

端口扫描之 autoscanner

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：

A terminal window showing the login process on a Red Hat Enterprise Linux Server. The text displayed is: Red Hat Enterprise Linux Server release 5.4 (Tikanga), Kernel 2.6.18-164.el5 on an i686, linux login: root, Password:, Last login: Sun Jan 27 09:13:03 on tty1, [root@linux ~]# _

```
Red Hat Enterprise Linux Server release 5.4 (Tikanga)
Kernel 2.6.18-164.el5 on an i686

linux login: root
Password:
Last login: Sun Jan 27 09:13:03 on tty1
[root@linux ~]# _
```

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：

```

[root@linux ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 6C:C2:67:6D:1A:AF
          inet addr:192.168.1.255  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::6ec2:67ff:fe6d:1aaf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:13096 errors:0 dropped:0 overruns:0 frame:0
          TX packets:354 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:3731463 (3.5 MiB)  TX bytes:45194 (44.1 KiB)
          Base address:0xc000 Memory:feba0000-febc0000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:63 errors:0 dropped:0 overruns:0 frame:0
          TX packets:63 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:6504 (6.3 KiB)  TX bytes:6504 (6.3 KiB)

[root@linux ~]#
[root@linux ~]#
[root@linux ~]#
[root@linux ~]#

```

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：

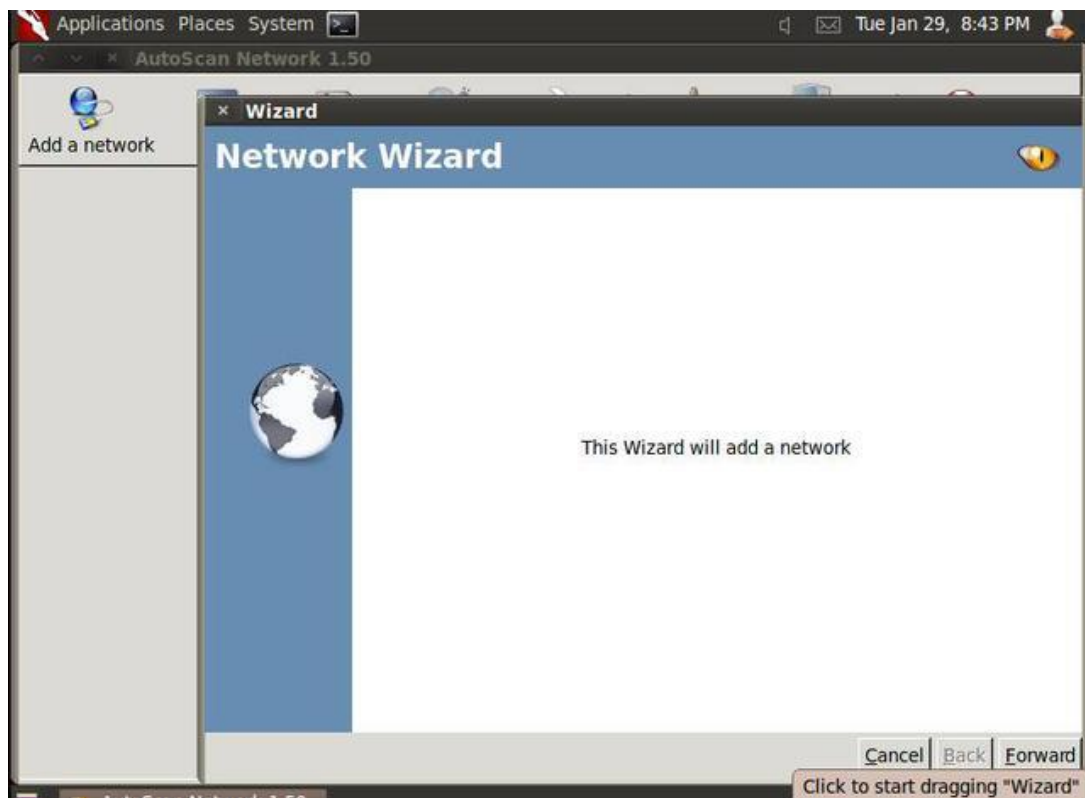
```

[ 1.612035] sd 0:0:0:0: Attached scsi generic sg0 type 0
[ 1.613129] ata2.00: configured for MWDMA2
[ 1.614119] sd 0:0:0:0: [sda] Write cache: enabled, read cache: enabled, doesn't support DPB or FUA
[ 1.615293] scsi 1:0:0:0: CD-ROM      QEMU      QEMU DVD-ROM      1.0. PQ: 0 ANSI: 5
[ 1.616592] sr0: scsi3-mmc drive: 4x/4x cd/rw xa/form2 tray
[ 1.617434] cdrom: Uniform CD-ROM driver Revision: 3.20
[ 1.619394] sda: unknown partition table
[ 1.620313] sr 1:0:0:0: Attached scsi generic sg1 type 5
[ 1.621265] sd 0:0:0:0: [sda] Attached SCSI disk
[ 1.622204] Freeing unused kernel memory: 704k freed
[ 1.626980] Write protecting the kernel text: 5508k
[ 1.633227] Write protecting the kernel read-only data: 2108k
[ 1.732386] Refined TSC clocksource calibration: 2666.356 MHz.
Loading, please wait...
[ 1.875817] udev: starting version 151
[ 1.880162] udevd (83): /proc/83/oom_adj is deprecated, please use /proc/83/oom_score_adj instead.
[ 2.112048] usb 1-1: new full-speed USB device number 2 using uhci_hcd
[ 2.359850] e1000: Intel(R) PRO/1000 Network Driver - version 7.3.21-k8-NAPI
[ 2.360820] e1000: Copyright (c) 1999-2006 Intel Corporation.
[ 2.388461] ACPI: PCI Interrupt Link [LNKB] enabled at IRQ 10
[ 2.389367] e1000 0000:00:12:0: PCI INT A -> Link[LNKB] -> GSI 10 (level, high) -> IRQ 10
[ 2.672502] FDC 0 is a S82078B
[ 2.687445] input: QEMU 1.0.50 QEMU USB Tablet as /devices/pci0000:00/0000:00:01.2/usb1/1-1/1-1:1.0/input2
[ 2.689677] generic-usb 0003:0627:0001:0001: input,hidraw0: USB HID v0.01 Pointer [QEMU 1.0.50 QEMU USB Tablet] on usb-0000:00:01.2-1/input0
[ 2.691679] usbcore: registered new interface driver usbhid
[ 2.692641] usbhid: USB HID core driver
[ 3.154412] e1000 0000:00:12:0: eth0: (PCI:33MHz:32-bit) 6c:62:10:b6:6b:ec
[ 3.156065] e1000 0000:00:12:0: eth0: Intel(R) PRO/1000 Network Connection
Linux bt 3.2.6 #1 SMP Fri Feb 17 10:40:05 EST 2012 i686 GNU/Linux

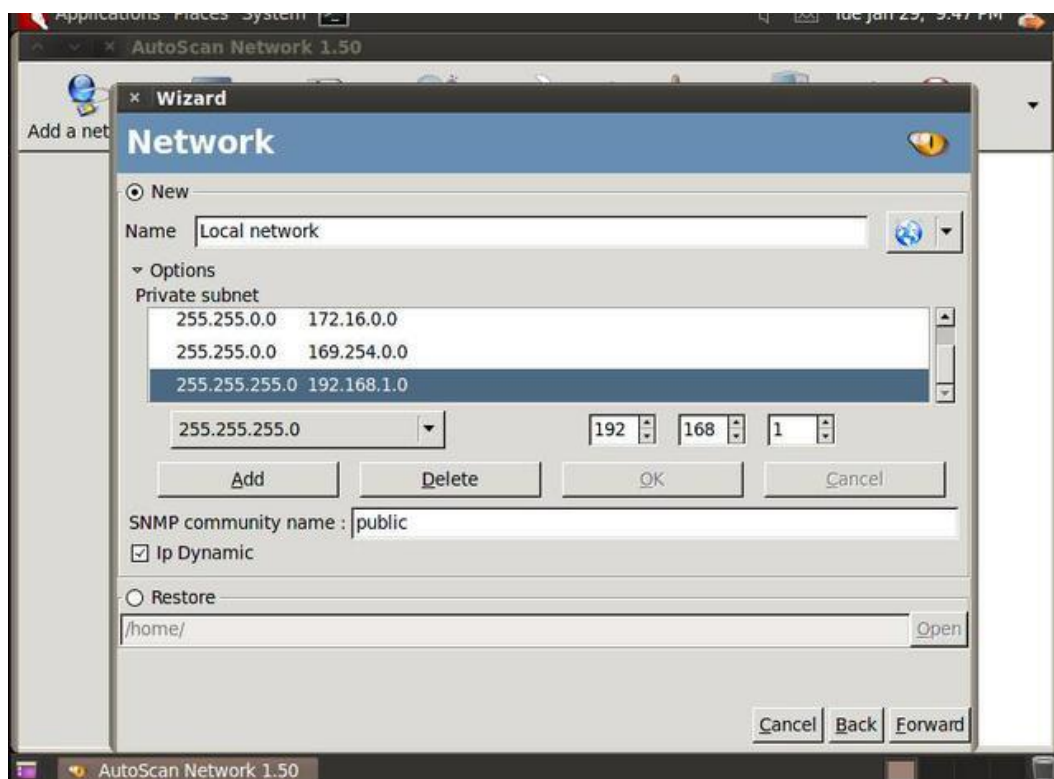
System information disabled due to load higher than 1.0
root@bt: # startx

```

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

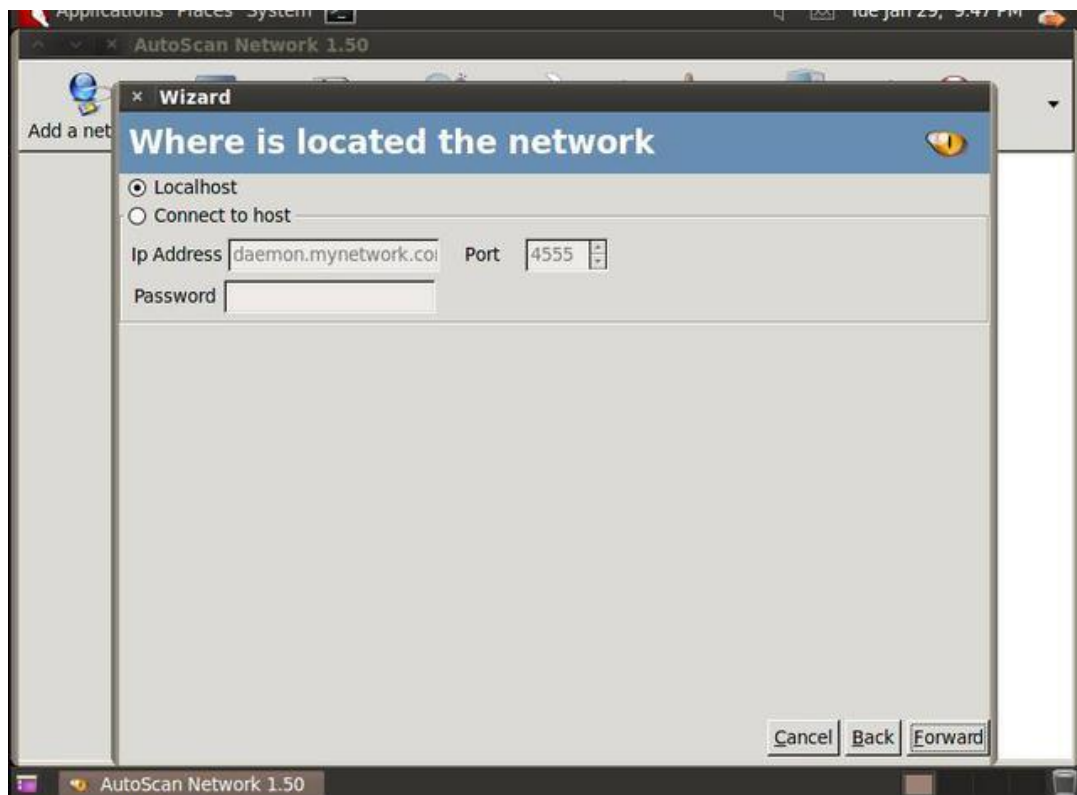


进入网络向导。采用 snmp 默认团体名称“public”，并选中 ip dynamic，完成创建网络后，点击 forward。如图：

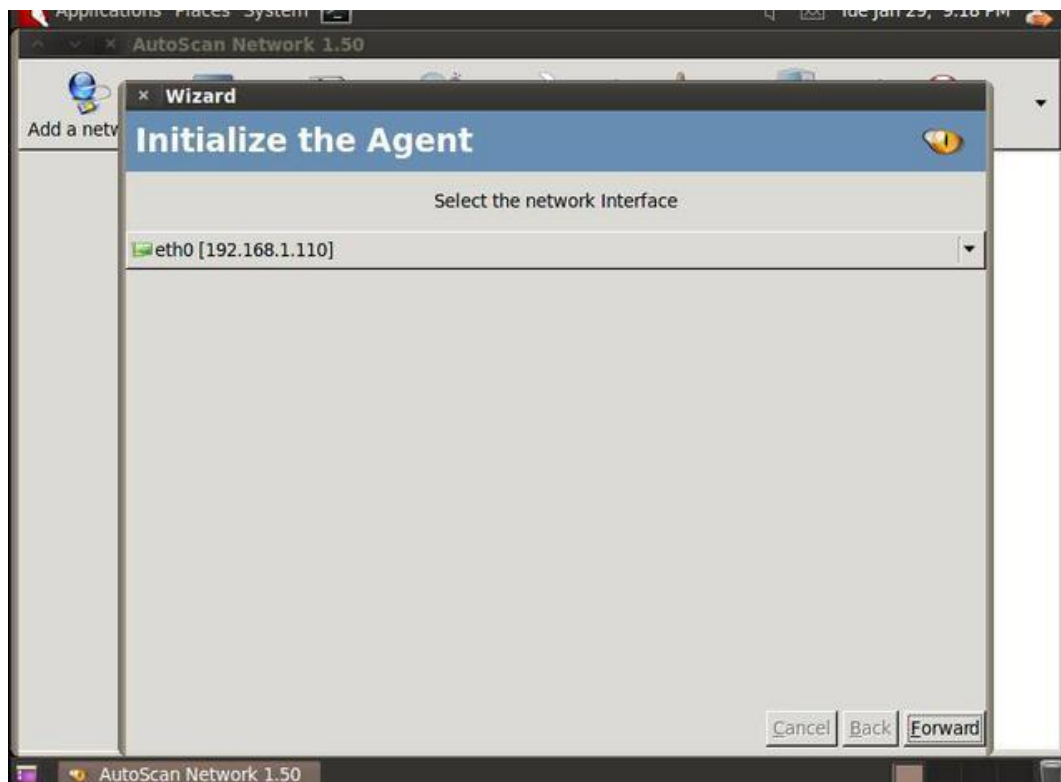


这里会显示代理设置，默认选择 localhost，因为这里没有远程任何代理。当

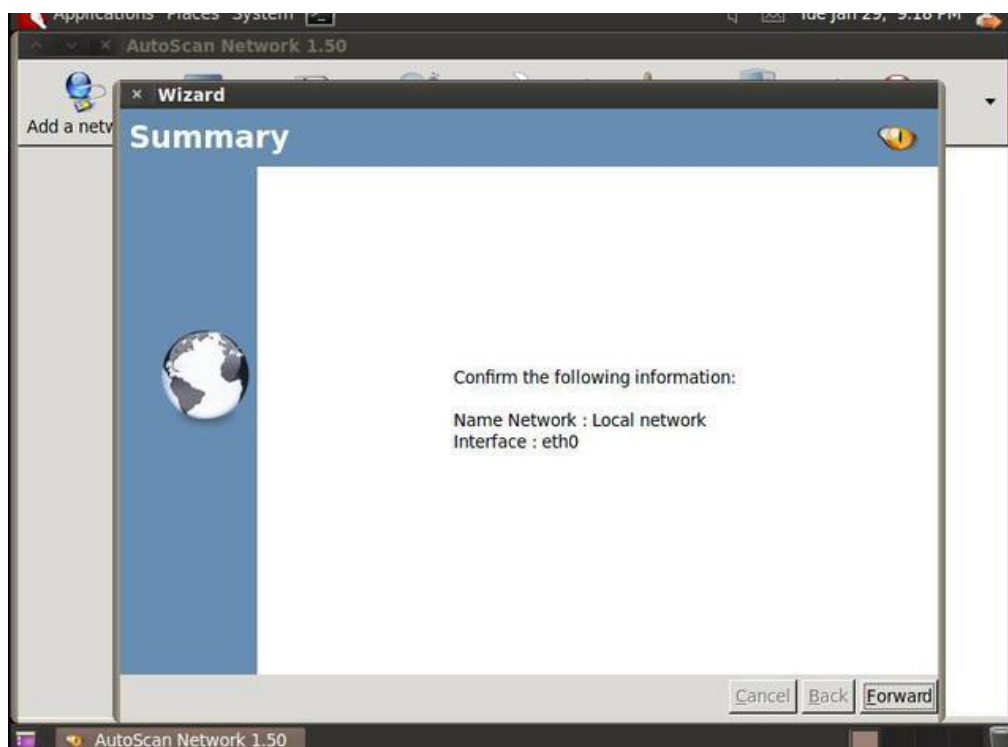
然，如果有代理我们也可以选择 connect to host，并输入 ip，端口，及密码。点击“forward”进入下一步设置。如图：



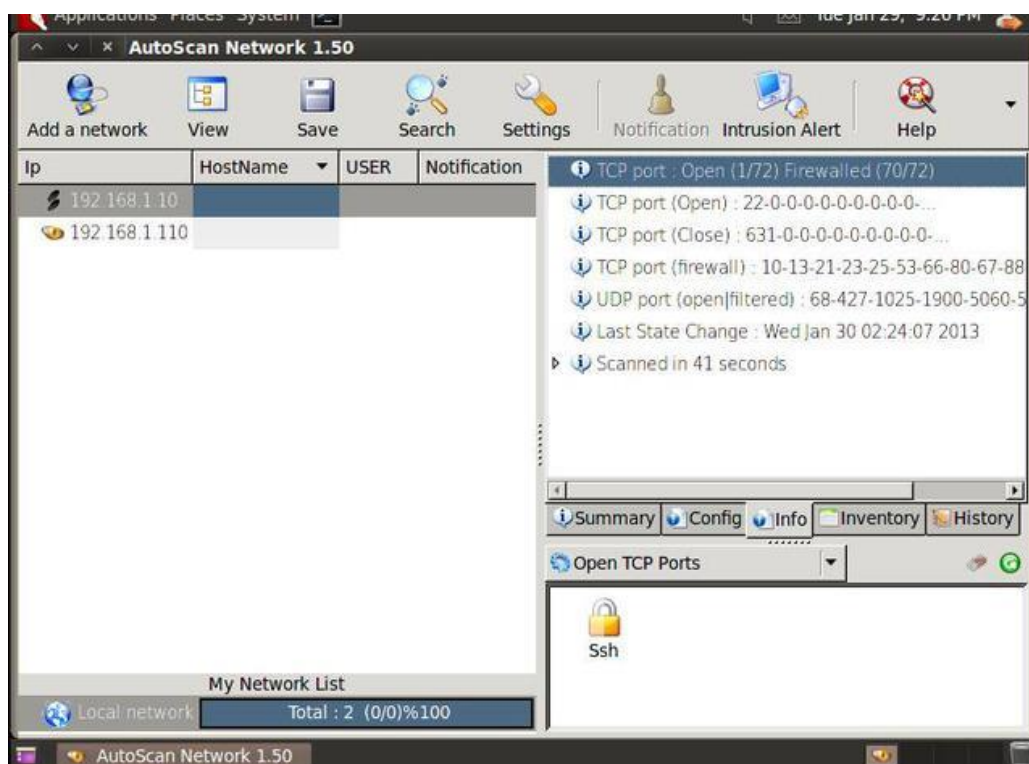
接下来将显示网卡选择窗口，点击 forward，进入下一步设置。如图：



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：

