kali linux渗透测试

第6课 使用Nmap进行网络扫描，网络嗅探

侦察类型：主动侦察，被动侦察

什么是被动侦察

被动侦察就是指分析公开的信息，在被动侦察的过程中，要尽可能的减少与目标的交互，与目标进行交互有可能会暴露自己的身份。

使用 theharvester 工具获取用户信息（网络爬虫，有编程基础的朋友，可以自己开发属于的自己的工具）

使用CUPP 创建分析用户密码列表

git clone https://github.com/Mebus/cupp.git

python3 cupp.py -i

Rencon-NG框架

Rencon-NG的基本用法

使用 help查看所有命令

使用 show modules 命令 查看可以使用的模块

谢谢观赏