``````````````````````````````````````````````````

Name: Rounak Bania
Role: Intern at H1K0R

``````````````````````````````````````````````````

# Topic 1

## Usage Of Chaps (Configuration Hardening Assessment PowerShell Script)

CHAPS is a PowerShell script for checking system security settings where additional software and assessment tools, such as Microsoft Policy Analyzer, cannot be installed. The purpose of this script is to run it on a server or workstation to collect configuration information about that system. The information collected can then be used to provide recommendations (and references) to improve the security of the individual system and systemic issues within the organization's Windows environment.

To Install CHAPS we have to do following steps:

1) Go to their GITHUB account and clone the official REPO.
2) We need to paste some Commands Follow the instructions thy provided
    - `powershell.exe -exec bypass`
    - `Set-ExecutionPolicy Bypass -scope Process`
3) run the chaps.ps1 in the terminal and wait for results.

## *Time to adress the issues that CHAPS recognized  on my Device*

After Running The Chaps The Issues On My System are :

```
raunak@raunak-UH-X ~/Task_1
$ cat server-chap.txt | grep -v "[+]\|[*]\|IPv6" | grep "[-]"
[-] Windows AutoUpdate is not configuration to automatically install updates:  : System.Collections.Hashtable.
[-] BitLocker not detected on Operating System Volume or encryption is not complete. Please check for other encryption methods: FullyDecrypted
[-] ProcessCreationIncludeCmdLine_Enabled Is Not Set
[-] EnableModuleLogging Is Not Set
[-] EnableScriptBlockLogging Is Not Set
[-] EnableScriptBlockInvocationLogging Is Not Set
[-] EnableTranscripting Is Not Set
[-] EnableInvocationHeader Is Not Set
[-] EnableProtectedEventLogging Is Not Set
[-] Microsoft-Windows-SMBServer/Audit max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-SMBServer/Audit] GB: 0.008 GB
[-] Security max log size is smaller than System.Collections.Hashtable[Security] GB: 0.02 GB
[-] Microsoft-Windows-PowerShell/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-PowerShell/Operational] GB: 0.015 GB
[-] Microsoft-Windows-TaskScheduler/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-TaskScheduler/Operational] GB: 0.01 GB
[-] Microsoft-Windows-WinRM/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WinRM/Operational] GB: 0.001 GB
[-] Microsoft-Windows-Security-Netlogon/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-Security-Netlogon/Operational] GB: 0.001 GB
[-] Microsoft-Windows-WMI-Activity/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-WMI-Activity/Operational] GB: 0.001 GB
[-] Windows PowerShell max log size is smaller than System.Collections.Hashtable[Windows PowerShell] GB: 0.015 GB
[-] System max log size is smaller than System.Collections.Hashtable[System] GB: 0.02 GB
[-] Application max log size is smaller than System.Collections.Hashtable[Application] GB: 0.02 GB
[-] Microsoft-Windows-TerminalServices-LocalSessionManager/Operational max log size is smaller than System.Collections.Hashtable[Microsoft-Windows-TerminalServices-LocalSessionManager/Operational] GB: 0.001 GB
[-] PowerShell Version 2 should be disabled: Enabled
[-] Execution Language Mode Is Not ConstrainedLanguage: FullLanguage
[-] CachedLogonsCount Is Not Set to 0 or 1: 10
[-] fDenyTSConnections should be set to not allow remote connections: 0
[-] More than one account is in local Administrators group: 3
[-] AppLocker not configured
[-] No WPAD entry detected. Should contain: wpad 255.255.255.255
[-] WinHttpAutoProxySvc service is: Running
[-] KB3165191 to harden WPAD is not installed.
[-] DNSEnabledForWINSResolution is enabled
[-] WINSEnableLMHostsLookup is enabled
[-] DNSClient.EnableMulticast does not exist or is enabled:
[-] Computer Browser service is: Running
[-] WSH Setting Enabled key does not exist.
[-] KB2871997 is not installed.
[-] WDigest UseLogonCredential key does not exist.
[-] SMBv1 is Enabled
[-] Kernel MitigationOptions key does not exist.
[-] LM Compatability Level registry key is not configured.
[-] RestrictAnonymous registry key is not configured: 0
[-] RestrictRemoteClients registry key is not configured:
[-] NTLM Session Server Security settings is not configured to require NTLMv2 and 128-bit encryption: 536870912
[-] NTLM Session Client Security settings is not configured to require NTLMv2 and 128-bit encryption: 536870912
raunak@raunak-UH-X ~/Task_1
$
```

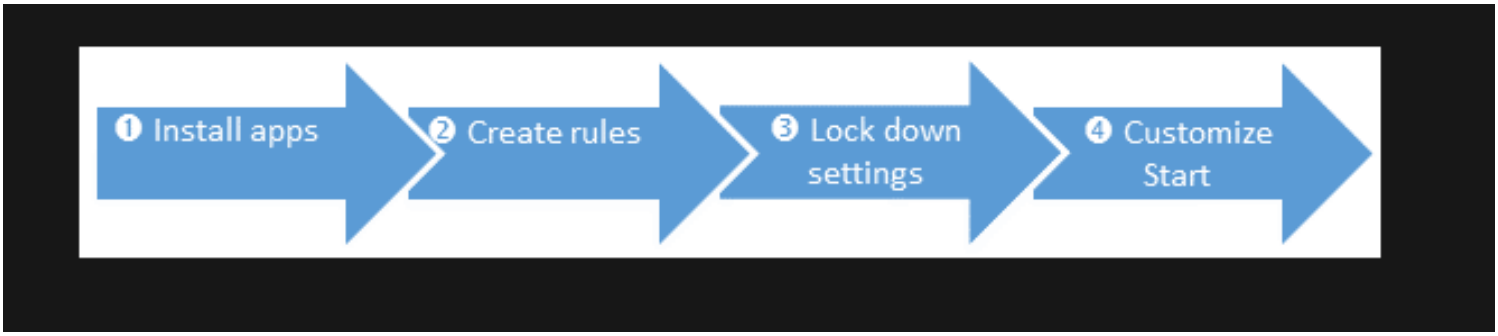
# *There are some Minior issues*.

1) Windows AutoUpdate is not Configured
   - FIX- We can enable auto updates from windows settings

2) Bitlocker not Detected (Bitlocker is a tool that we use to encrypt our Directories to make our files secure in windows)
   - FIX- We Can enable Bitlocker by searching bitlocker in windows search

3) Powershell 2.0 is Enabled
   - FIX- We can fix this by opening powershell as an Administrator and typing
   - powershell.exe Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowershellV2 -Remove

4) Applocker Not Configured (AppLocker helps you create rules to allow or deny apps from running based on information about the apps)
   - We can Configure applocker with the help of windows forum




5) Multiple Local Administrators Group
   - we can change Account Type from Control panel in windows settings