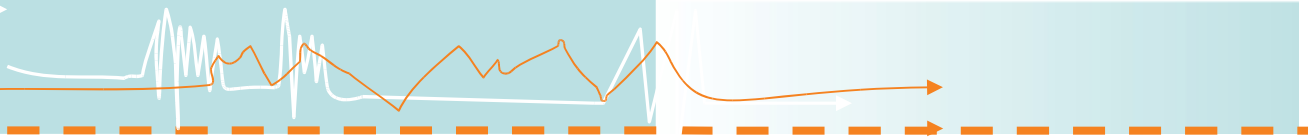
Organising a Technical IT Security Exercise

Varis Teivans, CERT.LV

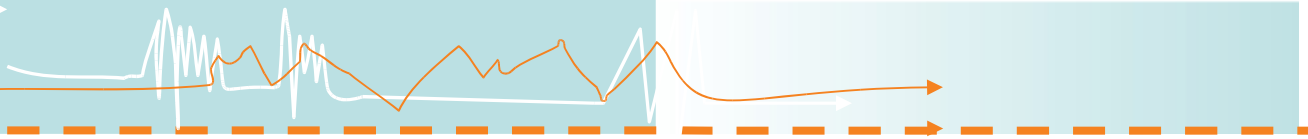
11.05.2012. Amsterdam, The Netherlands



Background information

CERT.LV

- Operational since 1 February 2011
- Operates on the basis of IT Security Law
- Tasks delegated to Institute of Mathematics and Computer Science, University of Latvia
- State funded
- Year 2011 - 5 FTE
  - At that time very limited resources for technical training



CERT.LV

Where to begin with technical exercise?

- **Where to get the ideas for:**
  - Scenario?
  - Attack vectors?
  - Environment setup?

- Technical resources – if you don't have them
  - It is possible that your training audience has much more resources than you have
  - Technical people are hungry for some fun
  - Some of them will be willing to provide technical resources for exercise time

Scenario

- Building our scenario almost entirely on real incidents

- **almost** - because you always have to include some tricks and catches to make it even more interesting

Scenario

- The blue team environment should not withstand exploitation - at the end of the day they just have to be hacked anyways :)

- Think about backup plan
    - In some cases you don't know the skill-set of your training audience

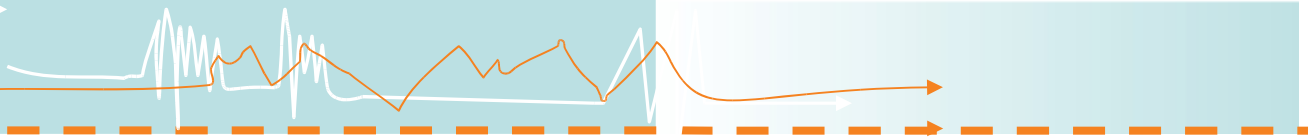
- Plan the time line and injects
    - Plant some backdoors
    - Tricks
- Be prepared to help your training audience

Important points

- Scenario on dashboard (brain storm session)
- Later can put it on mind map or paper
  - **Xmind** - useful tool for creating mind maps
- Use checklists while building the environment and more importantly while finishing it
  - file time stamp modification
  - history
  - cleanup
  - obfuscation

Setup

- 2 attacking teams (RED teams)
- 3 defending teams (BLUE teams)
- Each team in a separate room
- Blue Team: New and evolving software development company "BlueTeam Technologies"



Create a multi-flavored environment to make everyone busy

Setup

Windows 2008 server

- -Active directory
- -Exchange
- -FTP
- -RDP
- -NetBios

Setup

Unix

- -DNS server
  - -cache poisoning
    - -vulnerable FTP but service not needed
  - -MAIL
  - -Web server
    - -LAMP, FTP,
    - -wordpress, joomla, custom web site, phpmyadmin

-64 bit exploitable kernel to access the isolated storage server and get the bounty

Setup

WinXP

-user with clicking and double clicking skillset

- observers

-admin access to CMS on Web server

-client side attacks

Setup

-network/routing devices

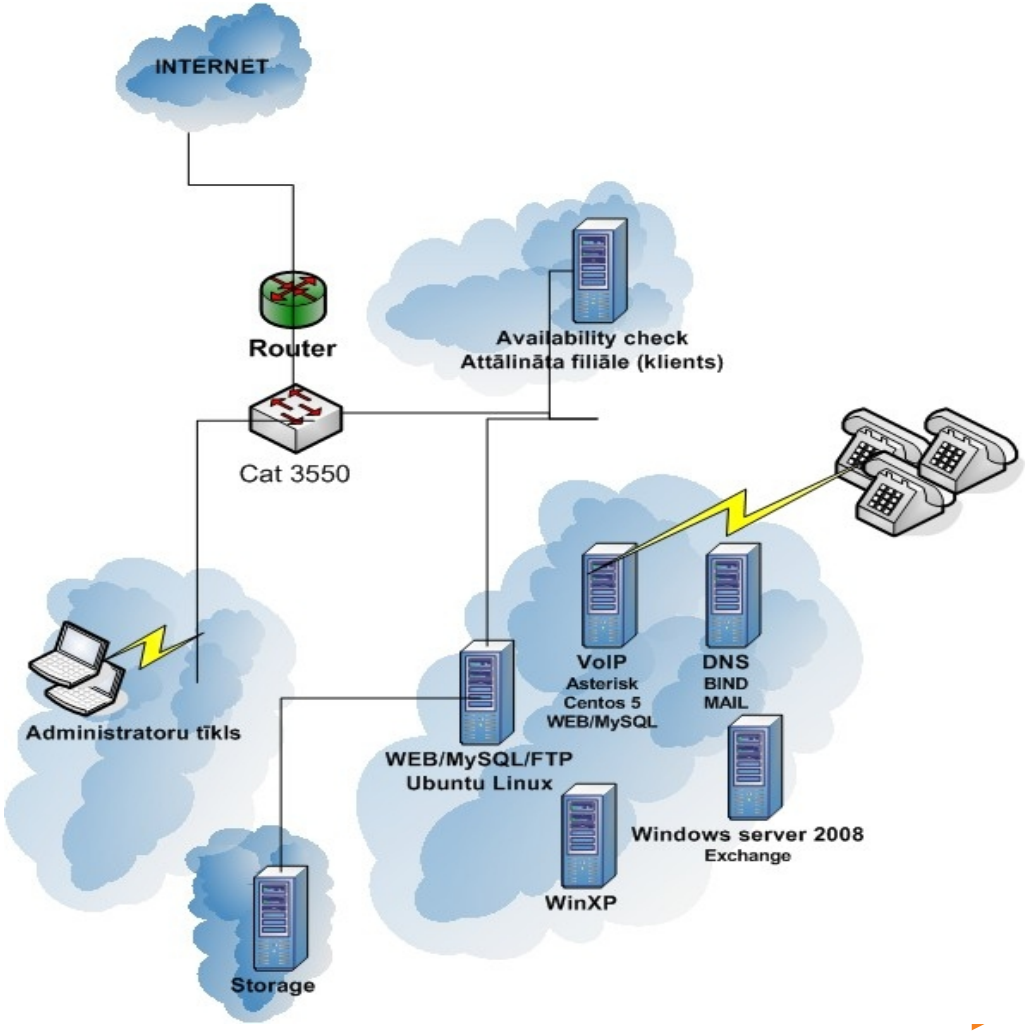
-IP telephony

-IP phones with web interface

-Asterisk server

-Availability checker / Network Noise generator

Setup


INTERNET
Router
Availability check
Attālināta filiāle (klients)
Cat 3550
Administratoru tīkls
VoIP
Asterisk
Centos 5
WEB/MySQL
DNS
BIND
MAIL
WEB/MySQL/FTP
Ubuntu Linux
Windows server 2008
Exchange
WinXP
Storage

Setup for Blue team

- Each team received only a brief description and diagram of technical environment few days before the training
    - Might not be the best approach in some cases
- Game rules are introduced to RED & BLUE teams
    - Useful for both
    - Both can act as reporters/whistleblowers :)

Some simple but effective tricks from reds

adduser certivo
Adding user `certivo' ...
Ading new group `certivo' (1001) ...
Adding new user `certivo' (1001) with group `certivo' …

```
drwxr-xr-x  23 root root  4096 2012-05-15 09:28 .
drwxr-xr-x   2 root root  4096 2012-05-15 09:28 .,
drwxr-xr-x  23 root root  4096 2012-05-15 09:28 ..
drwxr-xr-x   2 root root  4096 2012-03-26 22:18 bin
drwxr-xr-x   3 root root  4096 2012-04-23 09:49 boot
drwxr-xr-x   2 root root  4096 2012-03-01 14:09 cdrom
```

Lessons learned

Each blue team had IP telephony and IP phones on their desks

- Red teams noticed that before blue teams did :)

Lessons learned

- More than 2 months for preparation and more technical resources would be nice

However, it is possible

- 2 months
- 3 people on part time
- 2 servers
- XEN virtualisation

Lessons learned

Technical environment has to be more powerful

2 servers with 2.6 GhZ quad core CPU and 500MB RAM (Linux) 1GB (WIN) per VM was not enough

Clearly defined policy and rules for the game

Test run for each team a day before exercise?

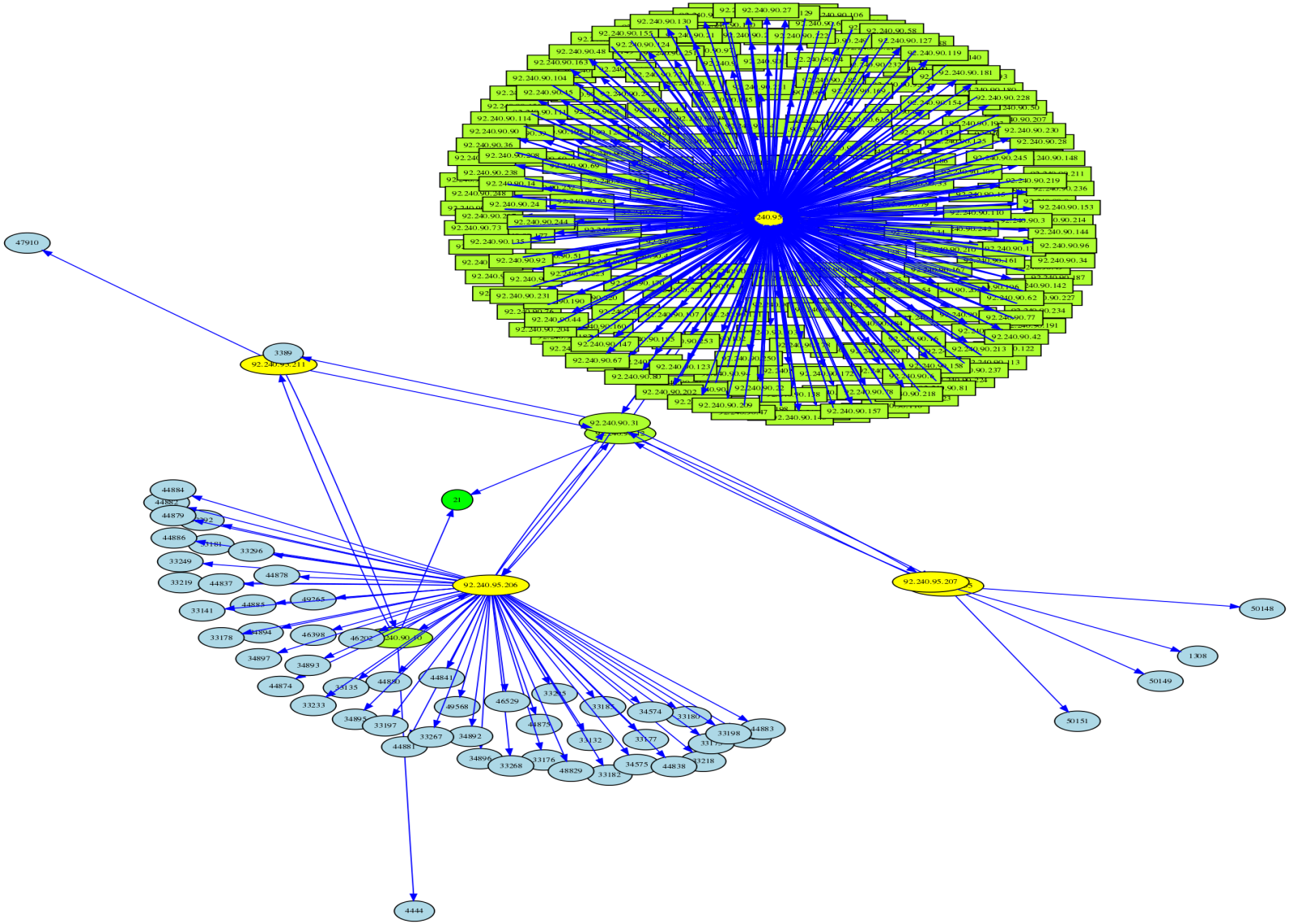
Lessons learned

- Scoring system + communication/reporting
  - Online messaging + monitoring tools (Nagios)
- Teamwork is vital for success
- Organising a technical training is also a training for organisers
- After briefing and discussions are essential

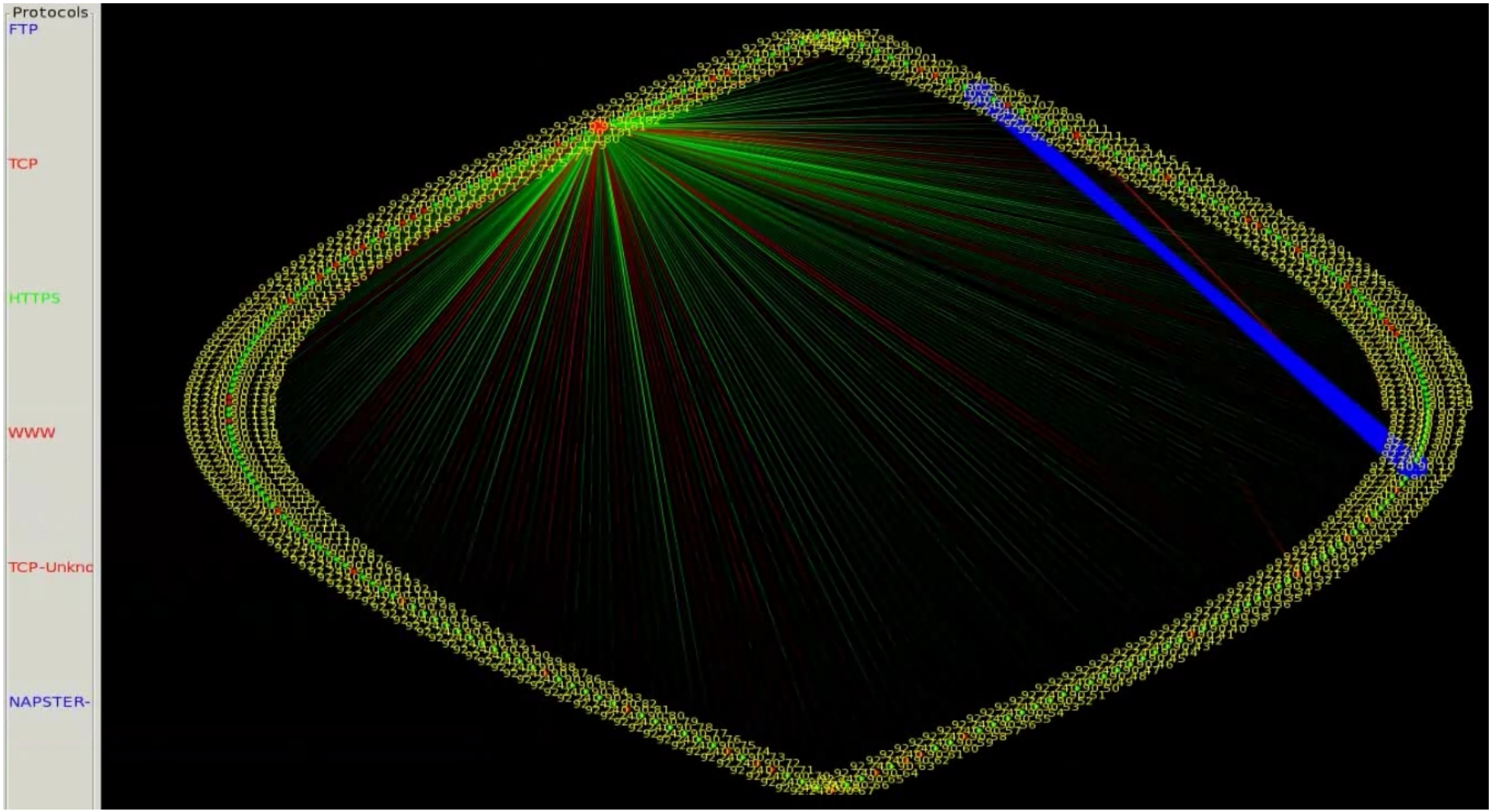
Lessons learned

- Visualizations - people love pictures, moving pictures are even more appreciated
- Davix visualization live CD
  - AfterGlow
  - EtherApe
  - ...

Attack Visualization



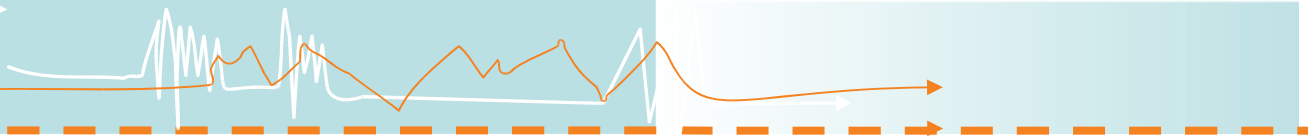
Attack Visualization



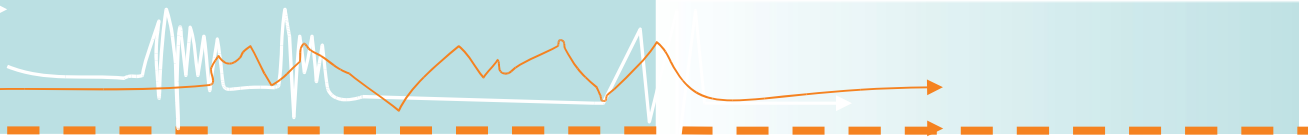
So where to get the ideas?

- Scenario?
- Attack vectors?
- Environment setup?

- Our everyday work covers all of the mentioned topics
- Learn from:
  - Incidents
  - Attackers
  - Constituency
  - Community
- A lot of information for scenario is already there



A lot of knowledge is here in this room...



CERT.LV

Thank you!!!

http://ww.cert.lv/
cert@cert.lv
varis.teivans@cert.lv