Local Network Analysis

Singhal, Madhur 2015CS10235

Chhajwani, Anant 2015CS50281

August 21, 2017

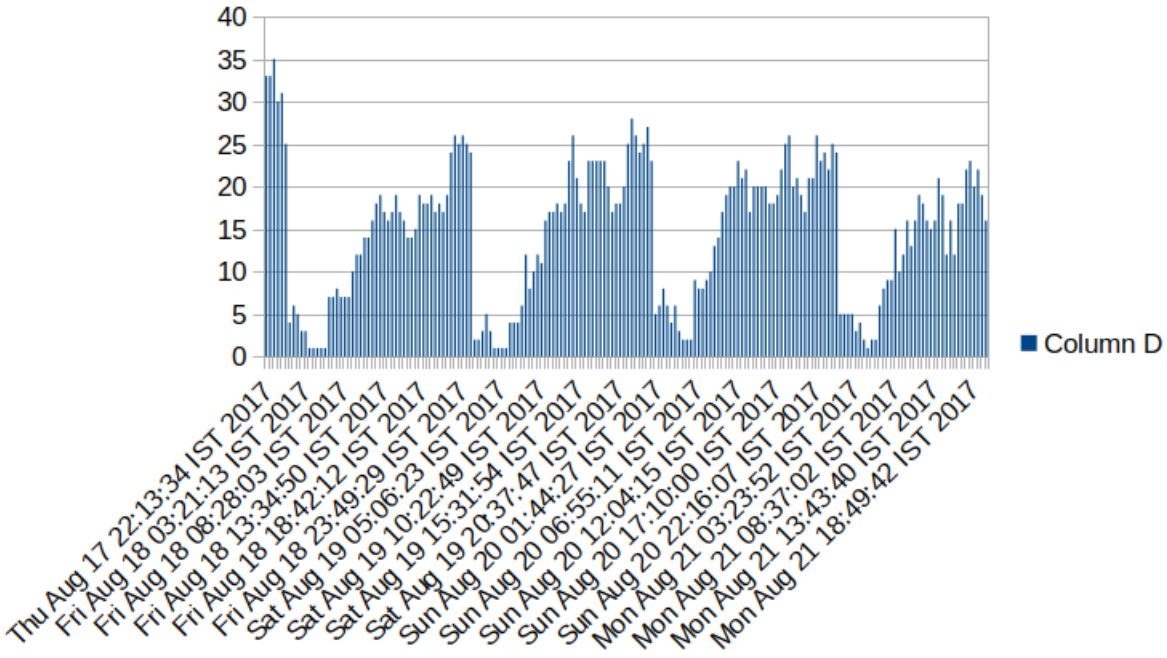
1 Introduction

Nmap is a free and open source utility for network exploration and security auditing. It is primarily used for probing networks to reveal the active hosts and discover the ports and services that the hosts respond to.

In this assignment we created a script to monitor a local subnet and track the number of hosts up at different points in time. We also ran nmap by itself on the local subnet to identify different hosts and services running.

2 Number of Hosts

The number of hosts was found to vary between 0 and 35. At nights, because of the LAN ban the number of hosts decreased significantly. Some hosts which are still up could be routers or mis-configured hosts. A graph is provided which plots the time dependence of the number of hosts. The median number of hosts is 17.



3 Hosts and Services

This question seems a bit broad, nevertheless I have provided a list of 16 hosts up when I checked today and their services.

1. Nmap scan report for 10.203.148.1
    - Host is up (0.031s latency).
    - Not shown: 996 closed ports
    - PORT STATE SERVICE
    - 22/tcp open ssh
    - 23/tcp open telnet
    - 80/tcp open http
    - 443/tcp open https
2. Nmap scan report for 10.203.148.15
    - Host is up (0.064s latency).

- Not shown: 994 closed ports
- PORT STATE SERVICE
- 668/tcp filtered mecomm
- 1079/tcp filtered asprovatalk
- 3851/tcp filtered spectraport
- 5906/tcp filtered unknown
- 7443/tcp filtered oracleas-https
- 49175/tcp filtered unknown

3. Nmap scan report for 10.203.148.32

- Host is up (0.073s latency).
- Not shown: 986 closed ports
- PORT STATE SERVICE
- 135/tcp open msrpc
- 139/tcp open netbios-ssn
- 445/tcp open microsoft-ds
- 1935/tcp open rtmp
- 2869/tcp open icslap
- 3517/tcp filtered 802-11-iapp
- 5357/tcp open wsdapi
- 8080/tcp open http-proxy
- 10025/tcp filtered unknown
- 49152/tcp open unknown
- 49153/tcp open unknown
- 49154/tcp open unknown
- 49155/tcp open unknown
- 49156/tcp open unknown

4. Nmap scan report for 10.203.148.72

- Host is up (0.013s latency).

- Not shown: 979 closed ports
- PORT STATE SERVICE
- 80/tcp open http
- 135/tcp open msrpc
- 139/tcp open netbios-ssn
- 301/tcp filtered unknown
- 443/tcp open https
- 445/tcp open microsoft-ds
- 1718/tcp filtered h323gatedisc
- 2909/tcp filtered funk-dialout
- 5033/tcp filtered jtnetd-server
- 5357/tcp open wsdapi
- 5925/tcp filtered unknown
- 8200/tcp filtered trivnet1
- 9011/tcp filtered unknown
- 30718/tcp filtered unknown
- 49152/tcp open unknown
- 49153/tcp open unknown
- 49154/tcp open unknown
- 49155/tcp open unknown
- 49156/tcp open unknown
- 49157/tcp open unknown
- 49999/tcp filtered unknown

5. Nmap scan report for 10.203.148.82
    - Host is up (0.013s latency).
    - All 1000 scanned ports on 10.203.148.82 are filtered
6. Nmap scan report for 10.203.148.94
    - Host is up (0.15s latency).

- Not shown: 986 closed ports
- PORT STATE SERVICE
- 714/tcp filtered iris-xpcs
- 1022/tcp filtered exp2
- 1028/tcp filtered unknown
- 1049/tcp filtered td-postman
- 1102/tcp filtered adobeserver-1
- 1352/tcp filtered lotusnotes
- 1687/tcp filtered nsjtp-ctrl
- 2008/tcp filtered conf
- 2323/tcp filtered 3d-nfsd
- 2525/tcp filtered ms-v-worlds
- 3880/tcp filtered igrs
- 5051/tcp filtered ida-agent
- 5910/tcp filtered cm
- 44442/tcp filtered coldfusion-auth

7. Nmap scan report for 10.203.148.125

    - Host is up (0.035s latency).
    - Not shown: 999 closed ports
    - PORT STATE SERVICE
    - 22/tcp open ssh

8. Nmap scan report for 10.203.148.144

    - Host is up (0.034s latency).
    - Not shown: 995 closed ports
    - PORT STATE SERVICE
    - 106/tcp filtered pop3pw
    - 1352/tcp filtered lotusnotes

- 1900/tcp filtered upnp
- 2608/tcp filtered wag-service
- 8652/tcp filtered unknown

9. Nmap scan report for 10.203.148.162
    - Host is up (0.029s latency).
    - Not shown: 986 closed ports
    - PORT STATE SERVICE
    - 42/tcp filtered nameserver
    - 135/tcp open msrpc
    - 139/tcp open netbios-ssn
    - 264/tcp filtered bgmp
    - 306/tcp filtered unknown
10. Nmap scan report for 10.203.149.14
    - Host is up (0.029s latency).
    - All 1000 scanned ports on 10.203.149.14 are closed
11. Nmap scan report for 10.203.149.20
    - Host is up (0.033s latency).
    - Not shown: 999 closed ports
    - PORT STATE SERVICE
    - 21/tcp filtered ftp
12. Nmap scan report for 10.203.149.30
    - Host is up (0.022s latency).
    - Not shown: 999 filtered ports
    - PORT STATE SERVICE
    - 6646/tcp open unknown
13. Nmap scan report for 10.203.149.59

- Host is up (0.025s latency).
- All 1000 scanned ports on 10.203.149.59 are closed

14. Nmap scan report for 10.203.149.62

    - Host is up (0.056s latency).
    - Not shown: 979 closed ports
    - PORT STATE SERVICE
    - 135/tcp open msrpc
    - 139/tcp open netbios-ssn
    - 445/tcp open microsoft-ds
    - 554/tcp open rtsp
    - 555/tcp filtered dsf
    - 1148/tcp filtered elfiq-repl
    - 1500/tcp filtered vlsi-lm
    - 1935/tcp open rtmp
    - 2869/tcp open icslap
    - 5357/tcp open wsdapi
    - 5862/tcp filtered unknown
    - 8089/tcp filtered unknown
    - 10243/tcp open unknown
    - 49152/tcp open unknown
    - 49153/tcp open unknown
    - 49154/tcp open unknown
    - 49155/tcp open unknown
    - 49156/tcp open unknown
    - 49158/tcp open unknown
    - 49165/tcp open unknown

15. Nmap scan report for 10.203.149.115

    - Host is up (0.078s latency).

- Not shown: 993 filtered ports
- PORT STATE SERVICE
- 80/tcp open http
- 515/tcp open printer
- 1801/tcp open msmq
- 2103/tcp open zephyr-clt
- 2105/tcp open eklogin
- 2107/tcp open msmq-mgmt
- 2869/tcp open icslap

16. Nmap scan report for 10.203.149.155

    - Host is up (0.042s latency).
    - Not shown: 999 filtered ports
    - PORT STATE SERVICE
    - 80/tcp open http

4 Gateways and DNS Servers

The DNS Servers **10.10.1.2 and 10.10.2.2**, are used in IIT Delhi for serving DNS requests of users. Many users also use external DNS servers like Google's 8.8.8.8 for their DNS needs.

The gateways are different for each area and I didn't find any list of them all. For my hostel (Jwalamukhi) the LAN gateways seem to be **10.254.203.6 and 10.254.203.2**.

For Vision Lab in Bharti Building, the gateways are **10.254.208.2 and 10.254.208.6**.