Internship Assessment for Tutelr Infinity Internships Week 1

NAME- PRAHLAD KUMAR

FINDINGS

1) ProcessCreationIncludeCmdLine_Enabled Is Not Set

This event is typically used to investigate suspicious activity on a Windows system and is part of the Endpoint Detection and Response (EDR) capabilities of Microsoft Defender for Endpoint.

When this policy setting is enabled, any user with access to read the security events will be able to read the command line arguments for any successfully created process. Command line arguments can contain sensitive or private information such as passwords or user data.

Remediation

This can be enabled at Administrative Templates > System > Audit Process Creation > set Include Command Line in Process Creation Events to enabled.

2) PowerShell Moduling is not set

PowerShell module logging is a security feature that can be used to detect and investigate malicious activity on a system. Enabling PowerShell module logging allows you to track the use of PowerShell modules and cmdlets, and can help identify potential security incidents and malicious activity.

Remediation

Open the Local Group Policy Editor and navigate to Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell > Turn on PowerShell Script Block Logging.

3) PowerShell EnableScriptBlockLogging is not Enabled ?

Enabling PowerShell script block logging is a security feature that can help identify potential security incidents and malicious activity on a Windows system. This information can be used to detect suspicious or unauthorized activity, such as the execution of malicious PowerShell commands or scripts.

Remediation

Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> “Turn on PowerShell Script Block Logging” to “Disabled”.

4) if PowerShell EnableScriptBlockInvocationLogging is not Enabled ?

script block invocation logging is enabled, PowerShell logs information about each script block that is invoked, including the text of the script block and the context in which it was invoked. This information can be used to identify potential security incidents and unauthorized activity, such as the execution of malicious PowerShell scripts.

Internship Assessment for Tutelr Infinity Internships Week 1

NAME- PRAHLAD KUMAR

Remediation

Open the Local Group Policy Editor and navigate to Computer Configuration > Administrative Templates > Windows Components > Windows PowerShell > Turn on PowerShell Script Block Logging.

5) PowerShell EnableTranscripting is not Enabled ?

PowerShell transcripting is another security feature that can be used to record all activity that occurs in a PowerShell session. When transcripting is enabled, PowerShell records all input and output from the session, including any errors that occur. This can be useful for auditing and troubleshooting purposes, as well as for detecting and investigating security incidents.

It is important to note that transcripting can generate a lot of data and may impact performance, so it should be used judiciously. It is also important to ensure that the transcript files are protected appropriately, as they may contain sensitive information.

Remediation

Configure the policy value for Computer Configuration >> Administrative Templates >> Windows Components >> Windows PowerShell >> "Turn on PowerShell Transcription" to "Enabled"

6) PowerShell EnableInvocationHeader is not Enabled ?

Enabling PowerShell invocation headers is a security feature that can help protect against malicious activity by providing information about the origin of a PowerShell command or script.

When invocation headers are enabled, PowerShell adds a header to each command or script that identifies the source of the command or script. This information can be used to verify the authenticity of the command or script and to detect potential security incidents, such as the execution of malicious PowerShell commands or scripts.

Remediation

This command sets a registry value to enable invocation headers. Note that this command should be run with administrative privileges.

Set-ItemProperty -Path 'HKLM:\Software\Wow6432Node\Policies\Microsoft\Windows\PowerShell\ScriptBlockLogging' -Name 'EnableInvocationHeader' -Value '1' -Type DWord

7) Event logs settings defaults are too small. Test that max sizes have been increased.

By default, the size of the Windows event logs is relatively small, which can lead to important events being overwritten or lost over time. Increasing the maximum size of the

event logs can help ensure that important events are retained for a longer period of time and that the logs do not fill up too quickly.

Remediation

To check if the maximum size of the event logs has been increased, you can use the following steps:

1. Open the Event Viewer by typing "Event Viewer" into the Start menu or search bar.
2. In the left-hand pane, navigate to the specific log you want to check, such as "Security" or "Application".
3. Right-click on the log and select "Properties".
4. In the "Log Properties" window, select the "Maximum log size" option.
5. Check the current maximum size of the log. If the size has been increased from the default value, it should be larger than the default size.

8) PowerShell Version 2 should be disabled: It is Enabled ?

Run the command to disable powershell version 2

Disable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root -NoRestart

9) NET Framework less than 3.0 installed which could allow PS2 execution: 2.0.50727.4927

This may allow for PowerShell Version 2 execution, which has security vulnerabilities and limitations.

Remediation

To resolve this issue, we can try updating the .NET Framework to a more recent version that includes security patches and updates. The current latest version of .NET Framework is 4.8, which includes all updates and security patches for all previous versions.

To update .NET Framework to version 4.8, we can follow these steps:

Download the appropriate .NET Framework 4.8 installer for your operating system from the Microsoft Download Center: https://dotnet.microsoft.com/download/dotnet-framework/net48

Run the downloaded file to start the installation process.

Follow the prompts in the installation wizard to complete the installation.

10) Testing for Microsoft LAPS failed

REMEDIATION

Internship Assessment for Tutelr Infinity Internships Week 1

NAME- PRAHLAD KUMAR

1. Verify that the LAPS client is installed on the computer: Make sure that the LAPS client is installed on the computer that you are testing. You can check this by going to the Control Panel and looking for the LAPS client in the list of installed programs.
2. Check the LAPS Group Policy settings: LAPS uses Group Policy to manage the password policy for local administrator accounts. Make sure that the LAPS Group Policy settings are configured correctly and are being applied to the computer. You can check this by running the "gpresult" command in a Command Prompt window.
3. Check the event logs: LAPS logs events in the Windows event log. Look for any error or warning events related to LAPS and use the information in the event to diagnose the problem.
4. Verify network connectivity: LAPS relies on Active Directory to store the password information for local administrator accounts. Make sure that the computer is connected to the network and can communicate with the Active Directory domain controllers.
5. Check permissions: The account used to test LAPS must have read permissions on the ms-Mcs-AdmPwd attribute in Active Directory. Verify that the account being used for the test has the required permissions.

11) KB3165191 to harden WPAD is not installed ?

KB3165191 is a security update for Windows that hardens the Web Proxy Auto-Discovery (WPAD) protocol. If this update is not installed on your system, it means that your system may be vulnerable to WPAD-related attacks.

REMEDIATION

1. Open the Windows Update settings by clicking on the Start menu and typing "Windows Update" in the search box. Click on the "Windows Update" application that appears in the search results.
2. Click on the "Check for updates" button to search for available updates.
3. If KB3165191 is listed as an available update, select it and click on the "Install" button to install the update.
4. If KB3165191 is not listed as an available update, you may need to download and install it manually. You can download the update from the Microsoft Update Catalog website: **https://www.catalog.update.microsoft.com/Search.aspx?q=KB3165191**
5. Follow the instructions provided by the installation wizard to install the update.

After installing KB3165191, Our system will be hardened against WPAD-related attacks, which can help to improve the security of our network.

Internship Assessment for Tutelr Infinity Internships Week 1

NAME- PRAHLAD KUMAR

Assessment questions

1. What are CHAPS?

   Ans-> A PowerShell script for assessing the configuration hardening of Windows machines.

2. What is the purpose of CHAPS?

   Ans->To provide an automated way to assess the configuration hardening of Windows machines.

3. What are some of the security settings assessed by CHAPS?

   Ans-> b. Internet connectivity settings, system update settings, and firewall settings.

   d. Disk encryption settings, user account settings, and virtual machine settings.

4. How does CHAPS assess the security settings of Windows machines?

   Ans-> a. By querying the Windows registry and security policy settings.

5. What is the output of CHAPS?

   Ans-> a. A report in CSV format that lists the security settings assessed and their status (enabled/disabled).

   d. A list of all network devices connected to the Windows machine.

6. How can CHAPS be useful in a corporate environment?

   Ans-> a. It can help identify security vulnerabilities and assist in hardening the configuration of Windows machines.

   d. It can be used to scan for and remove malware on Windows machines.

7. What are some limitations of CHAPS?

   Ans-> a. It can only be run on Windows machines running PowerShell version 5.1 or later.

   c. It requires administrative privileges to run.

   d. It may generate false positives or false negatives, depending on the system configuration.

8. What are some ways to improve CHAPS?

   Ans-> a. Add support for assessing security settings on Linux and macOS machines.

   c. Improve the accuracy of the assessments to minimize false positives and false negatives.

   d. Provide an automated way to remediate security vulnerabilities found during the assessment.

9. What are some alternatives to CHAPS?

   Ans-> a. Microsoft Baseline Security Analyzer (MBSA)

   b. Nessus Vulnerability Scanner

Internship Assessment for Tutelr Infinity Internships Week 1

NAME- PRAHLAD KUMAR

10. In your opinion, how useful do you think CHAPS is for assessing the configuration hardening of Windows machines? Why?

Ans-> CHAPS can be a useful tool for assessing the configuration hardening of Windows machines, but it should not be the only tool used. CHAPS provide a set of guidelines and recommendations for hardening Windows systems based on industry best practices, but it does not consider the specific requirements and risk profile of each organization. Therefore, it is important to use CHAPS in conjunction with other tools and methods, such as vulnerability scanners and penetration testing, to ensure that the security posture of Windows systems is robust and effective.

Additionally, CHAPS is a free tool, which means that it may not have the same level of support and maintenance as commercial solutions. While it is a valuable resource for organizations with limited budgets, it may not be suitable for larger organizations with more complex security needs.

In summary, CHAPS can be a useful tool for assessing the configuration hardening of Windows machines, but it should be used in with other tools and methods to ensure and approach for better security. It is also important to consider the specific requirements and risk profile of each organization when implementing security measures, and to ensure that the chosen tools and methods are well-maintained and supported.