Design and Implementation of Real-time Visualization tool for Network Security Monitoring

Aneela Safdar
Supervisor : Dr. Hanif Durad
Co-Supervisor : M. Masoom Alam
DCIS PIEAS

Motivation

- To look what's going on in network with minimal or no effort.

- Information Visualization turns data into interactive graphical displays which are easy to look at and digest.

Motivation (cont.)

- IDS (Intrusion Detection System) records Attacks and generates log files.
- Instead of handing someone a log file that describes how an attack happened, one can use a picture, a visual representation of the log records.

Motivation (cont.)


```
":"root","command":"USER","arg":"root","reply_code":331,"reply_msg":"Password required for root"}
{"ts":"2016-09-01T06:37:19.145139Z","uid":"CYp0vlvcji8TPg61g","id.orig_h":"192.168.227.102","id.orig_p":36996,"id.resp_h":"192.168.227.101","id.resp_p":21,"user"
:"onion","command":"USER","arg":"onion","reply_code":331,"reply_msg":"Password required for onion"}
{"ts":"2016-09-01T06:37:19.272344Z","uid":"C4dK3L3WTDwNleNue7","id.orig_h":"192.168.227.102","id.orig_p":35522,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"user2","command":"USER","arg":"user2","reply_code":331,"reply_msg":"Password required for user2"}
{"ts":"2016-09-01T06:37:19.435372Z","uid":"CLztoEF6KzJ4VVP0c","id.orig_h":"192.168.227.102","id.orig_p":38069,"id.resp_h":"192.168.227.101","id.resp_p":21,"user"
:"life","command":"USER","arg":"life","reply_code":331,"reply_msg":"Password required for life"}
{"ts":"2016-09-01T06:37:19.621429Z","uid":"CNEbpC40iktCmGfaia","id.orig_h":"192.168.227.102","id.orig_p":36342,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"air","command":"USER","arg":"air","reply_code":331,"reply_msg":"Password required for air"}
{"ts":"2016-09-01T06:37:19.758975Z","uid":"CeOJdbNSSUNbdVre","id.orig_h":"192.168.227.102","id.orig_p":44482,"id.resp_h":"192.168.227.101","id.resp_p":21,"user":
"sound","command":"USER","arg":"sound","reply_code":331,"reply_msg":"Password required for sound"}
{"ts":"2016-09-01T06:37:19.848177Z","uid":"CsNvT54fLQWR9F1B","id.orig_h":"192.168.227.102","id.orig_p":42167,"id.resp_h":"192.168.227.101","id.resp_p":21,"user":
"white","command":"USER","arg":"white","reply_code":331,"reply_msg":"Password required for white"}
{"ts":"2016-09-01T06:37:19.960098Z","uid":"CifV1c2SJOkVXxmHcj","id.orig_h":"192.168.227.102","id.orig_p":45920,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"real","command":"USER","arg":"real","reply_code":331,"reply_msg":"Password required for real"}
{"ts":"2016-09-01T06:37:20.284007Z","uid":"C8AAb53VU1MBI4vg43","id.orig_h":"192.168.227.102","id.orig_p":41403,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"hard","command":"USER","arg":"hard","reply_code":331,"reply_msg":"Password required for hard"}
{"ts":"2016-09-01T06:37:20.375790Z","uid":"CFhbRx1GZaq0GRCMDl","id.orig_h":"192.168.227.102","id.orig_p":41528,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"ram","command":"USER","arg":"ram","reply_code":331,"reply_msg":"Password required for ram"}
{"ts":"2016-09-01T06:37:20.534482Z","uid":"CXUUFy2rkYym0VBRB1","id.orig_h":"192.168.227.102","id.orig_p":43388,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"rom","command":"USER","arg":"rom","reply_code":331,"reply_msg":"Password required for rom"}
{"ts":"2016-09-01T06:37:20.621972Z","uid":"CGHwKQ1WmKCDZHHvDh","id.orig_h":"192.168.227.102","id.orig_p":44015,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"clear","command":"USER","arg":"clear","reply_code":331,"reply_msg":"Password required for clear"}
{"ts":"2016-09-01T06:37:20.765545Z","uid":"Co6u1q3dh1UI9G7Qe4","id.orig_h":"192.168.227.102","id.orig_p":39669,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"tiny","command":"USER","arg":"tiny","reply_code":331,"reply_msg":"Password required for tiny"}
{"ts":"2016-09-01T06:37:20.954137Z","uid":"CllNgi1mqSEKk0B7vk","id.orig_h":"192.168.227.102","id.orig_p":35938,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"user2","command":"USER","arg":"user2","reply_code":331,"reply_msg":"Password required for user2"}
{"ts":"2016-09-01T06:37:21.023734Z","uid":"CHu0RN2rUpvBiXATGc","id.orig_h":"192.168.227.102","id.orig_p":44051,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"life","command":"USER","arg":"life","reply_code":331,"reply_msg":"Password required for life"}
{"ts":"2016-09-01T06:37:21.140792Z","uid":"Cnp5Ua4CE572f1O3z6","id.orig_h":"192.168.227.102","id.orig_p":39507,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"air","command":"USER","arg":"air","reply_code":331,"reply_msg":"Password required for air"}
{"ts":"2016-09-01T06:37:21.266597Z","uid":"CX9eK51FRFXbDYnj9f","id.orig_h":"192.168.227.102","id.orig_p":35945,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"sound","command":"USER","arg":"sound","reply_code":331,"reply_msg":"Password required for sound"}
{"ts":"2016-09-01T06:37:21.392930Z","uid":"CKC0GE3Ux2UXHIKoB9","id.orig_h":"192.168.227.102","id.orig_p":40279,"id.resp_h":"192.168.227.101","id.resp_p":21,"user
":"white","command":"USER","arg":"white","reply_code":331,"reply_msg":"Password required for white"}
{"ts":"2016-09-01T06:37:21.455168Z","uid":"CIjThrvpamhwhdT4b","id.orig_h":"192.168.227.102","id.orig_p":36757,"id.resp_h":"192.168.227.101","id.resp_p":21,"user"
```


Figure 01 : FTP Log file

Motivation (cont.)

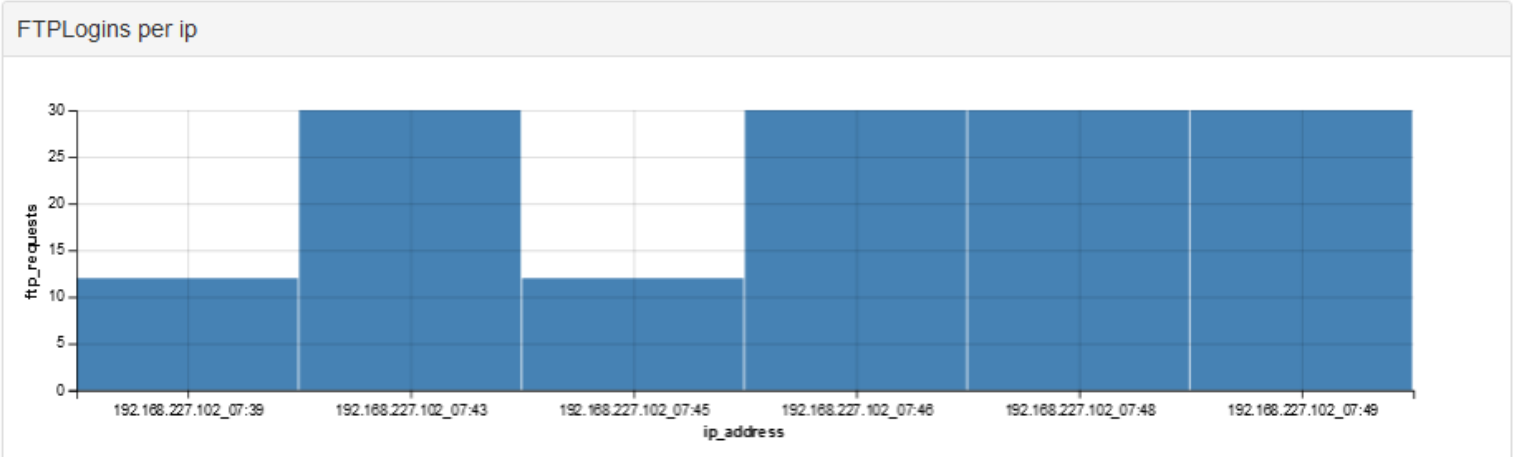


Figure 02 : Bar chart graph showing IPs involved in FTP traffic

Motivation (cont.)

- The main objective is to create a Real-time Visualization tool for Network Security Monitoring using open-source softwares/tools only.
- To look for Near Miss Events
  - Those which could lead to fatal conditions but never happened for some reason or other.

Thesis Dissection – NSM Cycle

WSO2 - Web Services Oxygen (O2)

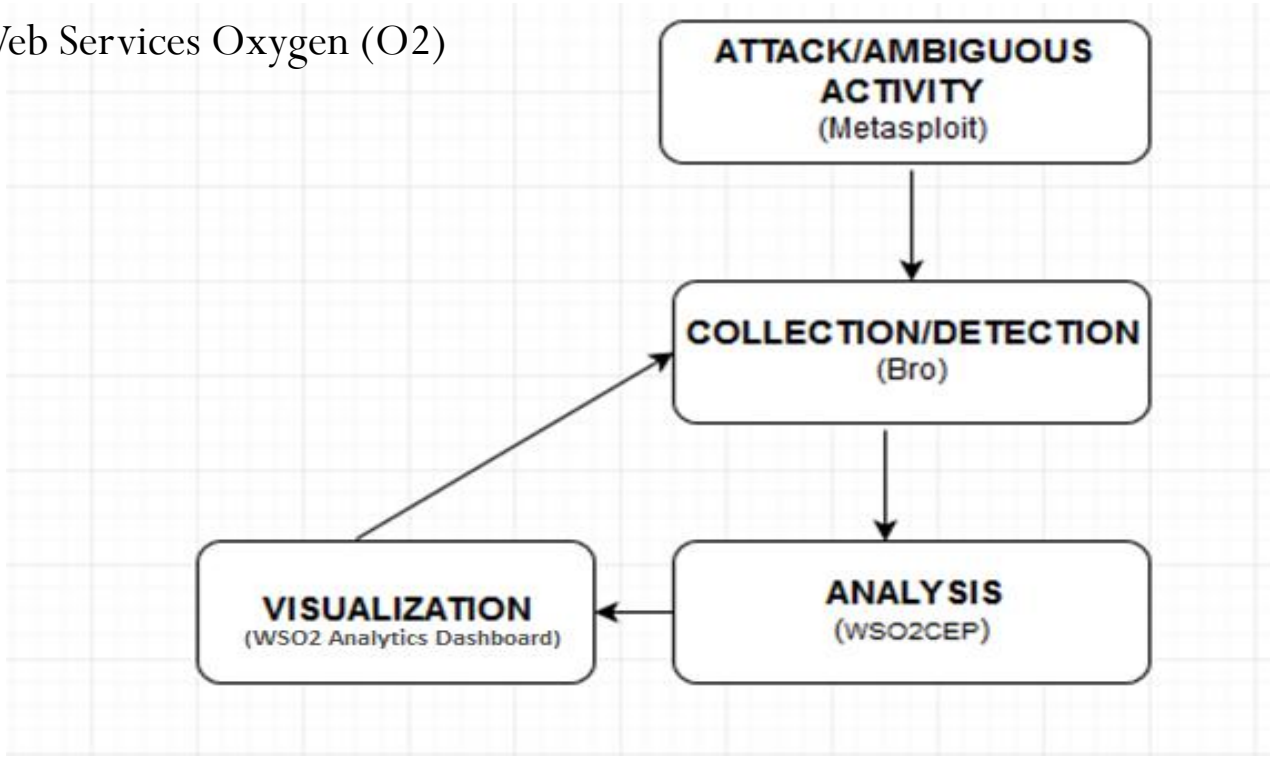


Figure 03 : Elements of of Real-time Visualization tool for Network Security Monitoring

Thesis Dissection (cont.)

- Attack / Pen Testing
- Data Collection
- Analysis
- Visualization
- (Notification)

Attack/Pen Testing (Data Generation)

- In order to follow stated steps, there must be some interesting facts/data to be collected, detected, analyzed and then finally viewed.
- There is no term such as 100% security.
- Defenders would like to look for all but Attacker is interested in just one vulnerability.
- Thread Modeling is inescapable.

Metasploit Framework

- Utilize world's largest exploit database
- Simulate real-world attacks against your defenses
- Testing across the network
- Ruby Framework
- Cross Platform

- Download Link
  - https://www.kali.org/downloads/

Metasploit (cont.)

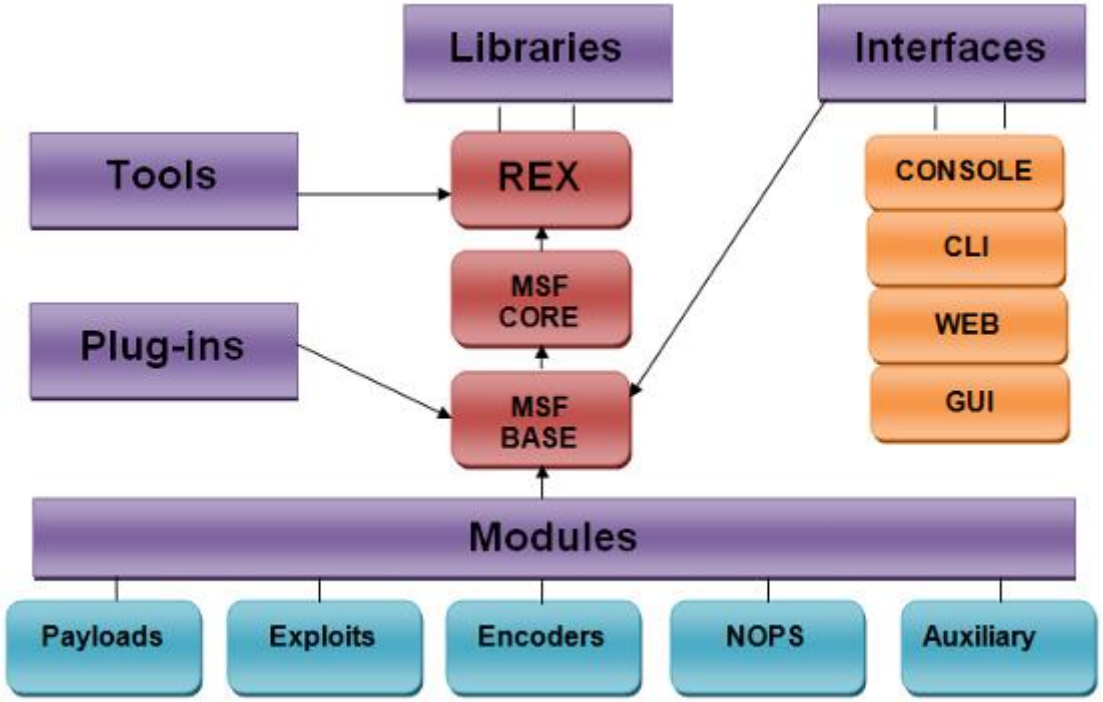


Figure 04 : Architecture of Metasploit [1]

Metaploit (cont.)

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
[*] Nmap: Nmap scan report for 192.168.227.101
[*] Nmap: Host is up (0.0019s latency).
[*] Nmap: Not shown: 989 closed ports
[*] Nmap: PORT     STATE SERVICE       VERSION
[*] Nmap: 21/tcp   open  ftp           ProFTPD 1.3.5rc3
[*] Nmap: |_ftp-anon: ERROR: Script execution failed (use -d to debug)
[*] Nmap: |_ftp-bounce: no banner
[*] Nmap: 22/tcp   open  ssh           OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
[*] Nmap: 25/tcp   open  smtp          Postfix smtpd
[*] Nmap: |_smtp-commands: Couldn't establish connection on port 25
[*] Nmap: 139/tcp  open  netbios-ssn?
[*] Nmap: 443/tcp  open  https?
[*] Nmap: 445/tcp  open  microsoft-ds?
[*] Nmap: 512/tcp  open  exec          netkit-rsh rexecd
[*] Nmap: 513/tcp  open  login?
[*] Nmap: 514/tcp  open  shell?
[*] Nmap: 3306/tcp open  mysql         MySQL 5.5.47-0ubuntu0.14.04.1
[*] Nmap: 9876/tcp open  sd?
[*] Nmap: MAC Address: 08:00:27:11:05:72 (Oracle VirtualBox virtual NIC)
[*] Nmap: OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
[*] Nmap: No OS matches for host
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Service Info: Host:  aneela-VirtualBox; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   1.89 ms 192.168.227.101
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 382.13 seconds
msf > services 192.168.227.101
```

Figure 05 : Scan using NMAP command

Metaploit (cont.)

```
root@kali: ~
File  Edit  View  Search  Terminal  Help

[*] 192.168.227.101:21 - Starting FTP login sweep
[-] 192.168.227.101:21 FTP - LOGIN FAILED: root:root123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: onion:onion123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: aneela:aneela123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: user:user123 (Incorrect: )
[+] 192.168.227.101:21 - LOGIN SUCCESSFUL: aneela:onion123
[-] 192.168.227.101:21 FTP - LOGIN FAILED: kali:kali123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: neeli:neeli123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: user1:user1123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: user2:user2123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: life:life123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: air:air123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: sound:sound123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: white:white123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: real:real123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: hard:hard123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: ram:ram123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: rom:rom123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: clear:clear123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: tiny:tiny123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: pass:pass123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: black:black123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: rude:rude123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: gray:gray123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: gamble:gamble123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: snow:snow123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: read:read123 (Incorrect: )
[-] 192.168.227.101:21 FTP - LOGIN FAILED: fast:fast123 (Incorrect: )
```

Figure 06 : FTP Brute Force Exploit

Metaploit (cont.)

```
msf auxiliary(ssh_login) > run

[*] 172.30.26.160:22 SSH - Starting bruteforce
[-] 172.30.26.160:22 SSH - Failed: 'root:root123'
[-] 172.30.26.160:22 SSH - Failed: 'onion:onion123'
[-] 172.30.26.160:22 SSH - Failed: 'aneela:aneela123'
[-] 172.30.26.160:22 SSH - Failed: 'user:user123'
[+] 172.30.26.160:22 SSH - Success: 'aneela:onion123' 'uid=1000(aneela) gid=1000(aneela) groups=1000(aneela),4(adm),24(cdrom),27(sudo),30(dip),46(plug
dev),108(lpadmin),124(sambashare) Linux aneela-VirtualBox 3.19.0-51-generic #58~14.04.1-Ubuntu SMP Fri Feb 26 22:02:58 UTC 2016 x86_64 x86_64 x86_64 G
NU/Linux '
[*] Command shell session 2 opened (10.0.3.15:33873 -> 172.30.26.160:22) at 2016-05-08 14:30:47 +0530
[-] 172.30.26.160:22 SSH - Failed: 'kali:kali123'
[-] 172.30.26.160:22 SSH - Failed: 'neeli:neeli123'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssh_login) >
```

Figure 07 : SSH Brute Force Exploit

Data Collection

- Data Collection is said to be the most important part of Network Security Monitoring process.
- The size of data collected matters a lot.
  - Having an overabundance of data that may not be relevant to realistic organizational threats is fast way to increase complexity.

Intrusion Detection System

- Detects intrusion or others anomalies and records related information in logs.
- Host based IDS and Network based IDS
- Commercial IDS are very expensive.

- Snort, Suricata and Bro – open-source

Comparison among IDSs

- Snort is a single-threaded and an immensely well tuned.
- Suricata makes use of Snort rule-set, in addition to other supporting products along with multi-threading.
- Bro provides additional features via its script-based analysis engine and ability to extend the response through scripts. [2]

BRO

- Bro as developed within universities, remains acceptable for high throughput research environments.
- The research-driven culture in universities provides the resources required to use full power of Bro as well as its robust scripting features.

- Download Link
  - https://github.com/Security-Onion-Solutions/security-onion/blob/master/Verify_ISO.md

BRO (cont.)

- Bro is often the best option for more critical tasks
  - Higher-level protocol knowledge
  - Working across multiple network flows
  - Using a custom algorithm to compute something about the traffic in question.
- One of the distinctive aspects of Bro is its categorization of logs.
- Bro generates several notices based on the customized or default scripting (Detection)

Data Analysis

- This is the most difficult and time consuming phase of NSM as the result of overall monitoring depends upon the success of this very process.
- The term Event processing is a phenomenon of tracking and analyzing streams of information about things that have occurred, known as events, and deriving a deduction from them.

Complex Event Processors - Storm

- Storm is a free and open source real-time computation system.
- It is effortless, can be integrated with any programming language and very easy to use.
- It also easily integrates with queuing and database technologies which are already known to us.

Complex Event Processors – Esper

- It is also an open source distributed event correlation and event series analysis engine for Java.
- It provides a rich Event Processing Language (EPL) to perform filtering, aggregation and joins over sliding windows of various event series.

Complex Event Processors – WSO2CEP

- It is very lightweight and easy-to-use open-source Complex Event Processing server.
- It is built for extremely high performance with WSO2 Siddhi and also scalable using Apache Storm.
- Databases - IBM, Derby, Microsoft SQL, MYSQL, Oracle and more.[3]

- Download Link
  - http://wso2.com/products/complex-event-processor/

WSO2CEP

- **Event Receiver** receives events coming to the CEP.
- **Event Stream** consists of unique sets of specific types of attributes.
- **Event Processors** perform actual event processing.
- **Event Publisher** publishes events to the external systems.

WSO2CEP (cont.)

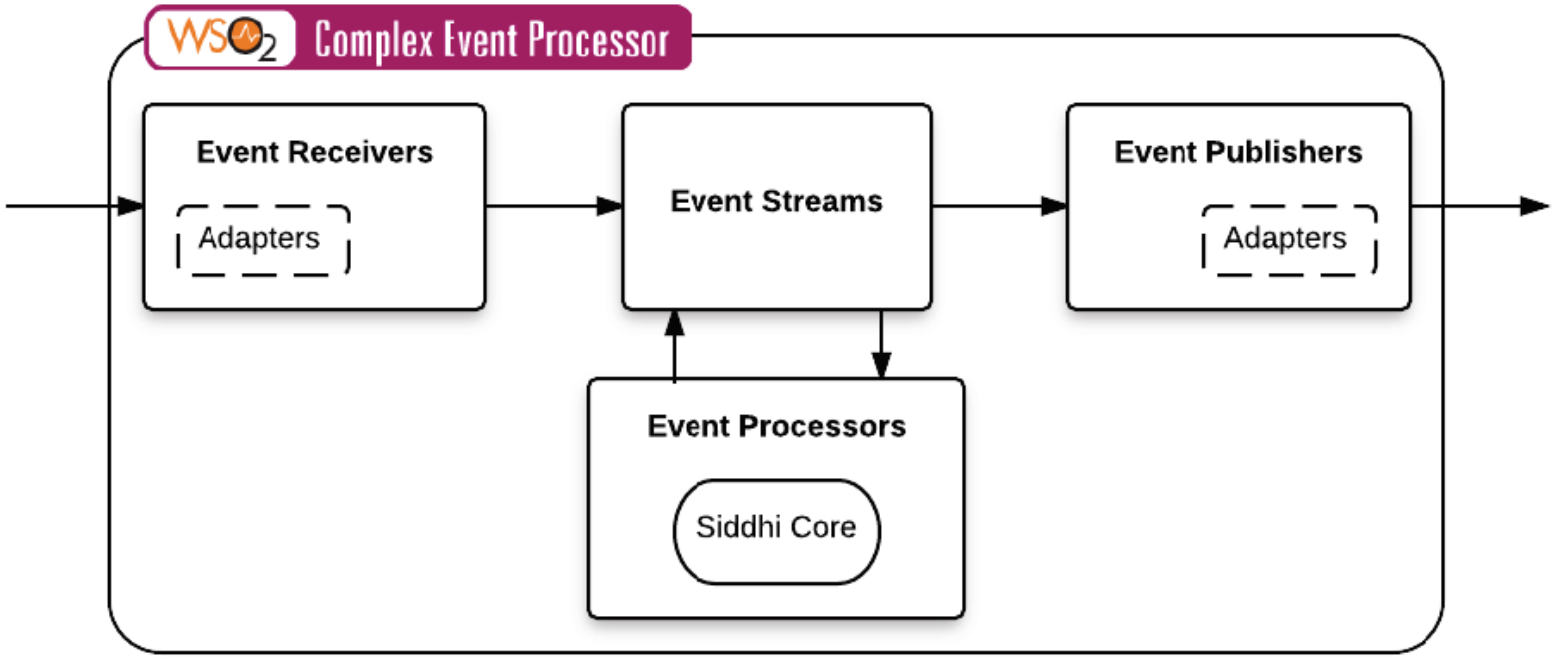


Figure 08 : Components of WSO2 CEP [3]

Siddhi Queries

- Siddhi query describes how to fuse existing event streams to create and populate new ones.
- It processes incoming event streams as specified by the queries, they generate new output event streams if they don't exist already.

Siddhi Queries (cont.)

```
@Plan:name('MAINExecutionPlan')

/* Enter a unique description for ExecutionPlan */
-- @Plan:description('ExecutionPlan')

/* define streams/tables and write queries here ... */

@Import('MAINInStream:1.0.0')
define stream MAINInStream (ts string, uid string, id_orig_h string, id_orig_p int, id_resp_h string, id_resp_p int, proto string, service string, duration double, orig_bytes long, resp_bytes long, conn_state string, local_orig bool, local_resp bool, missed_byte

@Export('PortScatterStream:1.0.0')
define stream PortScatterStream (src_ip string, src_port int, dest_ip string, dest_port int, protocol string);

@Export('ProtocolPieStream:1.0.0')
define stream ProtocolPieStream (protocol string, count long, total long, percentage float);

@from(eventtable = 'rdbms' , datasource.name = 'WSO2_CARBON_DB' , table.name ='conn_record_count')
define table conn_record_count (day_timestamp long, total_records long);

@from(eventtable = 'rdbms' , datasource.name = 'WSO2_CARBON_DB' , table.name ='conn_records')
define table conn_records (timestamp long, protocol string, id_orig_h string, id_orig_p int, id_resp_h string, id_resp_p int, proto string);

from MAINInStream
select
    time:timestampInMilliseconds(time:dateAdd(str:replaceAll(ts,'T',' '), 5, 'hour','yyyy-MM-dd HH:mm:ss'),'yyyy-MM-dd') as timestamp,
    (ifThenElse(id_resp_p == 21,'FTP', ifThenElse(id_resp_p == 22,'SSH', ifThenElse(id_resp_p == 25,'SMTP', ifThenElse(id_resp_p == 445,'SMB', ifThenElse(id_resp_p == 3306,'MYSQL','OTHER'))))))  as protocol,
    id_orig_h, id_orig_p, id_resp_h, id_resp_p, proto
insert into intermediateStream;

from intermediateStream
select *
insert into conn_records;

from intermediateStream
select timestamp as day_timestamp, count() as total_records
insert overwrite conn_record_count
on conn_record_count.day_timestamp == day_timestamp;

from intermediateStream
delete conn_record_count
on conn_record_count.day_timestamp != timestamp;

from intermediateStream#window.externalTimeBatch(timestamp, 1 day, timestamp, 2 min)
select protocol, count() as protocol_count
group by protocol
insert into protocolCountStream;

from protocolCountStream as pcs join conn_record_count as ct
select pcs.protocol as protocol, pcs.protocol_count as count, ct.total_records as total, cast(cast(pcs.protocol_count,'float')/cast(ct.total_records, 'float') *100, 'float') as percentage
insert into ProtocolPieStream;

from intermediateStream#window.externalTime(timestamp, 1 day)
select time:dateFormat(timestamp, 'yyyy-MM-dd HH:mm' ) as timestamp, protocol,id_orig_h, id_orig_p, id_resp_h, id_resp_p, proto
insert into PortDataOfDayStream;

from PortDataOfDayStream
select id_orig_h as src_ip, id_orig_p as src_port, id_resp_h as dest_ip, id_resp_p as dest_port, protocol
insert into PortScatterStream
```

Figure 09 : Siddhi Query

Data Visualization

- There is no need to pay heed towards collection, detection or analysis of data if one is not able to see it.
- This is the last phase of NSM cycle usually and can be tuned to customization as much as requirement will elicit.

Data Visualization (cont.)

- There are variety of visualization techniques that can be exercised like;
  - Histograms
  - Pie charts
  - Scatter plots
  - Parallel coordinates
  - Link graphs
  - Maps

Open-Source Visualization Tools

- Gnuplot
- Google Charts
- AfterGlow and so on

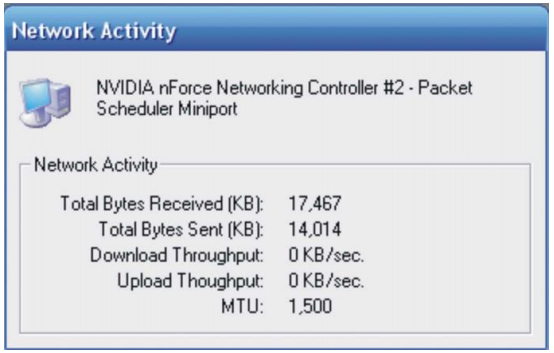
WSO2CEP Analytics Dashboard

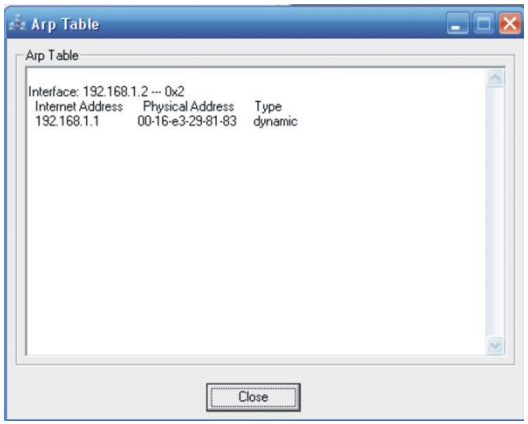
- It generates scatter plots, table charts, Geo map, Line chars, Number charts, Choropleth map and more
- As data arrive in real time, graphs are keep on updating.

Related Work

- Asiwe et al [4] – A NSM tool for simple tasks of monitoring as well as packet capturing.
  - Alerts via Yahoo Mail
  - Suite of network monitoring tools under a single GUI
  - Various forms like login form, network activity form, the ARP form

Related Work (cont.)





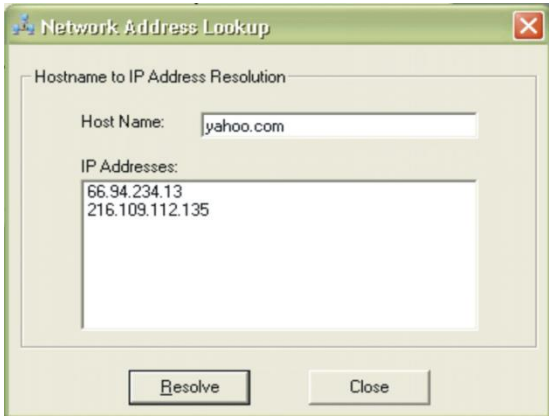


Figure 10 : Login , Network Activity, ARP table, Address Lookup Form

Related Work (cont.)

- Matogoro et al [5] - NMS in order to assist network administrators of Dodoma University Network.
  - *Nagios* is chosen to check operational status of network devices
  - *Cacti* for bandwidth management monitoring
  - *SmokePing* has been used for measurement of latency and packet loss

Related Work (cont.)

Figure 11 : Bandwidth Usage

Related Work (cont.)

- Hao et al. [6] - web based visualization system for network security.
  - Focus not on security data but on analysts
  - 2D visualization
  - Web-based charts

Related Work (cont.)

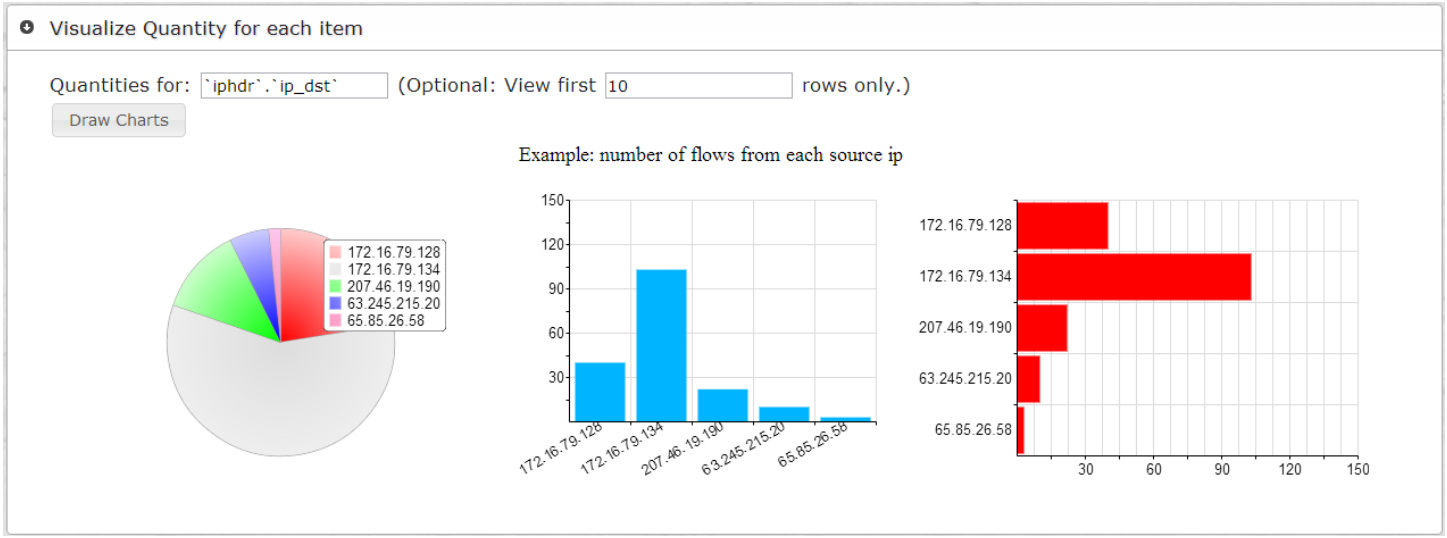


Figure 12 : Pie and Bar chart, analysis of proportion

Implementation Architecture

- Three kinds of Virtual Machines
  - Attackers (kali-Linux)
  - Target, Monitored Machines (security onion - Linux)
  - Monitoring Server (windows7-Microsoft Windows)

Implementation Methodology

- Exploited all open services in target, look NMAP results, Figure 05
  - FTP
  - SSH
  - SMTP
  - SMB
  - MYSQL

Implementation Methodology – Step by Step

- Metasploit (Attacker machines) attacks target machines.
- Bro (monitored machines) collects data and record in form of individual log files.
- A Java program (monitored machines) monitors log directory and all its files sending each file data to respective receivers in monitoring server.
- Receivers (monitoring server) takes data and forward to corresponding streams.

Implementation Methodology – Step by Step

- Execution plans (monitoring server) working in parallel on respective streams, process data and send the results to output streams.
- Each output stream (monitoring server) is registered with corresponding event publisher which puts data to display.

FTP Event Flow and Execution Flow

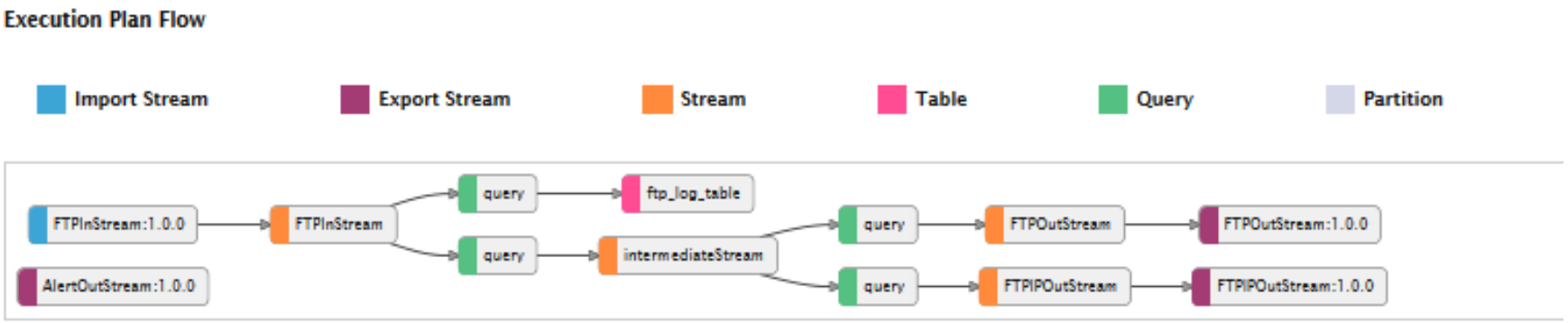


Figure 13 : FTP Event and Execution Flow

SSH Event Flow and Execution Flow

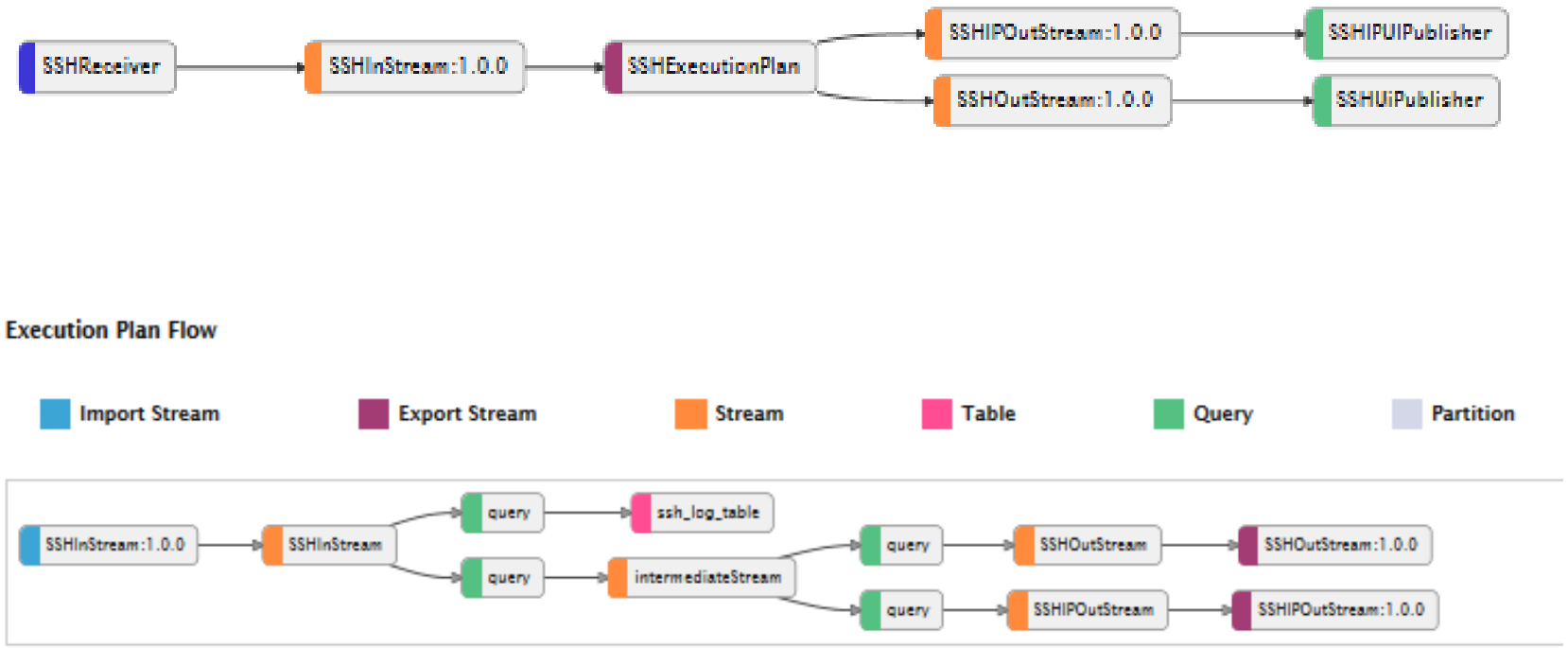


Figure 14 : SSH Event and Execution Flow

SMTP Event Flow and Execution Flow

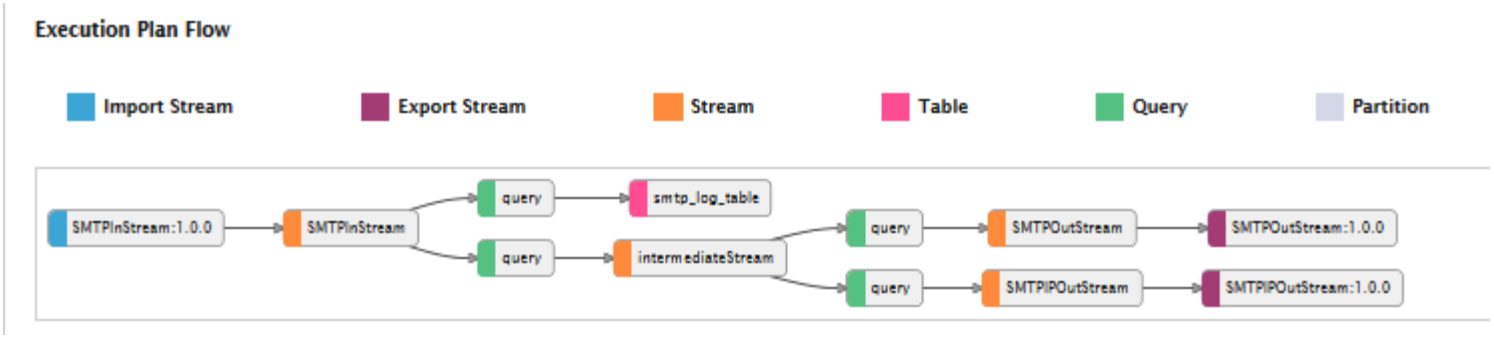
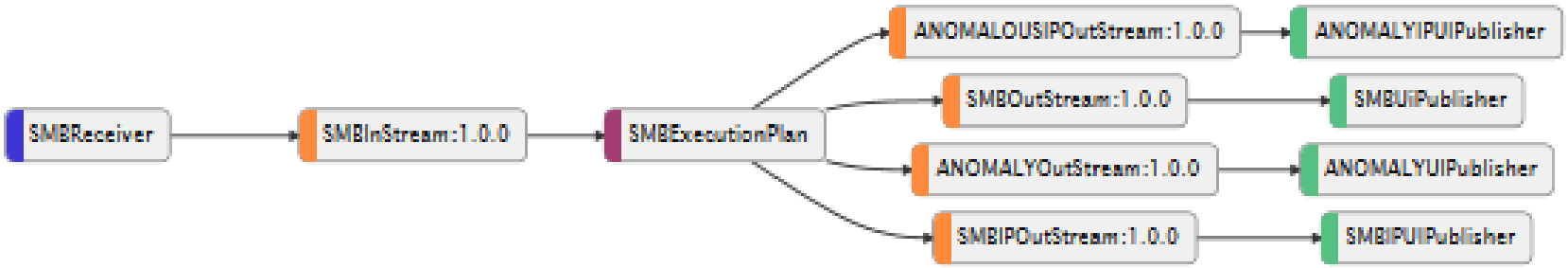


Figure 15: SMTP Event and Execution Flow

SMB Event Flow and Execution Flow



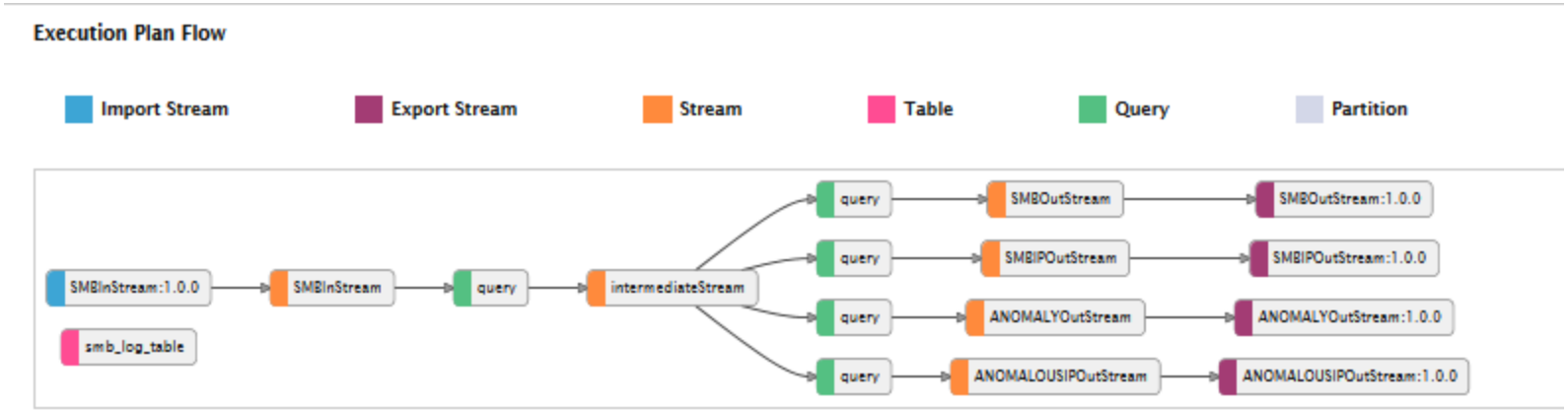


Figure 16 : SMB Event and Execution Flow

MYSQL Event Flow and Execution Flow

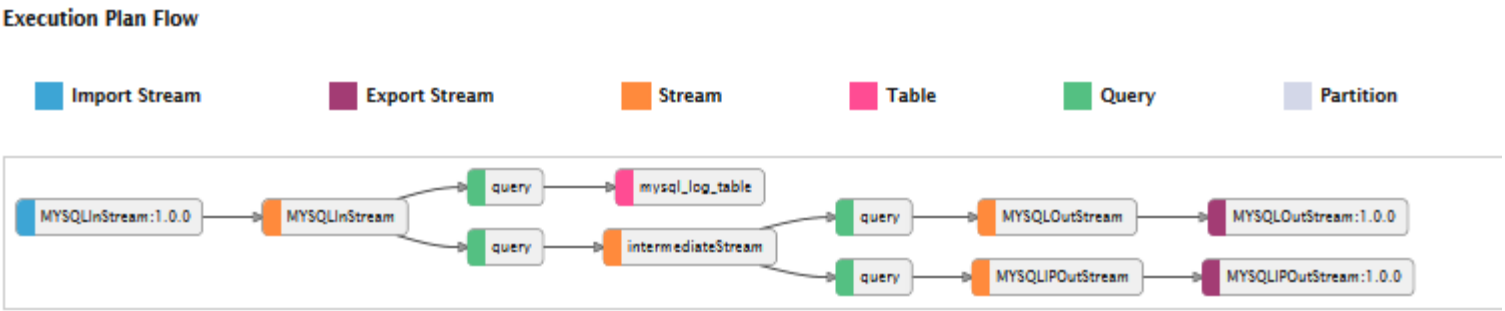
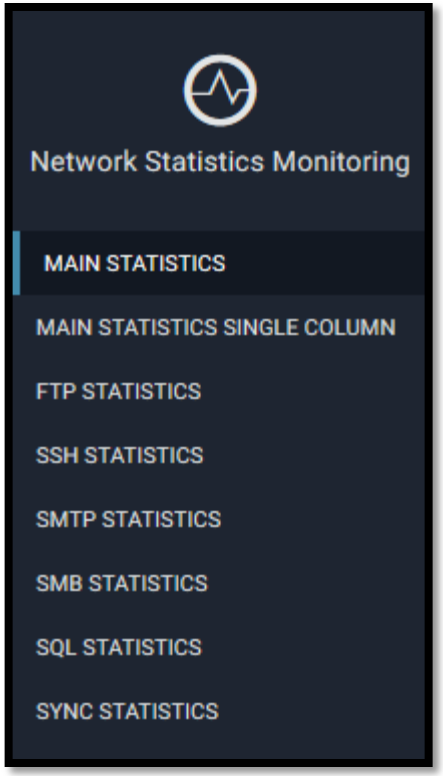


Figure 17 : MYSQL Event and Execution Flow

Results

- Dashboard has different pages showing statistics of different services/protocols.
  - Main page
  - FTP Statistics
  - SSH Statistics
  - SMTP Statistics
  - SMB Statistics
  - MYSQL Statistics



Main Page

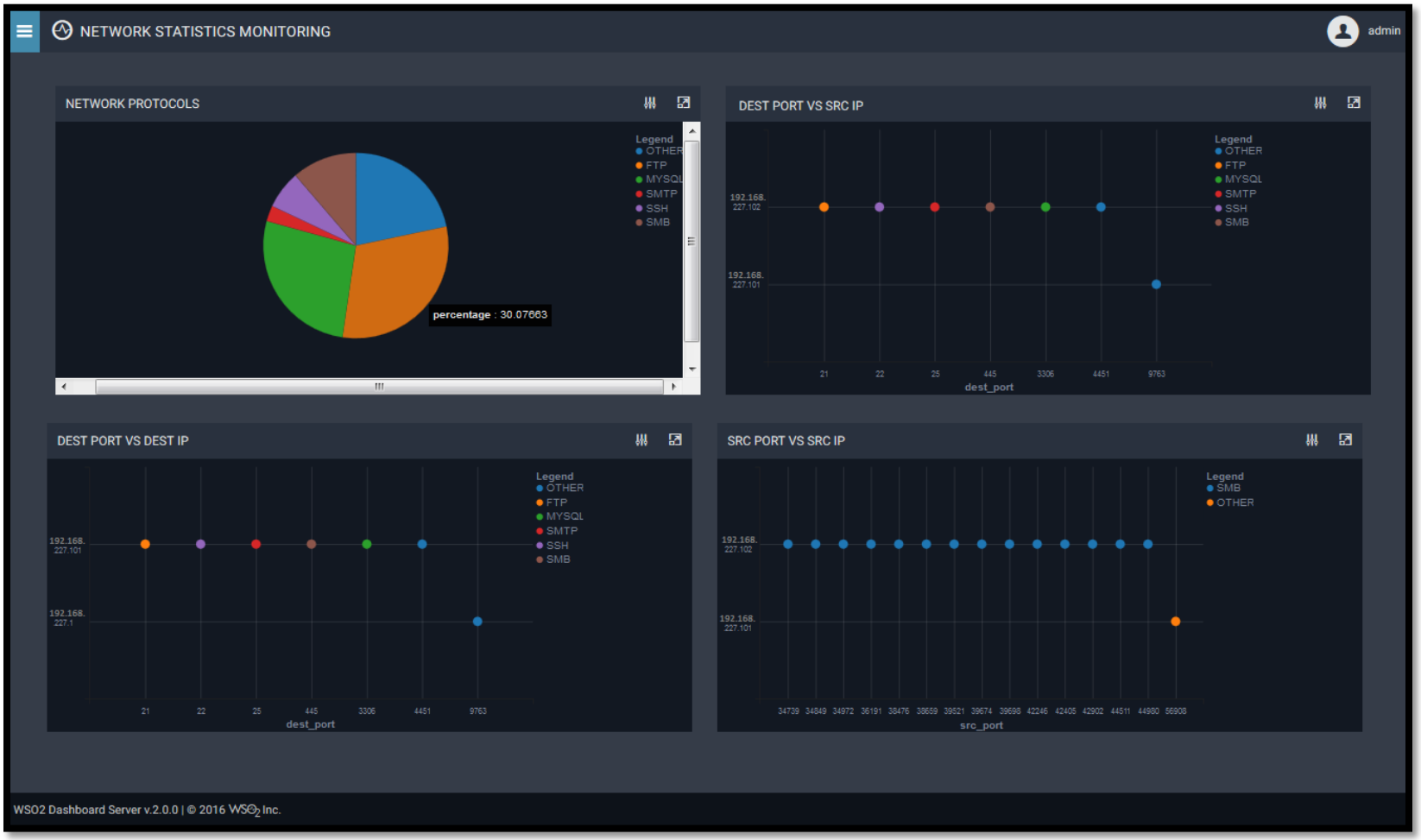


Figure 18 : Dashboard's Main page

Network Protocols Pie Chart

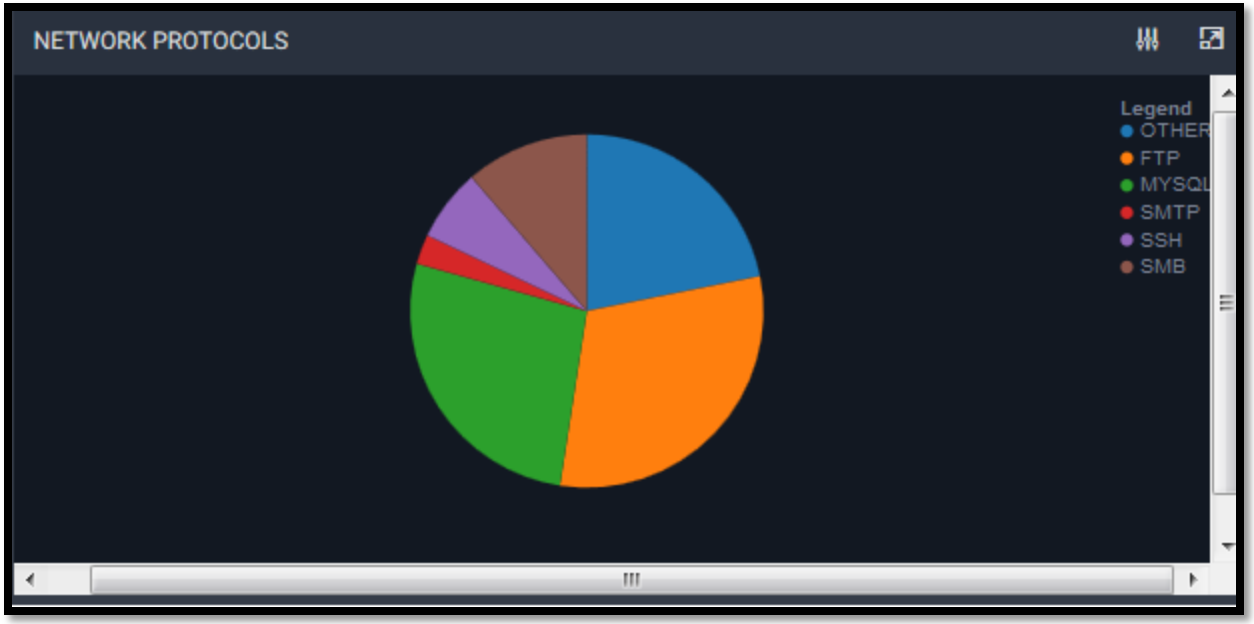


Figure 19 : Percentage of protocols/services in daily network traffic

IP Address and Ports Scatter Plot

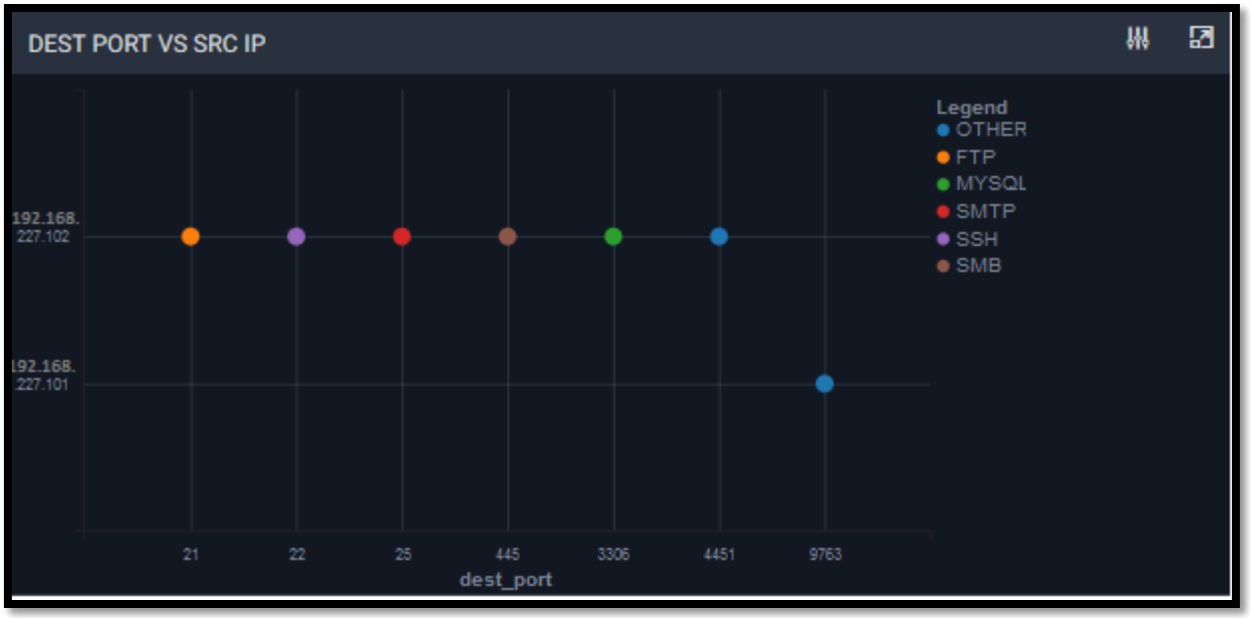


Figure 20 : Destination port vs Source IP

FTP Statistics

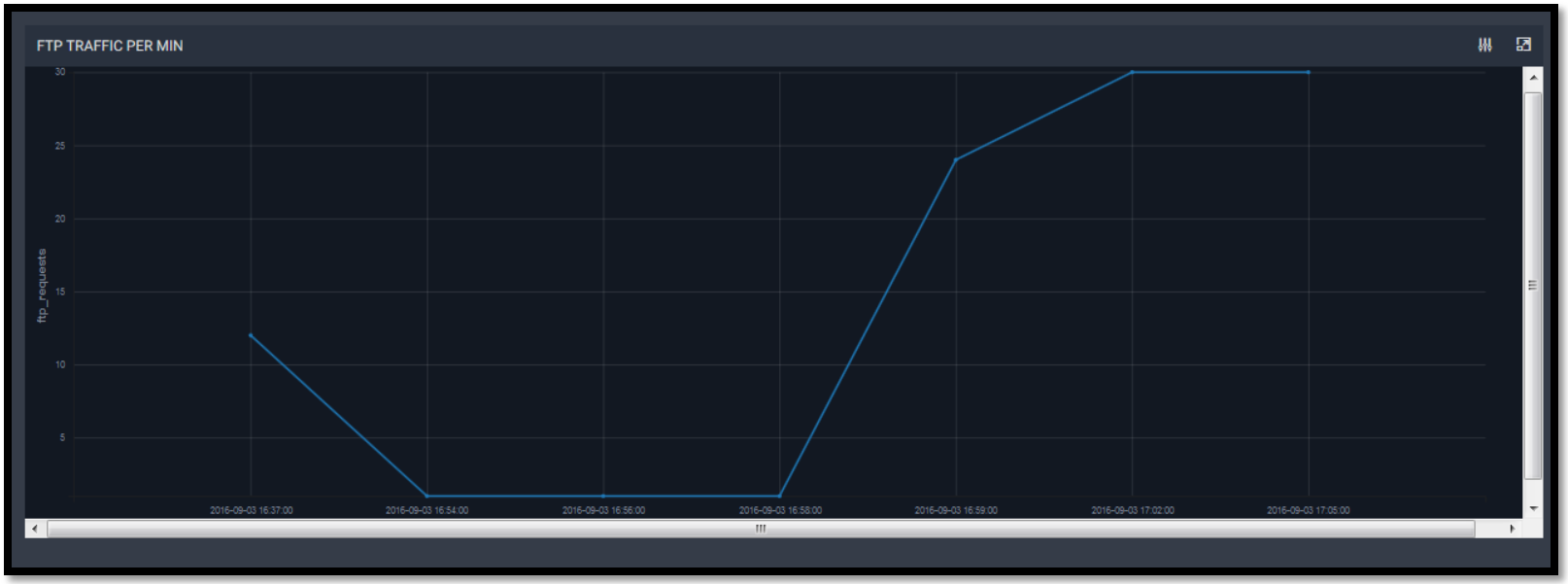


Figure21: FTP Traffic per Minute

FTP Statistics (cont.)

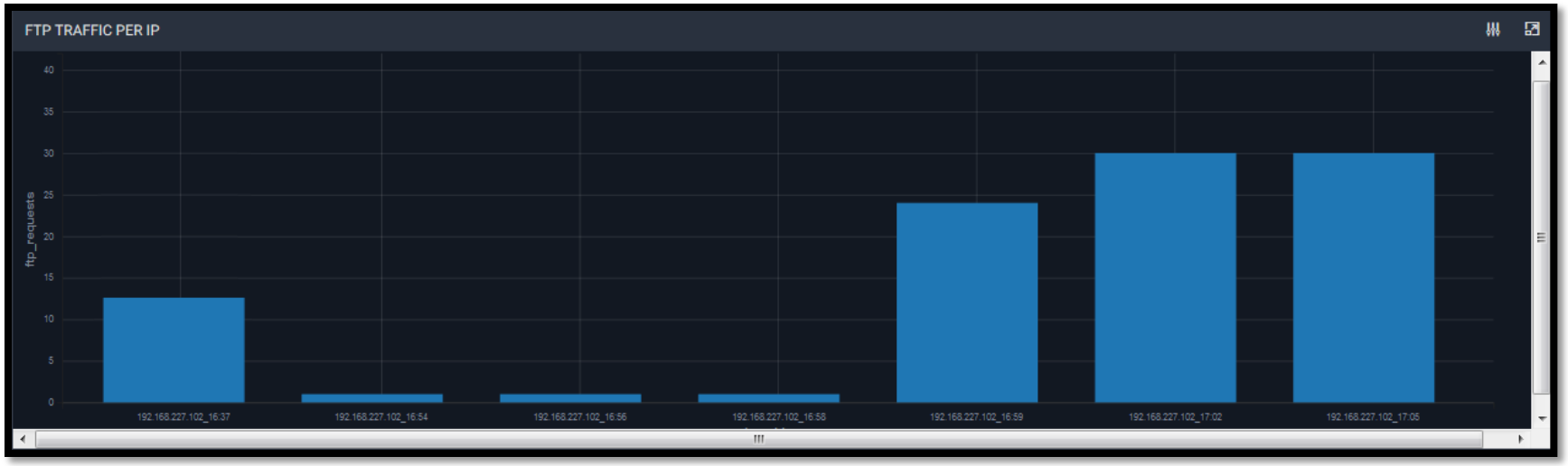


Figure 22: FTP Traffic per IP address

FTP Statistics Page

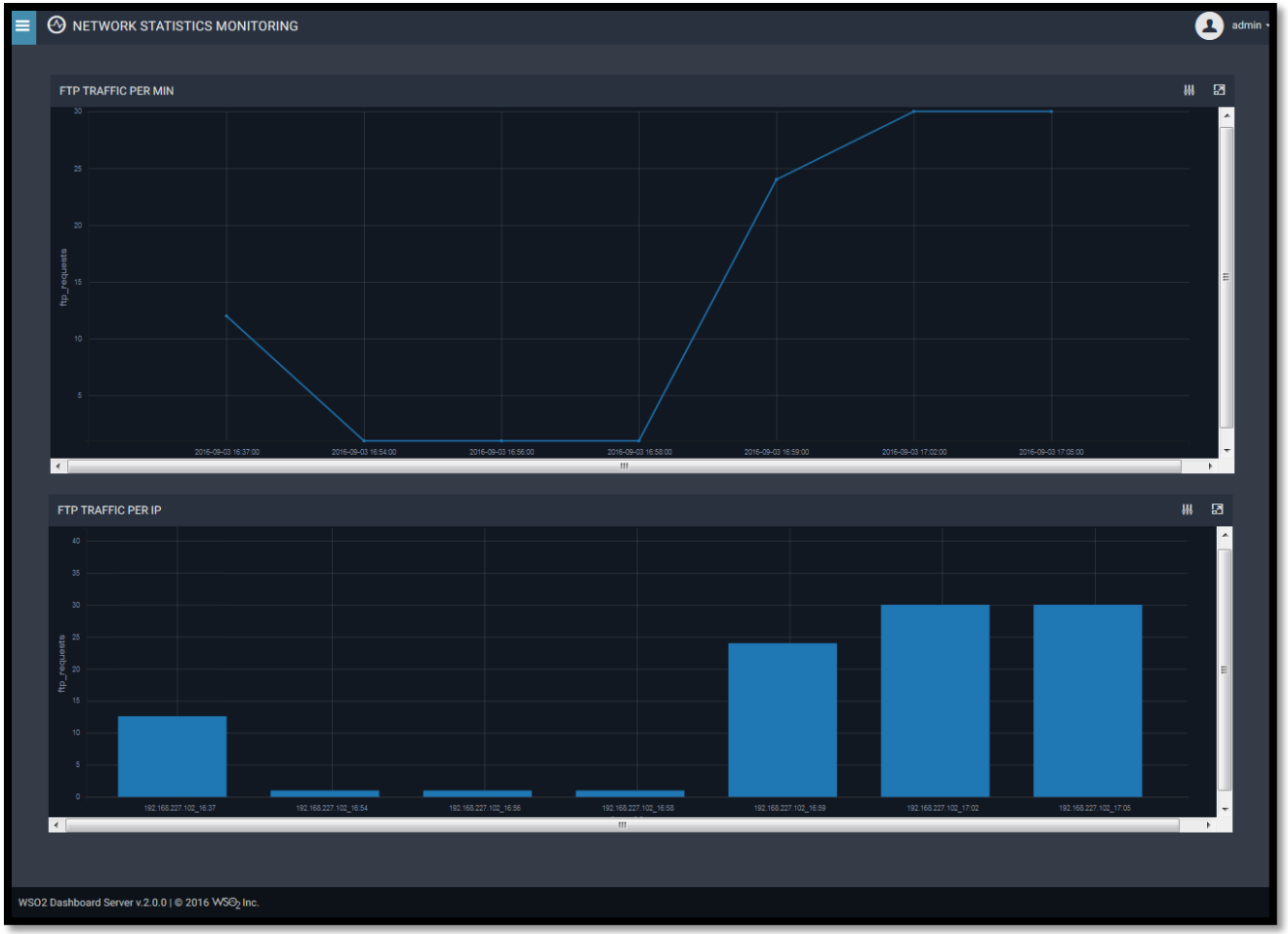


Figure 23 : FTP Statistics Page

SSH Statistics Page

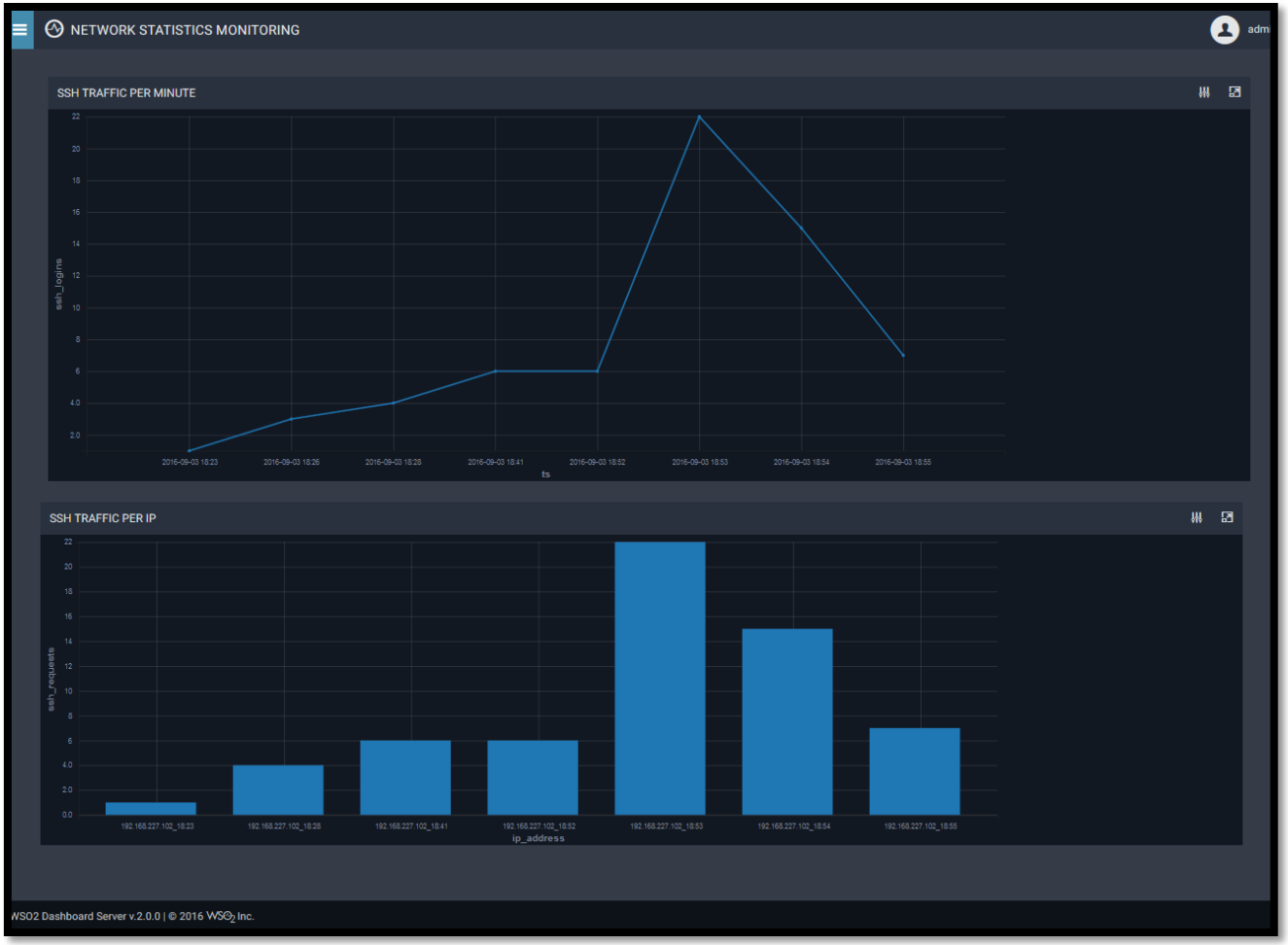


Figure 24 : SSH Statistics Page

SMTP Statistics Page

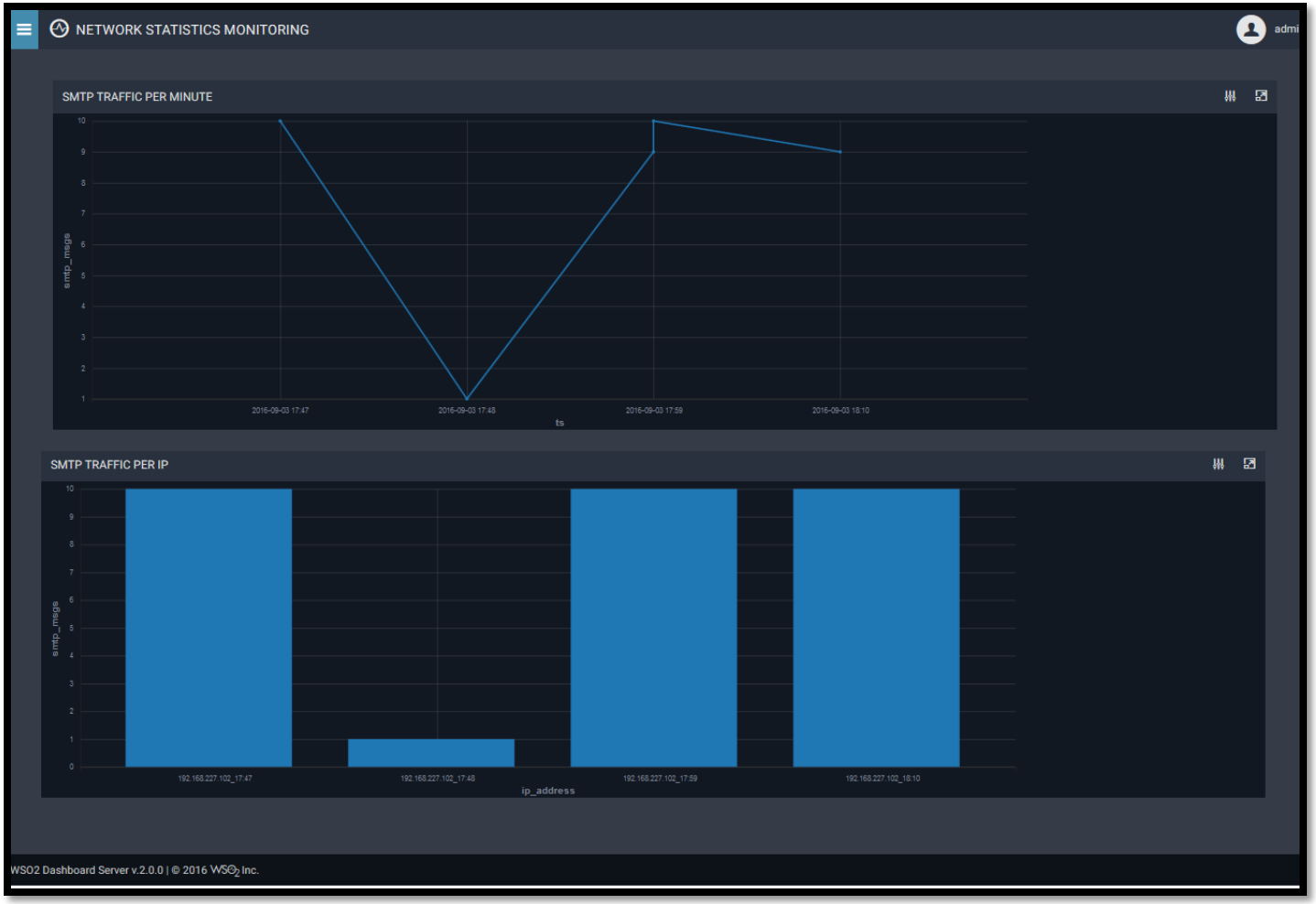


Figure 25 : SMTP Statistics Page

SMB Statistics Page

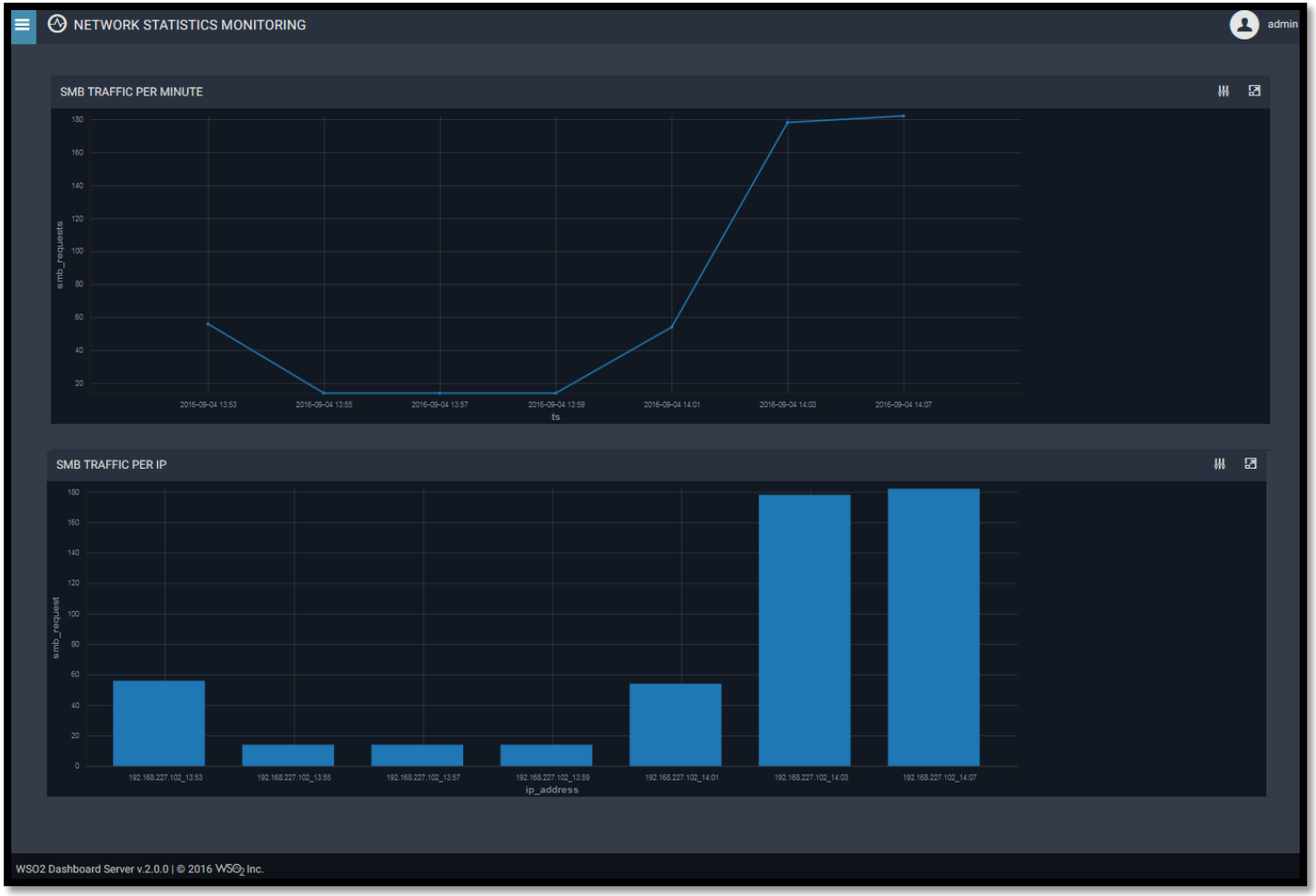


Figure 26 : SMB Statistics Page

MYSQL Statistics Page

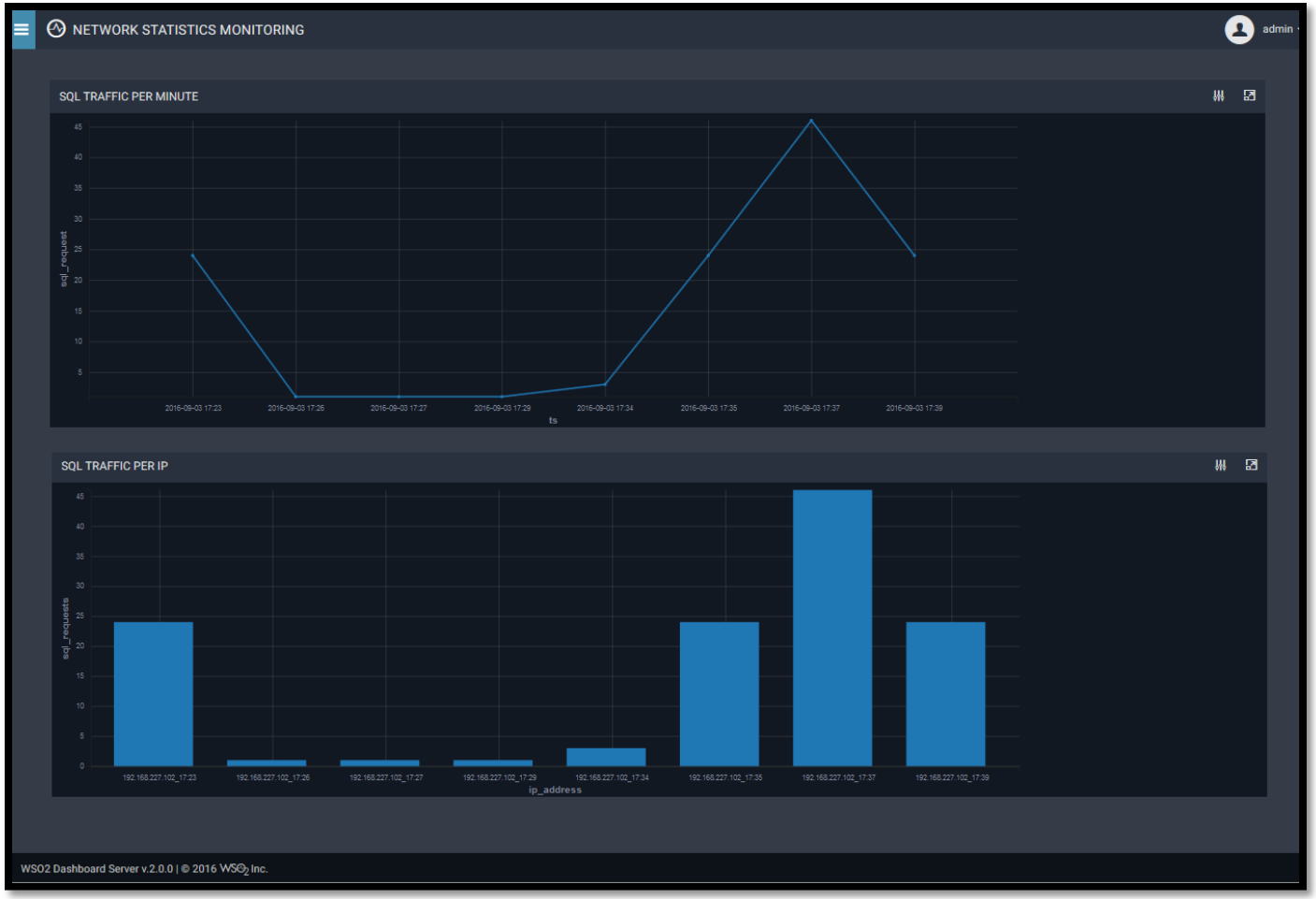


Figure 27 : MYSQL Statistics Page

Future Work

- More protocols and services can be added to monitor.
- Attacks exploiting particular characteristics of any protocol or service can be detected and analyzed.
- Collection process can be made more considerate to send only most relevant data to CEP.
- Alerts can be generated in form of emails etc.
- 2D visualization can be enhanced to 3D and can be made interactive.

Thanks

Any Questions?

References

- [1]. https://www.packtpub.com/books/content/ruby-and-metasploit-modules
- [2]. George Khalil. Open Source IDS High Performance Shootout. SANS Institute InfoSec Reading Room, February 2015
- [3]. WSO2 Inc. WSO2 Complex Event Processor Documentation Version 4.2.0. August 2016.
- [4]. V.C.Asiwe and P.S.Dowland. Advances in Networks Computing and Communications 4, Section 1, Network Systems Engineering, Implementing Network Monitoring Tools . 2004-2005.
- [5]. Jabhera Matogoro and Nerey H Mvungi. Design and Implementation of Network Monitoring System Using Open Source Software (Oss); A Case of University Of Dodoma Network. 2011.
- [6]. Lihua Hao and Christopher G. Healey and Steve E. Hutchinson. Flexible Web Visualization for Alert-Based Network Security Analytics. VizSec '13, October 2013.