Challenge Lab 5 Report

1. Challenge questions Description:

Briefly describe your analysis of how the brute force password attack is recognizable in NetWitness Investigator.

2. Tools used in this report:

In this report, we use the following two tools to analyze the potential password brute force.

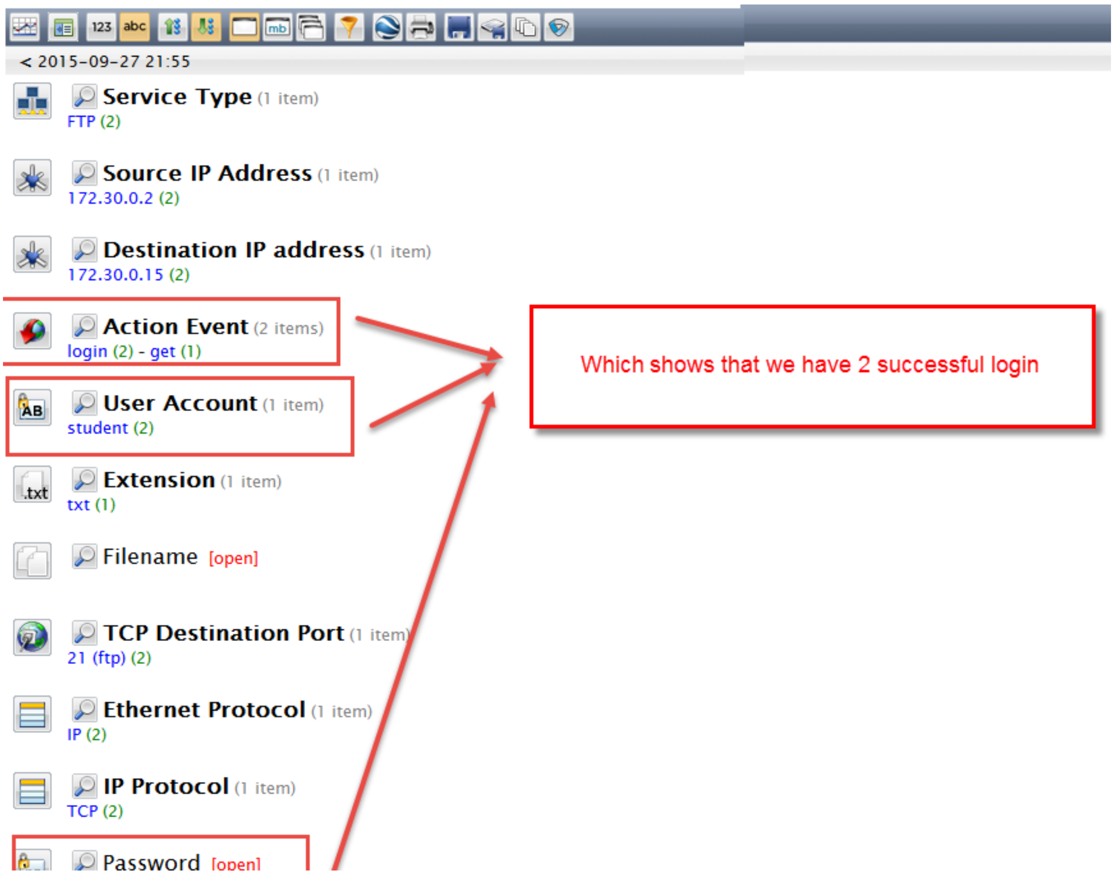
- Wireshark -> Capture all the packets
- NetWitness Investigator -> Visualize the result of Wireshark.

3. Analysis Report

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.

3.1 The previous normal communication traffics

Figure 1. Normal login event screenshot



< 2015-09-27 21:55

Service Type (1 item)
FTP (2)

Source IP Address (1 item)
172.30.0.2 (2)

Destination IP address (1 item)
172.30.0.15 (2)

Action Event (2 items)
login (2) - get (1)

User Account (1 item)
student (2)

Extension (1 item)
txt (1)

Filename [open]

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

Ethernet Protocol (1 item)
IP (2)

IP Protocol (1 item)
TCP (2)

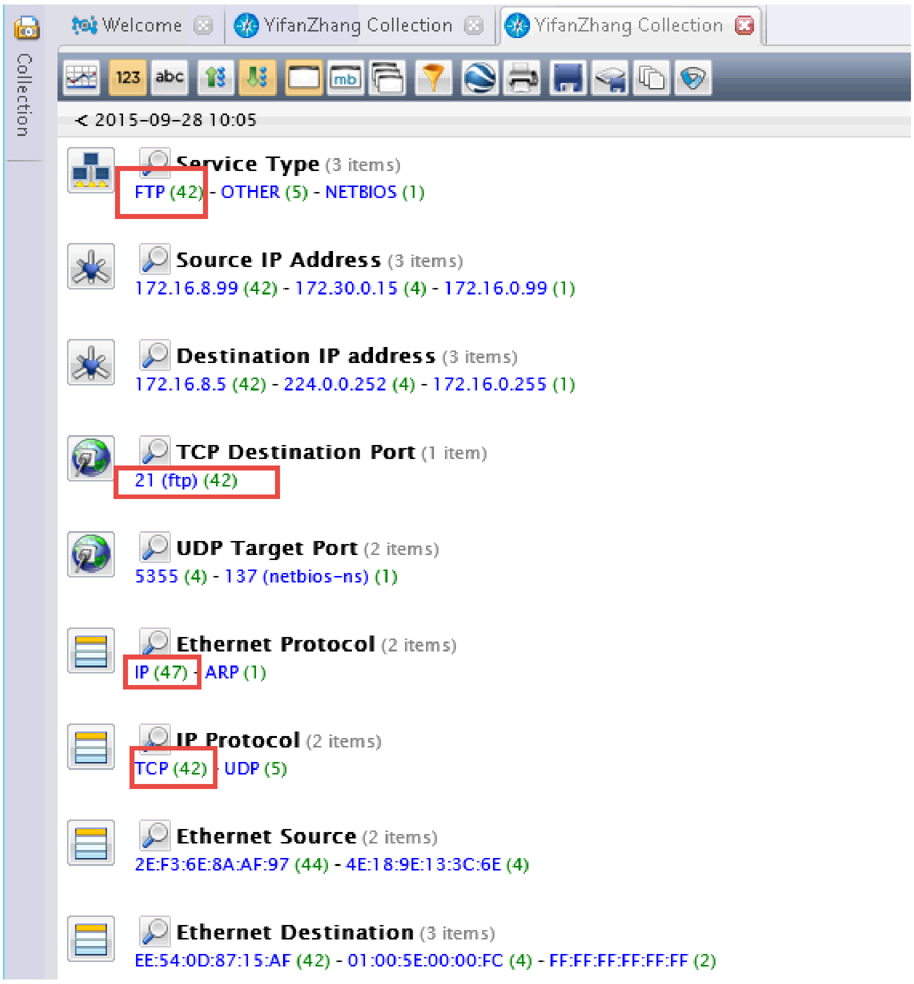
Password [open]

Which shows that we have 2 successful login

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.

3.2 The abnormal communication traffics

Figure 2. Abnormal NetWitness Investigator Summary



< 2015-09-28 10:05

Service Type (3 items)
FTP (42) - OTHER (5) - NETBIOS (1)

Source IP Address (3 items)
172.16.8.99 (42) - 172.30.0.15 (4) - 172.16.0.99 (1)

Destination IP address (3 items)
172.16.8.5 (42) - 224.0.0.252 (4) - 172.16.0.255 (1)

TCP Destination Port (1 item)
21 (ftp) (42)

UDP Target Port (2 items)
5355 (4) - 137 (netbios-ns) (1)

Ethernet Protocol (2 items)
IP (47) - ARP (1)

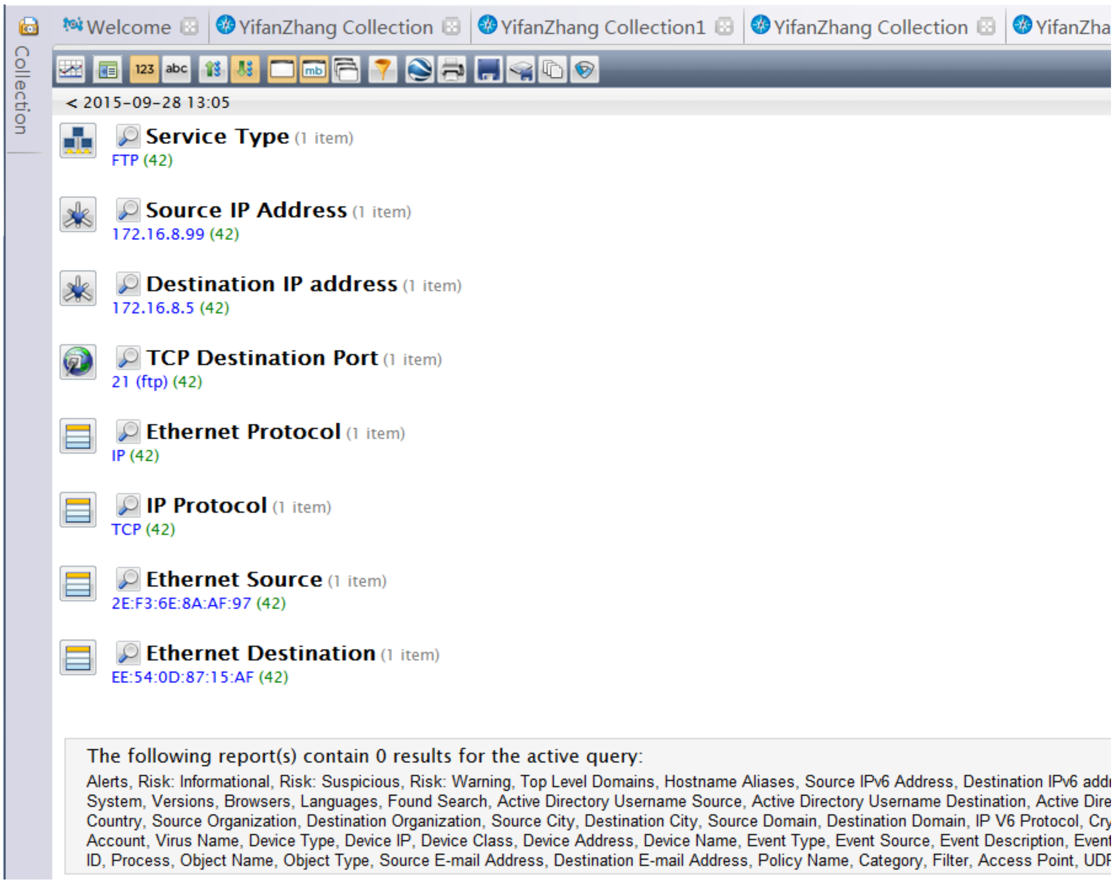
IP Protocol (2 items)
TCP (42) - UDP (5)

Ethernet Source (2 items)
2E:F3:6E:8A:AF:97 (44) - 4E:18:9E:13:3C:6E (4)

Ethernet Destination (3 items)
EE:54:0D:87:15:AF (42) - 01:00:5E:00:00:FC (4) - FF:FF:FF:FF:FF:FF (2)

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



< 2015-09-28 13:05

Service Type (1 item)
FTP (42)

Source IP Address (1 item)
172.16.8.99 (42)

Destination IP address (1 item)
172.16.8.5 (42)

TCP Destination Port (1 item)
21 (ftp) (42)

Ethernet Protocol (1 item)
IP (42)

IP Protocol (1 item)
TCP (42)

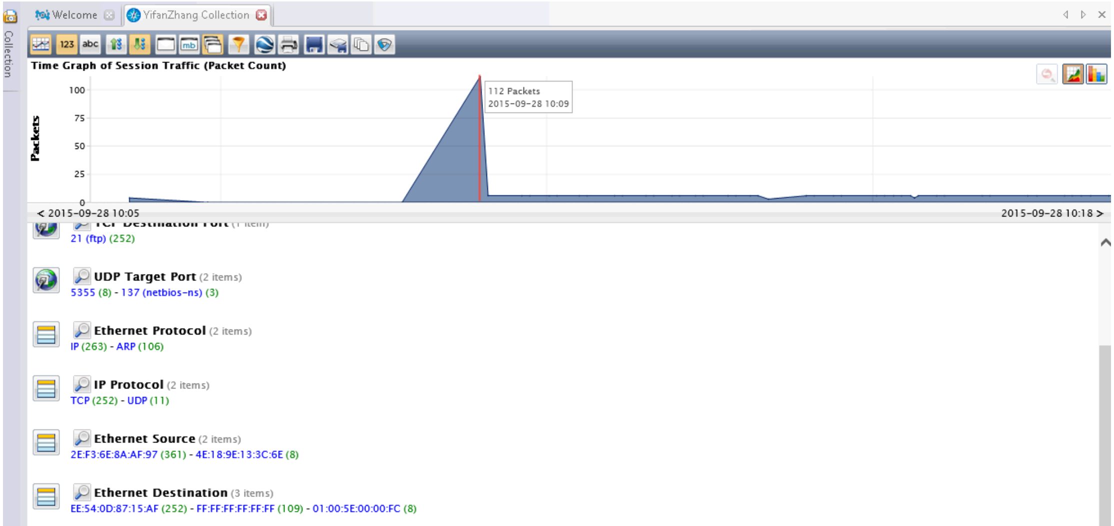
Ethernet Source (1 item)
2E:F3:6E:8A:AF:97 (42)

Ethernet Destination (1 item)
EE:54:0D:87:15:AF (42)

The following report(s) contain 0 results for the active query:
Alerts, Risk: Informational, Risk: Suspicious, Risk: Warning, Top Level Domains, Hostname Aliases, Source IPv6 Address, Destination IPv6 addı
System, Versions, Browsers, Languages, Found Search, Active Directory Username Source, Active Directory Username Destination, Active Dire
Country, Source Organization, Destination Organization, Source City, Destination City, Source Domain, Destination Domain, IP V6 Protocol, Cry
Account, Virus Name, Device Type, Device IP, Device Class, Device Address, Device Name, Event Type, Event Source, Event Description, Event
ID, Process, Object Name, Object Type, Source E-mail Address, Destination E-mail Address, Policy Name, Category, Filter, Access Point, UDF

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



TCP Destination Port (1 item)
21 (ftp) (252)

UDP Target Port (2 items)
5355 (8) - 137 (netbios-ns) (3)

Ethernet Protocol (2 items)
IP (263) - ARP (106)

IP Protocol (2 items)
TCP (252) - UDP (11)

Ethernet Source (2 items)
2E:F3:6E:8A:AF:97 (361) - 4E:18:9E:13:3C:6E (8)

Ethernet Destination (3 items)
EE:54:0D:87:15:AF (252) - FF:FF:FF:FF:FF:FF (109) - 01:00:5E:00:00:FC (8)

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.