
基于 Android 设备的 Kali Linux 渗透测试教程

（内部资料）



大学霸

www.daxueba.net



前言

Kali Linux 是业内最知名的安全渗透测试专用操作系统。它的前身就是业界知名的 BackTrack 操作系统。BackTrack 在 2013 年停止更新，转为 Kali Linux。Kali Linux 集成了海量渗透测试、攻击等专用工具。通过系统更新，用户可以快速获取最新的各类工具。所以，Kali Linux 是渗透测试专业人员的不二选择。

由于渗透目标多样化，使用传统形式的电脑 PC 或者笔记本并不是很方便。而智能手机和平板电脑的硬件性能飞速提升，已经可以满足大部分渗透工作需要。所以，基于手机和平板电脑已经成为渗透测试工作的很好的选择。

为了方便用户的使用，本教程主要介绍如何在 Android 设备实施渗透测试。内容包括搭建渗透测试环境，命令终端 Bash Shell 使用方法，网络侦查，渗透利用，网络渗透和监控等方面。本教程着重讲解 Android 设备上的实施方式，而不是渗透测试技术本身。如果读者想全面学习渗透测试技术，请参考本淘宝店对应的其他教程。

1.学习所需设备

- ☐ ☐Android 手机或平板
- ☐ ☐无线网卡
- ☐ ☐有线网卡
- ☐ ☐OTG 数据扩展线
- ☐ ☐TF 卡
- ☐ ☐键盘皮套

2.学习建议

大家学习之前，可以致信到 xxxxxxxxxx，获取相关的资料和软件。如果大家在学习过程遇到问题，也可以将问题发送到该邮箱。我们尽可能给大家解决。

目 录

第 1 章	渗透测试	1
1.1	什么是渗透测试	1
1.1.1	渗透测试的流程	1
1.1.2	渗透测试的分类	2
1.2	安装Kali Linux	2
1.2.1	在硬盘上安装Kali Linux	2
1.2.2	在树莓派上安装Kali Linux	12
1.2.3	在Android设备上安装Kali Linux	14
1.3	远程连接Kali Linux	17
1.3.1	SSH远程连接	17
1.3.2	VNC远程连接	20
1.4	Android设备使用技巧	23
1.4.1	安装黑客键盘	23
1.4.2	使用键盘皮套	26
1.4.3	扩展OTG接口	27
1.4.4	使用Micro SD卡扩展存储空间	28
第 2 章	Bash的基础知识	30
2.1	man手册	30
2.2	操作和搜索文件系统	34
2.2.1	切换目录	34
2.2.2	列出目录内容	35
2.2.3	搜索文件系统	36
2.3	使用标准输入/输出重定向	39
2.3.1	标准输出重定向	39
2.3.2	标准输入重定向	40
2.3.3	标准错误重定向	40
2.4	使用管道	41
2.5	Grep基础知识	42
2.5.1	正则表达式	42
2.5.2	Grep常使用的正则表达式	43
第 3 章	自定义Shell	46
3.1	格式化终端输出	46
3.2	自定义提示字符串	48
3.3	自定义别名	49
3.4	自定义历史命令条数	50
3.5	保护敏感信息	51
3.6	自定义自动补全	62

第 4 章	网络侦查	65
4.1	域名查询工具Whois.....	65
4.1.1	whois基本查询.....	65
4.1.2	whois的反向查询.....	66
4.1.3	查询域名信息	69
4.2	域名服务器查询工具Dig	71
4.2.1	dig命令基础使用	71
4.2.2	查询指定类型的服务器	72
4.2.3	反向IP解析.....	74
4.3	DNS枚举工具DNSenum	74
4.4	枚举本地网络上的目标	75
4.4.1	使用Arping工具发现主机.....	75
4.4.2	使用Nmap枚举目标.....	76
第 5 章	渗透利用	79
5.1	使用Metasploit命令行接口（MSFcli）	79
5.1.1	启动msfcli渗透攻击	79
5.1.2	使用msfcli的调用模式	80
5.1.3	在Bash下使用msfcli	82
5.2	准备攻击载荷	83
5.4	反汇编二进制文件	85
5.5	调试二进制文件	87
5.5.1	启动GDB调试器.....	87
5.5.2	设置并查看端点	88
5.5.3	检查寄存器、内存值和运行时信息	90
第 6 章	网络渗透并监控	93
6.1	滥用MAC和ARP	93
6.1.1	MAC地址欺骗.....	93
6.1.2	滥用地址解析协议（ARP）	95
6.2	中间人攻击	96
6.3	查询服务器	98
6.3.1	SNMP服务查询	98
6.3.2	SMTP服务查询.....	102
6.4	强力破解密码	103
6.5	使用TCPDump捕获数据	105
6.5.1	使用TCPDump.....	105
6.5.2	使用TCPDump过滤器	107
6.6	评估SSL实现安全	109

第 1 章 渗透测试

渗透测试（Penetration Testing）是一种通过模拟攻击者所采用的技术与方法，攻击目标系统的安全控制措施，并取得访问控制系统的安全测试方式。如果要进行渗透测试，必须有对应的工具。在 Kali Linux 中，集成了所有的渗透测试工具。本章将介绍渗透测试的基础知识，以及如何在各种设备上安装 Kali Linux 和远程连接 Kali Linux 等。

1.1 什么是渗透测试

渗透测试并没有一个标准的定义。国外一些安全组织达成共识的通用说法是，渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。渗透测试的过程并非简单地运行一些扫描器和自动化工具，该过程中包括对系统的任何弱点、技术缺陷或漏洞的主动分析。这个分析是从一个攻击者可能存在的位置来进行的，并且从这个位置有条件主动利用安全漏洞。

1.1.1 渗透测试的流程

渗透测试与其它评估方法不同。通常的评估方法是根据已知信息资源或其它被评估对象，去发现所有相关的安全问题。渗透测试也可以根据已知可利用的安全漏洞，去发现是否存在相应的信息资源。相比较而言，使用通常评估方法得到的评估结果更具有全面性，而渗透测试的更注重安全漏洞的严重性。渗透测试通常有七个阶段，如下所示：

- ❑ 前期交互阶段：该阶段通常是用来确定渗透测试的范围和目标的。
- ❑ 信息收集阶段：在该阶段需要采用各种方法来收集目标主机的信息，包括使用社交媒体网络、Google Hacking 技术、目标系统踩点等。
- ❑ 威胁建模阶段：该阶段主要是使用信息收集阶段所获取到的信息，来标识出目标系统上可能存在的安全漏洞与弱点。
- ❑ 漏洞分析阶段：在该阶段将综合从前面几个环节中获取到的信息，从中分析和理解那些攻击途径是可行的。特别是需要重点分析端口和漏洞扫描结果，截取到服务的重要信息，以及在信息收集环节中得到的其它关键信息。
- ❑ 渗透攻击阶段：该阶段可能是在渗透测试过程中最吸引人的过程。然而在这种情况下，往往没有用户所预想的那么一帆风顺，而是曲径通幽。在攻击目标主机时，一定要清晰地了解在目标系统上存在这个漏洞。否则，根本无法攻击成功。
- ❑ 后渗透攻击阶段：该阶段在任何一次渗透过程中都是一个关键环节。该阶段将以特定的业务系统作为目标，识别出关键的基础设施，并寻找客户组织最具价值和尝试进行安全保护的信息和资产。
- ❑ 报告阶段：报告是渗透测试过程中最重要的因素，使用该报告文档可以交流渗透测试过程中做了什么、如何做的以及最为重要的安全漏洞与弱点。

1.1.2 渗透测试的分类

到现在为止，大家已经对渗透测试的基本技术流程与环节有了一个初步的了解。接下来介绍一下渗透测试的两种基本类型，分别是黑盒测试和白盒测试。白盒测试有时也被称为“白帽子”，是指渗透测试者在拥有客户组织所有知识的情况下进行的测试；而黑盒测试是指对攻击主机一无所知的攻击者所进行的渗透测试。两种测试方法都拥有它们自己的优点和弱点。下面分别介绍详细介绍这两种类型。

1.白盒测试

使用白盒测试，需要和客户组织一起工作，来识别出潜在的安全风险。客户组织将会向用户展示它们的系统与网络环境。白盒测试最大的好处就是攻击者将拥有所有的内部知识，并可以在不需要害怕被阻断的情况下任意地实施攻击。而白盒测试的最大问题在于无法有效地测试客户组织的应急响应程序，也无法判断出它们的安全防护计划对检测特定攻击的效率。如果时间有限，或是特定的渗透测试环节（如信息收集并不在范围之内），那么白盒测试是最好的渗透测试方法。

2.黑盒测试

黑盒测试与白盒测试不同的是，经过授权的黑盒测试是设计成为模拟攻击者的入侵行为，并在不了解客户组织大部分信息和知识的情况下实施的。黑盒测试可以用来测试内部安全团队检测和应对一次攻击的能力。

黑盒测试是比较费时费力的，同时需要渗透测试者具备更强的技术能力。它依靠攻击者的能力通过探测获取目标系统的系统。因此，作为一次黑盒测试的渗透测试者，通常并不需要找出目标系统的所有安全漏洞，而只需要尝试找出并利用可以获取目标系统访问权代价最小的攻击路径，并保证不被检测到。

不论测试方法是否相同，渗透测试通常具有两个显著特点。

- ❑ 渗透测试是一个渐进的并且逐步深入的过程。
- ❑ 渗透测试是选择不影响业务系统正常运行的攻击方法进行的测试。

1.2 安装 Kali Linux

Kali Linux 是一个基于 Debian 的 Linux 发行版，该系统主要用于数字取证和渗透测试。在该操作系统中预装了许多渗透测试软件，如端口扫描器、数据包分析器、密码破解工具等。用户可以在硬盘、树莓派、Android 设备上安装该操作系统。本节将介绍在各种设备上安装 Kali Linux。

1.2.1 在硬盘上安装 Kali Linux

在硬盘上安装 Kali Linux，首先需要做一些准备工作。例如，需要查看安装 Kali Linux 的基本配置要求，如下所示：

- ❑ Kali Linux 安装的磁盘空间的最小值是 8GB。为了便于使用，这里推荐至少 25GB 去保存附加程序和文件。
- ❑ 内存最好为 512MB 以上。

Kali Linux 的下载地址 <http://www.kali.org/downloads/>，目前最新的版本是 1.0.8。下载界面如图 1.1 所示。

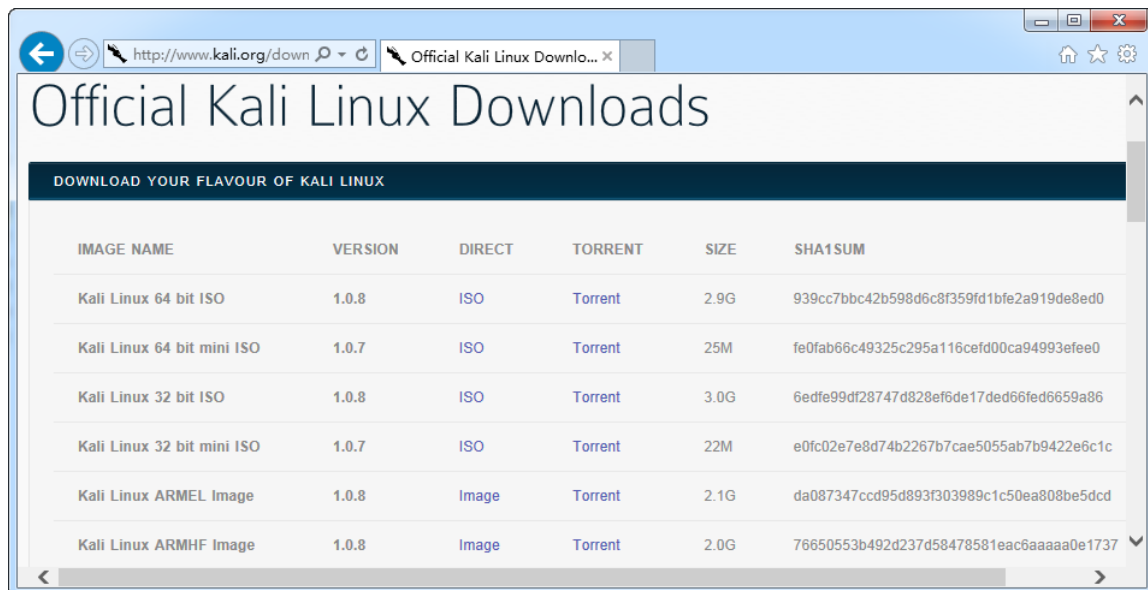


图 1.1 下载映像文件

Kali Linux 目前最新的版本是 1.0.8，该网站提供了 32 位和 64 位 ISO 文件。本书中以 32 位为例，讲解 Kali Linux 的安装和使用。用户可以根据自己的硬件配置，选择相应的 ISO 文件。在该界面下载完 ISO 文件后，将该映像文件刻录到一张 DVD 光盘上。接下来就可以在硬盘上安装 Kali Linux 操作系统了。

将以上准备工作完成后，就可以安装 Kali Linux 操作系统了。具体操作步骤如下所示：

(1) 将刻录好的 DVD 光盘插入到用户计算机的光驱中，重新启动系统设置 BIOS 以光盘为第一启动项。然后保存 BIOS 设置，启动系统后将显示如图 1.2 所示的界面。

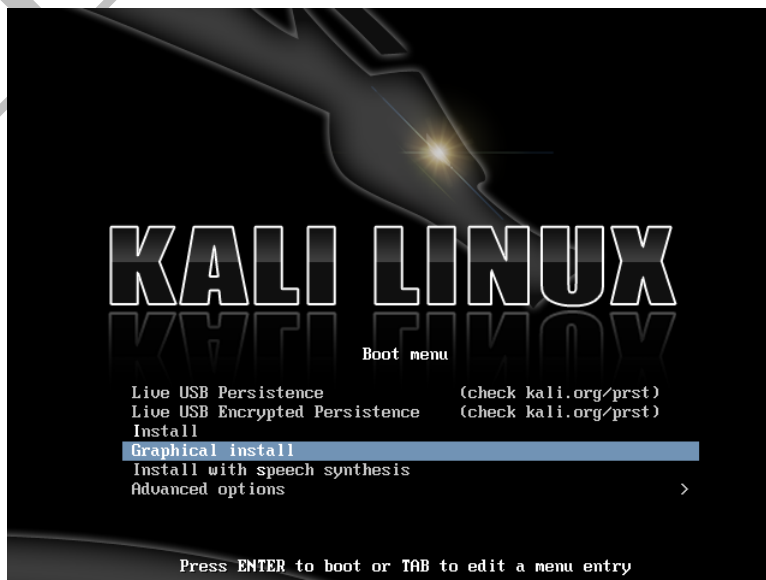


图 1.2 启动界面

(2) 该界面是 Kali 的启动界面。在该界面使用方向键向下选择 Graphical install 选项(图形界面安装)，将显示如图 1.3 所示的界面。

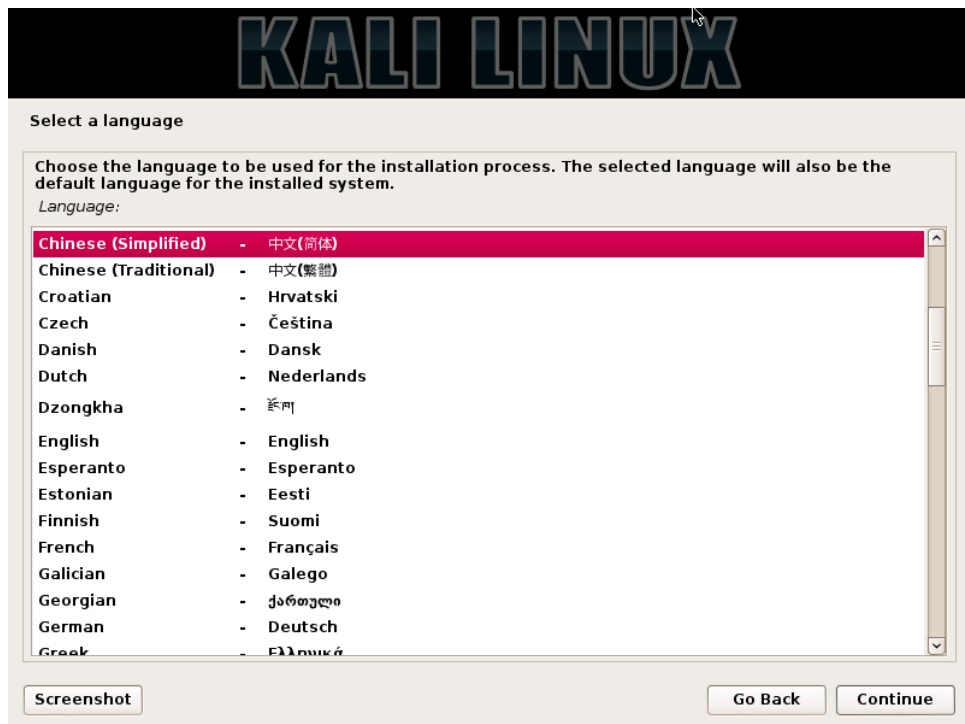


图 1.3 选择语言

(3) 在该界面选择安装系统语言，这里选择默认的语言 Chinese（Simplified）。然后单击 Continue 按钮，将显示如图 1.4 所示的界面。

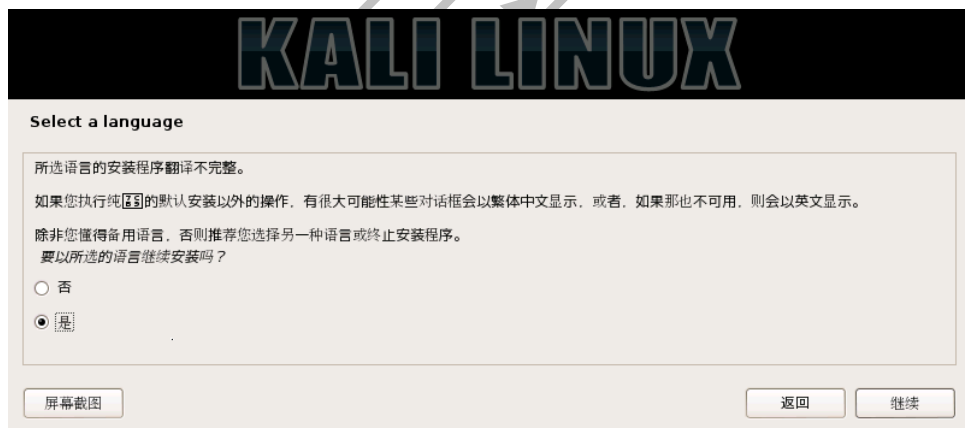


图 1.4 确认选择的安装语言

(4) 在该界面提示是否要以所选的语言继续安装，这里选择“是”复选框。然后单击“继续”按钮，将显示如图 1.5 所示的界面。

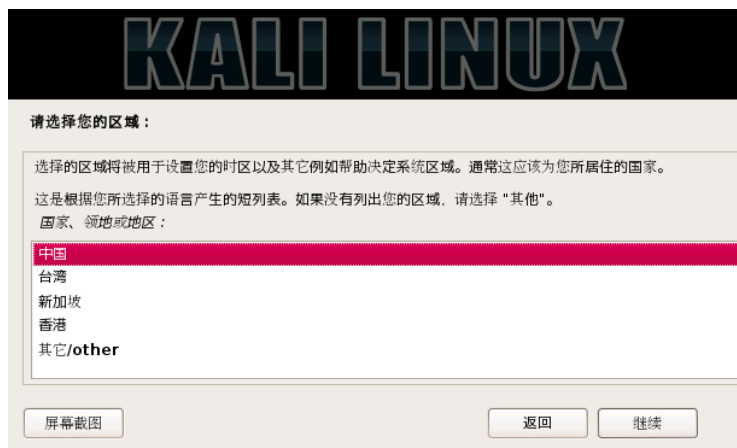


图 1.5 选择区域

(5) 在该界面选择用户当前所在的区域，这里选择默认设置中国。然后单击“继续”按钮，将显示如图 1.6 所示的界面。

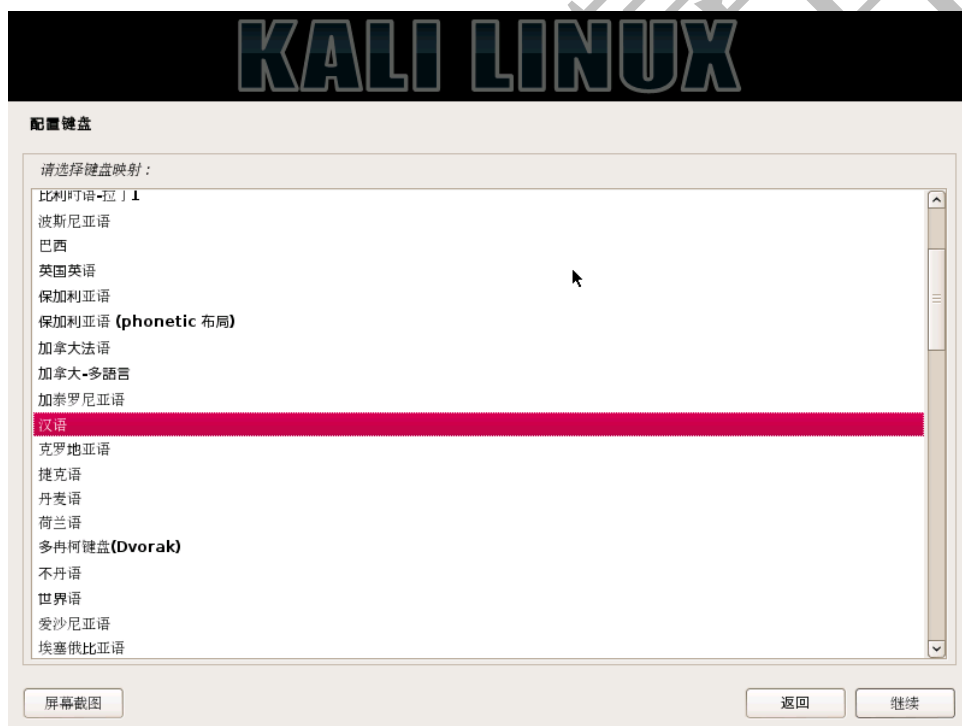


图 1.6 配置键盘

(6) 该界面用来配置键盘。这里选择默认的键盘格式汉语，单击“继续”按钮，将显示如图 1.7 所示的界面。



图 1.7 加载额外组件

(7) 该过程中会加载一些额外组件并且配置网络。当网络配置成功后，将显示如图 1.8 所示的界面。

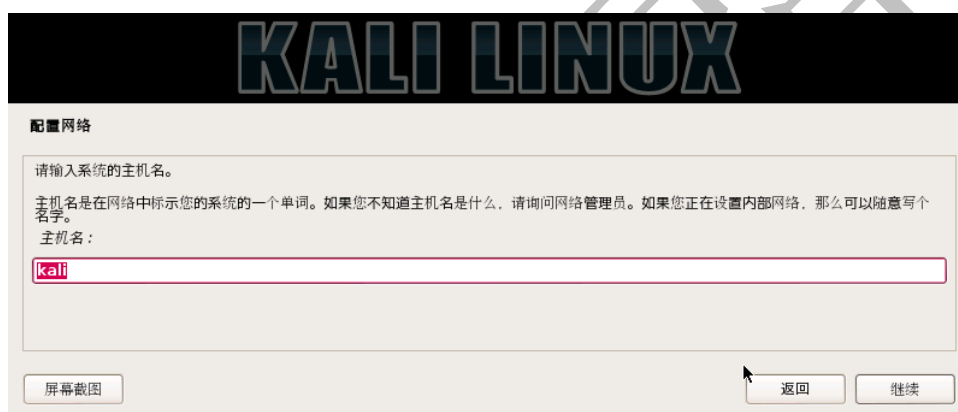


图 1.8 设置主机名

(8) 在该界面设置主机名，这里默认是 Kali。该名称可以自己设置，设置完后单击“继续”按钮，将显示如图 1.9 所示的界面。



图 1.9 设置域名

(9) 该界面用来设置计算机使用的域名。这里也可以不设置，直接单击“继续”按钮，将显示如图 1.10 所示的界面。

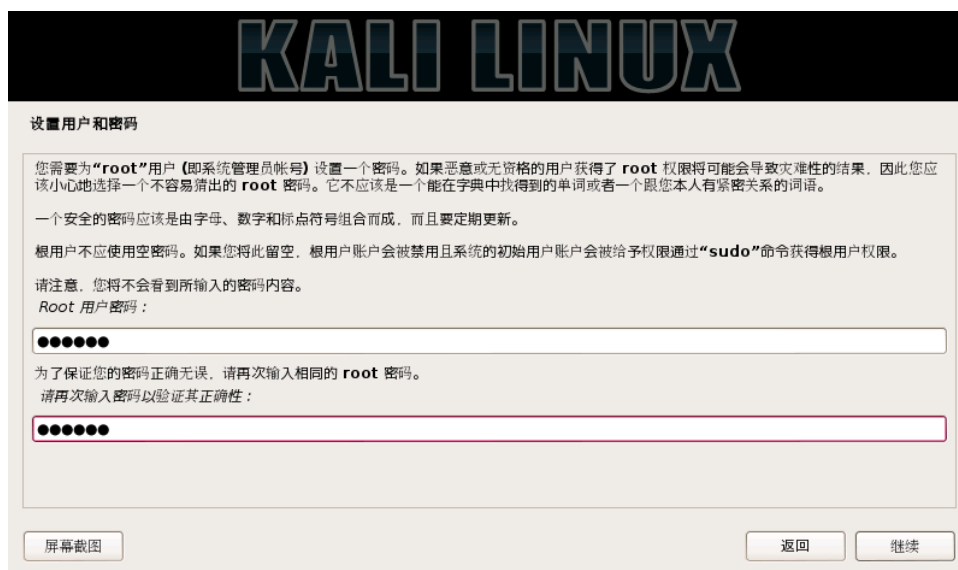


图 1.10 设置用户名和密码

(10) 该界面用来设置根 root 用户的密码。为了安全起见，建议设置一个比较复杂点的密码。设置完成后单击“继续”按钮，将显示如图 1.11 所示的界面。



图 1.11 磁盘分区

(11) 该界面用来选择分区方法。这里选择“使用整个磁盘”选项，然后单击“继续”按钮，将显示如图 1.12 所示的界面。



图 1.12 选择要分区的磁盘

（12）在该界面选择要分区的磁盘。当前系统中只有一块磁盘，所有这里选择这一块就可以了。然后单击“继续”按钮，将显示如图 1.13 所示的界面。



图 1.13 选择分区方案

（13）在该界面选择分区方案，默认提供了三种方案。这里选择“将所有文件放在同一个分区中（推荐新手使用）”，然后单击“继续”按钮，将显示如图 1.14 所示的界面。

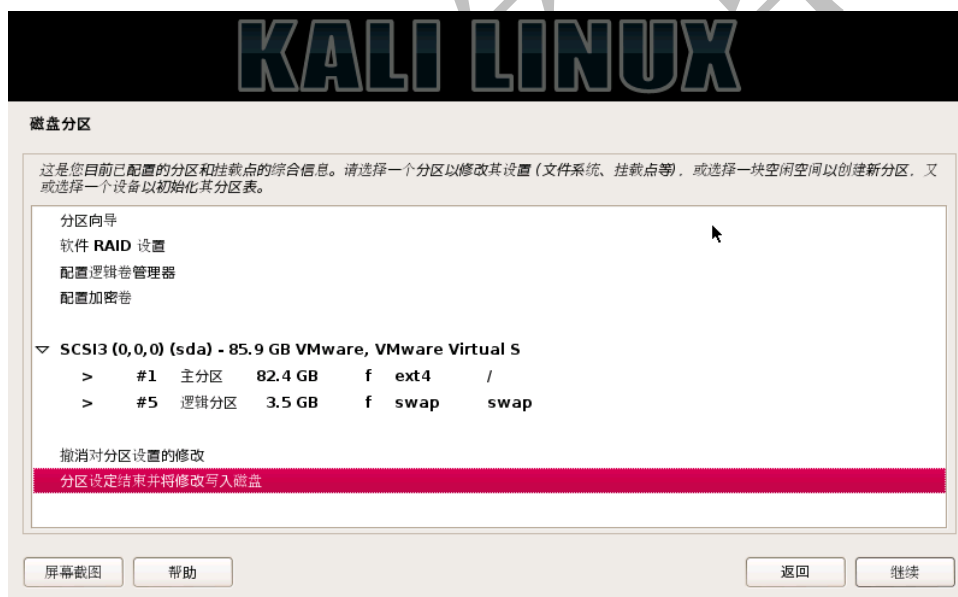


图 1.14 分区情况

（14）该界面显示了当前系统的分区情况。从该界面可以看到目前分了两个区，分别是根分区和 SWAP 分区。如果用户想修改目前的分区，选择“撤销对分区设置的修改”选项，重新进行分区。如果不进行修改，则选择“分区设定结束并将修改写入磁盘”选项。然后单击“继续”按钮，将显示如图 1.15 所示的界面。



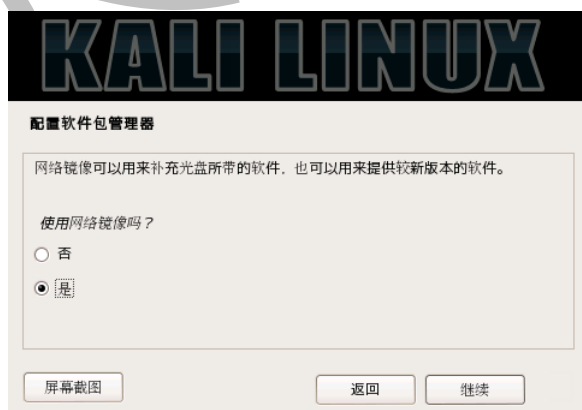
图 1.15 格式化分区

(15) 在该界面提示是否要将改动写入磁盘，也就是对磁盘进行格式化。这里选择“是”复选框，单击“继续”按钮，将显示如图 1.16 所示的界面。



图 1.16 安装系统

(16) 此时，开始安装系统。在安装过程中需要设置一些信息，如设置网络镜像，如图 1.17 所示。如果安装 Kali Linux 系统的计算机没有连接到网络的话，在该界面选择“否”复选框，然后单击“继续”按钮。这里选择“是”复选框，将显示如图 1.18 所示的界面。



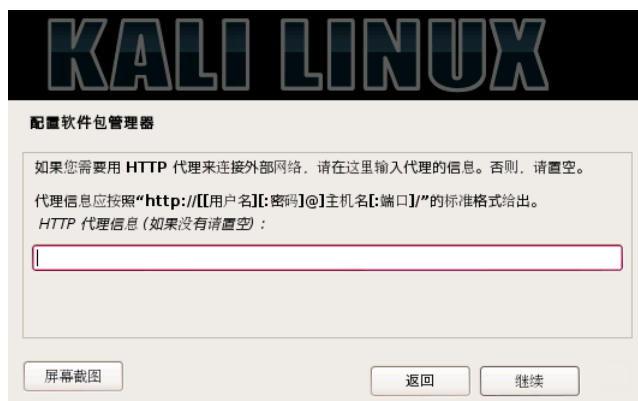


图 1.17 配置软件包管理器

图 1.18 设置 HTTP 代理

(17) 在该界面设置 HTTP 代理的信息。如果不需要通过 HTTP 代理来连接到外部网络的话，直接单击“继续”按钮，将显示如图 1.19 所示的界面。



图 1.19 扫描镜像站点

(18) 该界面显示正在配置软件包管理器。配置完成后，将显示如图 1.20 所示的界面。



图 1.20 将 GRUB 启动引导器安装到主引导记录（MBR）上吗？

（19）在该界面选择“是”复选框，然后单击“继续”按钮，将显示如图 1.21 所示的界面。

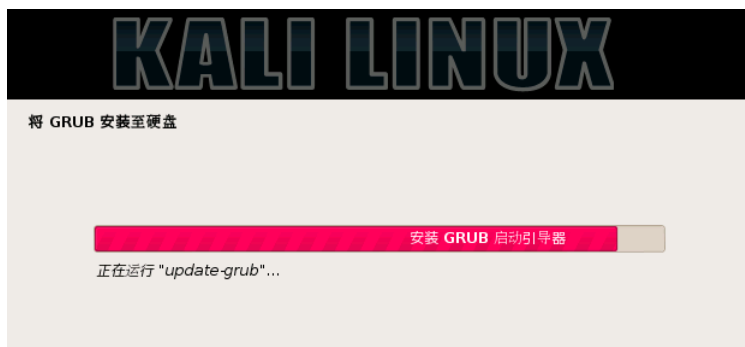


图 1.21 将 GRUB 安装至硬盘

（20）此时将继续进行安装，结束安装进程后，将显示如图 1.22 所示的界面。

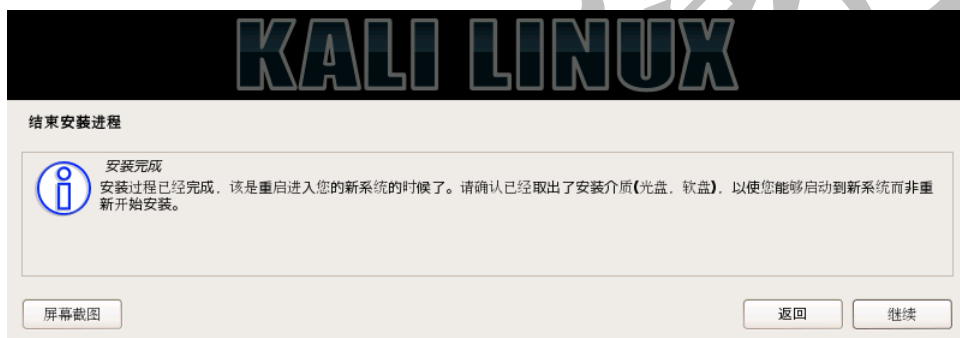


图 1.22 结束安装进程

（21）在该界面单击“继续”按钮，将返回到安装系统过程。安装完成后，将会自动重新启动系统。启动系统后，将显示如图 1.23 所示的界面。

（22）在该界面选择登录的用户。由于当前没有创建任何普通用户，所以该界面只显示了“其他”文本框。此时单击“其他”，将显示如图 1.24 所示的界面。

（23）在该界面输入登录系统的用户名，然后单击“登录”按钮，将显示如图 1.25 所示的界面。





图 1.23 登录系统

图 1.24 输入用户名

图 1.25 输入登录用

户密码

(24) 在该界面输入登录用户的密码。然后单击“登录”按钮，将显示如图 1.26 所示的界面。



图 1.26 登录系统界面

(25) 该界面显示了 Kali Linux 的默认桌面环境。此时，就可以在该操作系统中进行各种渗透测试。

1.2.2 在树莓派上安装 Kali Linux

树莓派（英文名为“Raspberry Pi”，简称为 RPi）是一款基于 ARM 的微型电脑主板，以 SD 卡为内存硬盘。为了方便携带，在树莓派上安装 Kali Linux 是一个不错的选择。本节将介绍在树莓派上安装 Kali Linux 操作系统。

(1) 从 <http://www.offensive-security.com/kali-linux-vmware-arm-image-download/> 网站下

载树莓派的映像文件，其文件名为 kali-linux-1.0.6a-rpi.img.xz。

（2）下载的映像文件是一个压缩包，需要使用 7-Zip 压缩软件解压。解压后其名称为 kali-linux-1.0.6a-rpi.img。

（3）使用 Win32 Disk Imager 工具，将解压后的映像文件写入到树莓派的 SD 卡中。启动 Win32 Disk Imager 工具，将显示如图 1.27 所示的界面。

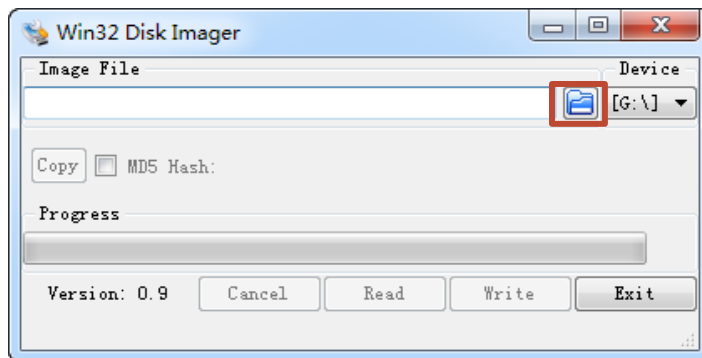



图 1.27 Win32 Disk Imager 启动界面

（4）在该界面单击  图标，选择 kali-linux-1.0.6a-rpi.img 文件，将显示如图 1.28 所示的界面。

（5）此时在该界面单击 Write 按钮，将显示如图 1.29 所示的界面。

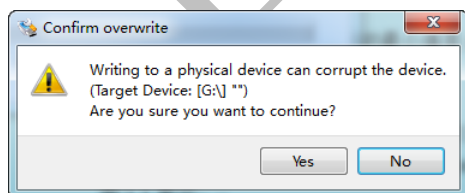
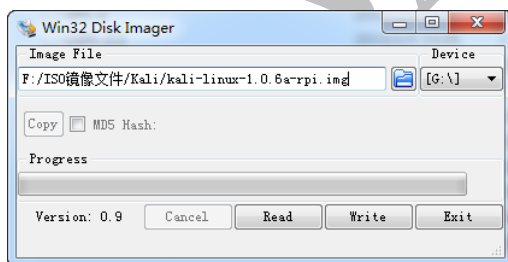


图 1.28 添加映像文件

图 1.29 确认写入数据的磁盘

（6）该界面提示是否确定要将输入写入到 G 设备吗？这里选择 Yes，将显示如图 1.30 所示的界面。

（7）从该界面可以看到正在写入数据。写入完成后，将显示如图 1.31 所示的界面。

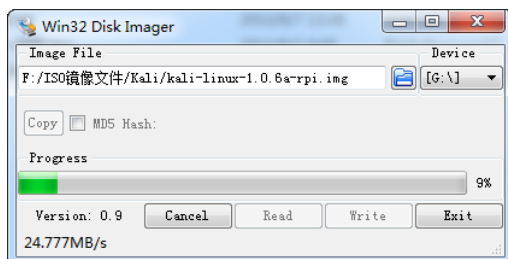


图 1.30 开始写入数据

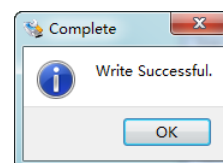


图 1.31 完成写入数据

（8）从该界面可以看到写入数据成功。此时单击 OK 按钮，将返回到图 1.28 所示的界面。然后单击 Exit 按钮，关闭 Win32 Disk Imager 工具。

（9）此时从 Windows 系统中弹出 SD 卡，并且将其插入到树莓派中。然后连接到显示器，插上网线、鼠标、键盘和电源，几秒后将起动 Kali Linux 操作系统。使用 Kali 默认的用户名和密码登陆，其默认用户名和密码为 root、toor。

1.2.3 在 Android 设备上安装 Kali Linux

Android 是一种基于 Linux 的自由及开放源代码的操作系统，主要使用于移动设备，如智能手机和平板电脑。现在大部分的用户，都使用的是 Android 操作系统的手机，而且随时都会带在身上。本节将介绍在 Android 设备上安装 Kali Linux 操作系统。

在安装之前，需要下载并安装 Linux Deploy 软件。该软件可以在一些应用商店（如 Play 商店）中找到，只需要将手机连接到网络。然后 Play 商店中，搜索并安装 Linux Deploy 软件。安装完后即可启动 Linux Deploy 软件，显示界面如图 1.32 所示。

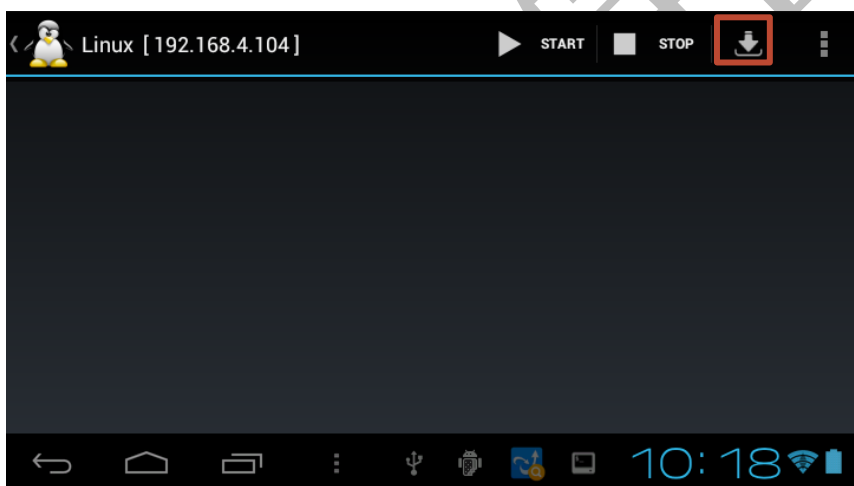



图 1.32 Linux Deploy 启动界面

在该界面单击  图标，配置并安装 Kali Linux，界面如图 1.33 所示。

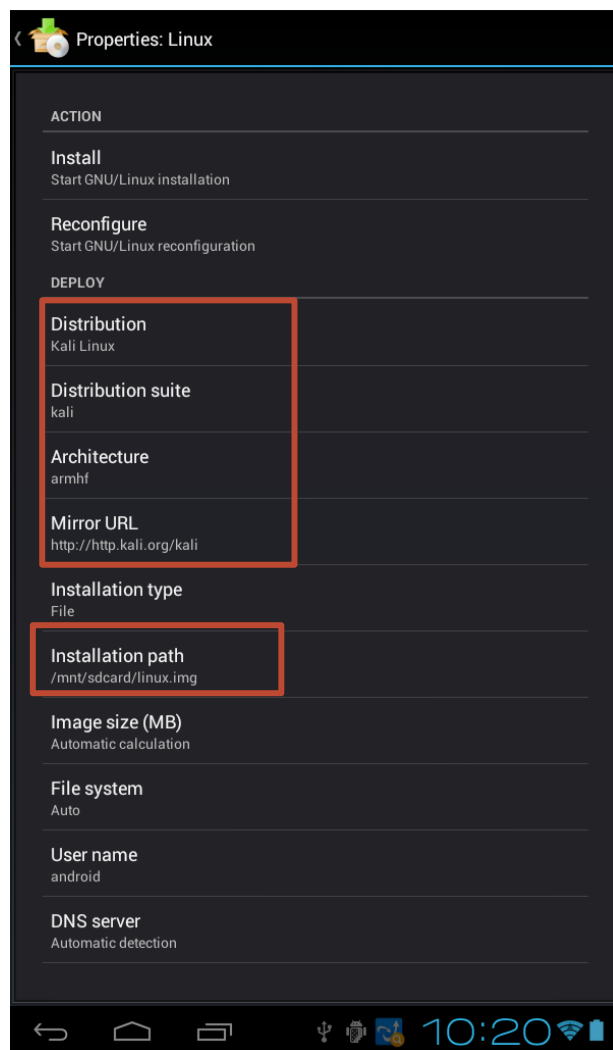


图 1.33 配置 Kali Linux

在该界面配置 Kali Linux 信息，需要配置的信息在图 1.33 中已经标出。设置完以上信息后，单击 Install 命令，将显示如图 1.34 所示的界面。

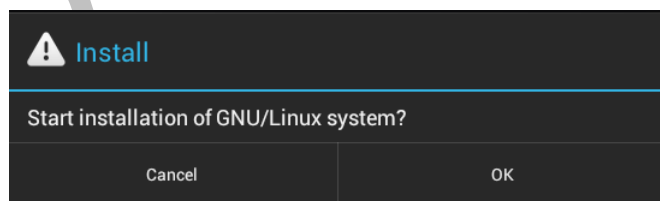


图 1.34 确认是否安装系统

在该界面提示是否要开始安装 GNU/Linux 系统，这里选择 OK 选项，将显示如图 1.35 所示的界面。

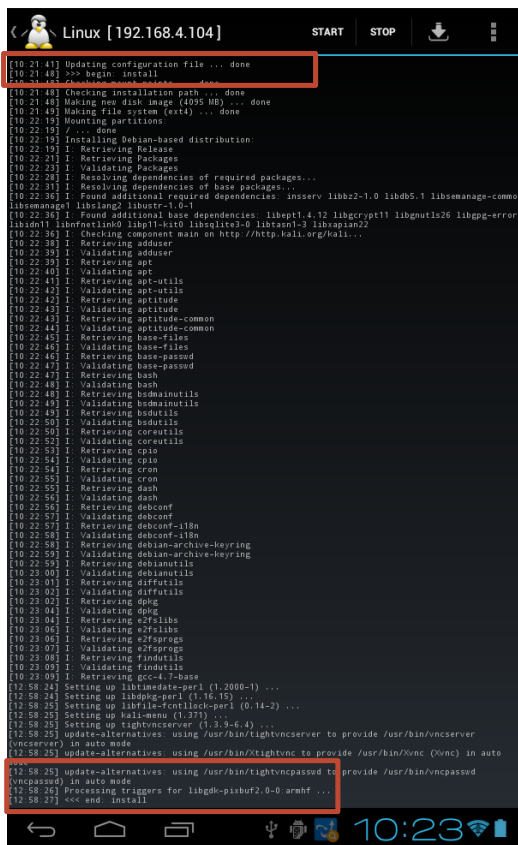


图 1.35 Kali Linux 安装完成

从该界面输出的信息中可以看到 Kali Linux 已安装完成。接下来就可以启动服务了，在该界面单击 Start 图标，将显示如图 1.36 所示的界面。

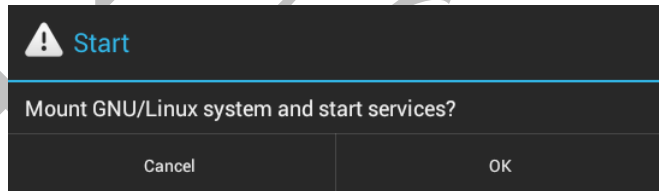


图 1.36 启动服务

该界面提示是否要挂载系统并启动服务，这里选择 OK 选项，将显示如图 1.37 所示的界面。



图 1.37 启动服务

从该界面可以看到，SSH 和 VNC 服务被启动了。如果没有成功启动的话，可以先选择 Stop 停止一下。然后在启动服务。成功启动 SSH 或 VNC 服务后，用户就可以使用获取到的 IP 地址远程连接到 Android 设备，本例中的 IP 地址为 192.168.4.104。具有远程连接 SSH 和 VNC 服务，将在下一节介绍。

1.3 远程连接 Kali Linux

本书主要以在 Android 设备上安装的 Kali Linux 操作系统为主，介绍基于 Bash Shell 渗透测试。由于在默认情况下，在 Android 设备上安装的 Kali 操作系统没有安装任何工具。如果直接在手机或平板上安装一些软件时，可能不太方便。此时，用户可以在各种操作系统中远程连接到 Kali Linux 的命令行或图形界面。本节将分别介绍使用 SSH 和 VNC 远程连接 Kali Linux。

1.3.1 SSH 远程连接

在 Android 设备上安装 Kali Linux 后，可以看到默认自动开启了 SSH 服务。在 Windows 和 Linux 中，都有相应的客户端可以远程连接到 SSH 服务。下面分别介绍 SSH 远程连接的方法。

1.在 Windows 下使用 PuTTY 实现 SSH 远程连接

【实例 1-1】演示在 Windows 下，使用 PuTTY 工具远程连接到 Kali Linux 操作系统（这里以 Android 设备上的 Kali 操作系统为例，其 IP 地址为 192.168.6.103）。具体操作步骤如下所示：

- （1）下载 PuTTY 软件的 Windows 版本。下载后，该软件可以直接使用，不需要进行安装。
- （2）启动 PuTTY 工具，将显示如图 1.38 所示的界面。

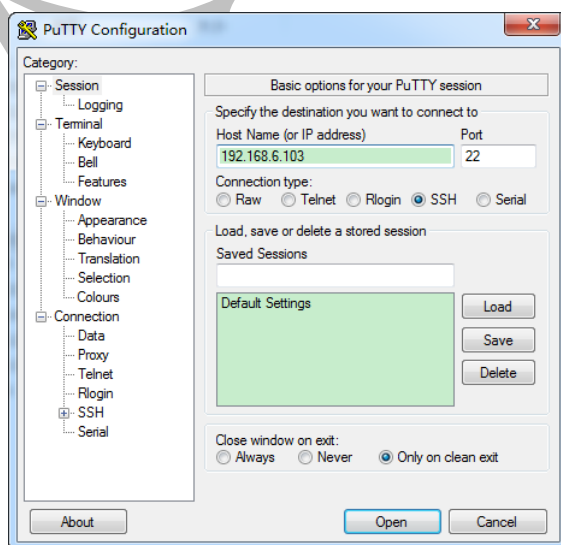


图 1.38 PuTTY 配置界面

- （3）在该界面 Host Name（or IP address）对应的文本框中输入 Linux Deploy 中获取的

IP 地址，并且在 Connection type 下面选择 SSH。然后单击 Open 按钮，将显示如图 1.39 所示的界面。

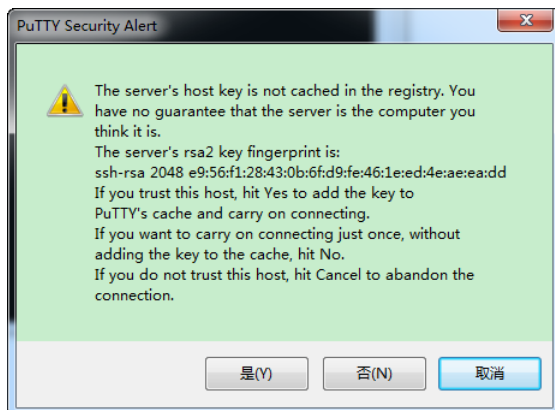


图 1.39 警告信息

(4) 该界面显示了一个警告信息，这是为了安全确认是否要连接到该服务器。该对话框只有在第一次连接某台主机时才会弹出。这里单击“是”按钮，将显示如图 1.40 所示的界面。

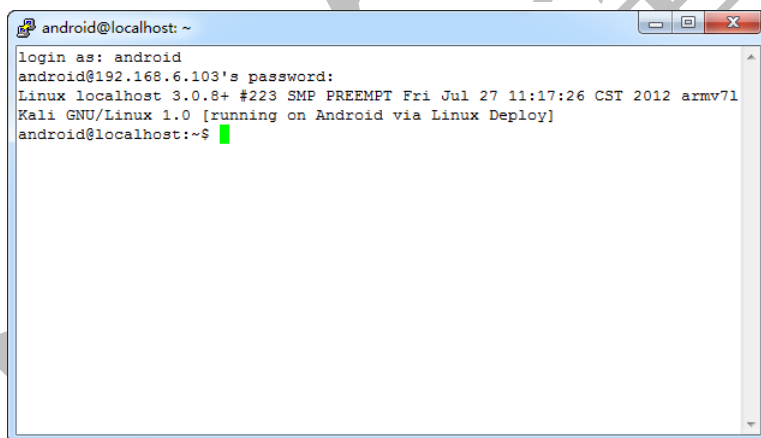


图 1.40 登录成功

(5) 在该界面输入登录 Kali 系统的用户名和密码即可登录到系统。在 Android 设备上安装的 Kali 操作系统，默认的用户名和密码分别是 android 和 changeme。这里远程连接的用户 android 是一个普通用户。但是在 Linux 中，通常一些操作必须是超级用户 root 来运行。此时就需要切换到 root 用户，执行命令如下所示：

```
android@localhost:~$ sudo su -
root@localhost:~#
```

从输出的信息中，可以看到命令提示符以变为#。此时所在的目录就是 root 用户的家目录。

2.在 Linux 下使用 ssh 命令实现 SSH 远程连接

SSH 是一个非常强大的工具。在 Linux 操作系统中远程连接服务器，ssh 是一个最佳的选择。下面将介绍使用 ssh 命令，远程连接到 Android 设备上的 Kali 操作系统。

ssh 命令的语法格式如下所示：

```
ssh -l [远程服务器上的账号] [远程服务器的主机名或 IP 地址]
```

或者

```
ssh 用户名@主机名/IP 地址
```

远程连接到 Android 设备上的 Kali 操作系统。执行命令如下所示：

```
root@kali:~# ssh android@192.168.6.103
```

执行以上命令后，将显示如下所示的信息：

```
The authenticity of host '192.168.6.103 (192.168.6.103)' can't be established.
```

```
ECDSA key fingerprint is 77:b3:21:2b:72:08:6c:6c:fb:f5:39:d8:66:04:f5:4a.
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

确认是否继续

```
续
```

以上信息是第一次登录 SSH 服务时，显示的欢迎信息并确认是否继续连接。这里输入 yes，将显示如下所示的信息：

```
Warning: Permanently added '192.168.6.103' (ECDSA) to the list of known hosts.
```

```
android@192.168.6.103's password:
```

输入 android

```
用户的密码
```

```
Linux localhost 3.0.8+ #223 SMP PREEMPT Fri Jul 27 11:17:26 CST 2012 armv7l
```

```
Kali GNU/Linux 1.0 [running on Android via Linux Deploy]
```

```
Last login: Wed Jul 30 13:45:42 2014 from 192.168.6.101
```

```
android@localhost:~$
```

在以上过程中，输入 android 用户的密码即可成功连接到主机 192.168.6.103。

3.在 Android 上使用超级终端实现 SSH 远程连接

在 Android 设备上，支持很多款 SSH 远程连接的软件，如超级终端、ConnectBot、SSHDroid 等。下面以超级终端为例，介绍在 Android 上实现 SSH 远程连接。

超级终端是一款 Android 平台上的 Linux Shell 工具，相当于 Windows 中的 CMD 命令提示符。使用它，可以在 Android 上进行 Linux 系统的命令操作。但是如果使用超级终端，还必须要安装 Busybox 工具集。Busybox 和超级终端都可以在应用宝中搜索到，然后点击安装就可以了。安装完成后，启动超级终端，显示界面如图 1.41 所示。

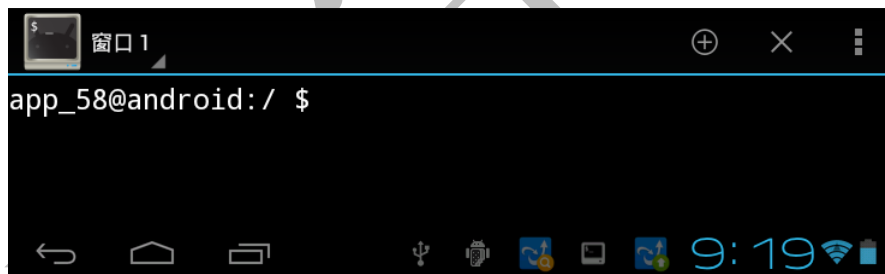


图 1.41 超级终端启动界面

该界面就是超级终端的启动界面。此时，就可以在该终端执行标准的 Linux 系统命令了。这里，就是使用 ssh 命令远程登录 SSH 服务器，如图 1.42 所示。

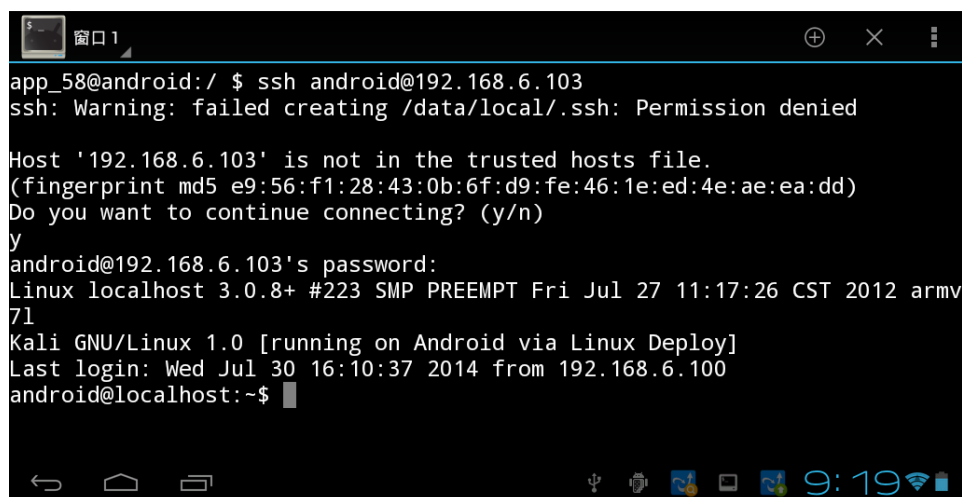


图 1.42 登录成功

该界面出现 `android@localhost:~$` 提示符，就表示成功登录了 Android 设备上的 Kali Linux。在此过程中，同样需要输入 `y` 继续连接，用户的密码也是 `changeme`。

1.3.2 VNC 远程连接

在上一节介绍了使用 SSH 远程连接到 Kali Linux，但是没有图形界面。有人比较喜欢在图形界面下进行各种操作，本节将介绍在各种系统中实现 VNC 远程连接的方法。

1.Android 设备的 VNC 远程连接

在 Android 设备上，可以在应用宝中搜索到一些 VNC 客户端软件。然后，点击安装到 Android 设备上就可以了。下面就是一个 VNC 客户端启动界面，如图 1.43 所示。



图 1.43 VNC 客户端

在该界面主要输入连接 VNC 服务器的密码，和远程主机的 IP 地址，如图 1.43 所示。在 Android 设备上安装的 Kali Linux，VNC 服务器默认密码是 changeme。设置完以上信息后，单击 Connect 按钮，将显示如图 1.44 所示的界面。



图 1.44 远程连接到桌面

从该界面可以看到，是 Kali Linux 默认桌面。但是此时的 Kali 没有安装任何工具，需要自己安装。

2.Windows 下实现 VNC 远程连接

在 Windows 操作系统中，可以使用 VNC Viewer 程序远程连接到 VNC 服务器。具体操作步骤如下：

- (1) 从 VNC 官网 <http://www.realvnc.com/download/viewer/> 下载，VNC Viewer 程序的 Windows 版本。
- (2) 在 Windows 中运行 vncviewer 程序，将显示如图 1.45 所示的界面。
- (3) 在该界面 VNC Server 对应的文本框中输入 VNC 服务器的地址，本例中是 192.168.6.103。然后单击“Connect”按钮，将显示如图 1.46 所示的界面。

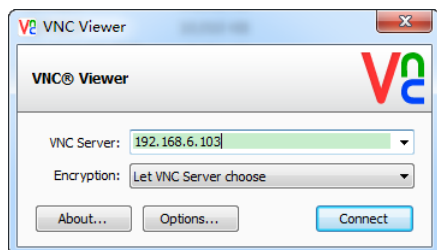


图 1.45 VNC Viewer



图 1.46 非加密连接

（4）该界面是一个警告信息，提示该连接没有加密。如果不想在下次连接时，再次弹出该窗口，将 Do not warn me about this for 192.168.6.103 again 的复选框勾上。然后单击 Continue 按钮，将显示如图 1.47 所示的界面。

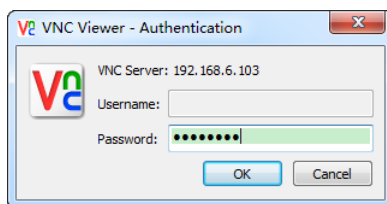


图 1.47 密码框

（5）在该界面输入登录 VNC 服务用户的密码，本例中的密码是 changeme。然后单击 OK 按钮，将显示如图 1.468 所示的界面。



图 1.48 远程连接到 VNC 服务器

（6）该界面就是远程连接到，Android 设备上的 Kali Linux 图形界面。

3.Linux 下实现 VNC 远程连接

在 Linux 中，也提供了 VNC 客户端。如在 RHEL 系统中，VNC 客户端名为 Tiger VNC Viewer；Kali Linux 中，默认安装了 VNC 客户端 vncviewer。下面演示使用 vncviewer 命令，远程连接 Android 设备上的 Kali Linux 操作系统。

vncviewer 命令的语法格式如下所示：

vncviewer 主机名/IP:端口

在 Android 设备上安装的 kali Linux 操作系统，VNC 服务默认开启的端口是 5900。远程连接 Android 设备上的 VNC 服务器，执行命令如下所示：

```
root@kali:~# vncviewer 192.168.6.103:5900
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
```

Performing standard VNC authentication

Password:

#输入用户密码

输入登录 VNC 服务器用户的密码后，将显示如图 1.49 所示的界面。

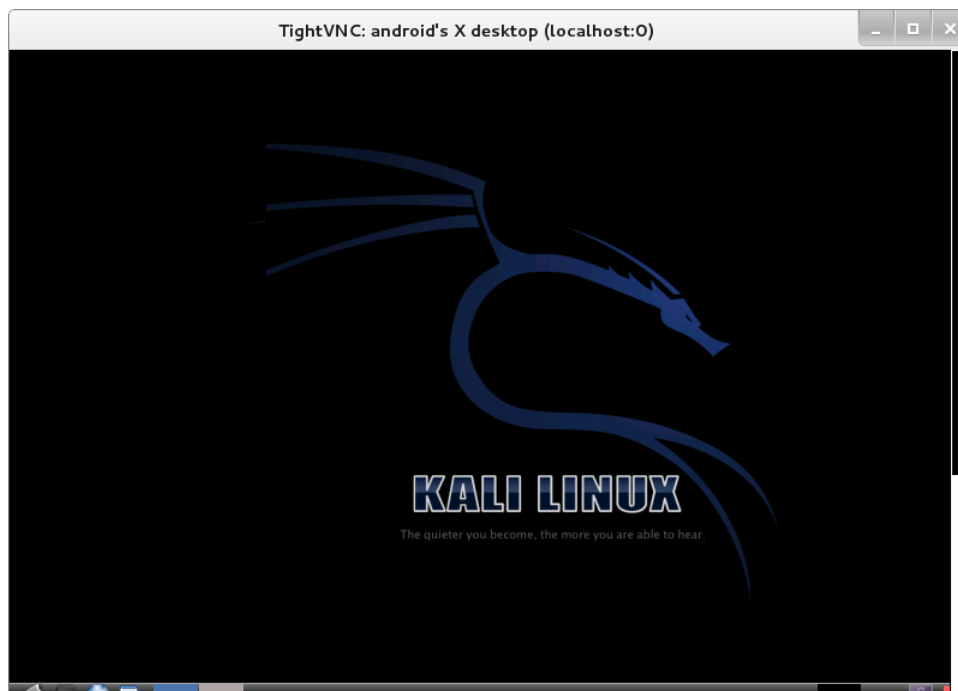


图 1.49 远程连接成功

从该界面可以看到，成功连接到 Kali Linux 的桌面。

如果 Kali Linux 安装在树莓派或者 Android 设备上，由于这些设备的显卡性能较差，所以不推荐使用 VNC 连接，建议使用 SSH 远程连接。

1.4 Android 设备使用技巧

在前面介绍了如何远程连接到 Kali Linux 操作系统，这是为了方便安装一些软件及配置。但在实际渗透测试工作中，还需要面临问题。解决这些问题，需要一定的技巧。为了更好的在 Android 设备上进行渗透测试，本节介绍使用 Android 设备进行渗透的一些技巧。

1.4.1 安装黑客键盘


一般的 Android 设备都默认安装有各种输入法，但是这些输入法虚拟机键盘提供的按键不是很全，尤其一些 Linux 命令常用的键。在 Android 设备上，这里推荐安装使用黑客键盘输入法。该输入法提供的虚拟键盘和计算机（笔记本、台式机）上的键盘一样。这样，用户就可以使用 Tab 键补全过长的命令，或者使用方向键查看以前执行的命令等。下面将介绍安装及设置黑客键盘的方法。

（1）在 Android 设备上的应用商店软件中提供了该软件的下载，如应用宝。将平板的数据线插到电脑上，然后打开应用宝并连接平板。

（2）将平板成功连接应用宝后，在手机应用标题栏搜索黑客键盘，搜索到的界面如图 1.50 所示。



图 1.50 安装黑客键盘

（3）从该界面可以看到，已经搜索到黑客键盘。在右侧可以看到，安装黑客键盘后的界面。此时，单击“安装到手机”按钮开始安装黑客键盘。安装成功后，在平板上将出现  图标。

（4）安装黑客键盘后，还需要设置一下才可使用。这时候打开黑客键盘，将显示如图 1.51 所示的界面。

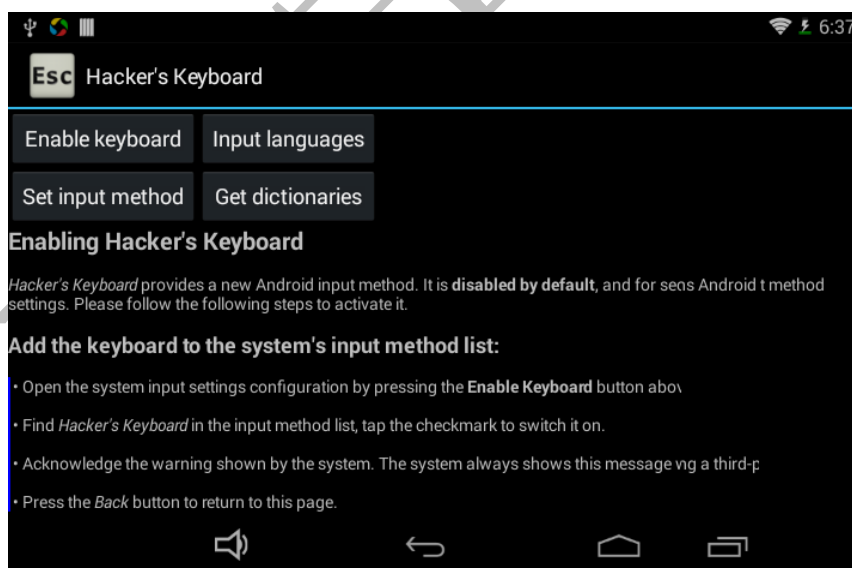


图 1.51 设置输入法

（5）在该界面选择 Enable Keyboard 按钮，将显示如图 1.52 所示的界面。



图 1.52 启动黑客键盘

(6) 在该界面选择 Hacker's Keyboard 选项，将显示如图 1.53 所示的界面。



图 1.53 警告对话框

(7) 该界面显示了使用黑客键盘的警告信息。这里选择“确定”按钮，然后返回到黑客键盘的设置界面，选择 Set input method 按钮，将显示如图 1.54 所示的界面。



图 1.54 选择输入法

(8) 在该界面选择 Hacker's Keyboard 输入法，这样黑客键盘就设置好了。这时候用户就可以使用该键盘了，该界面的界面如图 1.55 所示。

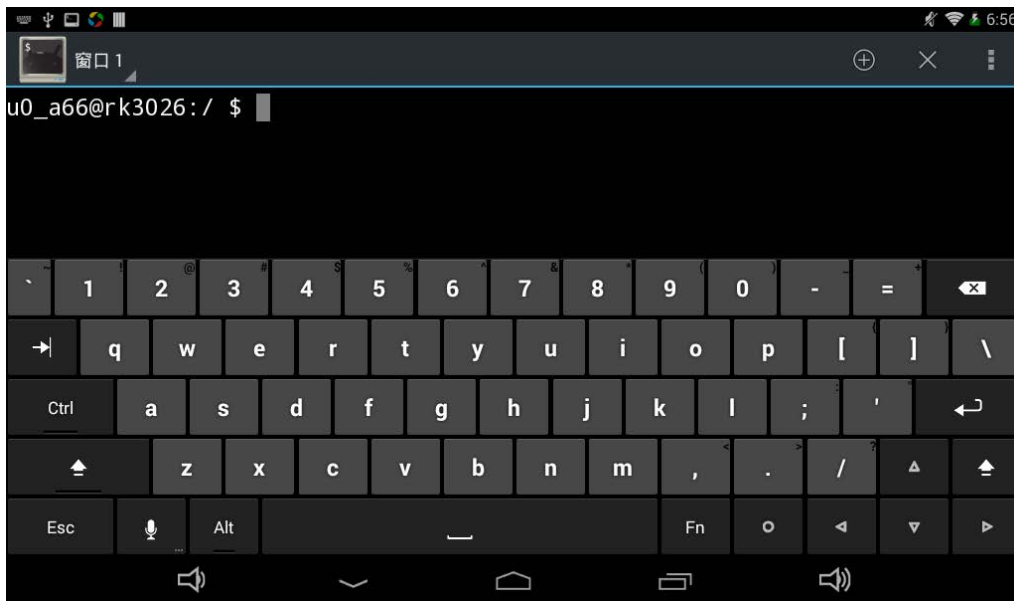


图 1.55 黑客键盘

(9) 该界面就是黑客键盘的使用界面。

1.4.2 使用键盘皮套

如果用户仍然觉得使用黑客键盘还是不够方便，还可以使用物理键盘——键盘皮套。下面介绍一下键盘皮套的使用方法。键盘皮套如图 1.56 所示。



图 1.56 键盘皮套

从图 1.56 可以看到，该键盘皮套包括键盘和一根 Micro USB 的数据线。此时将键盘皮套上的 MicroUSB 数据线插入到平板的数据线口上，然后将平板卡在皮套上，显示界面如图 1.57 所示。

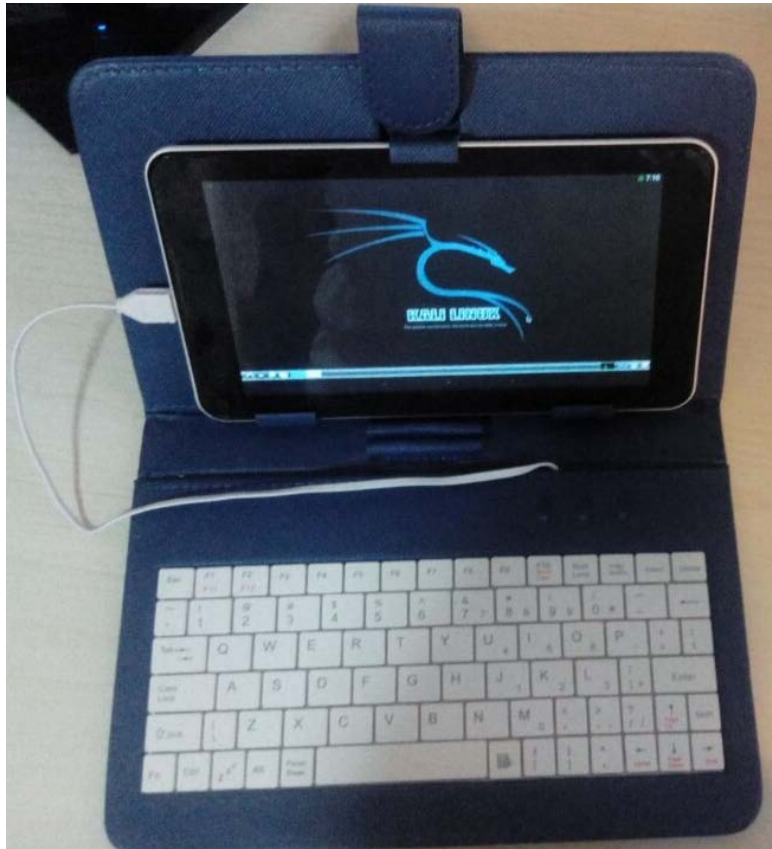


图 1.57 键盘皮套的使用

这样，就可以像使用笔记本一样，在平板上输入了。

1.4.3 扩展 OTG 接口

在平板上，往往默认只有一个 Micro USB 接口。在渗透测试的时候，我们往往还需要连接有线网络或者多个无线网络。这个时候，OTG 就不够用了。这个时候，我们就需要扩展 OTG 接口。这个时候，我们要使用 OTG 扩展线，如图 1.58 所示。



图 1.58 OTG 扩展数据线

该扩展线一端连接平板, 然后另外一段可以扩展出两个普通 USB 接口和一个 Micro USB 接口。这样就可以将更多的设备连接到平板上, 如鼠标、USB 接口的有线网卡、无线网卡等。下面介绍连接方式。

将 OTG 数据线的 Micro USB 一端插入到平板的 Micro USB 接口上, 然后将其它设备插入到 OTG 数据线另外一端。连接成功后, 界面如图 1.59 所示。

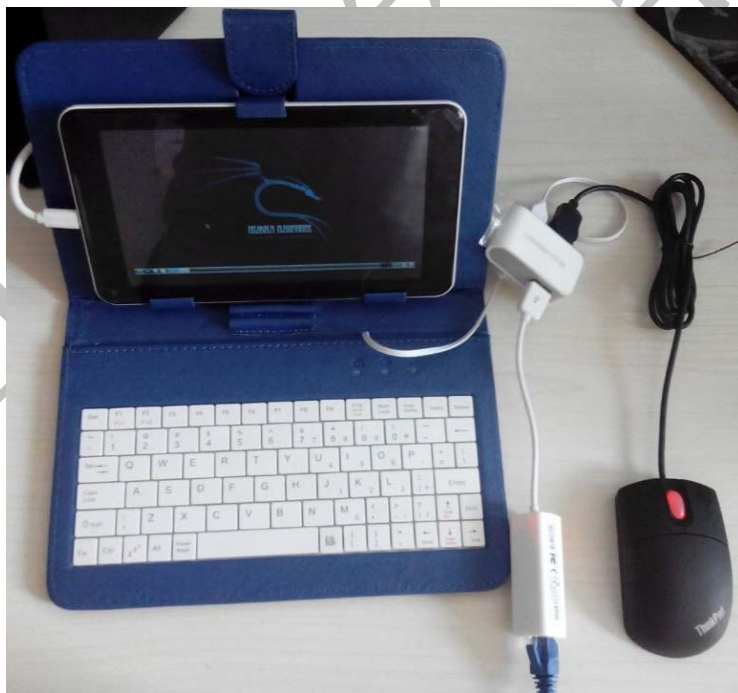


图 1.59 使用 OTG 数据线

从图 1.59 可以看到, 借助 OTG 扩展数据线, 可以同时使用鼠标、键盘、新增的无线网卡。如果 OTG 扩展数据线的接口多的话, 还可以插入其它的设备, 如 Micro USB 接口的有线网卡、无线网卡等。

1.4.4 使用 Micro SD 卡扩展存储空间

由于 Linux Deploy 安装 Kali Linux 会直接占用 4GB 的存储空间。如果平板原有存储空间较小，就很容易导致安装失败。这时，需要使用 Micro SD 之类的存储卡扩展存储空间。Micro SD Card，原名为 Trans-flash Card（TF 卡）。该卡是一种很小的快闪存储器卡，主要用于移动设备，如手机、平板等。当平板本身的存储空间不是很大时，就可以使用 Micro SD 卡来扩展。这样，用户使用该卡可以存储其它有用的东西。避免因平板本身出现故障，导致所有数据丢失等问题。下面将介绍 Micro SD 卡的使用。

Micro SD 卡有两面，正反两面是不同的，如图 1.60 所示。将该卡插入 TF 卡槽时，也是区分正反面的。



图 1.60 SD 卡的正、反面

从图 1.60 中可以看到，正反两面完全不同。正面没有任何东西，反面是有金属条的。这时候在平板上找见 TF 卡插槽，本例中使用的是原道 N70 的平板，其 TF 卡槽界面如图 1.61 所示。



图 1.61 TF 卡槽

从该图中可以看到，最右侧有一个卡槽，而且上面画有一个和 SD 卡类似的图案。这表示该位置是用来插入 SD 卡的。有的平板上没有这样类似的图片，而是写的 TF-CARD。

找到 TF 卡槽后，就可以将 SD 卡插入到平板中了。此时手拿住 SD 卡的正面，金属条向下，将 SD 卡插入到 TF 卡槽。当需要卸载该 SD 卡时，用手向里按一下 SD 卡，该卡将会被弹出。