kali linux渗透测试

第4课 被动侦察收集目标信息，分析密码列表

诸神之眼--Nmap

什么IP?

内网IP，外网IP

什么是端口?

端口对应相应的服务或软件

Nmap的基本操作

1.对单个主机的扫描

nmap <IP>

Nmap还支持大量的参数，参数都是以“横线”的形式表示，比如：-sn，注意：参数区分大小写。

在默认情况下，Nmap会对目标主机同时进行在线状态以及端口扫描，但有时我们只需要进行在线状态扫描，就可以是用-sn参数

nmap -sn <ip>

2.对多个不连续的主机进行扫描

nmap 192.168.3.2 192.18.3.155 192.158.13.56

不同的IP之间用空格分开

3.对连续的主机进行扫描

nmap 192.168.30.100-200

4.对整个子网进行扫描

nmap 192.168.30.1-255

IP的范围0-255

参　数	说　明
-sT	TCP connect()扫描，这种方式会在目标主机的日志中记录大批连接请求和错误信息。
-sS	半开扫描，很少有系统能把它记入系统日志。不过，需要Root权限。
-sF -sN	秘密FIN数据包扫描、Xmas Tree、Null扫描模式
-sP	ping扫描，Nmap在扫描端口时，默认都会使用ping扫描，只有主机存活，Nmap才会继续扫描。
-sU	UDP扫描，但UDP扫描是不可靠的
-sA	这项高级的扫描方法通常用来穿过防火墙的规则集
-sV	探测端口服务版本
-Pn	扫描之前不需要用ping命令，有些防火墙禁止ping命令。可以使用此选项进行扫描
-v	显示扫描过程，推荐使用
-h	帮助选项，是最清楚的帮助文档

-p	指定端口，如“1-65535、1433、135、22、80”等
-O	启用远程操作系统检测，存在误报
-A	全面系统检测、启用脚本检测、扫描等
-oN/-oX/-oG	将报告写入文件，分别是正常、XML、grepable 三种格式
-T4	针对TCP端口禁止动态扫描延迟超过10ms
-iL	读取主机列表，例如，“-iL C:\ip.txt”

谢谢观赏