Research Project @ BELNET

Virtual Infrastructure Security

Berry Hoekstra
Niels Monen

Supervisor
Jean-Christophe Real

Agenda

- Introduction
- BELNET
- Research
- Conclusions
- Questions

Introduction

- Research Project 1
  - Virtual Infrastructure Security; Study possible security issues with a virtual infrastructure

- BELNET, company located in Belgium
  - Too far to travel
  - Working at the OS3 lab
  - Contact via e-mail

About BELNET

- Belgian National research and education network
- ISP that focuses on research institutions

- Beginning in 1989, BELNET provides web services to
  - Higher education
  - Federal departments
  - Federal ministries
  - International organizations

BELNET

The network of knowledge

© BELNET

Main goal

- Successfully implement a secure Virtual Infrastructure
  - VMware based
  - Maintain current security level
  - Maintain current maintenance level
  - Serve VMs in different VLANs

- Researching security related issues on a virtualized platform, based on VMware virtualization technology

Research question

- Definition
  - "*What is the best way to successfully implement a virtual infrastructure while dealing with all possible security (related) issues?*"
- Findings
  - In the form of a Consultancy Report

Sub-questions (1)

- Provide recommendations in a consultancy report
  - Level of firewalling
  - Remote VI management
  - Secure SAN access
  - Guests in multiple VLANs

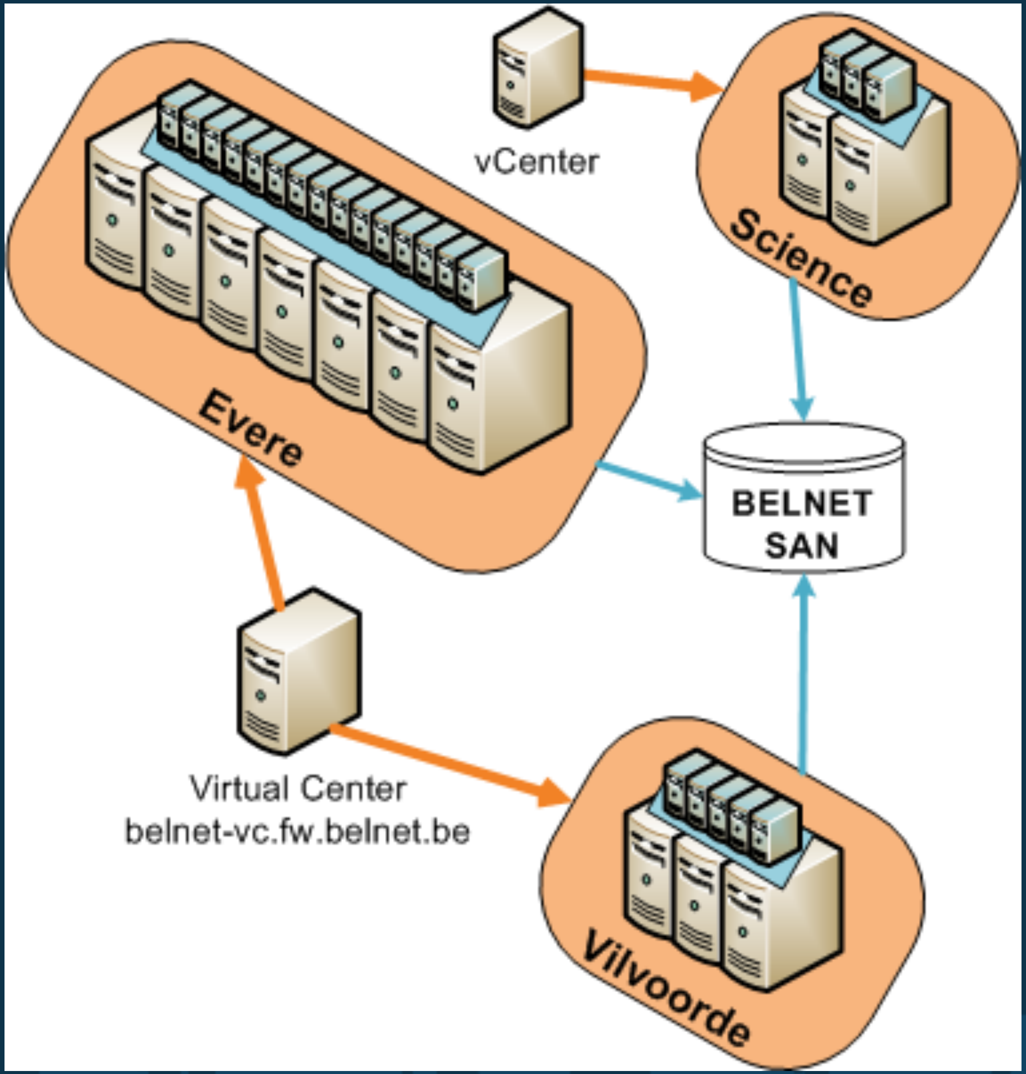
Sub-questions (2)

- Different passwords on hosts and guests
- Virtual Datacenter and Cluster security issues
- Host access from compromised guest
- Virtual Infrastructure security state
  - Monitoring
  - Auditing

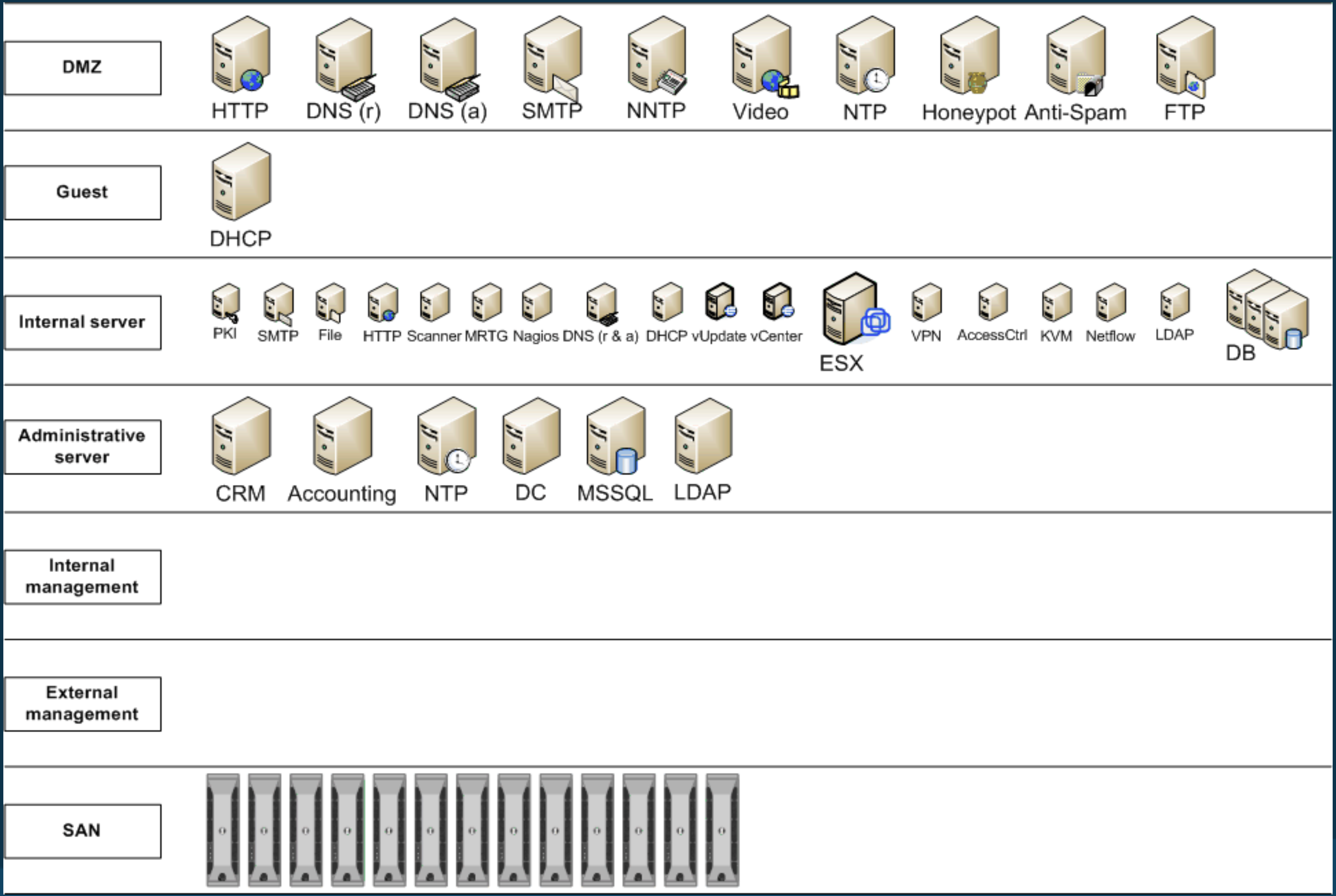
Existing setup

- 10 blade servers running VMware ESX 3.5
    - Virtual Infrastructure
    - Production environment
- 2 blade servers running VMware vSphere
    - Used for testing VMware vSphere
- A few servers running VMware ESXi and VMware Server
    - Hosting test VMs
- SAN environment
    - Central storage, backup and management
    - 13 x Dell EqualLogic PS4000E
    - iSCSI protocol

Virtual Infrastructure



VLAN setup



DMZ	HTTP, DNS (r), DNS (a), SMTP, NNTP, Video, NTP, Honeypot, Anti-Spam, FTP
Guest	DHCP
Internal server	PKI, SMTP, File, HTTP, Scanner, MRTG, Nagios, DNS (r & a), DHCP, vUpdate, vCenter, ESX, VPN, AccessCtrl, KVM, Netflow, LDAP, DB
Administrative server	CRM, Accounting, NTP, DC, MSSQL, LDAP
Internal management	
External management	
SAN	

DMZ security

- DMZ virtualization can cause security problems
- Solutions
  - Additional physical network adapter
    - Dedicated to DMZ traffic
    - No need to tag traffic
  - VMs of same DMZ on same virtual host
    - High server consolidation
    - Maintain DMZ consistency

SAN security

- Authentication with CHAP
- If possible use IPsec
- Use authorization
- Isolate the network
    - VLANs
    - Physically
- Only open the ports that are needed

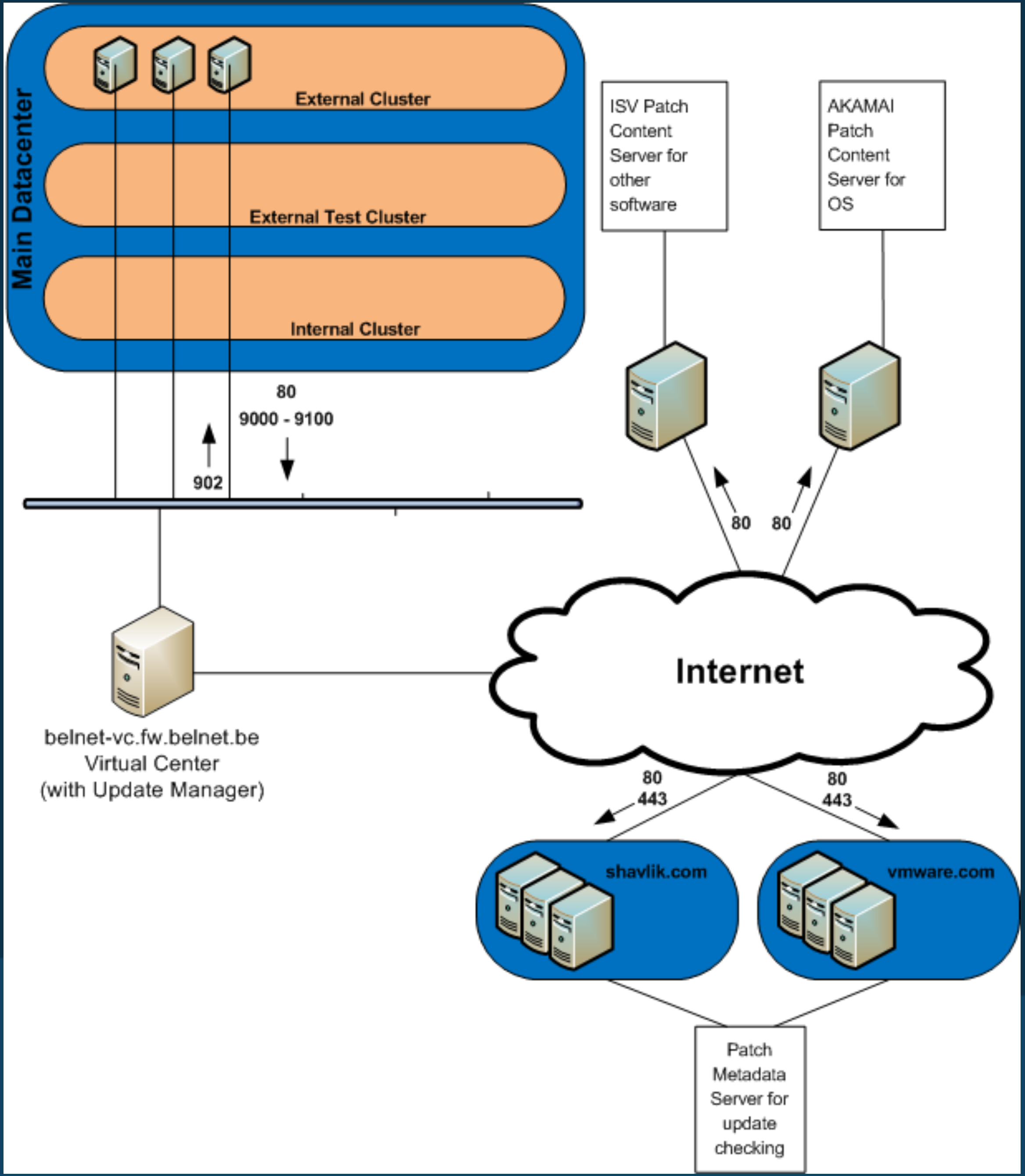
VI security

- Host
  - Limit access to Virtual Center/vCenter
  - Certificates
  - Updates
  - Firewalling
    - Only open required ports
    - Access: only from/to specific hosts
- Guests
  - OS updates
  - Limit resources to prevent DoS attacks
  - Passwords
  - Use templates

Updates

- VMware Update Manager
    - Part of Virtual Center/vCenter
    - Host updates
    - OS updates
    - Automated
    - Requires firewall changes
    - Queries
        - shavlik.com and vmware.com for metadata
        - AKAMAI and ISV servers for update content

Update infrastructure



Passwords

- Different passwords for hosts and guests
    - Password complexity
    - Way to securely store passwords
        - Not on paper
        - Encrypted like with KeePass
- Effects on the use of
    - Virtual Data Centers
    - Clusters
- Best to use different passwords stored encrypted

Monitoring (1)

- Monitoring the security state
  - Central logging
  - Event alerts (current Nagios setup)
  - Trend monitoring (current MRTG setup)
  - Virtual Center alerts
- Subscribe to VMware security mailing list
  - Security issues
  - Latest patches

Monitoring (2)

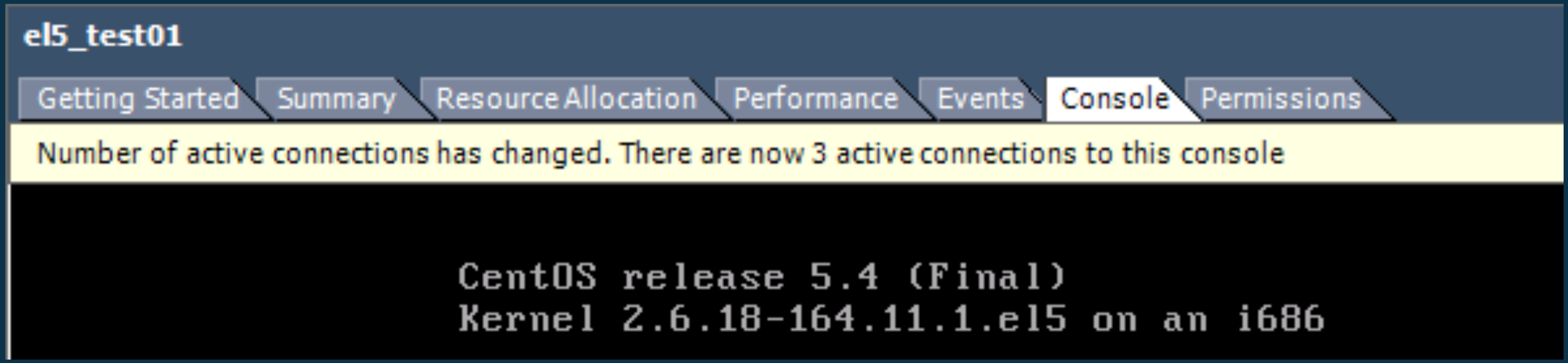
- Central logging
  - API user login (root/other/unkown)
  - Tech Support user login (root only)
  - Tech Support mode invocation
  - Root login via Tech Support Mode on local console
  - Root login via Direct Console User Interface (DCUI) on local console
  - Virtual Console events
    - Single Virtual Console
    - Multiple Virtual Consoles

Monitoring (3)

- Logins on host using Virtual Infrastructure Client
  - *User root@0.0.0.0 logged in*
  - *Rejected password for user root from 0.0.0.0*
  - *Rejected password for user unknown_user from 0.0.0.0*
- Logins on DCUI
  - *authentication of user root succeeded*
  - *authentication of user root failed*
  - *authentication of user berry failed*
- Logins on Console
  - *techsupport VMware Tech Support Mode available*
  - *authentication failure*

Monitoring (4)

- Virtual Console access
    - Multiple active connections



Number of active connections has changed. There are now 3 active connections to this console

```
CentOS release 5.4 (Final)
Kernel 2.6.18-164.11.1.el5 on an i686
```

© VMware Inc.

- Log alerts
    - *Ticket issued for mks connections to user: root*
    - *Local connection for mks established*
    - *New MKS connection count:3*
- Be sure to set tresholds

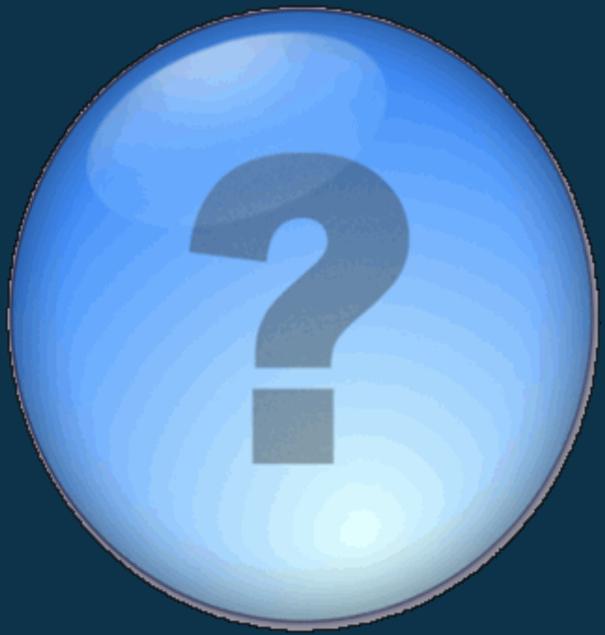
Auditing

- Auditing the security state
  - Treat VM like PM
  - Keep current auditing policies
  - Audits by different people
  - Roll back changes after a test phase

Conclusions

- Firewallling: Only open required ports
- DMZ security: Keep as many VMs from the same DMZ on one physical host or use seperate physical NIC for DMZ traffic
- SAN security: Use CHAP and, if possible, IPsec
- Updates: Keep everything up to date
- Passwords: Use different passwords stored encrypted
- Monitoring: Use central logging and monitor that
- Auditing: Regular audits by different people

Questions?



© Google Image Search