Login Session Length

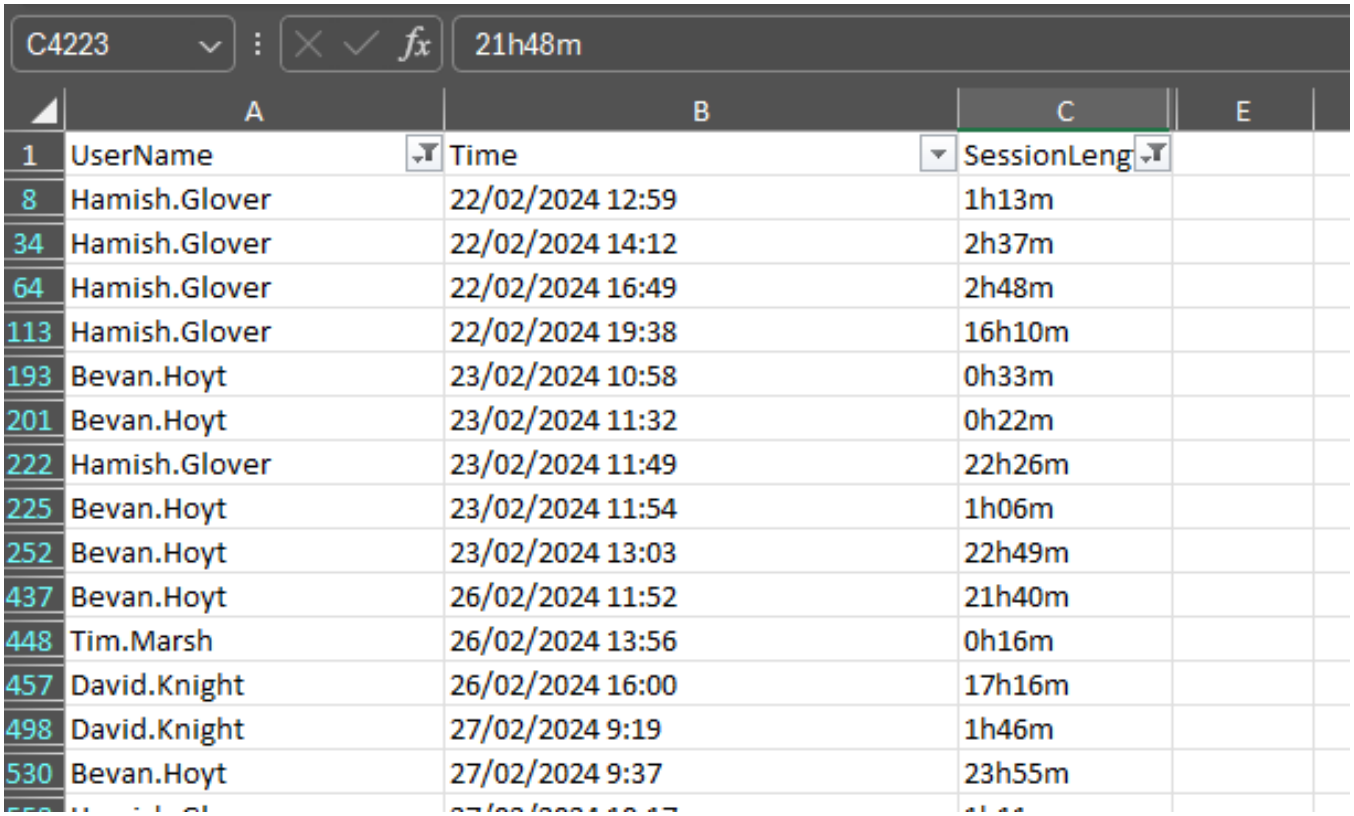
This PowerShell script gathers login and logoff events from the Security log, calculates session lengths for each user session, and exports the information to a CSV file.

Here's a breakdown of what each part of the script does:

1. **Convert-TicksToTime Function**: This function takes ticks (a unit of time in .NET framework) as input and converts them into a readable time format in hours and minutes.
2. **Get-WinEvent Cmdlet**: It retrieves events from the Security log with event IDs 4624 (logon events) and 4625 (logoff events). It sorts the events by their creation time.
3. **$logins Array**: This array will store login information.
4. **Loop Through Events**: For each event retrieved, it parses the XML representation of the event to extract relevant properties such as time, event ID, and username.
5. **Calculating Session Length**: For logoff events (event ID 4624), it looks for the next logon event for the same user and calculates the session length by subtracting the logon time from the logoff time. It uses the `Convert-TicksToTime` function to convert the time difference from ticks to a human-readable format.
6. **Export to CSV**: Finally, it exports the collected login information to a CSV file named 'LoginInfo.csv' without including type information.

In summary, this script is a utility to collect and analyze user login and logoff events from the Windows Security log and export them to a CSV file for further analysis or reporting.

Preview of output (fiiltered)



C4223 : fx 21h48m

	A	B	C	E
1	UserName	Time	SessionLeng	
8	Hamish.Glover	22/02/2024 12:59	1h13m	
34	Hamish.Glover	22/02/2024 14:12	2h37m	
64	Hamish.Glover	22/02/2024 16:49	2h48m	
113	Hamish.Glover	22/02/2024 19:38	16h10m	
193	Bevan.Hoyt	23/02/2024 10:58	0h33m	
201	Bevan.Hoyt	23/02/2024 11:32	0h22m	
222	Hamish.Glover	23/02/2024 11:49	22h26m	
225	Bevan.Hoyt	23/02/2024 11:54	1h06m	
252	Bevan.Hoyt	23/02/2024 13:03	22h49m	
437	Bevan.Hoyt	26/02/2024 11:52	21h40m	
448	Tim.Marsh	26/02/2024 13:56	0h16m	
457	David.Knight	26/02/2024 16:00	17h16m	
498	David.Knight	27/02/2024 9:19	1h46m	
530	Bevan.Hoyt	27/02/2024 9:37	23h55m	

```
# Function to convert ticks to a readable time format (hours and minutes)
function Convert-TicksToTime {
    param(
        [Parameter(Mandatory=$true)]
        [long]$Ticks
    )
    return [TimeSpan]::FromTicks($Ticks).ToString('h\hmm\m')
}

# Get all login events
$loginEvents = Get-WinEvent -FilterHashtable @{
    LogName='Security';
    ID=4624, 4625; # Logon and logoff event IDs
} -ErrorAction SilentlyContinue | Sort-Object TimeCreated

# Array to store login information
$logins = @()

foreach ($event in $loginEvents) {
    $eventXML = [xml]$event.ToXml()
```

```
    $properties = @{
        'Time' = $event.TimeCreated
        'EventID' = $event.Id
        'UserName' = $event.Properties[5].Value
        'SessionLength' = ''
    }

    # If it's a logoff event, calculate session length
    if ($event.Id -eq 4624) {
        $logoffEvent = $loginEvents | Where-Object { $_.Properties[5].Value -eq
$properties['UserName'] -and $_.TimeCreated -gt $event.TimeCreated } | Select-Object -First 1
        if ($logoffEvent) {
            $properties['SessionLength'] = Convert-TicksToTime ($logoffEvent.TimeCreated -
$event.TimeCreated).Ticks
        }
    }

    $logins += New-Object PSObject -Property $properties
}

# Export to CSV
$logins | Export-Csv -Path 'LoginInfo.csv' -NoTypeInformation
```

Revision #2
Created 2024-03-17 00:45:47 UTC by Slitzer
Updated 2024-03-17 00:51:30 UTC by Slitzer