使用wireshark抓包及分析网络 4.2

wireshark是一款非常优秀的网络抓包工具,可在多种平台上运行。下面介绍wireshark相关 的知识和抓包的操作步骤。

4.2.1 认识wireshark

wireshark是一款可运行在UNIX和Windows系统中的开源网络协议分析器。它可以实时检 测网络通信数据,也可以检测其抓取的网络通信数据快照文件。可以通过图形界面浏览这些数 据,也可以查看网络通信数据包中每一层的详细内容。wireshark拥有许多强大的特性,包括强 显示过滤器语言和查看TCP会话重构流的能力,支持上百种协议和媒体类型。

wireshark不会入侵侦测系统,对于网络上的异常流量行为,wireshark也不会产生警示或是 任何提示。仔细分析wireshark截取的数据包能够帮助使用者对于网络行为有更清楚的了解。 wireshark不会对数据包产生内容的修改,也不会发送出数据包到网络上。

wireshark的应用非常广泛,网络管理员使用wireshark来检测网络问题,网络安全工程师使 用wireshark来检查资讯安全的相关问题,开发者使用wireshark来为新的通信协议排除错误,普 通使用者使用wireshark来学习网络协议的相关知识。当然,有的人也会"居心叵测"地用它来 寻找一些敏感信息。

4.2.2 使用wireshark抓包

wireshark的工作流程包括:选择捕获接口、使用捕获过滤器、使用显示过滤器、使用着色 规则、构建图标以及重组数据。在Kali中自带了wireshark。

1. 启动侦听

首先介绍软件的启动和侦听的启动操作。

Step 01 在"嗅探/欺骗"组中找到并选择wireshark选项,如图4-5所示。

Step 02 在列表中显示了系统中的所有网络接口,这里双击eth0接口选项,如图4-6所示。



Niresbark 网络分析器 文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H) ☐ ☐ ▲ ◎ ⊑ ■ № ∅ ♀ ← → ∩ ← → ■ ■ □ □ □ □ ■ **--**+ Welcome to Wireshark .使用这个过滤器: 月 输入捕获过滤器 • 显示所有接口 😫 04 - 数据库评估软件 💷 macchange 💡 05 - 密码攻击 🕼 06 - 无线攻击 mitmproxy 🎛 07 - 逆向工程 netsniff-na 🗠 08 - 漏洞利用工具集 responder 🔂 09 - 嗅探/欺骗 scapy 🕄 7 10-权限维持 TCP tcpdump 🖑 11 - 数字取证 User's Guide · Wiki · Questions and Answers · Mailing Lists · SharkFest · Wireshark Discord n wireshark Don 📄 12 - 报告工具集 2 正在运行 Wireshark4.0.8 (Git v4.0.8 packaged as 4.0.8-1). 🛐 13 - Social Engineering Tools 已准备好加载或捕获 无分组 配置:C 图 4-5 图 4-6

Step 03 接下来wireshark会自动进行数据包的抓取,抓包信息会不断滚动,等待一段时间 后,单击"停止捕获分组"按钮,如图4-7所示。可以显示包的编号、时间、源地址、目标地 址、协议、包长度和信息。

	0 0 8
文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无	k(₩) 工具(T) 帮助(H)
🖉 🔲 🖉 🕼 📓 🖉 Q E + A FE + F	
[] 应用 停止捕获分组 Ctrl-/>	D -]+
No. Time Source Destination 1830 95.184546608 192.168.1.121 211.228.69.237 192.168.1.121 1832 95.38559130 Giga-Byt_9e:33:38 Baiduonl_41:97 192.168.1.121 1833 95.38559130 Giga-Byt_9e:33:38 Baiduonl_41:97 192.168.1.121 1833 95.38659130 Baiduonl_41:87:cc Giga-Byt_9e:32:38 192.168.1.121 1835 95.68452852 194.175.254.16 192.168.1.121 193.195.765266673 192.168.1.121 1836 95.785266673 192.168.1.121 56.222.51.113 192.168.1.121 193.95.7652.656.25 1838 96.444819158 192.168.1.122 23.255.6.168 192.168.1.122 23.255.6.169 > Frame 1: 291 bytes on wire (2328 bits), 291 bytes captur > 23.255.6.169 > > Ethernet II, Src: 18:3bi52:47.43:ce (1e:3bi52:47.43:ce (1e:3bi22:47.43:ce) > > > > Jeagram Protocol, Version 4, Src: 192.168.1.109, Dst: 22 > > > > > User Datagram Protocol, Src Port: 5353, State Port: 5353 > > Nulticast Domain Name System (response) >	Protocol Length Info TCP 68 [TCP Keep-Alive 4538 - 443 [ACK] Set TCP 68 [TCP Keep-Alive ACK] 443 - 4538 [ACK] 20 APP 69 Who has 192.166.1.102? Tell 192.168.1 21 64 J2.166.1.102? Tell 192.168.1 26 APP 69 Who has 192.166.1.102? Tell 192.168.1 26 APP 69 J2.166.1.102? Tell 192.168.1 27 28 Application Data TCP 68 [443 - 1027 [ACK] Seg-1 Ack=201 Win=52 TCP 69 [TCP Keep-Alive ACK] 443 - 7474 [ACK] TCP 69 [TCP Keep-Alive ACK] 443 - 7474 [ACK] UDP 77 1024 - 5001 Len=135 SSSDP 208 M-SEARCH * HTFP/1.1 UDP UDP 74 26883 - 19784 Len=32 0000 01 60 56 75 400 00 ff 11 d2 56 co 88 60 154 60 60 60 60 80 80 33 13 03 80 131 63 31 80 38 010 01 55 67 58 00 00 ff 11 d2 56 co 80 11 30 61 33 60 38 0200 01 60 00 60 60 80 33 13 03 80 131 63 31 63 38 0204 06 44 00 60 90 60 90 33 13 03 80 131 63 31 80 388 0205 01 60 00 60 co 80 80 13 160 33 16 30 80 131 63 38 0206 00 60 60 80 33 31 30 30 80 131 60 33 61 33 63 38 0208 05 44 00 60 90 60 90 33 31 03 80 61 31 61 33 61 30 61 30 61 30 61 30 61 30 61 30 61 30 61 30 61
th0: tive capture in progress>	│ 分组: 1040 · 已显示: 1040 (100.0%) │ 配置:Default _

图 4-7

2. 数据面板

Kali渗透测试技术标准教程(实战微课版

停止捕获后,就可以选择数据包进行分析了。wireshark可以分成3个面板部分:正上方是数 据包列表, 左下方是数据包的详细信息, 右下方是数据包的原始信息。这3个面板相互关联, 在 数据包列表中选中一个数据包之后,在数据包信息面板处就可以查看这个数据包的详细信息。

一般而言,数据包详细信息中包含的内容是用户最关心的。一个数据包通常需要使用多 个协议,这些协议一层层地将要传输的数据包封装起来,选择不同的数据包会显示不同的控 制层,本例中的数据包依次为Frame(物理层的帧信息)、EthernetⅡ(数据链路层的MAC信 息)、Internet Protocol Version4(网络层的IPv4信息)、Transmission Control Protocol(传输层的 TCP信息)、Data(数据信息),如图4-8所示。

每一层的前面有一个黑色的三角形图标,单击图标可以展开数据包这一层的详细信息,例 如,查看这个数据包中传输层的详细信息就可以单击前面的三角形图标,如图4-9所示,对应着

TCP拔乂的格式。	Transmission Control Protocol, Src Port: 8008, Dst Port
	Source Port: 8008
	Destination Port: 21114
	[Stream index: 23]
	[Conversation completeness: Incomplete (12)]
	[TCP Segment Len: 1]
	Sequence Number: 1 (relative sequence number)
Frame 2062: 60 bytes on wire (480 bits), 60 bytes captur	Sequence Number (raw): 1457619157
Ethernet II, Src: Giga-Byt_9e:3a:3e (18:c0:4d:9e:3a:3e),	[Next Sequence Number: 2 (relative sequence number
Internet Protocol Version 4, Src: 192.168.1.121, Dst: 11	Acknowledgment Number: 1 (relative ack number)
Transmission Control Protocol, Src Port: 8008, Dst Port:	Acknowledgment number (raw): 178606228
▶ Data (1 byte)	0101 = Header Length: 20 bytes (5)





知识抚展 其他层

除了以上的层之外,其他的数据包还可能显示Address Resolution Protocol (request)(地址解析协 议)、User Datagram Protocol(传输层UDP信息)、Simple Service Discovery Protocol(应用层,简 单服务发现协议)、Transport Layer Security(传输层安全)、Domain Name System(域名信息)等。

3. 筛选数据

很多用户面对这么多的包会无所适从。其实抓包后需要对包进行筛选,找到需要的数据 包。在wireshark中叫作应用显示过滤器,在主界面快捷按钮下方。常用的筛选数据包的语言格 式如下。

- ip.addr==1.2.3.4: 筛选源地址或目标地址为1.2.3.4的数据包。
- ip.src_host==1.2.3.4; 筛选源地址是1.2.3.4的数据包。
- ip.dst_host==1.2.3.4;筛选目标地址是1.2.3.4的数据包。
- ●如果需要筛选协议,直接使用数据协议的名称,如TCP、UDP、HTTP等。
- tcp.srcport==80: 筛选出TCP协议源端口号是80的包(筛选目标端口为80的TCP包, 则使用tcp.dstport==80。筛选所有使用80端口的TCP包,则使用tcp.port==80,UDP类似。)
- 筛选协议,则直接使用协议名,如TCP、UDP、DNS、IP、SSL、HTTP、FTP、ARP、 ICMP、SMTP、POP、TELNET、SSH、RDP、SIP等。

如筛选目标IP是192.168.1.121的数据包,可以输入ip.dst==192.168.1.121,按回车键后显示 结果如图4-10所示。

			*eth0			
文件(E) 编辑(E) 视图(⊻)	跳转(<u>G)</u> 捕获(<u>C</u>) 分析(<u>A</u>)	统计(S) 电话(Y) 无线(W)	工具(T) 帮助(H)	D .	
	🗆 🔬 🔘 🖪 🗎	À 🙆 ⊂ ← →	ᠬ᠂ᢣ ᢣ 📕 📕 ਯ			
📕 ip.:	src_host==192.168.1.121					× • •
No.	Time	Source	Destination	Protocol Leng	gth Info	
Г	6 0.230370175	192.168.1.121	180.110.193.149	TCP 1	155 3011 → 8080 [PSH, ACK] Seq	=1 Ack
	8 0.291803594	192.168.1.121	180.110.193.149	TCP	60 3011 → 8080 [ACK] Seq=102 /	Ack=75
	9 0.971001092	192.100.1.121	134 175 254 188	TLSv1 2	83 Application Data	K-I WII
	15 4.009601196	192.168.1.121	63.141.128.9	TLSv1.2 4	430 Application Data	
	31 4.475655680	192.168.1.121	63.141.128.9	TCP	60 9659 → 443 [ACK] Seg=377 A	ck=288
	34 4.485588407	192.168.1.121	63.141.128.9	TCP	60 9659 → 443 [ACK] Seq=377 A	ck=388
	35 4.485968433	192.168.1.121	63.141.128.9	TLSv1.2 4	464 Application Data	-
	40 4.816164732	192.168.1.121	222.186.177.101	TLSv1.2 2	279 Application Data	
	43 4.905174447	192.168.1.121	222.186.177.101	TCP	60 6517 → 443 [ACK] Seq=226 A	ck=118
	48 5.479234319	192.168.1.121	63.141.128.9	TLSv1.2 2	290 Application Data	-
→ Fr: → Et → In → In	ame 8: 60 bytes o hernet II, Src: G ternet Protocol Vo ansmission Contro	n wire (480 bits), 6 iga-Byt_9e:3a:3e (18 ersion 4, Src: 192.1 l Protocol. Src Port	0 bytes captured 0000 :c0:4d:9e:3a:3e), 0010 68.1.121, Dst: 1E 0020 : 3011, Dst Port: 0030	f8 8c 21 06 00 28 04 36 c1 95 0b c3 04 03 41 16	6 78 70 18 c0 4d 9e 3a 3e 08 e 40 00 40 06 fe 6c c0 a8 01 3 1f 90 a6 d4 15 66 60 26 ea 6 00 00 00 00 00 00 00 00 00	00 45 00 79 b4 6e e1 50 10



如果要通过多个条件组合筛选,则条件之间用比较运算符连接,如 "&&"(与)、"||" (或)、"!"(非)。如筛选源IP地址为192.168.1.121,且目标端口为80的TCP数据包,则使用 "ip.src_host==192.168.1.121 && tcp.dstport==80"命令,如图4-11所示。

		*eth0		
文件(E) 编辑(E) 视图(V)	跳转(<u>G)</u> 捕获(<u>C)</u> 分析(<u>A</u>)	统计(S) 电话(Y) 无线(W)	工具(T) 帮助(H)	
	🕅 🙆 Q ← →	n + + 📕 📕 🖬		
ip.src_host==192.168.1.121	&& tcp.dstport==80			⊠∎•]+
No. Time	Source	Destination	Protocol Length	n Info
256 27.111568895	192.168.1.121	183.60.8.150	TCP 60	6 14220 → 80 [SYN] Seq=0 Win=64240
257 27.119692735	192.168.1.121	183.60.8.150	TCP 60	6 14221 → 80 [SYN] Seq=0 Win=64240
260 27.146014004	192.168.1.121	183.60.8.150	TCP 60	0 14220 → 80 [ACK] Seq=1 Ack=1 Win
262 27.154001259	192.168.1.121	183.60.8.150	TCP 60	0 14221 → 80 [ACK] Seq=1 Ack=1 Win
263 27.154449333	192.168.1.121	183.60.8.150	HTTP 796	6 POST /mmtls/0000097e HTTP/1.1
264 27.159710552	192.168.1.121	183.60.8.150	HTTP 4626	6 POST /mmtls/0000097e HTTP/1.1
281 27.299051025	192.168.1.121	183.60.8.150	TCP 60	0 14221 → 80 [ACK] Seq=743 Ack=379
282 27.299345633	192.168.1.121	183.60.8.150	TCP 60	0 14221 → 80 [FIN, ACK] Seq=743 Ac
286 27.378611597	192.168.1.121	183.60.8.150	TCP 60	0 14220 → 80 [ACK] Seq=4573 Ack=57
287 27.378899693	192.168.1.121	183.60.8.150	TCP 60	0 14220 → 80 [FIN, ACK] Seq=4573 A
718 52.107506911	192.168.1.121	183.60.8.150	TCP 66	6 14244 → 80 [SYN] Seq=0 Win=64240
 Frame 256: 66 bytes Ethernet II, Src: Gi Destination: Tp-L: Source: Giga-Byt_ Type: IPv4 (0x0800) 	on wire (528 bits), iga-Byt_9e:3a:3e (18: inkT_06:78:70 (f8:8c: 9e:3a:3e (18:c0:4d:9e 9)	66 bytes capturε c0:4d:9e:3a:3e), 0010 21:06:78:70) :3a:3e) 0030 0040	f8 8c 21 06 00 34 06 3c 08 96 37 8c fa f0 6e 3d 04 02	78 70 18 c0 4d 9e 3a 3e 08 00 45 00 40 00 40 06 b2 94 c0 a8 01 79 b7 3c 00 50 03 67 48 ab 00 00 00 00 80 02 00 00 02 04 05 b4 01 03 03 08 01 01
Internet Protocol Ve Transmission Control	ersion 4, Src: 192.16	8.1.121, Dst: 18		

图 4-11

第4章

嗅探与欺骗

Kali渗透测试技术标准教程	
(实战微课版	

自得	妾搜索协议				
如搜	累索协议为ARI	P请求的数据包,	则输入arp即可,如	1图4-12所示。	
-			*etb0		
 文件(F)) 编辑(E) 视图(V)	跳转(G) 描获(C) 分析(A)	·····································	⊤具(T) 帮助(H)	
			•••••		
arp					
No.	Time	 Source 	Destination	Protocol Length Info	
	7 0.293865215	Tp-LinkT_06:78:70	Broadcast	ARP 60 Who has 192.168.1.114? Tell	L 192.:
	10 0.330464521	82:27:c0:ce:39:d3	Tp-LinkT_06:78:72	ARP 60 Gratuitous ARP for 192.168.	1.111
	29 1.293825335	Tp-LinkT_06:78:70	Broadcast	ARP 60 Who has 192.168.1.114? Tell	192.1
	03 3.293858703	Tp-LinkT_06:78:70	Broadcast	ARP 60 Who has 192.168.1.124? Tell	192.1
	67 E 204120400	Tp LipkT 06:78:70	Broadcast	ARP 00 WHO Has 192.100.1.11// Tell	1 102
	66 5 294120400	VMware c0:bf:29	Tn-LinkT 06:78:70	ARP 00 WHO Has 152.100.1.115? Tell	192.
	81 6 294030237	Tn-LinkT 06:78:70	Broadcast	ARP 60 Who has 192 168 1 1192 Tell	1 192
	84 7.293912500	Tp-LinkT_06:78:70	Broadcast	ARP 60 Who has 192,168,1 1192 Tell	192
	111 10.293856170	Tp-LinkT 06:78:70	Broadcast	ARP 60 Who has 192,168,1,1122 Tell	192.
	112 10.293856230	Tp-LinkT_06:78:70	Broadcast	ARP 60 Who has 192.168.1.103? Tell	L 192.:
	no 71 60 butos o	n wire (480 bite) 60	buton conturned 0000	ff ff ff ff ff ff f0 00 01 06 70 70 00	06.00.01
- Eren		H WILE 1400 DILST. DU	o bytes captured 0000		00 00 0.
→ Fran					

4. 捕获前过滤

捕获全部数据并在捕获后筛选是比较推荐的,这也是网络管理员的日常必备的操作项目。 如果发现有异常数据需要尝试监测,则需要在捕获前设置过滤条件。捕获前过滤和捕获后筛选 的命令不同,下面介绍一些捕获前过滤的常用命令及用法。

- host 1.2.3.4: 只捕获IP为1.2.3.4的数据包。
- net 1.2.3.0/24: 只捕获某个IP地址范围内的数据包。
- src 1.2.3.4: 只捕获源地址为1.2.3.4的数据包。
- dst 1.2.3.4: 只捕获目的地址为1.2.3.4的数据包。
- port 80: 只捕获HTTP(端口80)通信数据包。

在命令行中,也可以使用逻辑运算符号来执行更复杂的过滤,实现精准捕获。如捕获源地 址为本机的HTTP包,可以在过滤窗口中输入过滤条件,如捕获源地址为192.168.1.121、端口号 为80的数据包,可以使用"src 192.168.1.121&&port 80"命令,选择监控的网络接口,单击左上 角的"开始捕获分组"按钮,如图4-13所示。

2	Wireshark 网络分析器	
文件(E) 编辑(E)	视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(D) 帮助(H)	
	् 🖬 🔯 🙆 ९ २ २ २ २ ४ 📰 📰 🛛 🖬 🖬 🖬	
■应用显示过滤器	<ctrl-></ctrl->	C] • +
	Welcome to Wireshark	
	捕获	
	…使用这个过滤器: 📕 src 192.168.1.121&&port 80 🔍 🔤 🔻 显示所有接口 -	
	eth0 www.hummh	
	any www.hoursey.com Loopback: lo bluetooth-monitor	
	nflog nfqueue	
	dbus-system U dbus-session	

图 4-13

过滤完成后,可以查看捕获的效果,如图4-14所示。只有满足条件的数据包会被显示出来。

6			正在捕获 eth0 (src 192.168.1.121&&	port 80)		$\odot \odot \odot$
文件(E)	编辑(E) 视图(V) 3	跳转(<u>G)</u> 捕获(<u>C)</u> 分析(<u>A</u>)	统计(<u>S</u>) 电话(Y) 无线(<u>W</u>)	工具(I) 幕	将助(<u>H</u>)	
	🔊 🖻 🗎	📓 🙆 ९ + →	n + + 📕 🔳 🖬			
■应用显	显示过滤器 <ctrl- :<="" th=""><th>></th><th></th><th></th><th></th><th>+</th></ctrl->	>				 +
No.	Time	Source	Destination	Protocol	Length Info	
E C	1 0.000000000	192.168.1.121	183.47.124.77	TCP	66 9954 → 80 [S)	(N] Seq=0 Win=64240 Len=0
	2 0.032816485	192.168.1.121	183.47.124.77	TCP	60 9954 → 80 [A0	CK] Seq=1 Ack=1 Win=263424
	3 0.033120353	192.168.1.121	183.47.124.77	HTTP	782 POST /mmtls/0	000046a2 HTTP/1.1
	4 0.167962101	192.168.1.121	183.47.124.77	TCP	60 9954 → 80 [A0	CK] Seq=729 Ack=379 Win=26
L	5 0.168335549	192.168.1.121	183.47.124.77	TCP	60 9954 → 80 [F]	[N, ACK] Seq=729 Ack=379 W

图 4-14

5. 追踪数据流

一个完整的数据流传输一般由很多包组成,可以使用追踪数据流的方法查看并分析一组数 据包。下面介绍追踪的方法。

Step 01 在需要追踪数据流的某个数据包上右击,在弹出的快捷菜单中选择"追踪流" | "TCP流"选项,如图4-15所示。



图 4-15

📕 tcp.stream eq 4 Time 31 3.313270960 32 3.346050910 Source Destination Protocol Length Info 192.168.1.121 183.47.124.77 64240 Ack=1 3.47.124.77 Wireshark · 追踪 TCP 流 (tcp.stream eq 4) · eth0 33 3.346051106 192.168.1.121 =1 Win= 35 3.346427793 192.168.1.121 /1.1 =1425 W: POST /mmtls/00004981 HT Accept: */* Cache-Control: no<u>-cache</u> 04981 HTTP/1.1 36 3.379323406 37 3.379323569 183.47.124.77 183.47.124.77 2849 W 183.47.124.77 183.47.124.77 183.47.124.77 Cache-Control: no-cache Connection: close Content-Length: 4400 Content-Type: application/octet-stream Host: 183.47.124.77 Upgrade: mmtls User-Agent: MicroMessenger Client X-Online-Host: 183.47.124.77 38 3.379323589 4273 W 39 3.379323606 41 3.572757215 =4655 V 72 Ack 42 3.572757272 183.47.124.7 43 3.572757296 192.168.1.121 =573 Frame 35: 4708 bytes on wire (37664 bits),
 Ethernet II, Src: Giga-Byt_9e:38:38 (18:66 in the set of the se 00 45 00 79 b7 2f d5 50 18

 d5
 50
 18

 6d
 74
 6c

 54
 50
 2f

 2a
 2f
 2a

 6f
 6c
 3a

 6e
 6e
 65

 0a
 43
 6f

 20
 34
 34

 79
 70
 65

 2f
 6f
 63

 6f
 73
 74

 1客户端 分组,1服务器 分组,1 turn(s) Hypertext Transfer Protocol Data (4400 bytes) 整个对话(5,2. ▼ Show data as ASCII ▼ 流 4 查找下一个(<u>N</u>) 查找 另存为... 帮助 滤掉此流 返回 关闭 3a 20 61 70 70 6c 69 63 61 74 69 6f 74 65 74 2d 73 74 72 65 61 6d 0d 0a 6e 48 wireshark_eth0GQ1IB2.pcapng 分组: 4108 · 已显示: 18 (0.4%) · 已丢弃: 0 (0.0%) 配置: Default

图 4-16

Step 02 软件会筛选出该数据流的所有数据包,如图4-16所示。

109

4 章

(探与欺骗