7-1 Final Project: System and Communication Security Paper

Joshua Merren

Southern New Hampshire University

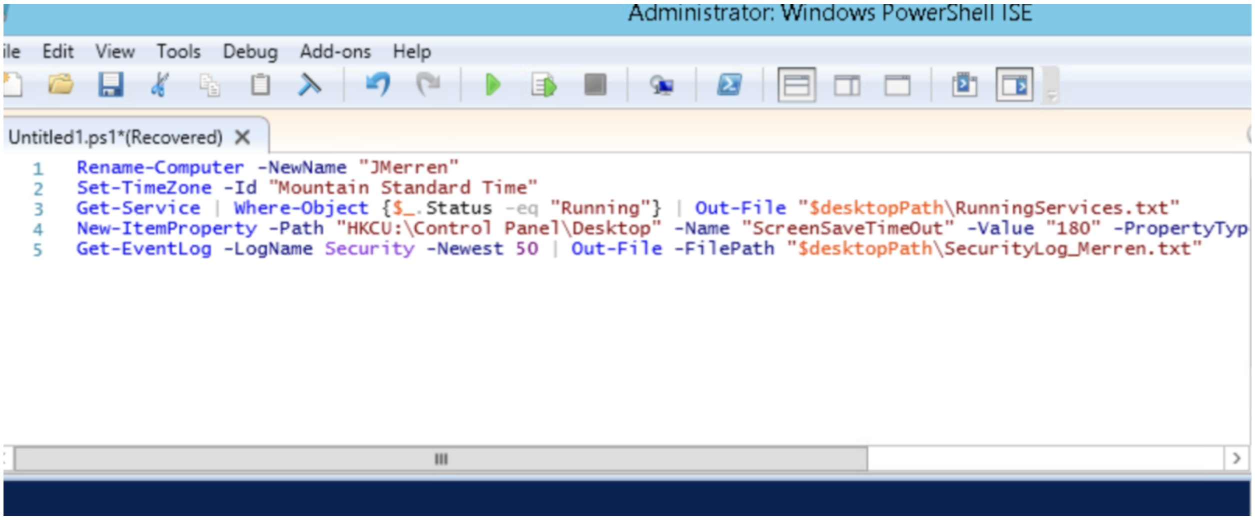
CYB-300-11432-M01 System and Comm Security

Professor Robert Chubbuck

13 August 2024

I. **Automated Hardening Scripts:** Compose a single executable script to automate hardening tasks to meet the requirements in the scenario.

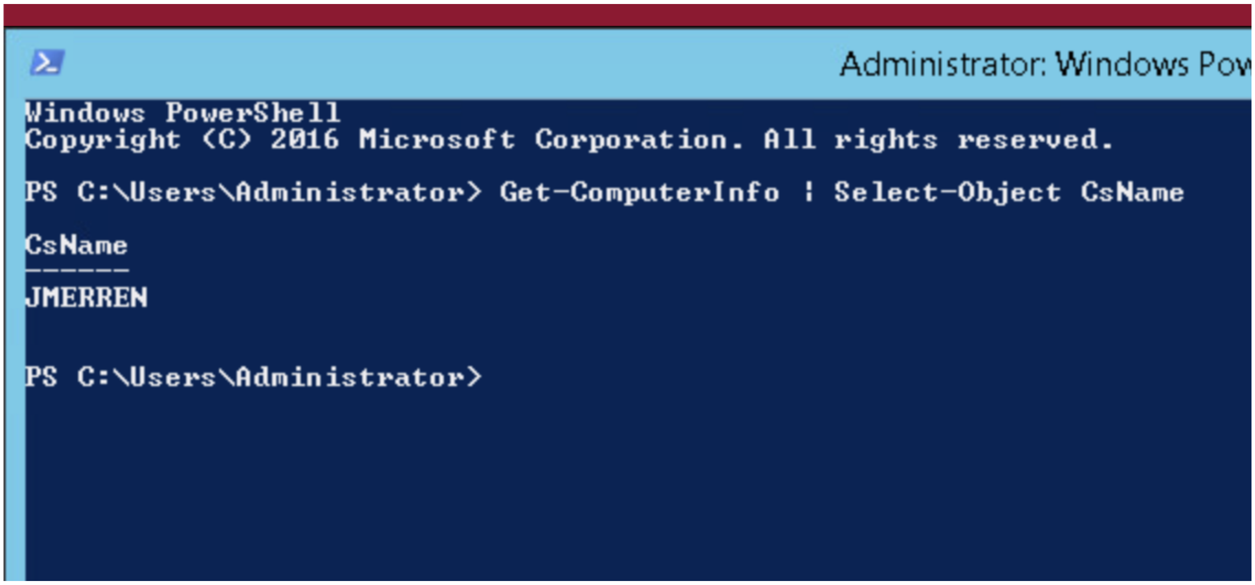
a. Screenshot of a single **executable script** in the Linux shell environment


Administrator: Windows PowerShell ISE
ile Edit View Tools Debug Add-ons Help
Untitled1.ps1*(Recovered)

```
Rename-Computer -NewName "JMerren"
Set-TimeZone -Id "Mountain Standard Time"
Get-Service | Where-Object {$_.Status -eq "Running"} | Out-File "$desktopPath\RunningServices.txt"
New-ItemProperty -Path "HKCU:\Control Panel\Desktop" -Name "ScreenSaveTimeOut" -Value "180" -PropertyTyp
Get-EventLog -LogName Security -Newest 50 | Out-File -FilePath "$desktopPath\SecurityLog_Merren.txt"
```

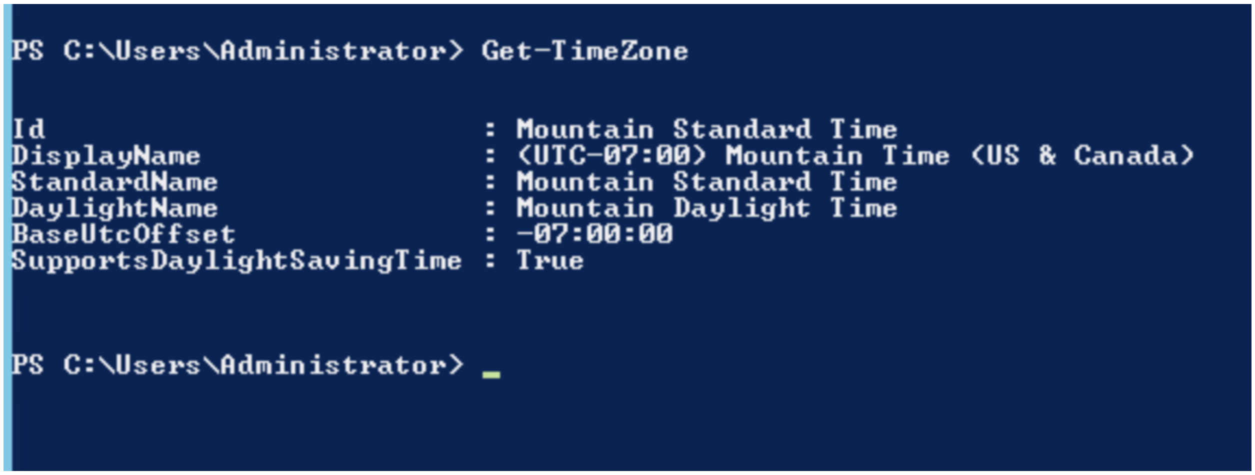
b. Screenshots that **evidence** each requirement has been met

1. Rename computer to First Initial_Last Name (use your first initial and your last name)



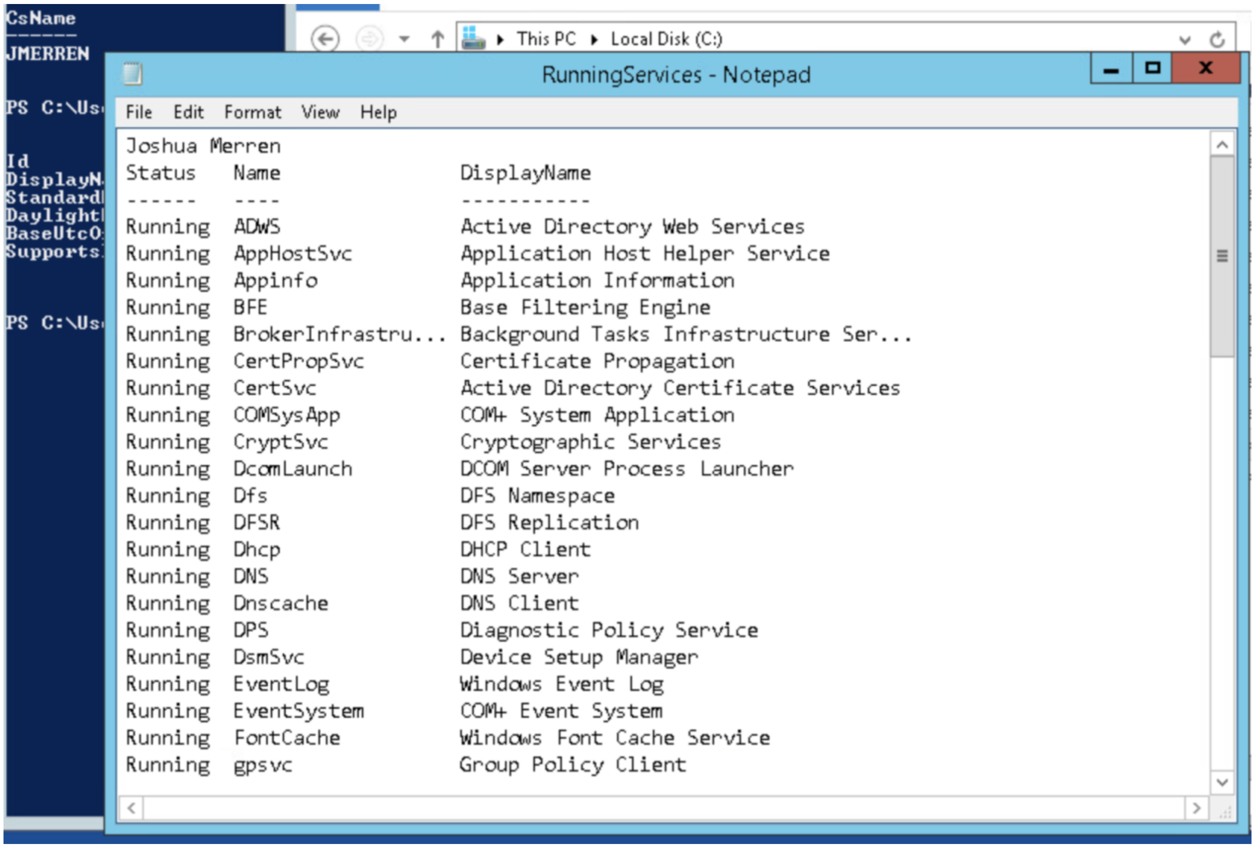
```
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Get-ComputerInfo | Select-Object CsName

CsName
-------
JMERREN


PS C:\Users\Administrator>
```

2. Change time zone to the time zone associated with Denver, Colorado



```
PS C:\Users\Administrator> Get-TimeZone

Id                         : Mountain Standard Time
DisplayName                : (UTC-07:00) Mountain Time (US & Canada)
StandardName               : Mountain Standard Time
DaylightName               : Mountain Daylight Time
BaseUtcOffset              : -07:00:00
SupportsDaylightSavingTime : True


PS C:\Users\Administrator> _
```

3. Get a list of running processes

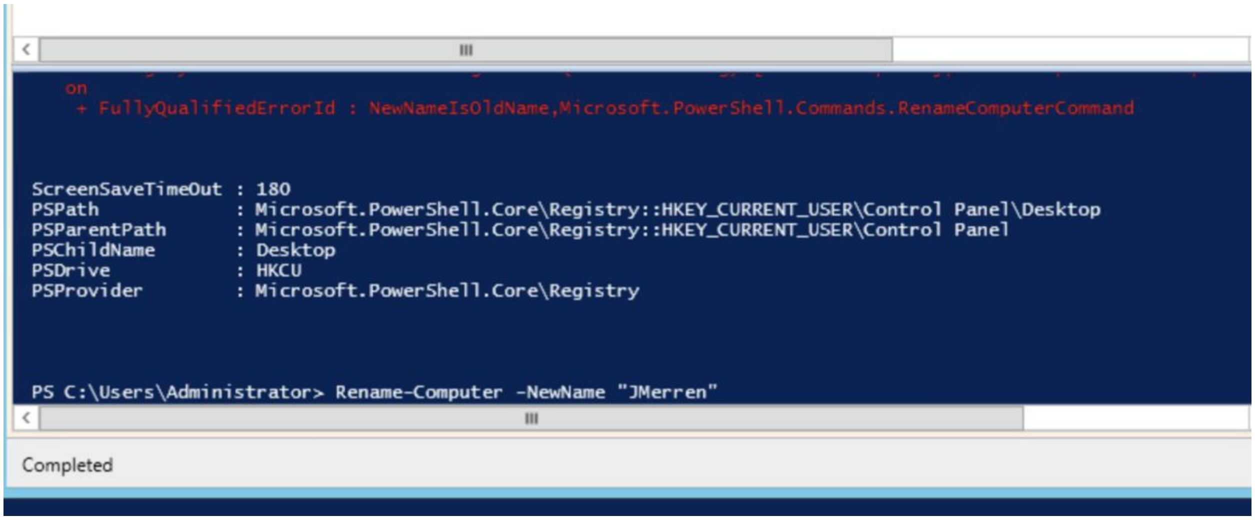


This PC ▸ Local Disk (C:)
RunningServices - Notepad
File Edit Format View Help

```
CsName
------
JMERREN

PS C:\Us

Id
DisplayN
Standard
Daylight
BaseUtcO
Supports

PS C:\Us
```

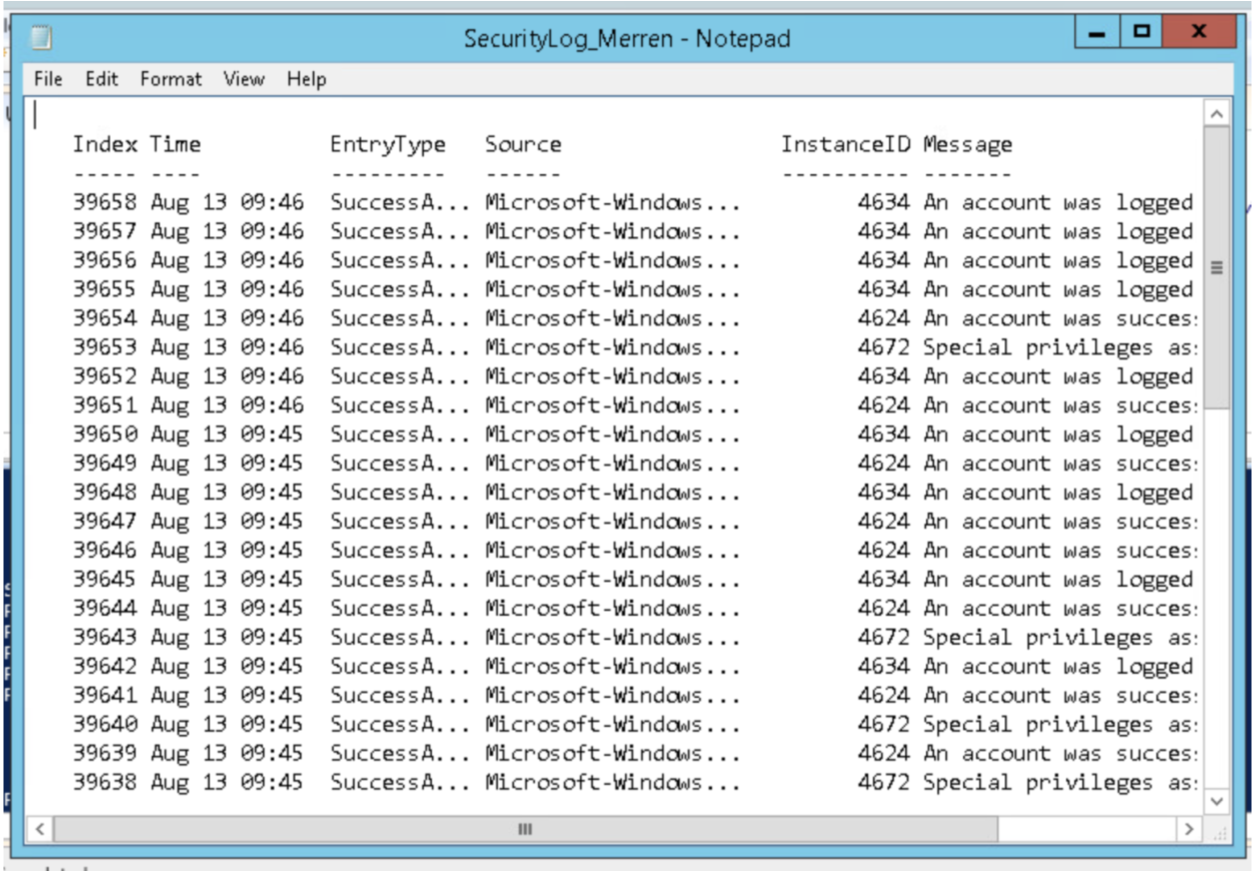
```
Joshua Merren
Status   Name               DisplayName
------   ----               -----------
Running  ADWS               Active Directory Web Services
Running  AppHostSvc         Application Host Helper Service
Running  Appinfo            Application Information
Running  BFE                Base Filtering Engine
Running  BrokerInfrastru... Background Tasks Infrastructure Ser...
Running  CertPropSvc        Certificate Propagation
Running  CertSvc            Active Directory Certificate Services
Running  COMSysApp          COM+ System Application
Running  CryptSvc           Cryptographic Services
Running  DcomLaunch         DCOM Server Process Launcher
Running  Dfs                DFS Namespace
Running  DFSR               DFS Replication
Running  Dhcp               DHCP Client
Running  DNS                DNS Server
Running  Dnscache           DNS Client
Running  DPS                Diagnostic Policy Service
Running  DsmSvc             Device Setup Manager
Running  EventLog           Windows Event Log
Running  EventSystem        COM+ Event System
Running  FontCache          Windows Font Cache Service
Running  gpsvc              Group Policy Client
```

4. Set idle lock time for screensaver to 3 minutes



```
    on
     + FullyQualifiedErrorId : NewNameIsOldName,Microsoft.PowerShell.Commands.RenameComputerCommand


ScreenSaveTimeOut : 180
PSPath            : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Control Panel\Desktop
PSParentPath      : Microsoft.PowerShell.Core\Registry::HKEY_CURRENT_USER\Control Panel
PSChildName       : Desktop
PSDrive           : HKCU
PSProvider        : Microsoft.PowerShell.Core\Registry



PS C:\Users\Administrator> Rename-Computer -NewName "JMerren"
```

5. Send the output of the last 50 entries in the /var/log/messages log to a text file named “SecurityLog_LastName.txt”



```
 Index Time          EntryType   Source                 InstanceID Message
 ----- ----          ---------   ------                 ---------- -------
 39658 Aug 13 09:46  SuccessA... Microsoft-Windows...         4634 An account was logged
 39657 Aug 13 09:46  SuccessA... Microsoft-Windows...         4634 An account was logged
 39656 Aug 13 09:46  SuccessA... Microsoft-Windows...         4634 An account was logged
 39655 Aug 13 09:46  SuccessA... Microsoft-Windows...         4634 An account was logged
 39654 Aug 13 09:46  SuccessA... Microsoft-Windows...         4624 An account was succes:
 39653 Aug 13 09:46  SuccessA... Microsoft-Windows...         4672 Special privileges as:
 39652 Aug 13 09:46  SuccessA... Microsoft-Windows...         4634 An account was logged
 39651 Aug 13 09:46  SuccessA... Microsoft-Windows...         4624 An account was succes:
 39650 Aug 13 09:45  SuccessA... Microsoft-Windows...         4634 An account was logged
 39649 Aug 13 09:45  SuccessA... Microsoft-Windows...         4624 An account was succes:
 39648 Aug 13 09:45  SuccessA... Microsoft-Windows...         4634 An account was logged
 39647 Aug 13 09:45  SuccessA... Microsoft-Windows...         4624 An account was succes:
 39646 Aug 13 09:45  SuccessA... Microsoft-Windows...         4624 An account was succes:
 39645 Aug 13 09:45  SuccessA... Microsoft-Windows...         4634 An account was logged
 39644 Aug 13 09:45  SuccessA... Microsoft-Windows...         4624 An account was succes:
 39643 Aug 13 09:45  SuccessA... Microsoft-Windows...         4672 Special privileges as:
 39642 Aug 13 09:45  SuccessA... Microsoft-Windows...         4634 An account was logged
 39641 Aug 13 09:45  SuccessA... Microsoft-Windows...         4624 An account was succes:
 39640 Aug 13 09:45  SuccessA... Microsoft-Windows...         4672 Special privileges as:
 39639 Aug 13 09:45  SuccessA... Microsoft-Windows...         4624 An account was succes:
 39638 Aug 13 09:45  SuccessA... Microsoft-Windows...         4672 Special privileges as:
```

c. One of the main reasons that practitioners use automated scripts is to save time by avoiding manual configurations. Describe **additional benefits** of using automated scripts for configuring systems in a secure manner for organizations.

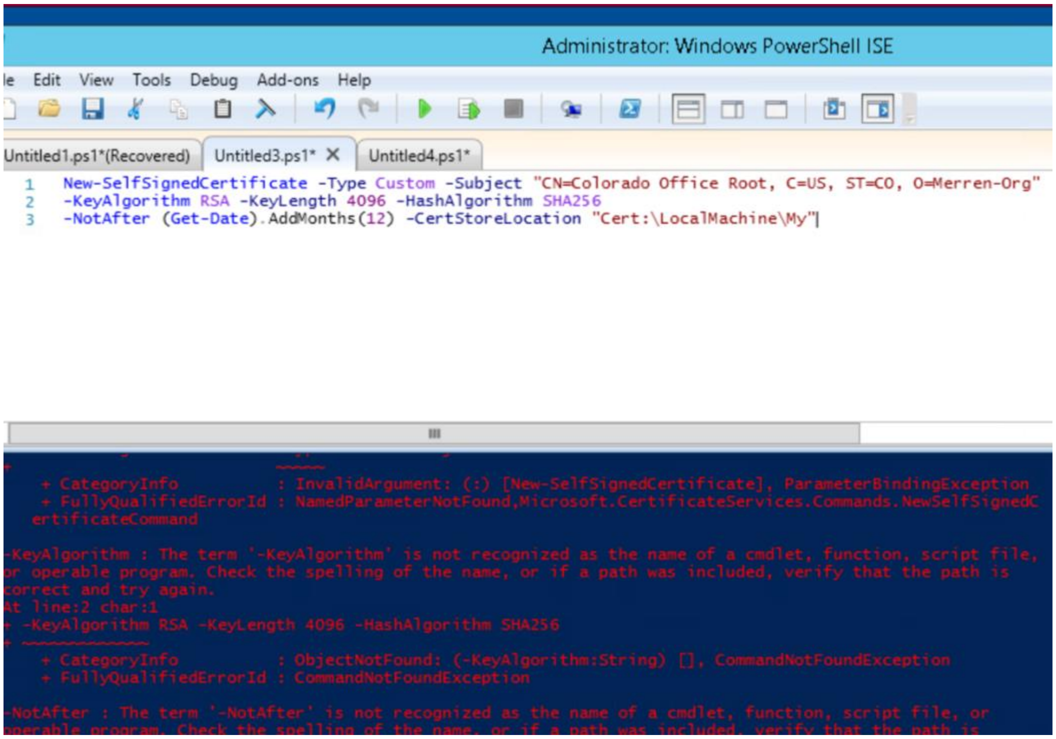
Automated scripts are invaluable tools for organizations seeking to maintain a secure and consistent IT environment. Beyond the obvious time savings by avoiding manual configurations, automated scripts offer several additional benefits. First and foremost, they ensure consistency across all systems, reducing the likelihood of human error, which is often a significant risk in manual processes. When a script is used, it applies the same configurations every time, ensuring uniform security settings across all devices. This consistency is crucial in large organizations where slight variations can lead to vulnerabilities (CrowdStrike, 2023).

Moreover, automated scripts enhance scalability. As organizations grow, so does the number of systems that need to be managed. Scripts allow IT teams to efficiently deploy configurations to hundreds or even thousands of systems without requiring a proportional increase in workforce. This scalability is critical to maintaining security in a rapidly growing or changing environment. Additionally, scripts are inherently repeatable. Once written and tested, a script can be reused across different environments or for future deployments, ensuring that best practices are consistently applied over time (Eperjesi, 2023).

Another significant advantage of automated scripts is their contribution to auditability and documentation. Automated processes create a clear record of what configurations were applied and when, which is essential for compliance audits and tracking changes over time. This audit trail can also be invaluable during troubleshooting, allowing IT teams to identify what was changed and why quickly. Finally, automated scripts enable rapid deployment and rollback of configurations. In the event of a misconfiguration or security incident, scripts can quickly apply changes or revert systems to a known good state, minimizing downtime and enhancing overall system reliability. By reducing the need for manual intervention, scripts also reduce the likelihood of introducing errors that could compromise security, strengthening the organization's overall security posture (Tanium Inc, 2024).

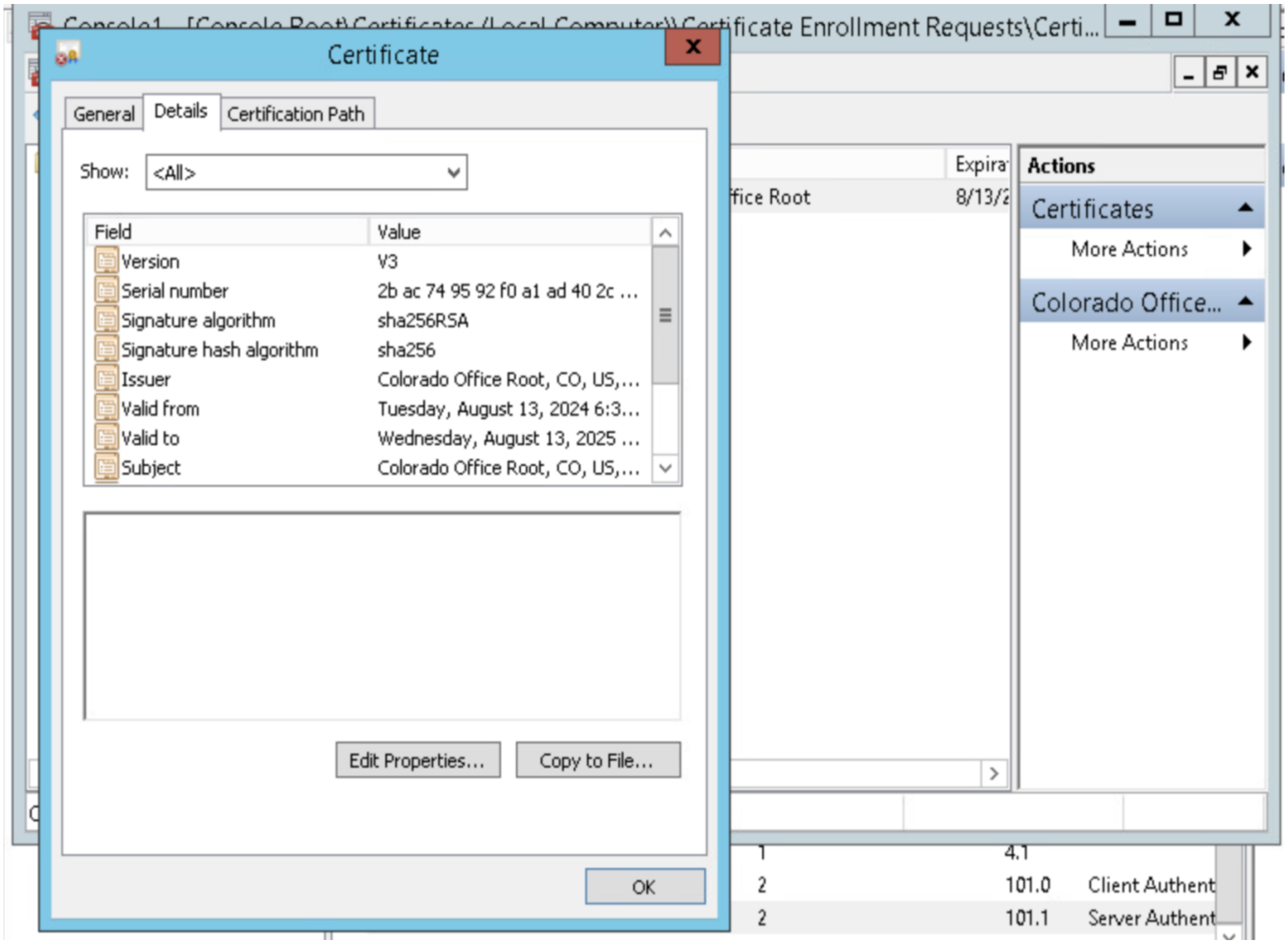
II. Certificate Authority:

a. Provide a screenshot of the **OpenSSL commands** to create a CA with settings that meet the organizational requirements


Administrator: Windows PowerShell ISE
le Edit View Tools Debug Add-ons Help
Untitled1.ps1*(Recovered)
Untitled3.ps1*
Untitled4.ps1*

```
New-SelfSignedCertificate -Type Custom -Subject "CN=Colorado Office Root, C=US, ST=CO, O=Merren-Org"
-KeyAlgorithm RSA -KeyLength 4096 -HashAlgorithm SHA256
-NotAfter (Get-Date).AddMonths(12) -CertStoreLocation "Cert:\LocalMachine\My"
```

```
+                         ~~~~~
    + CategoryInfo          : InvalidArgument: (:) [New-SelfSignedCertificate], ParameterBindingException
    + FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.CertificateServices.Commands.NewSelfSignedC
   ertificateCommand

-KeyAlgorithm : The term '-KeyAlgorithm' is not recognized as the name of a cmdlet, function, script file,
or operable program. Check the spelling of the name, or if a path was included, verify that the path is
correct and try again.
At line:2 char:1
+ -KeyAlgorithm RSA -KeyLength 4096 -HashAlgorithm SHA256
+ ~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (-KeyAlgorithm:String) [], CommandNotFoundException
    + FullyQualifiedErrorId : CommandNotFoundException

-NotAfter : The term '-NotAfter' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the path is
```



Field	Value
Version	V3
Serial number	2b ac 74 95 92 f0 a1 ad 40 2c ...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	Colorado Office Root, CO, US,...
Valid from	Tuesday, August 13, 2024 6:3...
Valid to	Wednesday, August 13, 2025 ...
Subject	Colorado Office Root, CO, US,...

b. Discuss how to create Certificate Signing Requests (**CSRs**) for the servers and workstations in the new location and submit to the CA for approval (CA Applied)

Creating Certificate Signing Requests (CSRs) and submitting them to a Certificate Authority (CA) for approval is fundamental to establishing a secure communications infrastructure. The first step involves generating a private key on each server or workstation that requires a certificate. This private key is essential as it is used to encrypt and decrypt communications, ensuring that data remains secure as it traverses the network. Once the private key is generated, the next step is to create a CSR. The CSR contains information about the organization and the specific server, including the common name (CN), which typically represents the server's domain name. This request is then signed using the private key and includes a hash of the key, which will later be used by the CA to verify the integrity of the request (CrowdStrike, 2023).

After the CSR is generated, it must be securely transferred to the CA. This is a critical step in the process, often done using secure methods such as Secure Copy Protocol (SCP) or Secure File Transfer Protocol (SFTP). These methods are used to ensure that the request is not intercepted or altered in transit, emphasizing the importance of data security at every stage. Once the CA receives the CSR, it is reviewed and, if deemed valid, the CA signs the request to create a digital certificate. This certificate is then returned to the originating server or workstation. The signed certificate, along with the CA's root certificate, is installed on the server. This setup allows the server to establish secure, authenticated connections with clients and other servers, ensuring that communications are encrypted and that the server's identity can be verified by any client that trusts the CA (Eperjesi, 2023).

c. Discuss how **implementing PKI** addresses two of the Fundamental Security Design Principles and how this maintains the tenets of the confidentiality, integrity, and availability (CIA) triad in an organization

Implementing Public Key Infrastructure (PKI) is a critical component of cybersecurity, particularly in upholding the principles of the CIA triad: confidentiality, integrity, and availability. PKI contributes to **confidentiality** by ensuring that data is encrypted and can only be accessed by authorized parties. This encryption process, integral to PKI, helps prevent unauthorized access and protects sensitive information from being exposed or manipulated by unauthorized users. Additionally, **integrity** is maintained through digital signatures and hashing techniques, which verify that data has not been altered during transmission. This guarantees that the information remains trustworthy and unaltered from its original state, thereby preserving its accuracy and reliability (Bristow, 2024; Checkred, 2023).

Furthermore, PKI supports the **availability** aspect of the CIA triad by ensuring that systems are resilient against disruptions. Using certificates ensures that systems can authenticate and continue to operate even when under threat, thereby maintaining the availability of critical services. Integrating PKI into an organization's security architecture effectively enforces these fundamental security principles, providing a robust defense against potential cyber threats (Sanchez, 2024).

III. **Hardening Systems:**

a. Discuss how to make the **transition** from industry guidelines to a baseline that is appropriate for your organization.

Transitioning from broad industry guidelines to a tailored organizational baseline is a critical process that requires careful customization to meet an organization's unique needs. Industry guidelines, such as those provided by NIST or CIS, offer a solid foundation but may only address some organization’s specific operational contexts or security challenges. Organizations must assess their security needs, including regulatory requirements and risk tolerance, to create an adequate baseline. This involves adapting standard guidelines to fit the organization's infrastructure, technology stack, and business processes (Bristow, 2024).

Engaging key stakeholders across departments is crucial during this transition to ensure that the baseline meets the organization's operational requirements without compromising security. This collaborative approach helps balance security with practicality, ensuring the baseline is practical and feasible. Regular reviews and updates of the baseline are also necessary to keep pace with emerging threats and technological advancements, ensuring that the organization's security posture remains solid and adaptive (CheckRed, 2023).

b. Create an **operating system security-configuration checklist** representing the elements used in Part I: Automated Hardening Scripts

Task	Description	Command	Expected Output/Verification	Checked
Hostname Configuration	Rename the computer to Merren.	Rename-Computer -NewName "Merren"	The hostname is set to Merren.	✓
Time Zone Setting	Set the time zone to Mountain Standard Time.	Set-TimeZone -Id "Mountain Standard Time"	The time zone is set to Mountain Standard Time.	✓
Running Processes Documentation	Get a list of running processes and save it to RunningServices.txt.	Get-Service | Where-Object { $_.Status -eq "Running" } \| Out-File "$desktopPath\RunningServices.txt"	File RunningServices.txt contains the list of running services.	✓
Screensaver Idle Lock Time	Set the screensaver idle lock time to 3 minutes.	New-ItemProperty -Path "HKCU:\Control Panel\Desktop" -Name "ScreenSaveTimeOut" -Value 180 -PropertyType String -Force	The screensaver idle timeout is set to 180 seconds.	✓
Security Log Extraction	Output the last 50 security log entries to SecurityLog_Merren.txt.	Get-EventLog -LogName Security -Newest 50 | Out-File "$desktopPath\SecurityLog_Merren.txt"	File SecurityLog_Merren.txt contains the last 50 security log entries.	✓

c. Explain why operating system security-configuration checklists are an important part of the **cybersecurity practices** in an organization.

Operating system security-configuration checklists are essential tools in cybersecurity practices, providing a structured approach to ensuring that all necessary security measures are consistently applied across an organization. These checklists help standardize security practices, ensuring each system meets a defined security baseline. This reduces the risk of configuration errors, which can introduce vulnerabilities, and ensures all systems are secured to the same standard. By following a checklist, organizations can streamline the process of securing systems, saving time and reducing the complexity of managing multiple systems (Bristow, 2024).

Moreover, security-configuration checklists play a vital role in compliance and audit readiness. They provide clear documentation of the security measures that have been implemented, making it easier for organizations to demonstrate compliance with regulatory standards during audits. This helps maintain regulatory compliance and strengthens the overall security posture by ensuring that all security measures are thoroughly documented and regularly reviewed (Sanchez, 2024).

References

Eperjesi, A. (2023, September 1). *10 Key benefits of Security Automation - Blink*. https://www.blinkops.com/blog/benefits-of-security-automation

CrowdStrike. (2023, March 1). *Security Automation: 5 best practices & more - CrowdStrike*. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/security-automation/

Tanium Inc. (2024, March 21). *What is Security Automation? Benefits, Importance, and Features | Tanium*. Tanium. https://www.tanium.com/blog/what-is-security-automation/

Checkred. (2023, December 27). Back to the basics: applying the CIA triad to modern security posture - checkred. *CheckRed*. https://checkred.com/resources/blog/back-to-the-basics-applying-the-cia-triad-to-modern-security-posture/

Bristow, T. (2024, June 24). The CIA triad: a foundation for cybersecurity. *The CIA triad: a foundation for cybersecurity*. https://www.nextdlp.com/resources/blog/the-cia-triad-a-foundation-for-cybersecurity

Sanchez, S. (2024, June 29). *The CIA triad: confidentiality, integrity, and availability*. The H.A.C.K.E.R. Project. Retrieved August 13, 2024, from https://thehackerproject.org/2024/05/19/the-cia-triad-confidentiality-integrity-and-availability/