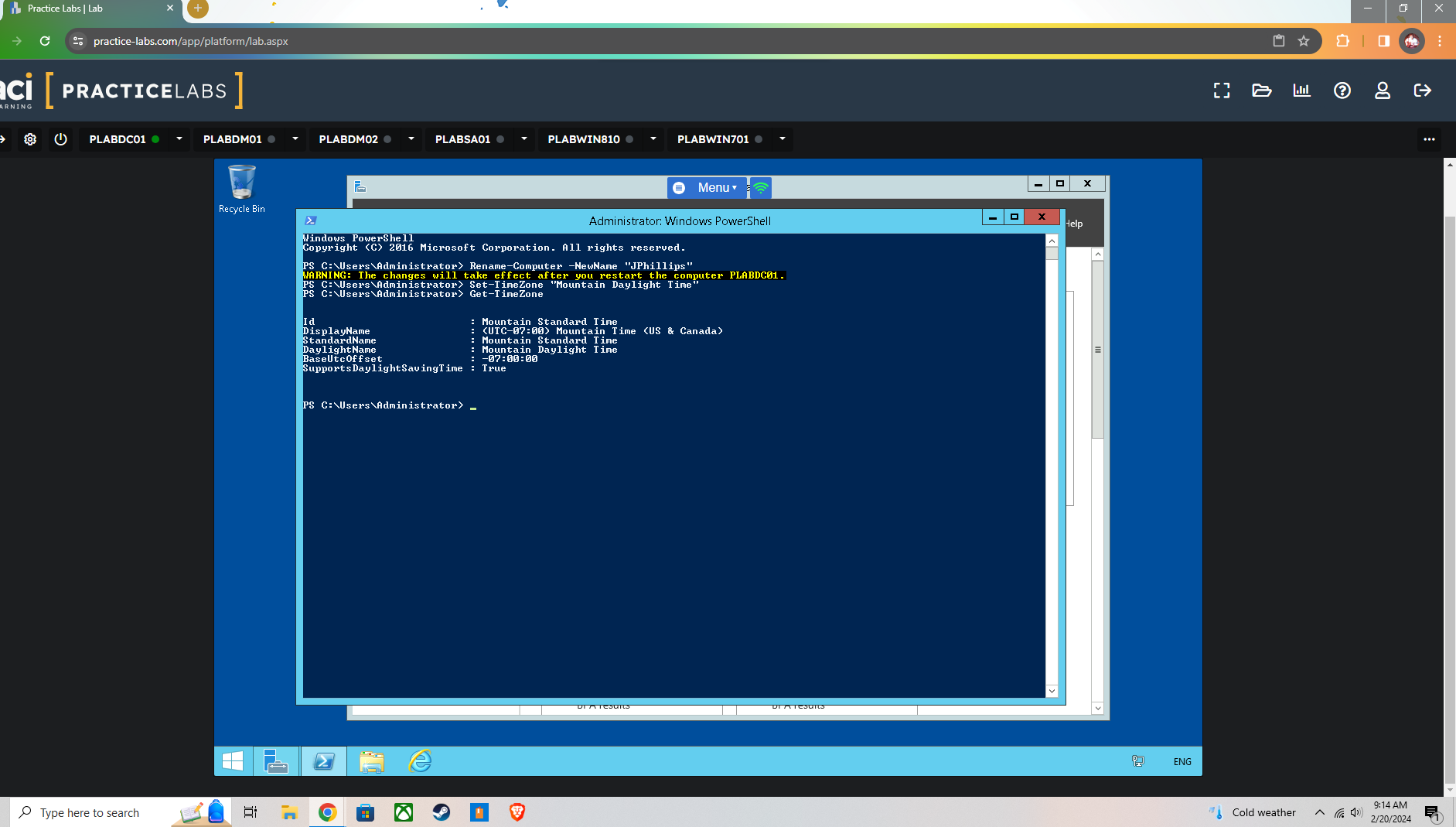
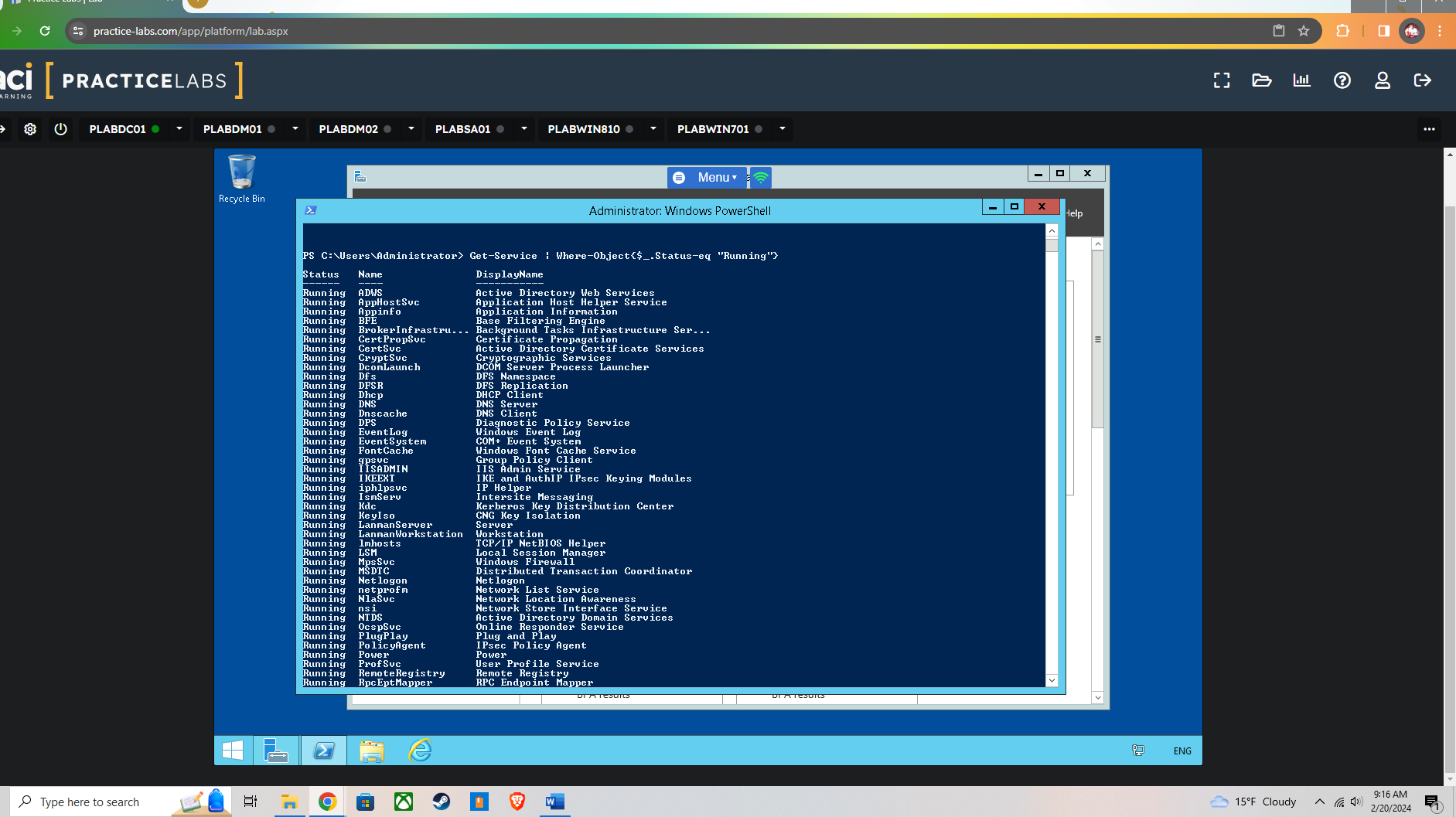
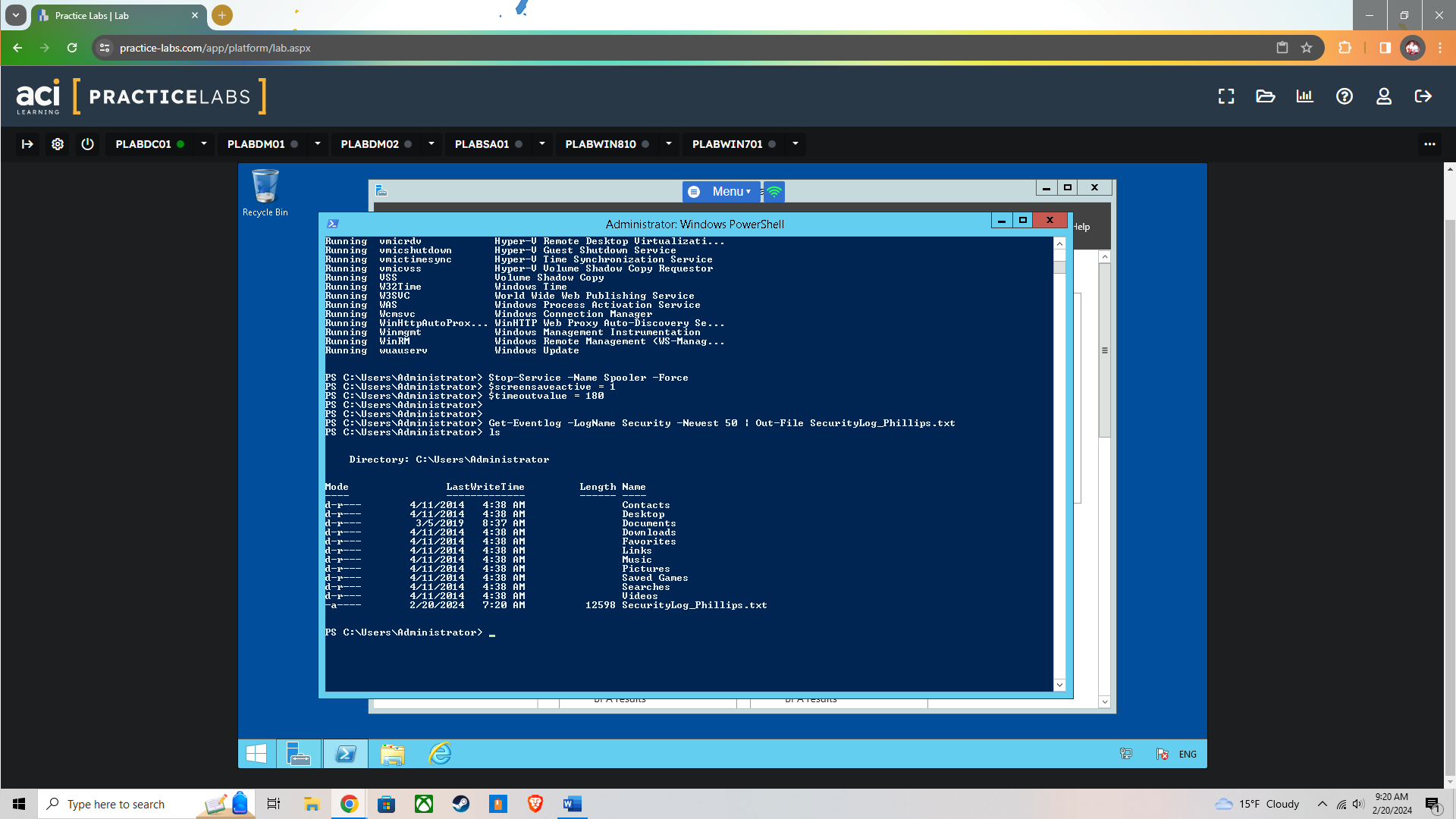
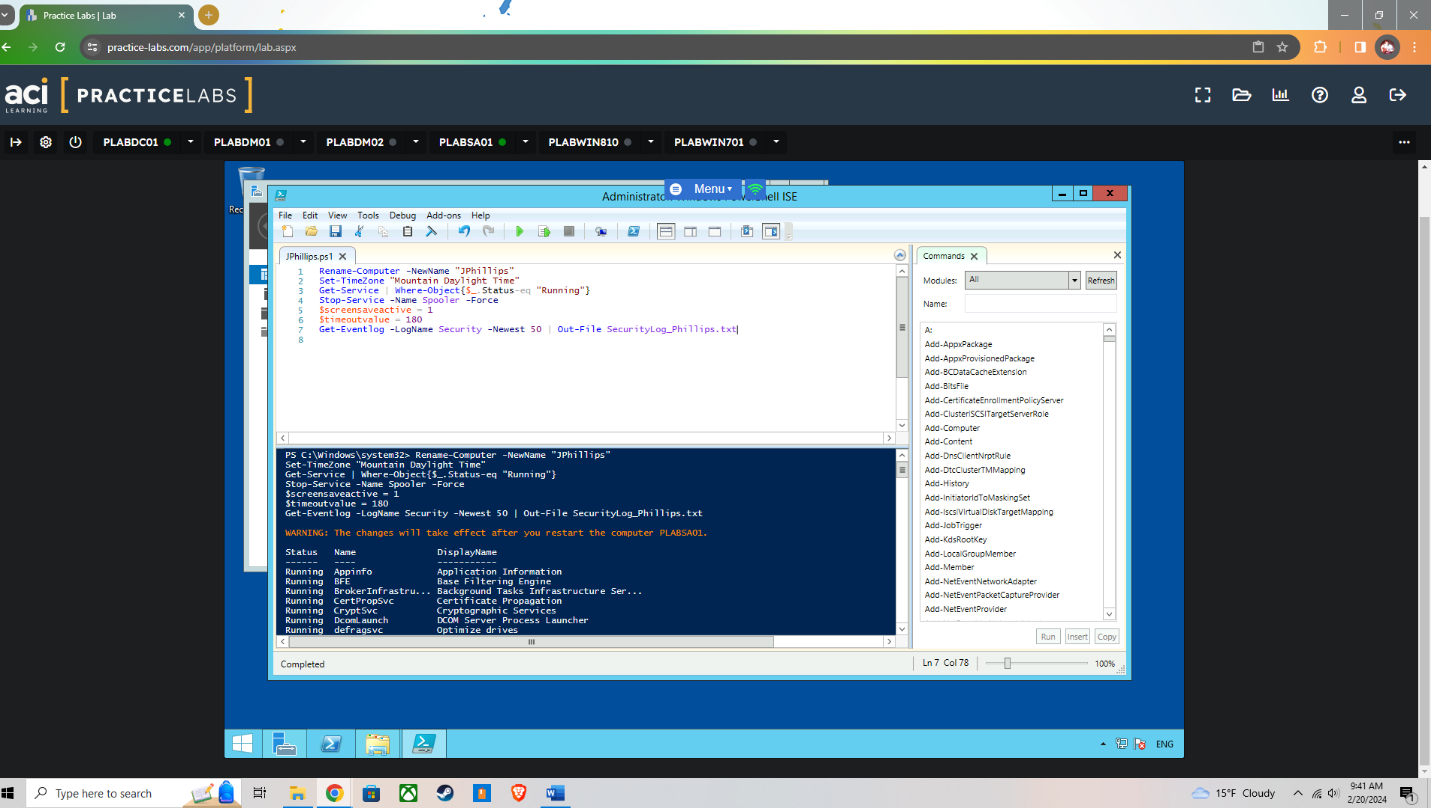
Part 1:  
  
Rename Computer to First Initial and last name, and change time zone to what Denver Colorado would be:  
  


Get a list of running Services:  
  


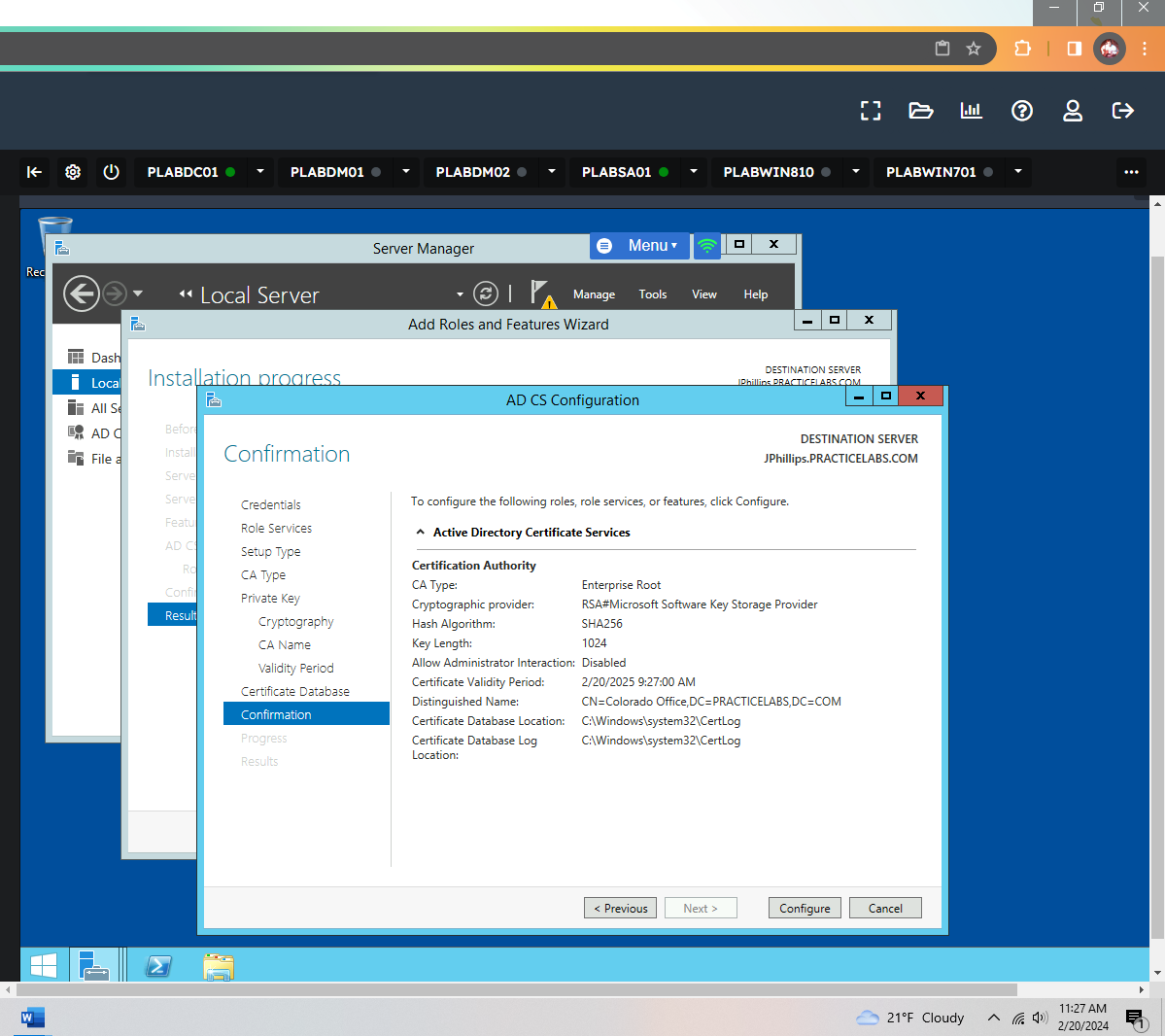
I tried to put all the commands into one screen shot instead of multiple that would end up taking up a mass amount of space and time. The next steps for stop the print spooler service, set idle lock time for screensaver, and send output of first 50 entries in security event log are shown below:  
  


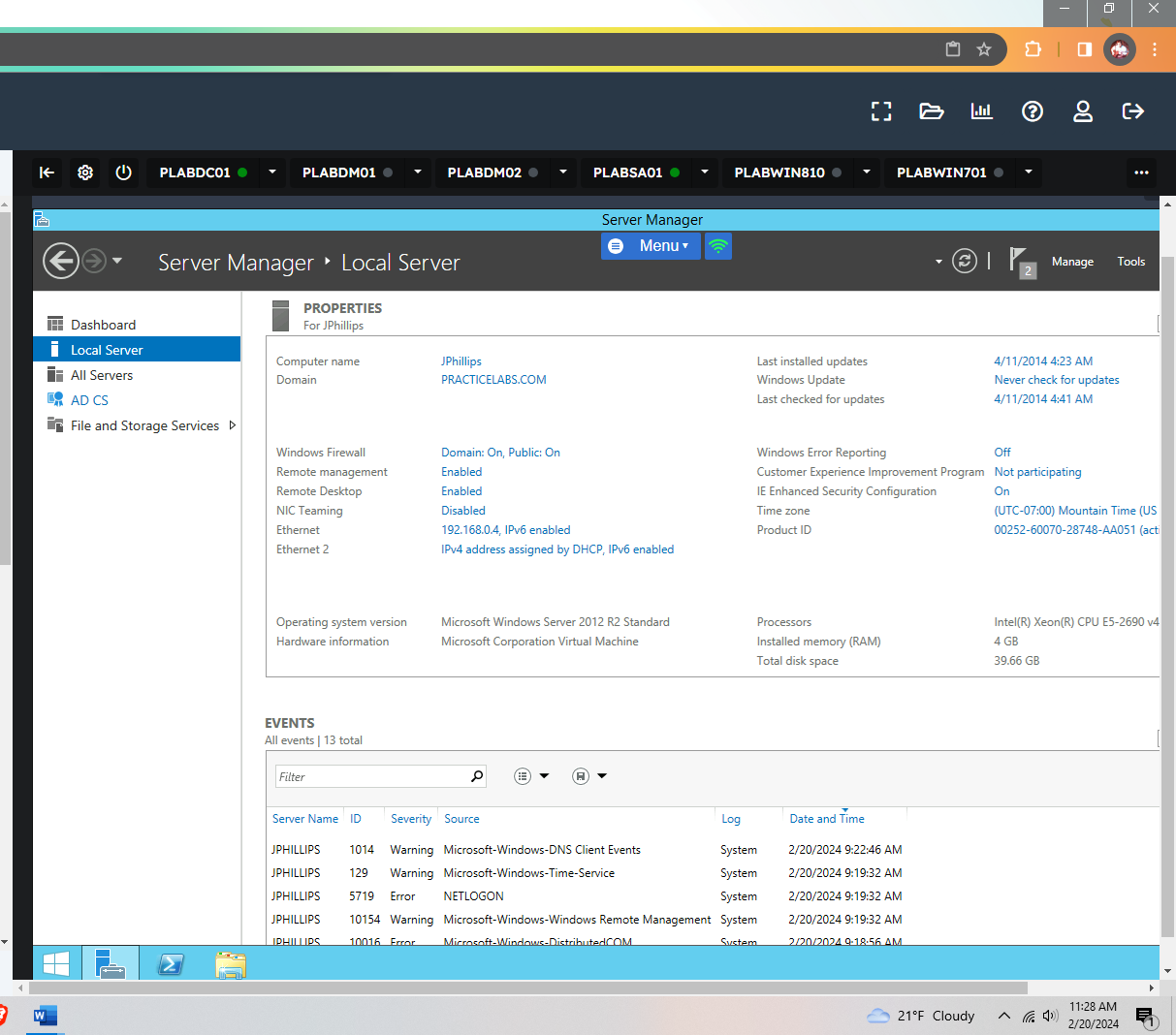
Verification that the script runs:  
  


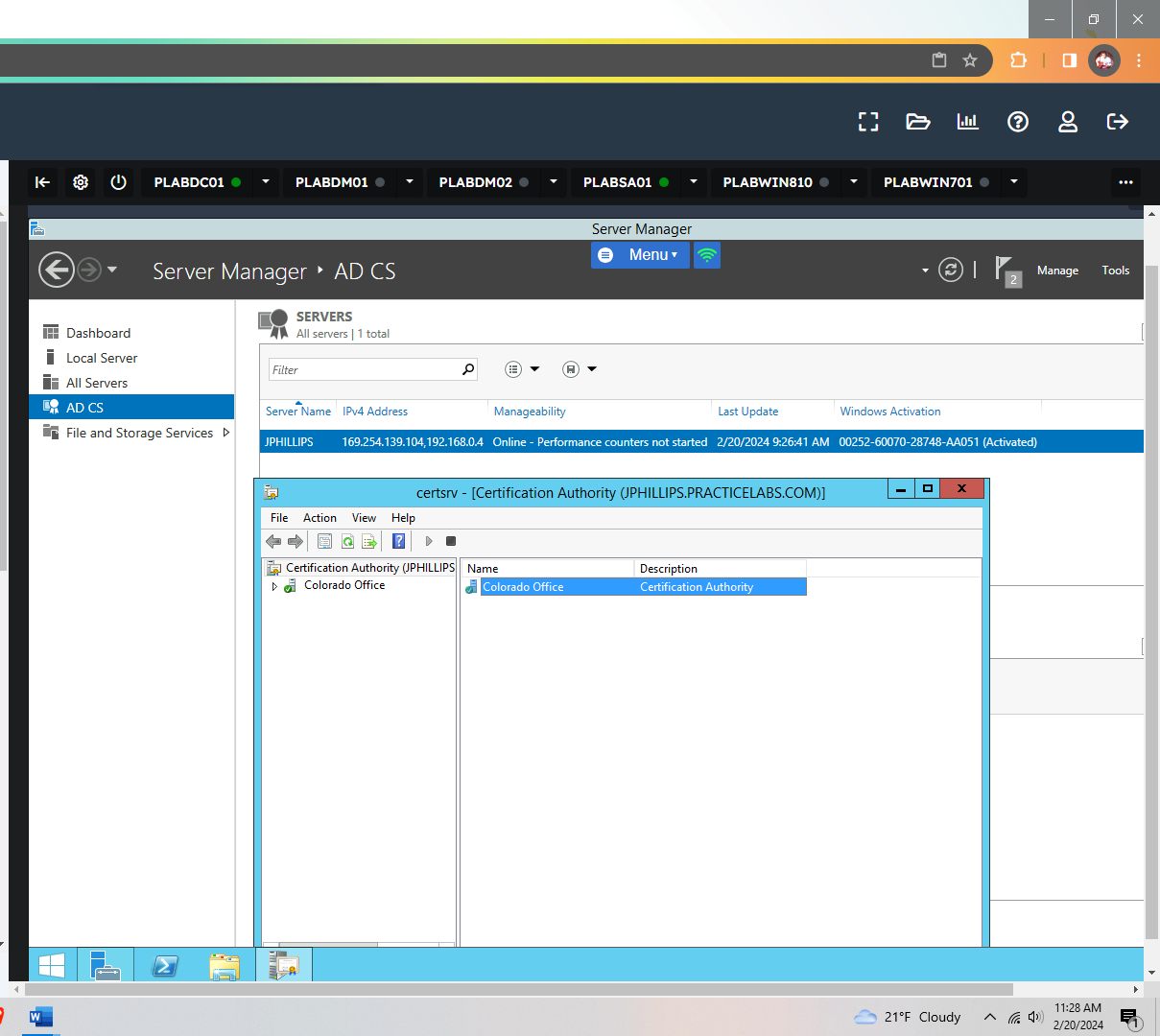
Automated scripts not only save time but also ensure consistency and accuracy across configurations, reducing the risk of human error. They enable organizations to implement security best practices uniformly across all systems, enhancing overall security posture. Additionally, automation supports rapid deployment and scaling, allowing security measures to be efficiently applied as the infrastructure grows or changes.

Part 2:

This took me quite some time because I followed what we had did in the labs, however I used the wrong computer and could not figure out why the script I was using would not work. Those labs are finicky to say the least.



Here is the computer I renamed to my name and the certificate running on it as such:  
  




Implementing Public Key Infrastructure (PKI) directly addresses the Fundamental Security Design Principles of Least Privilege and Layered Defense. By employing PKI, an organization ensures that only authorized individuals or systems can access certain data or resources, adhering to the Least Privilege principle by limiting access rights to the minimum necessary. Furthermore, PKI contributes to Layered Defense (or Defense in Depth) by adding an additional security layer through encryption, digital signatures, and certificate management, which secures data in transit and at rest against unauthorized access and tampering. This multifaceted approach reinforces the Confidentiality, Integrity, and Availability (CIA) triad by ensuring that sensitive information remains private (confidentiality), data is not altered by unauthorized entities (integrity), and information and resources are available to authorized users when needed (availability).

**Transition from Industry Guidelines to an Organizational Baseline**

**1.** Begin by thoroughly reviewing and understanding industry guidelines and standards relevant to your organization. These might include NIST frameworks, ISO/IEC standards, CIS Benchmarks, and others. These guidelines provide a wealth of knowledge on best practices for securing information systems and managing cybersecurity risks.

**2.** Evaluate your organization's specific needs, including the nature of your business, regulatory requirements, and unique risk profile. Consider factors such as the sensitivity of the data you handle, your IT infrastructure, and previous security incidents.

**3.** Conduct a gap analysis by comparing current security practices against industry guidelines. This analysis will highlight areas of strength and areas needing improvement, providing a clear picture of the adjustments needed to meet or exceed industry standards.

**4.** Use the insights from the gap analysis to tailor the industry guidelines to your organization's context. This involves prioritizing recommendations based on your specific risk assessment, legal and regulatory requirements, and business objectives. It may also involve adjusting security controls to be more stringent or adding new controls to address specific organizational vulnerabilities.

**5.** From this tailored set of guidelines, develop a security baseline that serves as the minimum security standard for your organization. This baseline should be comprehensive, covering various aspects of cybersecurity, including access control, data encryption, network security, and incident response.

**6.** Implement a process for regularly reviewing and updating the security baseline to reflect emerging threats, technological advancements, and changes in business processes or regulatory requirements.

|  |  |  |
| --- | --- | --- |
| Services | CMDLET | Complete |
| Change Computer name | Rename-Computer | X |
| Change Time Zone to MDT | Set-TimeZone | X |
| Get Running Services | Get-Services | X |
| Stop the Print Spooler | Stop Services | X |
| Activate Screensaver | $ScreenSaveActive | X |
| Idle lock time | $TimeOutValue | X |
| Event Log | Get-EventLog | X |
| Windows Firewall | Implement | X |
| Certificates | Colorado Office | X |
|  |  |  |
|  |  |  |

This is just an example, I had more boxes because I was going to go into extreme detail but I feel as if I have already went over board on the number of pages that are supposed to be within this project, and I spent about 2 days’ time figuring everything out with a lot of trial and errors. It is safe to say that I can now implement a certificate in my sleep, as for the scripting; this still needs plenty of work, but I am sure that within the field I will pick it up naturally, I also plan to keep furthering my education once I finish up a few more certifications. Checklists provide a framework that can be easily duplicated so all parts of the systems are uniform. A uniformed system is easier to manage and keep secure. These checklists are valuable when you need to expand the network you are working on or you are securing a new network. As a cybersecurity consultant, this can be helpful when working with different companies. The checklist can also be modified to suit the companies needs.