tblnetworks

SyrinxTechnologies

MOBILE.AGILE.FOCUSED

Security in a Virtualized World

Presented by:

Bryan Miller, Syrinx Technologies

Harley Stagner, TBL Networks

www.theblinkylight.com

4701 cox rd, suite 210 t: (804) 822 3640

glen allen, va 23060 f: (804) 822 3670

Bryan Miller, Syrinx Technologies

Disclaimer

tblnetworks

- The opinions expressed here are the views of the presenter and do not necessarily reflect the views and opinions of TBL Networks.

- I will freely admit that I am not a VMware expert or systems administrator. I focus solely on how to exploit weaknesses in the system. If you see something that doesn't look right, feel free to ask questions.

- I am not perfect, although I try to be and realize I fail miserably. You have been warned.

Agenda

tblnetworks

- Speaker Introductions
- Presentation Introduction
- Systems Administration
- Virtual Vulnerabilities
- Virtualization and Compliance
- Points to Remember
- Links
- Demo
- Q/A

Bryan Miller Introduction

- B.S. – Information Systems – VCU
- M.S. – Computer Science – VCU
- President, Syrinx Technologies since 2007
- Member of ISSA, HIMSS, InfraGard, ILTA
- Adjunct Faculty in Information Systems & Computer Science at VCU, FTEMS lecturer
- CISSP, former CCIE in R/S for 9 years
- Published author
- Over 25 Years in the Industry

Harley Stagner Introduction

tblnetworks

- Account Engineer for TBL Networks
- VMware Certified Design Expert (VCDX) number 46
- First VCDX in Virginia
- Published Author on the topic of virtualization technologies
- Specializing in virtualization technology since 2004

Presentation Introduction

tblnetworks

- Recently attended the SANS 577 Virtualization Security Fundamentals class
  - "VMware is a high performance virtualization platform, it is not a security platform."
- The clear implication is that when a choice was made between performance and security, performance always wins
- This presentation will focus on VMware ESX and ESXi

Quiz #1

tblnetworks

- How many people in the audience think that moving to a virtualized environment improves the overall security posture?
- How many people in the audience think that moving to a virtualized environment is neutral in regards to security?
- How many people think that virtualization makes the security challenge much harder than physical servers?

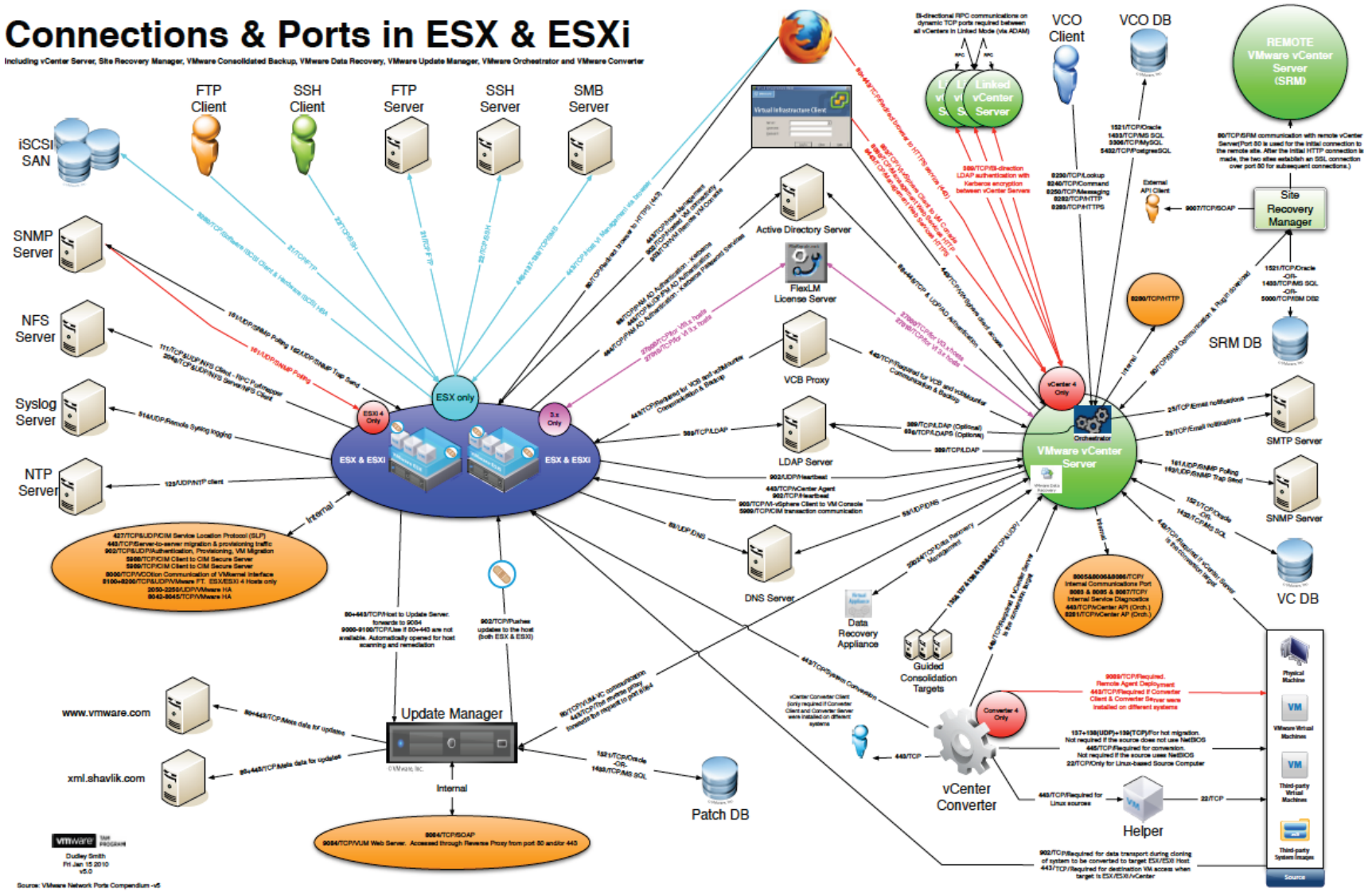
Quiz #2

- Q: On which popular Linux platform is the Service Console for VMware ESX built?
- A: Redhat Enterprise Linux
- Q: On which Linux shell is the VMware ESXi command line built?
- A: BusyBox

System Administration

- VMware Network Ports
- Patching Issues
- Auditing the System
- Hardening the System

VMware Network Ports



tblnetworks

SERIOUSLY???

Patching Issues

tblnetworks

- You must start with patching the Hypervisor
- Then, move onto the various guest OSes
- Next, the major applications
- Don’t forget about the “auxiliary” apps
  - Adobe Reader, Flash, Shockwave
  - iTunes, RealPlayer, Media Player, etc.
- What about patching offline VMs?
  - VMware recently purchased Shavlik
- How about snapshots and host profiles?

Auditing the System

tblnetworks

- How do we know if we're in the Matrix?
  - VMware MAC OUI Prefixes:
    - 00:50:56
    - 00:05:69
    - 00:0C:29
    - 00:1C:14
  - Popular Tools
    - Scoopy/ScoopyNG
    - Jerry
    - Redpill
    - VMDetect

Auditing the System

tblnetworks

- Best Practice Documents
  - VMware vSphere 4.0 Hardening Guide
  - Microsoft Hyper-V Security Guide
  - CIS Benchmarks for ESX
  - CIS Benchmarks for Citrix Xen
  - DISA Security Technical Implementation Guide (STIG) for ESX

- Perform a Virtualization Risk Assessment

Auditing the System

tblnetworks

- Auditing Tools
  - Configuresoft
  - Tripwire
  - DISA Gold disk
  - Core Impact
  - Tenable Nessus
  - Metasploit
  - Foundstone VIDigger

Hardening the System

tblnetworks

- NIC allocation
  - 2 NICs, 4 NICs, 6 NICs or even 8 NICs
    - Production traffic
    - Service Console traffic
    - VMKernel traffic
- Use vSwitch to properly VLAN traffic
  - 3 different DMZ models proposed by VMware

Hardening the System

- Start by hardening the vCenter host
  - By default, local Windows Administrators group has administrative access to vCenter
    - Create a local user, grant full Admin role and remove local Administrators group from vCenter
    - Create a domain Global group for all vCenter admins, add this to a new local group and grant the new local group vCenter administrative access
  - Restrict network port access
    - TCP 443 – vSphere client access to vCenter
    - TCP/UDP 902/903 – used by different applications

Hardening the System

tblnetworks

- vCenter Databases
  - Oracle 10g and 11g
  - MS SQL Server 2005 SP2 & 2008
- Databases should be on a separate server
- Default Oracle accounts are installed
- Watch those default passwords!
- Review roles & privileges

Hardening the System

tblnetworks

- Logging
  - Monitor vCenter logs and set the logging level to “Warning”
  - ESX Log Rotation
    - Default 36 month – can be used to crash partition
- Configure banners for legal purposes
  - /etc/issue
  - /etc/issue.net
  - /etc/issue.emergency
  - /etc/motd
  - /etc/ssh/sshd_config
- IPTables can be used in ESX to modify firewall rules
  - vCenter will not show any changes made by IPTables

Hardening the System

tblnetworks

- Modify ESX access controls as needed
  - SSH
  - TCP Wrappers
  - GRUB password for single-user mode access
  - Some users & groups can be removed
  - Limit root console logon
  - Configure *sudo*
  - Disable unneeded services
  - Secure SNMP
    - ESX supports 1, 2c & 3 while ESXi supports 1 & 2c
  - Disable removable media

Hardening the System

tblnetworks

- Modify ESXi access controls as needed
  - No built-in firewall
  - No TCP Wrappers
  - No audit/monitoring tools built-in
  - Secure the management console
  - Set a root password
  - Investigate “Lockdown Mode”
  - Enable syslog through PowerCLI
  - Change root password via PowerCLI

Hardening the System

tblnetworks

- Modify guest access controls as needed
  - Start with the OS
  - You can disable Guest<->Host copy & paste
  - Log management
  - Disable unnecessary devices
  - Prevent connection & removal of devices if needed

Virtual Vulnerabilities

tblnetworks

- Virtualization Threats
  - VM Sprawl
    - Where exactly are my servers/data?
  - Lack of Visibility
    - How do we monitor inter-VM traffic?
  - Separation of Duties
    - Who manages what aspects of the virtual world?
  - Rights/Privileges
    - How do we manage access without giving away too many rights?

Virtual Vulnerabilities

tblnetworks

- July 28, 2011 VMSA-2011-0010
- June 2, 2011 VMSA-2011-0009
- May 5, 2011 VMSA-2011-0008
- April 28, 2011 VMSA-2011-0007
- April 28, 2011 VMSA-2011-0001.2
- April 12, 2011 VMSA-2011-0005.2
- March 29, 2011 VMSA-2011-0006.1
- March 7, 2011 VMSA-2011-0004.1
- February 10, 2011 VMSA-2011-0003.2
- February 7, 2011 VMSA-2011-0002

Virtual Vulnerabilities

tblnetworks

- Ed Skoudis & Tom Liston – SANSFIRE 2007
  - VMchat : allows VMware guests to chat with each other over the VMware communications channel
  - VMftp : allows VMware guests to transfer files back and forth using the VMware communications channel
  - VMdrag-n-sploit : extends these tools to include chat, ftp, and execute between a guest and host
  - VMcat : can be used to “tunnel” a command shell between guests and hosts

Virtualization and Compliance

- To date, only PCI has specifically outlined how virtualization should be handled by auditors.
- In June 2011, the PCI Security Standards Council (SSC) Virtualization Special Interest Group released:
  - Information Supplement: PCI DSS Virtualization Guidelines
- First release of guidelines on how virtualization affects PCI compliance.

Virtualization and Compliance

- PCI 2.2.1 - Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.)

  Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.

- Scoping Guidelines:
  - Hypervisor
    - If any virtual component connected to (or hosted on) the hypervisor is in scope for PCI DSS, the hypervisor itself will always be in scope.
  - Guest
    - An entire VM will be in scope if it stores, processes or transmits cardholder data, or if it connects to or provides an entry point into the CDE. If a VM is in scope, both the underlying host system and the hypervisor would also be considered in scope, as they are directly connected to and have a fundamental impact on the functionality and security of the VM.

- Scoping Guidelines:
  - Virtual Switch
    - Networks provisioned on a hypervisor-based virtual switch will be in scope if provisioned with an in-scope component or if they provide services or connect to an in-scope component. Physical devices hosting virtual switches or routers would be considered in scope if any of the hosted components connects to an in-scope network.
  - Virtual Desktops/Applications
    - Virtual applications and desktops will be in scope if they are involved in the processing, storage, or transmission of cardholder data, or provide access to the CDE.

- General Recommendations:
  - Be very careful when mixing guests containing different levels of sensitive data.
    - In the virtual context, a VM of lower trust will typically have lesser security controls than VMs of higher trust levels
  - Recognize dormant VMs and ensure they are properly protected.
    - Dormant VMs are also unlikely to have up-to-date access policies and may be excluded from security and monitoring functions, possibly creating an unchecked back-door to the virtual environment.

Points to Remember

tblnetworks

- There are no forensics tools that work with VMFS.
- You can’t easily recover deleted files from VMFS.
- VMotion & SVMotion don’t have granular bandwidth management.
- Make sure DNS and NTP are setup correctly.
- You can create users directly on the hosts that do not show up in vCenter.

Links

- VMware
  - http://www.vmware.com/security/advisories

- Others
  - http://packetstormsecurity.org/search/?q=vmware
  - http://labs.idefense.com/intelligence/vulnerabilities
  - http://secunia.com/advisories/vendor/300/
  - https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

Links

- VMware
  - http://www.vmware.com/security/advisories

- Others
  - http://packetstormsecurity.org/search/?q=vmware
  - http://labs.idefense.com/intelligence/vulnerabilities
  - http://secunia.com/advisories/vendor/300/
  - https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf

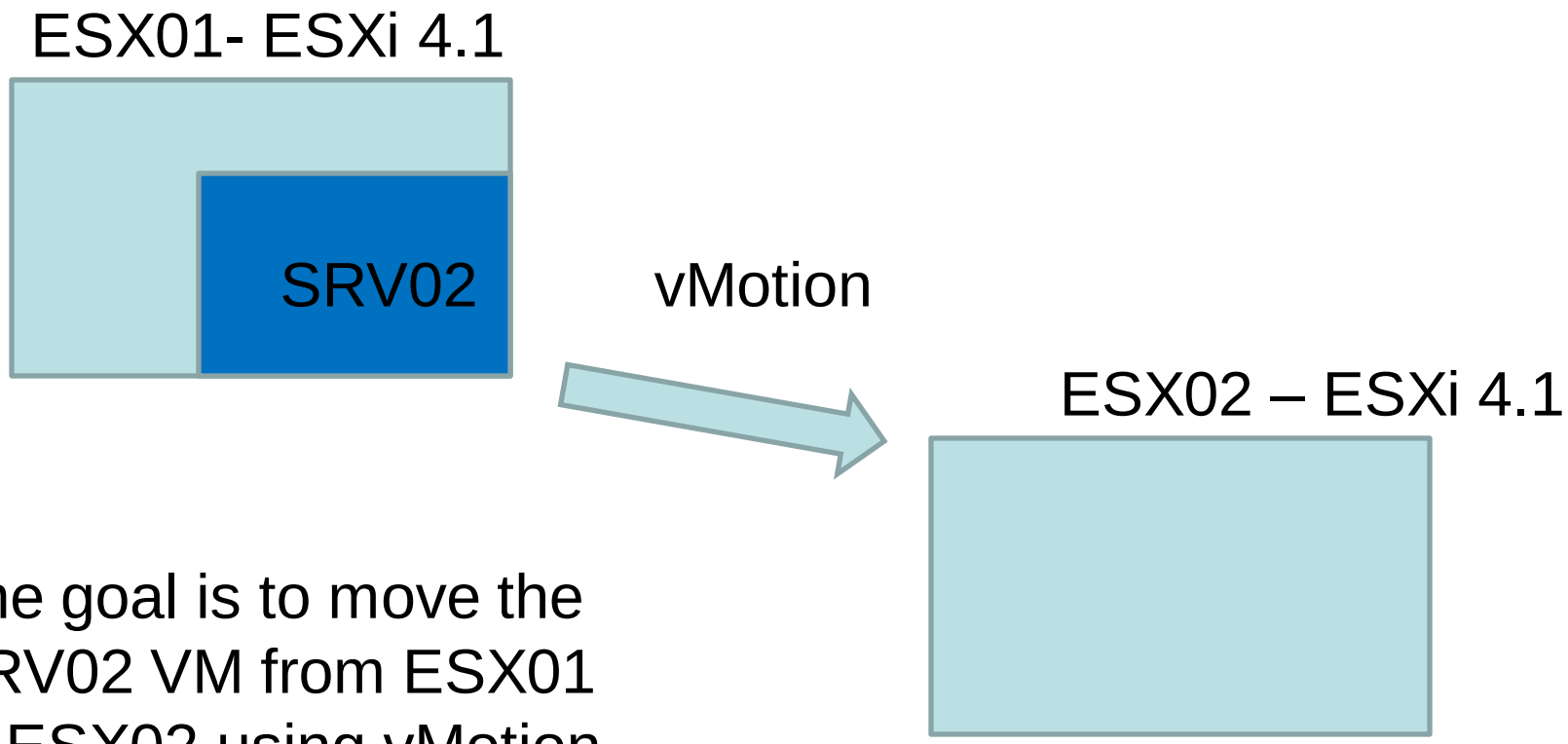
Quiz #3

tblnetworks

- Q: How many people think that there is no command-line support in ESXi?

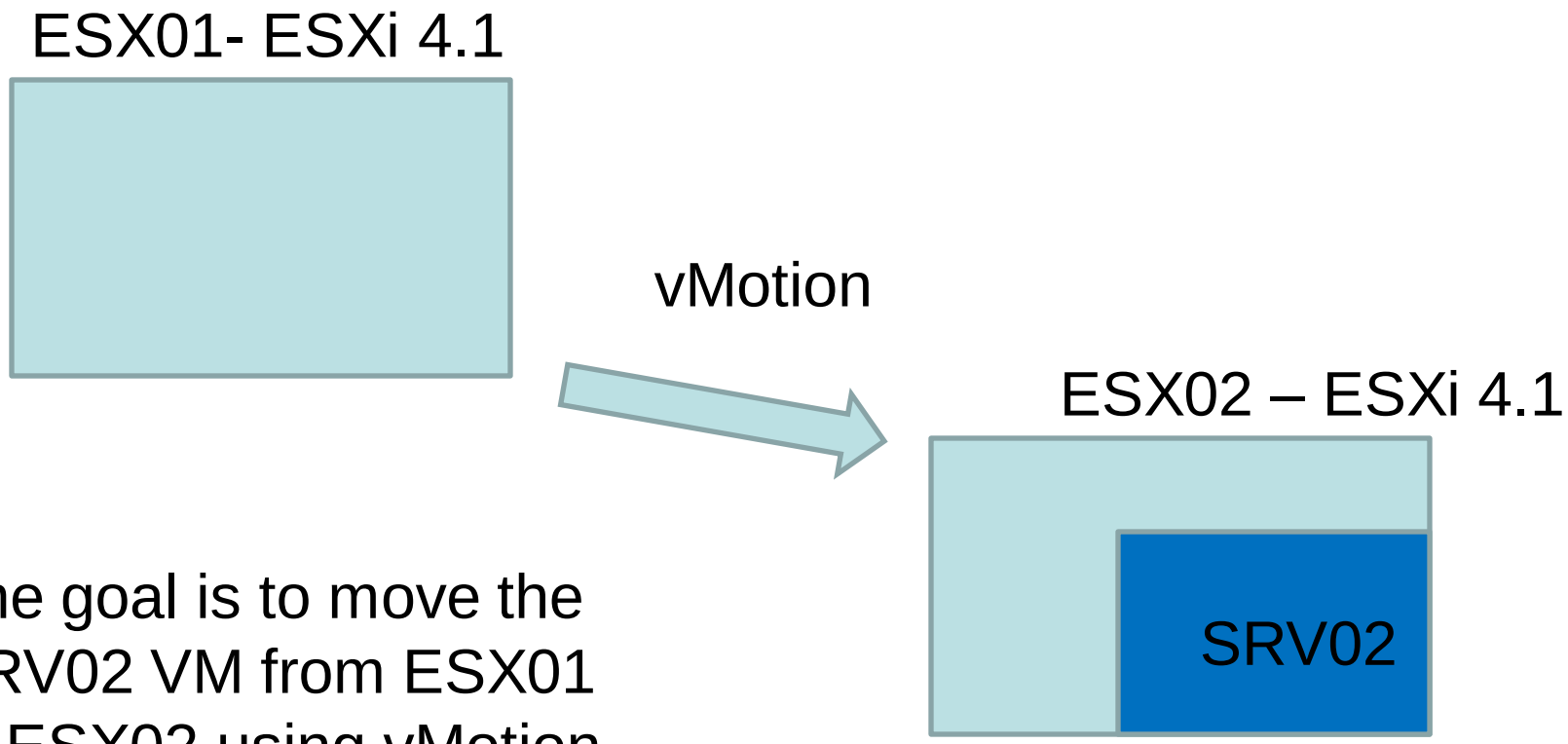
- A: Press ALT-F1 at main screen, type the magic phrase (depending on version) and you should see a login prompt.
  - The root password is blank by default, just press ENTER.

Demo - vMotion



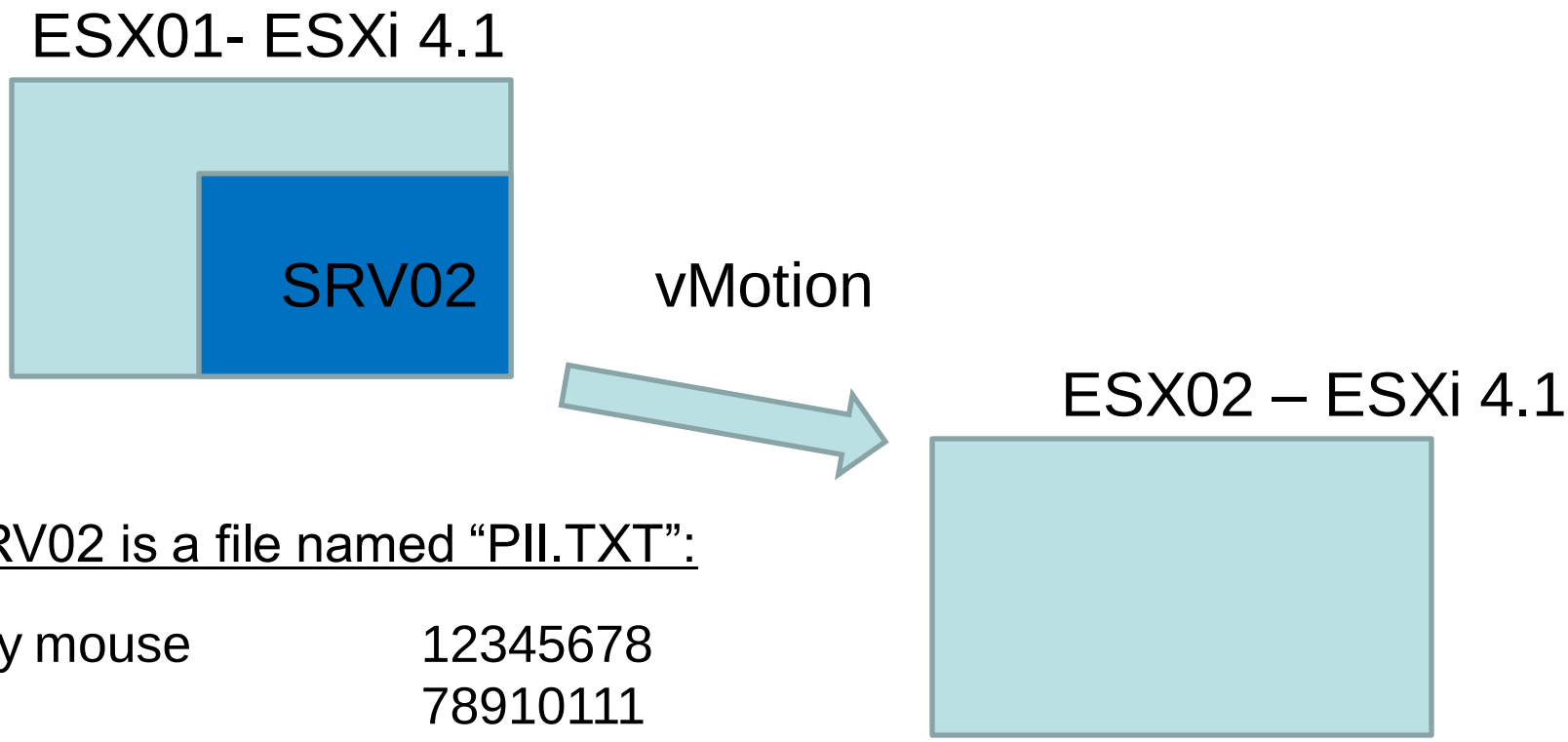
The goal is to move the SRV02 VM from ESX01 to ESX02 using vMotion.

Demo - vMotion



The goal is to move the SRV02 VM from ESX01 to ESX02 using vMotion.

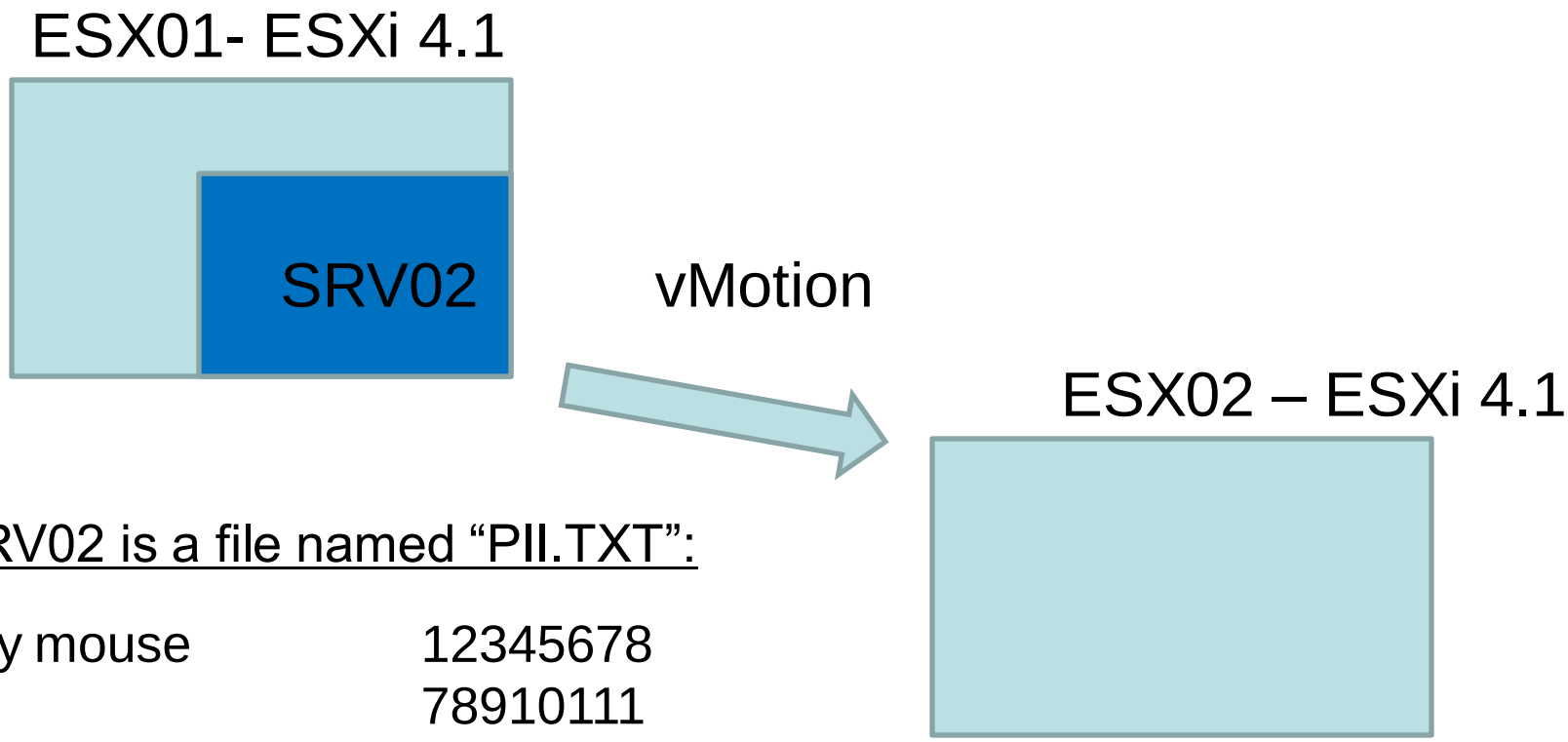
Demo - vMotion



On SRV02 is a file named “PII.TXT”:

mickey mouse	12345678
goofy	78910111
minney mouse	12131415

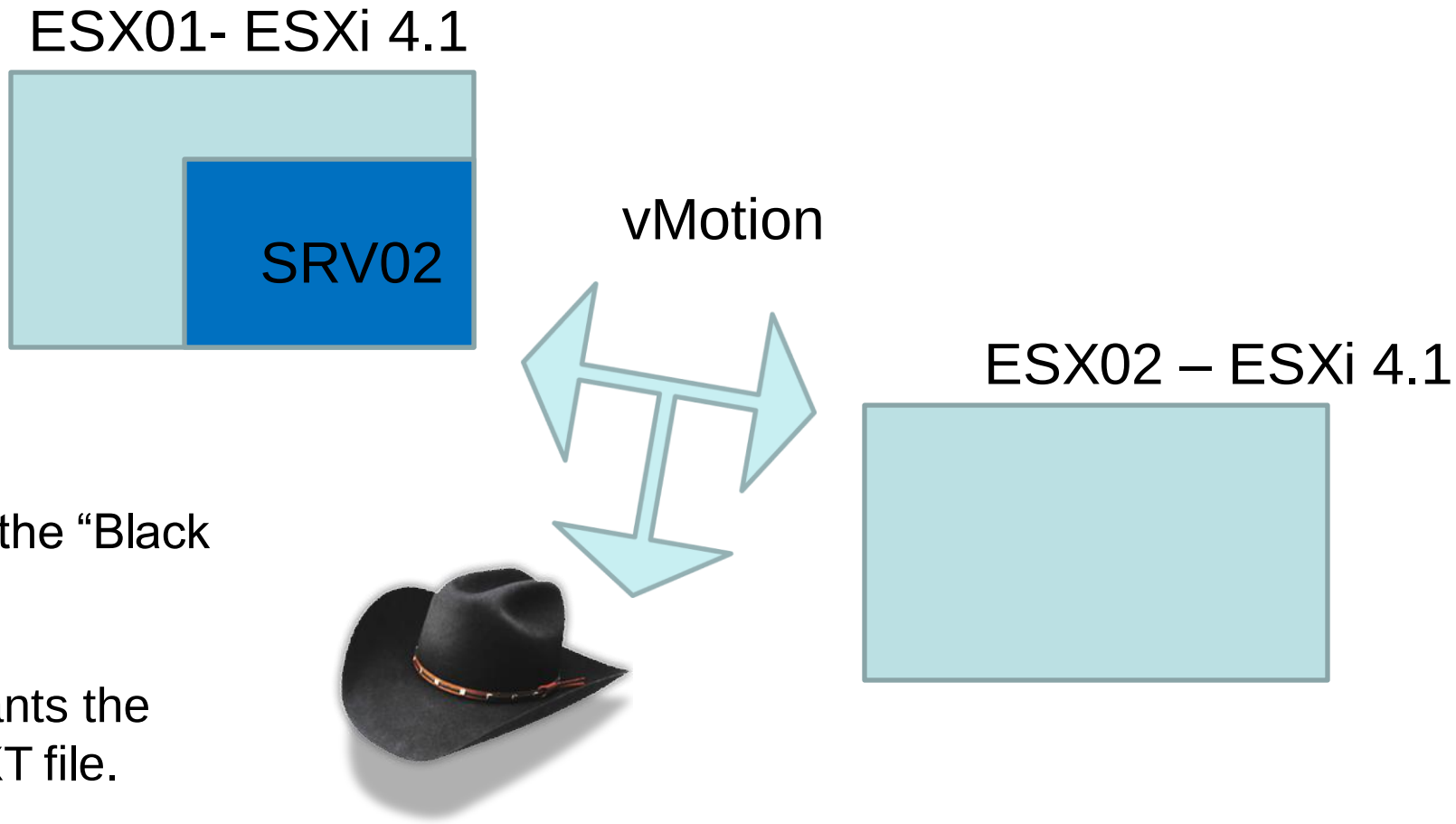
Demo - vMotion



On SRV02 is a file named “PII.TXT”:

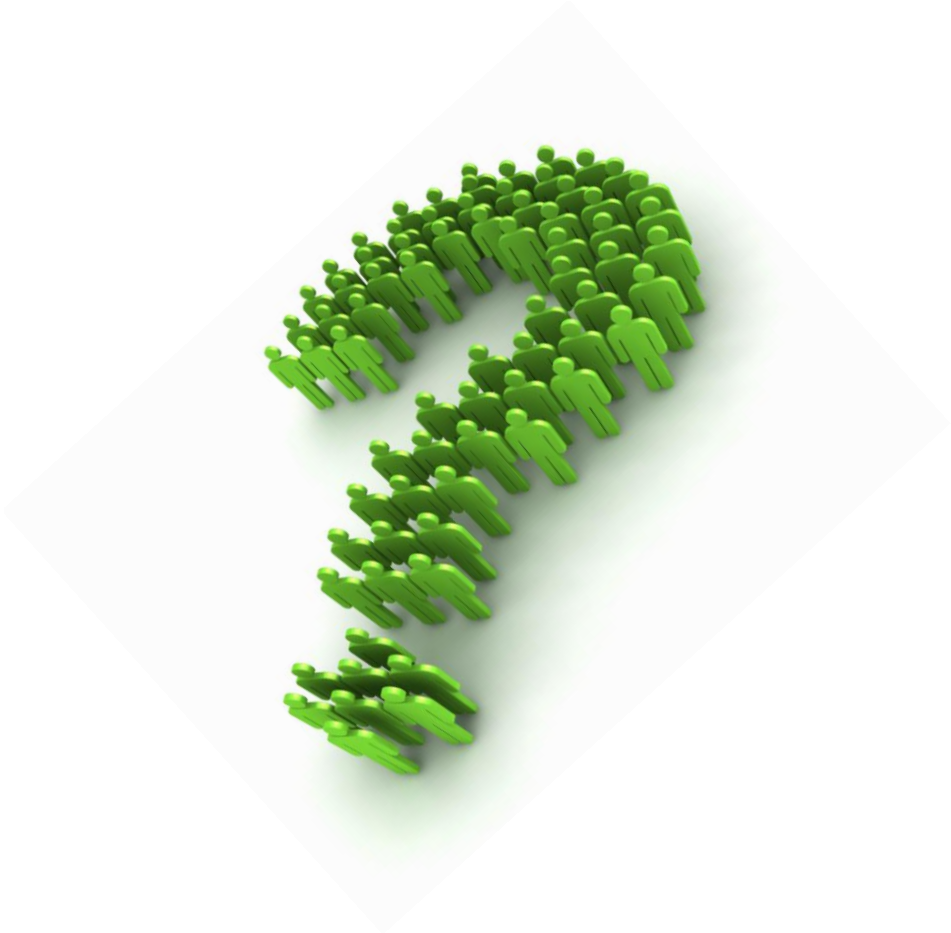
mickey mouse	12345678
goofy	78910111
minney mouse	12131415

Demo - vMotion



Enter the “Black Hat”.

He wants the PII.TXT file.




tbl
TM