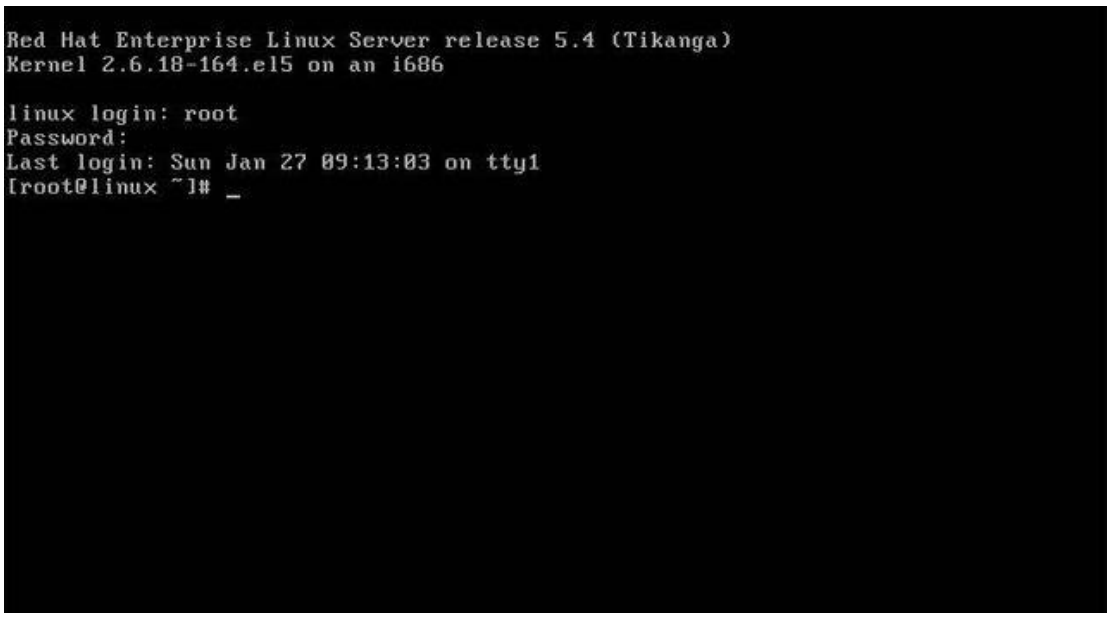
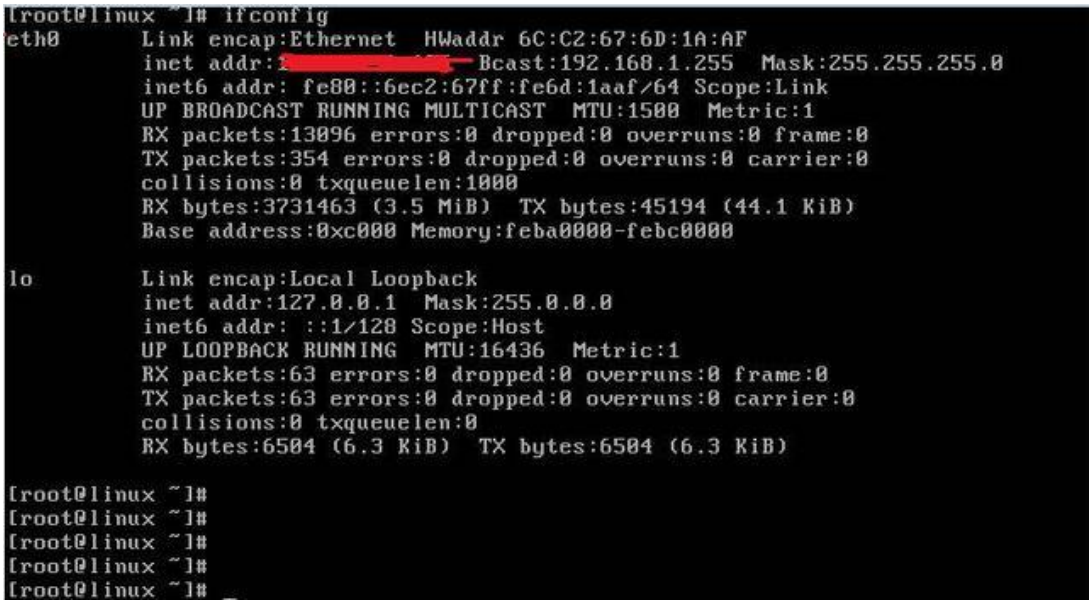
端口扫描之 autoscan

Autoscan 是一个用于查找在线主机的图形化网络扫描工具，该工具可以用来确定目标主机上开放的端口及确认目标主机的操作系统的类型。Autoscan 执行时，gui 会启用代理对目标主机进行信息收集，然后通过 tcp 内部连接将结果放回给 gui。Autoscan 的优点是简易，可以同时对多个网络进行扫描。

打开目标主机 linux，输入用户名：root，密码：123456.如图：

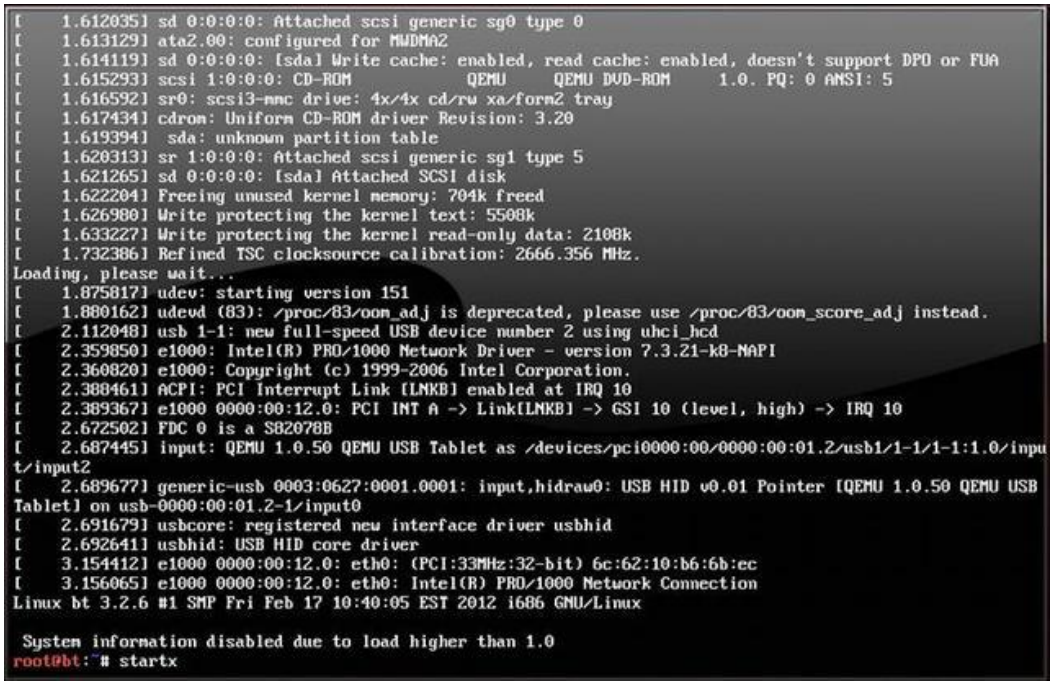


使用命令 ifconfig，查看 ip。Ip 为 192.168.1.10。(此处 ip 是通过 dhcp 获取的，不是每次都相同）如图：

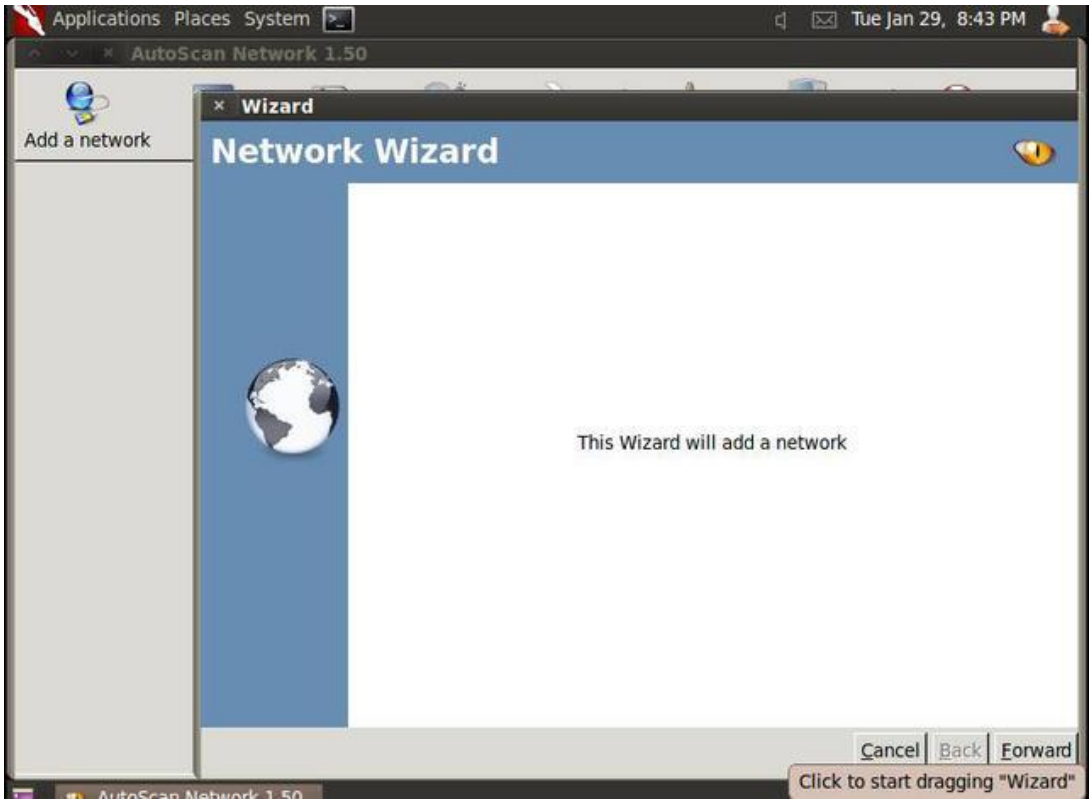


打开目标主机 bt5，进入如下命令行模式，然后输入 startx 进入图形界面。

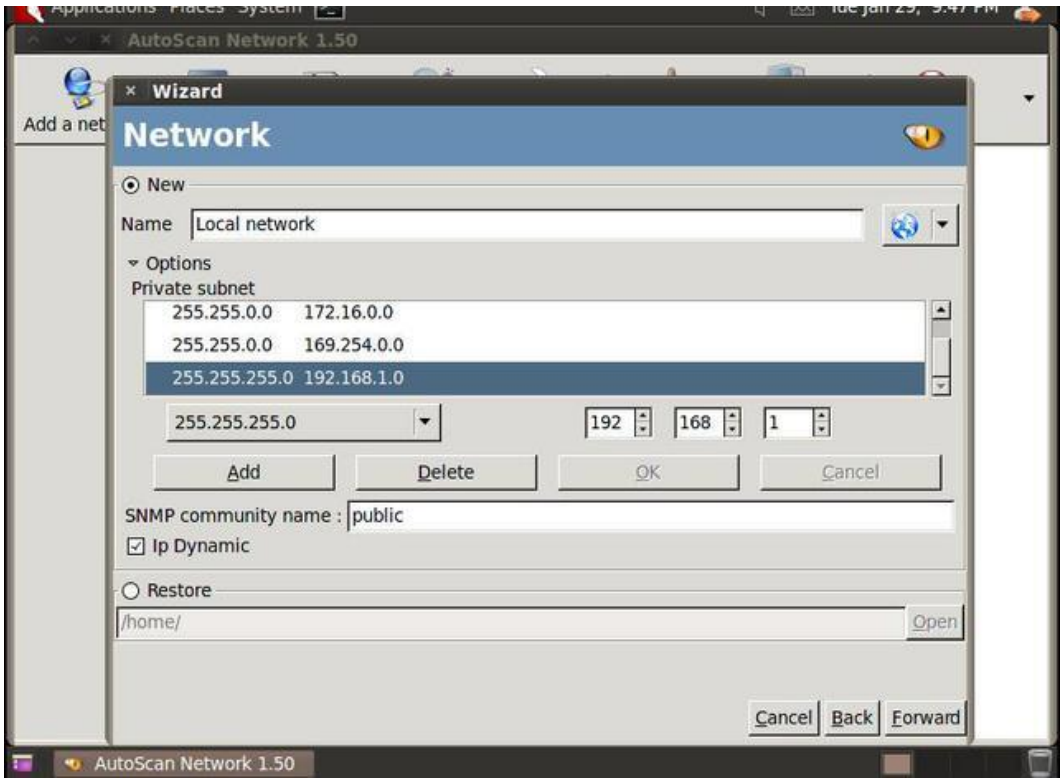
新手我们建议进入图形界面进行相应的操作。如图所示：



点击“application”——“backtrack”——“information gather”——“network analysis”——“network scanners”——“autoscan”，点击后，如下图所示：

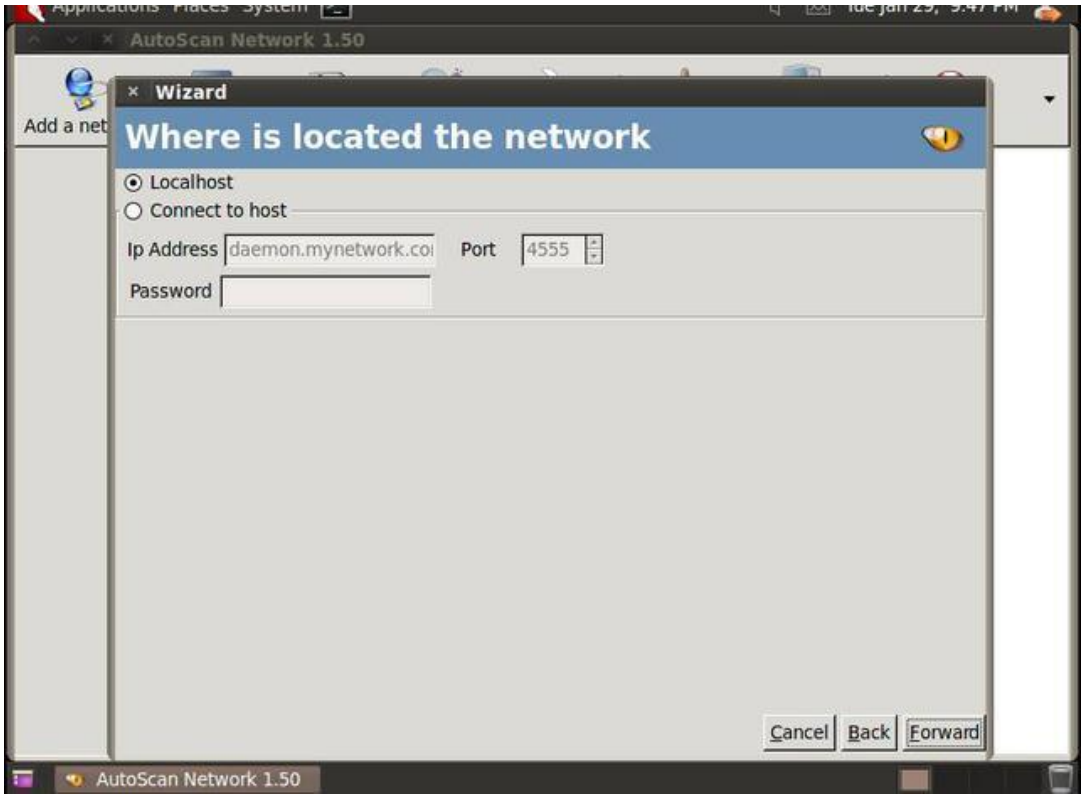


进入网络向导。采用 snmp 默认团体名称“public”，并选中 ip dynamic，完成创建网络后，点击 forward。如图：

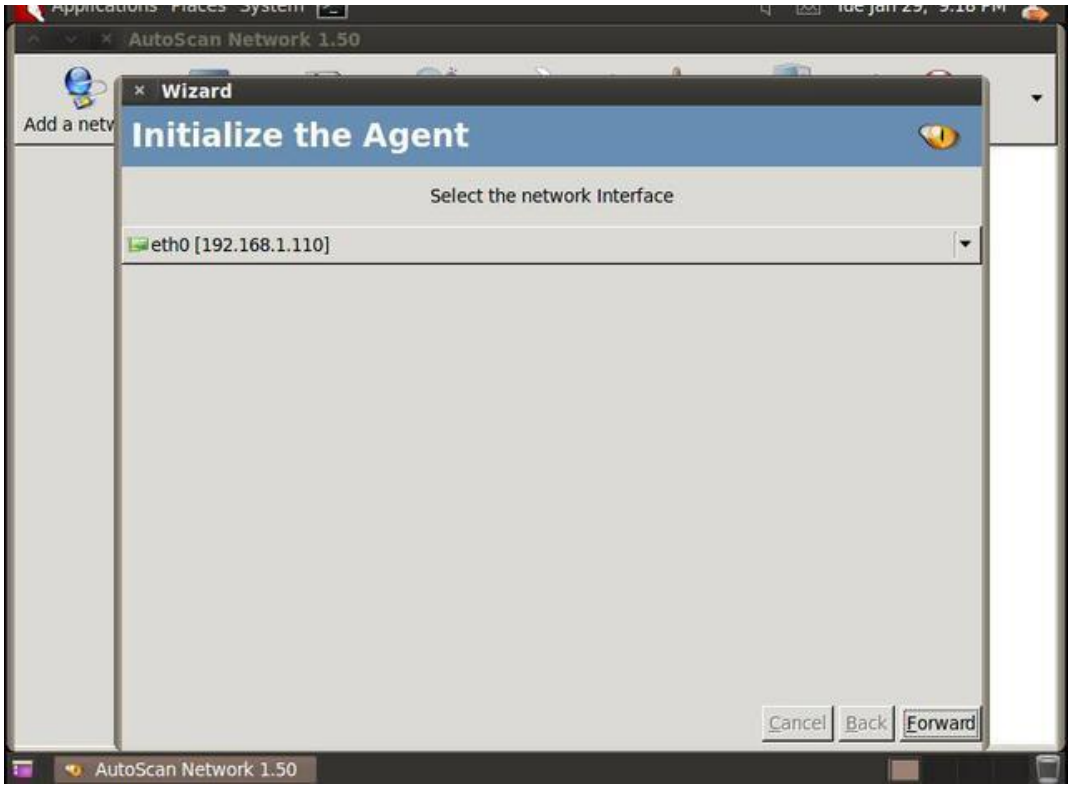


这里会显示代理设置，默认选择 localhost，因为这里没有远程任何代理。当

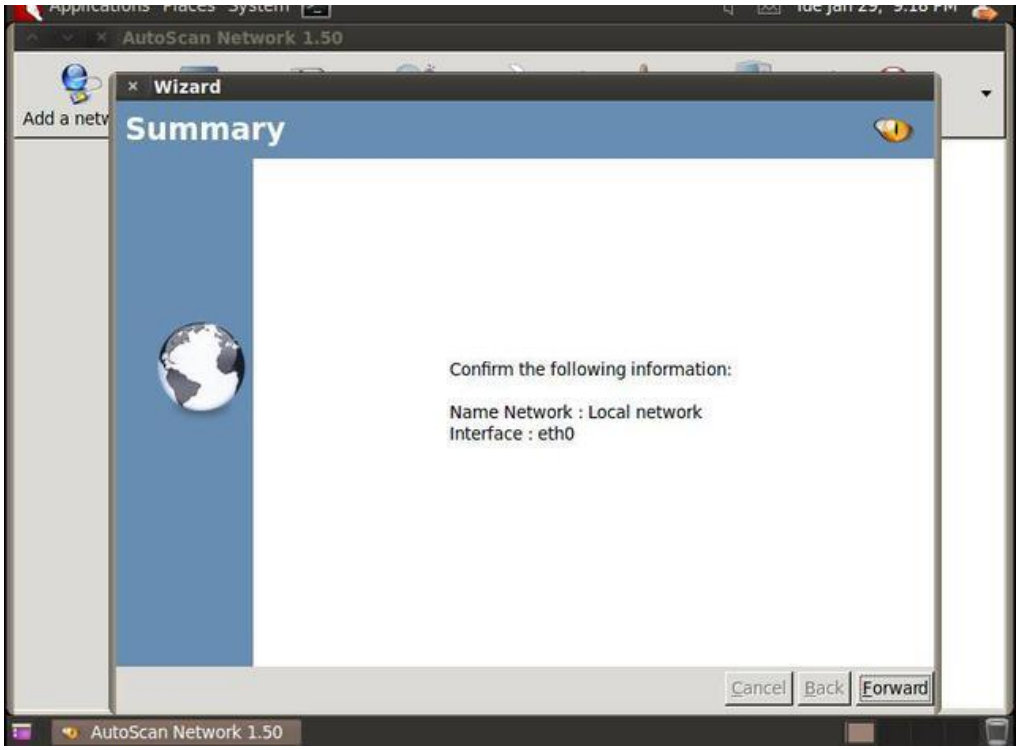
然，如果有代理我们也可以选择 connect to host，并输入 ip，端口，及密码。点击“forward”进入下一步设置。如图：



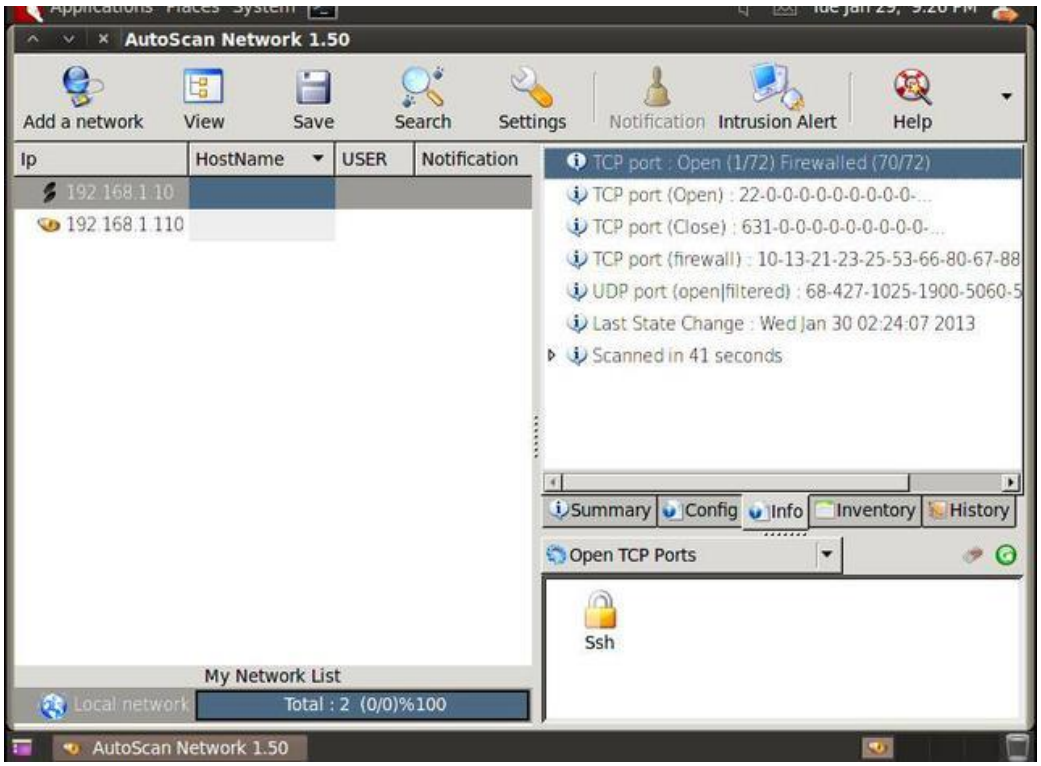
接下来将显示网卡选择窗口，点击 forward，进入下一步设置。如图:



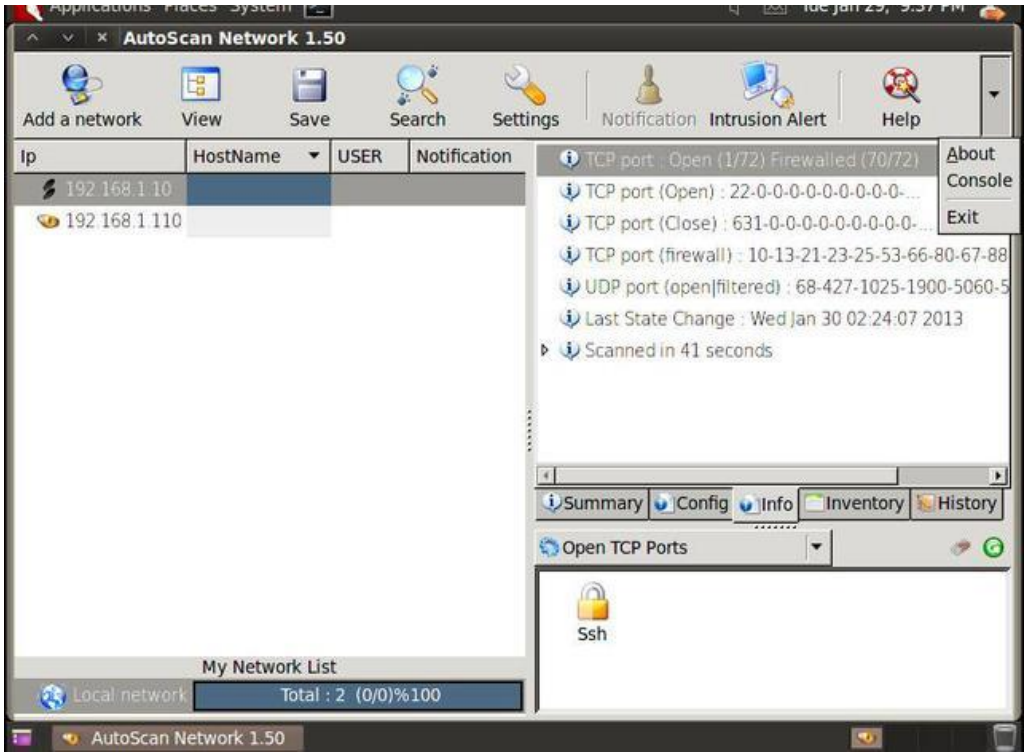
此时将显示引导配置的 summary，单击“forward”。如图：



确认配置后，开始扫描。从下图可知 linux 主机只开启了 ssh 端口。如图:



退出 autoscan 直接点击 exit。如图：


AutoScan Network 1.50
Add a network
View
Save
Search
Settings
Notification
Intrusion Alert
Help
Ip
HostName
USER
Notification
192.168.1.10
192.168.1.110
TCP port : Open (1/72) Firewalled (70/72)
TCP port (Open) : 22-0-0-0-0-0-0-0-0-0-...
TCP port (Close) : 631-0-0-0-0-0-0-0-0-0-...
TCP port (firewall) : 10-13-21-23-25-53-66-80-67-88
UDP port (open|filtered) : 68-427-1025-1900-5060-5
Last State Change : Wed Jan 30 02:24:07 2013
Scanned in 41 seconds
About
Console
Exit
Summary
Config
Info
Inventory
History
Open TCP Ports
Ssh
My Network List
Local network
Total : 2 (0/0)%100
AutoScan Network 1.50