1. **了解黑客**

1.1940 hacker

2.攻击流程： 扫描漏洞，试探漏洞，获取和提升权限，木马入侵，建立后门并清理痕迹。

3.所需理论知识：

（1）服务：指执行指定系统功能的程序、例程、进程。

（2）漏洞：操作系统软件在逻辑设计上的缺陷或在编写时产生的错误。

**第二章 攻防的准备工作**

1.IP地址 internet protocol 网络之间互联的协议。每个电脑分配32位地址4字节。IP地址有两种表现形式：二进制和点式十进制。

2.IP地址的组成：网络地址+主机地址。子网掩码 默认网关 和DNS. IP地址分为ABCDE 5类。

A类：1个字节的网络地址+3字节的主机地址。 网络地址最高位是0。

B类：2个字节的网络地址+2字节的主机地址。 网络地址最高位10。

C类：3个字节的网络地址+1字节的主机地址。 网络地址最高位110。

D类：1110

E类：1111

3.子网掩码是一种用来指明IP地址的哪些位标识的是网络地址哪些位是主机地址。网络地址标识为1主机地址标识为0

4.默认网关：一个可直接到达的IP路由器的IP地址，是一个用于TCP/IP的配置项，一台主机可以有多个网关。一个主机如果找不到可用的网关，就把数据包发给默认指定的网关。

5.DNS domain Name system 域名解析成IP地址 多个域名对应一个IP 或 1对1

(2) 端口

1.公认端口：0到1023 明确表明了某种服务的协议。

2.注册端口：1024到49151

3.动态和私有端口 49152到65535 不应为服务分配致谢端口。

可以重定向端口 将http端口重定向8080端口。

查看端口：netstat /an

常用命令：ping 主要测试目标主机的主机名和IP地址信息，以及验证本地主机与远程主机的连接。

Ipconfig

Net view:显示当前域的电脑列表。在 输入 net view 命令后再输入网络中的电脑名称 可查看该电脑共享的资源列表。

Net start 服务名 启动服务

Net stop 服务名 停止服务

Net user 查看电脑上的用户账号列表。 Net user fate 123456

Net localgroup

Tracert

本地配置虚拟机进行测试。

1. 收集网站信息

IP 地址 域名 备案信息 中国万网的信息 通过中国互联网络信息中心收集

结构信息收集

Internet 防火墙 路由器 服务器

木马攻防

木马：是一款用于窃取用户的密码资料，破坏硬盘内的程序或数据软件。