ANSIBLE FOR SERVER HARDENING

Making Security Procedures and Compliance less painful

Adam Miller
Principal Software Engineer

AGENDA

AGENDA

WHAT WE’RE GOING TO TALK ABOUT TODAY

- What do we mean by “Security”?
- Why Ansible?
- Compliance and Guideance
- Auditing
- Server Hardening Projects with Ansible
- Further Learning

SECURITY?

SECURITY?

What?

Server Hardening for SysAdmins

- SysAdmins vs SecOps
  - Traditionally disjoint roles and responsibilities
  - SysAdmins harden systems
    - Also manages infrastructure, deploys and maintains systems, etc
  - SecOps checks to make sure systems are hardened
    - Also tracks ongoing threats, IDS, firewall management, etc
- Things I don’t contextually mean by Security for this talk:
  - SecOps
  - Red Team
  - Pen Testing

WHY?

Why?

…. on Earth?

Ansible is an Automation Tool

- System hardening is something we (should) do for all systems
- This leads to repetitive work as you:
  - bring systems online
  - take systems offline
  - face new threats
  - Deploy new apps
- Moral of the story: it’s not special, it’s just another thing to automate

COMPLIANCE

COMPLIANCE

Everyone’s favorite pass time

Federal Information Processing Standards (FIPS)

- Standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors
- FIPS 140 Security requirements for cryptography modules
- FIPS 153 (3D graphics)
- FIPS 197 (Rijndael / AES cipher)
- FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
- FIPS 201 Personal Identity Verification for Federal Employees and Contractors

GUIDANCE

Don’t step on toes .. left, left, right

Security Technical Implementation Guide (STIG)

- Configuration standards for DOD IA and IA-enabled devices/systems
- Comes from the Defense Information Systems Agency (DISA), part of the United States Department of Defense.
- The guide is released with a public domain license and it is commonly used to secure systems at public and private organizations around the world.
- System and Version/Release specific
  - RHEL 7 STIG Version 1, Release 3 (Published on 2017-10-27)
  - RHEL 7 STIG Version 1, Release 1 (Published on 2017-02-27)

AUDITING

AUDITING

Everyone’s *other* favorite pass time

Security Content Automation Protocol (SCAP)

- method for using specific standards to enable the automated vulnerability management, measurement, and policy compliance evaluation of systems
    - Common Vulnerabilities and Exposures (CVE)
    - Common Configuration Enumeration (CCE) (prior web-site at MITRE)
    - Common Platform Enumeration (CPE)
    - Common Vulnerability Scoring System (CVSS)
    - Extensible Configuration Checklist Description Format (XCCDF)
    - Open Vulnerability and Assessment Language (OVAL)
    - Open Checklist Interactive Language (OCIL) Version 2.0
    - Asset Identification (AID)
    - Asset Reporting Format (ARF)
    - Common Configuration Scoring System (CCSS)
    - Trust Model for Security Automation Data (TMSAD)

AUDITING

Everyone’s *other* favorite pass time

SCAP

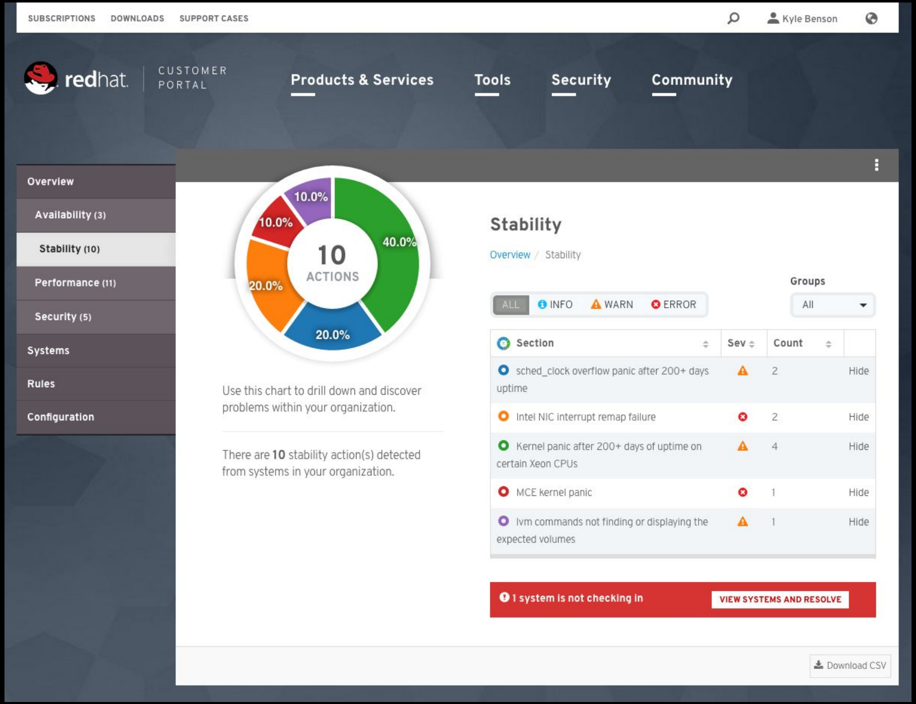
- OpenSCAP
    - An implementation of SCAP
    - Scans
    - Audits
    - Provides remediation recommendations/instructions
    - Defacto-standard in opensource/Linux land
    - https://www.open-scap.org/
- OpenSCAP + Ansible
    - OpenSCAP can audit and generate Ansible Playbooks for remediation
    - https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sect-using_openscap_with_ansible

AUDITING

Everyone’s *other* favorite pass time

Red Hat Insights

- Predictive Analytics powered by Ansible
- https://www.redhat.com/en/technologies/management/insights



Use this chart to drill down and discover problems within your organization.

There are **10** stability action(s) detected from systems in your organization.

Stability

Overview / Stability

Section	Sev	Count	
sched_clock overflow panic after 200+ days uptime	⚠	2	Hide
Intel NIC interrupt remap failure	☒	2	Hide
Kernel panic after 200+ days of uptime on certain Xeon CPUs	⚠	4	Hide
MCE kernel panic	☒	1	Hide
lvm commands not finding or displaying the expected volumes	⚠	1	Hide

1 system is not checking in

ANSIBLE HARDENING

USING ANSIBLE TO HARDEN SYSTEMS

ONE DOES NOT SIMPLY WALK INTO MORDOR

Ansible Lockdown

- Official Subproject of Ansible done in partnership with MindPoint Group
  - https://github.com/ansible/ansible-lockdown
- Community focused mailing list
  - https://groups.google.com/forum/#!forum/ansible-lockdown
- Covers STIG for the following Operating Systems
  - RHEL 6
  - RHEL 7
  - Windows Server 2012 DC
  - Windows Server 2012 MS
  - Windows Server 2008R2 MS

USING ANSIBLE TO HARDEN SYSTEMS

ONE DOES NOT SIMPLY WALK INTO MORDOR

Ansible Hardening

- DISA STIG Implementation, Checks, and Audit tool built with Ansible
- Sub project of OpenStack (though extends far beyond OpenStack's scope)
- Support for many distros
  - CentOS 7, Debian Jessie, Fedora 27, openSUSE Leap 42.2 and 42.3, Red Hat Enterprise Linux 7, SUSE Linux Enterprise 12 (experimental), Ubuntu 16.04
- https://github.com/openstack/ansible-hardening
-

USING ANSIBLE TO HARDEN SYSTEMS

ONE DOES NOT SIMPLY WALK INTO MORDOR

Dev-Sec.io (DevOps + Security)

- Security Hardening Community
  - Notable members: T-Mobile, Benocs, Convergint Technologies
- Provide Security Hardening Automation for Ansible, Puppet, and Chef
- Follows NSA Information Assurance, STIG, Deutsche Telekom, Group IT Security, Security Requirements, Arch Security, and Ubuntu Security Guidelines
- Support for many distros
  - RHEL/CentOS 6 and 7, Amazon Linux 1 and 2, Debian Jessie and Wheezy, Ubuntu Precise/Trusty/Xenial
- https://dev-sec.io/

LEARNING

Ansible + Security Resources

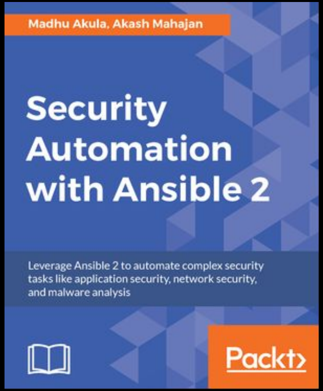
Books and stuff...

Security Automation with Ansible 2

- Book written by Madhu Akula and Akash Mahajan, published by Packt Pub
- Covers a lot of what we covered today but also Pen Testing topics, Forensics, containers, malware analysis, and more.

Companion Udemy Course

- Getting Started with Ansible 2 Security Automation
- https://www.udemy.com/getting-started-with-ansible-2-security-automation



Madhu Akula, Akash Mahajan

Security Automation with Ansible 2

Leverage Ansible 2 to automate complex security tasks like application security, network security, and malware analysis

Packt>

NOTE: I have no affiliation with the authors, nor do the authors have any affiliation with the Ansible Project or Red Hat.

THANK YOU

ADAM MILLER

maxamillion

maxamillion

@TheMaxamillion