

网络攻防技术基础课程实验报告

|  |  |
| --- | --- |
| 实验名称： | 实验二  Kali使用 |
| 实验日期： | 2024-3-12 |
| 实验地点： | 西部片区4号楼301 |
|  | |
| 学号： | 33920212204567 |
| 姓名： | 任宇 |
| 专业年级： | 软工2021级 |
| 学年学期： | 2023-2024学年第二学期 |

1. **实验目的**

* 熟悉kali基本操作
* 自由探索尝试Kali功能，如：社会工程学、信息收集、MSF、无线网络信息收集等，并在虚拟环境下完成测试。

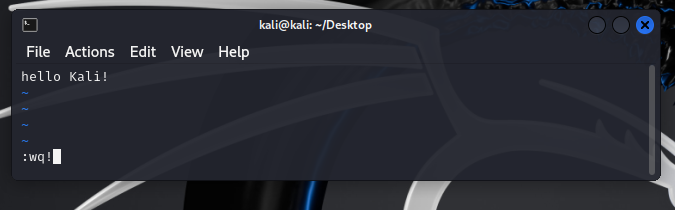
1. **实验用到的软件或工具**

虚拟机软件：VMware Workstation Pro 17

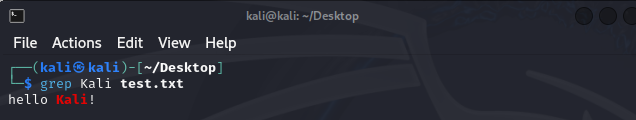
虚拟机系统：metasploitable-linux-2.0.0、Kali、Ubuntu18.04

1. **实验过程**
2. **Kali的基本使用：**
3. 编辑文件：vim





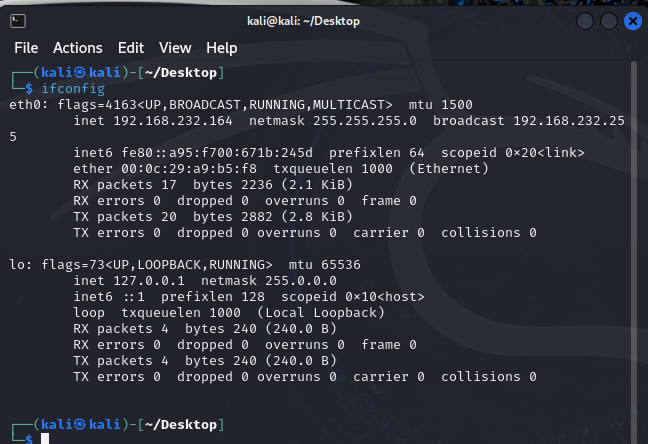
1. 字符串搜索：



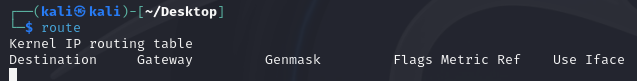
1. 关键字替换：



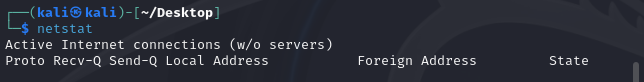
1. 查看网络信息：



1. 查看网关：



1. 查看开放端口：



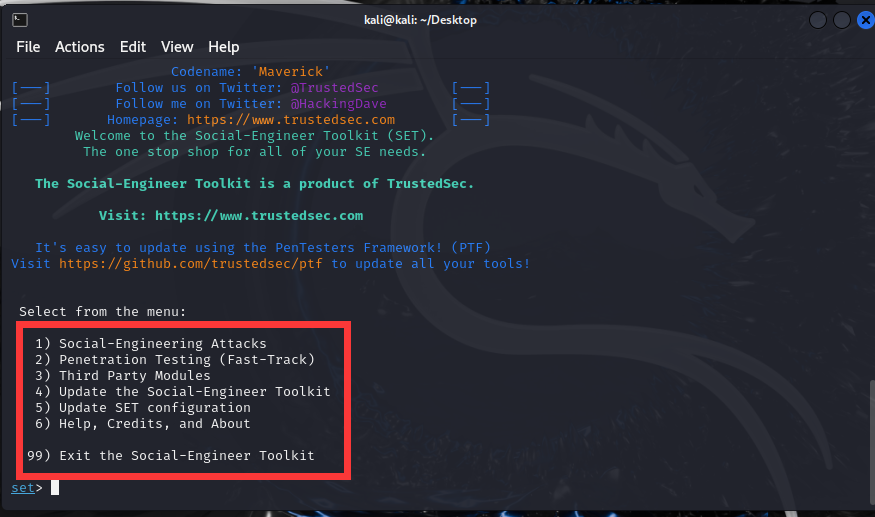
1. **Kali中的社会工程学（Social Engineering）工具：**

工具示例： Social-Engineer Toolkit (SET)

SET是一个开源的社会工程工具包，用于执行人为攻击模拟。它可以模拟钓鱼攻击、创建恶意文件等，测试步骤如下：

1. 打开Kali Linux终端，输入setoolkit来启动Social-Engineer Toolkit。

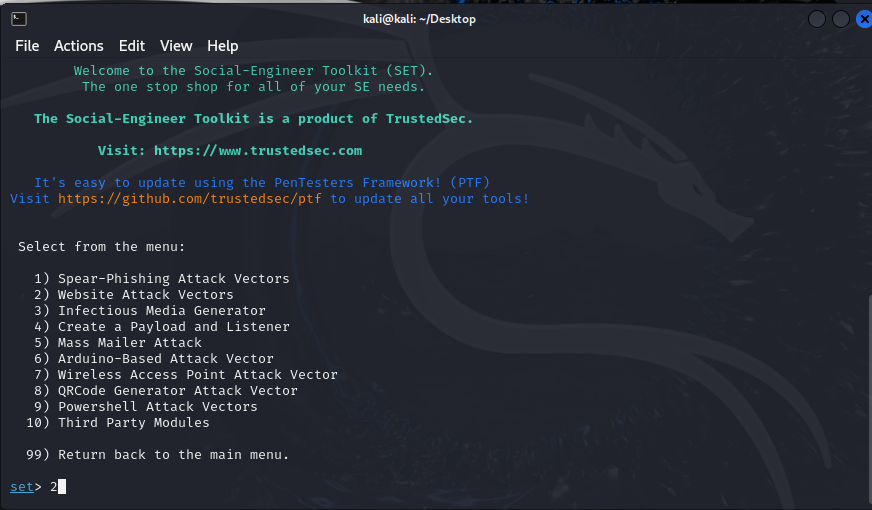




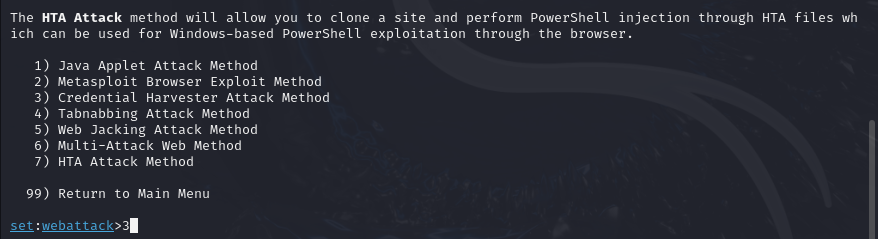
1. 选择1) Social-Engineering Attacks。



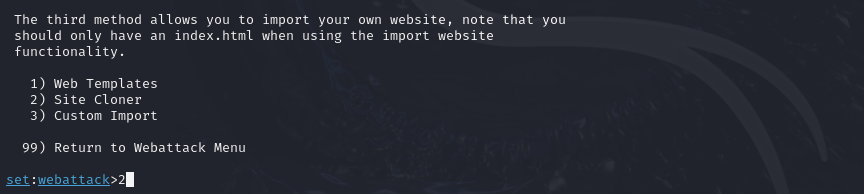
1. 选择2) Website Attack Vectors。



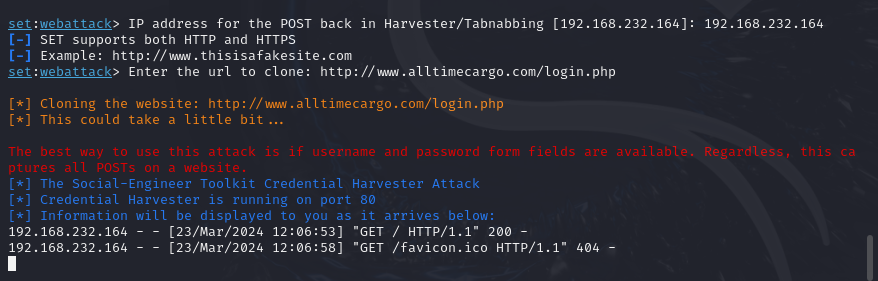
1. 选择3) Credential Harvester Attack Method。



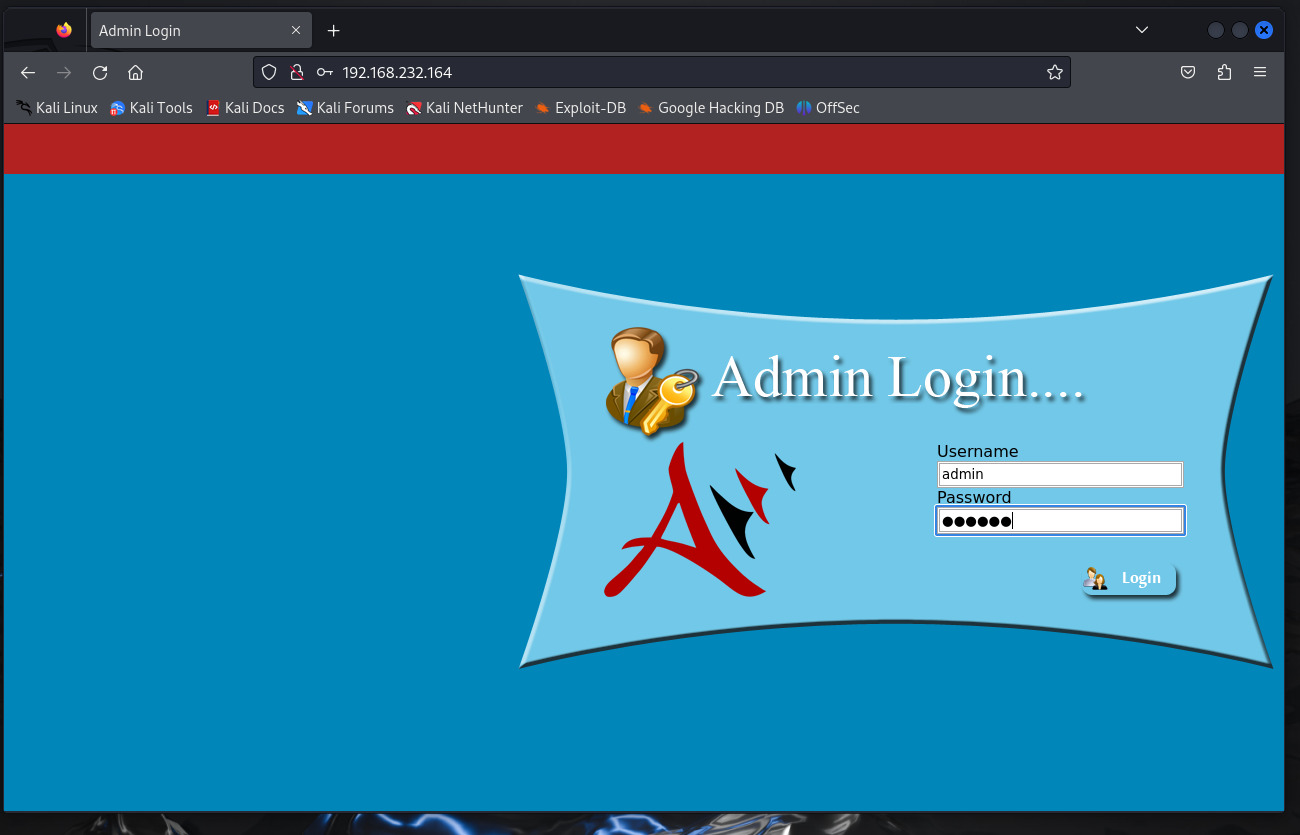
1. 选择2) Site Cloner。

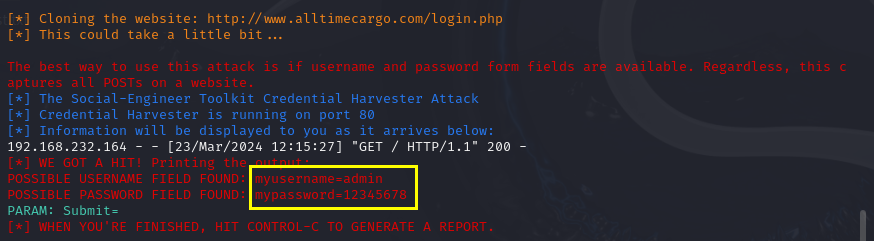


1. 按照提示输入想要克隆的网站URL和SET配置的IP地址。



1. SET将启动一个克隆的网站，并尝试收集访问该网站用户的凭证信息。



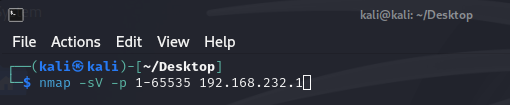


1. **Kali中的信息收集（Information Gathering）工具：**

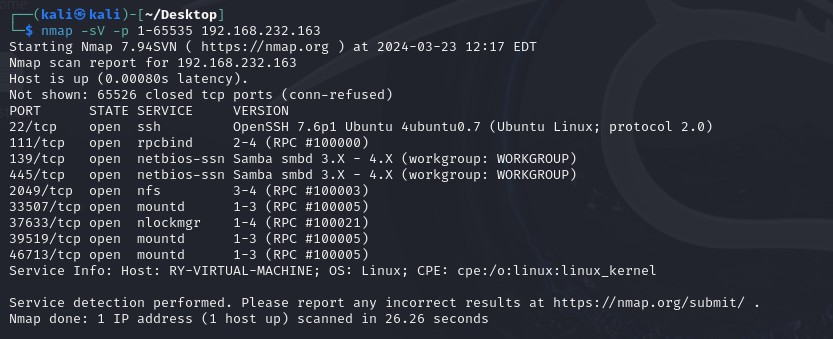
工具示例：Nmap

Nmap是一个开源的网络扫描工具，可以实现主机发现和端口扫描，同时自身也可带漏洞扫描的脚本可以完成对主机端口的漏洞扫描。

1. 打开Kali Linux终端，输入命令nmap -sV -p 1-65535 <目标IP地址>来扫描目标IP地址的所有端口，同时识别服务版本信息。



1. 输出将显示目标系统上开放的端口和运行的服务。



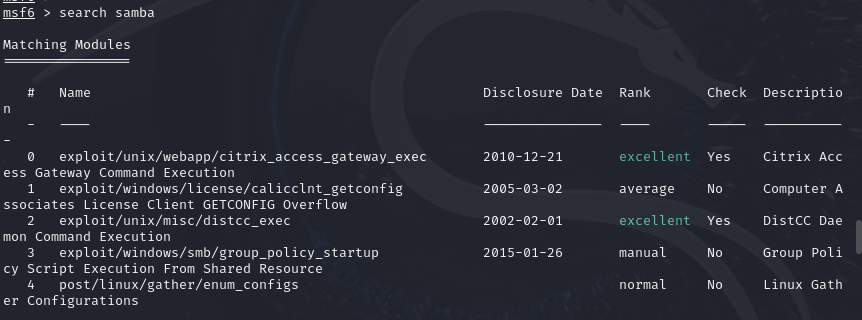
1. **Kali中的MSF（Metasploit Framework）工具：**

Metasploit是一个用于渗透测试的强大框架，允许用户开发和执行对目标计算机的攻击代码。

我有一台虚拟机安装了Ubuntu 18.04，假设其运行着Samba服务。Samba是一种在Linux和Windows系统间共享文件和打印服务的软件。过去，Samba的某些版本中存在漏洞，比如CVE-2017-7494，该漏洞允许远程执行代码。

1. 打开Kali Linux终端，输入msfconsole启动Metasploit Framework。在msfconsole中，搜索Samba漏洞的利用模块，可以使用search samba命令。

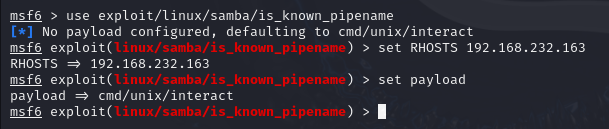




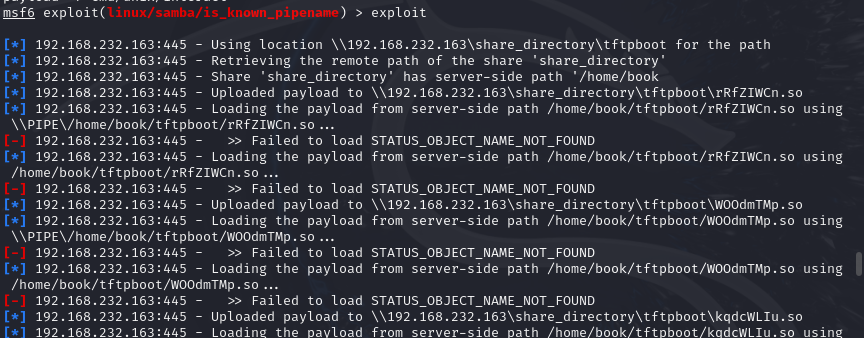
1. 假设找到了一个适合的利用模块，例如exploit/linux/samba/is\_known\_pipename。



1. 设置目标机器的IP地址，使用set RHOSTS <IP地址>命令。根据需要调整其他选项，例如set payload。



1. 输入exploit执行攻击。如果一切设置正确，并且目标机器上的Samba版本存在漏洞，这将允许执行远程代码。

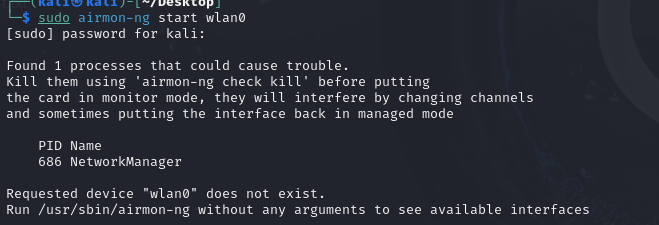


1. **Kali中的无线网络信息收集工具：**

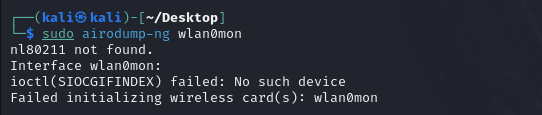
工具示例： Aircrack-ng

Aircrack-ng是一个完整的无线网络安全工具套件，可用于网络监控、攻击、测试和破解。

1. 打开Kali Linux终端，输入airmon-ng start wlan0启动无线接口的监控模式。



1. 使用airodump-ng wlan0mon开始捕获周围无线网络的流量。



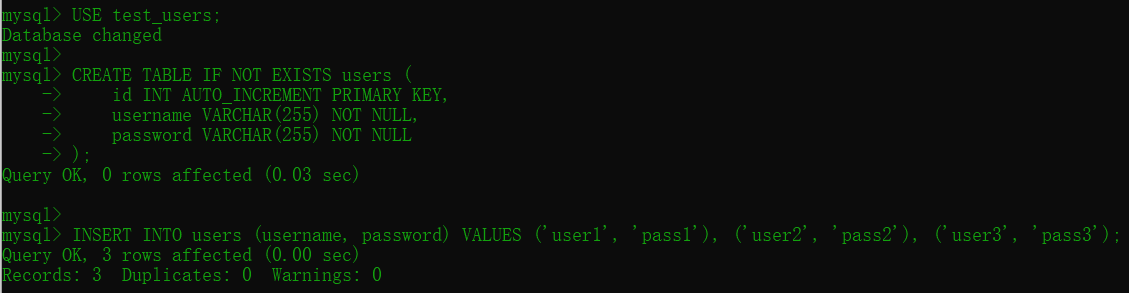
因为虚拟机没有无线网卡，无法继续后续步骤，如果有无线网卡，后续步骤即为：识别目标网络，然后使用Aircrack-ng的其他工具进行进一步的攻击或分析。

1. **Kali中的SQL注入探测工具：**

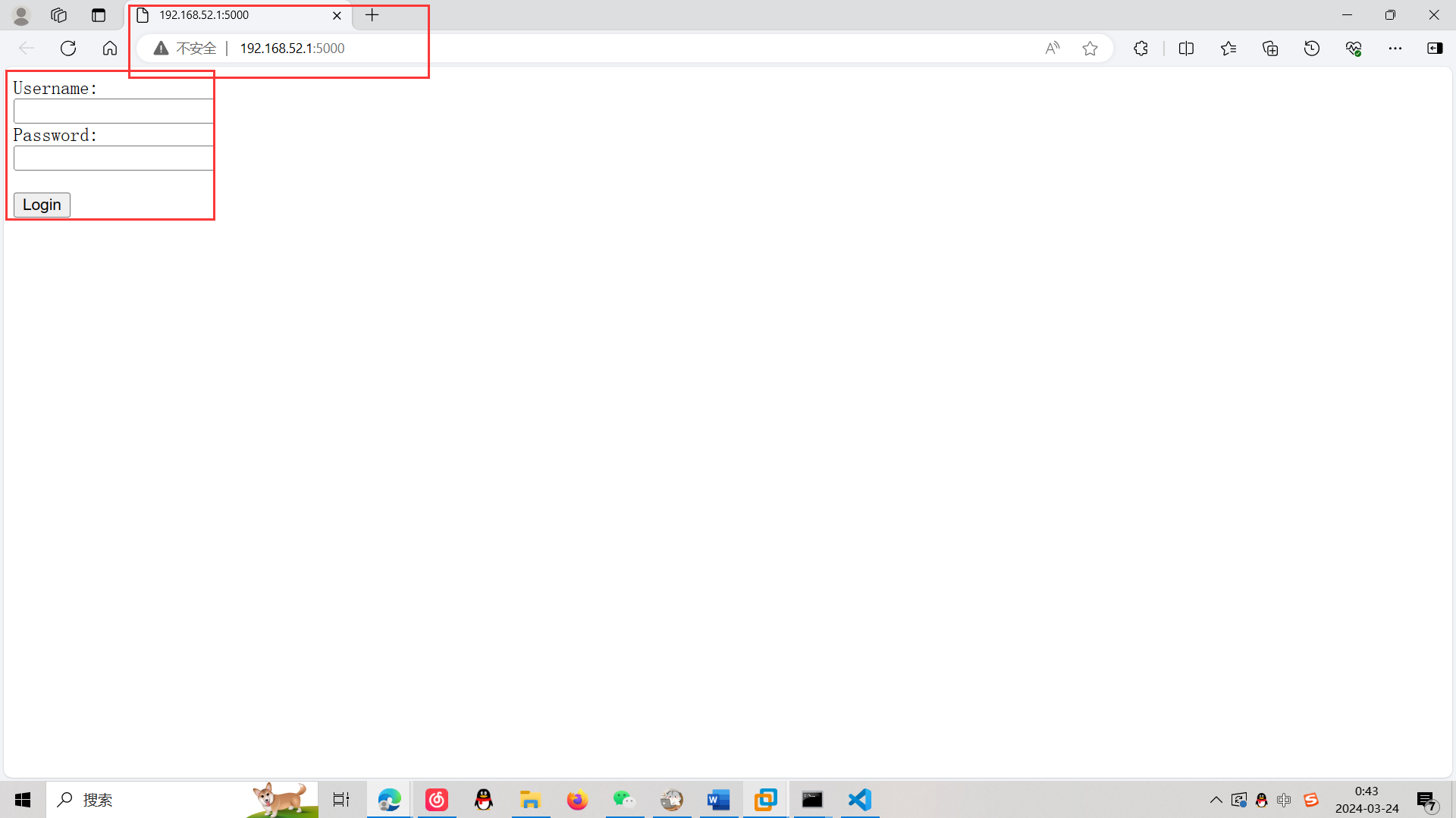
工具示例： SQLMap

SQLMap是一个功能强大的自动化SQL注入工具，可以用于检测和利用SQL注入漏洞。

在主机上创建数据库：



在主机上开放一个网页以供测试：



使用SQLMap进行攻击：

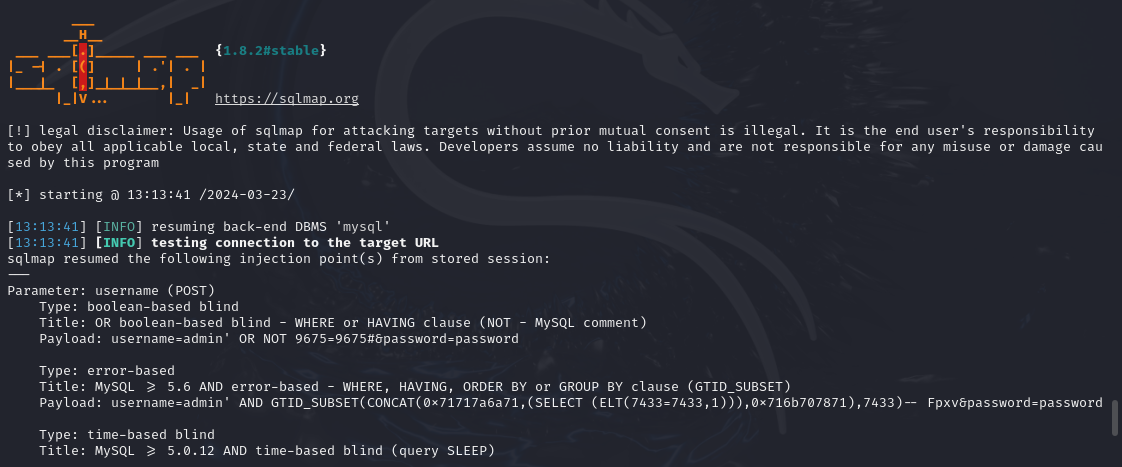
1. 为了使用sqlmap，需要捕获向你的应用发送的HTTP请求。对于简单的POST请求，可以直接使用curl命令来模拟这个请求。



1. 一旦有了请求的详细信息，就可以使用sqlmap来测试潜在的SQL注入点。sqlmap可以直接从HTTP请求中提取信息。可以将curl命令修改为生成一个请求文件，然后将该文件提供给sqlmap。

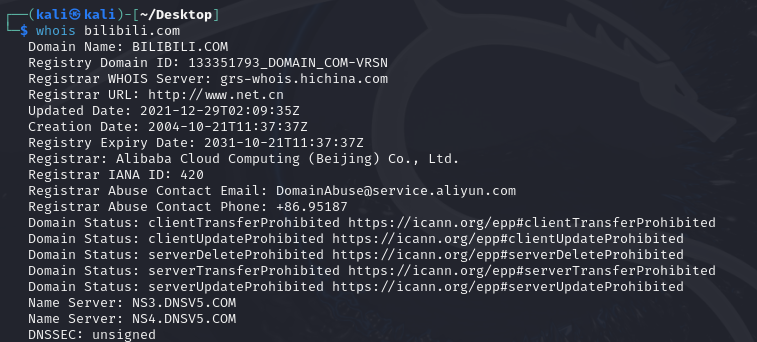


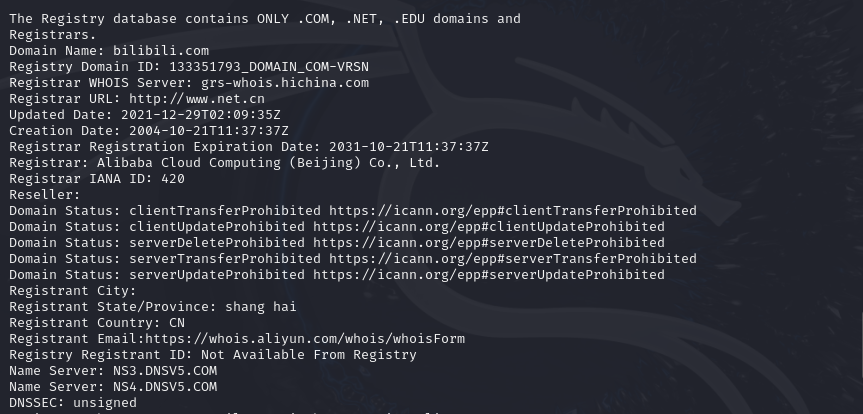
1. sqlmap将自动测试各种SQL注入技术来尝试识别漏洞。根据应用的配置和数据库的具体情况，这可能需要一些时间。sqlmap会提供详细的输出，包括成功发现漏洞的具体信息（如果有的话）。

1. **Kali中的开源情报收集工具：**

Whois <目标URL或IP地址>





1. **实验思考及心得**

通过这次实验，我对Kali Linux的基本操作以及它的强大功能有了深入的了解。在实验中，我尝试了多种工具，包括社会工程工具包（SET）、Nmap、Metasploit Framework（MSF）、Aircrack-ng和SQLMap等，这些工具覆盖了从信息收集、漏洞扫描到漏洞利用等多个阶段，使我对渗透测试的整个流程有了更全面的认识。

我特别对SQLMap进行SQL注入测试的部分感到兴趣，通过实际操作，我意识到了如何通过自动化工具检测和利用SQL注入漏洞，也意识到了防御措施的重要性。此外，尝试使用社会工程学工具集（SET）进行钓鱼攻击模拟，让我认识到安全意识的重要性，以及如何通过教育减少此类攻击的成功率。