Lab1 report

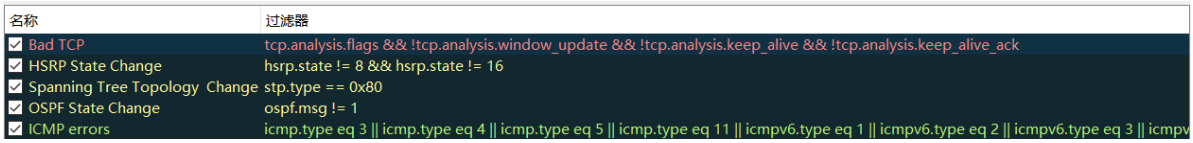
11912039 郑鑫颖

1. **Carefully read the lab instructions and finish all tasks above.**

   Finished!

2. **If a packet is highlighted by black, what does it mean for the packet?**

   The black shows that the TCP packages have some problem such as being delieved out of order or having OSPF state change, etc.



名称	过滤器
Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack
HSRP State Change	hsrp.state != 8 && hsrp.state != 16
Spanning Tree Topology Change	stp.type == 0x80
OSPF State Change	ospf.msg != 1
ICMP errors	icmp.type eq 3 || icmp.type eq 4 || icmp.type eq 5 || icmp.type eq 11 || icmpv6.type eq 1 || icmpv6.type eq 2 || icmpv6.type eq 3 || icmpv

3. **What is the filter command for listing all outgoing http traffic?**

   http and ip.src==10.17.24.110（host ip）

4. **Why does DNS use Follow UDP Stream while HTTP use Follow TCP Stream?**

   1.DNS provide the transformation between the domain name and the ip name.

   It has a relatively heavy load and UDP is much faster than HTTP.

   DNS requests are usually very tiny (url and ip are short), so they have no problems fitting into the UDP segments.

   Also, UDP support more than one client.

   2.HTTP is used when user requests something from web.

   Http needs to ensure the correctness and reliability of the content and TCP requests three times shakehands and if lost the package, it needs retransmisson, which meet the needs of the Http.

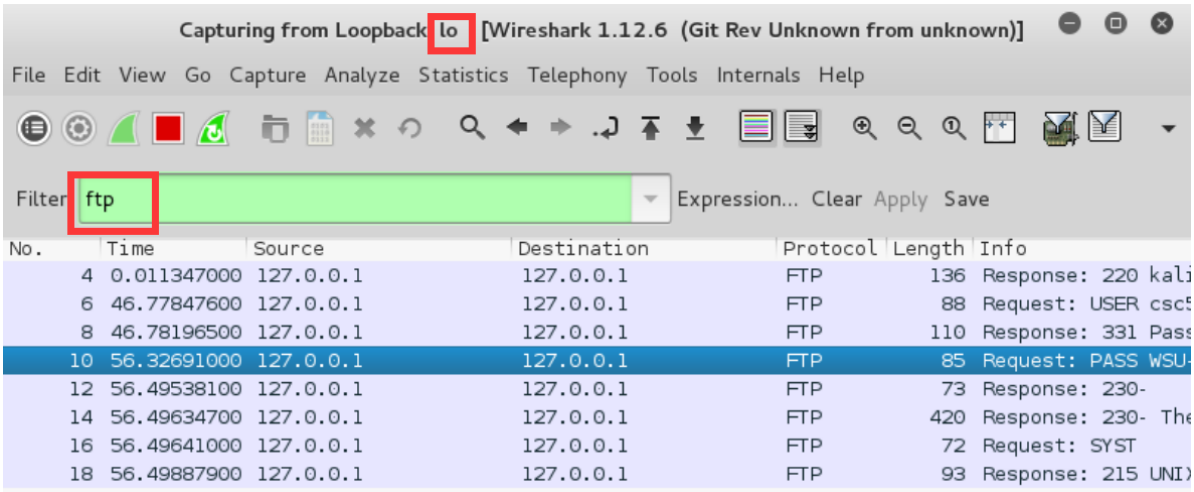
   The package for Http is sometimes very big (>1G), it cannot be fit into a UDP package.

5. **Using Wireshark to capture the FTP password.**

   Firstly: use command to log into the FTP systerm.

```
root@kali-WSU:~# ftp 127.0.0.1
Connected to 127.0.0.1.
220 kali-WSU FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
Name (127.0.0.1:root): csc5991-student
331 Password required for csc5991-student.
Password:
230-
230- The programs included with the Kali GNU/Linux system are free software;
230- the exact distribution terms for each program are described in the
230- individual files in /usr/share/doc/*/copyright.
230-
230- Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
230- permitted by applicable law.
230 User csc5991-student logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Secondly, use wireshark to capture the package and use "ftp" as filter command.



Lastly, we can see the usename and password in th Info.