Chromium Policy

## Summary

This lab demonstrates policies that enterprises can implement to control the behavior of Chromium based browsers. The current set of policies can be found here: <https://chromeenterprise.google/policies/>

OpenSCAP has developed a Security Technical Implementation Guide (STIG) for Chromium here: <https://static.open-scap.org/ssg-guides/ssg-chromium-guide-index.html>

As the administrator of your enterprise, you will implement the STIG based policy and observe changes in Chrome behavior.

## Tools/Resources

Parrot: Chrome(install required), various command line tools.

## Walkthrough

1. Install Chrome
2. Add policy
   1. Create /etc/chromium/policies/managed/chrome\_stig\_policy.json with the following text:

{

"PluginsAllowedForUrls": "none",

"ShowHomeButton": false,

"NewTabPageLocation": "about:blank",

"HomepageLocation": "chrome://newtab",

"AlwaysAuthorizePlugins": false,

"AuthSchemes": "negotiate",

"ExtensionSettings": {

"cjpalhdlnbpafiamejdnhcphjbkeiagm": {

"installation\_mode": "allowed"

},

"pkehgijcmpdhfbdbbnkijodmdjhbjlgp": {

"installation\_mode": "allowed"

},

"\*": {

"installation\_mode": "blocked"

}

},

"SafeBrowsingEnabled": true,

"DefaultSearchProviderSearchURL": "https://www.google.com/",

"SavingBrowserHistoryDisabled": false,

"EnabledPlugins": [],

"DefaultGeolocationSetting": 2,

"BlockThirdPartyCookies": true,

"CookiesSessionOnlyForUrls": [],

"SearchSuggestEnabled": false,

"ImportSavedPasswords": false,

"URLBlacklist": ["javascript://\*"],

"DefaultPopupsSetting": 2,

"DisabledPlugins": [ "\*" ],

"PasswordManagerEnabled": false,

"AllowOutdatedPlugins": false,

"DnsPrefetchingEnabled": false,

"IncognitoModeAvailability": 1,

"SyncDisabled": true,

"RemoteAccessHostFirewallTraversal": false,

"CloudPringProxyEnabled": false,

"PasswordManagerAllowShowPasswords": false,

"BackgroundModeEnabled": false,

"DisablePluginFinder": true,

"AutoFillEnabled": false,

"Disable3DAPIs": true,

"DefaultSearchProviderName": "https://www.google.com",

"DefaultSearchProviderEnabled": true,

"DefaultPluginsSetting": 3,

"EnableOnlineRevocationChecks": true,

"DefaultNotificationsSetting": 2,

"MetricsReportingEnabled": false

}

1. Restart Chrome, notice changes in behavior, screenshot of manage extensions page.

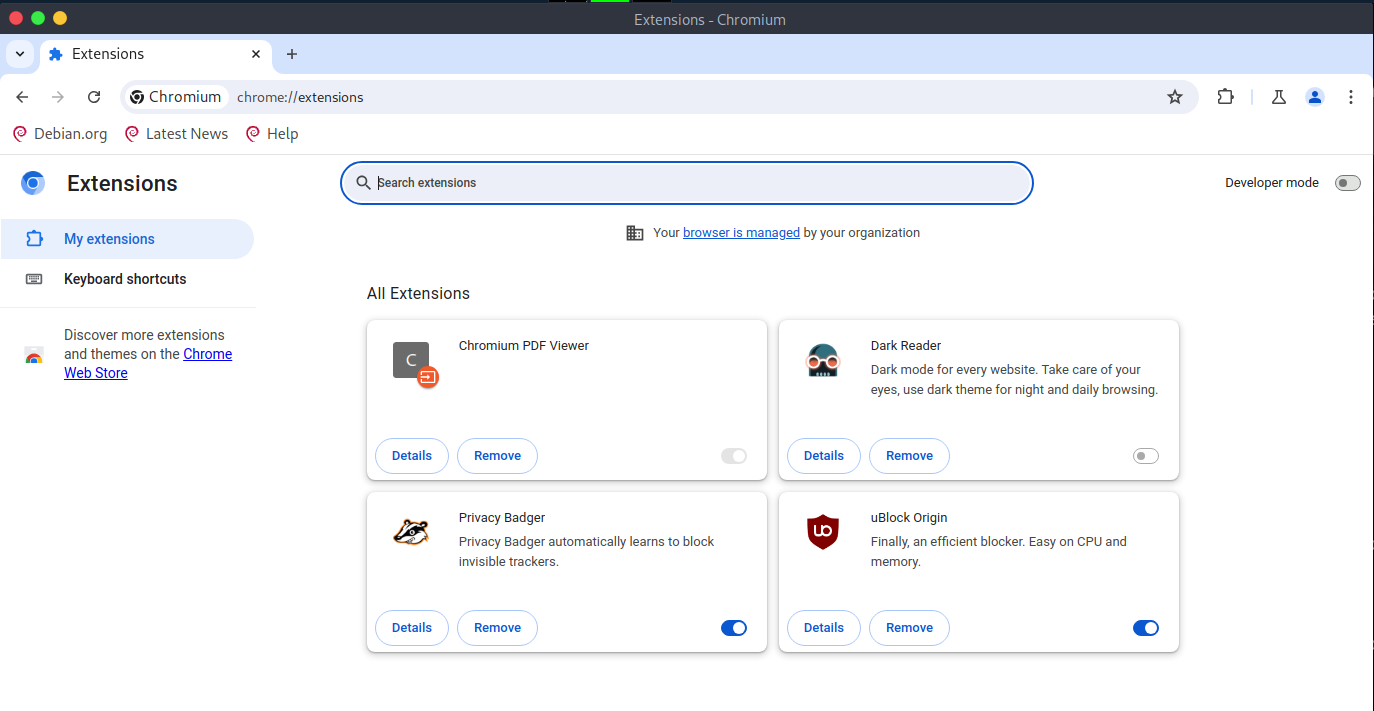
A screenshot of a computer

Description automatically generated

1. Load extensions from the Chrome Store. Ublock Origin and Privacy Badger will work, all others should not.
2. Close Chrome
3. Nuke the preloaded extensions (to rid of startup errors):

rm -rf /home/user/.config/Default/Extensions/\*

1. Restart Chrome, notice changes in behavior, screenshot of manage extensions page



## Submission

Upload to Canvas a docx or pdf containing the two requested screenshots of the manage extensions page

## Questions for the class:

The user reloading UBlock and PrivacyBadger, places the extensions under user control in /home/user/.config/chromium/Default/Extensions rather than /usr/share/chromium/extensions. Is this the right thing to allow?

What policies would impact your user experience?

What other policies might be included that are not in the STIG?

How do you address changes in Chrome and/or STIG policies?

What controls need to be in place to ensure the policy is enforced?

Review the recommended SCAP Chromium policy.

There are 40ish rules to review.  The group should divide and conquer.

Each team member should post to Discord the rule (from the ones they were assigned) that they feel would have the most negative impact on their personal browser usage.

As a group - 10 minutes:

From the individual selections.  The group selects the most impactful.

Create a recommendation on how an organization might enforce the selected policy.  Considering how individuals might bypass the recommendation.

Captain presentations - 15 minutes

The policy selected

The control recommended

Concerns about control bypass