Advent of Cyber, Day 23 is live! ⚡️🐚 Use PowerShell & Windows Event Logs to investigate an attack  
  
🎄Analyze event logs & see how an attack occurred  
🎄Recover key artifacts in unencrypted coms  
🎄Use PowerShell Scripting & recover a deleted artifact

One of the administrators with access to the Elf Dome Defense system realized that his password file was missing from his desktop. Without the password, he will not be able to log into the Mission Control panel. McSkidy suspects that perhaps one of the previous phishing attempts was successful. McSkidy jumps into action.

You need to inspect the event logs to determine what has occurred and see if you can retrieve the password from the deleted text file. -

Learning Objectives:

* Analyze Windows event logs to understand actions performed in an attack.
* Recover key artifacts in unencrypted web communications.
* Utilize PowerShell Scripting to recover a delete artifact.

**PowerShell** comes baked into the Windows Operating System. It is a beneficial tool for Windows Administrators to automate day-to-day tasks. PowerShell has also allowed adversaries to perform nefarious activities, a concept known as Living off the Land.

The official definition of PowerShell per Microsoft - "***PowerShell is a cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework. PowerShell runs on Windows, Linux, and macOS***."

Link - <https://docs.microsoft.com/en-us/powershell/scripting/overview?view=powershell-7.2>

As defenders, we can audit commands run in the PowerShell console on each workstation. This is known as **PowerShell Logging**. When a PowerShell command or script is run, the activity is logged into the Windows Event Log system.

<https://gtfobins.github.io/> // for the living off the land linux

Many event logs are generated in a Windows system, but the logs we care about are specific to PowerShell.

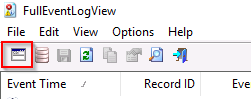
Event logs are categorized by providers, such as **Microsoft-Windows-PowerShell**. Each provider has specific event ids to identify particular events or actions that occurred on the workstation. The event ids of interest for us in this investigation are **4103** and **4104**.

Typically you'll use **Event Viewer** to view event logs locally on a Windows system, but we installed a nifty tool called **Full Event Log View** to help make this a painless experience.

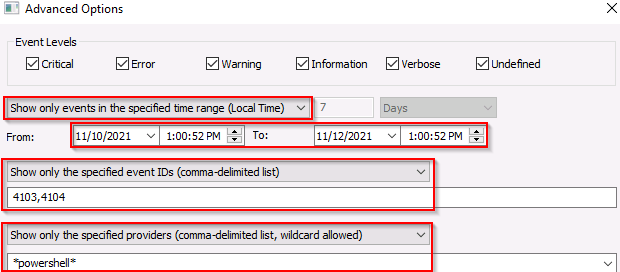
When you start the tool, it will display a large number of event logs. Fret not; search is your friend.

https://assets.tryhackme.com/additional/samaoc3/search-tool2.png

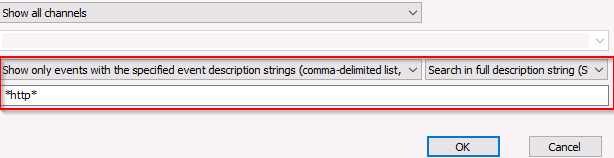
Open the **Advanced Options** to start your search.



The events of interest on this endpoint took place a few weeks ago, specifically during the week of **November 11th, 2021**. Use the below search criteria to get you started.



Alternatively, you can search based on a string value, a keyword. You know there is web traffic involved in the attack. Maybe a good keyword to use would be '**HTTP**.'



Additional resources:

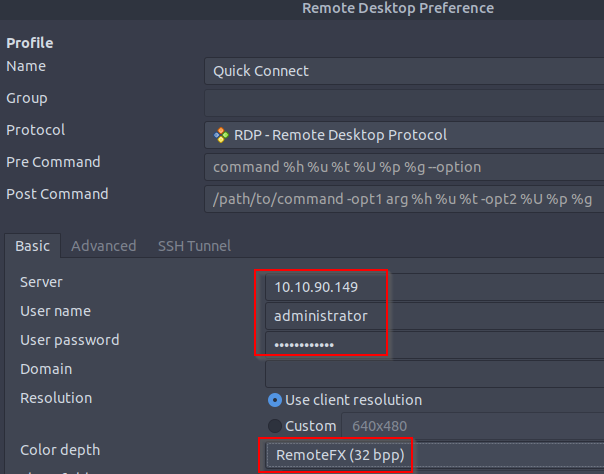
* Investigating Windows 2.0: <https://tryhackme.com/jr/investigatingwindows2>
* Investigating Windows 3.x: <https://tryhackme.com/jr/investigatingwindows3>
* PowerShell for Pentesters: <https://tryhackme.com/jr/powershellforpentesters>

If you wish to access the virtual machine via Remote Desktop, use the credentials below.

**Machine IP**: MACHINE\_IP

**User**: administrator

**Password**: sn0wF!akes!!!

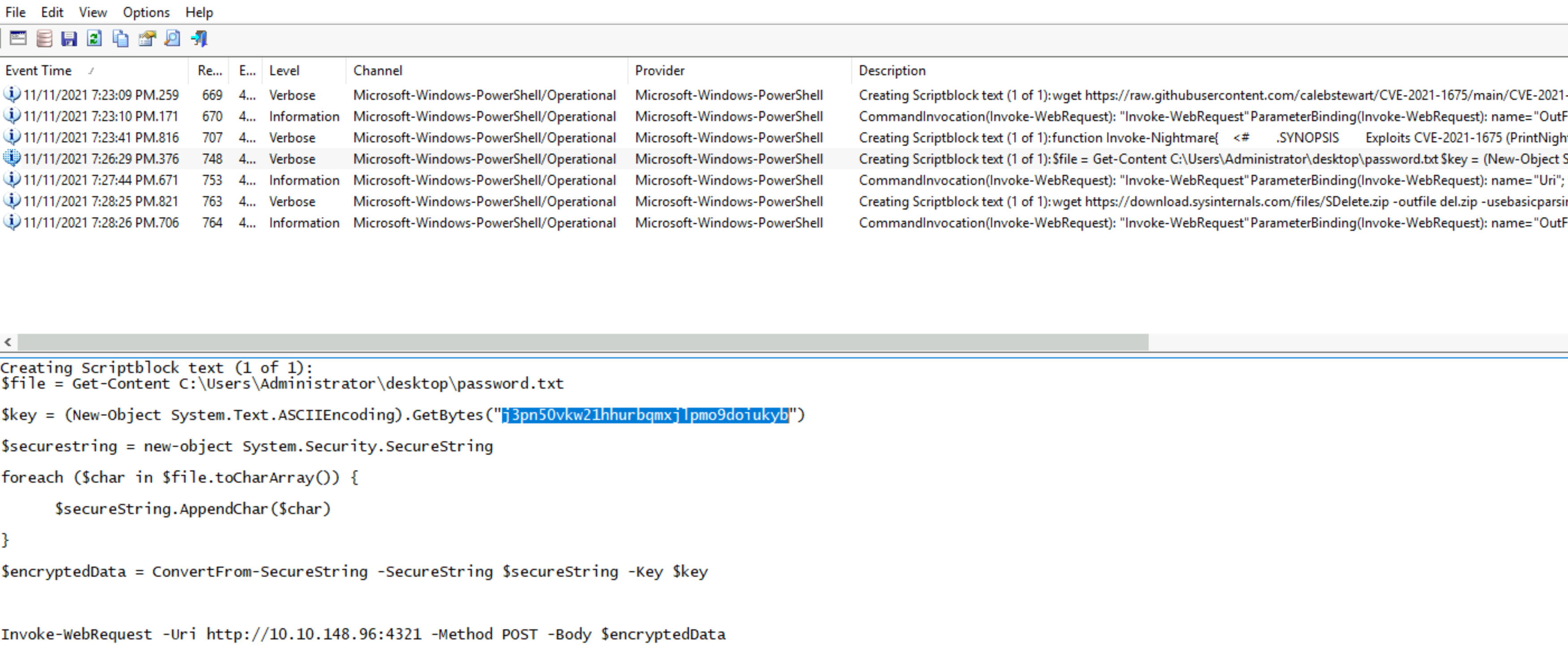


Accept the Certificate when prompted, and you should be logged into the remote system now.

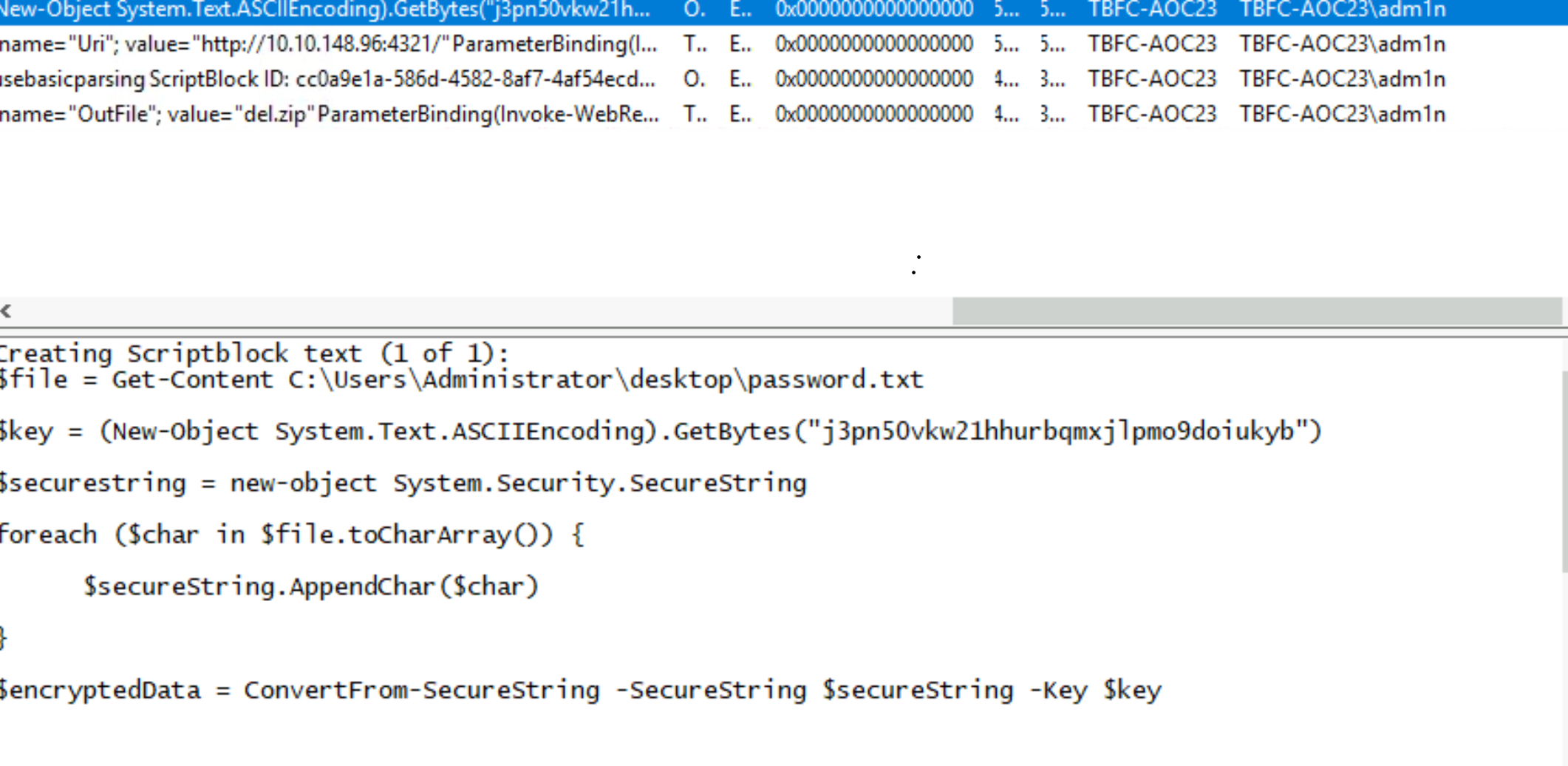
**Note**: The virtual machine may take up to 3 minutes to load.

***Answer the questions below***

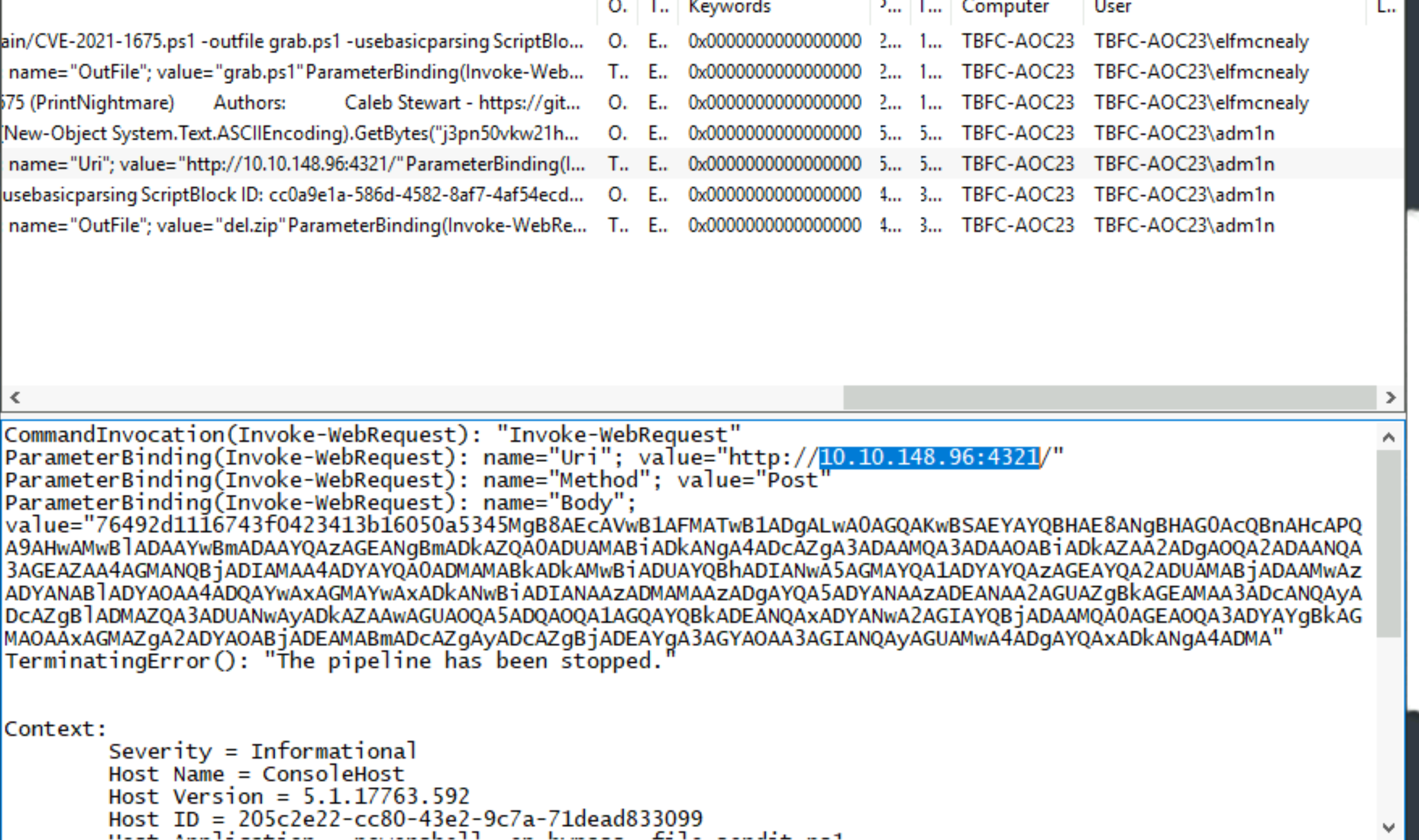
What command was executed as Elf McNealy to add a new user to the machine?



What user executed the PowerShell file to send the password.txt file from the administrator's desktop to a remote server?



What was the IP address of the remote server? What was the port used for the remote connection? (format: IP,Port)

What was the encryption key used to encrypt the contents of the text file sent to the remote server?



 Submit

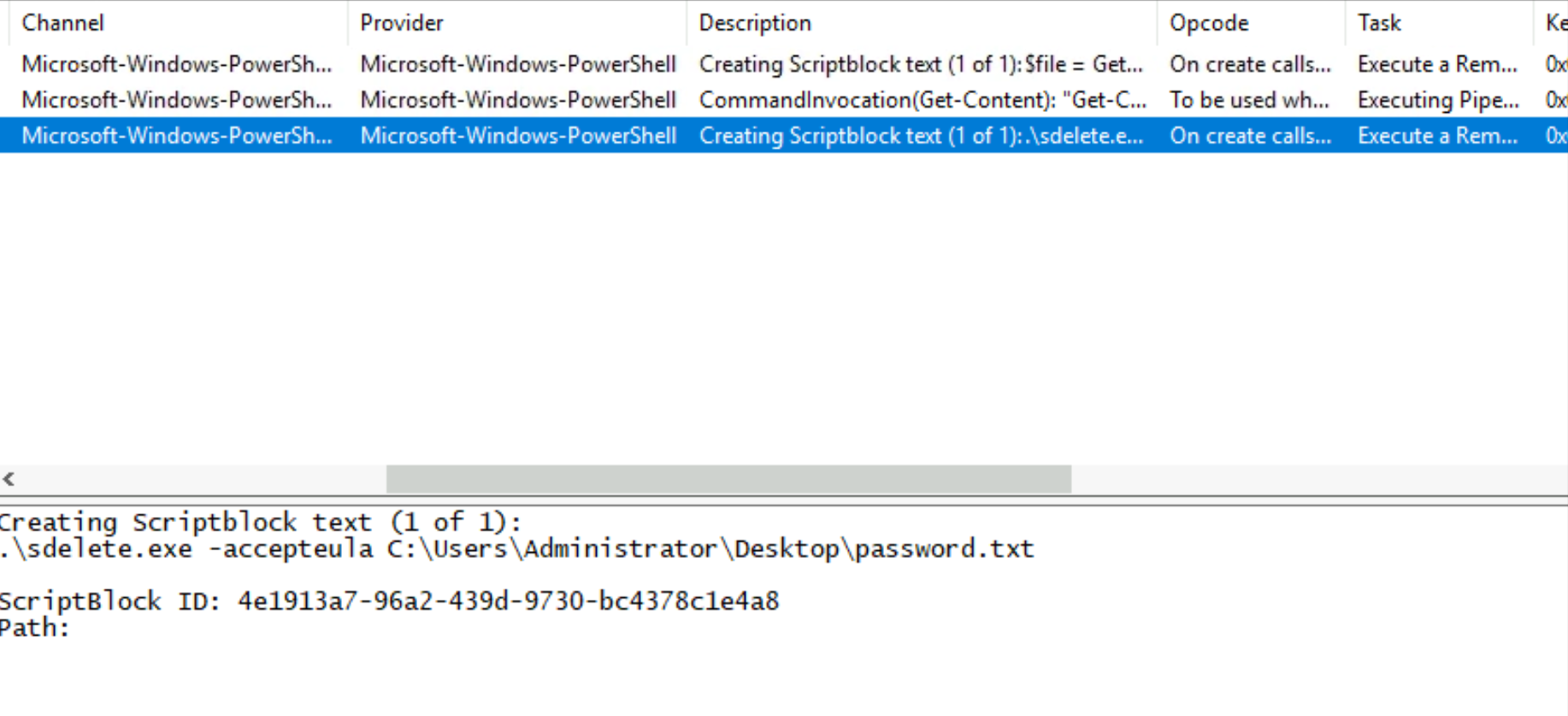
 Hint

What application was used to delete the password.txt file?

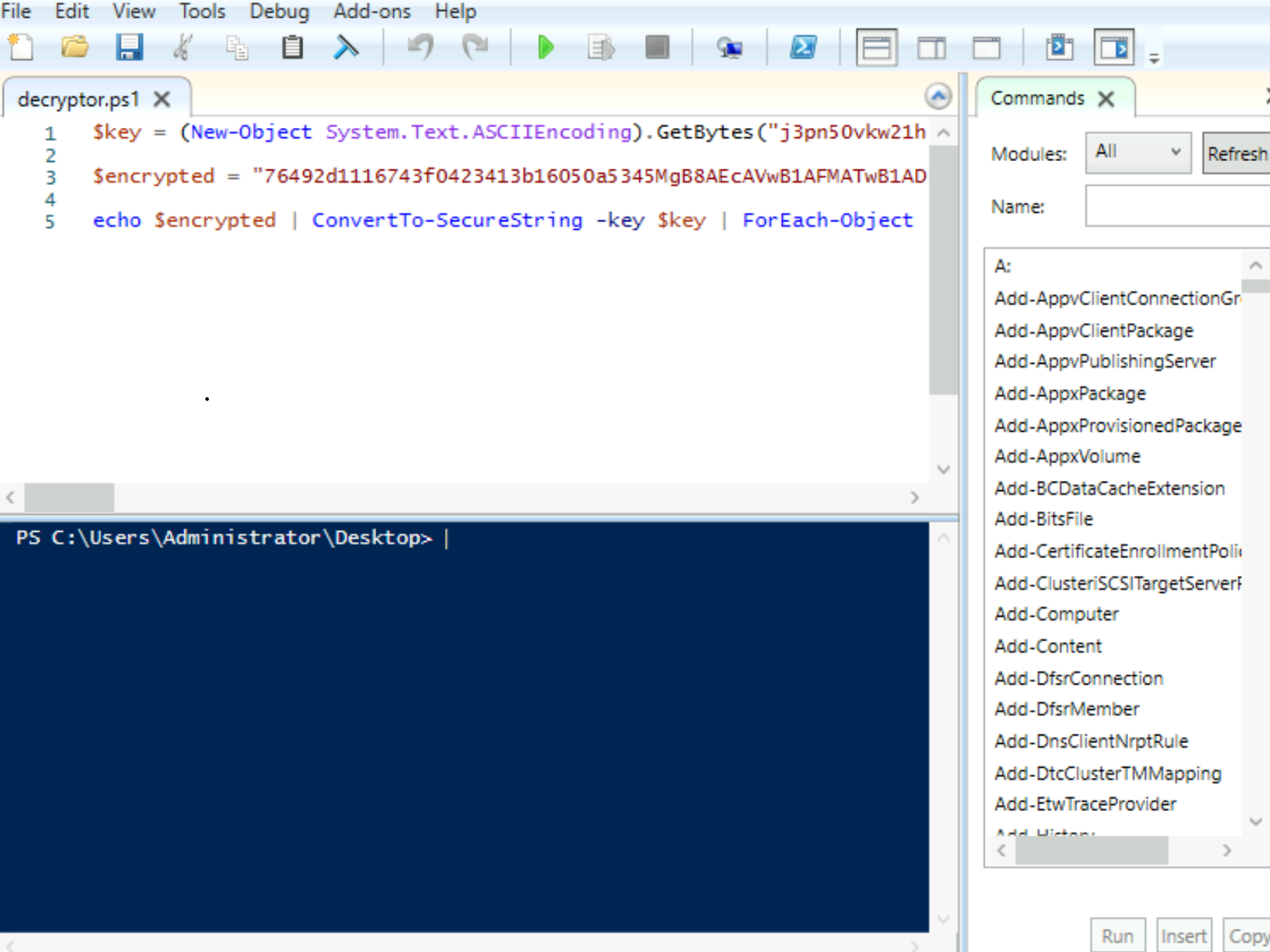


 Submit

What is the date and timestamp the logs show that password.txt was deleted? (format: MM/DD/YYYY H:MM:SS PM)



What were the contents of the deleted password.txt file?



Execution it give the phrase