Lab Report

1. Assessment Sheet
2. **Both Wireshark and NetWitness Investigator can be used for packet capture and analysis. Which tool is preferred for each task, and why?**

Wireshark is better suit for capture and otherwise, NetWitness Investigator is good at analysis. Particularly, the Wireshark doesn’t limit the number of protocol in capture but NetWitness Investigator has a limitation of 1G protocol capture per session. Although, Wireshark can be used to analysis the capture but NetWitness Investigator is a 7 layer protocol analyzer which we can see detailed protocol analysis and protocol behavior analysis.

1. **What is the significance of the TCP three-way handshake for applications that utilize TCP as transport protocol?**

The three-way handshake provides two significant features – securable and reliable (compare to UDP). Through three-way handshake, we can minimize the possibility that our data is compromised or even loss during the network transmission

1. **How many different source IP host addresses did you capture in your protocol capture?**

We have totally 9 source IP addresses which include IP 0.0.0.0. If we don’t count IP 0.0.0.0, we have 8 source IP host addresses in total.

1. **How many different protocols did your protocol capture session have? What function in Wireshark provides you with a breakdown of the different protocol types on the LAN segment?**

We have totally 11 protocols and the functionality to get protocol hierarchy in Wireshark is the protocol hierarchy command in statistic menu.

1. **How and where can you find Wireshark network traffic packet size counts? Can you distinguish how many of each packet size was transmitted on your LAN segment? Why is this important?**

We can find packets size through using the command packet lengths under statistic menu of Wireshark. Through this utility, we can easily see the packet length distribution which shows how many packets are in a particular packets length range. This distribution is important because it helps us to set up a baseline and identify suspicious activities. Normally, we don’t have too many packets falling in the large length range. For example, in packet length range 5120 – 4294967295, normally we have only 134 packets. But, if we find that there are 1000 or more packets falling into this range, there must be something happening in our system. So, we know that this is abnormal.

1. **Why is it important to use protocol capture tools and protocol analyzers as an information systems security professional?**

By using these protocol capture and analysis tools, we could make up a benchmark which can be used for experts to know which is the normal traffic and which is abnormal one. In addition, these tools help us to locate problems and respond to the problems as soon as possible.

1. **What are some challenges to baseline analysis?**

For baseline analysis, we met the following challenges: simplifying the data for better analysis, dealing with large-size capture file, working with multiple tools to gain an accurate perspective on the network.

1. **Why would an information systems security practitioner want to see network traffic on both internal and external network traffic?**

Monitor external network help us to see who and what is attempting to infiltrate our IP network. And, monitor internal network help us to identify which hosts might be compromised and what destination IP addresses internal employees are accessing.

1. **Which transactions in the lab used TCP as a transport protocol? Which used UDP? Which ports were used in the lab?**

TCP: Telnet (port 23), SSH (port 21), rdp (3389)

UDP: netbios-dgm (port 138), NetBIOS name service –netbios-ns (port 137), TFTP (port 69)

1. Challenge Questions

**Description: use information in this lab and your own research, explain how you might create a baseline definition for the network in this lab. Was the capture file created in this lab enough data to create a baseline? How can a baseline help identify suspicious activities on the network.**

1. Explain how you might create a baseline definition for the network in this lab?

With the information obtained in this lab, I will make a baseline like the followings. First, the most important thing is to monitor the traffic. I would run Wireshark and NetWitness Investigator when everything is normally operating on that network. From the report, I can know how much the normal traffic is and then I would be able to set a threshold based on the normal traffic. For instance, if the normal traffic is 100 packets per second, I will make the baseline to 120 packets per second. Secondly, I will make the baseline on packets length. From the functionality of Wireshark, we can get the packets length distribution. Same as traffic, I will firstly get a normal packets length distribution as a baseline and secondly monitor the network to see whether the packets length distribution has a bigger variation. Lastly, I will make a baseline of ports opening and services types. From the report of NetWitness Investigator, we can know the overall situation of ports and services. So, same as previous two baselines, I first obtain the normal open ports and available services, then I will keep monitor the network to see whether there are some big changes. For instance, if normally the server only opens port 80 for HTTP request, but abnormally when we monitor the server, we found that the port 3389 used for remote login is opening. This means that we are facing risks and somebody might attack this server in the future.

So, according to above analysis, we have four baseline elements and they are packets counts per second (network traffic), packets length distribution, ports opening and services availability.

1. Was the capture file created in this lab enough data to create a baseline?

No, a baseline is not limited only on technical aspect but also some sociology aspect such as policies, rules, laws and so on. So, the Capture files in this lab only can help us to make technical baseline but not the baseline of other parts.

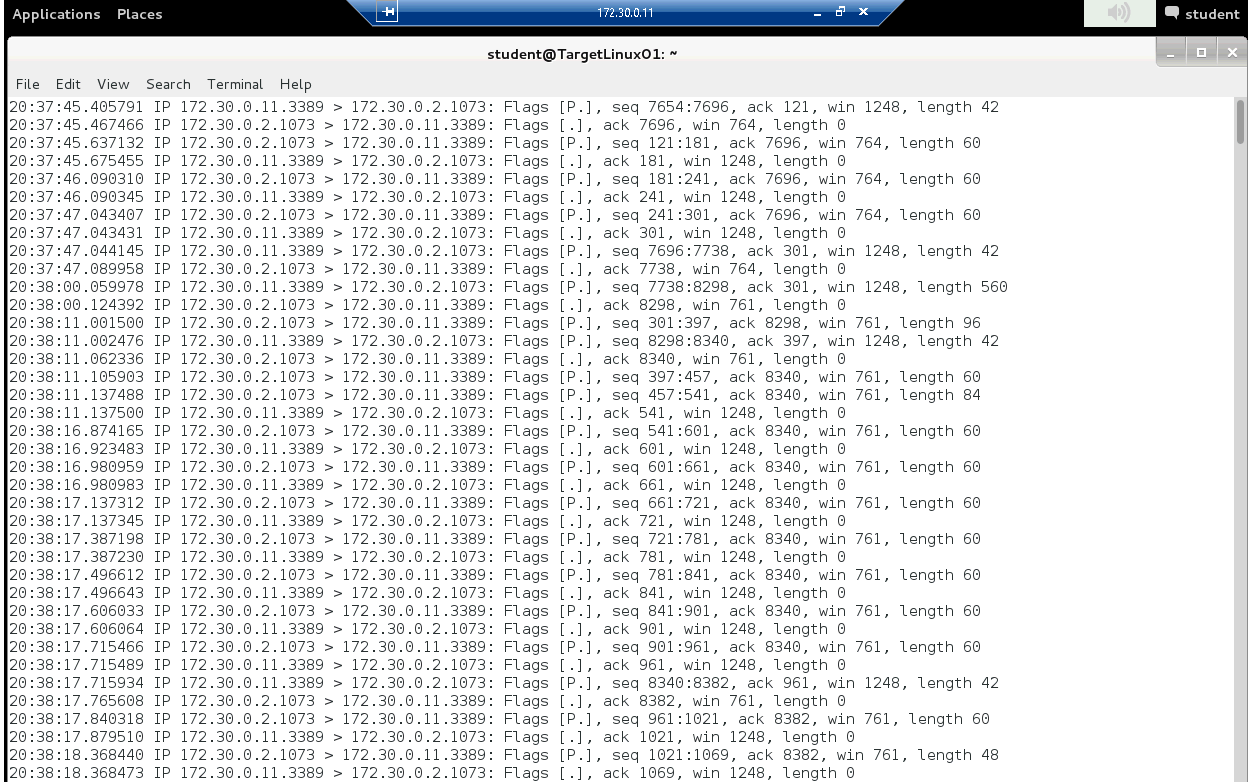
1. How can a baseline help identify suspicious activities on the network?

A baseline helps us to identify which activities are normal and which activities are suspicious. A baseline can make experts well-prepared for attacks in the future. Once we know that something suspicious happens, then we can quickly respond to them in order to reduce losses. For example, if normally the traffic between two hosts is 100 packets, but someone you find that the traffic between those two hosts becomes to 10000 packets, and then we can judge that there must be some unusual things are taking place between the two hosts.

1. Report Screenshot

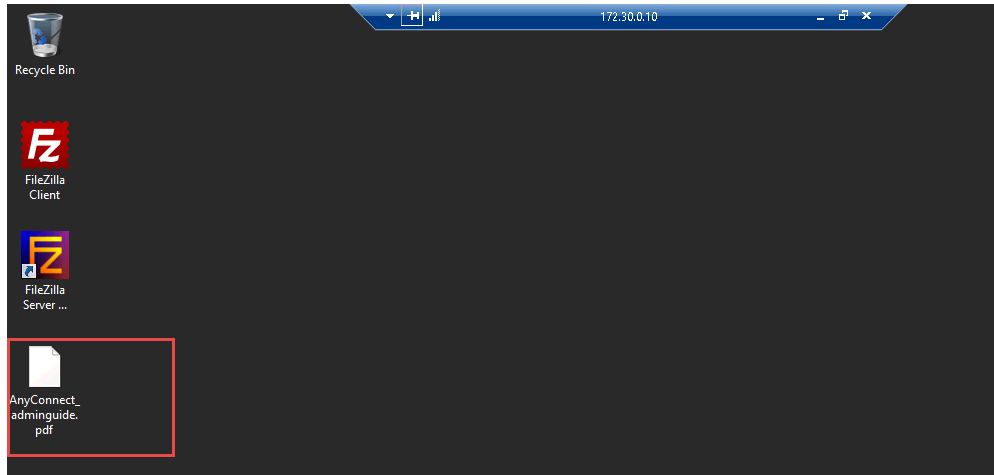
# Result of tcpdump in Linux (Kali)

Figure 1. tcpdump results

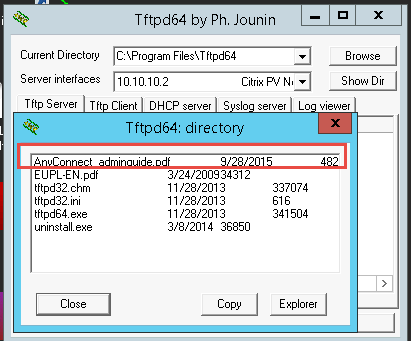


Note: because the tcpdump scan result is too long, so here we just show the first part of the result.

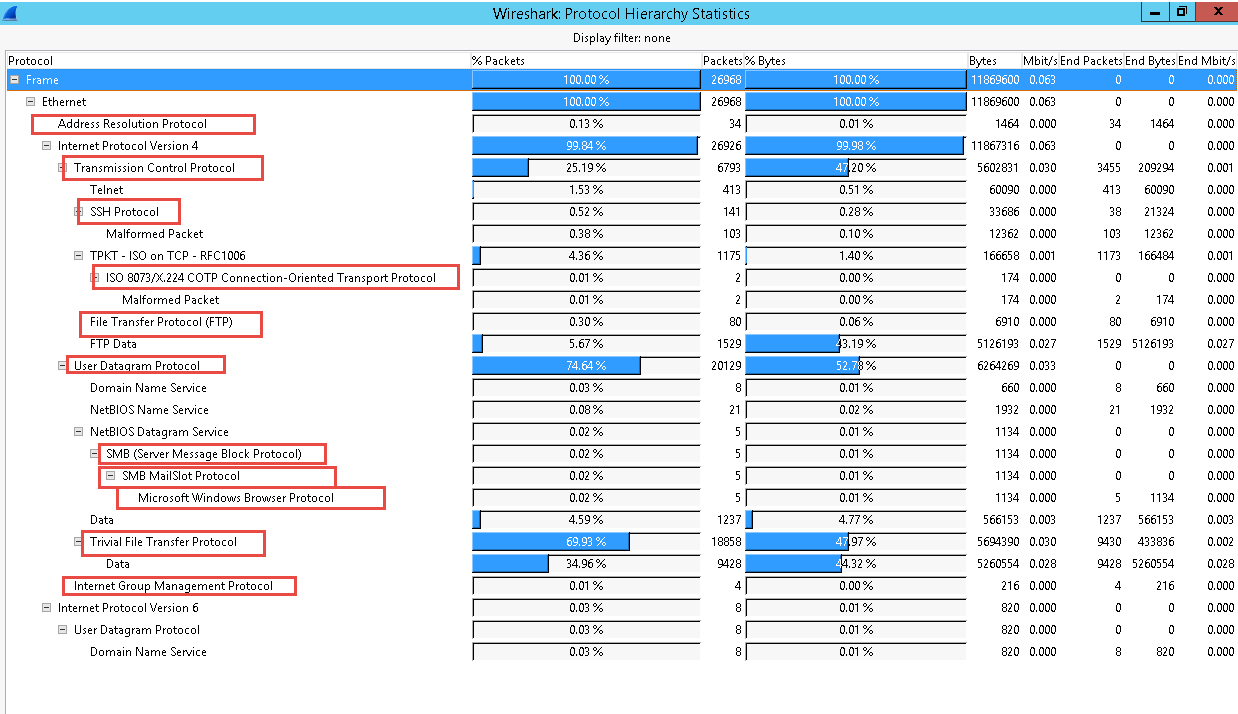
# AnyConnect\_adminguide.pdf on the targetWindows01 desktop



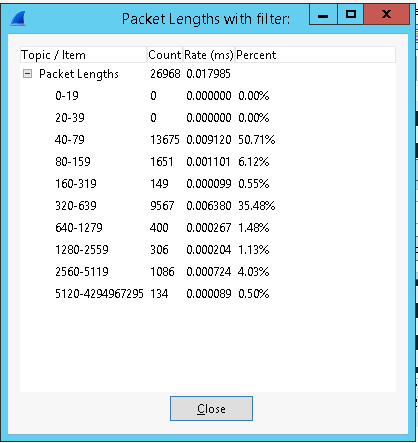
# Transferred file in the Tftp64 directory



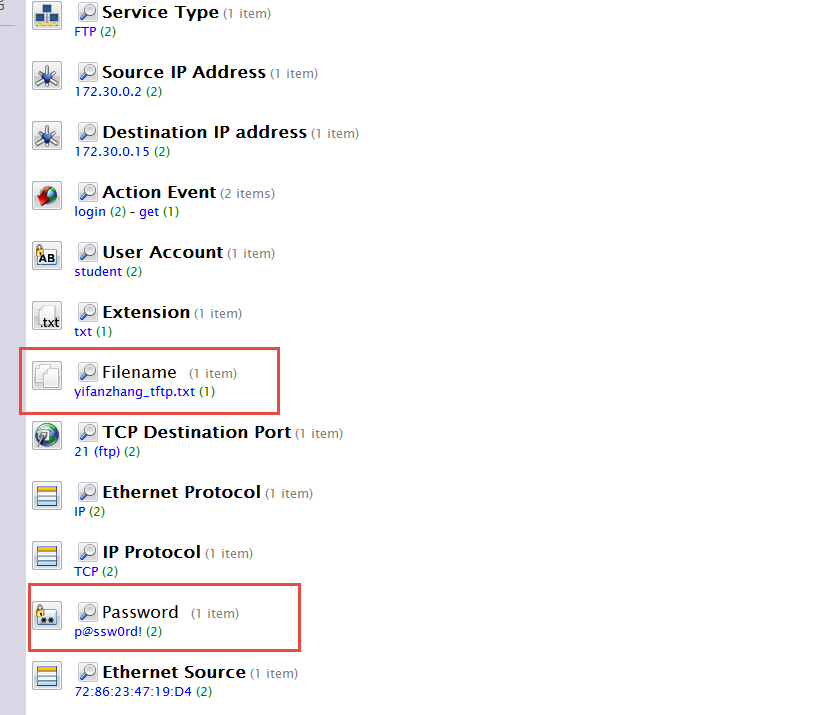
# Protocol Hierarchy Statistics



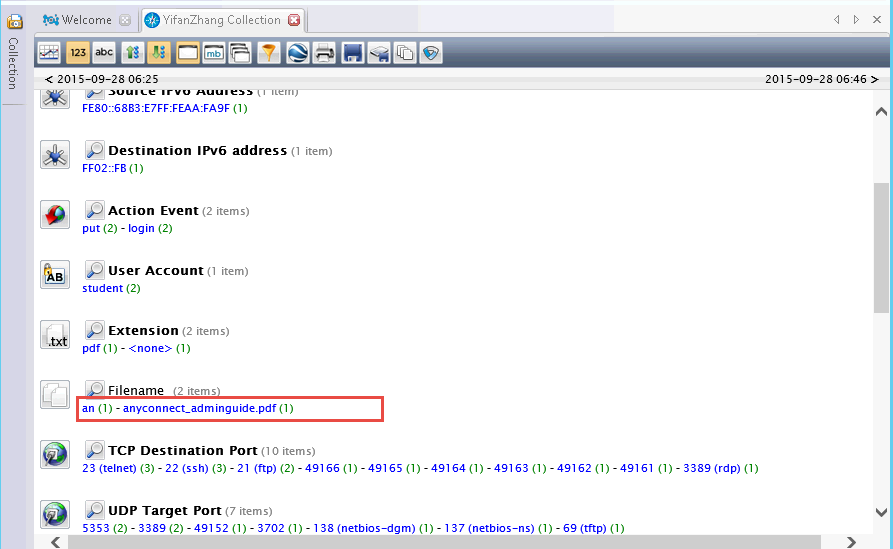
# Packet Lengths distribution



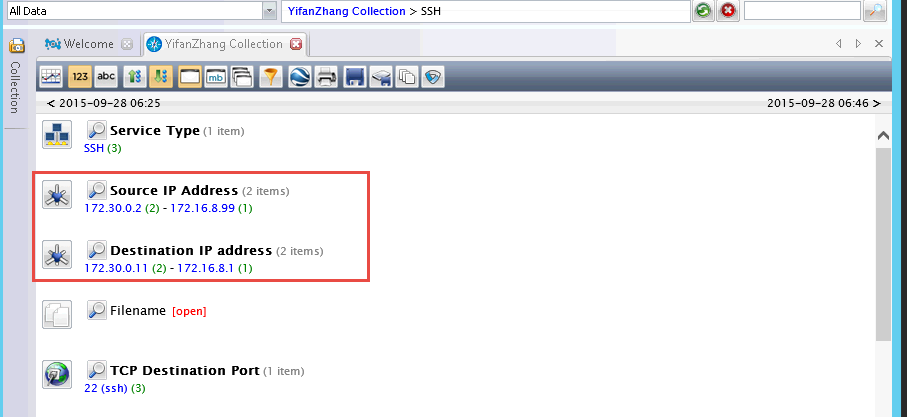
# Password and filename used in the FTP transfer

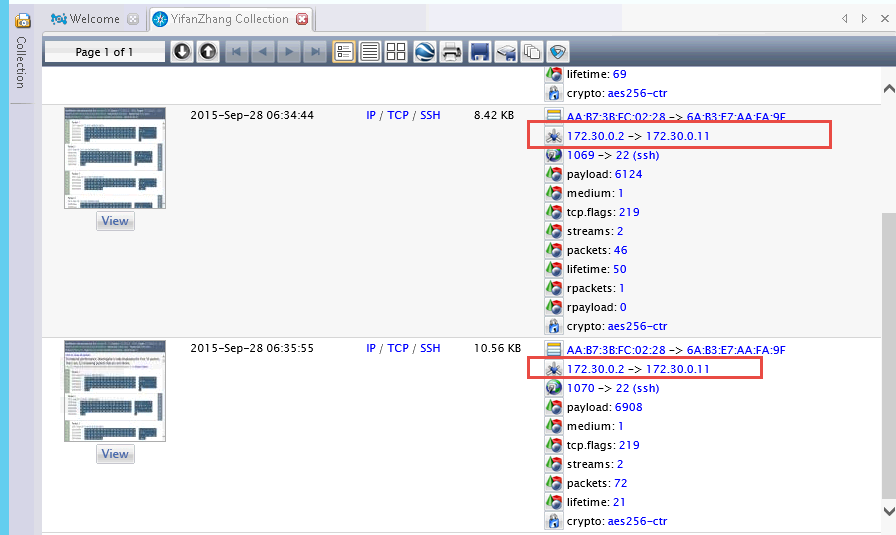


# Filename used in the TFTP file transfer



# IP addresses for the SSH sessions





Explanation:

From the above three pictures, we can see that there are total 3 ssh sessions and 4 IP addresses involved. Their IP addresses are 172.30.0.2, 172.30.0.11, 172.16.8.99 and 172.16.8.1.

1. Other additional supporting text/image content