

1. Finished
2. Means error or other

名称	过滤器
<input checked="" type="checkbox"/> Bad TCP	tcp.analysis.flags && !tcp.analysis.window_update
<input checked="" type="checkbox"/> HSRP State Change	hsrp.state != 8 && hsrp.state != 16
<input checked="" type="checkbox"/> Spanning Tree Topology Change	stp.type == 0x80
<input checked="" type="checkbox"/> OSPF State Change	ospf.msg != 1
<input checked="" type="checkbox"/> 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 icmpv6.type eq 4
<input checked="" type="checkbox"/> ARP	arp
<input checked="" type="checkbox"/> ICMP	icmp icmpv6
<input checked="" type="checkbox"/> TCP RST	tcp.flags.reset eq 1
<input checked="" type="checkbox"/> SCTP ABORT	sctp.chunk_type eq ABORT
<input checked="" type="checkbox"/> TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !ipim && !ospf) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp carp))
<input checked="" type="checkbox"/> Checksum Errors	eth.fcsh.status == "Bad" ip.checksum.status == "Bad" tcp.checksum.status == "Bad" udp.checksum.status == "Bad" sctp.checksum.status == "Bad" mstp.checksum.status == "Bad"
<input checked="" type="checkbox"/> SMB	smb nbss nbns netbios
<input checked="" type="checkbox"/> HTTP	http tcp.port == 80 http2
<input checked="" type="checkbox"/> DCERPC	dcerpc
<input checked="" type="checkbox"/> Routing	hsrp eigrp ospf bgp cdp vrrp carp gvrp igmp ismp
<input checked="" type="checkbox"/> TCP SYN/FIN	tcp.flags & 0x02 tcp.flags.fin == 1
<input checked="" type="checkbox"/> TCP	tcp
<input checked="" type="checkbox"/> UDP	udp
<input checked="" type="checkbox"/> Broadcast	eth[0] & 1
<input checked="" type="checkbox"/> System Event	systemd_journal sysdig

3. http.request==1 and http

#	Time	Source	Destination	Protocol	Length	Info
14	0.376163	10.17.64.229	183.60.137.245	HTTP	318	GET /pc/misc/files/20140513/files/b4d0f0710c4a0742a5606966b8213f4.png HTTP/1.1
51	1.826790	10.17.64.229	140.206.78.195	HTTP	520	POST /cloudquery.php HTTP/1.1
80	1.471734	10.17.64.229	125.94.49.78	HTTP	284	GET /qqweb/qunactivity/img/icon_qq_2014.png HTTP/1.1

4. 因为 DNS 只是查询 ip 值，要求 DNS 要快，而因为只传输 ip 值，包小，对完整性的要求不高，所以 DNS 用 UDP 协议。然而 HTTP 要求传输的数据要完整，所以用 HTTP 用 TCP 协议。
5. 第一步，打开 wireshark 准备抓包
第二步，使用密码连接 ftp 服务器

```

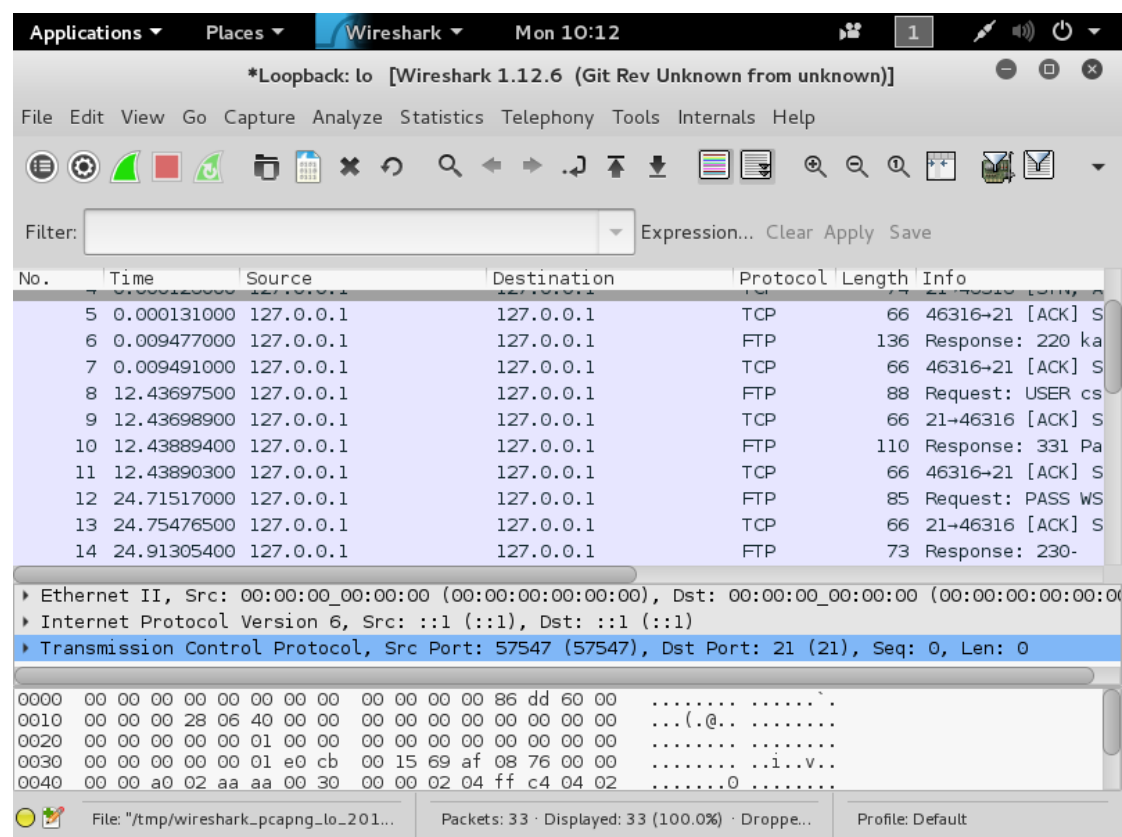
Applications ▾ Places ▾ Terminal ▾ Mon 10:11
root@kali-WSU: ~

File Edit View Search Terminal Help

Connected to localhost.
220 kali-WSU FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
Name (localhost:root): csc5991-student
331 Password required for csc5991-student.
Password:
530 Login incorrect.
Login failed.
ftp> ^Z
[1]+  Stopped                  ftp localhost
root@kali-WSU:~# ftp localhost
ftp: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
220 kali-WSU FTP server (Version 6.4/OpenBSD/Linux-ftpd-0.17) ready.
Name (localhost: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>

```

第三步，停止 wireshark 抓包



第四步，使用过滤命令过滤包，并得到含有 pass 的传送出去的 ftp 报文。

