# 实验1 扫描工具试用

## 一、实验要求

寻找几个扫描器使用，比较各自的特色的擅长，写出评价

## 二、实验内容

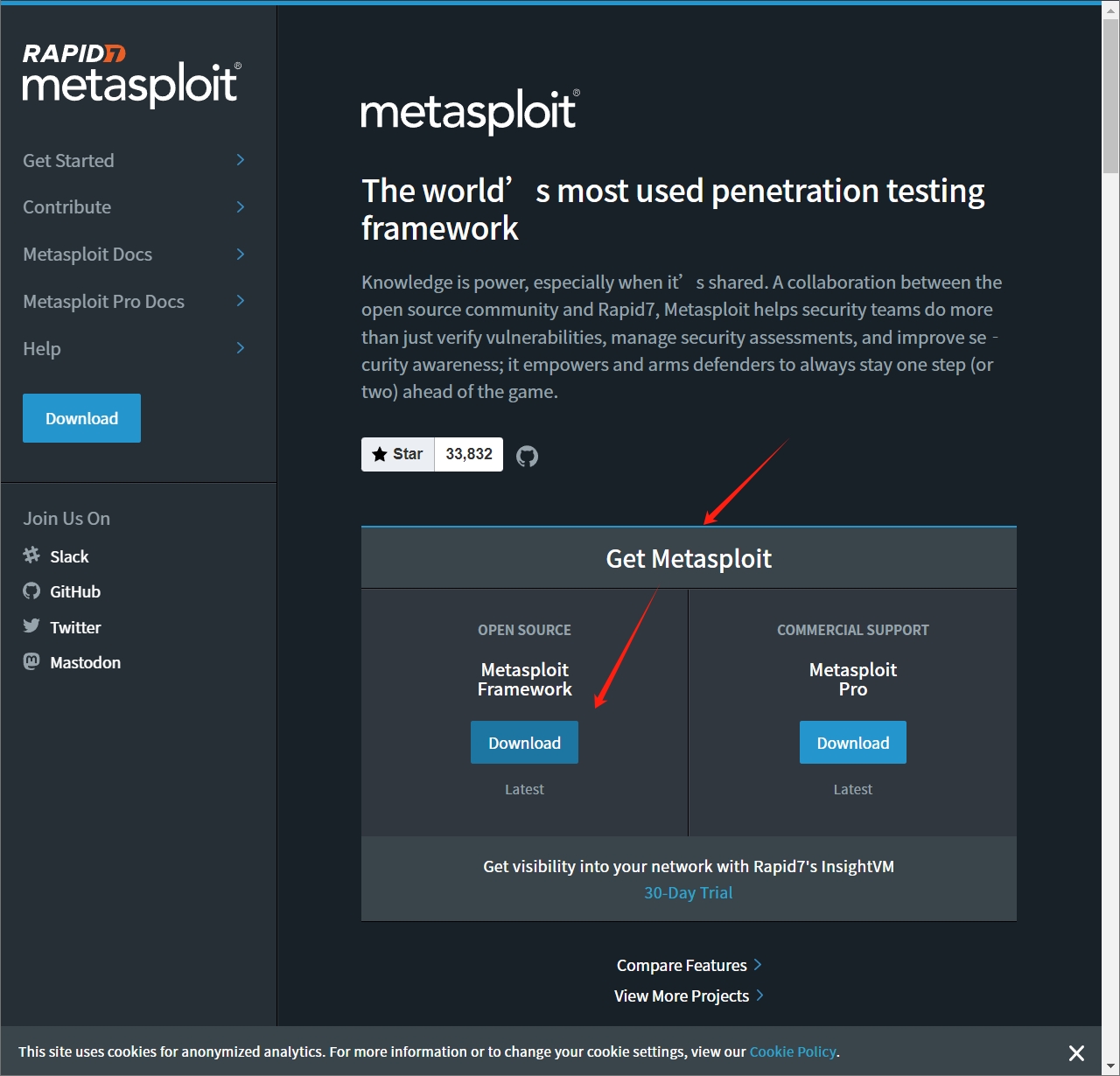
### Metasploit

#### 软件简介

Metasploit是一款开源的安全漏洞检测工具，可以帮助安全和IT专业人士识别安全性问题，验证漏洞的缓解措施，并管理专家驱动的安全性进行评估，提供真正的安全风险情报。

#### 软件安装

进入[metasploit官网](https://www.metasploit.com/)，找到Get Metasploit中的OPEN SOURCE模块，点击Download



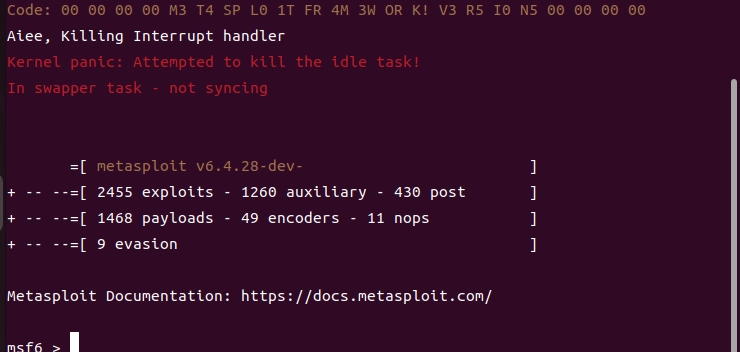
进入到[Metasploit Documentation](https://docs.metasploit.com/docs/using-metasploit/getting-started/nightly-installers.html),找到Using Metasploit下GettingStarted下的Nightly Installers,里面记录了各个系统如何安装软件

在ubuntu虚拟机下执行安装命令安装Metasploit

curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-framework-wrappers/msfupdate.erb > msfinstall && \
  
 chmod 755 msfinstall && \
  
 ./msfinstall

使用msfconsole命令运行Metasploit框架

msfconsole



#### 软件使用

##### 一、配置扫描目标

1. 设置扫描范围：
   * 在Metasploit控制台中，使用set RHOSTS命令设置要扫描的目标IP地址或IP地址范围。例如，set RHOSTS 192.168.1.1-192.168.1.255。
2. 配置其他扫描参数（可选）：
   * 根据需要，可以使用set PORTS命令设置要扫描的端口范围，如set PORTS 1-1024。
   * 使用其他命令配置扫描的具体参数，如线程数（set THREADS）、超时时间（set TIMEOUT）等。

##### 二、选择扫描模块

Metasploit提供了多种扫描模块，用于执行不同类型的扫描任务。常见的扫描模块包括：

* **端口扫描模块**：如auxiliary/scanner/portscan/tcp，用于扫描目标主机的开放端口。
* **服务扫描模块**：如auxiliary/scanner/http/http\_version，用于探测目标主机上运行的服务及其版本信息。
* **操作系统探测模块**：如使用Nmap的auxiliary/scanner/discovery/nmap或db\_nmap命令，尝试识别目标主机的操作系统。

选择适当的扫描模块，并使用use命令加载它。例如，use auxiliary/scanner/portscan/tcp。

##### 三、执行扫描

配置好扫描目标和扫描模块后，使用run命令开始执行扫描。扫描过程中，Metasploit会向目标发送请求，并收集响应信息。

##### 四、分析扫描结果

扫描完成后，Metasploit会显示扫描结果。根据扫描结果，可以了解目标主机的开放端口、运行的服务、潜在的漏洞等信息。这些信息对于后续的渗透测试和安全加固至关重要。

### Nmap

#### 软件简介

nmap是一个网络连接端扫描软件，用来扫描网上电脑开放的网络连接端。确定哪些服务运行在哪些连接端，并且推断计算机运行哪个操作系统。它是网络管理员必用的软件之一，以及用以评估网络系统安全。

#### 软件安装

进入[Nmap官网](https://nmap.org/download.html#linux-rpm)，阅读文档下载对应操作系统下的nmap

linux系统下，直接在终端执行

sudo apt-get install nmap

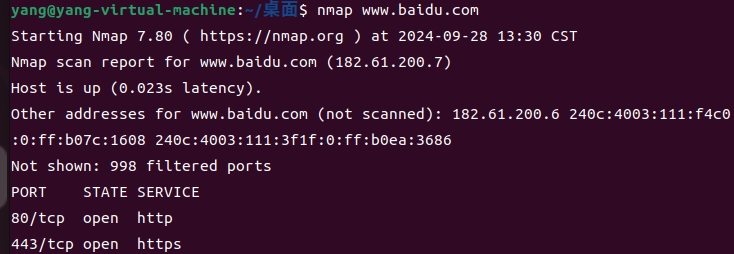
下载即可

#### 软件使用

1. 使用nmap列举远程主机开放的端口

nmap 目的主机地址

执行该命令可以列举远程主机开放的端口



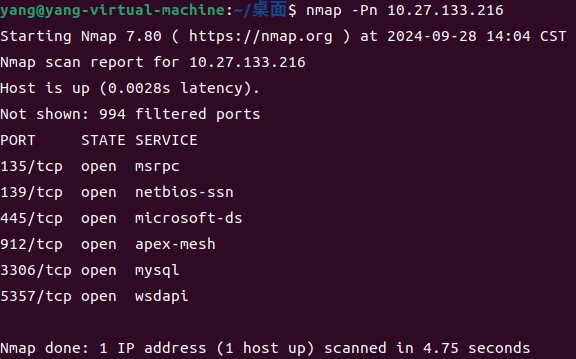
1. 使用nmap嗅探目的主机的操作系统

nmap -O 目的主机地址



根据给出的Nmap扫描结果，目标主机<www.baidu.com>的操作系统类型为Linux，具体版本为2.4.X或3.X。

1. 扫描本机的开放端口



## 三、实验收获

Nmap是一款功能强大且易于使用的网络扫描工具。它适用于各种场景下的网络安全评估工作，无论是快速发现网络中的设备和主机还是深入分析特定主机上的开放端口和服务版本信息。通过使用Nmap，用户可以更好地了解网络拓扑结构和潜在安全风险从而采取相应的防护措施。然而需要注意的是虽然Nmap提供了丰富的功能和选项但在使用过程中仍需谨慎以避免对目标系统造成不必要的影响或损害。

Metasploit是一款功能强大、易于使用的渗透测试工具。它适用于各种级别的安全研究人员，无论是初学者还是资深专家。通过使用Metasploit，用户可以快速发现并利用目标系统中的漏洞，提高系统的安全性。然而，需要注意的是，由于Metasploit的强大功能，如果被恶意使用，可能会对系统造成严重损害。因此，在使用Metasploit时，请务必遵守相关法律法规和道德准则。

通过这次实验，我初步了解了网络安全扫描工具的简单实用，给我后续的学习打下了一定基础