

基于 Kali Linux 的 Nmap



5.1 Kali Linux 简介

Kali Linux 是基于 Debian 的 Linux 发行版,用于数字取证操作系统,由 Offensive Security Ltd. 维护和资助,最先由 Offensive Security 的 Mati Aharoni 和 Devon Kearns 通过重写 BackTrack Linux 来完成,BackTrack Linux 是之前用于取证的 Linux 发行版, 第一版于 2014 年 5 月 27 日发布。

Kali Linux 预装了许多渗透测试工具,包括信息收集、漏洞分析、Web 程序、数据库 评估软件、密码攻击、无线攻击、逆向工程、漏洞利用工具集、嗅探工具、权限维持、数字取 证、报告工具集等,为所有工具运行提供了一个稳定一致的操作系统基础。

5.2 Kali Linux 主要特性

Kali Linux 是 BackTrack Linux 完全遵循 Debian 开发标准的完整重建,创建了全新的目录框架,复查并打包所有工具,还为 VCS 建立了 Git 树。其具有以下特点。

(1) 超过 300 个渗透测试工具。复查了 BackTrack Linux 里的每一个工具之后,去 掉了一部分已经无效或功能重复的工具。

(2) 永久免费。使用者无须为 Kali Linux 付费。

(3) 开源 Git 树。那些想调整或重建包的人可以浏览开发树得到所有源代码。

(4) 遵循 FHS。Kali 的开发遵循 Linux 目录结构标准,用户可以方便地找到命令文件、帮助文件、库文件等。

(5) 支持大量无线设备。尽可能地使 Kali Linux 支持更多的无线设备,能正常运行 在各种各样的硬件上,能兼容大量 USB 和其他无线设备。

(6)集成注入补丁的内核。作为渗透测试者或开发团队经常需要做无线安全评估, 所用的内核包含了最新的注入补丁。

(7)安全的开发环境。Kali Linux 开发团队由一群可信任的人组成,他们只能在使用多种安全协议的时候提交包或管理源。

(8) 包和源有 GPG 签名。每个开发者都会在编译和提交 Kali 的包时对它进行签 名,并且源也会对它进行签名。

(9)多语言。虽然渗透工具趋向于用英语,但为了确保 Kali 有多种语言支持,可以让

用户使用本国语言找到他们工作时需要的工具。

(10) 完全的可定制。不是每个人都赞同一致的设计,所以让更多有创新精神的用户 能定制 Kali Linux(甚至定制内核)成他们喜欢的样子。

5.3 Kali Linux 安装

可到 Kali Linux 的官网下载安装文件,但速度较慢,到清华大学开源软件镜像站下载较快,如图 5.1 所示。选择任意安装版本均可,下载的是 kali-2020.4 目录下的 Kali-Linux-2020.4-live-i386.iso 文件。因为教学使用,所以在虚拟机下安装 Kali Linux,安装步骤如下。

https://mirrors.tuna.tsinghua.edu.cn/kali-images/		11 + ~ Q
R ② 同社大全 〇, 360復要 営 百亥一下 ⑥ 調放中心 デ Index of 図 Kali Linu		
funa 清华大学开源软件镜像站	HOME EVENT	S BLOG RSS PODCAST MIRRORS
Index of /kali-images/		Last Update: 2021-02-09 08:27
File Name ↓	File Size 4	Date ↓
Parent directory/	-	2
current/		2020-11-17 23:39
kali-2020.1/	0.220	2020-02-14 15:54
kali-2020.1b/	1.52	2020-03-18 03:47
kali-2020.2/		2020-05-12 00:48
kali-2020.3/	543	2020-08-18 22:31
kali-2020.4/		2020-11-17 23:39
kali-weekly/		2021-02-07 10:03
project/	-	2014-12-04 22:11
README	519 B	2019-01-14 21:57

图 5.1 下载网站

1. 新建虚拟机

(1) 虚拟机的安装比较简单,这里就不再叙述,在"虚拟机文件(F)"下新建虚拟机,选择"自定义(高级)(C)"单选按钮,如图 5.2 所示,单击"下一步"按钮。



图 5.2 自定义安装

(2)选择"稍后安装操作系统(S)"单选按钮,如图 5.3 所示,单击"下一步"按钮。

V建1位9人17日91年9				6
安装客户机操作系统 虚拟机如同物理机	1,需要操作系	系统。您将如何到	安装客户机操作系	系统?
安装来源:				
○安装程序光盘(D):				
无可用驱动器			~	
_				
〇安装程序光盘映像文	;件(iso)(M):			
〇安装程序光盘映像文 F:\攻防软件\kall-lin	(†(iso)(M): ux-2020.4-live	e-i386.iso	~	浏览(R)
〇安装程序光盘映像文 F:\攻防软件\kali-lin	(#(iso)(M): ux-2020.4-live	e-i386.iso	×	浏览(R)
○ 安装程序光盘映像文 F:\政防软件\kali-lin ● 稍后安装操作系统(5	(†(iso)(M): ux-2020.4-live ;)。	e-i386.iso	~	浏览(R)
 安装程序光盘映像文 F:\攻防软件\kall-lin 商后安装操作系统(S 创建的虚拟机将包含 	(件(iso)(M): ux-2020.4-live ;)。 ;一个空白硬盘	e-1386.iso	×	浏览(R)
 ・ ・ ・	(件(iso)(M): ux-2020.4-live ;)。 ;一个空白硬盘	e-1386.iso	×	浏览(R)
 ・ ・ ・	(件(iso)(M): ux-2020.4-live 5)。 ;一个空白硬盘	e-386.iso to	×	浏览(R)

图 5.3 稍后安装操作系统

(3) 客户机操作系统选择"Linux(L)",版本选择 Debian 7.x,如图 5.4 所示,单击"下一步"按钮。

4.择宽白机操作玄结	
此虚拟机中将安装哪种操作系统	
户机操作系统	
Microsoft Windows(W)	
Linux(L)	
VMware ESX(X)	
其他(0)	
本(V)	
ebian 7.x	~

图 5.4 操作系统的选择

(4) 定义虚拟机的名字和安装的位置,这里名字为 kali,安装到 F:\kali,如图 5.5 所示,单击"下一步"按钮。

(5)分配虚拟机的内存,至少为2GB,如图5.6所示,单击"下一步"按钮。

(6) 网络选择默认的 NAT 方式,如图 5.7 所示,单击"下一步"按钮。



程虚拟机向导		
命名虚拟机 您希望该虚拟机	使用什么名称?	
虚拟机名称(V):		
kali		
位置(L):		
F:\kali	浏览(R)	
在"编辑">"首选项"中可	更改數认位置。	

图 5.5 定义名字和安装目录

此虚拟机的	的内存	
您要 2	的此虚拟机使用多少内存?	
指定分配给此	虚拟机的内存重。内存大小必须为 4 MB 的倍数。	
64 GB -	此虎拟机的内存(M): 2048 🗄	мв
32 GB	and the second	1000
16 GB	•	
8 G8		
4 GB -	■ 取入推祥/01行・ 12 4 CD	
2 GB 🕊	13.4 00	
1 GB -		
512 MB	▲ 推行/1/1子· 512 MB	
256 MB	512 PD	
128 MD -	■ 方白机晶化系结晶低体装肉方・	
32 MB	64 MB	
16 MB	01110	
8 MB -		
4 MB		
#coh	< 上 下(N) 、	un este

图 5.6 定义内存

建虚拟机向导	E3
网络类型 要添加哪类网络?	,
网络连接	
○使用桥接网络(R) 为客户机操作系统提 有自己的 IP 地址。	供直接访问外部以太网网络的权限。客户机在外部网络上必须
●使用网络地址转换(N/ 为客户机操作系统提 权限。	AT)(E) 供使用主机 IP 地址访问主机拨号连接或外部以太网网络连接的
○使用仅主机模式网络(将客户机操作系统连	H) 接到主机上的专用虚拟网络。
○不使用网络连接(T)	

图 5.7 选择 NAT 方式

(7) 其他选择默认方式安装,指定磁盘大小为 50GB,将虚拟磁盘存储为单个文件,如 图 5.8 所示,单击"下一步"按钮。

新建虚拟机向导			23
指定磁盘容量 磁盘大小为多少?			
最大磁盘大小 (GB)(S):	50.0 🔹		
针对 Debian 7.x 的建议大):: 20 GB		
立即分配所有磁盘空间(A)•		
分配所有容重可以提高 空间,虚拟磁盘的空间	性能,但要求所有物理。 最初很小,会随着您向其	载盘空间立即可用。如果 其中添加数据而不断变大	不立即分配所有 。
● 将虚拟磁盘存储为单个5	2件(0)		
○ 将虚拟磁盘拆分成多个5	z件(M)		
拆分磁盘后,可以更轻	松地在计算机之间移动。	尉以机,但可能会降低大 得	等里磁盘的性能。

图 5.8 定义磁盘大小

(8) 指定 50GB 的磁盘文件存储的位置,存储到 F:\kali 下,文件名为 kali. vmdk,如 图 5.9 所示,单击"下一步"按钮。

的建造我们们可导		Σ
指定磁盘文件 您要在何处存储磁	盘文件?	
磁盘文件(F)		
将使用此文件名创建一个	▶ 50 GB 磁盘文件。	
F:\kali\kali.vmdk		浏览(R)

图 5.9 创建 Kali 的虚拟机文件

(9) 完成 Kali 虚拟机的创建, 如图 5.10 所示, 单击"完成"按钮。

(10) 创建完成后,在虚拟机的左面显示创建的虚拟机的名字 kali,如图 5.11 所示。

使用下列设置创	建虚拟机:
名称:	kali
位置:	F:\kali
版本:	Workstation 15.x
操作系统:	Debian 7.x
硬盘:	50 GB
内存:	2048 MB
网络适配器:	NAT
其他设备:	CD/DVD, USB 控制器, 打印机, 声卡

图 5.10 完成创建



图 5.11 创建好的虚拟机 Kali

2. 安装 Kali Linux

(1) 单击对话框中部"设备"下的"CD/DVD(IDE)"选项,添加 kali-linux-2020.4-livei386.iso 文件,如图 5.12 所示,单击"确定"按钮。

(2) 单击主界面下的绿色按钮,启动客户机操作系统,Kali 启动后的界面如图 5.13 所示,选择 Graphical install 选项,按回车键开始安装 Kali。

网络攻防项目实战(微课视频版)

设备 ■内存 型处理器 □ 硬盘 (SCSI) ③ CD/DVD (IDE) □ 网络适配器	摘要 2 GB 1 50 GB 自动检测 NAT	设备状态 □已连接(C) ☑ 启动时连接(O) 注接 ○ 使用物理驱动器(P):
④US8 控制器 □ 声卡 □ 打印机 □ 显示器	存在 自动检测 存在 自动检测	自动检测 ● 使用 ISO 映像文件(M): F:\攻防软件\kall-linux-2020.4 ✓
	添加(A) 移除(R)	7.8

图 5.12 添加 Kali 映像文件



图 5.13 Kali 启动后的界面

50

(3) 语言选择"中文(简体)",如图 5.14 所示,单击 Continue 按钮。

择一种语言	
Choose the language t anguage for the instal Language:	o be used for the installation process. The selected language will also be the default lled system.
Bangla	- বালা
Basque	- Euskara
Belarusian	- Беларуская
Bosnian	- Bosanski
Bulgarian	- Български
Burmese	- မြန်မာစာ
Catalan	- Català
Chinese (Simplified)	- 中文(简体)
Chinese (Traditional)	- 中文(繁體)
Croatian	- Hrvatski
Czech	- Čeština
Danish	- Dansk
Dutch	- Nederlands
Dzongkha	• 长 月
5	rlish

图 5.14 选择中文简体

(4) 区域选择"中国",如图 5.15 所示,单击"继续"按钮。

选择您的区域					
指的区域将被用于设置您	的时区以及其他例如帮	帮助决定系统区域。	通常这应该为您月	f居住的国家或地区。	
2是根据您所选择的语言产 <i>国家或地区:</i>	生的短列表。如果没有	亨列出您的区域, ;	青选择"其他"。		
PE					
清					
所加坡					
1港					
C 他					

图 5.15 区域选择



(5) 键盘选择"汉语",如图 5.16 所示,单击"继续"按

K sv offe				
記』後盘				
请选择键盘映射:				
英式英语				<u>_</u>
保加利亚语 (BDS 布局)				
保加利亚语(拼音布局)				- E
缅甸语				
加拿大法语				_
加拿大多语言				_
加泰罗尼亚语				
汉语			antan dia amin'ny sola	
克罗地亚语				
捷克语				_
丹麦语				
荷兰语				_
德沃夏克式 (Dvorak)				
不丹语				
世界语				~
屏幕截图		Г	50 KO	維統

图 5.16 键盘的选择

(6) 定义主机名,此处为 kali,如图 5.17 所示,单击"继续"按钮。

	KALI BY OFFENSIVE SECUR	IIIY		
記量网络				
请输入系统的主机名。 主机名是在网络中标示您的系统的一个单词 名字。	。如果您不知道主机名是什么,请该	间网络管理员。如果您正在设置	内部网络,那么可	可以随意写个
主机名: [1]				
屏幕截图			返回	继续

图 5.17 定义主机名



重网络			
轻是您的互联网地址的一部分,附加在主机名之后。它通常是以,com、 【随意写一个,但是要确保您所有计算机的域名都是一样的。 域名:	.net、.edu 或 .org	结尾。如果您正在设置一个	内部网络,您可

图 5.18 配置网络

(8)设置用户名,如图 5.19 所示,单击"继续"按钮。

设置用户和密码		
程序将创建一个用来取代 root 执行非管理任务的普通用户帐号。 请输入此用户的真实名称。这项信息将被用作该用户所发邮件的默认来源,同时还会被用于所有显示和使用该用户 名就是一个很合适的选择。 <i>请输入新用户的全名</i> :	□真实名称的程序	亨中。您的全
malimei		
屏幕截图	返回	继续

图 5.19 设置用户名