DevSec Baselines

Overview

DevSec offers a range of baseline tests for configuring basic security across various applications. These can be ran via commandline or manually reviewed at dev-sec.io

> These baseline tests requires Inspec to be installed. If you don't have it installed, it can be grabbed for RHEL, Ubuntu, and Mac using the following command.
> `curl https://omnitruck.chef.io/install.sh | sudo bash -s -- -P inspec`

Required Configuration / Installations

To run a baseline test, grab the required repository from the DevSec GitHub and run the following command
`inspec exec BASELINETEST`

For example, to run SSH-Baseline, just run the following

```
# Don't forget to install Inspec
# curl https://omnitruck.chef.io/install.sh | sudo bash -s -- -P inspec
git clone https://github.com/dev-sec/ssh-baseline
inspec exec ssh-baseline
```

> When running these baselines, they will output the results as test success and failures in green and red, respectively. Some tests may be *intended* to fail in order to meet security needs. The ssh-baseline test sshd-07 will output an intended error if you have modified your `/etc/sshd_config` to use a custom port instead of the default 22. For example, if you have changed your SSH port to 999, the following error will be displayed.
>
> Note that the similar test, ssh-07, is not the same and refers to the configuration stored at `/etc/ssh/ssh_config`

```
  ×  sshd-07: Server: Specify the listen ssh Port
     ×  SSHD Configuration Port should eq "22"


     expected: "22"
```

```
       got: "999"
```

If you are unsure if the results of a test should be a concern, check the description on the baseline's overview page. For ssh-baseline, test sshd-07 has the following description.

```
control 'sshd-07' do
  impact 1.0
  title 'Server: Specify the listen ssh Port'
  desc 'Always specify which port the SSH server should listen to. Prevent unexpected settings.'
  describe sshd_config do
    its('Port') { should eq('22') }
  end
end
```

You can see by the description above that this test is intended to alert you to always specify your port within `/etc/sshd_config`

Running the SSH-Baseline Test

When initially running this test, first be sure to check your file can be read by inspec by checking the permission checks output when running `sudo inspec exec ssh-baseline`

```
...

✔  sshd-04: Server: Check SSH folder owner, group and permissions.
     ✔  File /etc/ssh should exist
     ✔  File /etc/ssh should be directory
     ✔  File /etc/ssh should be owned by "root"
     ✔  File /etc/ssh should be grouped into "root"
     ✔  File /etc/ssh should be executable
     ✔  File /etc/ssh should be readable by owner
     ✔  File /etc/ssh should be readable by group
     ✔  File /etc/ssh should be readable by other
     ✔  File /etc/ssh should be writable by owner
     ✔  File /etc/ssh should not be writable by group
     ✔  File /etc/ssh should not be writable by other
  ✔  sshd-05: Server: Check sshd_config owner, group and permissions.
     ✔  File /etc/ssh/sshd_config should exist
     ✔  File /etc/ssh/sshd_config should be file
     ✔  File /etc/ssh/sshd_config should be owned by "root"
     ✔  File /etc/ssh/sshd_config should be grouped into "root"
```

```
    ✔  File /etc/ssh/sshd_config should not be executable
    ✔  File /etc/ssh/sshd_config should be readable by owner
    ✔  File /etc/ssh/sshd_config should not be readable by group
    ✔  File /etc/ssh/sshd_config should not be readable by other
    ✔  File /etc/ssh/sshd_config should be writable by owner
    ✔  File /etc/ssh/sshd_config should not be writable by group
    ✔  File /etc/ssh/sshd_config should not be writable by other


...


  ✔  ssh-01: client: Check ssh_config owner, group and permissions.
    ✔  File /etc/ssh/ssh_config should exist
    ✔  File /etc/ssh/ssh_config should be file
    ✔  File /etc/ssh/ssh_config should be owned by "root"
    ✔  File /etc/ssh/ssh_config should be grouped into "root"
    ✔  File /etc/ssh/ssh_config should not be executable
    ✔  File /etc/ssh/ssh_config should be readable by owner
    ✔  File /etc/ssh/ssh_config should be readable by group
    ✔  File /etc/ssh/ssh_config should be readable by other
    ✔  File /etc/ssh/ssh_config should be writable by owner
    ✔  File /etc/ssh/ssh_config should not be writable by group
    ✔  File /etc/ssh/ssh_config should not be writable by other


...
```

Revision #5
Created 4 May 2019 15:09:00 by Shaun Reed
Updated 20 May 2020 07:06:31 by Shaun Reed