

wireshark抓包实验 分析 详解

转载

淘豆豆么 于 2011-10-11 20:21:26 发布 8816 收藏 3
分类专栏: [Tool 常用debug](#) 文章标签: [dst internet networking url class 网络](#)



[Tool](#) 同时被 2 个专栏收录

31 篇文章 0 订阅
订阅专栏



[常用debug](#)

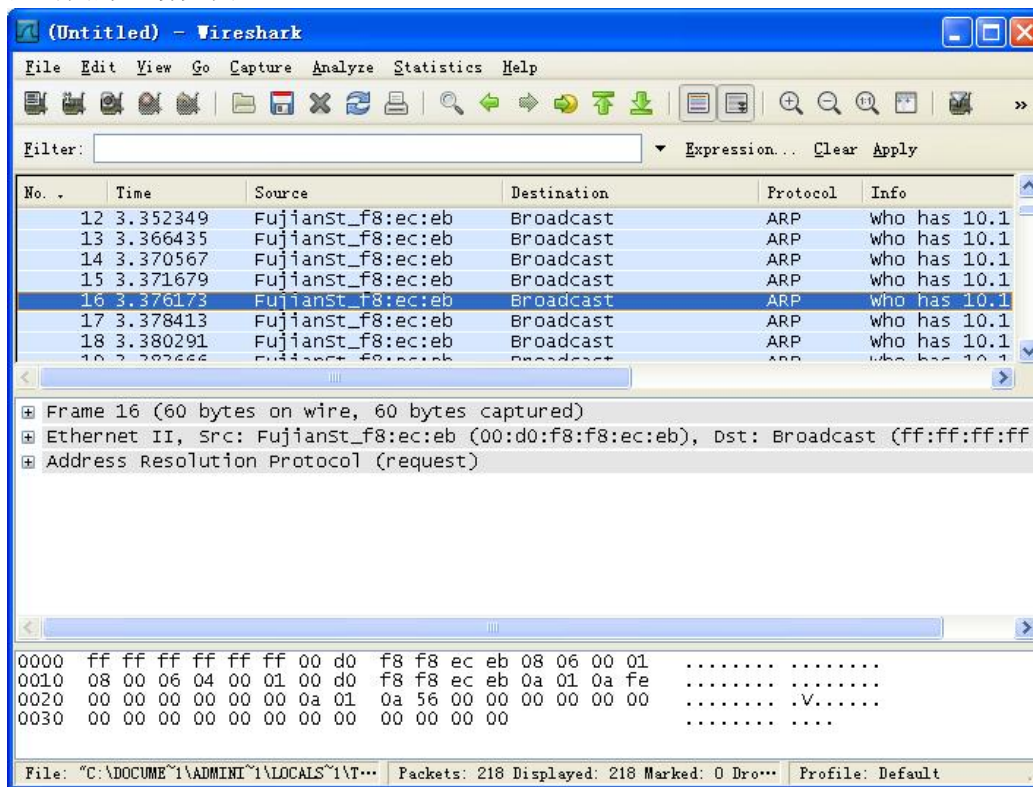
14 篇文章 0 订阅
订阅专栏

Wireshark(Formerly Ethereal) is an award-winning network protocol analyzer developed by an international team of networking experts.

WireShark是一款很好的抓包工具，我们今天用它来做几个实验，复习一下网络基础知识。

- 1、安装WireShark。这个不用说了，中间会提示安装WinPcap,一切都是默认。
- 2、实验前把网络断一下（关掉联网的软件），防止产生一些不必要的流量，不利于分析。
- 3、ok。打开WireShark,选择"Capture>>Interfaces",选择自己的网卡（物理网卡，如果装了，VM或是VPN软件，会产生很多虚拟网卡，但软件不使用时，流量是零）。选择"Start"开始监控流量。
- 4.HTTP协议分析。迅速打开一个网页，因为我是在局域网环境下，ARP广播较多。然后选择"Stop The running live capture"停止抓包。截图一。

点击图片查看大图！



抓包过程中发现UDP组播、ARP广播等。

A.组播分析.

Ethernet II帧,

Src: RealtekS_46:f2:4f (00:e0:4c:46:f2:4f), Dst:IPv4mcast_66:74:6e (01:00:5e:66:74:6e).

源地址RealtekS, 目的地址IPv4mcast 66:74:6e.

Internet Protocol(IP数据包),

Src: 10.1.10.154 (10.1.10.154), Dst: 225.102.116.110(225.102.116.110)这个不用说吧。

User Datagram Protocol(UDP数据包), Src Port: irisa (11000), Dst Port: irisa (11000)。

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.10.154	225.102.116.110	UDP	Source port: irisa Destination port: irisa
2	0.000622	10.1.10.171	225.102.116.110	UDP	Source port: irisa Destination port: irisa
3	0.000679	10.1.10.29	225.102.116.110	UDP	Source port: irisa Destination port: irisa
4	0.001084	10.1.10.29	225.102.116.110	UDP	Source port: irisa Destination port: irisa
5	0.001302	10.1.10.154	225.102.116.110	UDP	Source port: irisa Destination port: irisa
6	0.001472	10.1.10.171	225.102.116.110	UDP	Source port: irisa Destination port: irisa
7	0.262166	Micro-St_cb:0a:ef	Broadcast	ARP	who has 10.1.10.137? Tell 10.1.10.113

Frame 5 (66 bytes on wire, 66 bytes captured)
Ethernet II, Src: RealtekS_46:f2:4f (00:e0:4c:46:f2:4f), Dst: IPv4mcast_66:74:6e (01:00:5e:66:74:6e)
Internet Protocol, Src: 10.1.10.154 (10.1.10.154), Dst: 225.102.116.110 (225.102.116.110)
User Datagram Protocol, Src Port: irisa (11000), Dst Port: irisa (11000)
Data (24 bytes)

650) this.width=650;"<

B.ARP广播。

Ethernet II帧,

Src: FujianSt_f8:ec:eb (00:d0:f8:f8:ec:eb)[锐捷网络的交换机, 这里显示"福建实达网络"], Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Address Resolution Protocol (request)(ARP数据包)

Sender MAC address: FujianSt_f8:ec:eb (00:d0:f8:f8:ec:eb)

Sender IP address: 10.1.10.254 (10.1.10.254)

Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)

Target IP address: 10.1.10.135 (10.1.10.135)

ARP是一个三层的协议, 直接跑在Frame之上

No.	Time	Source	Destination	Protocol	Info
1	0.000000	10.1.10.154	225.102.116.110	UDP	Source port: irisa Destination port: irisa
2	0.000622	10.1.10.171	225.102.116.110	UDP	Source port: irisa Destination port: irisa
3	0.000679	10.1.10.29	225.102.116.110	UDP	Source port: irisa Destination port: irisa
4	0.001084	10.1.10.29	225.102.116.110	UDP	Source port: irisa Destination port: irisa
5	0.001302	10.1.10.154	225.102.116.110	UDP	Source port: irisa Destination port: irisa
6	0.001472	10.1.10.171	225.102.116.110	UDP	Source port: irisa Destination port: irisa
7	0.262166	Micro-St_cb:0a:ef	Broadcast	ARP	who has 10.1.10.137? Tell 10.1.10.113
8	0.262946	Micro-St_cb:0a:ef	Broadcast	ARP	who has 10.1.10.231? Tell 10.1.10.113
9	3.073559	00000000_0010dccb0aef	00000000_ffffffffffff	IPX SAP	General Response
10	3.156778	192.168.249.1	255.255.255.255	UDP	Source port: 1004 Destination port: 1004
11	3.351991	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.142? Tell 10.1.10.254
12	3.352349	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.135? Tell 10.1.10.254
13	3.366435	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.231? Tell 10.1.10.254
14	3.370567	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.98? Tell 10.1.10.254
15	3.371679	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.116? Tell 10.1.10.254
16	3.376173	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.86? Tell 10.1.10.254
17	3.378413	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.205? Tell 10.1.10.254
18	3.380291	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.68? Tell 10.1.10.254
19	3.383666	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.207? Tell 10.1.10.254

650) this.width=650;"<

5.再次启动WireShark, 打开网页[url]www.google.cn[url], 抓包。

http.pcap - Wireshark

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
194	4.220419	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.227? Tell 10.1.10.254
195	4.221790	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.169? Tell 10.1.10.254
196	4.233353	FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.230? Tell 10.1.10.254
197	4.262590	Micro-St_cb:0a:ef	Broadcast	ARP	who has 10.1.10.237? Tell 10.1.10.113
198	4.709334	192.168.1.248	192.168.1.255	BROWSER	domain/workgroup Announcement WORKGROUP, NT workst
199	5.356992	10.1.10.157	203.208.33.100	hpprotonetman	> http [SYN] Seq=0 Win=65535 Len=0 MSS
200	5.367442	203.208.33.100	10.1.10.157	TCP	http > hpprotonetman [SYN, ACK] Seq=0 Ack=1 Win=5720
201	5.367500	10.1.10.157	203.208.33.100	TCP	hpprotonetman > http [ACK] Seq=1 Ack=1 Win=65535 Len
202	5.367669	10.1.10.157	203.208.33.100	HTTP	GET / HTTP/1.1
203	5.378874	203.208.33.100	10.1.10.157	TCP	http > hpprotonetman [ACK] Seq=1 Ack=613 Win=6732 Le
204	5.452374	203.208.33.100	10.1.10.157	TCP	[TCP segment of a reassembled PDU]
205	5.453492	203.208.33.100	10.1.10.157	TCP	[TCP segment of a reassembled PDU]
206	5.453611	10.1.10.157	203.208.33.100	TCP	hpprotonetman > http [ACK] Seq=613 Ack=2395 Win=6553
207	5.453635	203.208.33.100	10.1.10.157	TCP	[TCP segment of a reassembled PDU]
208	5.490402	203.208.33.100	10.1.10.157	HTTP	HTTP/1.1 200 OK (text/html)
209	5.490558	10.1.10.157	203.208.33.100	TCP	hpprotonetman > http [ACK] Seq=613 Ack=3737 Win=6419
210	5.618202	EpoXComp_97:bd:ba	Broadcast	ARP	who has 10.1.10.191? Tell 10.1.10.190
211	6.262894	Micro-St_cb:0a:ef	Broadcast	ARP	who has 10.1.10.144? Tell 10.1.10.113
212	8.174844	192.168.249.1	255.255.255.255	UDP	Source port: 1004 Destination port: 1004
213	8.262482	Micro-St_cb:0a:ef	Broadcast	ARP	who has 10.1.10.213? Tell 10.1.10.113
214	8.263693	10.1.10.157	203.208.33.100	TCP	hpprotonetman > http [FIN, ACK] Seq=613 Ack=3737 Win

Frame 198 (258 bytes on wire, 258 bytes captured)
Ethernet II, Src: Elitegro_64:d1:7e (00:0d:87:64:d1:7e), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol, Src: 192.168.1.248 (192.168.1.248), Dst: 192.168.1.255 (192.168.1.255)
User Datagram Protocol, Src Port: netbios-dgm (138), Dst Port: netbios-dgm (138)
NetBIOS Datagram Service
SMB (Server Message Block Protocol)
SMB Mailslot Protocol
Microsoft Windows Browser Protocol

0000 ff ff ff ff ff ff 00 0d 87 64 d1 7e 08 00 45 00d...E.
0010 00 f4 45 c5 00 00 80 11 6e ec c0 a8 01 f8 c0 a8 ..E.....n....
0020 01 ff 00 8a 00 8a 00 e0 c9 18 11 02 a0 db c0 a8
0030 01 f8 00 8a 00 ca 00 00 20 45 4d 45 46 45 4f 45EMEFOE
0040 50 46 47 45 50 43 4e 44 46 44 45 45 46 44 44 45 PPGPCND FDEEFDDE
0050 46 45 47 45 45 45 45 45 45 45 45 45 45 45 45 45 PPGPCND FDEEFDDE

File: C:\Documents and Settings\Admin... Packets: 218 Displayed: 218 Marked: 0 Profile: Default

650) this.width=650;"<

C.HTTP数据包分析。

Ethernet II Frame,

Src: Elitegro_59:a7:88 (00:16:ec:59:a7:88) 【VIA的网卡，这里显示Elitegro】，

Dst: FujianSt_f8:ec:eb (00:d0:f8:f8:ec:eb)

Internet Protocol,

Src: 10.1.10.157 (10.1.10.157), Dst: 203.208.33.100 (203.208.33.100)

【Google.cn的IP地址】

Transmission Control Protocol,

Src Port: hppronetman (3908), Dst Port: http (80), Seq: 0, Len: 0

从抓的包中可以看到TCP的连接建立过程(Three-way Handshake).[syn][syn,ack][ack]

192.168.1.248	192.168.1.255	BROWSER	Domain/workgroup Announcement WORKGROUP, NT Workst.
10.1.10.157	203.208.33.100	TCP	hppronetman > http [SYN] seq=0 win=65535 Len=0 MSS=
203.208.33.100	10.1.10.157	TCP	http > hppronetman [SYN, ACK] seq=0 Ack=1 win=5720
10.1.10.157	203.208.33.100	TCP	hppronetman > http [ACK] seq=1 Ack=1 win=65535 Len=
10.1.10.157	203.208.33.100	HTTP	GET / HTTP/1.1
203.208.33.100	10.1.10.157	TCP	http > hppronetman [ACK] seq=1 Ack=613 win=6732 Len=
203.208.33.100	10.1.10.157	TCP	[TCP segment of a reassembled pmtu] (650) this.width=650;"<

6.再次启动WireShark，启动FlashFXP连接远程服务器，抓包。

D.FTP数据包分析

先建立TCP的连接，然后传送密码，命令。不多说了。密码以明文方式传送（涂黑的部分）。

10.1.10.71	10.1.10.255	NBNS	Name query NB WORKGROUP<1b>
10.1.10.157	115.47.134.72	TCP	hp-device-disc > ftp [SYN] seq=0 win=65
EpoxComp_97:bd:ba	Broadcast	ARP	who has 10.1.10.191? Tell 10.1.10.190
115.47.134.72	10.1.10.157	TCP	ftp > hp-device-disc [SYN, ACK] seq=0 A
10.1.10.157	115.47.134.72	TCP	hp-device-disc > ftp [ACK] seq=1 Ack=1
115.47.134.72	10.1.10.157	FTP	Response: 220 welcome
10.1.10.157	115.47.134.72	FTP	Request: USER webmaster@netseagull.com.
115.47.134.72	10.1.10.157	TCP	ftp > hp-device-disc [ACK] seq=14 Ack=3
115.47.134.72	10.1.10.157	FTP	Response: 331 welcome 'webmaster@netsea
10.1.10.157	115.47.134.72	FTP	Request: PASS [REDACTED]
115.47.134.72	10.1.10.157	FTP	Response: 230-You are using 4% of 20480
10.1.10.157	115.47.134.72	FTP	Request: SYST
115.47.134.72	10.1.10.157	FTP	Response: 215 UNIX Type: L8
10.1.10.64	10.1.10.255	NBNS	Name query NB LENOVO-E1328FC7<00>
10.1.10.157	115.47.134.72	FTP	Request: FEAT
115.47.134.72	10.1.10.157	FTP	Response: 500 FTP: command not recognis
10.1.10.157	115.47.134.72	FTP	Request: REST 100 (650) this.width=650;"<

7.再次启动WireShark，打开cmd,ping [url]www.g.cn[/url]，抓包。

E.PING [url]www.g.cn[/url] 【DNS和ICMP】

DNS服务走的53端口UDP

Internet Protocol,

Src: 192.168.175.5 (192.168.175.5) 【这是我们内部的DNS】，

Dst: 10.1.10.157 (10.1.10.157)

User Datagram Protocol,

Src Port: domain (53), Dst Port: 59161 (59161)

[url]www.g.cnDNS[/url]查询的返回值[url]www.g.cn[/url]: type CNAME, class IN, cname g.cn

g.cn: type A, class IN, addr 203.208.33.100

g.cn: type A, class IN, addr 203.208.33.101

而ICMP走的是IP协议。

FujianSt_f8:ec:eb	Broadcast	ARP	who has 10.1.10.230? Tell 10.1.10.254
10.1.10.157	192.168.175.5	DNS	Standard query A www.g.cn
192.168.175.5	10.1.10.157	DNS	Standard query response CNAME g.cn A 203.208.33.100 A 203.20
10.1.10.157	203.208.33.100	ICMP	Echo (ping) request
203.208.33.100	10.1.10.157	ICMP	Echo (ping) reply
00000000.0013d3291698	00000000.ffffffffffff	NBIPX	Find name <01><02>_MSBROWSE_<02><01>

总结：我们一共抓了组播、ARP、HTTP、FTP、DNS、ICMP，通过实验复习下网络的基础知识。WireShark的功能很强大，需要仔细研究。要继续努力呀！

转自：海鸥博客