Security Automation with Ansible

Michelle Perz, Associate Manager-Ansible Support, Ansible by Red Hat
AGENDA

Ansible use cases
Information security
Why Ansible?
Examples
Get involved
COMMON ANSIBLE USE CASES

Configuration Management
Continuous Integration/Delivery
Orchestration
Infrastructure Provisioning
Application Deployment
COMMON ANSIBLE USE CASES

- Configuration Management
- Continuous Integration/Delivery
- Orchestration
- Infrastructure Provisioning
- Security Automation
- Application Deployment
Application Security
Network Security
Forensics
Incident Response
Penetration Testing
Fraud Detection and Prevention
Governance, Risk, Compliance
SECURITY IS HARD

People

Processes

Technology

Economics

FreeImages.com/tijamen
UNICORN
WHY ANSIBLE FOR SECURITY AUTOMATION?

Agentless
SSH/WinRM
Desired State
Extensible and modular
Push-based architecture
Easy targeting based on facts
NOT ZERO SUM

\[ A + 12 \neq 0 \]

ANSIBLE
WHY ANSIBLE?

Developers

Operations

Security Team
Security Technical Implementation Guides (STIG)
Payment Card Industry Data Security Standard (PCI DSS)
Remediation
Internal Standards
Incident Response
**Rule Title:** The SSH daemon must not allow authentication using an empty password.

**Fix Text:** To explicitly disallow remote logon from accounts with empty passwords, add or correct the following line in "/etc/ssh/sshd_config":

```
PermitEmptyPasswords no
```

```yaml
- name: "HIGH | RHEL-07-010270 | PATCH | The SSH daemon must not allow authentication using an empty password."
  lineinfile:
    state: present
    dest: /etc/ssh/sshd_config
    regexp: ^#?PermitEmptyPasswords
    line: PermitEmptyPasswords no
    validate: sshd -tf %s
    notify: restart sshd
```
Rule Title: The operating system must implement address space layout randomization to protect its memory from unauthorized code execution.

Fix Text:
Check the kernel setting for virtual address space randomization with the following command:

```bash
# /sbin/sysctl kernel.randomize_va_space
```

```
sysctl

name: kernel.randomize_va_space
value: 2
state: present
reload: yes
ignoreerrors: yes
notify: reboot system
```

- name: "MEDIUM | RHEL-07-020190 | PATCH | The operating system must implement address space layout randomization to protect its memory from unauthorized code execution."

```bash
sysctl:
  name: kernel.randomize_va_space
  value: 2
  state: present
  reload: yes
  ignoreerrors: yes
  notify: reboot system
```
Rule Title: The network element must only allow management connections for administrative access from hosts residing in to the management network.

Fix Text: Configure an ACL or filter to restrict management access to the network from only the management network.

- hosts: ios
  connection: local
  gather_facts: false

tasks:
- name: Create management ACL
  ios_config:
    parents: ip access-list mgmnt
    before: no ip access-list mgmnt
    lines:
    - 10 permit ip host 192.168.1.99 log
    - 20 permit ip host 192.168.1.121 log
  provider: "{{ login_info }}"

- name: Harden VTY lines
  ios_config:
    parents: line vty 0 15
    lines:
    - exec-timeout 15
    - transport input ssh
    - access-class mgmnt in
  provider: "{{ login_info }}"
**Rule Title:** Anonymous enumeration of shares must be restricted.

**Fix Text:** Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Do not allow anonymous enumeration of SAM accounts and shares" to "Enabled".

```yaml
- hosts: windows
  tasks:
    - name: Restrict enumeration of shares
      win_regedit:
        key: 'HKLM\System\CurrentControlSet\Control\Lsa'
        value: RestrictAnonymous
        data: 1
        datatype: dword
```
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

- name: RHEL | Install updates
  yum:
    name: "*"
    state: latest
    exclude: "mysql* httpd* nginx*"
  when: "ansible_os_family == 'RedHat'"

- name: DEBIAN | Install updates
  apt:
    update_cache: yes
    cache_valid_time: 7200
    name: "*"
    state: latest
  when: "ansible_os_family == 'Debian'"
- name: Protect against CVE-2016-5696
  hosts: all
  become: yes
  become_user: root

tasks:
  - name: CVE-2016-5696 | Limit TCP challenge ACK limit
    sysctl:
      name: net.ipv4.tcp_challenge_ack_limit
      value: 999999999
      sysctl_set: yes
- name: Protect against CVE-2018-5390 | CVE-2018-5391
  hosts: all
  become: yes
  become_user: root

tasks:
  - name: Protect against SegmentSmack and FragmentSmack
    sysctl:
      name: "{{item.name}}"
      value: "{{item.value}}"
      state: present
    loop:
      - { name: 'net.ipv4.ipfrag_high_thresh', value: '262144' }
      - { name: 'net.ipv4.ipfrag_low_thresh', value: '196608' }
- name: Protect against MacOS High Sierra root bug
  hosts: macs
  become: yes

  tasks:
  - name: change root password
    user:
      name: root
      update_password: always
      password: "{{root_password |password_hash('sha512')}}"

  - name: address CVE-2017-13872
    command: "softwareupdate -i 'Security Update 2017-001'"

  - name: reboot after security updates
    reboot:
name: Patch Linux systems against Meltdown and Spectre
hosts: "{{ target_hosts | default('all') }}"
become: yes

vars:
  reboot_after_update: no
  packages:
    # https://access.redhat.com/security/vulnerabilities/speculativeexecution
    RedHat7:
      - kernel-3.10.0-693.11.6.el7
      - microcode_ctl-2.1-22.2.el7
      - perf-3.10.0-693.11.6.el7
      - python-perf-3.10.0-693.11.6.el7
    RedHat6:
      - kernel-2.6.32-696.18.7.el6
      - kernel-firmware-2.6.32-696.18.7.el6
      - perf-2.6.32-696.18.7.el6
      - python-perf-2.6.32-696.18.7.el6

tasks:
  - name: RHEL | Install kernel updates
    yum:
      name: "{{ packages[ansible_os_family ~ ansible_distribution_major_version] }}"
      state: present
      when: ansible_pkg_mgr == 'yum'
    notify: reboot system
- name: Gather log files from remote systems
  hosts: lab
  become: yes

tasks:
  - name: Find logs
    find:
      paths: /var/log/
      patterns: '*.log'
      recurse: yes
      register: _logs

  - name: Fetch logs
    fetch:
      src: "{{ item.path }}"
      dest: logs
      with_items: "{{ _logs.files }}"
INTERNAL STANDARDS

Change root password every 60 days

- name: Change root password
  hosts: all
  become: yes

vars:
  root_password: "{{ vault_root_password }}"
  root_password_salt: "{{ vault_root_password_salt }}"

tasks:
  - name: Change root password
    user:
      name: root
      password: "{{ root_password | password_hash(salt=root_password_salt) }}"
ANSIBLE SECURITY AUTOMATION
ENTERPRISE FIREWALLS

SIEM

IDS/IPS

NAC

ENDPOINT PROTECTION PLATFORMS

THREAT INTELLIGENCE PLATFORMS

SECURE WEB GATEWAYS

SECURE EMAIL GATEWAYS
GET INVOLVED

Ansible Lockdown
Ansible Hardening
Mailing List
Ansible Galaxy

https://github.com/samdoran/demo-playbooks
THANK YOU!

Michelle Perz, Associate Manager-Ansible Support, Ansible by Red Hat