VAST 2012 Challenge
Mini-Challenge 2:

Team Members:

- **Roberto Abalde rabalde@gmail.com PRIMARY**
- **Marcos Wolff wmarcos@gmail.com**

Student Team:YES

Tool(s):

- PostgreSQL
- Libre Office Calc
- Tableau software

Video:

http://www.youtube.com/watch?v=brIz0vj14lw

Answers to Mini-Challenge 2 Questions:

MC 2.1 Using your visual analytics tools, can you identify what noteworthy events took place for the time period covered in the firewall and IDS logs? Provide screen shots of your visual analytics tools that highlight the five most noteworthy events of security concern, along with explanations of each event.

For the development of the visualization we used two main tools:

- PostgreSQL database for data processing
- Tableu Software for charts and visualizations

The steps to build the main table with all the connection were:

1. Loaded the .csv files to two tables: firewall_log and ids_log
2. Filtered out all the connections from firewall_log where operation was not "Teardown" because this row shows when two computers disconnect, and this was not interesting for our analysis
3. Created a new reference table "computers" with all the IP addresses used in the log tables. Then, translated all the ip addresses to the corresponding type of machine ("workstation", "web server", "financial/email server", …).
4. Created the final table, as a union of firewall_log and ids_log tables. To know the type of the connecting and connected computers, we use the "computers" table.
5. We analyzed the type of connection., grouping the destination ports in: official, unofficial and private ports, but also we selected some important ports that we detected in the data and that define connections we wanted to visualize. Specifically:
    - Special: Ports 21, 22, 23, 25, 53, 80, 110, 113, 143, 137, 138, 139, 143, 161, 443, 445, 514, 993, 995 and 6667
    - Unofficial: Ports between 1024 and 49152 (excluding 6667)
    - Private: Ports between 49152 and 65535

After building the visualization, we following identified the following noteworthy security events:

event #1 - network meltdown

On Figure 1.1, we can see that most of the connections on the logs are made by workstations connecting with the web or the financial/email server, using port 80 (http) and 6667 (IRC).

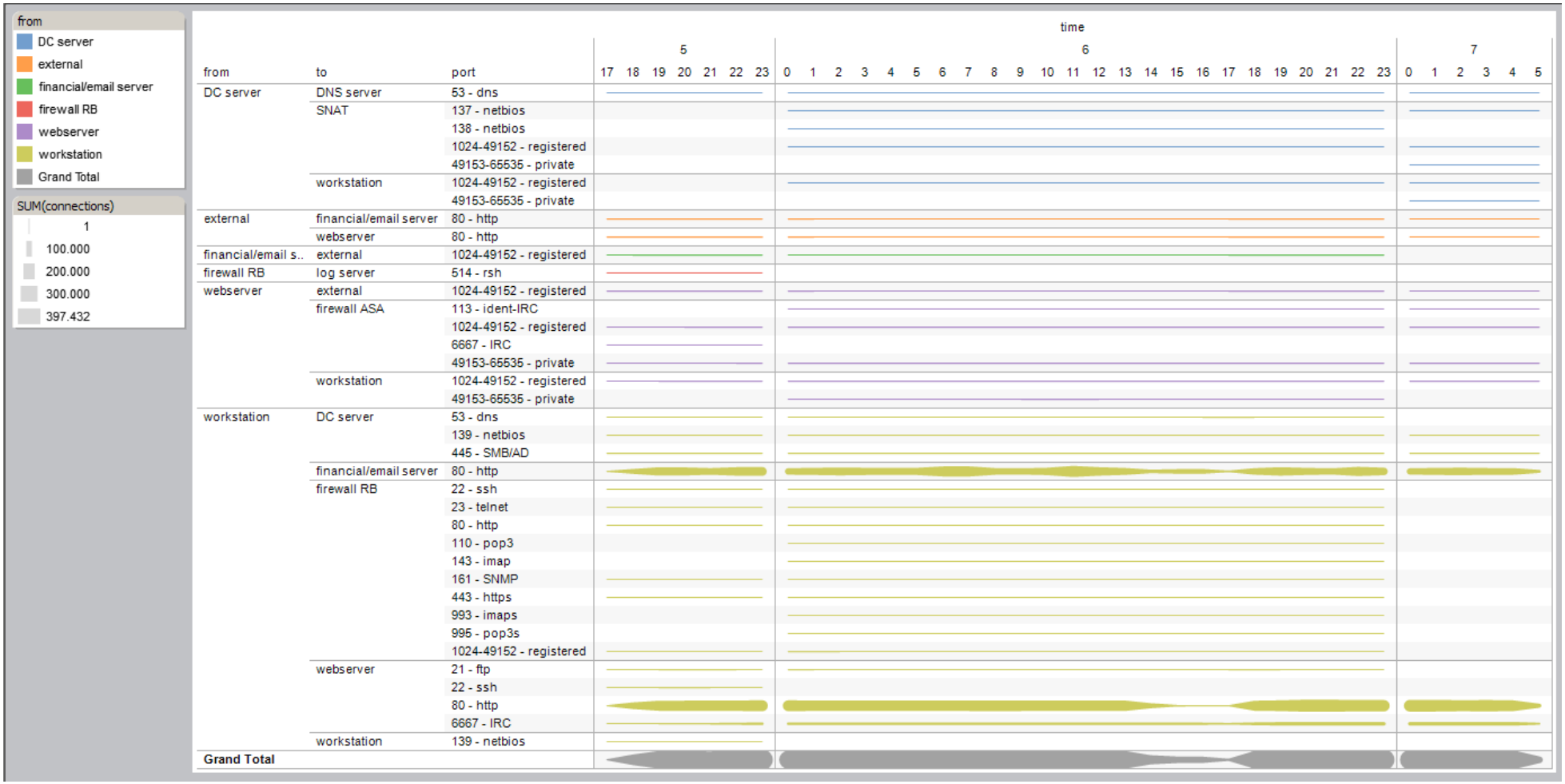

Figure 1.1

But also, we can see on day 6, from 15:00 to 18:00 (approx) that the amount of connections drops drastically. Figure 1.2 gives a more detailed view of the issue.

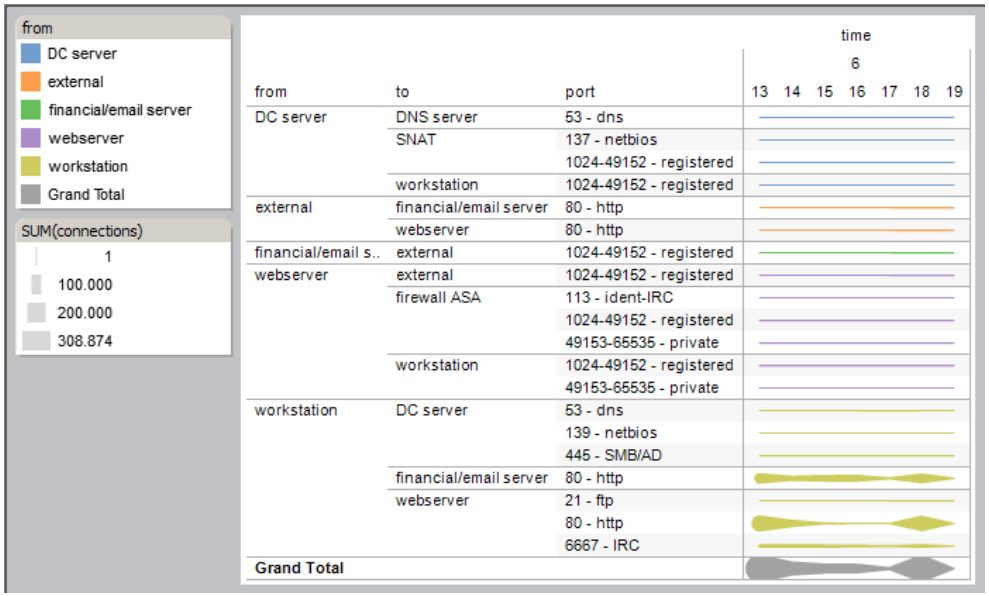

Figure 1.2

In this view, we can see that most of the connections from workstations to port 80 (http) drop, but connections to port 6667 (IRC) don't.

event #2 - ftp connections

On figure 1.3, we can that if we filter out connections to port 80, there's a massive number of connections from workstations to the port 21 (FTP) of web servers: on day 5 at 20:00 and on day 6 at 18:00.

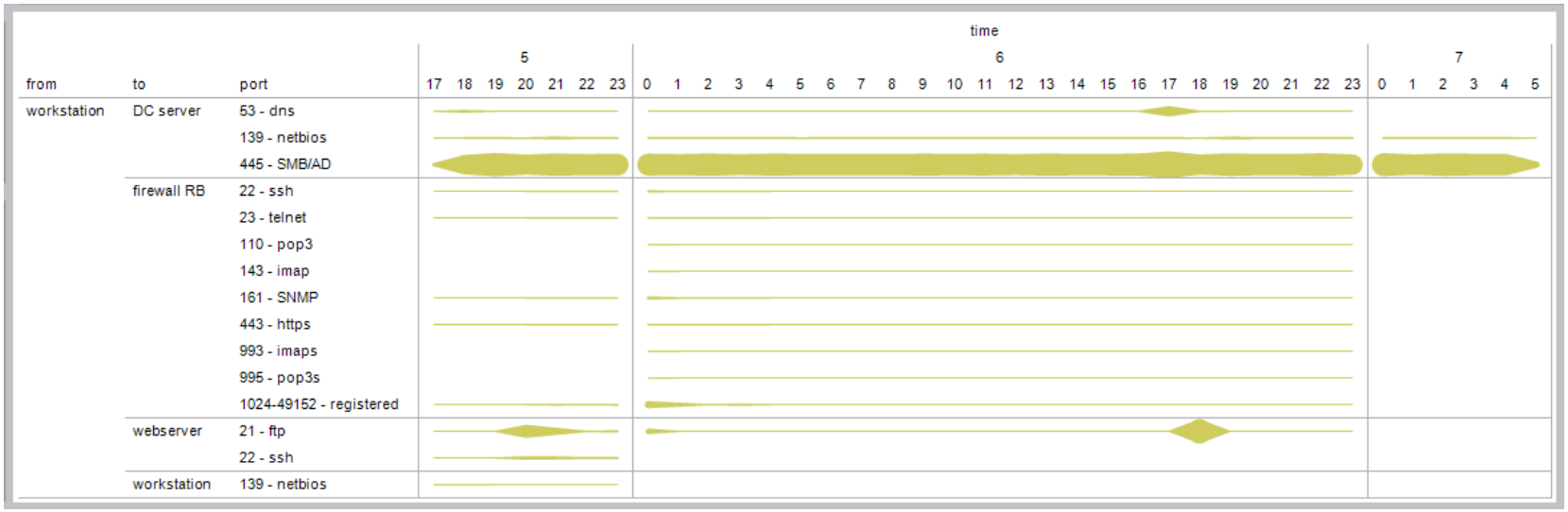

Figure 1.3

A possible explanation to this behavior could be that workstations infected with malware are attacking web servers through the FTP port to gain privileged access.

event #3 - DDoS attack

Figure 1.4 shows pikes in the number of connections from computers outside the Bank's network to the financial/email servers, at 18:00, 11:00, 19:00 and 22:00.

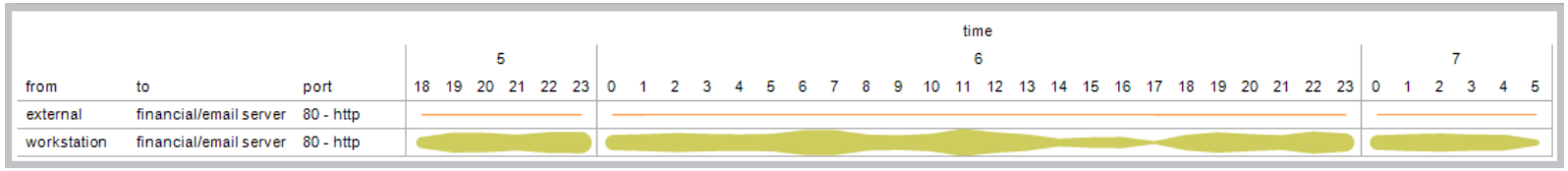

Figure 1.4

This could be caused by a DDoS (distributed denial of service) attack from workstations to the financial/email servers.

event #4 - botnet

Figure 1.5 shows an increasing number of connections from workstations to web servers. If we analyze these connections by web server port, we can see that there are a lot of connections to port 80 (http), the usual expected behavior when workstations connect to a web server.

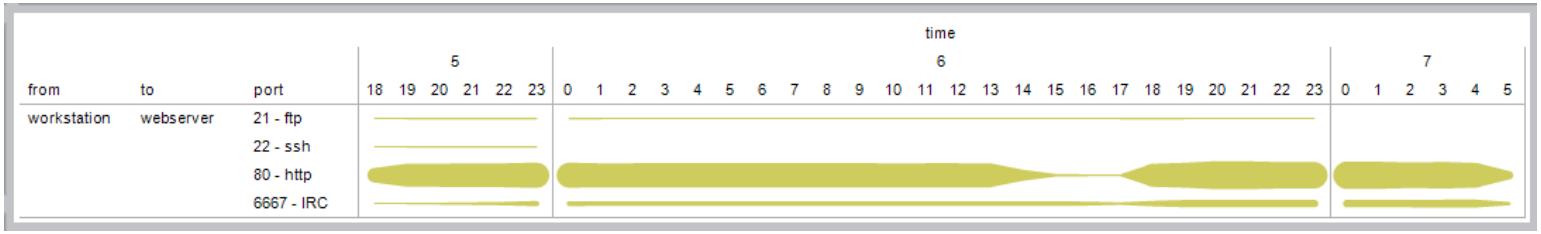

Figure 1.5

We can also see that some workstations connect to web servers through port 6667 (IRC). The possible cause to this behavior could be that some workstations are infected with malware and form a botnet that is attacking the web servers. The attacks of these botnets are usually coordinated using an IRC server.

event #5 - external connections

From 18:00 to midnight on days 5 and 6 we can see (Figure 1.6) a lot connections made from computers outside the Bank network ("external") to the financial/email servers. Bank policy says that this behavior is not allowed.

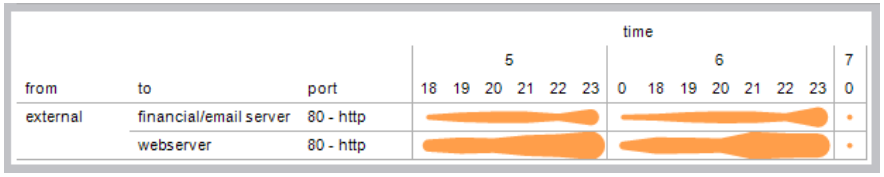

Figure 1.6

Possibly the firewall accepts connections from the outside because is not configured correctly, leaving those servers exposed to malware.

MC 2.2 What security trend is apparent in the firewall and IDS logs over the course of the two days included here? Illustrate the identified trend with an informative and innovative visualization.

Over the two days, the security trend that is apparent in the logs servers is that the network has been compromised and there are an increasing amount of unusual connections that shouldn't exist in a healthy network.

An example of these connections are the ones originating in web servers and workstation connecting to the port 6667 (IRC) in the web servers and the ASA firewall (Figure 2.1).

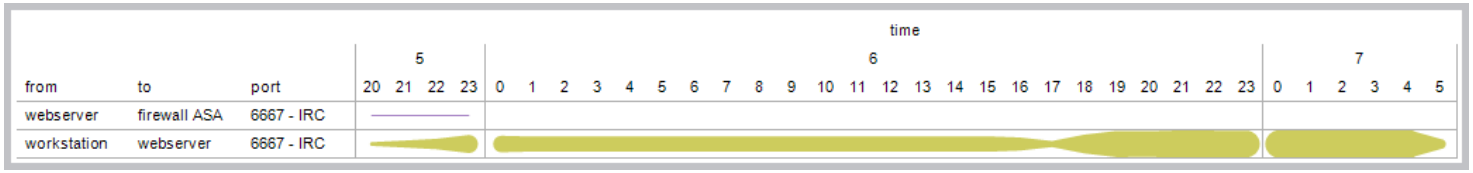

Figure 2.1

This could be only an IRC (Internet Relay Chat) installed unofficially, but also could be a botnet software using computers in the local network to perform DDoS attacks or other kind.

Another example can be seen in Figure 2.2, where the web servers are connecting to computers outside the Bank network (external) during the first day.

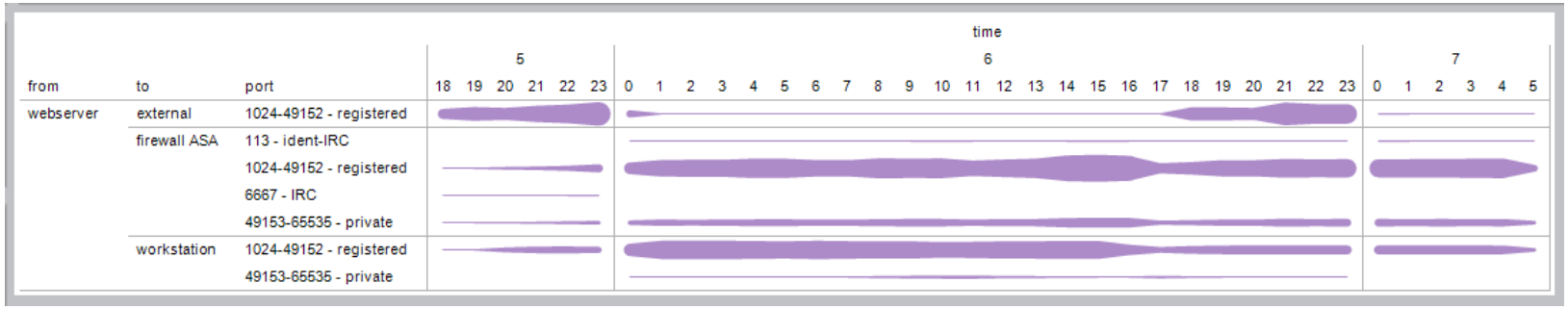

Figure 2.2

The next two days they start dropping connections to the exterior and start connecting to ASA firewalls and to workstations, using many port, but mostly registered ports and 6667 (IRC). All these connections are not usual for a web server because this type of server doesn't need to start a connection to any other computer except to the workstations (responding to client connections). It may be explained if the web server has been infected by a malware and is trying to spread the malware to other computers.

MC 2.3 What do you suspect is (are) the root cause(s) of the events identified in MC 2.1? Understanding that you cannot shut down the corporate network or disconnect it from the internet, what actions should the network administrators take to mitigate the root cause problem(s)?

We suspect that the root causes of events identified in MC 2.1 are:

- There are connections from outside the bank network that should not be allowed. This could happen if employees connect to the servers from home
- The firewall configuration has errors, because they're allowing connections from the outside to the Bank network
- There are workstations infected with malware. This could happened because employees can plug thumb drives that haven't been scanned properly or install software on infected with malware

To fix these causes we propose doing the following actions:

- Fix the firewall configuration to ban external connections to the local network
- Ban all use of thumb drive in workstations. System administrators should scan for malware and then copy the thumb drive's contents to the workstation
- Update/upgrade antivirus/malware software on all workstations
- Install firewalls on every workstation, and configure them to filter all connections that have a destination port not allowed, for example 6667 (IRC)
- Filter all connections not coming from an allowed MAC addresses