第 3 章　Kali Linux 攻防系统实验

3.1　Kali Linux 及基本攻防技术简介

3.1.1　Kali Linux 简介

Kali Linux 是基于 Debian 的 Linux 发行版，是用于数字取证的操作系统，由 Offensive Security 公司开发、维护和资助。Kali Linux 最先是由 Offensive Security 公司的 Mati Aharoni 和 Devon Kearns 通过重新编写 BackTrack 来完成的，BackTrack 是他们编写的用于取证的 Linux 发行版。

Kali Linux 预装了许多渗透测试软件，包括 nmap、Wireshark、John the Ripper 以及 Aircrack-ng。用户可通过硬盘、LiveCD 或 LiveUSB 运行 Kali Linux。Kali Linux 有 32 位和 64 位的镜像，可用于 x86 指令集；同时还有基于 ARM 架构的镜像，可用于树莓派和三星公司的 ARM Chromebook。

Kali Linux 的设计目的是进行高级渗透测试和安全审核。Kali 包含数百种工具，可用于各种信息安全任务，例如渗透测试、安全研究计算机取证和逆向工程。

1. Kali Linux 的特点

Kali Linux 主要有以下特点：

(1) Kali Linux 包括 600 多个渗透测试工具。

(2) Kali Linux 是永久免费的。

(3) Kali Linux 提供开源开发树。Kali Linux 向用户提供了开源的开发模型，其开发树可供所有人使用。

(4) Kali Linux 符合文件系统层次结构标准，使 Linux 用户可以轻松地找到二进制文件、支持文件和库等。

(5) Kali Linux 对无线设备有广泛的支持。对无线接口缺乏支持是 Linux 发行版的常见症结。Kali Linux 广泛支持各种无线设备，从而使其能够在各种硬件上正常运行，并使其与众多 USB 和其他无线设备兼容。

(6) Kali Linux 拥有自定义内核，其中包含最新的注入补丁。

(7) Kali Linux 是在安全的环境中开发的。Kali Linux 开发团队由很少的人组成，这些人是被授权提交包并与存储库交互的可信的人。所有开发工作通过用多种安全协议来完成。

(8) Kali Linux 拥有 GPG 签名的软件包和存储库。Kali Linux 中的每个软件包均由构建和提交该软件包的开发人员签名，存储库也对软件包进行了签名。

(9) Kali Linux 支持多种语言。尽管渗透工具通常是用英语编写的，但 Kali 真正支持多种语言，从而使更多的用户可以使用其母语进行操作并找到他们所需的工具。

(10) Kali Linux 是完全可定制的。用户可以轻松地按照自己的喜好自定义 Kali

Linux，包括 Kali Linux 的内核。

(11) Kali Linux 支持 ARMEL 和 ARMHF。由于 Raspberry Pi 和 BeagleBone Black 等基于 ARM 的单板系统正变得越来越常见和廉价，因此，Kali Linux 提供了对 ARM 的强大支持。Kali Linux 在大量的 ARM 设备上可用，并且具有与主线发行版集成的 ARM 存储库。

2. Kali Linux 与其他 Linux 系统的区别

提到 Kali Linux，就不能不提另一款广为人知的操作系统，即 Kali Linux 的前身 BackTrack。从 BackTrack 变为 Kali Linux 的原因主要是：人们发现一直以来使用的 BackTrack 内核版本(V.10.04) 出现了问题。因此有必要整合一些常用的工具，摒弃一些因为时代变化而不再适用的工具或者长时间没有更新的工具。

通过对比 Kali Linux 和 BackTrack 可以发现，虽然二者在 UI 和界面上没有明显的变化，但是 Kali Linux 明显包含了更多的新工具，从内部系统架构来说发生了根本性的改变。

3. Kali Linux 包含的测试工具

Kali Linux 包含网络安全渗透测试需要的绝大部分测试工具。下面介绍其中 10 个主要工具。

(1) AssassinGo。AssassinGo 是基于 Go 的高并发可拓展式 Web 渗透框架。AssassinGo 是一个可扩展和并发的信息收集和漏洞扫描框架，该框架基于 Vue 的 WebGUI，前后端交互主要采用 WebSocket 技术，会将结果实时显示在前台。AssassinGo 集成了高可用信息收集、基础攻击向量探测、Google-Hacking 综合搜索和 PoC 自定义添加并对目标进行批量检测等功能的自动化 Web 渗透框架。

(2) burpa:burp。burpa:burp 是自动化扫描工具。它使用 burpsuite 自动化扫描网站，并将扫描结果输出成报告。

(3) websocket-fuzzer。websocket-fuzzer 用于应用程序渗透测试。它提供了两个工具：websocket-fuzzer.py 用于接收一个 WebSocket 的消息，修改该消息，然后以不同的连接发送该消息，并对响应进行分析以发现潜在的漏洞；send-one-message.py 使用新连接发送 WebSocket 消息

(4) Reptile。Reptile 是 LKM Linux rootkit(内核级病毒木马)。Reptile 的功能包括获得 root 权限、隐藏文件和目录、隐藏文件内容、隐藏进程、隐藏自己、设置 TCMP/UDP/TCP 端口后门。

(5) juice-shop。juice-shop 是用 Node.js 编写的 Web 安全漏洞测试工具。

(6) badpdf。badpdf 可以创建恶意 PDF 文档，从 Windows 计算机上窃取 NTLM 哈希值。

(7) GPON。GPON 是路由器远程代码执行漏洞利用脚本工具。vpnMentor 公布了 GPON 路由器的高危漏洞：验证绕过漏洞(CVE-2018-10561) 和命令注入漏洞(CVE-2018-10562)。将这两个漏洞结合，只需要发送一个请求，就可以利用 GPON 编写脚本，在路由器上执行任意命令。

(8) watchdog。watchdog 是一款全面的安全扫描和漏洞管理工具，其扫描引擎包括 Nmap、Skipfish、Wapiti、BuiltWith、Phantalyzer 和 Wappalyzer。watchdog 安装时自带 CVE 漏洞数据库，由多个 CVE 数据源(exploitdb、cves 等)集合而成。

(9) pypykatz。pypykatz 是轻量级调试器 mimikatz 的纯 Python 语言版本。mimikatz 是用 C 语言编写的开源工具,功能非常强大,它支持从 Windows 系统内存中提取明文密码、哈希值、PIN 码和 Kerberos 凭证。

(10) CertDB。CertDB 是一个免费的 SSL 证书搜索引擎和分析平台,通过 API 可以进行证书的查询。

3.1.2 Kali Linux 基本攻防技术简介

1. 网络嗅探技术

无线局域网(俗称 WiFi)基于 IEEE 802.11b/g/n 标准。因为它在搭建时使用廉价、简便、小型的设备,所以在许多领域获得了越来越广泛的应用。尤其是随着智能手机近两年的普及,更是加速了人们在日常生活和工作中对无线网络的需求甚至是依赖。无线终端设备通过服务及标识符(也就是 SSID)来标识和加入无线局域网。当无线终端进入一个接入点的覆盖范围时,便接入了无线局域网。由于无线网络通信可能会将电磁信号泄露于室外,建筑无法完全屏蔽信号,如果不使用认证或者安全的加密技术,入侵者只要监听到这个无线网络的 SSID,就可以将自己的设备加入这个无线网络。即使路由器中使用了 MAC 地址访问限制等手段,入侵者也可以采用伪造 MAC 地址的方法让 MAC 地址控制表的作用失效。在网络中窃取数据就叫嗅探,它是利用计算机的网络接口截获网络中流转的数据报文的一种技术。嗅探一般工作在网络的底层,可以在不被察觉的情况下将网络传输的全部数据记录下来,从而捕获账号和口令信息;甚至可以用来危害处在同一无线局域网中的其他网络使用者的安全,或者用来获取更高级别的访问权限、分析网络结构、进行网络渗透等,网络嗅探往往是黑客入侵的前奏。

很多人对无线网络安全不以为然,认为自己所使用的 WiFi 是经过加密的,别人即便知道了密码,也无法看到自己的浏览记录。在无线局域网中,网络嗅探的隐蔽性来自其被动性和非干扰性。运行监听程序的主机在窃听的过程中只是被动地接收网络中传输的信息,而不会跟其他主机交换信息,也不修改在网络中传输的信息包,使得网络嗅探具有很强的隐蔽性,往往让网络信息泄密事件很难被发现。尽管网络嗅探没有对网络进行主动攻击和破坏的危害明显,但它造成的损失也是不可估量的。只有通过分析网络嗅探的原理与本质,才能有效地防患于未然,增强无线局域网的安全防护能力。

要理解网络嗅探的实质,首先要清楚数据在网络中封装、传输的过程。根据 TCP/IP 协议,数据包是经过层层封装后被发送的。假设客户机 A、B 和 FTP 服务器 C 通过无线连接设备连接,主机 A 通过使用一个 FTP 命令向主机 C 进行远程登录,进行文件下载。那么首先在主机 A 上输入登录主机 C 的 FTP 口令,FTP 口令经过应用层 FTP 协议、传输层 TCP 协议、网络层 IP 协议、数据链路层上的以太网驱动程序一层一层包裹,最后送到物理层,再通过无线的方式发送出去。主机 C 接收到数据帧,并在比较之后发现是发给自己的,接下来它就对此数据帧进行分析处理。这时主机 B 也同样接收到主机 A 发送的数据帧,随后就检查数据帧中的地址是否和自己的地址相匹配,发现不匹配,就把数据帧丢弃。这就是基于 TCP/IP 通信的一般过程。

网络嗅探就是从通信中捕获和解析信息。假设主机 B 想知道登录服务器 C 的 FTP 口令是什么,那么它要做的就是捕获主机 A 发送的数据帧,对数据帧进行解析,依次剥离出以

太帧头、IP 包头、TCP 包头等，然后对包头部分和数据部分进行相应的分析处理，从而得到包含在数据帧中的有用信息。

在实现嗅探时，首先设置用于嗅探的计算机，即在嗅探机上装好无线网卡，并把网卡设置为混杂模式。在混杂模式下，网卡能够接收一切通过它的数据包，进而对数据包进行解析，实现数据窃听。其次实现循环抓取数据包，并将抓到的数据包送入数据解析模块处理。最后进行数据解析，依次提取出以太帧头、IP 包头、TCP 包头等，然后对各个包头部分和数据部分进行相应的分析处理。

Ettercap 是 Kali Linux 下的一个强大的欺骗工具，在 Windows 下也有相应的版本，使用它能够快速创建和发送伪造的包，可以发送从网络适配器到应用软件各种级别的包。它可以绑定监听数据到一个本地端口中，即从一个客户端连接到这个端口，并且对不知道的协议进行解码或者把数据插进去。

Ettercap 是一款在局域网中进行中间人攻击的软件，它通过 ARP 攻击作为网络信息传输中的中间人，一旦 ARP 攻击奏效，它就可以修改数据连接，截获 FTP、HTTP、POP 和 SSH 等协议的密码，通过伪造 SSL 证书的手段劫持被测主机的 HTTPS 会话。

ARP 是地址解析协议，用来把 IP 地址解析为物理地址，也就是 MAC 地址，当某个网络设备需要与其他网络设备通信时，它会通过 ARP 广播查询目标设备的 MAC 地址。目标设备会通过 ARP 的数据包反馈自己的 MAC 地址，然后通信双方都会将 IP 地址和 MAC 地址所对应的信息保存在自己的 ARP 缓存中，这样做能够提高效率，节省后续通信的查询成本。当某台主机要进行通信时，它会首先查询目标主机的 IP 地址和 MAC 地址，此时，攻击者可以将自己的主机的 MAC 地址回复给查询 MAC 地址的主机，以发动中间人攻击。这种攻击叫作 ARP 污染攻击和 ARP 欺骗，只有攻击者的主机和目标主机处于局域网的同一网段，这种攻击才会有效。

Ettercap 有两种运行方式：UNIFIED 和 BRIDGED。

UNIFIED 方式是以中间人方式嗅探；BRIDGED 方式是在双网卡情况下嗅探两块网卡之间的数据包。UNIFIED 方式的大致原理为：同时欺骗主机 A 和 B，把 A 和 B 原本要发给对方的数据包都发送到第三者 C 上，然后由 C 再转发给目标主机。这样 C 就充当了一个中间人的角色。因为数据包会通过 C，所以 C 可以对数据包进行分析和处理，导致原本只属于 A 和 B 的信息泄露给 C。UNIFIED 方式将完成以上欺骗并对数据包进行分析。Ettercap 劫持的是 A 和 B 之间的通信。从 Ettercap 的角度来看，A 和 B 的关系是对等的。

BRIDGED 方式有点像笔记本计算机上有两个网卡，一个是有线网卡，另一个是无线网卡。可以将有线网卡的网络连接共享给无线网卡，这样笔记本计算机就变成了一个无线 AP。无线网卡产生的所有数据流量都将传送给有线网卡。在 BRIDGED 方式下，Ettercap 嗅探的就是这两个网卡之间的数据包。

本实验使用 UNIFIED 方式。

2. 渗透测试技术

渗透测试是通过模拟攻击者使用的手段攻破目标系统安全防线，取得服务器或者设备的访问权与控制权，并且发现某些存在安全隐患的漏洞的一种测试手段。

渗透测试的过程就是对目标主机系统进行一些主动探测，以发现潜在的系统安全隐患，包括错误的系统配置以及已知或者未知的操作系统漏洞和软件硬件漏洞。渗透测试分为两

种类型：黑盒测试和白盒测试。

黑盒测试就是模拟一个对目标系统的技术细节一无所知的攻击者的测试。白盒测试恰恰相反，是模拟拥有全部目标系统资料的攻击者的测试。

PTES渗透测试执行标准是由安全业界很多领军企业共同发起的，在这个标准中定义的渗透测试过程得到安全业界的普遍认同，包括以下7个阶段。

1）前期交互阶段

在前期交互阶段，渗透测试团队与客户组织进行交互，最重要的是确定渗透测试的范围、目标、限制条件和服务合同细节。

2）情报搜集阶段

在目标范围确定之后，就进入情报搜集阶段，渗透测试团队会利用各种信息来源和搜集技术，尝试获取关于目标组织网络拓扑、系统配置和安全防御措施的信息。渗透测试者可以使用的情报搜集方法包括公开信息查询、搜索引擎、社会工程学、网络踩点、扫描探测、被动监听等技术手段。情报搜集得越多、越详细，对渗透测试的帮助越大。情报搜集是否充分在很大程度上决定了渗透测试的成败。

3）威胁建模阶段

在搜集到充分的情报后，渗透团队的成员会针对获取的信息进行威胁建模与攻击规划。这是渗透测试过程中很重要但往往会被遗漏的一个关键点。它可以从大量的情报信息中理清头绪，确定最可行的攻击通道。

4）漏洞分析阶段

在确定最可行的攻击通道后，接下来考虑如何取得目标系统的访问控制权，也就是进入漏洞分析阶段。在该阶段，渗透测试者需要综合分析前几个阶段获取和汇总的情报、安全漏洞扫描结果、服务信息和渗透代码资源，找出可以实施渗透攻击的切入点，并在实验环境中进行验证。在这个阶段还可以针对攻击通道上的一些关键系统与服务进行安全漏洞探测与挖掘，找出可被利用的安全漏洞，开发渗透代码，打开攻击通道上的关键路径。

5）渗透攻击阶段

在渗透攻击阶段，渗透测试团队需要利用找出的目标系统安全漏洞入侵真正的目标系统，获得其访问控制权限。渗透攻击可以采用公开渠道的开源的渗透代码，但在实际环境中，需要根据灵活多变的环境具体决定攻击方法，并且需要击败目标网络和系统中可能存在的防御体系和防御机制，才能成功渗透。在黑盒测试中，渗透攻击者还需要考虑在渗透过程中的逃逸机制，避免引起目标主机系统的警觉和发现，从而彻底暴露自己。

6）后渗透攻击阶段

后渗透攻击阶段是整个渗透过程中最能体现渗透测试团队的技术能力的环节。在这个阶段中，渗透测试团队要根据目标组织的业务经营模式、保护资产形式与安全防御计划的不同特点自主发现攻击目标，识别关键基础设施，并寻找客户组织最具价值和受到安全保护的信息和资产，最终打开能够对客户组织造成最重要业务影响的攻击途径。在不同的渗透测试场景中，这些攻击目标与途径可能是千变万化的，而设置是否准确及可行，也取决于渗透测试团队自身的创新意识、知识范畴、实际经验和技术能力。

7）报告阶段

渗透测试过程最终向客户组织提交，取得认可并成功获得合同付款的就是渗透测试报

告。这份报告凝聚了前面所有阶段中渗透测试团队获取的关键情报、探测和发现的系统安全漏洞、成功渗透攻击的过程以及造成业务影响后果的攻击途径，同时还要站在防御者的角度，帮助他们分析安全防御体系中的薄弱环节、存在的问题以及修补与升级技术方案。

渗透测试最核心的目的就是找出目标系统中存在的漏洞，并且利用这个安全漏洞扩大战果，实施渗透攻击，从而达到进入目标主机系统的最终目的。而这一过程中最主要的基础就是目标系统中可能存在的安全漏洞。安全漏洞是指系统中存在的缺陷，这个缺陷往往是操作系统编写者或应用软件编写者在软件开发过程中无意地留下的，它可以使攻击者在未获授权的情况下访问系统、提升特权并且破坏系统。安全漏洞是有生命周期的，它的周期主要分为 7 部分：

(1) 安全漏洞研究与挖掘。

(2) 升渗透代码开发与测试。

(3) 安全漏洞和渗透代码在封闭团队中的流传。

(4) 安全漏洞和渗透代码的扩散。

(5) 恶意程序的开发和传播。

(6) 渗透代码和恶意程序大规模的传播并对互联网造成危害。

(7) 渗透攻击代码和恶意程序的消亡。

在 Kali Linux 系统中，有很多与渗透相关的专用软件，例如 Nmap、Zenmap，以及很有名气的 Metasploit。

端口扫描是一种用来确定目标主机 TCP 端口和 UDP 端口状态的方法。目标主机开放了某个端口，就表示它的这个端口提供某种网络服务，如果这个端口关闭，就说明主机在这个端口上没有网络服务。

TCP/IP 是很多网络协议的统称。IP 提供了寻址、路由等主机互联的功能；而 TCP 协议则约定了连接管理，在两台主机间建立了可靠的数据通信的标准。IP 是 OSI 参考模型中的第三层协议，而 TCP 协议则是传输层协议。

Nmap 的全称是 Network mapper，翻译过来也就是网络映射工具。Nmap 是一个开源的网络探测工具。开发它的目的是为了快速扫描庞大的网络，它通过扫描并且使用原始的 IP 报文来发现网络上都有哪些主机和终端，这些主机与终端都提供什么样的互联网服务，运行哪些应用程序以及软件版本，运行在什么样的操作系统上，使用了什么类型的报文过滤器和防火墙以及杀毒软件。虽然 Nmap 常用于渗透测试和安全审计中，其实许多网络管理员和大型信息系统管理员也常用它来做一些日常运维工作，例如监视主机系统服务运行的情况，管理对服务器的升级计划，使其管辖的网络整体情况尽收眼底，极大地提高了管理效率。

Nmap 是被网络管理员和黑客广泛使用的一款功能全面的端口扫描工具，除了端口扫描以外，Nmap 还具备以下功能：

(1) 主机探测。Nmap 可查找目标网络环境中的所有在线主机。一般来说，它通过 4 种方式发现目标主机，分别是 ICMP echo 请求、向 443 端口发送 TCP SYN 包、向 80 号端口发送 TCP ACK 包和 ICMP 时间戳请求。

(2) 版本和服务检测。在发现了开放的端口之后，Nmap 可以进一步检查目标主机的服务协议、应用程序名称和版本号。

(3) 操作系统检测。Nmap 向目标主机发送一系列数据包，并能够将目标主机的响应与操作系统的指纹数据库进行比较，一旦发现了有匹配结果，就会显示目标主机的操作系统。

(4) 网络路由跟踪。Nmap 通过多种协议访问目标主机的不同端口，Nmap 路由跟踪功能从 TTL 高值开始测试，逐步递减，直到 TTL 为 0。

(5) Nmap 脚本引擎。它扩充了 Nmap 的用途，可以利用它编写检测脚本。

Nmap 可以识别 6 种端口状态：

(1) Open(开放)。在目标主机开放的端口工作的程序可以接收 TCP 连接请求、UDP 数据包或者响应 SCTP 请求。

(2) Closed(关闭)。关闭的目标主机端口可以被探测到，但是在该端口没有运行的应用程序。

(3) Filtered(过滤)。Nmap 不能确定目标主机的某端口是否开放，包过滤设备屏蔽了 Nmap 向目标主机发送的探测包。

(4) Unfiltered(未过滤)。Nmap 可以访问目标主机的某个端口，但是无法确定这个端口是否开放。

(5) Open|Filtered(打开|过滤)。Nmap 认为目标主机的指定端口处于开放或者过滤状态，但是无法确定是其中的哪一个状态。在遇到没有响应的开放端口时，Nmap 会将其识别为这种状态。这种情况可能是由于防火墙丢弃数据包造成的。

(6) Closed|Filtered(关闭|过滤)。Nmap 认为目标主机的指定端口处于关闭或者过滤状态，但是无法确定是其中的哪一个状态。

在 Kali Linux 系统中，集成了一款堪称神器的渗透测试工具——Metasploit。它是一个渗透测试的框架，也是一个日益成熟的软件漏洞研究与探索开发的平台。正是因为这个平台的出现，使安全工作者及白帽黑客告别了以往烦琐的渗透测试过程，从搜索公开的渗透代码再到编译、测试、修改代码，最后通过不断地测试、失败、再测试、再失败……直至成功，这个传统的过程令行业初学者望而生畏。正因为如此，Metasploit 在发布之后很快得到了安全社区的青睐。

任何一个有效的网络攻击都起步于事先完善的侦察，攻击者必须在挑选并确定利用目标中的哪一个漏洞之前找出目标在哪里有漏洞。为了与 TCP 端口进行交互，首先要建立 TCP 套接字。与其他编程语言类似，Python 也提供了访问 BSD 套接字的接口。BSD 套接字提供了一个应用编程接口(Application Programming Interface，API)，使程序员能编写在主机之间进行网络通信的应用程序。通过一系列 API 函数，可以创建、绑定、监听、连接以及在 TCP/IP 套接字上发送数据。所有成功的网络攻击一般都是以端口扫描拉开序幕的。有一种类型的端口扫描会向一系列常用的端口发送 TCP SYN 数据包，并等待 TCP ACK 响应，通过响应能确认这个端口是开放的。而 TCP 连接扫描通过完整的三次握手来确定服务器和端口是否可用。

除了渗透攻击，Metasploit 还逐渐完善了对渗透测试的全过程的支持，包括如下 5 个阶段：

(1) 情报搜集阶段。

(2) 威胁建模阶段。

(3) 漏洞分析阶段。

(4) 后渗透攻击阶段。

(5) 报告生成阶段。

情报搜集就是搜集渗透攻击的成功实施必不可少的精确资料。Metasploit 一方面通过内建的一系列扫描探测以及查点辅助模块获取远程服务信息;另一方面通过插件机制集成调用前面介绍过的端口扫描工具(如 Nmap 等),从而具备全面的信息搜索能力。在获得并掌握了目标主机和网络的大量第一手资料后,Metasploit 会将这些资料以数据的形式汇总并且存储于 MySQL 等数据库中,为用户提供简洁的数据查询命令,这就是 Metasploit 的威胁建模功能,它能帮助渗透测试者在海量的情报中找出最可行的攻击路径。除了情报搜集阶段使用扫描工具能够扫描出一些已经发布的安全漏洞外,Metasploit 还提供了大量的协议模糊测试器和 Web 应用漏洞探测分析模块,可以让渗透测试者尝试挖掘出零日漏洞。在成功实施了渗透攻击并且取得目标主机的远程控制权限后,Metasploit 提供了一个强大的工具——Meterpreter。它是一个支持多种操作系统平台,可以驻留在内存中并且具备免杀能力的高级后门工具,它包含特权提升、系统监控、跳板攻击以及内网拓展等功能模块。

Kali Linux 预装了几款高级漏洞利用程序工具集,其中就有大名鼎鼎的 Metasploit 框架(Metasploit Framework)。Metasploit 框架是用 Ruby 语言编写的模板化框架,具有极佳的扩展性,为渗透开发与测试人员提供了极为方便的工具模板。Metasploit 框架可以分为三大组成部分:库、界面和模板。Metasploit 框架的模板主要有以下 5 个:

(1) exploit。这是漏洞利用程序模板,包含了各种 PoC(Proof of Concept,概念验证)程序,用于验证利用特定漏洞的可行性。

(2) payload。这是有效载荷模板,包含了各种恶意程序,用于在目标系统上运行任意命令,它既可以是 exploit 的一部分,也可以是独立编译的应用程序。

(3) Auxiliaries。这是辅助工具模板,包含了一系列扫描、嗅探、指纹识别、拨号测试以及其他类型的安全评估程序。

(4) Encoder。这是编码工具模板。在渗透测试中,这个模板用来加密有效载荷,以避免被杀毒软件、防火墙、IDS(Intrusion Detection System,入侵检测系统)或者 IPS(Intrusion preventon System,入侵防御系统)以及其他类似的软件检测出来,能起到一定的免杀作用。

(5) NOP。这是空操作模板,这个模板用于在 Shellcode 中插入 NOP 指令。虽然这个指令不会进行实际的操作,但是在构造 Shellcode 时可以用来暂时替代 Playload,从而形成完整的 Shellcode 程序。Shellcode 指的是能够完成某一项任务的自包含的二进制代码,这个任务既可以是发出一条系统命令,也可以是为攻击者提供一个 Shell(这正是 Shellcode 产生的根源)。Shellcode 的编写方式有 3 种:直接编写十六进制操作码;采用 C 语言等高级语言编写程序,然后进行编译,最后进行反汇编以获取汇编指令和十六进制操作码;编写汇编程序,将该程序汇编,然后从二进制数码中提取十六进制操作码。

3.2 攻防实验

实验器材

Kali 镜像文件 1 套。

PC(Linux/Windows 10)1 台。

预习要求

做好实验预习,了解 Kali Linux 有关内容。
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) 了解 Ubuntu 以及 Kali Linux。
(2) 了解 Kali Linux 攻防基本原理并上机实践。

实验环境

下载虚拟机软件、Kali Linux 镜像。PC 使用 Windows 操作系统或 Linux 操作系统。

预备知识

了解 Kali Linux 和 Ubuntu 的相关知识。
了解虚拟机的使用以及安装方式。

实验步骤

1. 下载并安装虚拟机软件

(1) 经进入 VMware 官方下载地址 https://www.vmware.com/cn.html,在首页顶部导航栏选择“下载”选项,进入“下载”界面,如图 3-1 所示。

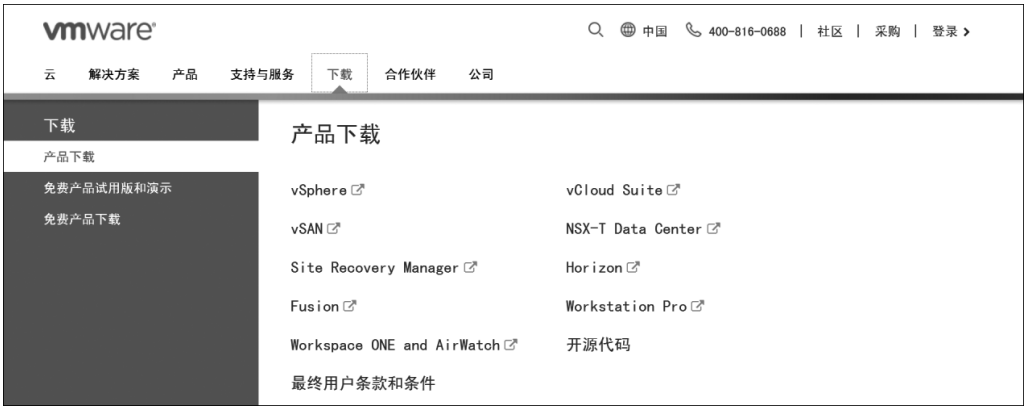

图 3-1 VMware 官网的“下载”界面

(2) 在“下载”界面选择 Workstation Pro,进入“下载 VMware Workstation Pro”界面。在这里以 Windows 系统为例,单击 VMware Workstation 14.1.2 Pro for Windows 右侧的“转至下载”按钮,如图 3-2 所示。

(3) 进入“下载产品”界面后,可以在“选择版本”右侧的下拉列表框中选择要安装的版

图 3-2　“下载 VMware Workstation Pro”界面

本。本实验使用的版本是 14.1.2。选择版本后，单击“立即下载”按钮，开始下载 VMware Workstation Pro 安装文件，如图 3-3 所示。

图 3-3　“下载产品”界面

(4) 打开扩展名为.exe 的 VMware Workstation Pro 安装文件，即可启动 VMware Workstation Pro 安装向导，如图 3-4 所示。

(5) 安装位置默认在 C 盘中。用户可以根据需要设置安装路径，本实验将 VMware Workstation Pro 安装到 D 盘的 VMware 文件夹中，如图 3-5 所示。注意，安装路径中不要有中文。

图 3-4　VMware Workstation Pro 安装向导

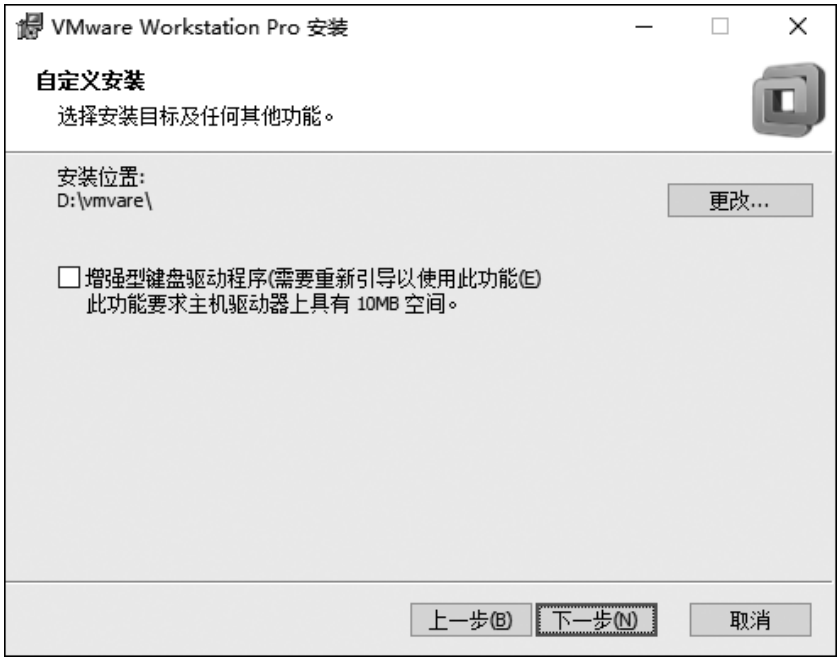

图 3-5　设置安装路径

(6) 按照 VMware Workstation Pro 安装向导的指示一步一步地进行下去。当采用默认方式安装时,可以在每一步直接单击“下一步”按钮,直至出现安装完成提示时为止,如

图 3-6 所示。

图 3-6　安装完成提示

（7）在第一次运行程序时会要求用户输入许可证密钥，如图 3-7 所示。在此可以选中“我希望试用 VMware Workstation 14 30 天”单选按钮。

图 3-7　输入许可证密钥

随后即可进入 VM Workstation 的主界面，如图 3-8 所示。

2. 创建虚拟机

创建虚拟机时，可以采用两种方案。

图 3-8　VM Workstation 主界面

1）第一种方案

创建虚拟机的第一种方案步骤如下：

（1）在 www.kali.org 网站下载 Kali Linux 安装程序光盘映像文件 kali-linux-2019.4-amd64.iso。

（2）在 VM Workstation 主界面中单击“创建新的虚拟机”按钮，在“新建虚拟机向导”对话框中选中“典型（推荐）”单选按钮，如图 3-9 所示。

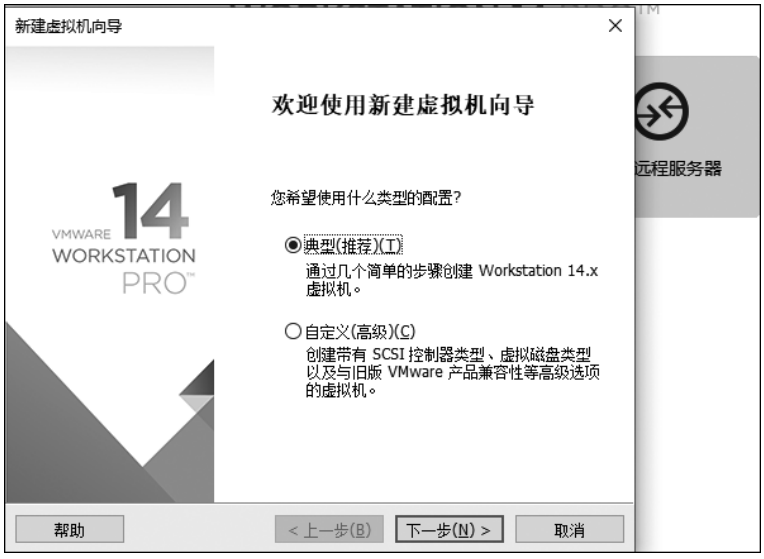

图 3-9　“新建虚拟机向导”对话框

（3）安装客户机操作系统。在“安装来源”下选中“安装程序光盘映像文件(iso)”单选按钮，在下面的下拉列表框中选择在步骤(1)中下载的 F:\kali-linux-2019.4-amd64.iso 所在的路径，如图 3-10 所示。

图 3-10　导入安装程序光盘映像文件界面

(4) 选择客户机操作系统及其版本。在“客户机操作系统”下选中 Linux 单选按钮,在“版本”下拉列表中选择“Debian 7.x 64 位”选项,如图 3-11 所示。

图 3-11　选择客户机操作系统及其版本

(5) 为虚拟机命名。给出虚拟机的名称,并确定其位置,如图 3-12 所示。

图 3-12　为虚拟机命名

(6) 指定磁盘容量。将“最大磁盘大小(GB)”设置为 50,选中“将虚拟磁盘存储为单个文件”单选按钮,如图 3-13 所示。单击“下一步”按钮,然后单击“完成”按钮,完成虚拟机的创建。

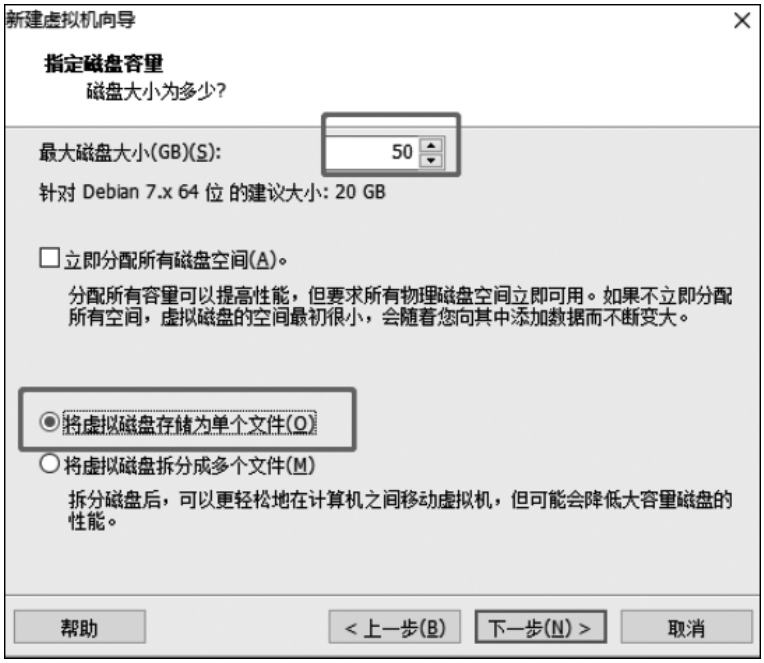

图 3-13　指定磁盘容量

(7) 启动虚拟机，进行配置，选择 Graphical install（图形界面安装）选项，如图 3-14 所示。

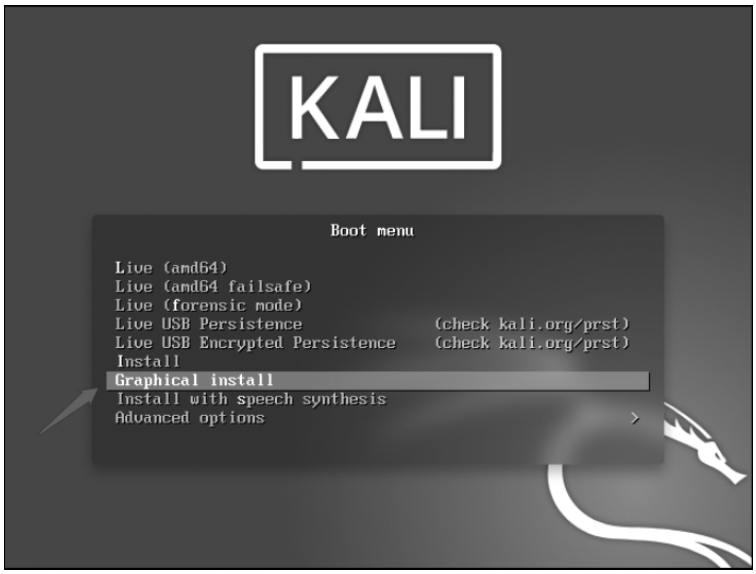

图 3-14　选择 Graphical install 选项

(8) 接下来选择语言，本实验选择中文。然后一直单击“继续”按钮，直到“配置网络”界面出现，在此输入主机名，如图 3-15 所示。

图 3-15　输入主机名

（9）设置用户和密码，如图 3-16 所示。

图 3-16　设置用户和密码

（10）接下来进行磁盘分区。推荐选择使用整个磁盘的分区方法，如图 3-17 所示。

图 3-17　进行磁盘分区

（11）接下来选择磁盘分区方案。推荐选择将所有文件放在同一分区中的分区方案，如图 3-18 所示。

图 3-18　选择磁盘分区方案

（12）选择“结束分区设定并将修改写入磁盘”，如图 3-19 所示。

图 3-19　选择“结束分区设定并将修改写入磁盘”

(13) 安装向导询问用户是否将改动写入磁盘，选中“是”单选按钮，如图 3-20 所示。

图 3-20　确认将改动写入磁盘

(14) 单击“继续”按钮之后，就正式开始系统安装，此时等待时间较长。在安装过程中，安装向导会询问用户是否将 GRUB 启动引导器安装到主引导记录(MBR)上，选中“是”单选按钮，如图 3-21 所示。

图 3-21　确认将 GRUB 启动引导器安装到主引导记录上

(15)选择安装启动引导器的设备。这里选择第二个选项：/dev/sda，如图 3-22 所示。

图 3-22　选择安装启动引导器的设备

(16)至此安装完成，如图 3-23 所示。

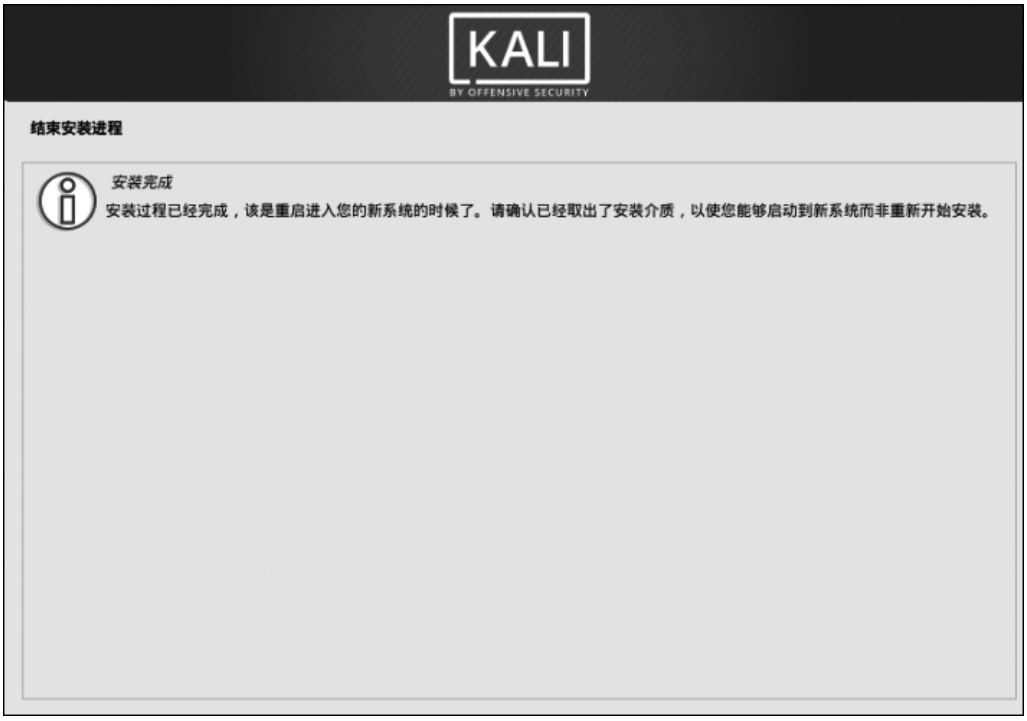

图 3-23　安装完成界面

2）第二种方案

创建虚拟机的第二种方案步骤如下：

(1) 在 www.kali.org 网站下载 kali-linux-2020-1-vmware-amd64-7z。

(2) 在 VM Workstation 主界面的菜单栏中选择“文件”→“扫描虚拟机”命令，如图 3-24 所示。

(3) 在弹出的“浏览文件夹”对话框中选择扫描路径，然后单击“确定”按钮，如图 3-25 所示。