Netdiscover

Time required: 30 minutes

How to Create Screenshots: Please use the Windows Snip and Sketch Tool or the Snipping Tool. Paste a screenshot of just the program you are working on. If you are snipping a virtual machine, make sure your focus is outside the virtual machine before you snip.

1. Press and hold down the **Windows key** & **Shift**, then type **S.** This brings up the on-screen snipping tool.
2. Click and Drag your mouse around whatever you want to snip.
3. Release the mouse button. This places the snip into the Windows Clipboard.
4. Go into Word or wherever you want to paste the snip. Hold down **CTRL**, then type **V** to paste the snip.

Network Scanning

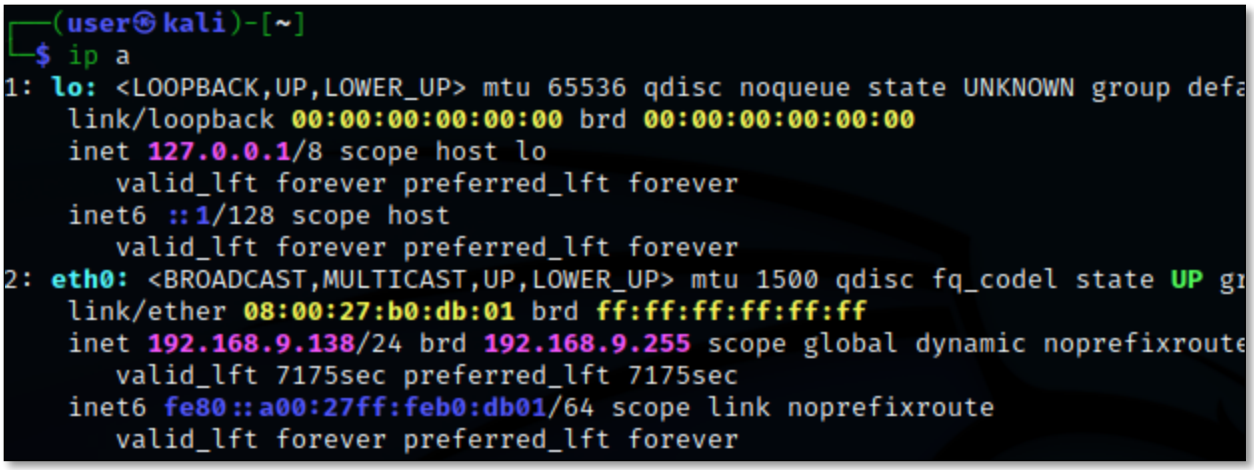
Please use a bridged adapter for this assignment. We want to scan your local network. Only scan a network you own or have permission to scan.

What is Netdiscover?

Netdiscover is a simple ARP scanner which can be used to scan live hosts in a network. It can scan for multiple subnets also. It simply produces the output in a live display(ncurse). This can be used in the first phases of a pentest where you have access to a network. Netdiscover is a simple and initial-recon tool which can be very handy.

Netdiscover Tutorial

1. Start Kali Linux → open a terminal session.
2. Make sure the Kali Linux VM is connected to the **Bridged Network**.
3. Type **ip -a**
4. You should get a response like this. Notice **eth0: inet** is 192.168.9.0/24 That is the network range you will scan. Yes, your network range will be different.



5. **Insert a screenshot:**

Click or tap here to enter text.

6. Type **sudo netdiscover -help**
7. The resulting help screen shows the arguments that can be used

This example is how to scan a network range. In a few moments, you should see your network devices.

```
# sudo netdiscover -r <range>
sudo netdiscover -r 192.168.9.0/24
```

8. **Insert a screenshot:**

Click or tap here to enter text.

9. Type **CTRL-C** to exit netdiscover.
10. Parse the output to a file as shown. Use your network settings.

```
# sudo netdiscover -r <range> -P ls
sudo netdiscover -r 192.168.9.0/24 -P > network.txt
```

11. You won't see anything as the stdout was piped to a file.
12. Type **ls** to list the directory.
13. Type **nano network.txt**
14. You should see the devices on your network in the text file.

Assignment Submission

Attach this completed document and network.txt to the assignment in Blackboard.