CHAPS (Hardening Assessment PowerShell Script) Assignment Report

Prepared by: Adarsh Tiwari

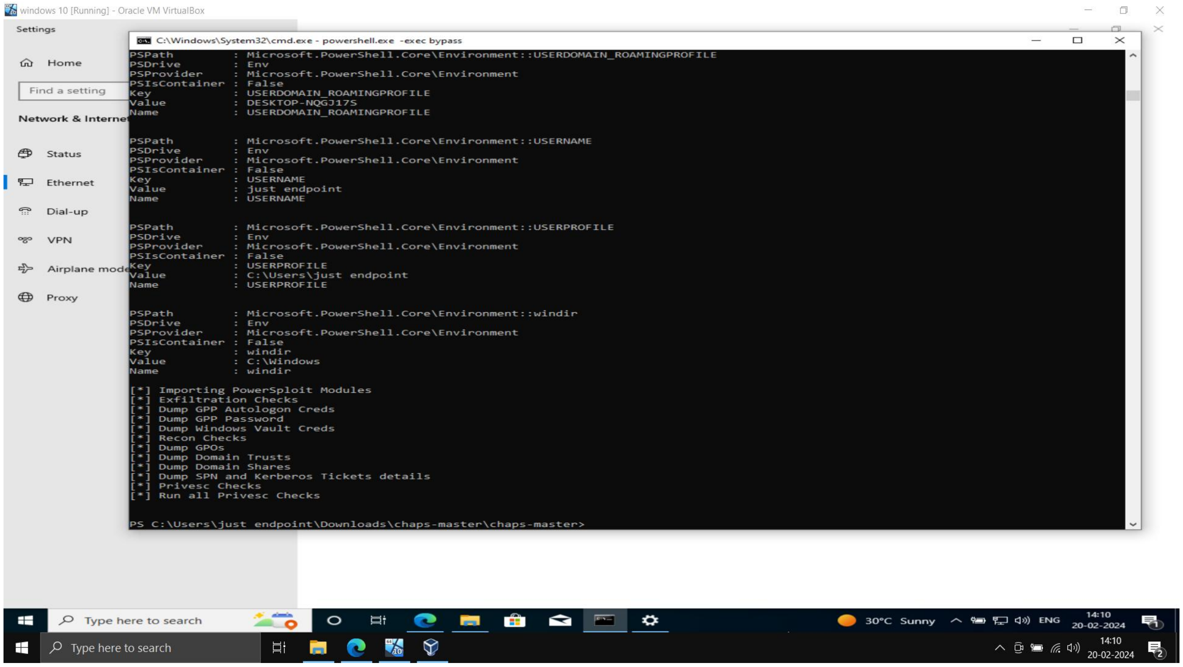
Date: 23/02/2024

Client: XYZ Corporation

Executive Summary:

The CHAPS assessment was conducted on the systems belonging to XYZ Corporation to evaluate their security posture and identify potential vulnerabilities. This report provides an overview of the findings and recommendations for improving the security of the systems.

Assessment Overview:



```
PSPath        : Microsoft.PowerShell.Core\Environment::USERDOMAIN_ROAMINGPROFILE
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERDOMAIN_ROAMINGPROFILE
Value         : DESKTOP-NQGJ17S
Name          : USERDOMAIN_ROAMINGPROFILE


PSPath        : Microsoft.PowerShell.Core\Environment::USERNAME
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERNAME
Value         : just endpoint
Name          : USERNAME


PSPath        : Microsoft.PowerShell.Core\Environment::USERPROFILE
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : USERPROFILE
Value         : C:\Users\just endpoint
Name          : USERPROFILE


PSPath        : Microsoft.PowerShell.Core\Environment::windir
PSDrive       : Env
PSProvider    : Microsoft.PowerShell.Core\Environment
PSIsContainer : False
Key           : windir
Value         : C:\Windows
Name          : windir

[*] Importing PowerSploit Modules
[*] Exfiltration Checks
[*] Dump GPP Autologon Creds
[*] Dump GPP Password
[*] Dump Windows Vault Creds
[*] Recon Checks
[*] Dump GPOs
[*] Dump Domain Trusts
[*] Dump Domain Shares
[*] Dump SPN and Kerberos Tickets details
[*] Privesc Checks
[*] Run all Privesc Checks


PS C:\Users\just endpoint\Downloads\chaps-master\chaps-master>
```

The assessment covered the following areas:

Windows Security Settings and Configurations

Patch Management

User Account Settings and Permissions

Group Policy Settings

Firewall Configurations

Common Security Vulnerabilities

Findings and Recommendations:

Increase log file sizes: The maximum sizes for many event logs, including Security and PowerShell logs, are too small. Increase the maximum sizes for these logs to ensure that important events are not overwritten.

Enable additional PowerShell logging: Enable various PowerShell logging options, such as ProcessCreationIncludeCmdLine_Enabled, EnableModuleLogging, EnableScriptBlockLogging, EnableScriptBlockInvocationLogging, and EnableTranscripting. This will provide more detailed information about PowerShell activity on the system.

Secure local administrator accounts: There are two accounts in the local Administrators group. Consider removing unnecessary accounts or setting strong passwords for all accounts.

Disable unused services: The WinRM service is not running, but it is recommended to disable it if it is not needed.

Review firewall rules: Ensure that the Windows Network Firewall rules are configured to block unauthorized remote access.

Patch the system: Keep the system up-to-date with the latest security patches.
Specific Recommendations:

Enable SMBv1 auditing: While SMBv1 is disabled, it is still recommended to enable auditing for SMBv1 activity to monitor any potential attempts to use this insecure protocol.

Disable NetBIOS: NetBIOS is enabled on the system. Consider disabling it if it is not needed.
Configure LM Compatibility Level: Set the LM Compatibility Level registry key to 0 to disable LM hash support and improve password security.

Enforce NTLMv2 and 128-bit encryption: Configure NTLM session server and client security settings to require NTLMv2 and 128-bit encryption for secure authentication.

Conclusion:

The CHAPS assessment identified several areas where improvements can be made to enhance the security posture of XYZ Corporation's systems. By implementing the recommendations outlined in this report, XYZ Corporation can reduce the risk of security breaches and protect sensitive data from unauthorized access.

This concludes the CHAPS Hardening Assessment Report for XYZ Corporation.