Distributed Computer Systems Lab
http://disco.informatik.uni-kl.de

Network Forensic System for Internet Scanners

Subin Joseph P
subin.joseph7@gmail.com

Table of Contents

Motivation

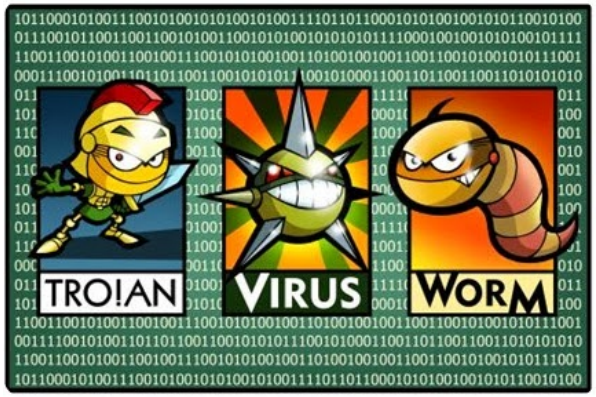
- What is Network Security?
  - Network security involves all activities that organizations and institutions undertake to protect the usability and integrity of the network and data.

- Why care about network security?
  - Using computers for everything now

  - Confidentiality is needed (eg: Email)

Motivation

- Threats to Network Security
  - Viruses, Computer Worm
  - Attacks
    - Reconnaissance attacks (Port Scanning)
    - Denial of service attacks



Motivation

- Port Scanning/ Internet Scanning
  - A port scan is a method used to discover the services running on a target machine
  - Determine the status of that port (open/closed)
- Port Scanning Use
  - Researchers - to learn new types of vulnerabilities
  - Attackers - to locate opened/vulnerable ports

Motivation

- How to detect Port scans?
  - Using Network Telescope
- What is network telescope?
- Any previous works on Port scanning Detection ?
  - Yes
  - Relied on large network telescope
  - Used passive network telescope

Motivation

- What differs our work from previous works?
  - Consists of very small number of IP addresses
  - WHY?
    - Check the feasibility of port scanning detection from very small network telescope
  - Considered two configurations of network telescope for packet capturing
- Network telescope Configurations Used
  - Passive Network Telescope
  - Network Telescope with Honeypot

Problem Statement

- Our Objectives are:
  - Analyse the packets captured using very small network telescope and find pattern depending on behavior of port scanners
  - Compare the results from the packets captured using two different configurations of network telescope
  - Find pattern depending on transport layer protocols used to send port scans

Background

- What is Network Telescope
  - Monitors range of unused routed Internet address space
  - No active services or servers reside
  - Little or no legitimate traffic
  - Usually consists of very large number of IP addresses (eg: CAIDA - single /8 network block)

- Types of Network Telescopes
  - Passive : able to capture the incoming packets, however is unable to respond to these packets
  - Active : responds to the incoming packets and try to establish the connection using 3-way TCP handshake

Background

- Port Scanning Techniques
  - TCP SYN Scan
    - SYN ----> SYN/ACK ----> RST (If port is open)
    - SYN ----> RST (If port is closed)
  - TCP Connect Scan
    - SYN ----> SYN/ACK ----> ACK ---->RST (If port is open)
    - SYN ----> RST (If port is closed)
  - TCP FIN, Xmas Tree, Null Scans
    - Closed ports send RESET
    - Open ports send nothing.
  - UDP Scan
    - Open ports send nothing (except some specific ports to which protocol specific payload is sent)
    - Closed ports send ICMP port unreachable error message

Background

- Types of port scanning activity
  - Based on pattern of destination ports and target machines the scan examines

    Vertical and Horizontal
  - Vertical Scan - Targets multiple destination ports on a same IP address
  - Horizontal Scan - Scans multiple IP addresses, but targets only one specific port
  - Block Scan – Combination of both scans

Design

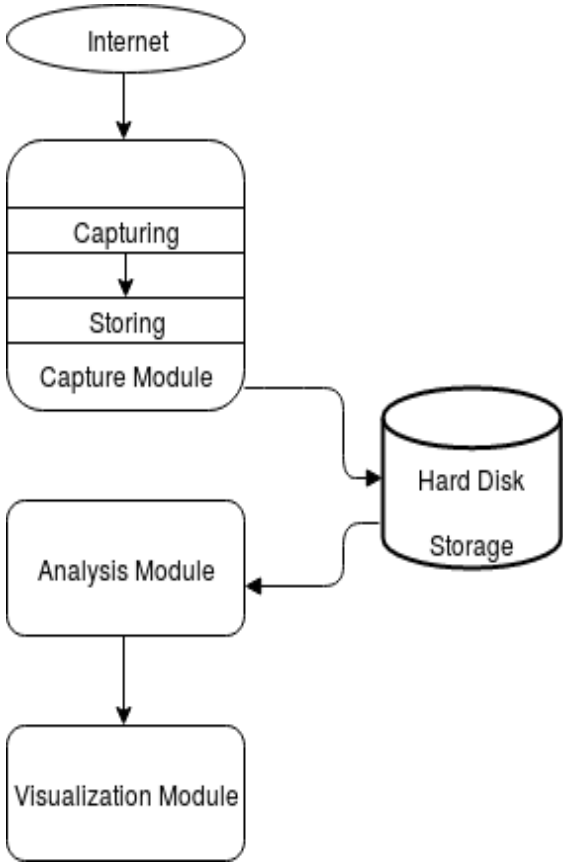
- Architecture of Network Forensic System
  - Capture Module
    - Packet Capturing System for UNIX
  - Analysis Module
    - Separate port scans from other packets

    But How??

    Several Methods to hide port scanning from host system

    1. Increase timing between successive scans

    2. Scan from block of addresses using Spoofed IPs



Design

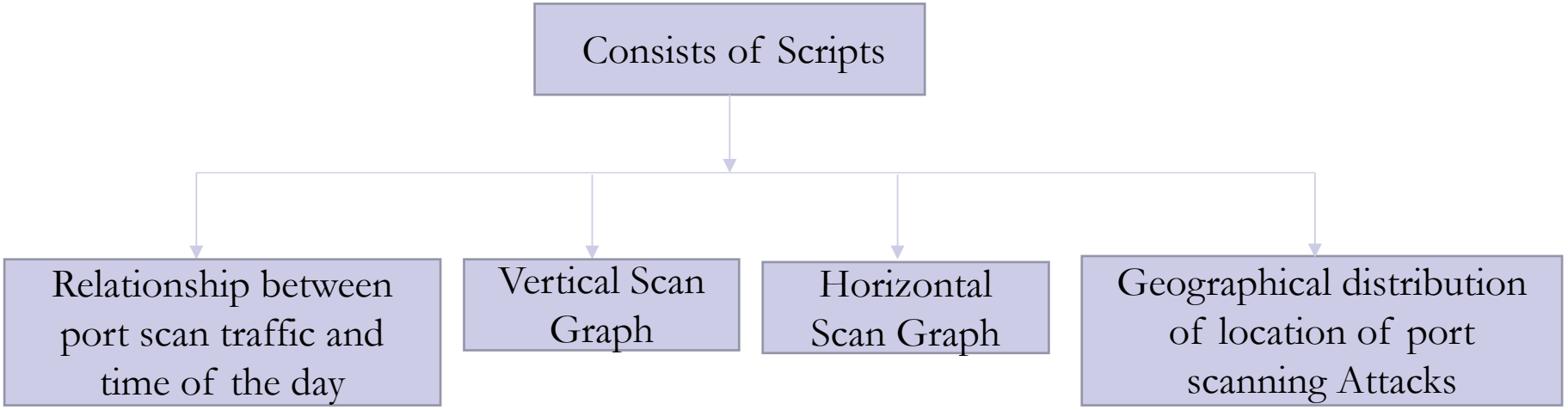
- Architecture of Network Forensic System
  - Analysis Module

    1. Look for port scans from the same source for definite amount of time
    2. Using two methods:
       - 2.1. Group scans of source IPs from same /24 network
       - 2.2. Group scans of source IPs from same ISP

    - Filter out TCP and UDP port scans
    - Divide into Vertical and Horizontal scans
    - Categorize the port scans into different port scanning techniques

Design

- Architecture of Network Forensic System
  - Visualization Module



- Consists of several scripts
- Numerical and Graphical Results
- Get better perception about port scans

Implementation

- Capture Module
  - Packet capturing system - Implemented using C (libpcap)
  - Store packets for further analysis
- Analysis Module
  - Port scanning detection - Implemented using Python
  - Implemented using a buffer – Stores each packet till next comes

```
for each IPv4 packet in the captured file do
    if the packet matches TCP then
        if the packet fulfills three way handshake condition then
            if the packet is TCP connect scan then
                increment the occurrence of connect scan;
                continue;
        else if the packet is TCP half connect scan then
            increment the occurrence of half connect scan;
            continue;
        else if the packet does not fulfill three way handshake condition then
            if the packet is FIN scan then
                increment the occurrence of FIN scan;
                continue;
        else if the packet is Xmas scan then
            increment the occurrence of Xmas scan;
            continue;
        else if the packet is null scan then
            increment the occurrence of null scan;
            continue;
    else if the packet matches UDP then
        if the packet is UDP scan then
            increment the occurrence of UDP scan;
            continue;
end
```

Algorithm 1: port scanning detection

Implementation

- Analysis Module
  - Counter Methods to avoid port scan detection

  1. Look for port scans from the same source for 300 seconds

  2.1. Combines the source IPs with same first 3 bytes of the IP address

  2.2. Using IPWhois to identify ASN of each ISP

- Visualization Module
  - Implemented using Python scripts
  - Used GEOLITE: Geolocation library from MaxMind
  - Used Pytz: library allows timezone calculations

Experimental Setup

- Network Telescope - 25 IP addresses from same /24 network

First Stage

- Passive Network Telescope
- Port 22 is Open
- Used Ubuntu-16.04
- Capture Duration – 450 hrs
- Packet Capture – **12** – **31** Jan 2017

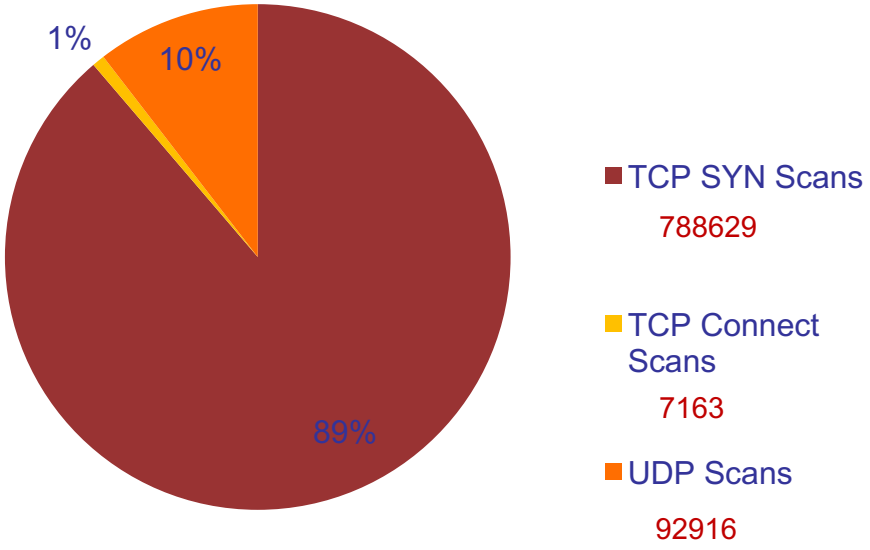
Second Stage

- Network Telescope with Honeypot
- Used T-Pot from Deutsche Telekom
- Used Ubuntu-14.04
- Capture Duration – 450 hrs
- Packet Capture – **13 - 23** March 2017 and **28** March **- 5** April 2017

Evaluation

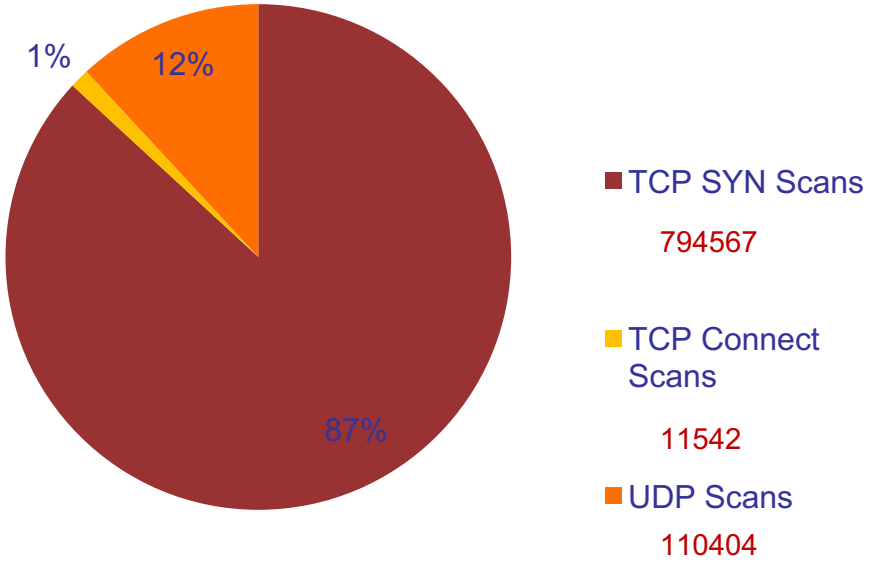
- Detecting scans and categorizing it

Network Telescope Without Honeypot



Total port scans - 888708

Network Telescope With Honeypot



Total port scans - 916513

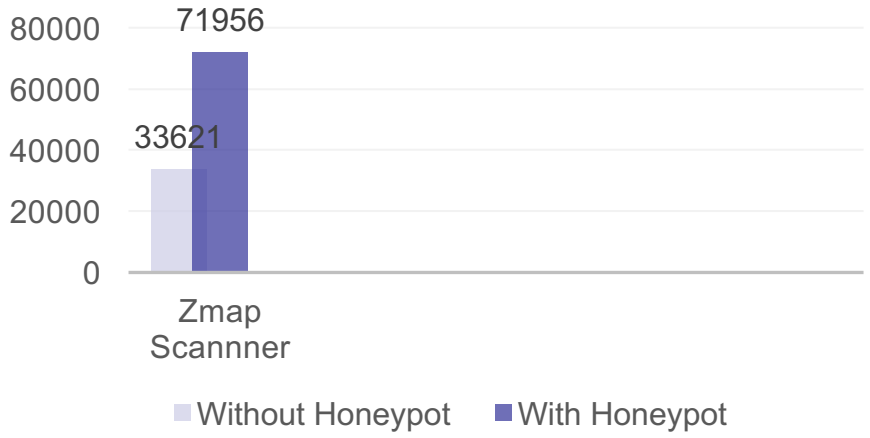
Evaluation

- Detecting scans and categorizing it

  - TCP SYN scans – 89% and 87% of Total scans
  - No occurrence of Xmas scan, Null scan and FIN scan
  - Similar Behavior
  - TCP port scans > UDP port scans

Evaluation

- How to identify Internet scanners?
  - Uses IP identification field
  - Zmap – Constant Value (**54321**)
  - Massscan - $IP\_id = Dest\_address \oplus Dest\_port \oplus TCP\_seqno$
  - Could not find a method for fingerprinting Nmap scans
  - Massscan is negligible (6 observations during both periods of time)



Evaluation

- Horizontal and Vertical Scans
  - Horizontal Scan Size - Number of distinct destination IPs scanned
  - Vertical Scan Size - Number of distinct destination ports scanned

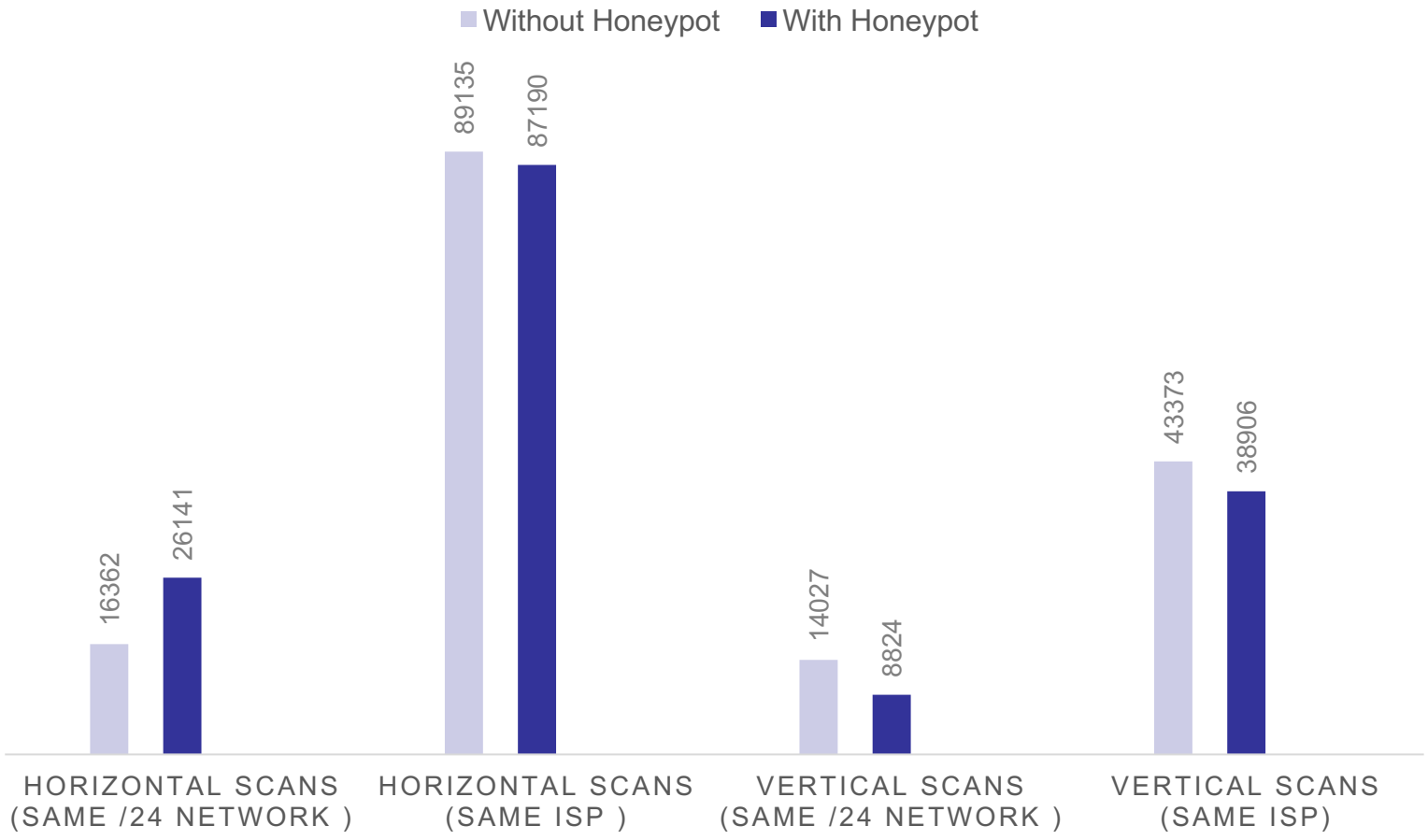
- Analyse the packets based on number of scans on each scan size for horizontal and vertical scans

- Group horizontal scans/ vertical scans of source IPs from same /24 network or same ISP

- Considered horizontal and vertical scans in TCP and UDP port scans separately

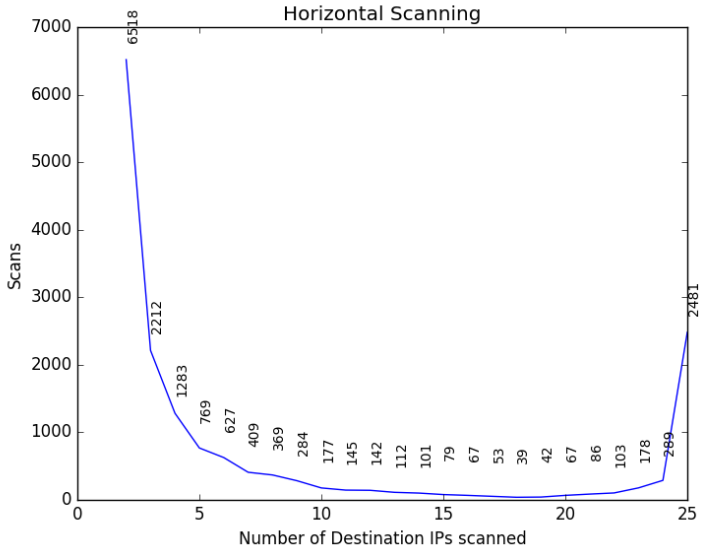
Evaluation

- Horizontal and Vertical Scans in TCP Port Scans



Evaluation

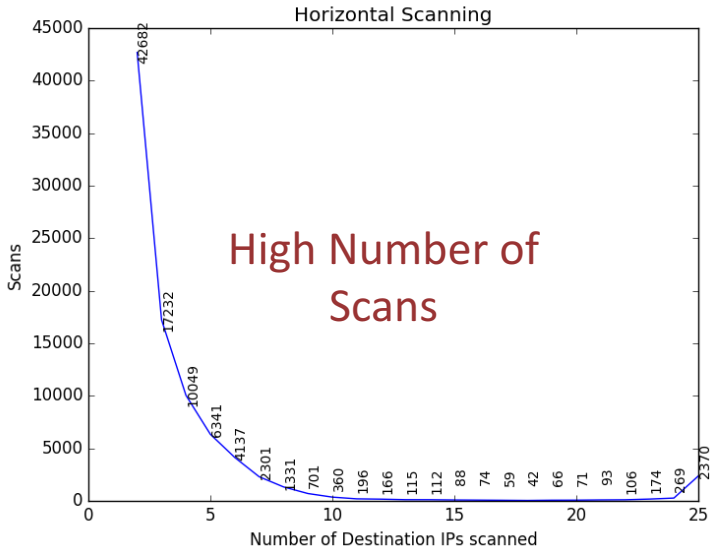
- Horizontal Scans in TCP Port Scans
- Used 1st configuration
  (network telescope without honeypot)



Grouped by same /24 network

- Behavior - Number of horizontal scans keep reducing when scan size increases

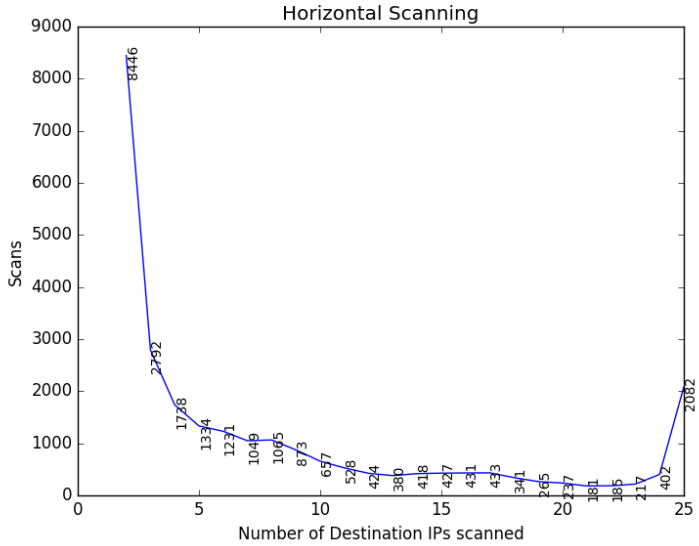
- Why small spike at scan size 25?
  - 35% of the total scan sources scanned multiple times (Contributed 80% of total scans)
  - 40% of the total port scans were block scans
  - But No way to check the behavior beyond 25 IPs



Grouped by same ISP

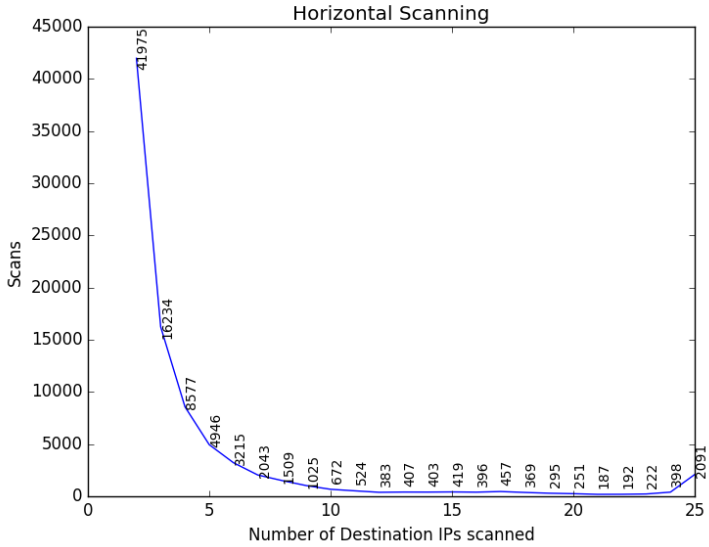
Evaluation

- Horizontal Scans in TCP Port Scans
- Used 2nd configuration
  (network telescope with honeypot)
- Behavior - Same as first configuration



Grouped by same /24 network

- Comparison to 1st Configuration
  - More number of scans at 2nd configuration
    (same /24 Network)
  - More number of scans at 1st onfiguration (same ISP)
  - Not easy to compare the behavior in terms of number of horizontal scans
  - But No Change in General Behavior



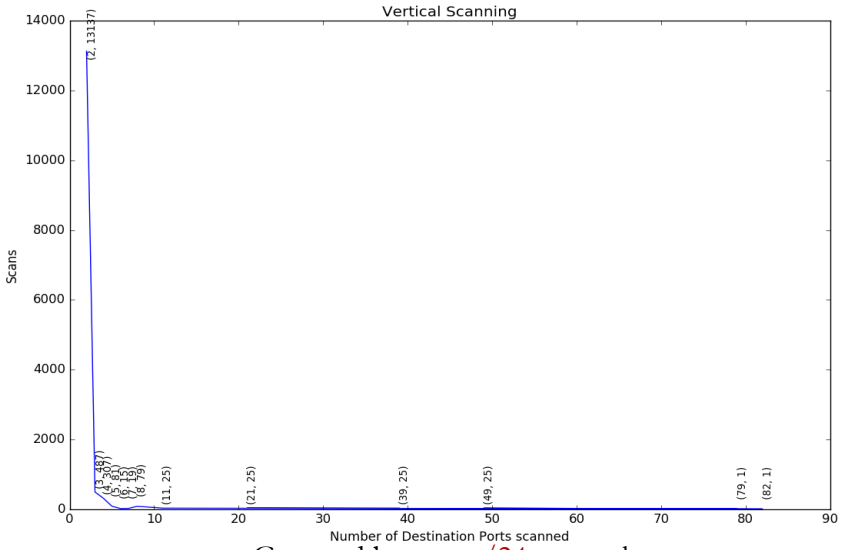
Grouped by same ISP

Evaluation

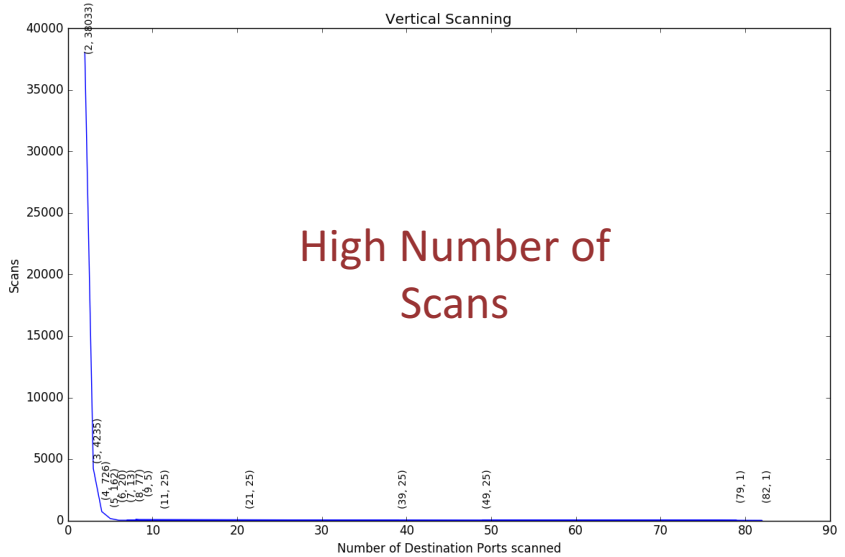
- Vertical Scans in TCP Port Scans
- Used 1st configuration
  (network telescope without honeypot)

- Behavior – Number of vertical scans keep reducing when scan size increases.

- Got 99% of scans before scan size 10
- Number of scans are same
  after scan size 10
  - From 4 class C networks
    - 185.40.4.0/24
    - 212.71.238.0/24
    - 183.3.227.0/24
    - 62.210.246.0/24
- Very few number of large scans



Grouped by same /24 network

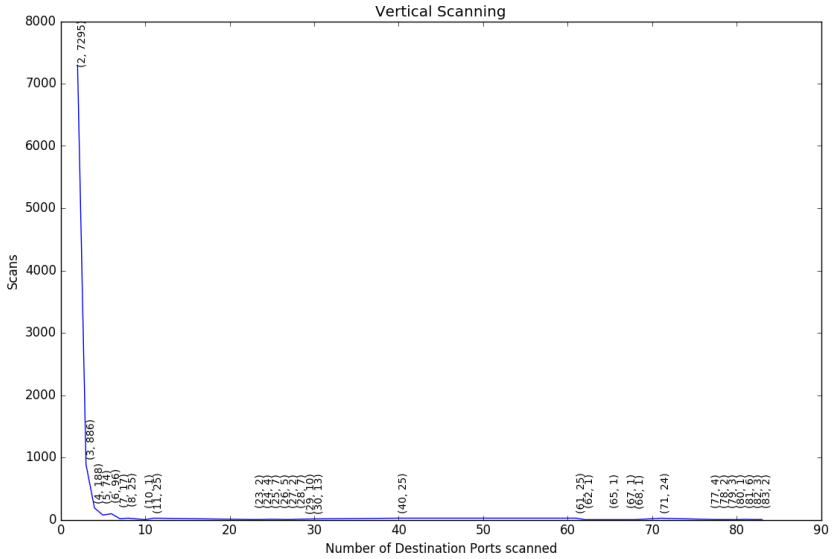


Grouped by same ISP

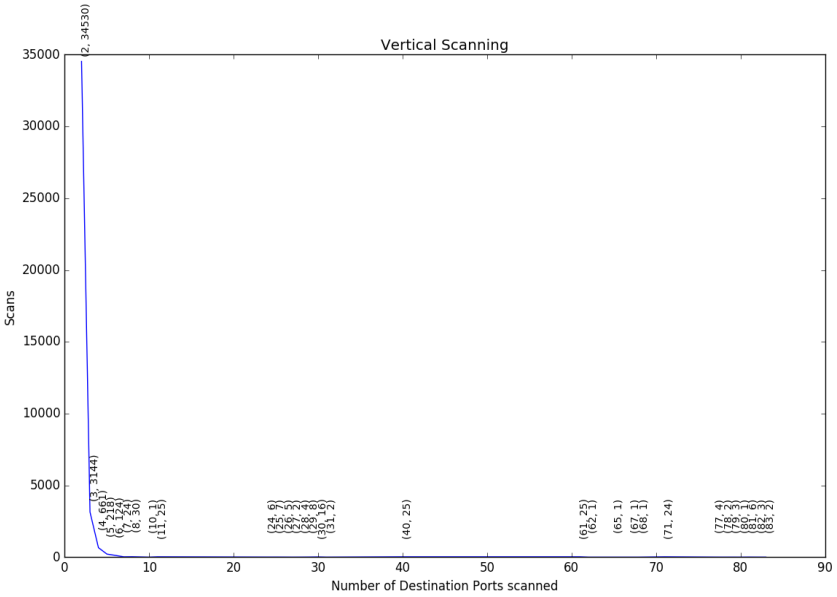
Evaluation

- Vertical Scans in TCP Port Scans
- Used 2nd configuration

  (network telescope with honeypot)
- Behavior - Same as 1st Configuration
- Number of scans are same after scan size 10
  - From 6 class C networks
    - 113.240.250.0/24 , 69.64.33.0/24
    - 222.186.34.0/24, 163.172.99.0/24
    - 193.138.215.0/24, 173.254.236.0/24
- Comparison to 1st Configuration
  - Number of large scans are high at 2nd configuration
  - But total number of scans less at 2nd configuration
  - No behavioral difference in terms of number of vertical scans



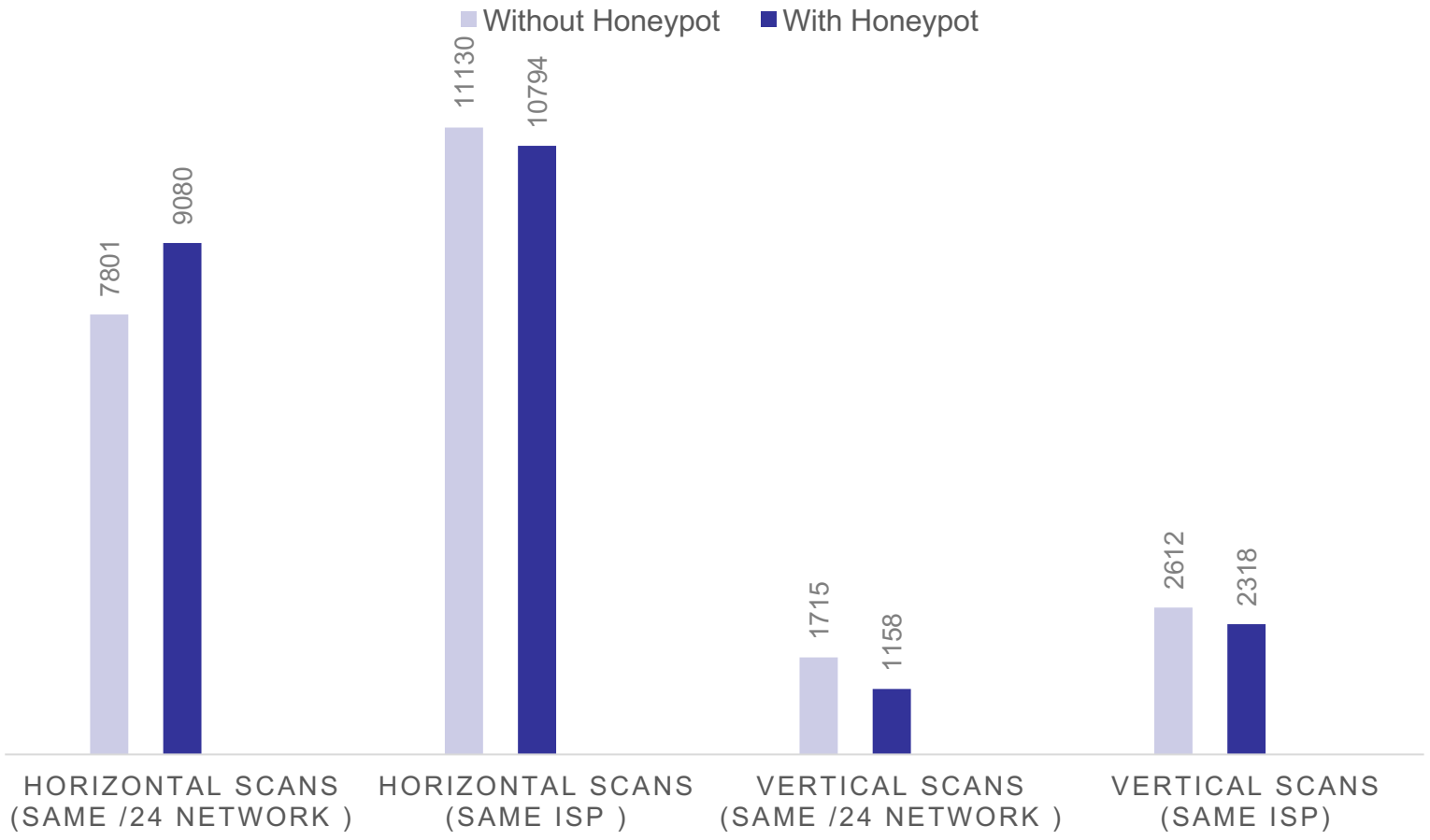
Grouped by same /24 network



Grouped by same ISP

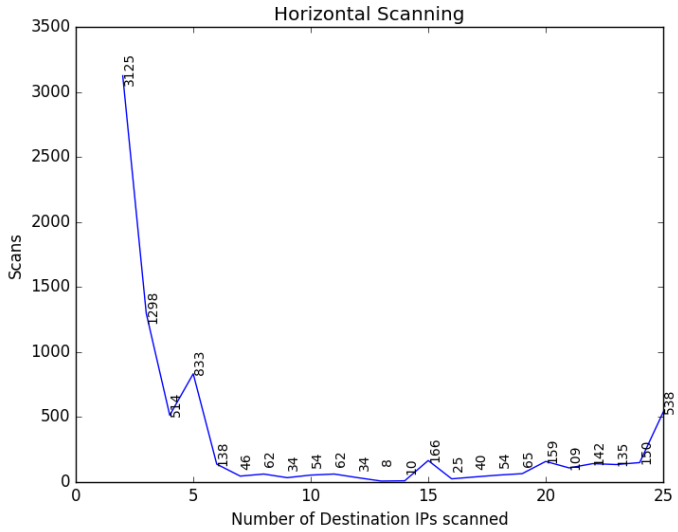
Evaluation

- Horizontal and Vertical Scans in UDP Port Scans



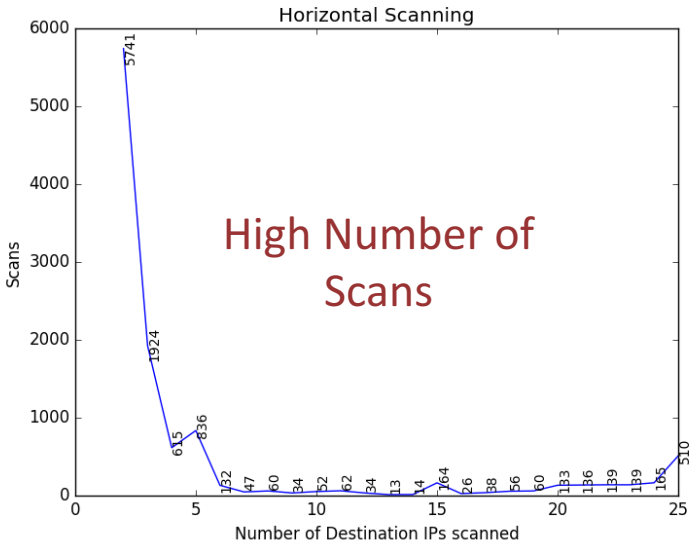
Evaluation

- Horizontal Scans in UDP Port Scans
- Used 1st configuration
  (network telescope without honeypot)



Grouped by same /24 network

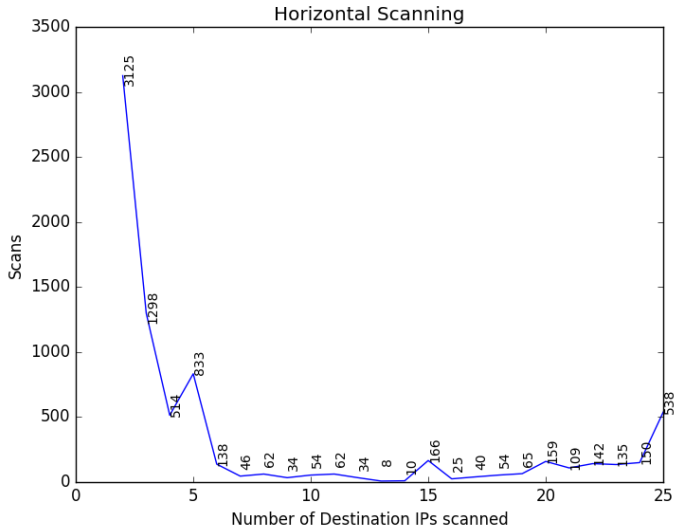
- Behavior - Number of horizontal scans keep reducing when scan size increases
- Number of UDP scans **less than** Number of TCP scans



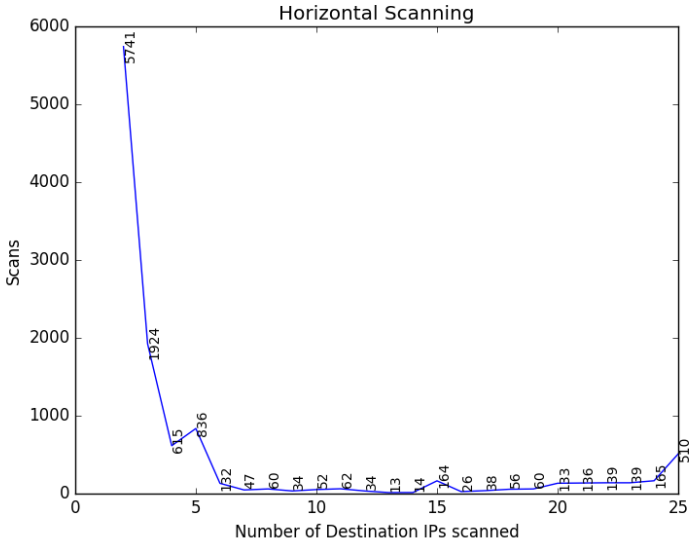
Grouped by same ISP

Evaluation

- Horizontal Scans in UDP Port Scans
- Used 2nd configuration
  (network telescope with honeypot)
- Behavior – Same as TCP horizontal scans behavior
- Number of UDP scans **less than** Number of TCP scans



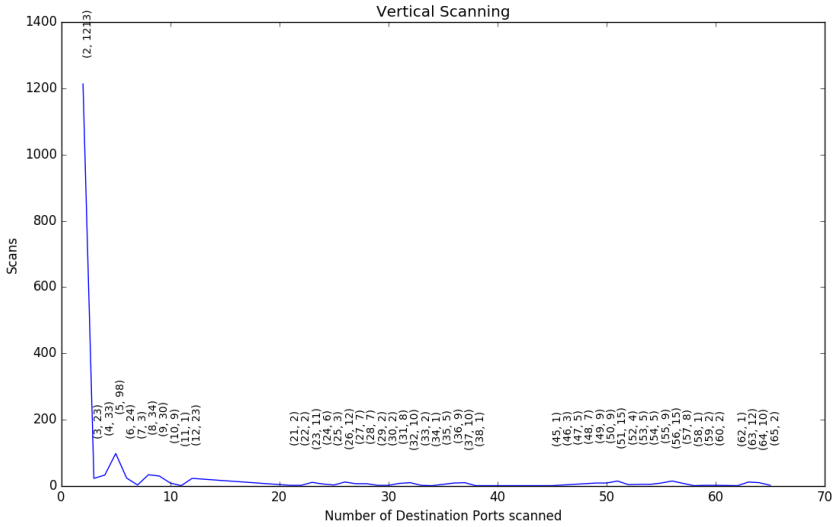
Grouped by same /24 network



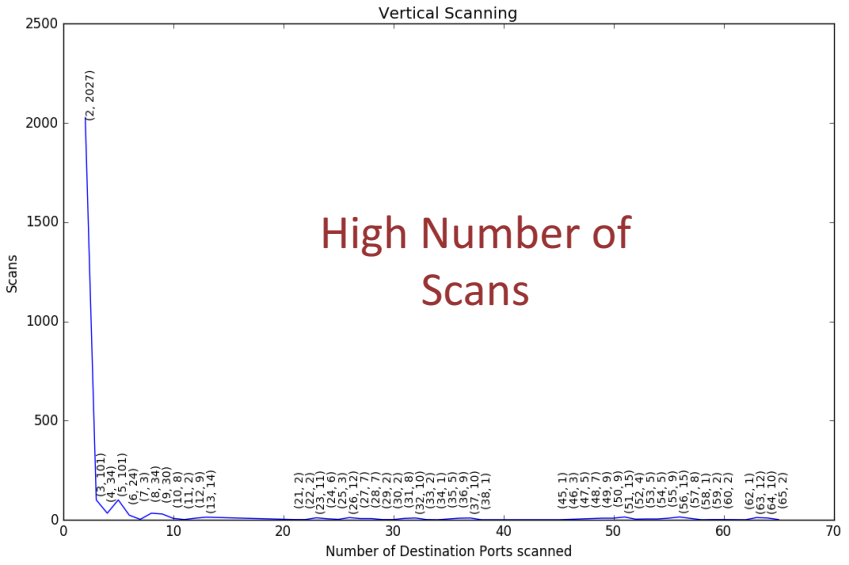
Grouped by same ISP

Evaluation

- Vertical Scans in UDP Port Scans
- Used 1st configuration
  (network telescope without honeypot)
- Behavior - Number of vertical scans keep reducing when scan size increases
- Got 87% of scans before scan size 10
- Number of scans are same after scan size 20
  - Originated from one /24 network
    104.193.11.0/24
- Source IPs performing large scans in TCP and UDP port scans are different
- Very few number of large scans



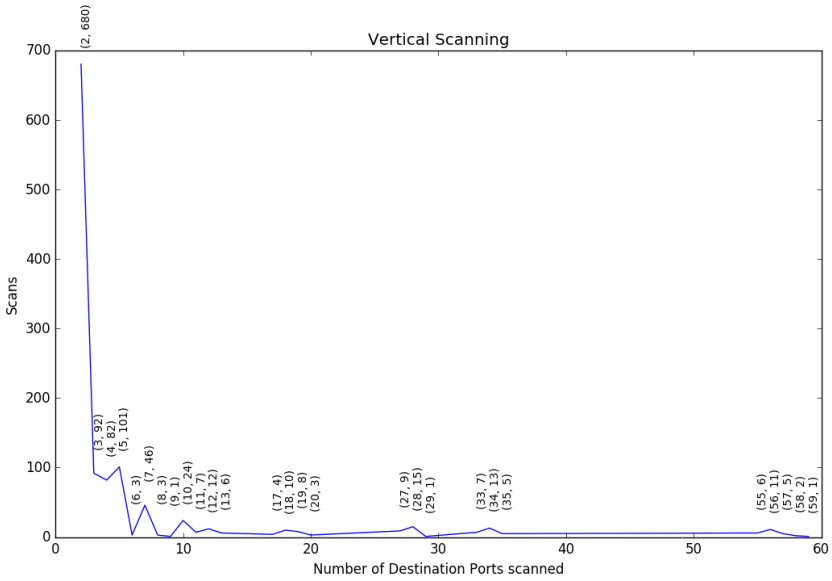
Grouped by same /24 network



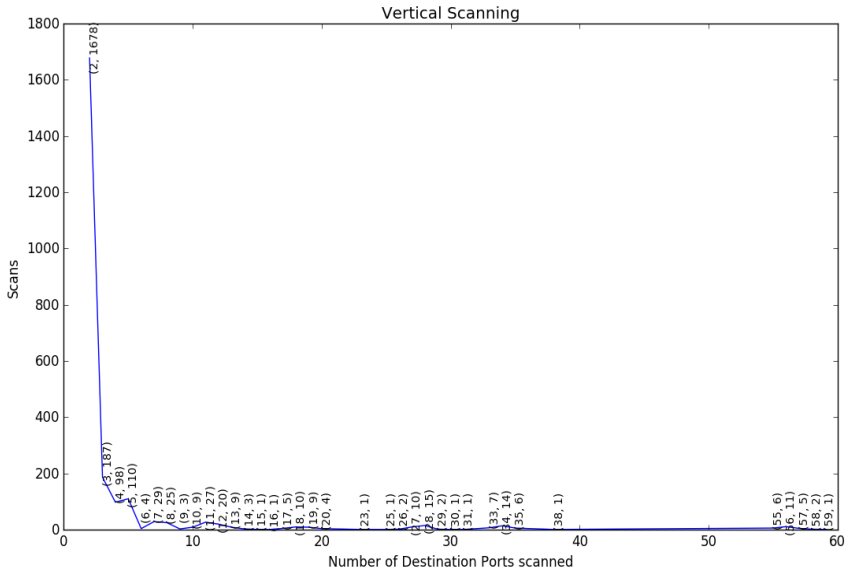
Grouped by same ISP

Evaluation

- Vertical Scans in UDP Port Scans
- Used 2nd configuration
  (network telescope with honeypot)
- Behavior – Similar to TCP vertical scans
- Got 89% of scans before scan size 10
- Source IPs performing large scans in TCP and UDP port scans are different
- Fewer number of large scans compared to 1st Configuration



Grouped by same /24 network

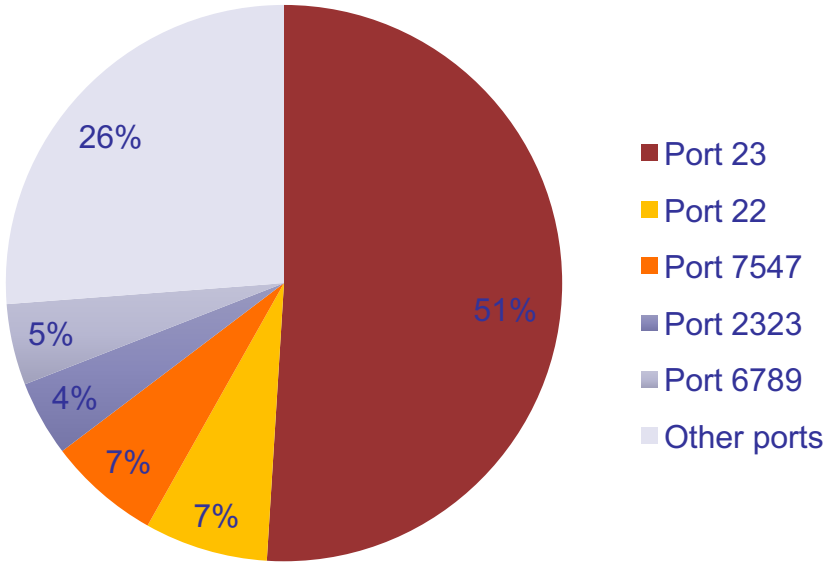


Grouped by same ISP

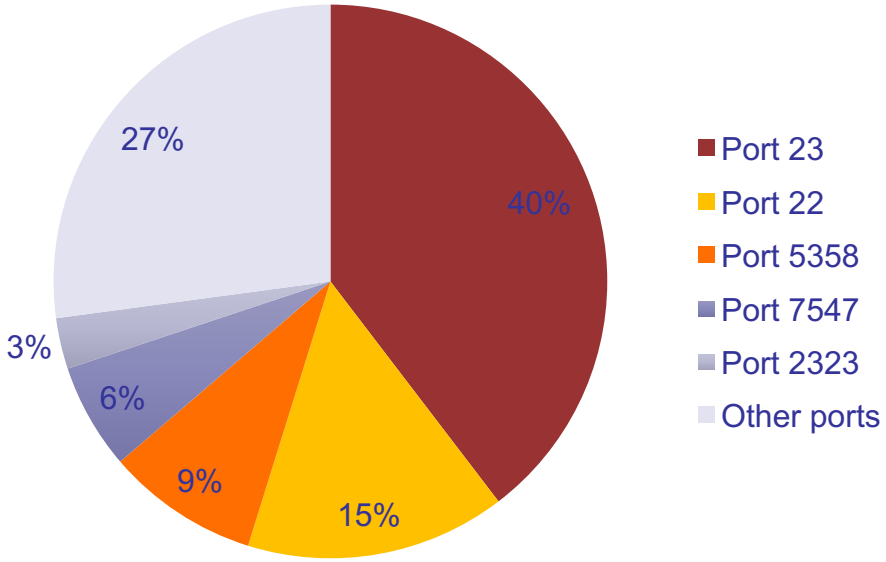
Evaluation

- Target Ports
  - Most targeted TCP ports in both configurations

Most actively scanned TCP ports (without honeypot)



Most actively scanned TCP ports (with honeypot)

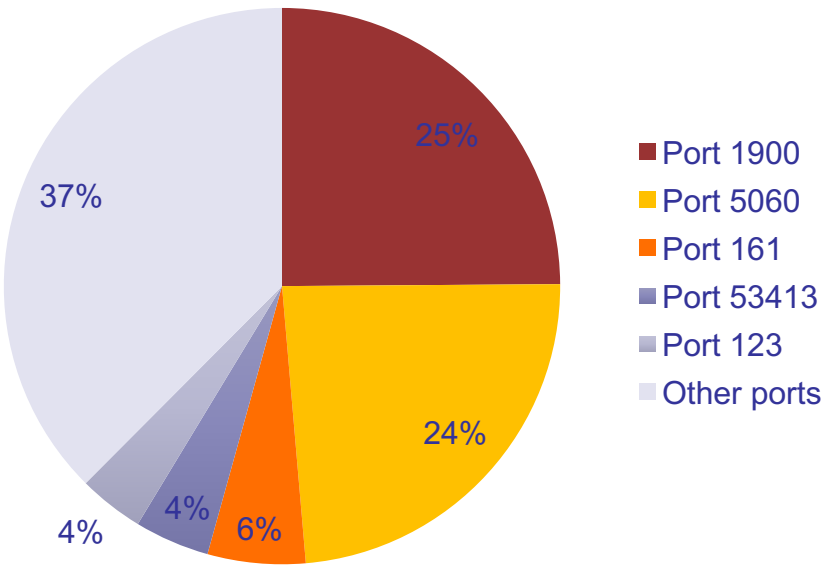


  - Similar ports in both configurations except one.

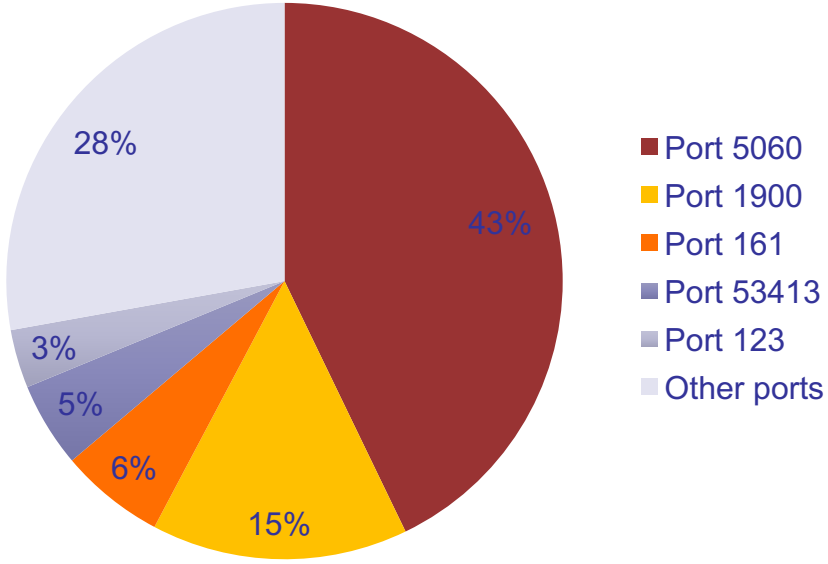
Evaluation

- Target Ports
  - Most targeted UDP ports in both configurations

Most actively scanned UDP ports (without honeypot)



Most actively scanned UDP ports (with honeypot)

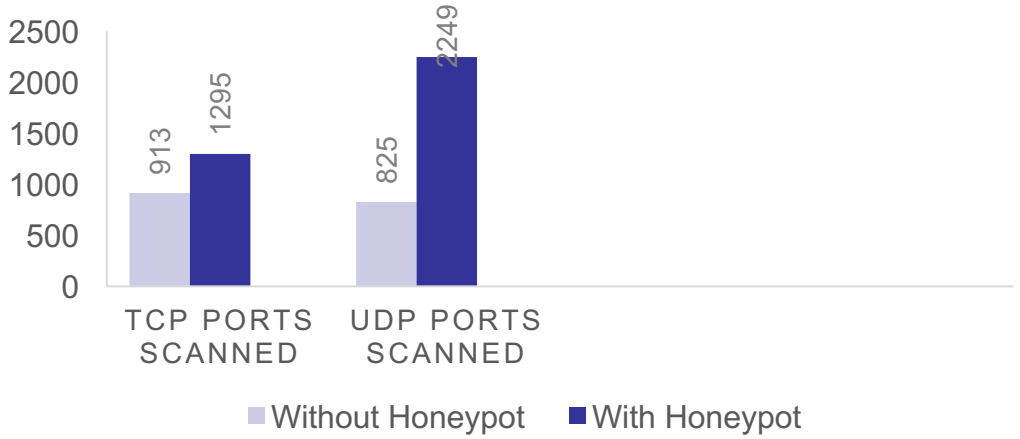


  - Similar ports in both Configurations

Evaluation

- Target Ports
  - Almost similar TCP ports scanned in both configurations
  - All UDP ports are same in both configurations
  - More no. of ports were scanned during 2nd phase (both TCP & UDP)
    - Large number of ports were scanned through vertical scans

      78% of total TCP ports, 70% of total UDP ports



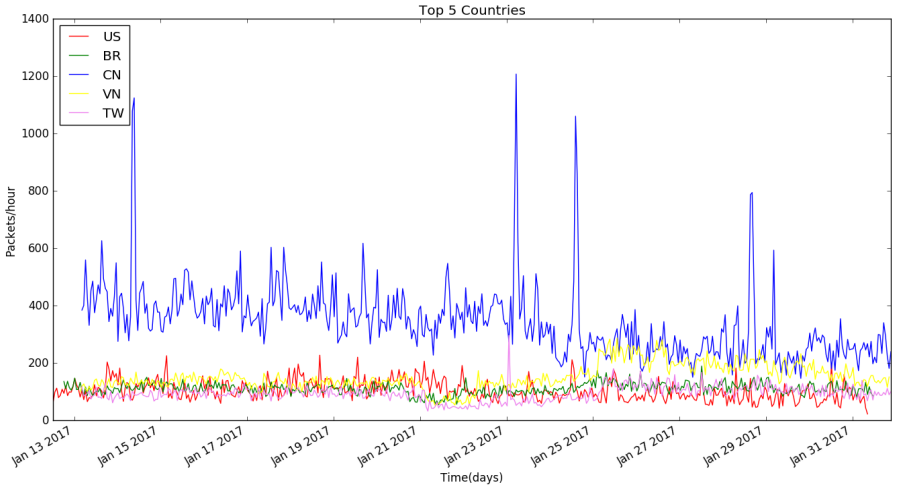
  - More than 55 % of scans targeted on port 23 and port 22 (TCP), port 5060 and port 1900 (UDP)

Evaluation

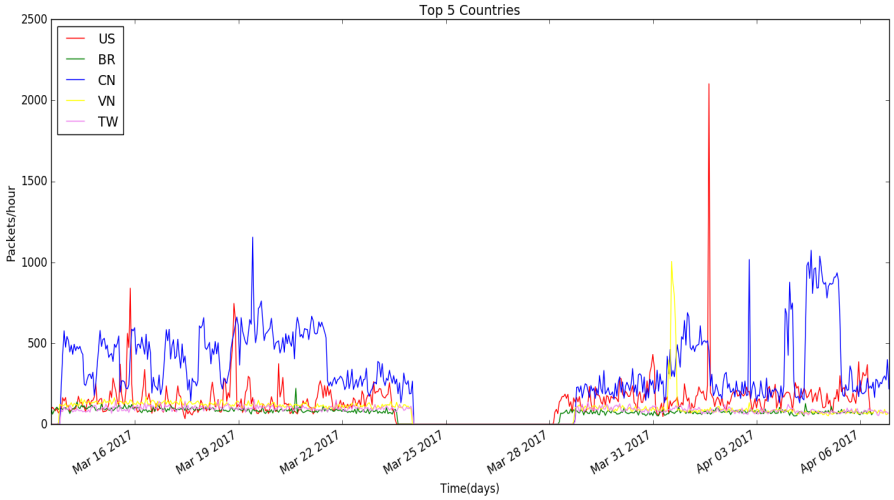
- Relationship between Traffic and Time of the Day
  - Time distribution of port scan traffic for top 5 countries
  - Considered TCP and UDP port scans separately
  - Based on local time of the source of port scans

Evaluation

- Relationship between Traffic and Time of the Day (TCP)



Traffic rate of top 5 countries participated in TCP port scan (without Honeypot)

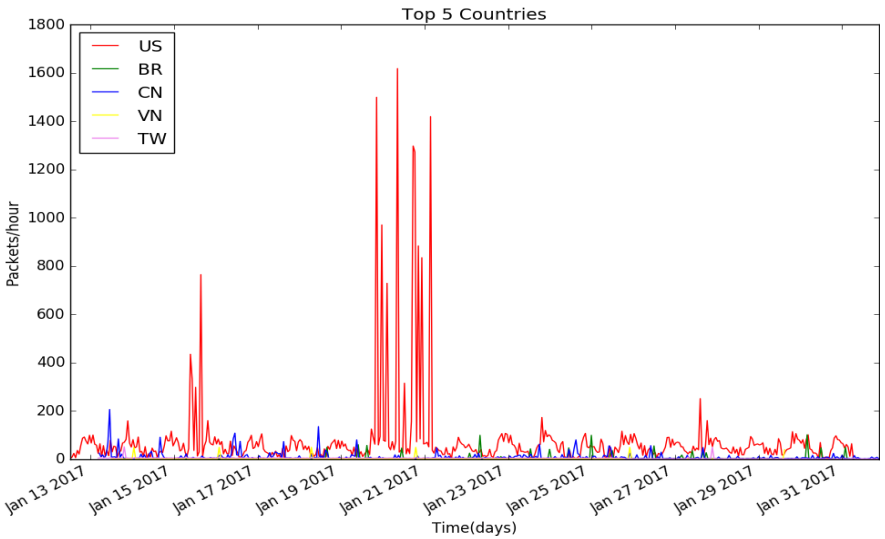


Traffic rate of top 5 countries participated in TCP port scan (with Honeypot)

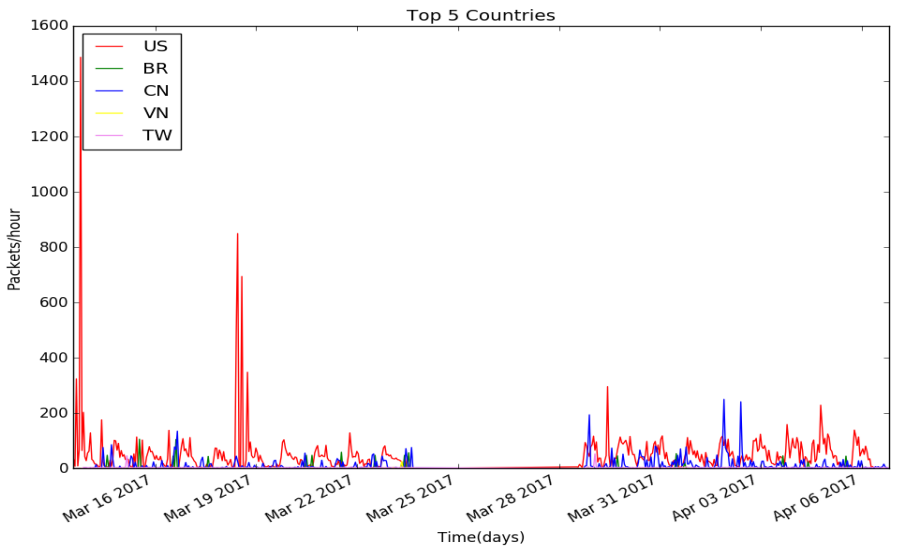
- Port scanning is a constant activity
- Top 5 countries – Same during both Configurations

Evaluation

- Relationship between Traffic and Time of the Day (UDP)



Traffic rate of top 5 countries participated in UDP port scan (without Honeypot)_

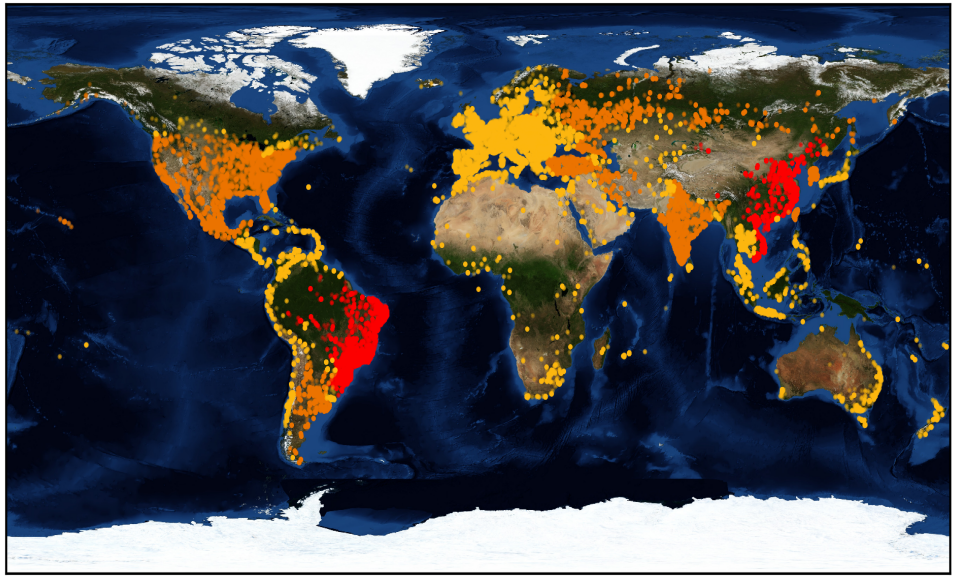


Traffic rate of top 5 countries participated in UDP port scan (with Honeypot)_

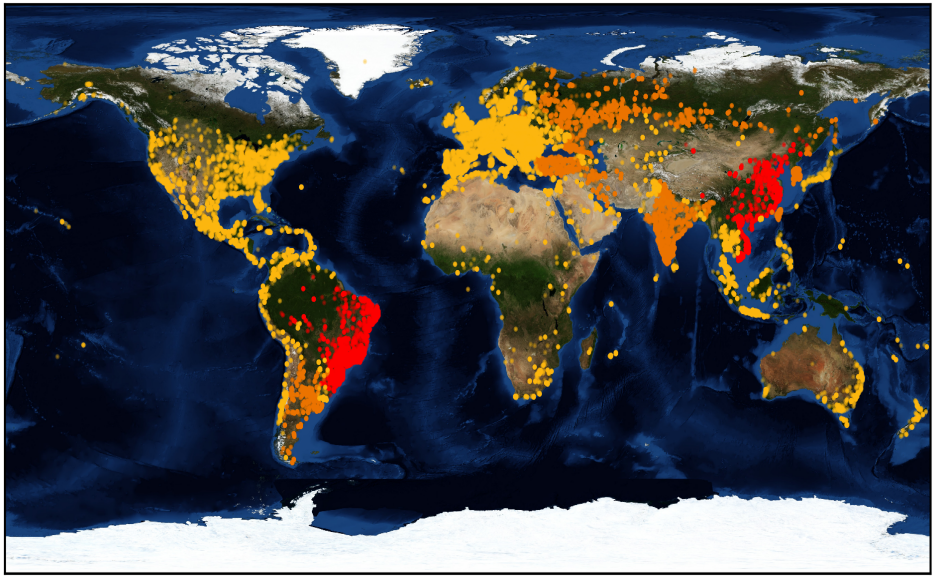
- Not frequent as TCP port scan activity
- No relation between traffic and time of the day
- Top 5 countries – Same during both Configurations

Evaluation

- Geographical Distribution of Port scan Sources
  - How port scans are geographically distributed?



Geographical Distribution of Port Scan Source IP Addresses
(NT without Honeypot)



Geographical Distribution of Port Scan Source IP Addresses
(NT with Honeypot)

  - Port scans are a global phenomena
  - Both heat maps show similar behavior

Conclusion

- What was done:
  - Analysed packets from network telescope to find pattern depending on behavior of port scanners.
  - Checked if behavior will change when network telescope combines with honeypot
  - Compared behavior of TCP and UDP port scans
- What was discovered
  - TCP SYN scan is more popular than other scans.
  - TCP port scans are greater than UDP port scans

Conclusion

- What was discovered (continuation)
  - Horizontal scans - Number of scans keep reducing when scan size increases
  - Vertical scans – Large amount of small scans, few number of large scans
  - No apparent difference in the behavior of horizontal and vertical scans between two configurations
  - Increase in number of ports (both TCP and UDP) scanned at 2nd configurations
  - Most actively scanned ports were similar at both stages
  - No relation between traffic rate and time of the day
  - Port scans are global phenomena