第5章 Kali Linux 渗透测试实验

5.1 Wireshark 简介

5.1.1 Wireshark 的特点

Wireshark 是一个网络封包分析软件。网络封包分析软件的功能是捕获网络封包,并 尽可能显示出详细的网络封包信息。作为目前世界上最受欢迎的协议分析软件,Wireshark 可将捕获的各种协议的网络二进制数据流翻译为人们容易读懂和理解的文字和图表等形 式,极大地方便了对网络活动的监测分析和教学实验。它有十分丰富和强大的统计分析功 能,可在 Windows、Linux 和 UNIX 等系统上运行。Wireshark 于 1998 年由美国 GeraldCombs 开发,原名 Ethereal,2006 年 5 月改为 Wireshark。目前世界各国有 100 多位网络专家和软 件人员共同参与此软件的升级、完善和维护。它大约每两三个月推出一个新的版本,目前的 最新版本号为 3.4.1。它是一个开源代码的免费软件,任何人都可自由下载,也可参与共同 开发。

Wireshark 可以十分方便、直观地应用于计算机网络原理和网络安全教学实验、网络日常安全监测、网络性能参数测试、网络恶意代码捕获和分析、网络用户行为监测、黑客活动追踪等。因此它在世界范围的网络管理、信息安全、软硬件开发以及大学的科研、实验和教学工作中得到广泛的应用。Wireshark 在日常应用中具有许多优点,无论是初学者还是数据包分析专家,Wireshark 都能通过丰富的功能满足其需要。

Wireshark 的特点体现在以下 6 方面。

1. 支持的协议

Wireshark 在支持协议的数量方面是出类拔萃的,Wireshark 提供了对超过 1000 种协议的支持。这些协议既包括最基础的 IP 协议和 DHCP 协议,也包括高级的专用协议(例如 DNP3 和 BitTorrent 等)。由于 Wireshark 是在开源模式下开发的,因此每次更新都会增加一些对新协议的支持。在特殊情况下,如果 Wireshark 不支持用户需要的协议,那么用户还可以自己编写代码以提供相应的支持,并将代码提供给 Wirshark 的开发者,以便他们考虑 是否将之包含在以后的版本中。可以在 Wireshark 的项目网站上找到更多的相关信息。

2. 用户友好度

Wireshark 的界面是数据包嗅探工具中用户友好度比较高的。它基于图形用户界面并 提供了清晰的菜单栏和简明的布局。为了增强实用性,它还提供了针对不同协议的彩色高 亮显示以及通过图形展示原始数据细节等功能。与 tcpdump 等使用复杂命令行的数据包 嗅探工具相比,Wireshark 的图用户化界面对于数据包分析初学者而言是十分方便的。

3. 价格

由于 Wireshark 是开源的,因此它是免费的。Wireshark 是遵循 GPL 协议发布的自由 软件,任何人无论出于私人目的还是商业目的都可以下载并且使用。虽然 Wireshark 是免

• 102 •

费的,但是仍然会有一些人由于不了解这一点而付费"购买"它。如果在 eBay 搜索"数据包 嗅探",会发现会有很多人以 39.95 美元的"跳楼价"出售 Wireshark 的"专业企业级许可证"。显而易见,这些都是骗人的把戏。

4. 软件支持

一个软件的成败取决于其后期支持的好坏。像 Wireshark 这样的自由软件很少提供类 似于商业软件的官方正式支持,它们主要依赖于开源项目社区的用户群提供帮助。 Wireshark 社区是最活跃的开源项目社区之一。Wireshark 网站上给出了很多软件帮助的 相关链接,包括在线文档、支持与开发维基条目和 FAQ。很多顶尖的开发者也加入并关注 Wireshark 的邮件列表。河床技术(Riverbed Technology)公司也提供对 Wireshark 的付费 支持。

5. 源码访问

因为 Wrreshark 是开源软件,所以用户可以在任何时间访问其源码。这对查找程序漏洞、理解协议解释器的工作原理或上传自己的代码都有很大帮助。

6. 支持的操作系统

Wireshark 对主流的操作系统都提供了支持,其中包括 Windows、Mac OS X 以及基于 Linux 的系统。用户可以在 Wireshark 的主页上查询 Wireshark 支持的所有操作系统的 列表。

5.1.2 安装 Wireshark

Wireshark 的安装过程极其简单,但在安装之前要确保计算机满足如下要求:

- 32 位或 64 位 CPU。
- 至少 400MB 可用内存(主要为了处理大流量文件)。
- 至少 300MB 的可用存储空间(不包括捕获的流量文件需要的存储空间)。
- 支持混杂模式的网卡。
- WinPcap 或 LibPcap。

WinPcap 是 Windows 平台 pcap 数据包捕获软件包的应用程序接口(API)的实现。简 单来说,WinPcap 能够通过操作系统捕捉原始数据包、应用过滤器,并能够让网卡切入或切 出混杂模式。

虽然可以单独下载并安装 WinPcap,但最好使用 Wireshark 安装包中的 WinPcap。这个版本的 WinPcap 经过了测试,能够和 Wireshark 一起工作。

1. 在 Windows 系统中安装 Wireshark

在 Windows 中安装 Wireshark 的第一步就是在 Wireshark 的官方网站上找到下载页面,并选择一个镜像站点下载最新版的安装包。

在下载好安装包之后,按照如下步骤安装 Wireshark:

- (1) 双击安装包中的 EXE 文件开始安装,在介绍界面上单击 Next 按钮。
- (2) 阅读许可证协议,如果接受此协议,单击 I Agree 按钮。
- (3) 选择要安装的 Wireshark 组件,如图 5-1 所示,然后单击 Next 按钮。
- (4) 在 Aditional Tasks 界面单击 Next 按钮。
- (5) 选择 Wireshark 的安装位置,然后单击 Next 按钮。

Wireshark 3.2.2 64-bit Setup – 🗆 🗙								
Choose Components Choose which features of Wireshark 3.2.2 64-bit you want to install.								
The following components are available for installation.								
Select components to install:	✓ Wireshark ✓ TShark ● ✓ Plugins & Extensions ● ✓ ✓ Tools ✓ Documentation							
Space required: 193.2 MB	Description Install an offline copy of the User's Gu	ide and I	FAQ.					
Wireshark® Installer —	< <u>B</u> ack <u>N</u> ext	:>	Car	ncel				

图 5-1 选择要安装的 Wireshark 组件

(6) 当弹出询问是否需要安装 WinPcap 的对话框时,确保 Install Npcap 0.9986 复选框 被选中,如图 5-2 所示,然后单击 Install 按钮开始安装。

Wireshark 3.2.2 64-bit Setup – 🗆 🗙
Packet Capture Wireshark requires either Npcap or WinPcap to capture live network data. Image: Capture live network data.
Currently installed Npcap or WinPcap version Neither of these are installed
Install Install Npcap 0.9986 (Use Add/Remove Programs first to uninstall any undetected old Npcap or WinPcap
Get WinPcap
Learn more about Npcap and WinPcap
Wireshark® Installer
< <u>B</u> ack <u>N</u> ext > Cancel

图 5-2 选中 Install Npcap 0.9986 复选框

(7) Wireshark 的安装过程进行了大约一半的时候,会开始安装 WinPcap。在 WinPcap

介绍页面单击 Next 按钮之后,阅读许可证协议并单击 I Agree 按钮。

(8) 选择是否安装 USBPcap 工具。USBPcap 用于从 USB 设备中收集数据。完成必要的选择后单击 Next 按钮。

(9) WinPcap 和 USBPcap 安装完成后,单击 Finish 按钮。

(10) Wireshark 安装完成后,单击 Finish 按钮。

(11) 在安装完成确认界面中单击 Finish 按钮。

2. 在 Linux 系统中安装 Wireshark

Wireshark 可以在大部分 Linux 系统中运行。可以通过 Linux 系统包管理器下载并安装适合用户当前系统的 Wireshark 版本。这里只介绍在几个常见的 Linux 系统中安装 Wireshark 的步骤。

一般来说,如果作为系统软件安装,安装者需要具有 root 权限;而如果通过编译源代码 使之成为本地软件,通常就不需要 root 权限了。

1) 在使用 RPM 的 Linux 系统中安装 Wireshark

对于类似红帽 Linux(Red Hat Linux)等使用 RPM 的 Linux 系统,很可能系统默认安装 了 Yum 包管理器。如果是这样,可以从 Linux 系统软件源中获取并快速安装 Wireshark。此时,打开控制台窗口,并输入以下命令:

sudo yum install Wireshark

如果需要依赖组件,可以根据提示安装它们。如果一切顺利,就可以使用命令行启动 Wireshark 并通过图形界面来操作它。

2) 在使用 DEB 的 Linux 中系统安装 Wireshark

对于类似于 Debian 和 Ubuntu 等使用 DEB 的 Linux 系统,可以使用 APT 包管理器安装 Wireshark。要从 Linux 系统软件源中安装 Wireshark。此时,打开控制台窗口并输入如下命令:

sudo apt-get install Wireshark Wireshark-qt

如果需要依赖组件,那么可以根据提示安装它们。

3) 使用源代码编译

因为操作系统架构和 Wireshark 功能的改变,所以从源代码安装 Wireshark 的方法可 能也会随之变化,这也是建议从系统包管理器安装 Wireshark 的一个原因。然而,如果用户 的 Linux 系统没有自动安装包管理器,那么安装 Wireshark 的一种高效的方法就是使用源 代码编译。下面给出这种安装方法。

(1)从Wireshark网站下载源代码包。

(2) 输入下面的命令将压缩包解压:

tar -jxvf 源代码包括名.tar.bz2

(3) 在安装和设置 Wireshark 之前,可能需要安装一些依赖组件。例如,Ubuntu 14.04 需要一些额外的软件包才能让 Wireshark 工作。这些依赖组件可以用以下的命令安装(可能需要 root 权限):

sudo apt-get install pkg-config bison flex qt5-default libgtk-3-dev libpcap-dev

• 105 •

```
qttools5-dev-tools
```

(4) 进入源代码包解压缩后创建的文件夹。

(5) root 权限的用户使用 jconfigure 命令配置源代码,以便它能正常编译。如果不使用 默认的设置,那么可以在这时指定安装选项。如果缺少相关软件支持,用户会得到相关错误 信息;如果安装成功了,用户会得到安装成功提示。

(6) 输入 make 命令,将源代码编译成二进制文件。

(7) 输入 sudo make install 命令完成最后的安装。

(8) 输入 sudo /sbin/ldconfig 命令结束安装。

3. 在 Mac OS X 系统中安装 Wireshark

在 Mac OS X 系统中安装 Wireshark 的步骤如下:

(1)从Wireshark网站下载针对Mac OS X系统的软件包。

(2)运行安装程序,阅读并接受许可证协议。

(3) 按照安装向导的提示完成安装。

5.1.3 Wireshark 入门

1. 主窗口

Wireshark 的主窗口将捕获的数据包拆分并以更容易使人理解的方式呈现。也是用户花费时间较多的地方。Wireshark 的主窗口如图 5-3 所示。

IL:D:B32 WUAN	
2000 ##RD #800 #RD #8000 #RD #8000	~
Interactive Control 36. Time Surve Destination Protected Langth Infe 576 126.660.0105 122.468.0.255 UDP 305 54915 - 54915 Len-263 578 127.661.0105 111.30.159.57 192.468.0.105 117.76 578 127.68744 122.168.0.105 117.76 106 80 + 54099 Perstool 591 127.71729 127.166.0.105 117.76 106 80 + 54099 Perstool Ack 99 kin-255 Len-263 591 127.7563074 192.168.0.105 117.76 106 80 + 54099 Perstool Ack 99 kin-255 Len-263 591 127.7563074 192.168.0.105 117.76 106 80 + 54099 Perstool Ack 91 kin-254 Len-0 591 127.7563074 192.168.0.105 192.168.0.105 102.168.0.105 102.168.0.255 UDP 305 54915 + 54915 Len-263 591 127.563014 192.168.0.105 102.168.0.255 UDP 305 54915 + 54915 Len-263 516 129.5640 12.168.0.105 119.2.168.0.105 110.2.168.0.105 516	_
Diplement of the second seco	
Bac Time Bearce Destination Proteosil Langth Info 556 556 125.668.0.105 111.36.159.57 192.168.0.105 0100 012 121 0120 Proteosil 252 122.668.0.105 111.36.258 111.36.258 111.36.258 111.36.258 111.36.258 111.36.258 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 111.768.208 112.755.607.4 112.755.757.657.4 112.755.757.657.4 112.755.757.657.4 112.755.757.657.4 112.755.757.657.4 112.755.257.575.657.4 112	3 - +
56 126.564122 192.168.0.165 192.168.0.255 UOP 305 54915 + 54915 Lem-263 527 126.564125 111.5.155.57 121.1.68.0.355 111.7.68.268 111.7.68.268 111.7.68.268 528 127.0.88748 192.168.0.165 111.7.68.268 111.7.68.268 111.7.68.268 111.7.68.268 528 127.0.88748 192.168.0.163 111.7.68.268 111.7.68.268 111.7.68.268 111.7.68.268 538 127.0.12759 192.168.0.135 111.7.68.268 111.7.68.268 112.1.66.758 110.7.68.268 531 277.5621 192.168.6.138 111.7.68.268 112.1.66.758 110.7.66.2765 110.7.66.2765 531 277.5627 192.168.6.135 111.7.68.268 122.168.6.215 112.1.66.758 110.7.66.2765 531 277.56278 127.662.68 102.1663.68 102.1663.68 102.1663.68 102.1663.68 102.1663.68 102.1663.68 103.17.575 111.7.68.268 103.17.575 111.7.68.268 103.17.575 111.7.68.268 103.18.575 111.7.68.268 103.18.575 111.7.68.268 103.18.575 111.7.68.268 103.18.575 111.7.68.268	^
 52 2126.63105 111.30.155.57 102.680.015 11.3.68.208 112.680.015 107 22 26499 40 [P5H, ACK] Seq-285 ACK-69 Min-255 Len-228 259 212.087017 11.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 117.7.68.208 102.1680.015 1127.564074 102.1680.015 1127.5740474 102.1680.015 1127.5740474 102.1680.015 1127.5740474 102.1680.015 1127.5740474 102.1680.015 1127.5740474 102.1680.0154074 102.1680.0154074 102.1680.0154074 102.1680.0154074 102.1680.0154074 102.	
528 127.088748 192.168.0.105 111.7.68.208	
59 127.087017 111.7.63.208 192.168.0.105 TCP 16 80 + 34099 [PSH, ACK] Seq=0 A Ck-513 kin-255 lem-52 59 127.087017 192.168.0.105 117.7.63.208 TCP 54 34099 × 80 (KS Seq=131 A Ck-121 kin-254 lem-0 59 127.08701 192.168.0.105 192.168.0.105 192.168.0.255 UDP 305 54015 + 54015 lem-263 59 127.08701 109.168.0.105 192.168.0.255 UDP 305 54015 + 54015 lem-263 59 127.08701 109.168.0.105 192.168.0.105 192.168.0.105 192.168.0.105 59 127.08701 109.168.0.105 192.168.0.105 192.168.0.105 192.168.0.105 59 127.08701 109.168.0.105 109.168.0.255 UDP 305 54015 + 54015 lem-263 59 127.08701 109.168.0.105 109.168.0.255 UDP 305 54015 + 54015 lem-263 59 127.08701 109.168.0.105 100.168.0.255 UDP 305 54015 + 54015 lem-263 50 127.568488 109.168.0.105 117.158.0.205 100.168.0.255 UDP 305 54015 + 54015 lem-263 51 127.568.0.105 117.56.77.551 199.168.0.105 118.0.168 118.0.168 118.0.168 51 127.567.015 109.168.0.105 118.0.168	
531127:12759 192.168.0.105 111.7.68.208 TCP 54 54059 + 80 [ACK] Sect-331 (ACK212 Min-254 Len-0 531127:16281 HomHalPr_g3:27:05 BroadCast AMP 42 Mon has 169.254.255.253 Tcl 1192.168.0.105 531127:16281 HomHalPr_g3:27:05 BroadCast AMP 42 Mon has 169.244.255.253 Tcl 1192.168.0.105 531128.16281 HomHalPr_g3:27:05 BroadCast AMP 42 Mon has 169.244.255.253 Tcl 1192.168.0.105 531129.16281 HomHalPr_g3:27:05 BroadCast AMP 42 Mon has 169.224.255.253 Tcl 1192.168.0.105 531129.16281 HomHalPr_g3:27:05 HomAlPr_g3:27:05 Hom has 169.224.255.253 Tcl 1192.168.0.105 531129.16281 HomEant Products AMP 42 Mon has 169.224.255.253 Tcl 1192.168.0.105 531129.16281 HomEant Products AMP 42 Mon has 169.224.255.253 Tcl 1192.168.0.105 531129.16281 HomEant Products Hom has 169.224.255.253 Tcl 1192.168.0.105 HomEant Products 531129.16281 HomEant Products HomEant Products HomEant Products HomEant Products 531129.1628.101 HomEant Product HomEant Products HomEant Products HomEant Products 531129.1628.101 HomEant Product HomEant Product	
531 127.563074 192.168.0.105 192.168.0.255 UDP 305 54915 + 54915 (em-263) 532 127.56316 HomHalPr_esi3r205 Broadcast AAP 42 kho has 160.254.255.555 Tell 192.168.0.105 531 127.56231 HomHalPr_esi3r205 Broadcast AAP 42 kho has 160.254.255.555 Tell 192.168.0.105 531 127.56231 HomHalPr_esi3r205 Broadcast AAP 42 kho has 160.254.255.255 Tell 192.168.0.105 531 127.56231 HomHalPr_esi3r205 Broadcast AAP 42 kho has 160.254.255.255 Tell 192.168.0.105 535 129.16416 HomHalPr_esi3r205 Broadcast AAP 42 kho has 160.254.255.255 Tell 192.168.0.105 536 129.564368 HomHalPr_esi3r205 Broadcast AAP 42 kho has 160.254.255.257 Tell 192.168.0.105 536 129.564416 HomHalPr_esi3r205 Broadcast AAP 42 kho has 160.254.255.257 Tell 192.168.0.105 547 127 125 129.156.0.105 Directore Directore A2 kho has 160.254.255.257 Tell 192.168.0.105 547 127 127 127 127 127 127 127 127 127 12	
532 127.563816 HomeLiPr_@13.705 Broadcast AAP 42 Moh has 160.254.255.557 Tell 192.168.0.105 531 128.162673 HOMELiPr_@13.705 Broadcast AAP 42 Moh has 160.254.255.557 Tell 192.168.0.105 534 128.162673 HOMELiPr_@13.705 HOMELiPr_@13.705 HOMELiPr_@13.705 HOMELiPR_@13.705 535 129.164616 HOMELiPr_@13.705 HOMELiPR_@13.705 HOMELiPR HOMELiPR 535 129.164616 HOMELiPR HOMELiPR HOMELiPR HOMELiPR 535 129.164616 HOMELiPR HOMELiPR HOMELiPR 535 129.16463 HOMELiPR HOMELiPR HOMELiPR 536 129.16463 HOMELiPR HOMELiPR HOMELiPR 536 129.16463 HOMELiPR HOMELiPR HOMELiPR 537 129.16463 HOMELiPR HOMELiPR HOMELiPR 538 129.16463 HOMELiPR HOMELiPR HOMELiPR 538 129.16463 HOMELiPR HOMELiPR HOMELiPR 538 129.16463 HOMELiPR HOMELiPR HOMELiPR 548 129.1745 HOMELiPR HOMELiPR </th <th></th>	
531 218.166738 HomHaiPr_e1:32:05 Broadcast ARP 42 Who has 160;24,255.257 101 102.1686.0155 534 728.26673 192.166.0.015 192.166.0.015 DUP 305 2415.542015 102.1661.0155 535 129.166416 HomHaiPr_e1:32:05 Broadcast ARP 42 Who has 160;254.255.257 101 102.168.0.1055 535 129.166416 HomHaiPr_e1:32:05 Broadcast ARP 42 Who has 160;254.255.257 101 102.168.0.105 536 129.56416 HomHaiPr_e1:32:05 Broadcast ARP 42 Who has 160;254.255.257 101 102.168.0.105 54 Filth Filth Filth Filth Filth Filth 54 Filth Filth Filth Filth Filth 54 Filth Filth Filth Filth Filth 54 Filth Horiz Filth Filth Filth 54 Filth Filth Filth Filth Filth 54 Filth Filth Filth Filth Filth 54 Filth Filth Filth Filth Filth 55 Filth Filth Filth Filth Filth 56 Filth Filth Filth Filth Filth 56 Filth Filth Filth Filth Filth 57 Filth Filth	
53 129.56263 192.168.0.105 192.168.0.255 UDP 305 54915 + 54915 Lem-263 53 129.56428 190.168.0.105 192.168.0.255 UDP 305 54915 + 54915 Lem-263 53 129.564288 192.168.0.105 192.168.0.255 UDP 305 54915 + 54915 Lem-263 5 Frame 1: 12 192.168.0.105 192.168.0.255 UDP 305 54915 + 54915 Lem-263 5 Frame 1: 12 192.168.0.105 192.168.0.255 UDP 305 54915 + 54915 Lem-263 5 Frame 1: 12 192.168.0.105 192.168.0.255 UDP 305 54915 + 54915 Lem-263 5 Internet Frontocol Version 4, 570 Edb 1513, 211 Uptes captured (Deb 1514), 211 Lem-263 2015 (560 Edb 151 c) on 1147 (660 Edb 151 c) on 1147 (660 Edb 151 c) on 1147 (641 Eca8) (637 Edb 161 c) on 1247 (641 Eca8) (631 FC 61 Edb 161 c) on 1247 (641 Eca8) (637 Edb 161 c) on 1247 (641 Eca8) (637 Edb 161 c) on 1247 (641 Eca8) (631 FC 61 Edb 161 c) on 1247 (641 Eca8) (631 FC 61 Edb 161 c) on 1248 (641 Eca8) (631 FC 61 Edb 161 c) on 1248 (641 Eca8) (6	
S51 I29.166416 HomHaiPr_G137455 Broadcast APP 42 Who has 160.244.255.257 Tell 132.1685.0185 S51 I29.166416 HomHaiPr_G137458 IDP 32 SH315 4 SH315 158.1055 1015 > Frame 1: 121 bytes on wire (966 bits), 121 bytes captured (966 bits) on interface \pevice\WF(5734682-7960-47CD-8868-91AA4EEA6C98), id 0 101 > Ethernet I: 70.500 Force: 11.30.55.57, 051: 199.168.0.105 0 101 > User Datagram Protocol, Scr Ort: 8880, 055.57, 051: 199.168.0.105 0 0411(138163):37:05) > User Datagram Protocol, Scr Ort: 8880, 055.57, 051: 199.168.0.105 0 0411(138163):37:05) > User Datagram Protocol, Scr Ort: 8880, 055.57, 051: 199.168.0.105 0 0411(138163):37:05) > 01CQ - 1M software, popular in china 0 0 0 00001 44 1c a8 e3 a7 05 80 88 17 a5 10 95 00 a8 -138e^- *-0-9- 0010 00 e5 44 23 40 00 35 11 2a f6 ef 1e 9f 39 c6 a8 -138e^- *-0-9- 0020 00 e5 1f 40 ef 2a 20 57 5 10 23 80 30 08 16 3 -168e^- *-0-9- 0030 8e 115 44 d6 00 00 00 05 31 75 63 f7 50 77 67 -090 0031 96 1f 40 ef 2a 20 57 5 10 82 38 03 08 81 61 -168e^- *-0-9- 0031 86 12 32 32 d4 d4 61 11 b1 c8 ba 82 78 80 98 80 f6 -198e^- *-0-9- 0031 86 11 20 6 06 c4 00 a0 00 00 00 00 00 00 00 00 00 00 00	
35 129.56498 102.168.0.105 102.168.0.255 UUP 305 54015 + 54015 Lem-263 5 Fame: 1:1 J bytes on wire (obb bit), 101 Jbytes captured (obb bit), 01 interface Upweicker(PE)(573602E-7960-47CD-8060-91A44EEA6C90), id 0 > Ithermet II, Src: T1-LinkT_45:30:05 (00:30:17453:08:05), Dtt: HowHaiPr_03:37:05 (44:11:28:2:187:05) > Intermet Protocal Version 4, Src: 111.30.159.57, Dtt: 192.168.0.105 > User Datagrame Protocal, Src Port: 8000, Dtrov: 4002 > User Datagrame Protocal, Src Port: 8000, Dtrov: 4002 > DICQ - 2H software, popular in china	
2 Frame 1: 121 bytes on wire (966 bits), 121 bytes captured (966 bits) on interface \Device\Dev_[c\9724602-7960-47CD-8060-91A44E6A6C98], id 0 5 Herner II: No: To: To:Link asioned (1773531985), 121 bytes (1800410F_03137185) (4411c138163):37:05) > Internet Protocol Version 4, Src: 111.30.159.57, Dist: 192.168.0.105 > User Datagram Protocol, Src. To:Link asioned (1800 b)	~
0000 41 tc a8 c3 a7 05 50 88 17 z5 30 85 01 05 50 80 60 45 60 D·············· 010 00 cb da z2 40 40 35 11 z 25 40 67 16 20 37 93 cc a8 ··La9 c-··· 0202 00 65 1f 40 67 a2 00 57 5c 10 62 38 03 00 81 c5 3 ··L9···N \··8···c 0303 De 11 54 d6 60 40 00 00 00 51 75 56 17 9 c2 76 ··D··· ·D··· ·D··· 0404 b 68 29 23 64 d6 00 00 00 00 51 75 56 17 9 c2 76 ··D··· ·D··· ·D··· 0404 b 68 29 23 64 d6 11 1b 1 c9 8b a8 27 88 99 88 b6 ·h)#·F······· ···· ···· 0405 d 66 27 23 64 61 11 b c 80 e4 a3 ·k····· ····· ·····	
0410 040 04	_
0040 0040 105 42 00 10 11 10 12 10 <t< th=""><th></th></t<>	
0000 b6 11 50 44 00 00 00 00 00 00 00 00 00 00 00 00	
0050 fd 55 6b 66 fc c4 7a b7 03 98 98 eb ce 36 e0 a8 ·UK···z·····6··	
0000 C9 CC 52 9a a4 15 4a e5 7D 03 2C 9T 7C de C2 54 ···R···J·{···	
0070 e1 b8 15 19 36 fd f1 5e 03	
●27 WW (live contine in moments) 日見示: 536 (100.08) 配置:	efault.
	and a c

图 5-3 Wireshark 的主窗口

Wireshark 主窗口有 3 个面板。下面介绍每个面板的内容。

(1)数据包列表(packet list)面板。这个面板用列表显示当前捕获文件中的所有数据 包,其中包括数据包序号、数据包被捕获时的相对时间、数据包的源地址和目的地址、数据包 的协议以及在数据包中找到的概况信息等。 (2)数据包细节(packet details)面板。这个面板分层次显示了一个数据包中的内容, 并且可以通过展开或收缩来显示从这个数据包中捕获的全部内容。

(3)数据包字节(packet bytes)面板。这个面板可能是最令人困惑的,因为它显示了一个数据包未经处理的原始状态,也就是其在链路上传播时的样子。这些原始数据看上去不容易理解。

2. 首选项

Wireshark 提供了一些首选项设定,可以让用户根据需要进行定制。如果需要设定 Wireshark 首选项,那么需要在主菜单中选择"编辑"→"首选项"命令,然后便可以看到"首 选项"对话框,里面有一些可以设置的选项,如图 5-4 所示。

🙍 Wireshark · 首选项			×
Name Resolution > Protocols RSA 密钥 > Statistics 专家 > 外观 捕获 过滤器按钮 高级	 ✓ 记住主窗口的大小及位置 打开文件夹中的文件 ● 最近使用的文件夹 ○ 该文件夹: C:\Users\LIU\Documents 显示最多 ① 过滤器项目 ① 个最近文件 ✓ 确认未保存的捕获文件 ✓ 确认未保存的捕获文件 ✓ 显示过滤器文本的自动完成 主工具栏样式: 只有圆标 ~ 语言: 使用系统设置 ~ 	浏览…	
	OK Cancel	Help	

图 5-4 "Wireshark·首选项"对话框

Wireshark 首选项分9部分,下面介绍其中的7部分。

(1) Name Resolutions(名称解析)。通过其中的选项设置,可以开启 Wireshark 将地址 (包括 MAC 地址等)解析成更容易分辨的名字的功能,并且可以设置并发处理名称解析请 求的最大数目。

(2) Protocols(协议)。其中的选项可以调整关于捕捉和显示各种 Wireshark 解码数据 包的功能。虽然并不是针对每一个协议都可以进行调整,但是有一些协议的选项可以更改。 除非用户有特殊的原因修改这些选项,否则最好保持它们的默认值。

(3) Statistics(统计)。其中提供了 Wireshark 统计功能的选项。

(4)外观。其中的选项决定了 Wireshark 将如何显示数据。用户可以根据个人喜好对 大多数选项进行调整,例如是否保存窗口位置、3个主要窗口的布局、滚动条的摆放、数据包 列表面板中列的摆放、显示捕获数据的字体、前景色和背景色等。

(5)捕获。其中选项可以对捕获数据包的方式进行设置,例如默认使用的设备、是否默认使用混杂模式、是否实时更新数据包列表面板等。

(6) 过滤器按钮。其中的选项用于生成和管理过滤器。

(7)高级。在以上6部分中不包括的设置会被归入这里。通常这些设置只有 Wireshark的高级用户才会修改。

3. 数据包彩色高亮显示

数据包列表面板中用不同颜色显示数据包,如图 5-5 所示。看上去这些颜色是随机分 配给每一个数据包的,但其实并不是这样的。

No.	Tine	Source	Destination	Protocol	Length Info
	9513 1411.217867	192.168.0.105	20.45.3.193	TCP	54 58803 → 443 [ACK] Seq=198 Ack=2681 Win=66048 Len=0
	9514 1411.249891	HonHaiPr_e3:a7:05	Broadcast	ARP	42 Who has 169.254.255.2557 Tell 192.168.0.105
	9515 1411.648155	192.168.0.105	192.168.0.255	UDP	305 54915 → 54915 Len=263
	9516 1411.750187	HonHaiPr_e3:a7:05	Tp-LinkT_a5:30:95	ARP	42 Who has 192.168.0.1? Tell 192.168.0.105
	9517 1411.751819	Tp-LinkT_a5:30:95	HonHaiPr_e3:a7:05	ARP	42 192.168.0.1 is at 80:89:17:a5:30:95
	9518 1411.778521	192.168.0.105	111.7.68.208	TCP	546 54699 → 80 [PSH, ACK] Seq=2734 Ack=900 Win=257 Len=492
	9519 1411.825531	111.7.68.208	192.168.0.105	TCP	162 80 → 54699 [PSH, ACK] Seq=900 Ack=3226 Win=374 Len=108
	9520 1411.853491	192.168.0.105	111.7.68.208	TCP	54 54699 → 80 [ACK] Seq=3226 Ack=1008 Win=257 Len=0
	9521 1412.249871	HonHaiPr_e3:a7:05	Broadcast	ARP	42 Who has 169.254.255.2557 Tell 192.168.0.105
	9522 1412.427642	192.168.0.105	58.251.121.55	тср	66 [TCP Retransmission] 58855 → 8000 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
	9523 1412.644420	192.168.0.105	192.168.0.255	UDP	305 54915 → 54915 Len=263

图 5-5 数据包彩色高亮显示

每一个数据包的颜色都是有依据的,不同颜色对应数据包使用的不同协议。例如,所有 DNS数据包都是蓝色的,而所有 HTTP 数据包都是绿色的。将数据包以彩色高亮形式显示,可以让用户迅速将不同协议的数据包分开,而不需要查看每个数据包的 Protocol(协议) 列。在浏览较大的捕获文件时,这样可以节省很多时间。

如图 5-6 所示,可以在"着色规则"对话框中查看每个协议对应的颜色。在主菜单中选 择"视图"→"着色规则"命令,即可打开这个对话框。

▲ Wireshark · 着色规则 Default	×
名称	讨准器
Bad TCP	tcp analysis flags && Itcp analysis window update
✓ HSRP State Change	hsrn state != 8 & W hsrn state != 16
Spanning Tree Topology Chang	$s_{\rm tot} = 0.80$
✓ 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
ARP ARP	arp
✓ ICMP	icmp icmpv6
✓ TCP RST	tcp.flags.reset eq 1
SCTP ABORT	sctp.chunk_type eq ABORT
TTL low or unexpected	(! ip.dst == 224.0.0.0/4 && ip.ttl < 5 && !pim && !ospf) (ip.dst == 224.0.0.0/24 && ip.dst != 224.0.0.251 && ip.ttl != 1 && !(vrrp ca
Checksum Errors	eth.fcs.status=="Bad" ip.checksum.status=="Bad" tcp.checksum.status=="Bad" udp.checksum.status=="Bad" sctp.checksum.sta
SMB	smb nbss nbns netbios
HTTP	http tcp.port == 80 http2
DCERPC	dcerpc
☑ Routing	hsrp eigrp ospt bgp cdp vrrp carp gwrp igmp ismp
	tcp.flags & 0x02 tcp.flags.fm == 1
	tcp
Provident	uap ath/01.9x.1
Suctom Event	entond journal II and in
System Event	systemu_Journal systig
<	
双击编辑。指线移动。规则投顺序进行处理,直到 	特性的一个过程的。
+ - 9 10	
	OK 有制白 ▼ Cancel Import… Hypert… Help

图 5-6 "Wireshark · 着色规则 Default"对话框

用户可以创建自己的着色规则,也可以修改已有的着色规则。

在使用 Wireshark 时,有可能处理某个协议的工作比较多。这时,对着色规则进行相应的修改能让工作更加方便。例如,如果网络中有一个恶意的 DHCP 服务器在分发 IP 地址,

• 108 •

那么可以修改 DHCP 的着色规则,使其呈现明黄色(或者其他易于辨识的颜色),这样就可 以更快地找出所有 DHCP 数据包,使数据包分析工作效率更高。还可以通过用户自定义的 过滤器创建新的着色规则,以扩展着色规则。

5.2 渗透测试实验

实验器材

PC(Linux/Windows 10)1 台。

预习要求

做好实验预习,掌握数据还原内容。 熟悉实验过程和基本操作流程。 撰写预习报告。

实验任务

通过本实验,掌握以下技能:

(1)利用 nc、ncat 建立网络连接通道,进行信息传递。

(2)利用 Wireshark 捕获并分析数据。

(3) 利用 ncat 进行 SSL 加密传输。

实验环境

在 VMware 中安装两个 Kali Linux 虚拟机,分别作为服务器和客户机。安装 nc、ncat、 Wireshark 工具(Kali Linux 默认已安装这些工具)。

预备知识

了解 VMware、Kali Linux、nc、ncat、Wireshark 的安装以及使用方法。

实验步骤

本实验主要在两台虚拟机上用 nc 建立网络连接通道并进行信息传递,然后用 Wireshark 捕获数据包。开始实验之前,需要对两台虚拟机进行网络设置,将两台虚拟机的 "网络连接"选项设置为"仅主机模式",一台定义为服务器(192.168.241.131),另一台定义为 客户机(192.168.241.130),如图 5-7 所示。

用 nc 建立网络连接通道。在服务器上打开一个接口。例如,打开 333 号端口进行通信 的命令为 nc -lp 333 -c bash,如图 5-8 所示。

在客户机上打开 Wireshark 并选择用于捕获数据包的网卡,然后开始捕获数据包,如图 5-9 所示。

打开客户机的终端,输入 ncat -nv 192.168.241.131 333 命令,连接服务器的 333 号端口 并进行通信,如图 5-10 所示。

虚拟机设置		×
硬件 选项		
设备 ■内存 章处理器 →硬金(SCSI) ③ CD/DVD(DE) · · · · · · · · · · · · ·	摘要 2 GB 4 40 GB 正在使用文件 E:\迅雷下载\kal-l 仅主机模式 存在 自动检测 存在 自动检测	 设备状态 □ 已连接(C) □ 启动时连接(O) 网络连接 □ 复制物理网络连接状态(P) □ NAT 模式(N): 用于共享主机的 IP 地址 ④ 仅主机模式(H): 与主机共享的专用网络 □ 自定义(U): 特定虚拟网络 ✓Mnet0(自动桥接) ○ LAN 区段(L): ▲
		确定 取消 帮助

图 5-7 "虚拟机设置"对话框



图 5-8 打开 333 号端口

Wireshark网络分析器									_ 0	×			
文件(<u>F</u>) 编辑	≹(<u>E</u>) 视图(<u>V</u>)	跳转(<u>G</u>)	甫获(<u>C</u>)	分析(<u>A</u>)	统计(<u>S</u>)	电话(<u>Y</u>)	无线(<u>W</u>)	工具(<u>T</u>)	帮助	(<u>H</u>)			
			6	۹ 🖝			⊻.		Ð	Q		3 6	
▲ 应用显示过	滤器 <ctrl- :<="" td=""><th>></th><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td>+</td></ctrl->	>											+
	沈迎使用) 捕获 …使用这个过 Ecopbar any nflog nfqueue bluetool ⑥ Cisco re ⑥ Displayi ⑧ Random ⑧ systemo 学习 User's Guid 正在运行 Wir	Wireshark 滤器: []] 緒 :k: lo th0 mote captu ort AUX ch a packet get d Journal Ex de · Wiki eshark3.2.1	入捕获过 ire: cisco annel mo nerator: sijo 	滤器 dump onitor ca randpkt ournal stions a 2.1 pack.	pture: dp ind Ans aged as	pauxmon wers · 1 3.2.1-1).		• (显示所	ī有接	•		
2 已准备好	ħ加载或捕获						无分约	且			RC 1	🗄 : Default	

图 5-9 选择用于捕获数据包的网卡



图 5-10 连接服务器的 333 号端口并进行通信

查看 Wireshark 捕获的数据包并进行分析: 首先是 ARP 协议, ARP 用来查看对方的 MAC 地址(ARP 解析); 有了 MAC 地址, 接下来组装二层包头; 然后建立 TCP 连接(三次

• 111 •