

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 delivered out of order or having OSPF state change, etc.

名称	过滤器
<input checked="" type="checkbox"/> Bad TCP	<code>tcp.analysis.flags && !tcp.analysis.window_update && !tcp.analysis.keep_alive && !tcp.analysis.keep_alive_ack</code>
<input checked="" type="checkbox"/> HSRP State Change	<code>hsrp.state != 8 && hsrp.state != 16</code>
<input checked="" type="checkbox"/> Spanning Tree Topology Change	<code>stp.type == 0x80</code>
<input checked="" type="checkbox"/> OSPF State Change	<code>ospf.msg != 1</code>
<input checked="" type="checkbox"/> ICMP errors	<code>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 icmpv6.type eq 4 icmpv6.type eq 5 icmpv6.type eq 11 icmpv6.type eq 12 icmpv6.type eq 13 icmpv6.type eq 14 icmpv6.type eq 15 icmpv6.type eq 16 icmpv6.type eq 17 icmpv6.type eq 18 icmpv6.type eq 19 icmpv6.type eq 20 icmpv6.type eq 21 icmpv6.type eq 22 icmpv6.type eq 23 icmpv6.type eq 24 icmpv6.type eq 25 icmpv6.type eq 26 icmpv6.type eq 27 icmpv6.type eq 28 icmpv6.type eq 29 icmpv6.type eq 30 icmpv6.type eq 31</code>

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 retransmission, 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 system.

```

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.

Capturing from Loopback **lo** [Wireshark 1.12.6 (Git Rev Unknown from unknown)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter **ftp** Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4	0.011347000	127.0.0.1	127.0.0.1	FTP	136	Response: 220 kali
6	46.77847600	127.0.0.1	127.0.0.1	FTP	88	Request: USER csc5
8	46.78196500	127.0.0.1	127.0.0.1	FTP	110	Response: 331 Pass
10	56.32691000	127.0.0.1	127.0.0.1	FTP	85	Request: PASS WSU-
12	56.49538100	127.0.0.1	127.0.0.1	FTP	73	Response: 230-
14	56.49634700	127.0.0.1	127.0.0.1	FTP	420	Response: 230- The
16	56.49641000	127.0.0.1	127.0.0.1	FTP	72	Request: SYST
18	56.49887900	127.0.0.1	127.0.0.1	FTP	93	Response: 215 UNI

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

Info

Response: 220 kali-WSU FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.

Request: **USER csc5991-student**

Response: 331 Password required for csc5991-student.

Request: **PASS WSU-csc5991.**

Response: 230-

Response: 230- The programs included with the Kali GNU/Linux system are free software;

Request: SYST

Response: 215 UNIX Type: L8 (Linux)