Lab Report

1. Assessment Sheet
2. **Why would a network administrator use Ireshark and NetWitness Investigator together?**

Wireshark provides the packet-level capture ability and it is able to filter large amount of data quickly. People can understand full conversations among network systems through the usage of Wireshark. But its analysis is not easy to read and understand. NetWitness Investigator provides us a powerful ability to format the result of Wireshark which makes the analysis much easier. So, we prefer to use both tools together to make analysis effective.

1. **What was the IP address for LanSwitch1**

The IP address for LanSwitch1 is 172.16.8.5.

1. **When the 172.16.8.5 IP host responded to the ICMP echo-request, how many ICMP echo-reply packets were sent to the vWorkstation?**

There are total 4 ICMP echo-reply packets were sent to the vWrokstation and captured by Wireshark.

1. **What was the terminal password for LanSwitch 1 and LanSwitch 2?**

The terminal password for LanSwitch 1 and LanSwitch 2 are the same and this password is cisco.

1. **When using SSH to remotely access a Cisco router, can you see the terminal password? Why or why not?**

The terminal password is invisible if we use SSH to remotely connect a Cisco router. All the traffics send by SSH are encrypted instead of transmitting in a manner of clear-text.

1. **What were the Destination IP addresses discovered by the NetWitness Investigator analysis?**

The Destination IP addresses discovered by the NetWitness Investigator as follows:

172.30.0.15, 224.0.0.252, 172.30.0.2, 172.16.8.5, 172.16.0.225, 239.255.255.250, 224.0.0.22, 172.16.20.5

1. **Are packet-capturing tools like Wireshark less dangerous on switched LANs?**

Wireshark is so powerful that no matter which type of network we use, we can use it to capture all packets on one or several interfaces. If the traffic is not encrypted properly, for example not using SSH, through the capture results, we can know the clear text of password or file contents.

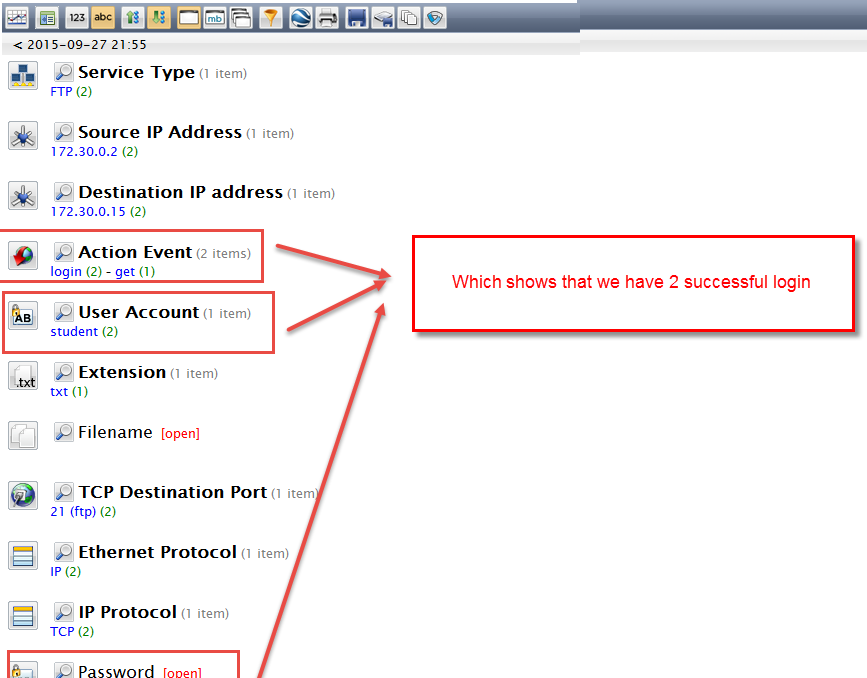
1. Challenge Questions

**Description: briefly describe your analysis of how the brute force password attack is recognizable in NetWitness Investigator. Use screen captures as appropriate to illustrate your finds**

By using Wireshark and NetWitness Investigator, I found there is a high possibility that our system on machine 172.16.8.5 is experiencing password brute force attack because we can see the abnormal communication traffics between Vworkstation desktop and our target IP 172.16.8.5.

1. The previous normal communication traffics

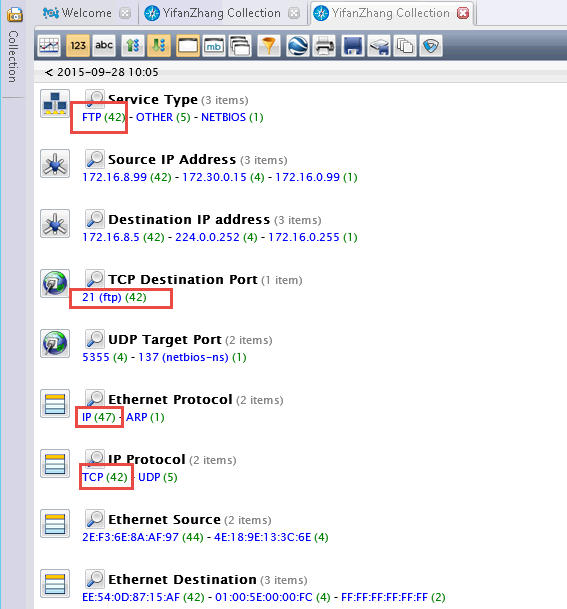
Figure 1. Normal login event screenshot



In the screen short of previous normal part lab result, we can see that there are only 2 FTP transmissions. And, when we drill down to the FTP service in NetWitness Investigator, we can see the Login Event along with the user login account and their password. It is quite normal for a system. We can take this roughly as a baseline.

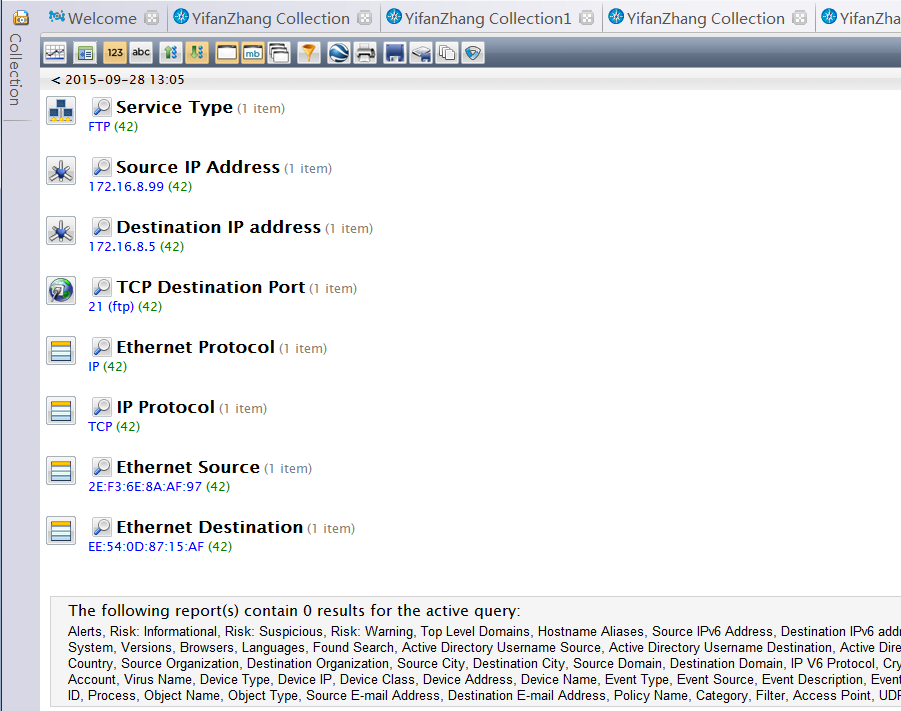
1. The abnormal communication traffics

Figure 2. Abnormal NetWitness Investigator Summary



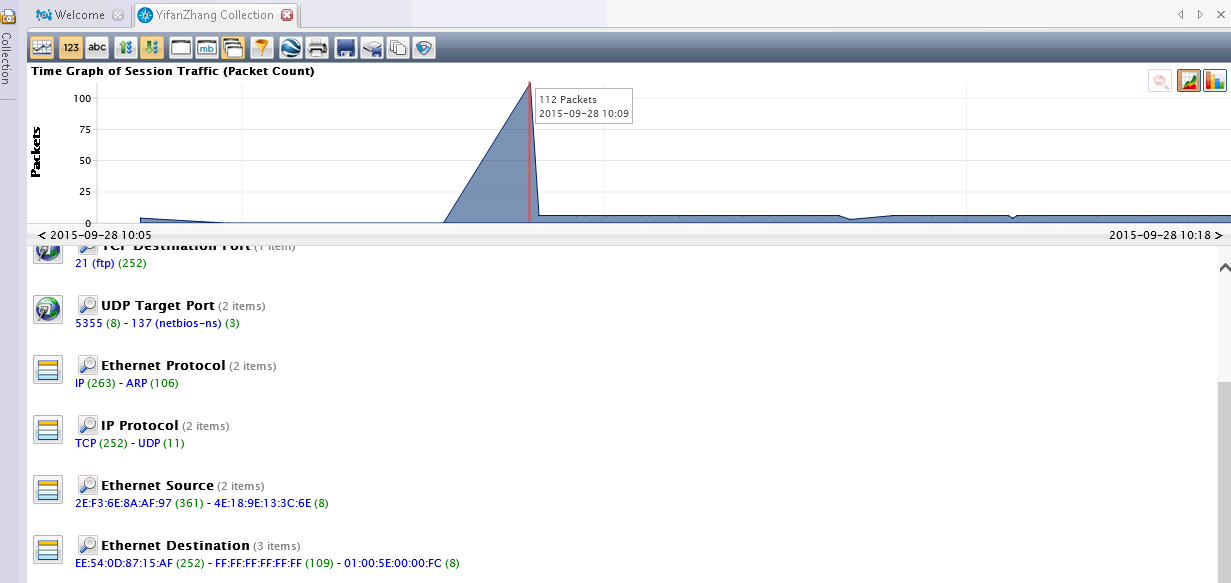
We can figure out in the summary page that there are totally 42 FTP sessions there. And, now we drill down to the FTP service to see the details as figure 2 shows.

Figure 3. Abnormal NetWitness Investigator FTP service details



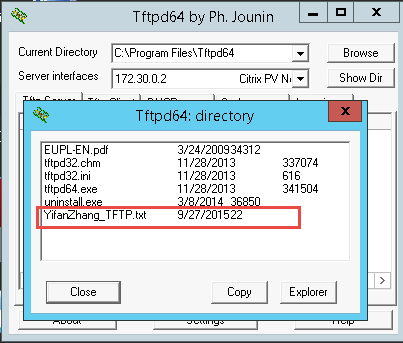
From the details showed in figure 3, we found that although there are 42 FTP sessions there, no any session is successfully logged in because we cannot see the login events along with user account and password information. It shows that there must be some suspicious communications between source IP address to destination IP address. There are two possible explanations at this time. One is that a user always mistypes the password and another is that someone is trying to brute force login password. So, in order to we check the packets count graph that is showed as follow figure – figure 4.

Figure 4. packet count graph



In figure 4, we see that there is a huge amount of packets that are sent and received within a quit short time. So, the normal user might not have the ability and patience to login in 42 times within a short time. Therefore, we can almost certain that our system on IP 172.16.8.5 are experiencing brute force attack.

1. Report Screenshot
2. Tftpd 64 Directory

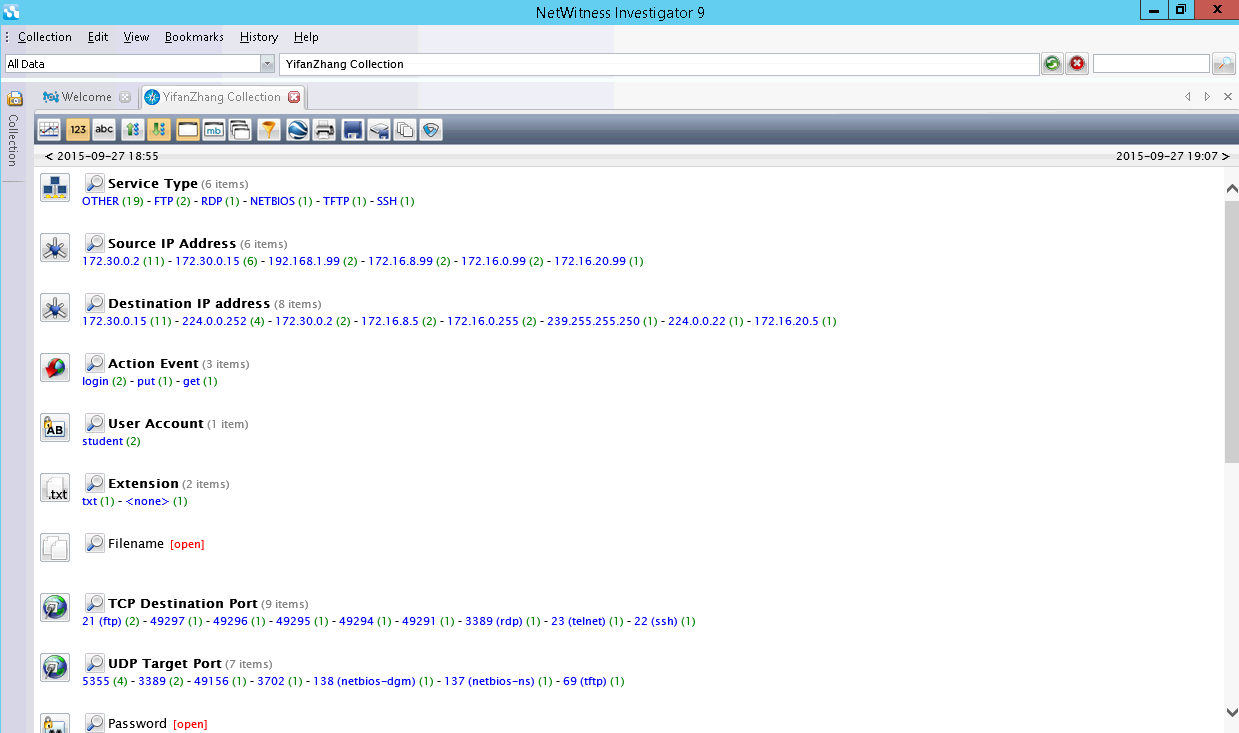


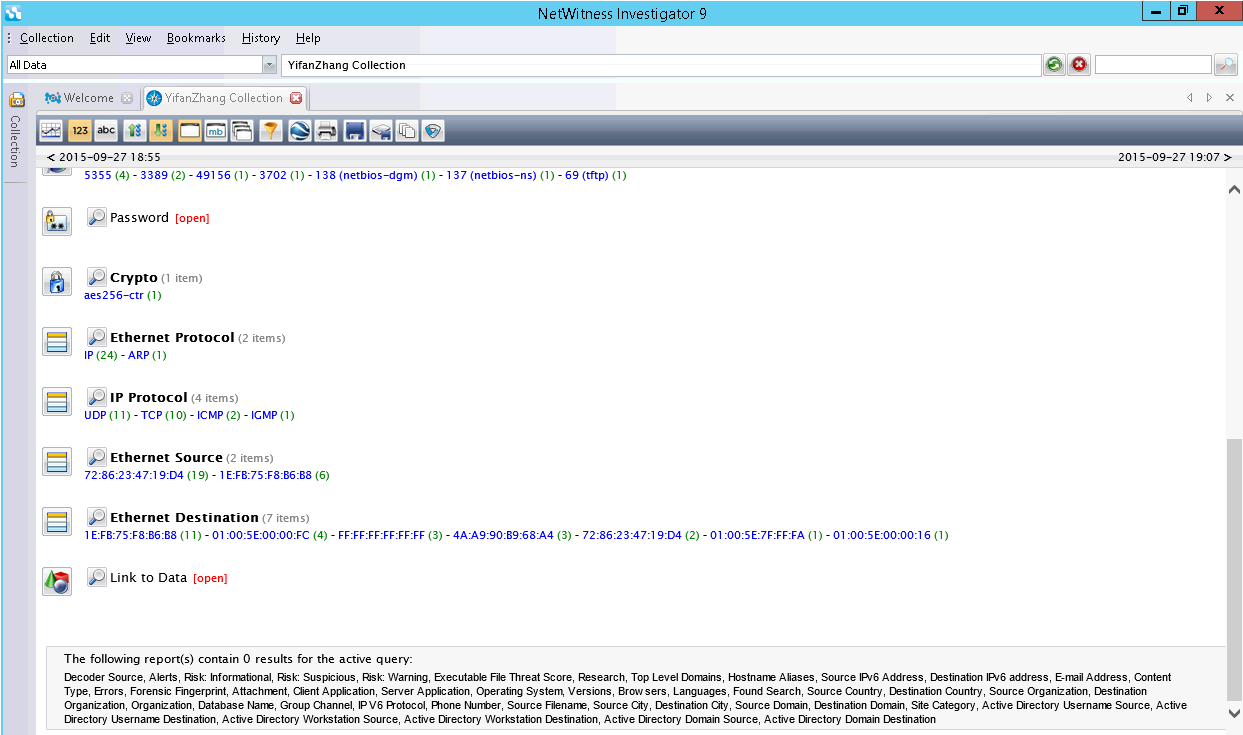
Explanation:

In this step, we use the following command to transfer a file to Tftpd64 client.

ftp 172.30.0.2 put c:\\users\administrator\desktop\YifanZhang\_TFTP.txt

1. NetWitness Investigator summary





Explanation:

This above two pictures shows that the categorized information from previous Wireshark dump file. We can see there are numerous information such as clear text password, protocols, source destination IP, action events, account, the way to encrypt communication and how many services are involved in the packets capture file ...etc.

1. Other additional supporting text/image content