Scanning a Clone in the Cloud; Safe DCS Vulnerability Scanning

Bernard Pella

Savannah River Nuclear Solutions

ICSJWG 2010 Spring Conference

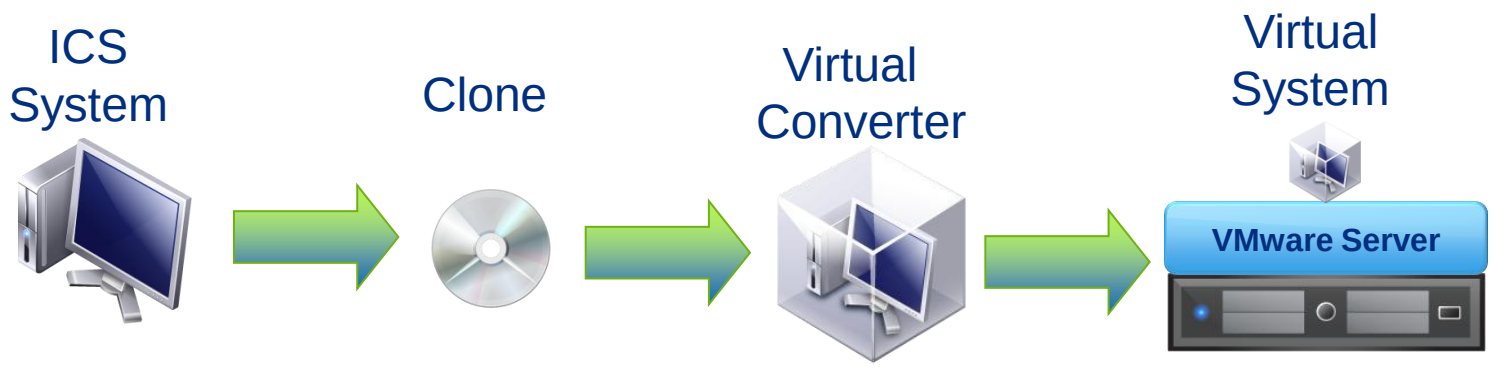
SRS Public Release Document Number: SRNS-CSP-2010-00013

Introduction

- Vulnerability scanning is the preferred method to identify vulnerabilities on computer systems
- Vulnerability scanning tools have the potential to cause unexpected and undesirable actions when used on production industrial control systems
- A method of validating vulnerability and patch remediation on production industrial control systems was desired at the Savannah River Site
- The method of scanning a clone of the system in a virtual environment was developed and tested to resolve the scanning of production industrial control systems

Virtual Scanning

- Virtual Scanning is the use of an image (clone) of a ICS and loading the image in a virtual environment (cloud) then scanning the virtual system using a vulnerability scanning tool.



Equipment and Software Needed

- Equipment
  - Industrial Control System
  - Server
- Software
  - Image software compatible with VM Converter
  - VMServer by VMware
  - Windows Server Operating System (2003 or 2008)
  - VMConverter

Process Overview

- Use Acronis to generate backup images (.tib)
- Transfer Image files via removable storage to Cloud machine
- Transfer image file to Cloud computer and run through VMConverter
- Launch VM session with converted file into VM space
- Run vulnerability scans and save scan results
- Save converted VM session for archive and restoration purposes

From TIB to VM Scan

- Use restore function to apply to the tib image to the VMServer (true image backup)
- Apply appropriate settings/locations
- Create the OVF (Open Virtualization File) which is .vmdk (virtual machine disk) and .vmx (virtual configuration)
- Open VMconverter to convert .vmx and .vmdk
- Apply VMware tools and allocate resources (hard drive space, memory, processors
- Populates status through the conversion process
- Add the newly created/converted virtual machine to the inventory of the VMserver
- Start the VM session, login and perform scan

Scanning Results

- Cloud vulnerability scans provide reliable results for patch installation
- Cloud vulnerability scans do not provide accurate port or network device scans
- Scanning is always a privileged scan in the cloud

Issues with Cloud Scanning

- Windows activation is required by some operating systems
  - Some versions of Windows Server 2003 require immediate activation some give 3 days and some don't require activation
- Windows EULA (End User License Agreement) may require additional copies of operating system
- Windows DataCenter resolved many activation and EULA issues
- Administrator rights/privileges are needed to load and scan clone

Benefits of Cloud Scanning

- A production industrial control system can be checked for vulnerabilities without an impact to facility operations
- The clone provides a copy of operating system, driver and specialty files for use in failure recovery
  - Most backup data regularly
  - Most do not backup OS and other files
- The clone provides a restore point when patching goes bad
- A clone is easier to perform than running vulnerability scans

Summary

- A clone of a production industrial control system can be loaded into the cloud and safely scanned for vulnerabilities
- The clone provides a backup of operating system, driver and specialty files for restoration from a hardware failure

Credits

- Christopher Desrocher, Savannah River Site, Savannah River Nuclear Solutions, Process Controls Cyber Security
- Hasan Syed, Savannah River Site, Savannah River Nuclear Solutions, Process Controls Cyber Security

Contact Information

- Bernard (Bernie) Pella, GSLC
- Savannah River Nuclear Solutions, Savannah River Site
- Process Controls and Engineering Automation
- E-Mail bernie.pella@srs.gov
- Phone (803) 208-8041

References

- NIST 800-82, Guide to Industrial Control Systems (ICS) Security
- NIST 800-53, Recommended Security Controls for Federal Information Systems
- Microsoft.com websites for technical information
- VMware.com websites for technical information