**新手指南：手把手教你如何搭建自己的渗透测试环境**

## 介绍

白帽子是指个体发起的黑客攻击，找到系统潜在的可能被恶意黑客利用的的漏洞或脆弱点。在目标不知情或者没得到授权的情况下发起黑客攻击是非法的。所以通常是建立一个自己的实验室，练习黑客技术。

在这个实验室里，你能看到如何创建一个自己的黑客环境，练习各种各样的黑客攻击技术。我们将会探讨不同类型的虚拟系统，构建一个虚拟网络，在虚拟环境中运行试用版的操作系统，搭建一个有漏洞的web应用程序，安装Kali LInux，执行渗透测试。

## 所需条件：

VMware Workstation

Windows XP系统映像

Kali Linux虚拟映像

下面的步骤中会进一步详细介绍。

## 虚拟环境

当我们谈到道德黑客的时候，最好最安全的方法就是在虚拟环境下练习。可以使用虚拟机创建虚拟环境。虚拟机是运行在物理机上的虚假机器。在虚拟世界中，物理机上运行的真实的操作系统称为“host”，虚拟机上运行的操作系统称为“guest”。如果guest被攻破，host仍然是安全的，所以说虚拟机是安全的。

常用的虚拟系统有VMware Workstation、VMware Workstation Player、Oracle VirtualBox等。在这个实验室中，我们将使用VMware workstations。VMware Workstation和VMware Workstation Player二者之间的不同之处是，Workstation可以创建和运行虚拟机，而Player只能用于运行虚拟机。

其它的不同之处有：

**快照** ：快照是虚拟机的硬盘文件在某个时间点上的拷贝。它保留了虚拟机的状态，因此我们可以返回或者恢复到之前的状态。如果VM发生了某些错误，我们就可以恢复到任意时刻的快照。快照保存的状态包括：

虚拟机内存的内容

虚拟机的设置

虚拟机硬盘的状态

在VM Workstation中有这些功能。

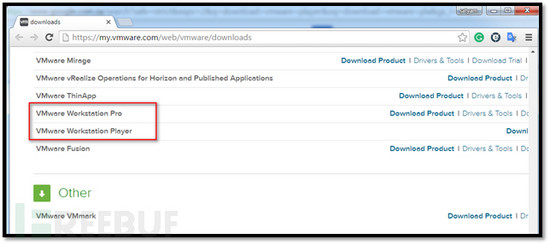
**克隆** ：克隆是对当前虚拟机的拷贝。当前已存在的虚拟机被称为父虚拟机，当克隆操作完成后，克隆机是一个独立的虚拟机，当然它与父虚拟机会共享虚拟硬盘。

在VM Workstation中有这些功能。

不要把克隆和快照混淆了。快照保存了虚拟机当前的状态，当你遇到一些错误的时候可以恢复到那个状态。然而，克隆是虚拟机的一个拷贝，可以单独使用。

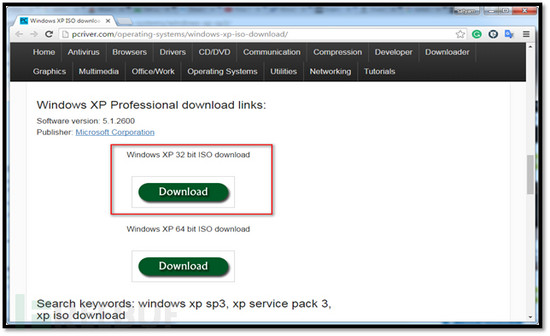
**免费版VS商业版** ：VMware Workstation Player可以免费供于个人使用，VMware Workstation Pro是一个收费的供商业使用的软件。

可以在 [***这里***](https://my.vmware.com/web/vmware/downloads) 下载到这两个产品。

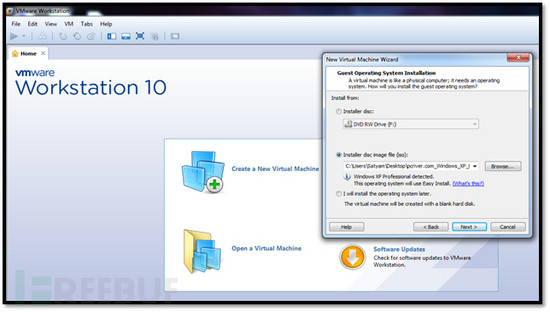


## 步骤1：在VMware Workstation上运行Windows试用版操作系统

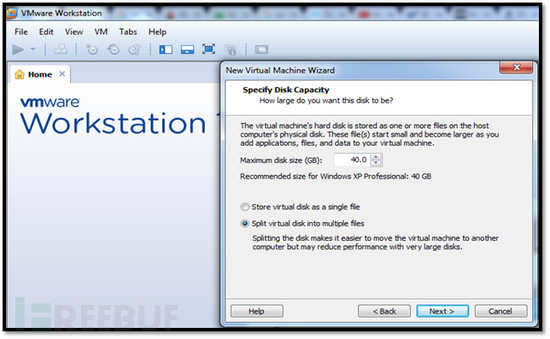
一旦我们下载并安装了VMware Workstation，下一步就是下载并安装Windows XP, Vista, Server 2003，因为这些系统有许多著名的安全问题。可以在 [***这里***](https://dev.windows.com/en-us/microsoft-edge/tools/vms/windows/) 或 [***这里***](http://pcriver.com/operating-systems/windows-xp-iso-download/) 下载到映像。



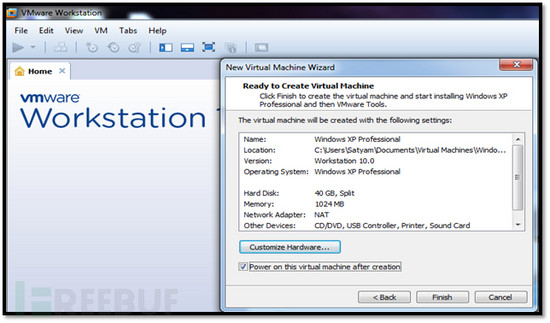
在下载了“.iso”文件后，打开VMware Workstation，选择“File”，单击“New virtual machine”，选择下载好的“.iso”文件。



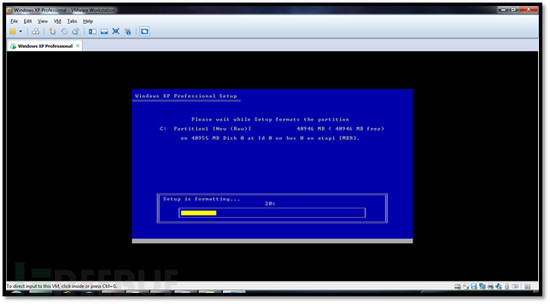
按照屏幕上的指令在workstation上安装windwos XP。

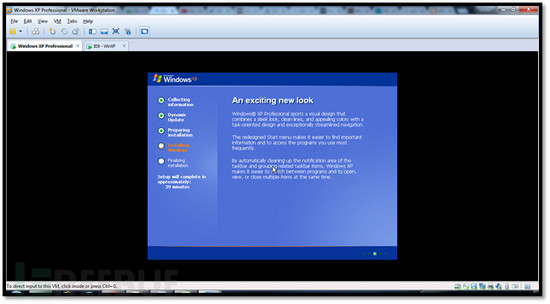


点击“Customize Hardware”按钮，配置其它的设置选项，比如内存，USB设置等。RAM大小可以根据需要增加或减少。



如上图所示，选择“Power on this virtual machine after creation”选项，单击“Next”按钮。







## 步骤2：寻找并配置有漏洞的web应用程序

有很多有漏洞的应用程序，我们可以用来以学习为目的练习渗透测试。下面是一些应用程序：

[***Damn Vulnerable Web Applications (DVWA):***](http://www.dvwa.co.uk/)基于PHP, Apache以及MySQL，需要安装到本地。

[***OWASP WebGoat :***](https://code.google.com/archive/p/webgoat/)J2EE web 应用程序，需要在本地运行。

[***Hack This Site***](https://www.hackthissite.org/)**:**在线学习渗透测试的网站。

[***Testfire***](http://testfire.net/): 在线学习渗透测试的网站。

下面，我们将学习如何在虚拟机中安装有漏洞的运行程序。因为我们已经有了一个正在运行的Windwos XP虚拟机。我们将看到如何在该系统上运行有漏洞的应用程序。在这个练习中，我们将配置Damn Vulnerable Web Application (DVWA)。这个应用程序有若干基于web的漏洞，比如跨站脚本 (XSS), SQL注入, CSRF,命令注入等。

下面的步骤会帮你安装一个web服务器，并运行应用程序。

1、现在并安装XAMPP [***https://www.apachefriends.org/download.html***](https://www.apachefriends.org/download.html) ，对于Windows XP，可以在这里 [***https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/1.8.2/xampp-win32-1.8.2-6-VC9-installer.exe/download***](https://sourceforge.net/projects/xampp/files/XAMPP%20Windows/1.8.2/xampp-win32-1.8.2-6-VC9-installer.exe/download) 下载XAMPP。

2、一旦安装了XAMPP，到控制面板点击“Start”按钮，开启Apache和MySql服务。

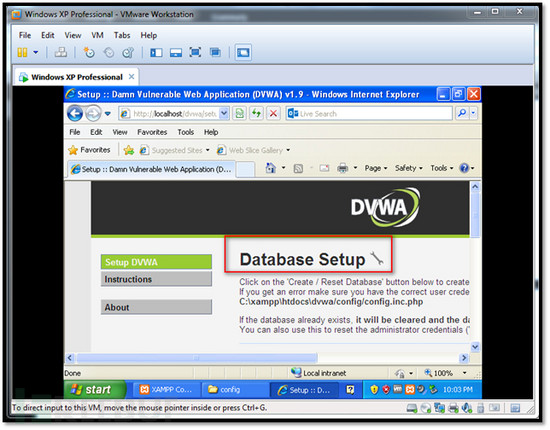
3、在这里 [***http://www.dvwa.co.uk/***](http://www.dvwa.co.uk/) 下载DVWA应用程序，解压文件到一个新的文件夹中，命名为“dvwa”。

4、打开“C:\xampp\htdocs”文件夹，把该文件夹里的内容移动到另外一个地方。

5、把“dvwa”文件夹拷贝到“C:\xampp\htdocs”目录。

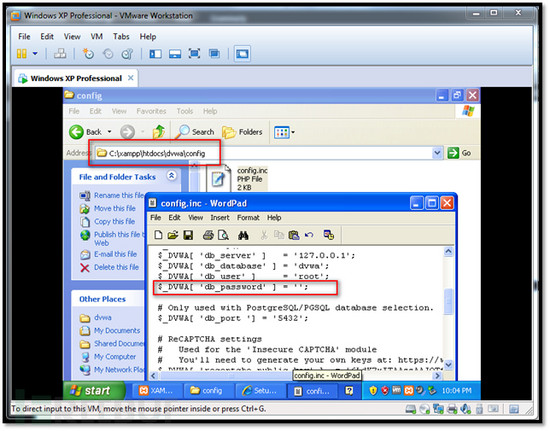
6、在浏览器的地址栏中输入下面的内容并访问： [***http://127.0.0.1/dvwa/login.php***](http://127.0.0.1/dvwa/login.php)

会显示一个数据库设置页面。

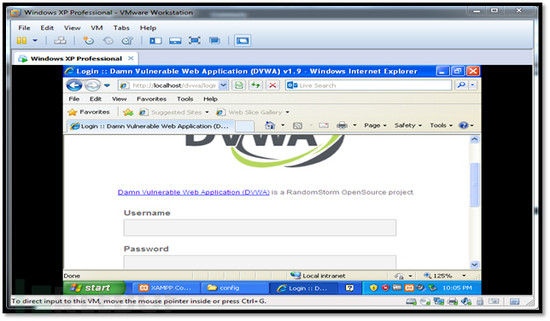


7、到“C:\xampp\htdocs\dvwa\config”文件夹下，用记事本打开“config.inc”文件。

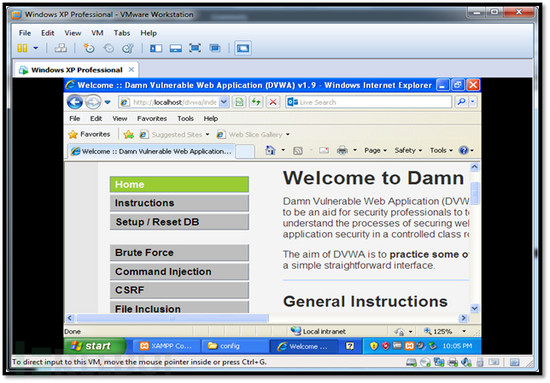
8、移除“db\_password”的值，如下图所示.



9、回到浏览器，然后刷新页面，会显示一个登录页面。

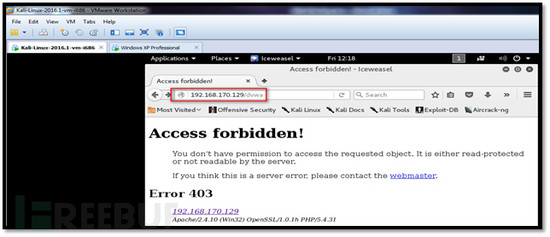


10、输入默认的登录凭证，比如“admin/password”，登录应用程序。

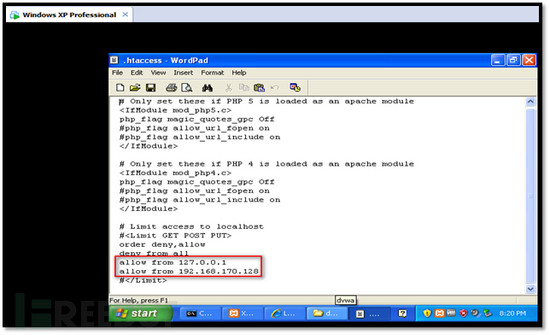


我们成功配置了一个web服务器并在其上安装了一个应用程序，现在我们通过Kali Linux或者BackTrack访问应用程序，访问 [***http://ip-address-of-windows-xp-machine/dvwa/login.php***](http://ip-address-of-windows-xp-machine/dvwa/login.php) ，就可以开始攻击练习了。

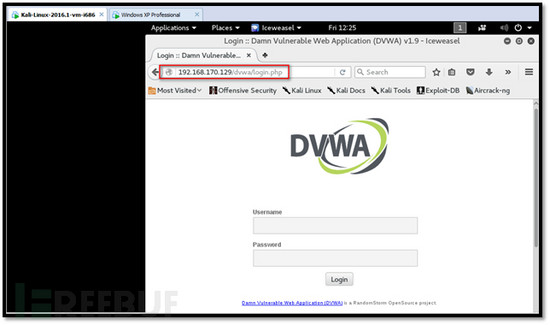
当你通过Kali Linux或者BackTrack访问DVWA的时候，你可能会遇到“Access forbidden”错误，如下：



进入“c:\xampp\htdocs\dvwa”文件夹，打开“HTACCESS File”,定位到“allow from”行，输入Kali Linux的IP地址，如下图所示：

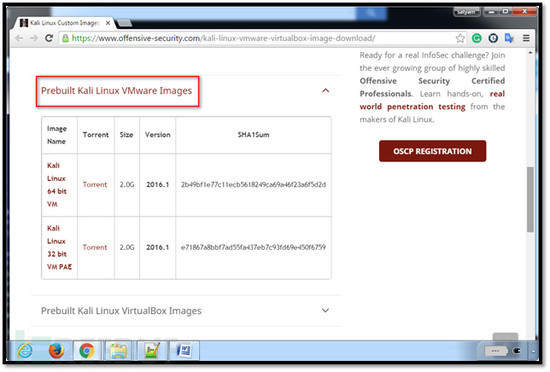


再次访问URL，你可以看到DVWA的登录页面了。



## 步骤3：下载和安装Kali Linux

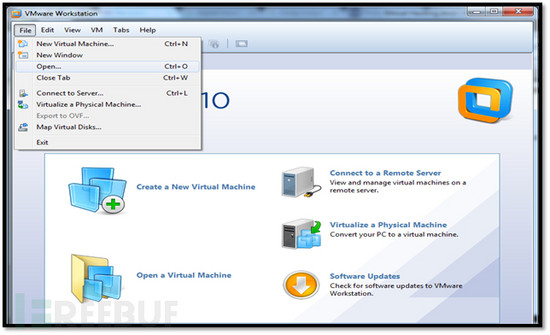
Kali Linux是一个基于Debian的功能强大的渗透测试平台，全世界渗透测试专家都在使用。Kali包含很多与信息安全相关的工具。可以在 [***这里***](https://www.offensive-security.com/kali-linux-vmware-virtualbox-image-download/) 下载Kali Linux的虚拟映像。



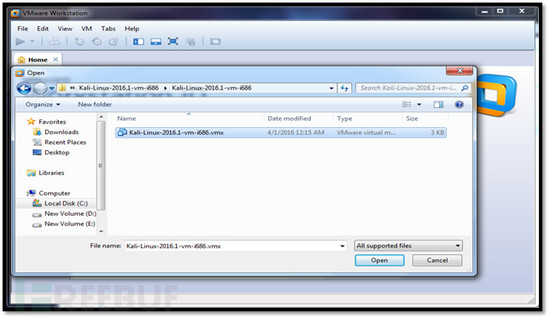
下载之后，按照下面的步骤运行Kali：

第一步：启动VMware Workstation。

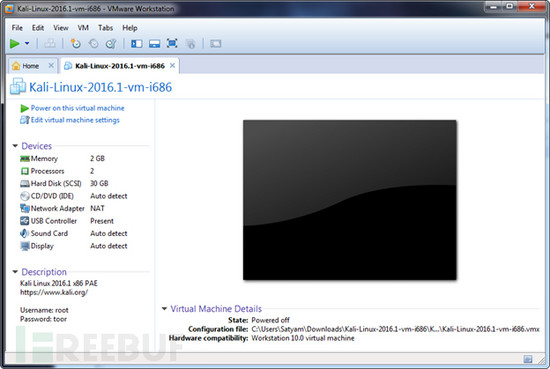
第二步：选择“File”，单击“Open”。



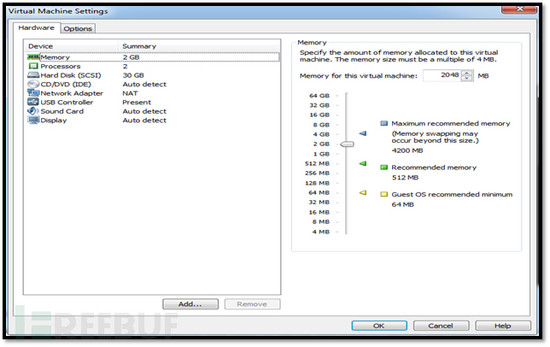
第三步：找到下载目录，选择“Kali\_Linux-2016.1-vm-i686.vmx”文件，点击“Open”按钮。



第四步：可以看到虚拟机的详细配置。



第五步：单击“Edit virtual machine settings”按钮，配置其它信息。



1、内存：你可以给虚拟机分配内存。RAM大小可以根据需要增加或减少，Kali最合适的RAM是2GB。

2、处理器：你可以配置VM虚拟机的处理器的数量，每个处理器可以选择CPU内核的个数。

3、硬盘：你可以给虚拟机分配保存操作系统、程序和数据的硬盘的大小。

4、网络适配器：我们可以给虚拟机增加虚拟以太网卡，改变当前适配器的配置，下面是网络适配器的可选配置：

**桥接模式** ：在桥接网络中，guest操作系统共享host操作系统的网络适配器，连接到物理网络中。这意味着虚拟机在网络中将会是一个独立的机器。虚拟机可以通过这个连接在网络中共享资源。guest操作系统与host操作系统共享同一个DHCP服务器和DNS服务器。

**NAT模式** ：NAT表示网络地址转换（Network Address Translator）。在这个网络中，虚拟机位于host之后，通过一个与host的默认连接访问网络。在这个网络中，通信就好像是来源于host。这意味着虚拟机能够访问网络或互联网，但是它不能在网络中共享资源。连接到这个网络的IP是由DHCP服务器分配的。

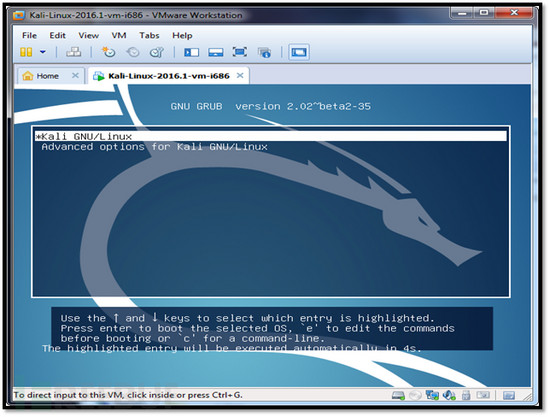
这是最常用的配置，也是新创建的虚拟机的默认配置。

**Host-only模式** ：Host-only虚拟网络是最私密和最严格的网络配置。它不是一个公共网络，不能访问外部的网络或互联网，没有默认的网关，接入这个网络的IP是由DHCP服务器分配的。

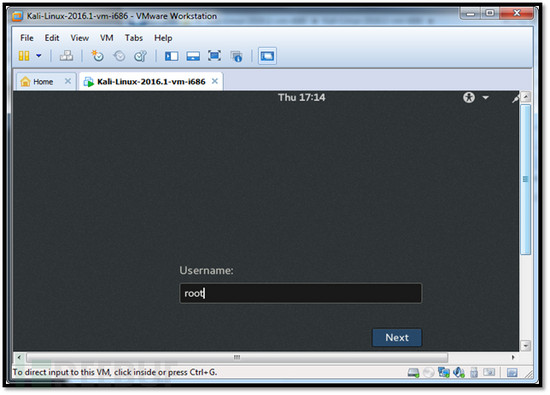
配置供个体使用的渗透测试实验环境，推荐使用“Host-only”模式作为网络适配器的设置，我们可以通过它访问VM网络。

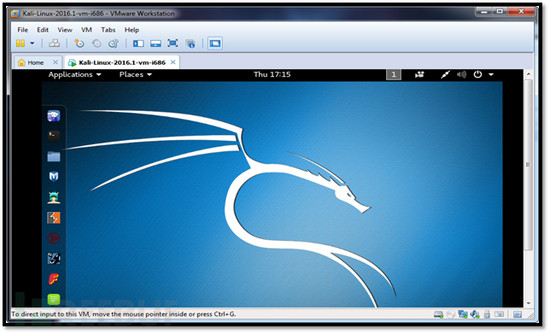
第六步：选择“OK”按钮，单击“Play”按钮，启动VM。

第七步：现在，虚拟机启动了，你可以看到启动界面，如下图所示。在虚拟机的任何位置单击鼠标，按下回车键。



第八步：如果要求输入登录用户名和口令，你可以使用“root”和“toor”分别作为用户名和口令。





现在，我们可以使用Kali Linux虚拟机了，它将用于黑客攻击。我们可以打开浏览器，访问在步骤二中创建的DVWA应用程序。

## Windows下的工具：

在渗透测试中，有一些常用且重要的基于Windows的工具：

**1、Nmap** -Nmap是一个免费的网络发现和安全审计工具。它能用于主机发现，端口扫描、识别服务，识别OS等。Nmap发送特制的数据包并且分析响应结果。Nmap可以在 [***这里***](http://nmap.org/) 下载到。

**2、Wireshark** -Wireshark是一个免费开源的网络协议和数据包解析器。它能把网络接口设置为混杂模式，监视整个网络的流量。可以在 [***这里***](https://1.na.dl.wireshark.org/download.html) 下载到Wireshark。

**3、PuTTY** -PuTTY是一个免费且开源的SSH和telnet客户端。可以用于远程访问其它的机器，可以在 [***这里***](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) 下载到PuTTY。

**4、SQLmap** -SQLmap是一个免费且开源的工具，主要用来检测和执行应用程序中的SQL注入。它也有攻击数据库的选项，SQLmap可以在 [***这里***](http://sqlmap.org/) 下载到。

**5、Metasploit Framework** -Metasploit是一个流行的黑客工具和渗透测试框架。它由Rapid7开发，被每一个渗透测试者和道德黑客使用。可以用于针对有漏洞的目标机执行漏洞利用代码。可以在 [***这里***](http://www.metasploit.com/) 下载到Metasploit。

**6、Burp Suite** -Burp Suite是一个集成的对web应用程序执行安全测试的平台。它集成了多个工具。有两个主要的免费工具Spider和Intruder。Spider是用来抓取应用程序的页面的。Intruder是用来自动化对页面攻击的。Burp专业版有一个额外的工具叫做Burp Scanner,能够扫描应用程序的漏洞，Burp Suite可以在 [***这里***](http://portswigger.net/burp/) 下载到。

**7、OWASP Zed Attack Proxy** -OWASP zap是OWASP工程的其中一部分。它是一个对web应用程序进行渗透测试的工具，具有与Burp Suite类似的功能，有一个自动扫描器，可以发现应用程序的漏洞。其它附加的功能有，针对基于Ajax应用程序的爬虫器。OWASP zap也可以用作代理。可以在 [***这里***](http://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project%23tab=Main) 下载到OWASP zap。

**8、Nessus** -Nessus是一个漏洞、配置和规则审计工具。它有免费和付费版。免费版供个人使用。它使用插件进行扫描。简单得给一个目标机的IP地址，就可以开始扫描。也有一个下载详细报告的选项。可以在 [***这里***](http://www.tenable.com/products/nessus) 下载到Nessus。

**9、Nikto** -Nikto是一个开源的Web服务器漏洞扫描器。它检测未更新的软件和配置，潜在的危险文件和CGI等。他也有创建报告的功能。Nikto可以在 [***这里***](http://www.cirt.net/nikto2) 下载到。

**10、John the Rippe** r-它是一个密码爆破工具，常被用来执行基于字典的爆破攻击。可以在 [***这里***](http://www.openwall.com/john/) 下载到John the Ripper。

**11、Hydra** -另外一个与John the Ripper类似的密码破解工具。Hydra是一个快速的网络登录破解器。它可以针对超过50个协议快速字典攻击，包括telnet, ftp, http, https, smb，若干数据库以及其它更多协议。可以在 [***这里***](https://www.thc.org/thc-hydra/) 下载到Hydra。

**12、Getif-** Getif是一个免费的基于Windows的图形界面工具，用来收集SNMP设备的信息。Getif可以在 [***这里***](https://pentestlab.wordpress.com/2013/01/07/windows-tools-for-penetration-testing) 下载到。

## 工具仓库

在互联网上有一个渗透测试工具仓库，包含了渗透测试学习、exploit开发、社会工程学、渗透测试工具、扫描器、无线网络工具、十六进制编辑器、密码破解器、逆向工程工具等其它与渗透测试相关的重要在线资源。可以在 [***这里***](https://github.com/enaqx/awesome-pentest) 访问仓库。

## 结论

这个实验室可以根据需要定制。我们可以在虚拟机上搭建其它类型的操作系统，并尝试攻击，我们可以通过安装和开启防火墙或者入侵检测系统增加攻击的难度。