网络安全工作者的必杀技 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/252/2021_2022__E7_BD_91_E7_BB_9C_E5_AE_89_E5_c101_252825.htm 1.最基本，最常用的，测试物理网络的 ping 192.168.0.8 －t，参数－t是等待用户去中断测试 2.查看DNS、IP、Mac等 A.Win98：winipcfg B.Win2000以上：Ipconfig/all C.NSLOOKUP：如查看河北的DNS C:\>nslookup Default Server: ns.hesjptt.net.cn Address: 202.99.160.68 >server 202.99.41.2 则将DNS改为了41.2 > pop.pcpop.com Server: ns.hesjptt.net.cn Address: 202.99.160.68 Non-authoritative answer: Name: pop.pcpop.com Address: 202.99.160.212 3.网络信使 Net send 计算机名/IP * (广播) 传送内容，注意不能跨网段 net stop messenger 停止信使服务，也可以在面板－服务修改 net start messenger 开始信使服务 4.探测对方对方计算机名，所在的组、域及当前用户名 （追捕的工作原理） ping －a IP －t，只显示NetBios名 nbtstat -a 192.168.10.146 比较全的 5.netstat -a 显示出你的计算机当前所开放的所有端口 netstat -s -e 比较详细的显示你的网络资料，包括TCP、UDP、ICMP 和 IP的统计等 6.探测arp绑定（动态和静态）列表，显示所有连接了我的计算机，显示对方IP和MAC地址 arp -a 7.在代理服务器端 捆绑IP和MAC地址，解决局域网内盗用IP！： ARP －s 192.168.10.59 00 －50－ff－6c－08－75 解除网卡的IP与MAC地址的绑定： arp -d 网卡IP 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com