open]

Ethernet Protocol (1 item)

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.

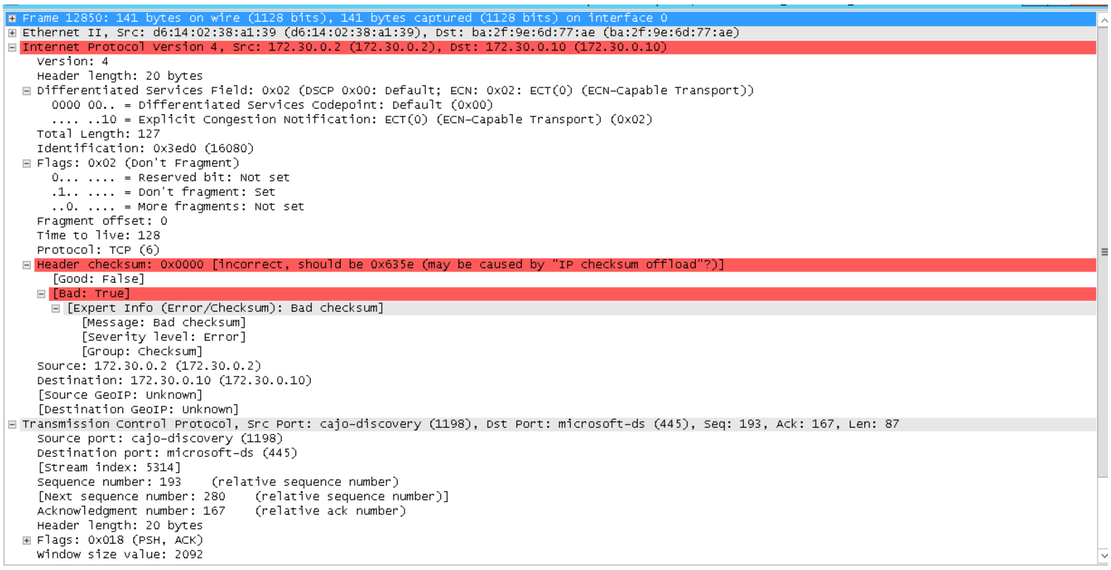


*Student [Wireshark 1.10.5 (SVN Rev 54262 from /trunk-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: smb
Expression... Clear Apply Save

```
No.   Time       Source      Destination  Protocol Length Info
10682 17.8272030 172.30.0.2  172.30.0.10  SMB      222 Negotiate Protocol Request
10710 17.8345790 172.30.0.10 172.30.0.2   SMB      181 Negotiate Protocol Response
12593 82.3986160 172.30.0.2  172.30.0.10  SMB      129 Negotiate Protocol Request
12830 83.5931090 172.30.0.2  172.30.0.10  SMB      107 Negotiate Protocol Request
12831 83.5950430 172.30.0.10 172.30.0.2   SMB      185 Negotiate Protocol Response
12842 83.8431300 172.30.0.2  172.30.0.10  SMB      107 Negotiate Protocol Request
12843 83.8448880 172.30.0.10 172.30.0.2   SMB      181 Negotiate Protocol Response
12846 83.9693030 172.30.0.2  172.30.0.10  SMB      193 Session Setup AndX Request, User: \guest
12848 84.0014150 172.30.0.10 172.30.0.2   SMB       93 Session Setup AndX Response, Error: STATUS_ACCOUNT_DISABLED
12850 84.0930760 172.30.0.2  172.30.0.10  SMB      141 Session Setup AndX Response, Error: STATUS_ACCOUNT_DISABLED
12851 84.0943610 172.30.0.10 172.30.0.2   SMB       93 Session Setup AndX Response, Error: STATUS_ACCESS_DENIED
12859 85.0302160 172.30.0.2  172.30.0.10  SMB      107 Negotiate Protocol Request
12860 85.0325600 172.30.0.10 172.30.0.2   SMB      185 Negotiate Protocol Response
12870 85.4054880 172.30.0.2  172.30.0.10  SMB      107 Negotiate Protocol Request
12871 85.4071850 172.30.0.10 172.30.0.2   SMB      185 Negotiate Protocol Response
12880 86.7178370 172.30.0.2  172.30.0.10  SMB      107 Negotiate Protocol Request
12881 86.7195630 172.30.0.10 172.30.0.2   SMB      185 Negotiate Protocol Response
```

```
⊞ Frame 12850: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0
⊞ Ethernet II, Src: d6:14:02:38:a1:39 (d6:14:02:38:a1:39), Dst: ba:2f:9e:6d:77:ae (ba:2f:9e:6d:77:ae)
⊟ Internet Protocol Version 4, Src: 172.30.0.2 (172.30.0.2), Dst: 172.30.0.10 (172.30.0.10)
    Version: 4
    Header length: 20 bytes
  ⊟ Differentiated Services Field: 0x02 (DSCP 0x00: Default; ECN: 0x02: ECT(0) (ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..10 = Explicit Congestion Notification: ECT(0) (ECN-Capable Transport) (0x02)
    Total Length: 127
    Identification: 0x3ed0 (16080)
  ⊟ Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
```

```
0000  ba 2f 9e 6d 77 ae d6 14  02 38 a1 39 08 00 45 02   ./.mw... .8.9..E.
0010  00 7f 3e d0 40 00 80 06  00 00 ac 1e 00 02 ac 1e   ..>.@... ........
0020  00 0a 04 ae 01 bd e9 08  51 fa c6 61 88 31 50 18   ........ Q..a.1P.
0030  08 2c 58 ba 00 00 00 00  00 53 ff 53 4d 42 73 72   .,X..... .S.SMBsr
0040  00 00 c0 98 45 60 00 00  b4 21 9d 7c 98 f0 3e 8e   ....E`.. .!.|..>.
```



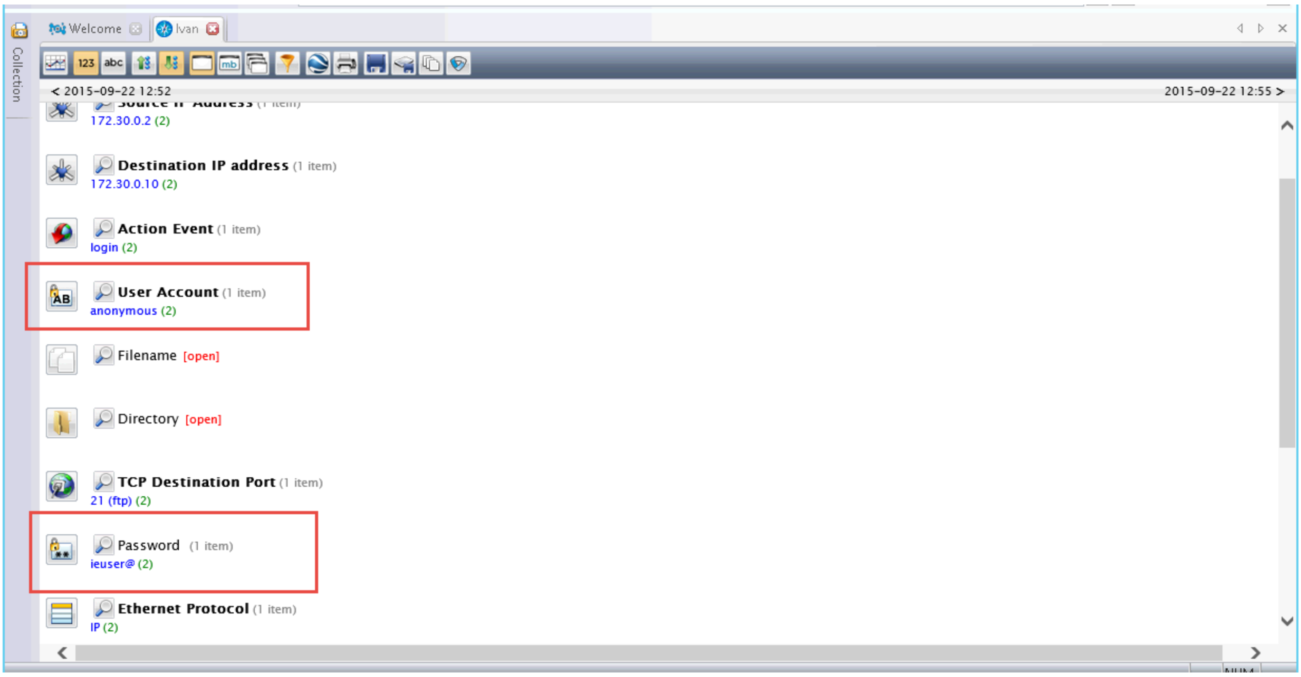
```
⊞ Frame 12850: 141 bytes on wire (1128 bits), 141 bytes captured (1128 bits) on interface 0
⊞ Ethernet II, Src: d6:14:02:38:a1:39 (d6:14:02:38:a1:39), Dst: ba:2f:9e:6d:77:ae (ba:2f:9e:6d:77:ae)
⊟ Internet Protocol Version 4, Src: 172.30.0.2 (172.30.0.2), Dst: 172.30.0.10 (172.30.0.10)
    Version: 4
    Header length: 20 bytes
  ⊟ Differentiated Services Field: 0x02 (DSCP 0x00: Default; ECN: 0x02: ECT(0) (ECN-Capable Transport))
      0000 00.. = Differentiated Services Codepoint: Default (0x00)
      .... ..10 = Explicit Congestion Notification: ECT(0) (ECN-Capable Transport) (0x02)
    Total Length: 127
    Identification: 0x3ed0 (16080)
  ⊟ Flags: 0x02 (Don't Fragment)
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (6)
  ⊟ Header checksum: 0x0000 [incorrect, should be 0x635e (may be caused by "IP checksum offload"?)]
      [Good: False]
    ⊟ [Bad: True]
      ⊟ [Expert Info (Error/Checksum): Bad checksum]
          [Message: Bad checksum]
          [Severity level: Error]
          [Group: Checksum]
    Source: 172.30.0.2 (172.30.0.2)
    Destination: 172.30.0.10 (172.30.0.10)
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
⊟ Transmission Control Protocol, Src Port: cajo-discovery (1198), Dst Port: microsoft-ds (445), Seq: 193, Ack: 167, Len: 87
    Source port: cajo-discovery (1198)
    Destination port: microsoft-ds (445)
    [Stream index: 5314]
    Sequence number: 193    (relative sequence number)
    [Next sequence number: 280    (relative sequence number)]
    Acknowledgment number: 167    (relative ack number)
    Header length: 20 bytes
  ⊞ Flags: 0x018 (PSH, ACK)
    Window size value: 2092
```

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.

## 3.2 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.



< 2015-09-22 12:52 2015-09-22 12:55 >

Source IP Address (1 item)
172.30.0.2 (2)

Destination IP address (1 item)
172.30.0.10 (2)

Action Event (1 item)
login (2)

User Account (1 item)
anonymous (2)

Filename [open]

Directory [open]

TCP Destination Port (1 item)
21 (ftp) (2)

Password (1 item)
ieuser@ (2)

Ethernet Protocol (1 item)
IP (2)

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.