

实验报告

课程名称： 网络攻防技术

实验项目： 实验三：漏洞扫描实验

学 生 姓 名：

学 号：

二级学院名称：

专 业：

指 导 教 师：

# 1实验目的和要求

1）掌握漏洞扫描的原理和方法；

2）掌握Nmap漏洞扫描工具的使用。

# 2实验设备及材料

1）VMware虚拟机：VMware-workstation-full-14.1.3.zip

2）Kali虚拟机系统：Kali-linux-2018.1-vm-amd64.ova

账密：root toor

3）Metasploitable靶机系统：Metasploitable-linux-2.0.0.zip

账密：msfadmin msfadmin

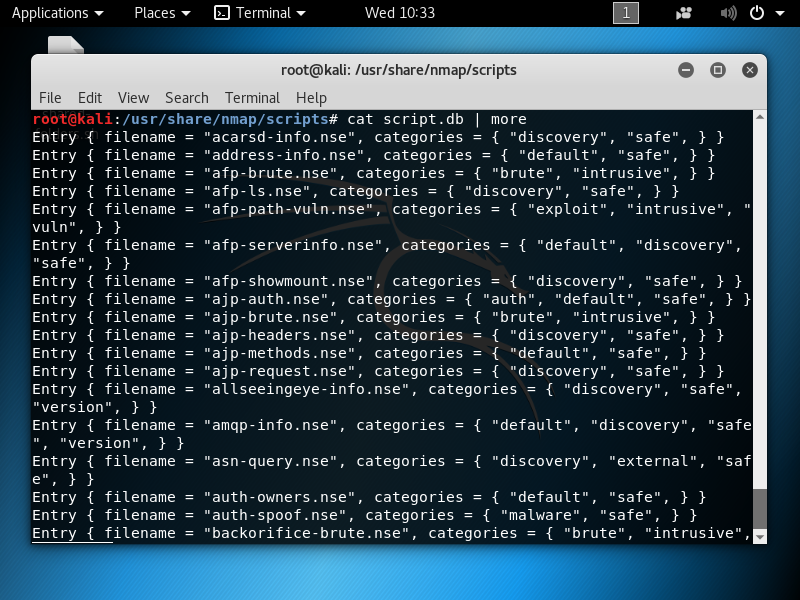
5）Nmap工具

# 3实验内容

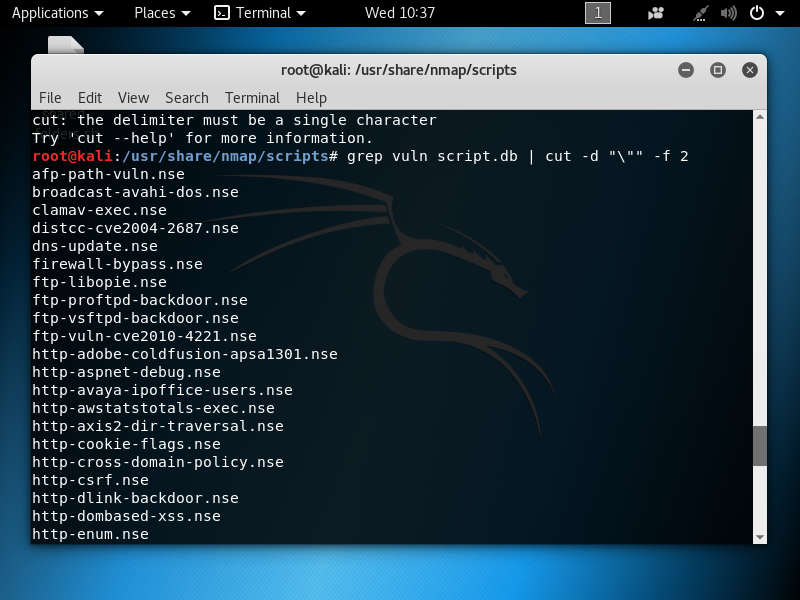
用Nmap对网络系统漏洞进行扫描和收集。

## 3.1 Nmap脚本引擎文件的使用

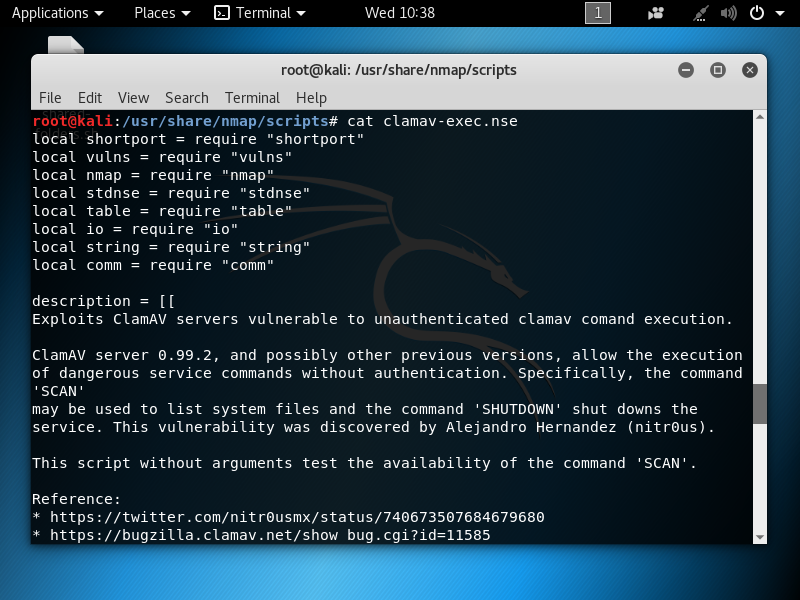
1）查看Nmap脚本数据库文件；



2）查看与漏洞相关的脚本；

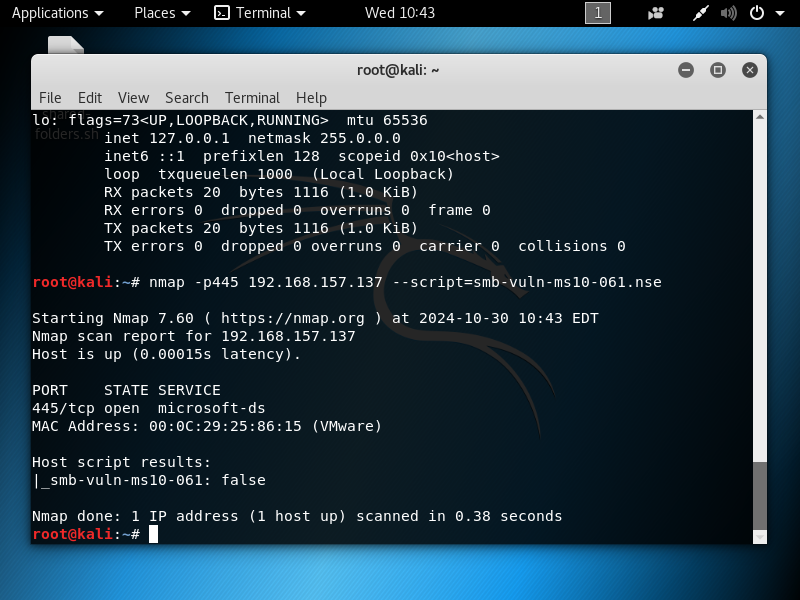


3）查看对应脚本文件的内容。



## 3.2 Nmap扫描Metasploitable靶机系统漏洞

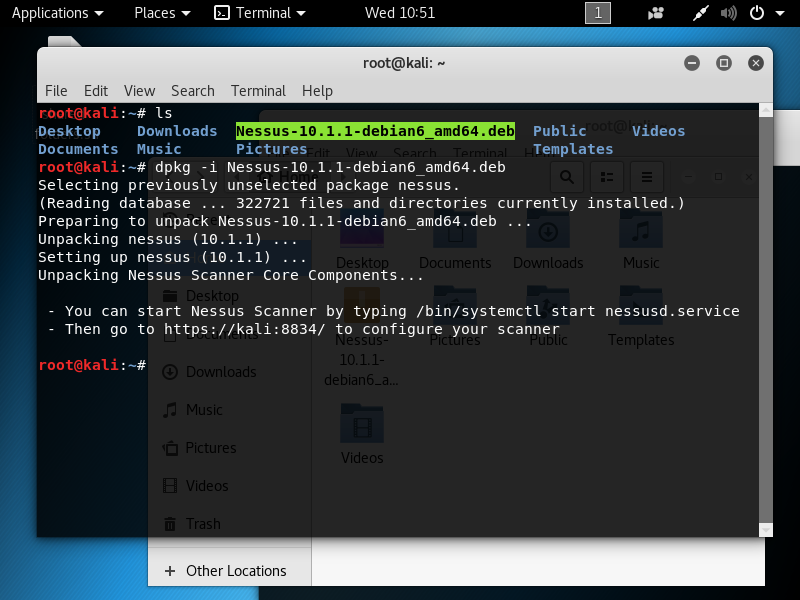
对Metasploitable靶机系统漏洞CVE-2010-2729进行扫描。



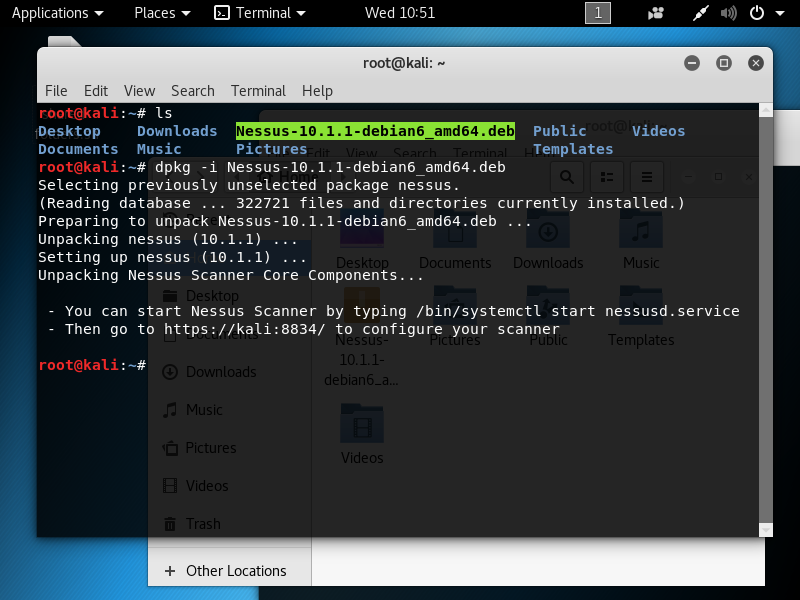
**3.3 Nessus的安装和配置**

1）下载Nessus；

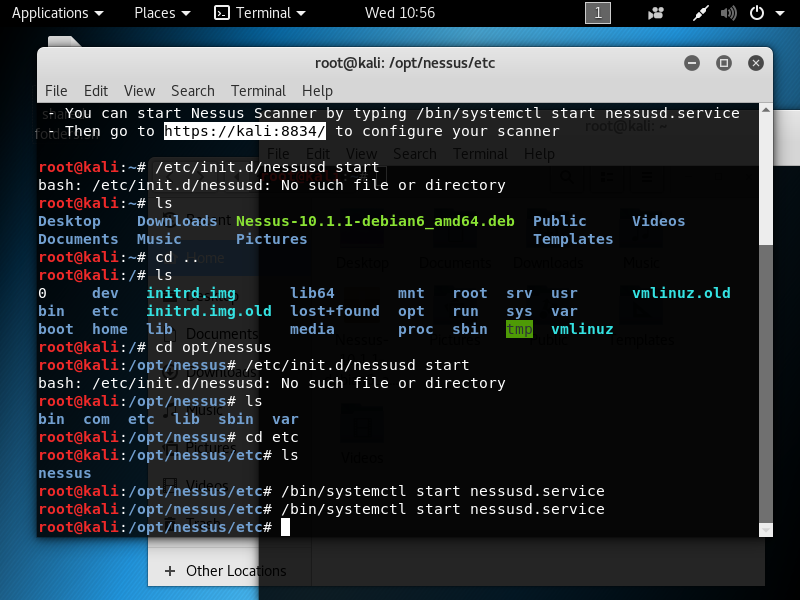
2）将Nessus移到home文件夹下

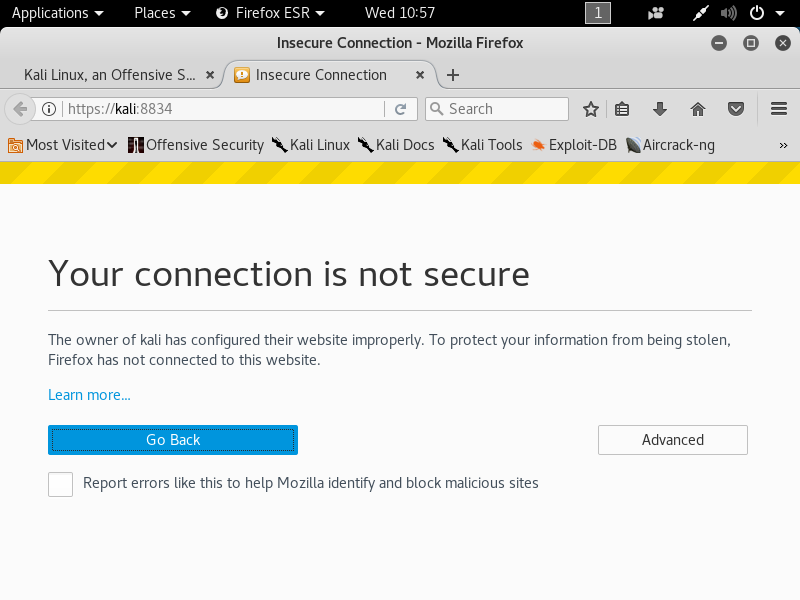


3）安装启用Nessus；



4）浏览器访问Nessus；





# 4实验总结

以前只是使用nmap进行端口或者ip的扫描，使用功能有限，学会了使用nmap进行漏洞扫描后极大提高了工作效率。