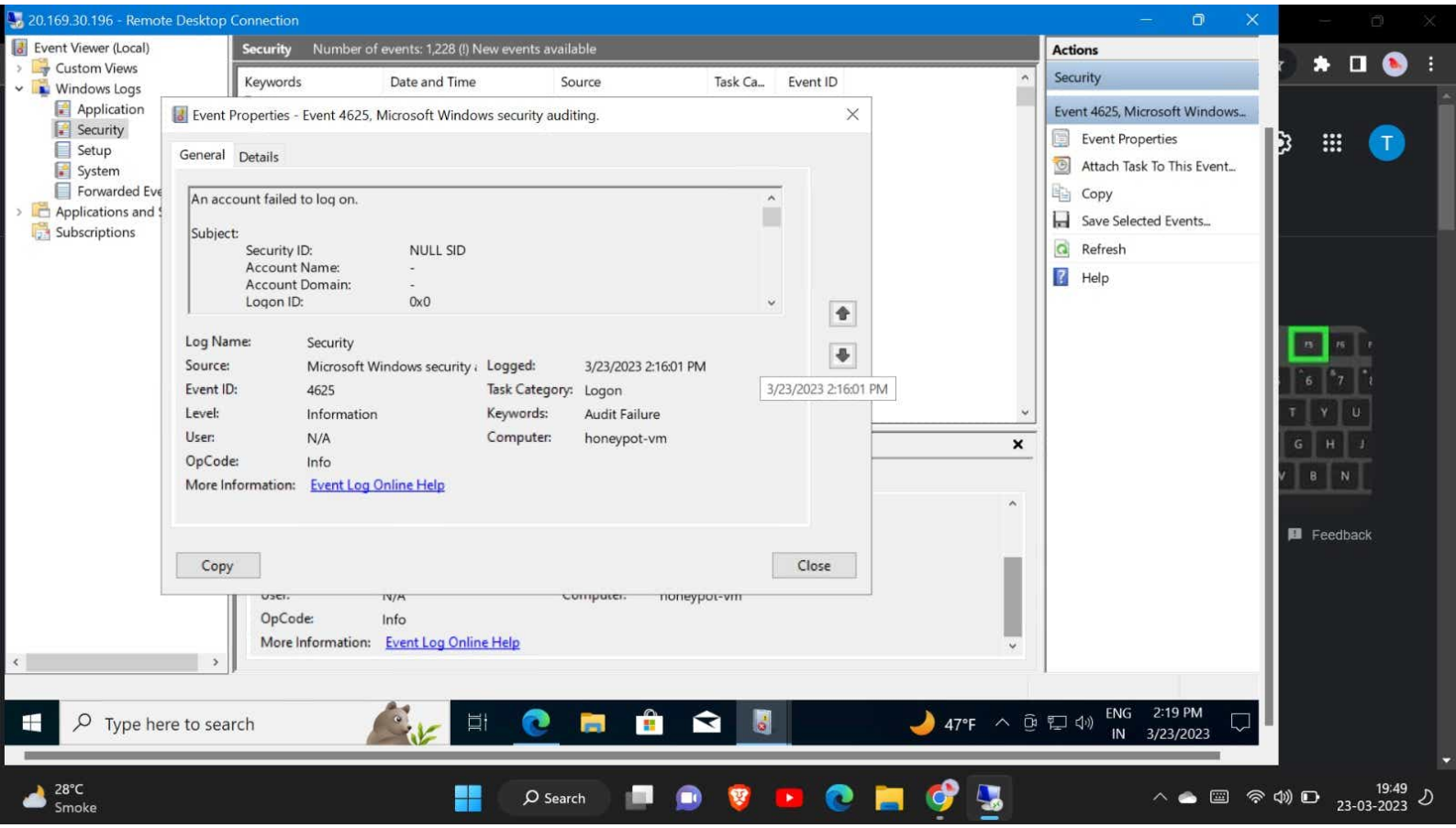
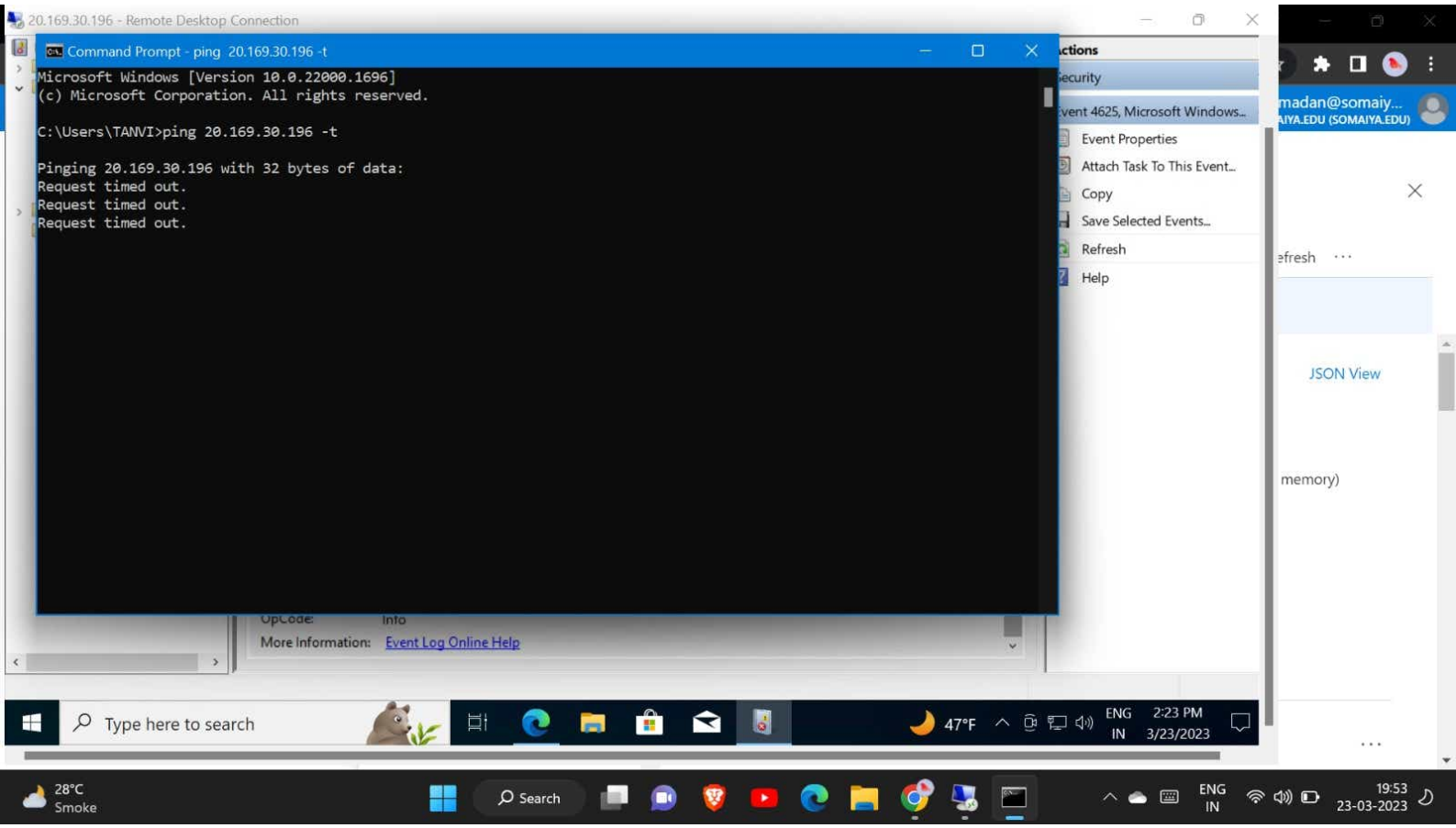
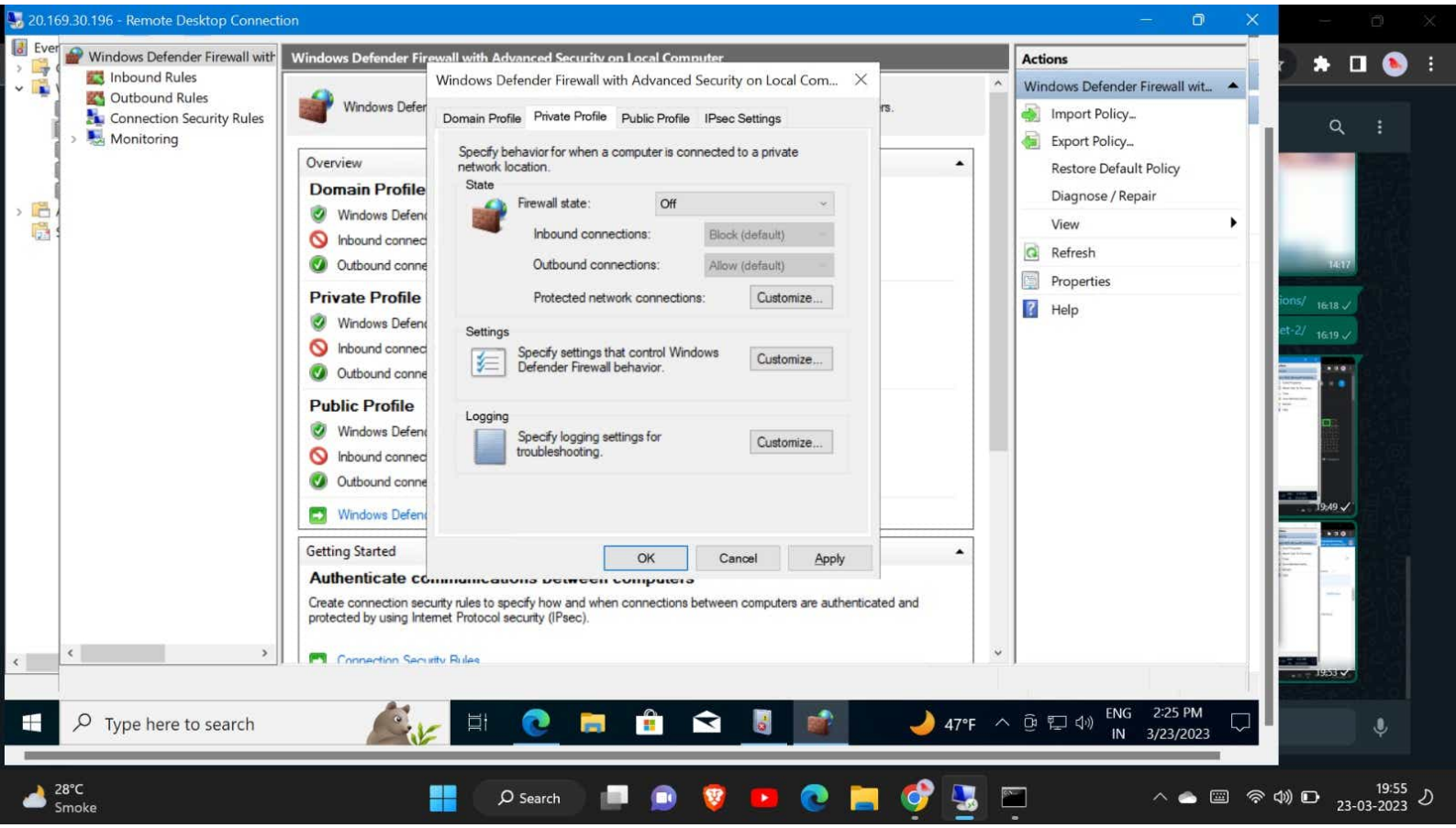
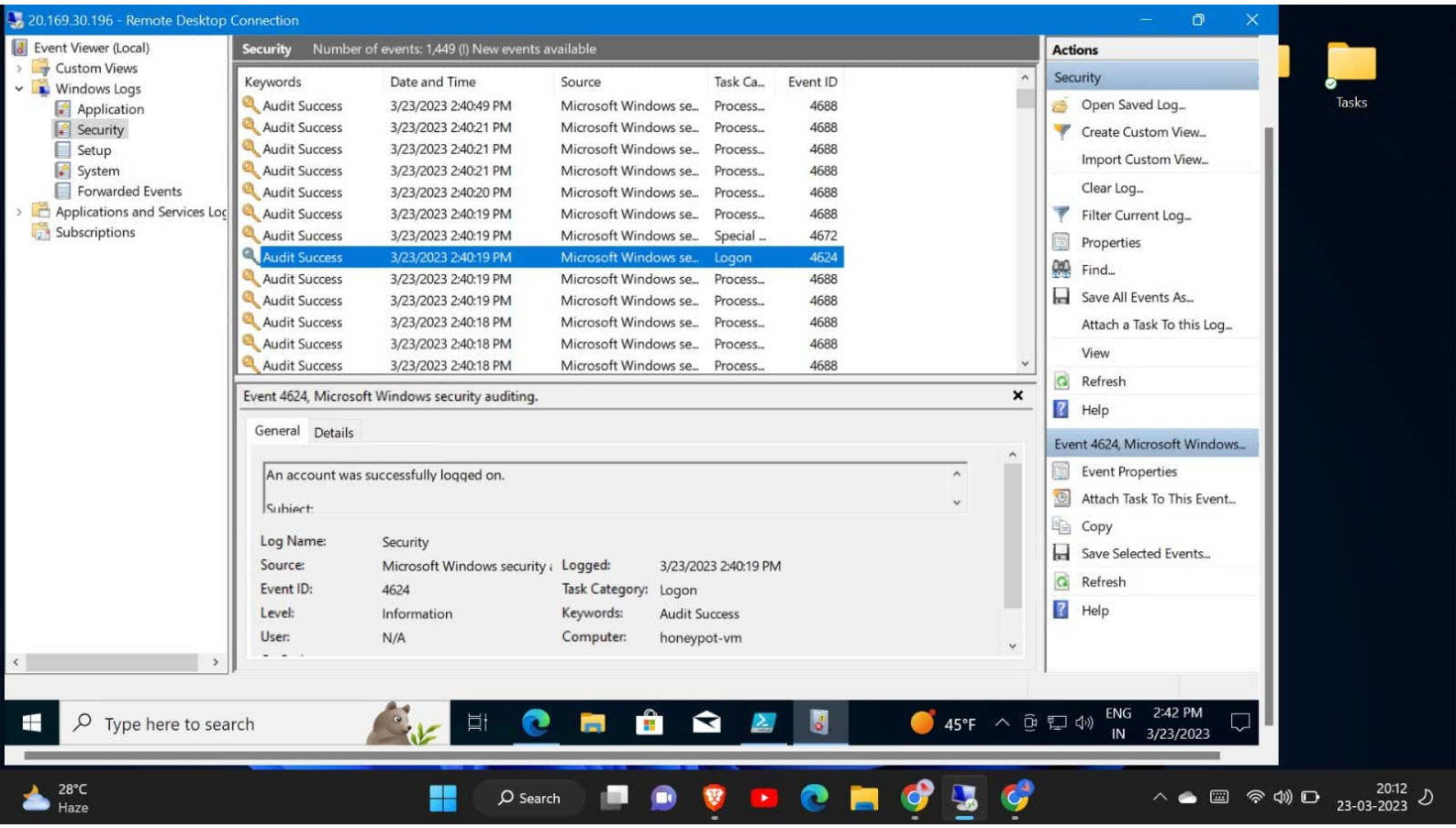
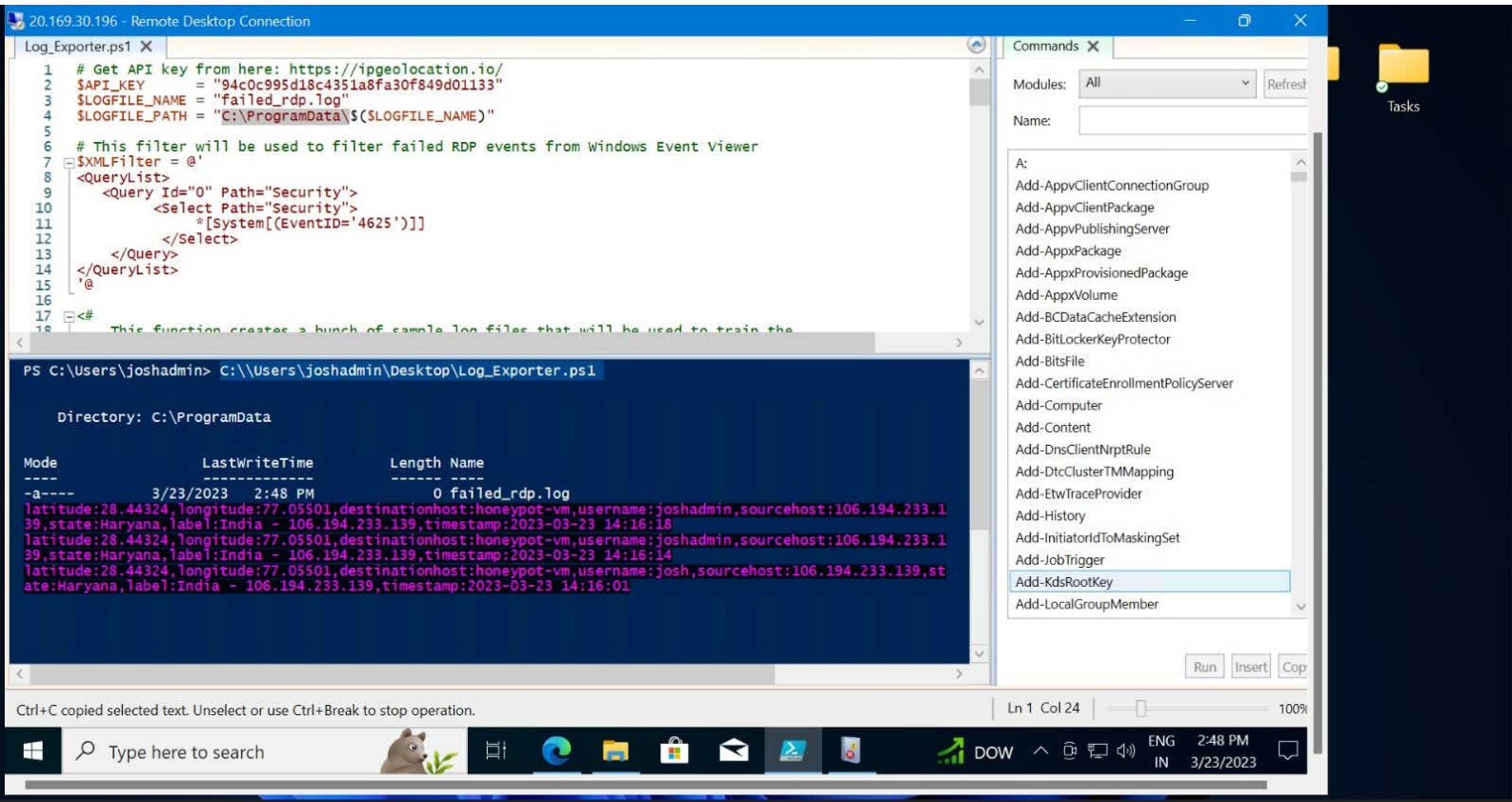
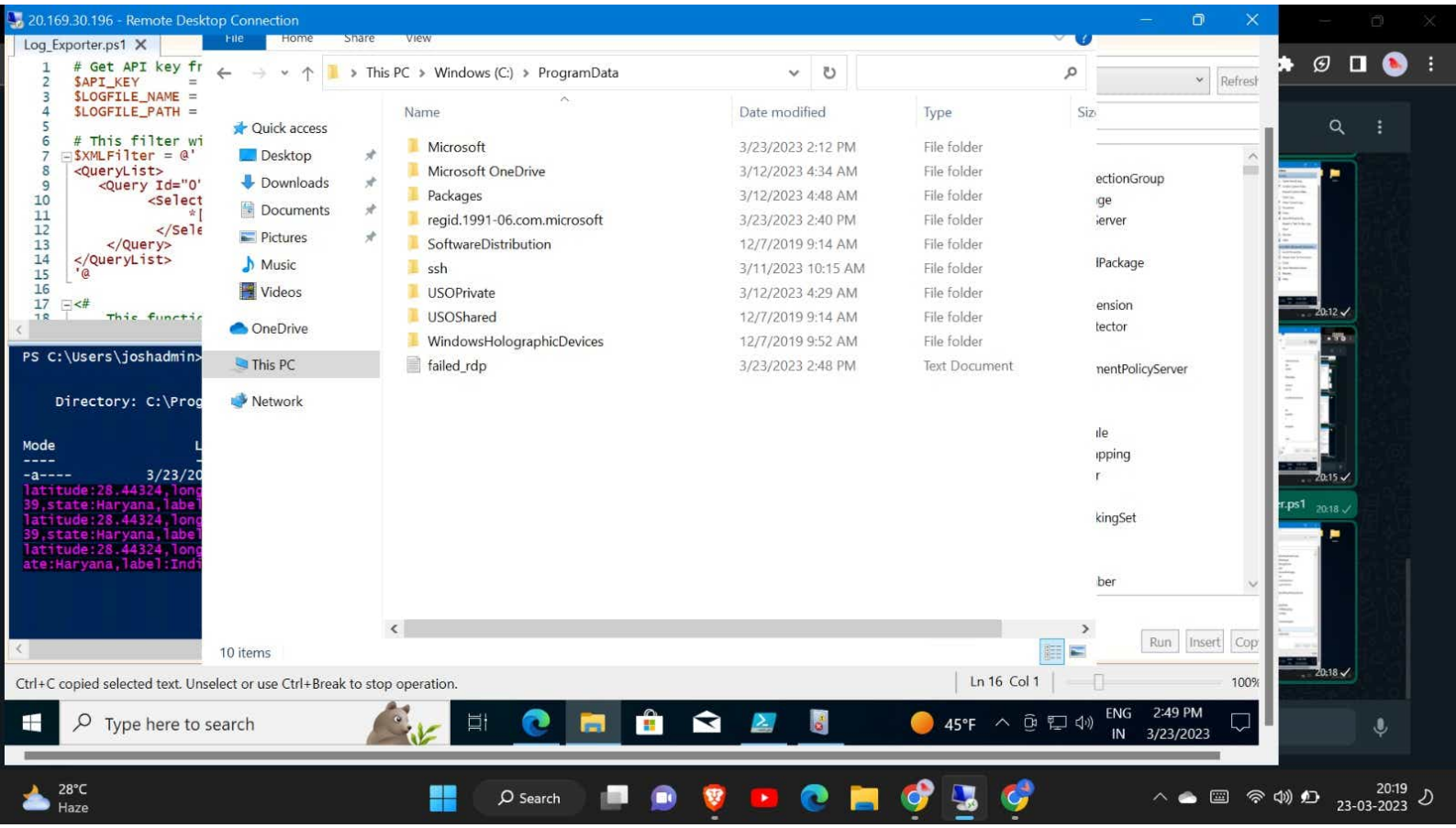

20.169.30.196 - Remote Desktop Connection
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Eve
Applications and S
Subscriptions
Security Number of events: 1,228 (!) New events available
Keywords
Date and Time
Source
Task Ca...
Event ID
Event Properties - Event 4625, Microsoft Windows security auditing.
General
Details
An account failed to log on.
Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0
Log Name: Security
Source: Microsoft Windows security
Logged: 3/23/2023 2:16:01 PM
Event ID: 4625
Task Category: Logon
Level: Information
Keywords: Audit Failure
User: N/A
Computer: honeypot-vm
OpCode: Info
More Information: Event Log Online Help
Copy
Close
3/23/2023 2:16:01 PM
OpCode: Info
More Information: Event Log Online Help
Actions
Security
Event 4625, Microsoft Windows...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help
Feedback
Type here to search
47°F
ENG
IN
2:19 PM
3/23/2023
28°C
Smoke
Search
19:49
23-03-2023

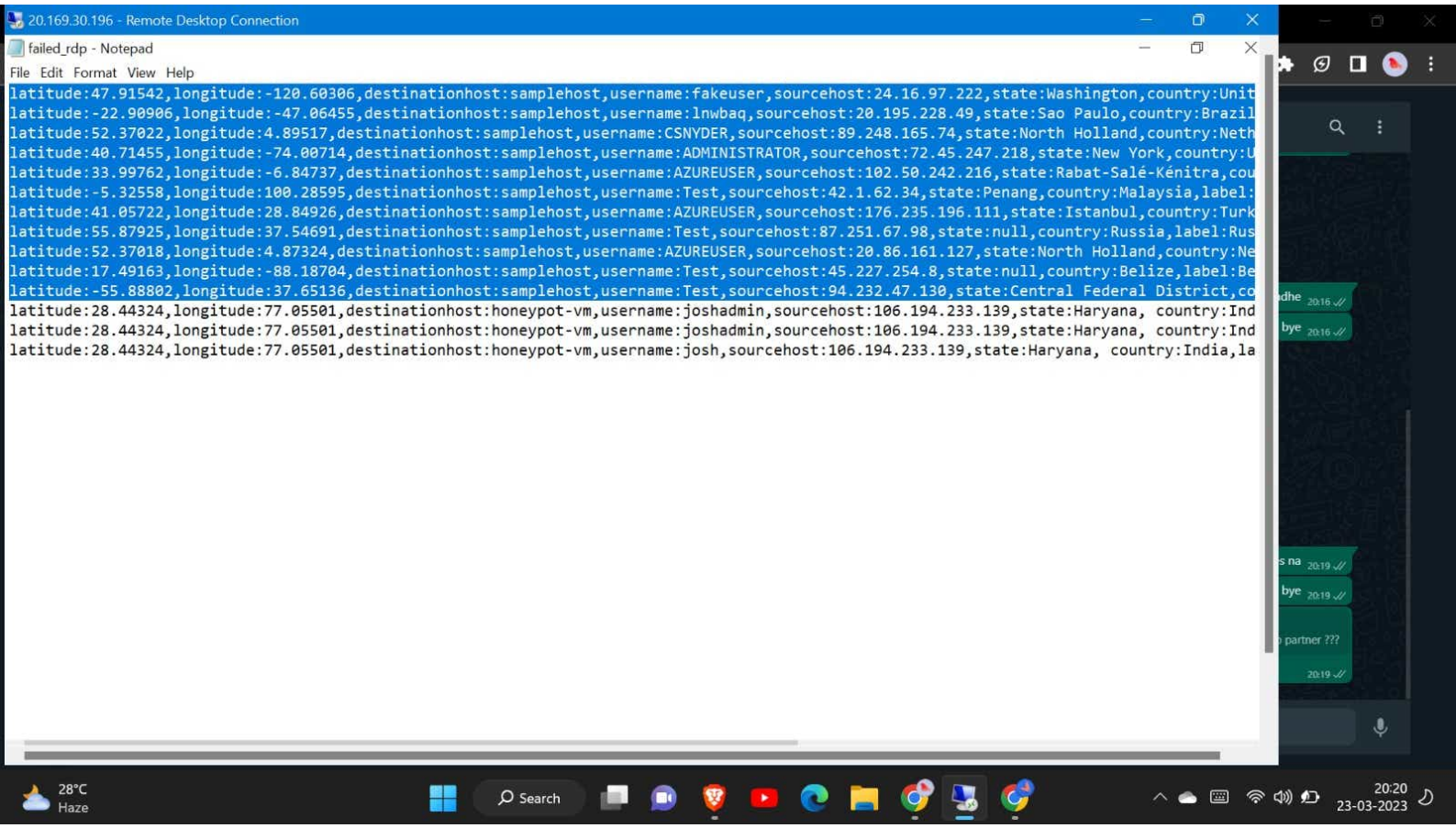

20.169.30.196 - Remote Desktop Connection
Command Prompt - ping 20.169.30.196 -t
Microsoft Windows [Version 10.0.22000.1696]
(c) Microsoft Corporation. All rights reserved.
C:\Users\TANVI>ping 20.169.30.196 -t
Pinging 20.169.30.196 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help
JSON View
More Information: Event Log Online Help
Type here to search
47°F
ENG IN
2:23 PM 3/23/2023
28°C Smoke
Search
ENG IN
19:53 23-03-2023

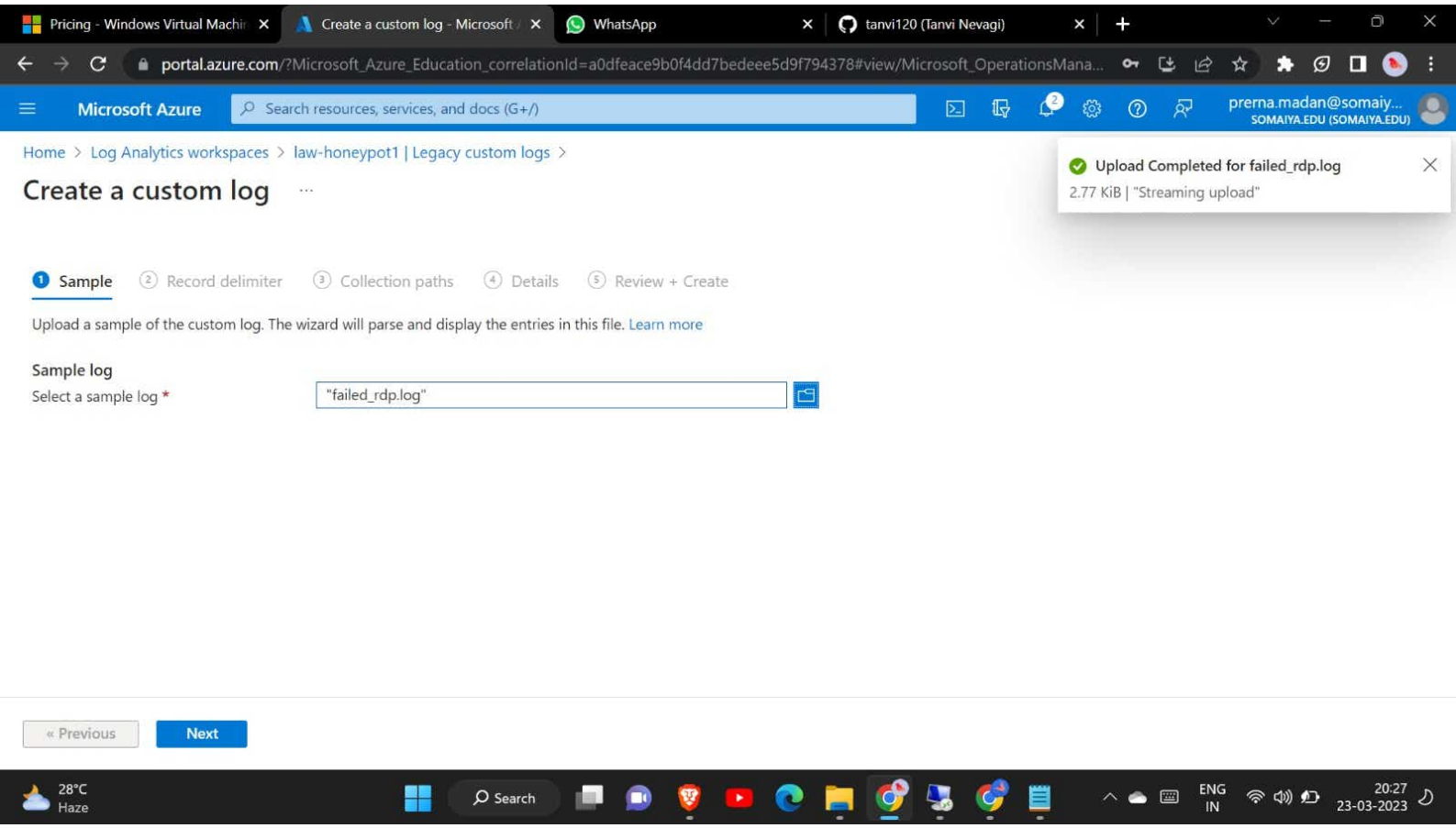

20.169.30.196 - Remote Desktop Connection
Windows Defender Firewall with
Inbound Rules
Outbound Rules
Connection Security Rules
Monitoring
Windows Defender Firewall with Advanced Security on Local Computer
Windows Defender Firewall with Advanced Security on Local Com...
Domain Profile
Private Profile
Public Profile
IPsec Settings
Specify behavior for when a computer is connected to a private network location.
State
Firewall state:
Off
Inbound connections:
Block (default)
Outbound connections:
Allow (default)
Protected network connections:
Customize...
Settings
Specify settings that control Windows Defender Firewall behavior.
Customize...
Logging
Specify logging settings for troubleshooting.
Customize...
OK
Cancel
Apply
Overview
Domain Profile
Private Profile
Public Profile
Getting Started
Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).
Actions
Windows Defender Firewall wit...
Import Policy...
Export Policy...
Restore Default Policy
Diagnose / Repair
View
Refresh
Properties
Help
Type here to search
47°F
ENG
IN
2:25 PM
3/23/2023
28°C
Smoke
Search
19:55
23-03-2023

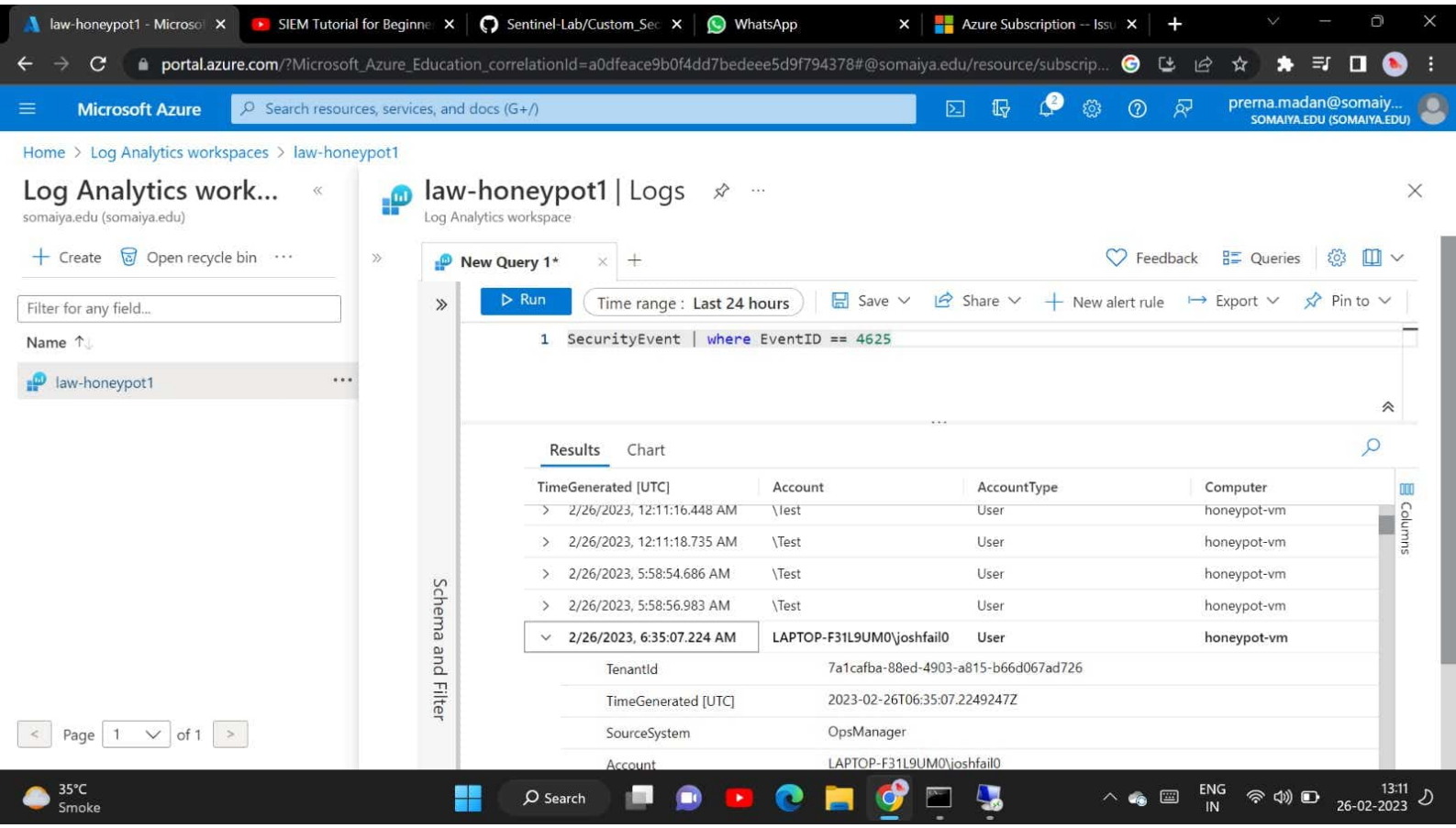

20.169.30.196 - Remote Desktop Connection
Event Viewer (Local)
Custom Views
Windows Logs
Application
Security
Setup
System
Forwarded Events
Applications and Services Log
Subscriptions
Security Number of events: 1,449 (!) New events available
Keywords Date and Time Source Task Ca... Event ID
Audit Success 3/23/2023 2:40:49 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:21 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:21 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:21 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:20 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:19 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:19 PM Microsoft Windows se... Special ... 4672
Audit Success 3/23/2023 2:40:19 PM Microsoft Windows se... Logon 4624
Audit Success 3/23/2023 2:40:19 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:19 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:18 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:18 PM Microsoft Windows se... Process... 4688
Audit Success 3/23/2023 2:40:18 PM Microsoft Windows se... Process... 4688
Event 4624, Microsoft Windows security auditing.
General Details
An account was successfully logged on.
Subject:
Log Name: Security
Source: Microsoft Windows security Logged: 3/23/2023 2:40:19 PM
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: honeypot-vm
Actions
Security
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 4624, Microsoft Windows...
Event Properties
Attach Task To This Event...
Copy
Save Selected Events...
Refresh
Help
Tasks
Type here to search
45°F
ENG IN
2:42 PM 3/23/2023
28°C Haze
Search
20:12 23-03-2023

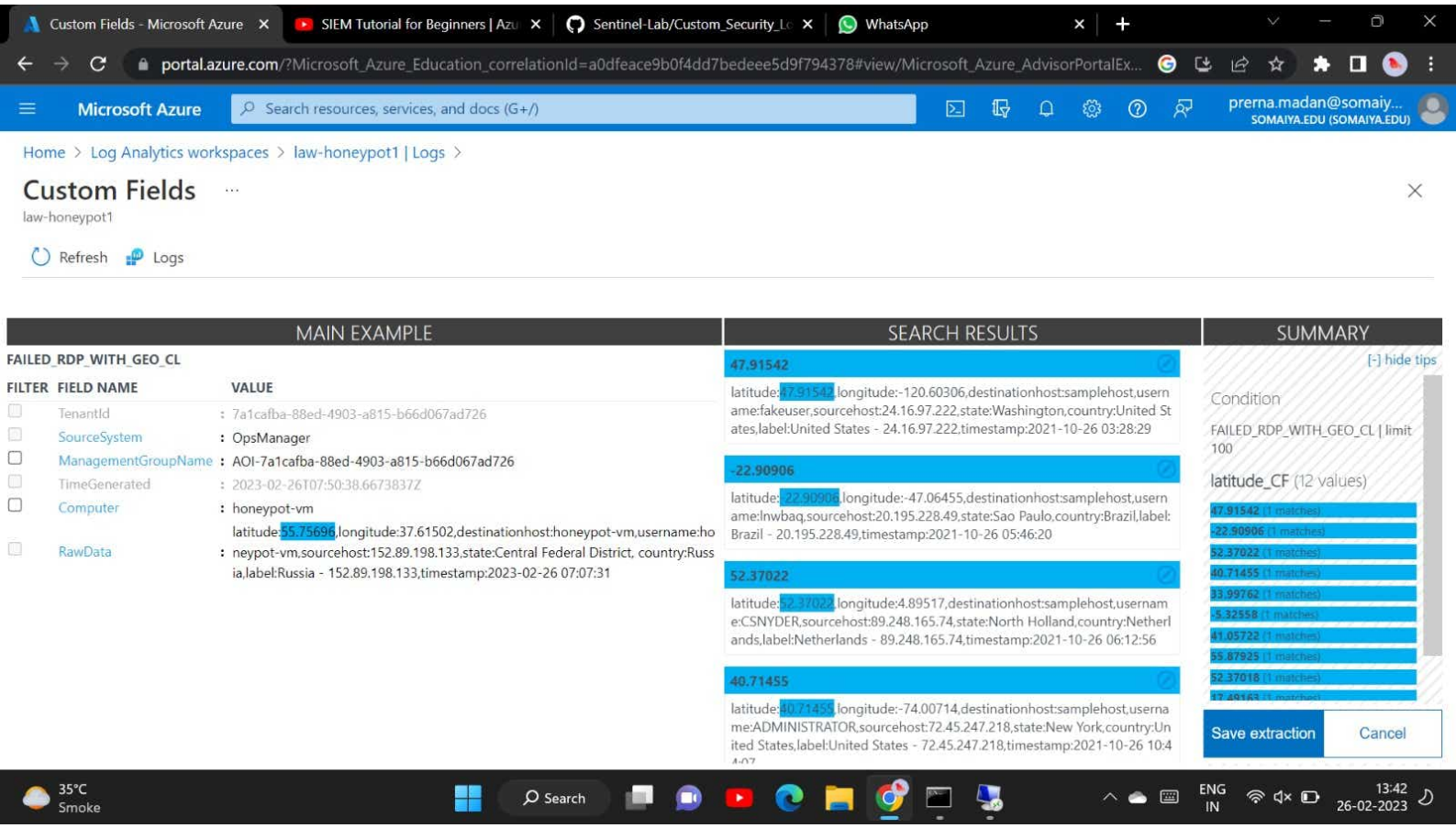

20.169.30.196 - Remote Desktop Connection
Log_Exporter.ps1
Get API key from here: https://ipgeolocation.io/
$API_KEY = "94c0c995d18c4351a8fa30f849d01133"
$LOGFILE_NAME = "failed_rdp.log"
$LOGFILE_PATH = "C:\ProgramData\$($LOGFILE_NAME)"
This filter will be used to filter failed RDP events from Windows Event Viewer
$XMLFilter = @'
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">
*[System[(EventID='4625')]]
</Select>
</Query>
</QueryList>
'@
<#
This function creates a bunch of sample log files that will be used to train the
PS C:\Users\joshadmin> C:\\Users\joshadmin\Desktop\Log_Exporter.ps1
Directory: C:\ProgramData
Mode LastWriteTime Length Name
-a---- 3/23/2023 2:48 PM 0 failed_rdp.log
latitude:28.44324,longitude:77.05501,destinationhost:honeypot-vm,username:joshadmin,sourcehost:106.194.233.139,state:Haryana,label:India - 106.194.233.139,timestamp:2023-03-23 14:16:18
latitude:28.44324,longitude:77.05501,destinationhost:honeypot-vm,username:joshadmin,sourcehost:106.194.233.139,state:Haryana,label:India - 106.194.233.139,timestamp:2023-03-23 14:16:14
latitude:28.44324,longitude:77.05501,destinationhost:honeypot-vm,username:josh,sourcehost:106.194.233.139,state:Haryana,label:India - 106.194.233.139,timestamp:2023-03-23 14:16:01
Commands
Modules: All
Refresh
Name:
A:
Add-AppvClientConnectionGroup
Add-AppvClientPackage
Add-AppvPublishingServer
Add-AppxPackage
Add-AppxProvisionedPackage
Add-AppxVolume
Add-BCDataCacheExtension
Add-BitLockerKeyProtector
Add-BitsFile
Add-CertificateEnrollmentPolicyServer
Add-Computer
Add-Content
Add-DnsClientNrptRule
Add-DtcClusterTMMapping
Add-EtwTraceProvider
Add-History
Add-InitiatorIdToMaskingSet
Add-JobTrigger
Add-KdsRootKey
Add-LocalGroupMember
Run
Insert
Cop
Ctrl+C copied selected text. Unselect or use Ctrl+Break to stop operation.
Ln 1 Col 24
100%
Type here to search
DOW
ENG
IN
2:48 PM
3/23/2023
Tasks
28°C
Haze
Search
20:18
23-03-2023


20.169.30.196 - Remote Desktop Connection
Log_Exporter.ps1
Get API key fr
$API_KEY =
$LOGFILE_NAME =
$LOGFILE_PATH =
This filter wi
$XMLFilter = @'
<QueryList>
<Query Id="0"
<Select
</Sele
</Query>
</QueryList>
'@
<#
PS C:\Users\joshadmin>
Directory: C:\Prog
Mode
-a----
3/23/20
latitude:28.44324,long
39,state:Haryana,label
latitude:28.44324,long
39,state:Haryana,label
latitude:28.44324,long
ate:Haryana,label:Indi
This PC > Windows (C:) > ProgramData
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
Network
Name
Date modified
Type
Microsoft 3/23/2023 2:12 PM File folder
Microsoft OneDrive 3/12/2023 4:34 AM File folder
Packages 3/12/2023 4:48 AM File folder
regid.1991-06.com.microsoft 3/23/2023 2:40 PM File folder
SoftwareDistribution 12/7/2019 9:14 AM File folder
ssh 3/11/2023 10:15 AM File folder
USOPrivate 3/12/2023 4:29 AM File folder
USOShared 12/7/2019 9:14 AM File folder
WindowsHolographicDevices 12/7/2019 9:52 AM File folder
failed_rdp 3/23/2023 2:48 PM Text Document
10 items
Ctrl+C copied selected text. Unselect or use Ctrl+Break to stop operation.
Ln 16 Col 1
100%
Run
Insert
Type here to search
45°F
ENG
IN
2:49 PM
3/23/2023
28°C
Haze
Search
20:19
23-03-2023


20.169.30.196 - Remote Desktop Connection
failed_rdp - Notepad
File Edit Format View Help
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:Unit
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Neth
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:U
latitude:33.99762,longitude:-6.84737,destinationhost:samplehost,username:AZUREUSER,sourcehost:102.50.242.216,state:Rabat-Salé-Kénitra,cou
latitude:-5.32558,longitude:100.28595,destinationhost:samplehost,username:Test,sourcehost:42.1.62.34,state:Penang,country:Malaysia,label:
latitude:41.05722,longitude:28.84926,destinationhost:samplehost,username:AZUREUSER,sourcehost:176.235.196.111,state:Istanbul,country:Turk
latitude:55.87925,longitude:37.54691,destinationhost:samplehost,username:Test,sourcehost:87.251.67.98,state:null,country:Russia,label:Rus
latitude:52.37018,longitude:4.87324,destinationhost:samplehost,username:AZUREUSER,sourcehost:20.86.161.127,state:North Holland,country:Ne
latitude:17.49163,longitude:-88.18704,destinationhost:samplehost,username:Test,sourcehost:45.227.254.8,state:null,country:Belize,label:Be
latitude:-55.88802,longitude:37.65136,destinationhost:samplehost,username:Test,sourcehost:94.232.47.130,state:Central Federal District,co
latitude:28.44324,longitude:77.05501,destinationhost:honeypot-vm,username:joshadmin,sourcehost:106.194.233.139,state:Haryana, country:Ind
latitude:28.44324,longitude:77.05501,destinationhost:honeypot-vm,username:joshadmin,sourcehost:106.194.233.139,state:Haryana, country:Ind
latitude:28.44324,longitude:77.05501,destinationhost:honeypot-vm,username:josh,sourcehost:106.194.233.139,state:Haryana, country:India,la
bye 20:16
bye 20:19
partner ???
20:19
28°C
Haze
Search
20:20
23-03-2023


Pricing - Windows Virtual Machir
Create a custom log - Microsoft
WhatsApp
tanvi120 (Tanvi Nevagi)
portal.azure.com/?Microsoft_Azure_Education_correlationId=a0dfeace9b0f4dd7bedeee5d9f794378#view/Microsoft_OperationsMana...
Microsoft Azure
Search resources, services, and docs (G+/)
prerna.madan@somaiy...
SOMAIYA.EDU (SOMAIYA.EDU)
Home > Log Analytics workspaces > law-honeypot1 | Legacy custom logs >
Create a custom log
Upload Completed for failed_rdp.log
2.77 KiB | "Streaming upload"
1 Sample
2 Record delimiter
3 Collection paths
4 Details
5 Review + Create
Upload a sample of the custom log. The wizard will parse and display the entries in this file. Learn more
Sample log
Select a sample log *
"failed_rdp.log"
« Previous
Next
28°C
Haze
Search
ENG
IN
20:27
23-03-2023


law-honeypot1 - Microso
SIEM Tutorial for Beginne
Sentinel-Lab/Custom_Sec
WhatsApp
Azure Subscription -- Issu
portal.azure.com/?Microsoft_Azure_Education_correlationId=a0dfeace9b0f4dd7bedeee5d9f794378#@somaiya.edu/resource/subscrip...
Microsoft Azure
Search resources, services, and docs (G+/)
prerna.madan@somaiy...
SOMAIYA.EDU (SOMAIYA.EDU)
Home > Log Analytics workspaces > law-honeypot1
Log Analytics work...
somaiya.edu (somaiya.edu)
Create
Open recycle bin
Filter for any field...
Name
law-honeypot1
Page 1 of 1
law-honeypot1 | Logs
Log Analytics workspace
New Query 1*
Feedback
Queries
Run
Time range : Last 24 hours
Save
Share
New alert rule
Export
Pin to
1 SecurityEvent | where EventID == 4625
Results
Chart
TimeGenerated [UTC]
Account
AccountType
Computer
2/26/2023, 12:11:16.448 AM \Test User honeypot-vm
2/26/2023, 12:11:18.735 AM \Test User honeypot-vm
2/26/2023, 5:58:54.686 AM \Test User honeypot-vm
2/26/2023, 5:58:56.983 AM \Test User honeypot-vm
2/26/2023, 6:35:07.224 AM LAPTOP-F31L9UM0\joshfail0 User honeypot-vm
TenantId 7a1cafba-88ed-4903-a815-b66d067ad726
TimeGenerated [UTC] 2023-02-26T06:35:07.2249247Z
SourceSystem OpsManager
Account LAPTOP-F31L9UM0\joshfail0
Schema and Filter
Columns
35°C
Smoke
Search
ENG
IN
13:11
26-02-2023


Custom Fields - Microsoft Azure
SIEM Tutorial for Beginners | Azu
Sentinel-Lab/Custom_Security_Lo
WhatsApp
portal.azure.com/?Microsoft_Azure_Education_correlationId=a0dfeace9b0f4dd7bedeee5d9f794378#view/Microsoft_Azure_AdvisorPortalEx...
Microsoft Azure
Search resources, services, and docs (G+/)
prerna.madan@somaiy...
SOMAIYA.EDU (SOMAIYA.EDU)
Home > Log Analytics workspaces > law-honeypot1 | Logs >
Custom Fields
law-honeypot1
Refresh
Logs
MAIN EXAMPLE
FAILED_RDP_WITH_GEO_CL
FILTER FIELD NAME VALUE
TenantId : 7a1cafba-88ed-4903-a815-b66d067ad726
SourceSystem : OpsManager
ManagementGroupName : AOI-7a1cafba-88ed-4903-a815-b66d067ad726
TimeGenerated : 2023-02-26T07:50:38.6673837Z
Computer : honeypot-vm
RawData : latitude:55.75696,longitude:37.61502,destinationhost:honeypot-vm,username:honeypot-vm,sourcehost:152.89.198.133,state:Central Federal District, country:Russia,label:Russia - 152.89.198.133,timestamp:2023-02-26 07:07:31
SEARCH RESULTS
47.91542
latitude:47.91542,longitude:-120.60306,destinationhost:samplehost,username:fakeuser,sourcehost:24.16.97.222,state:Washington,country:United States,label:United States - 24.16.97.222,timestamp:2021-10-26 03:28:29
-22.90906
latitude:-22.90906,longitude:-47.06455,destinationhost:samplehost,username:lnwbaq,sourcehost:20.195.228.49,state:Sao Paulo,country:Brazil,label:Brazil - 20.195.228.49,timestamp:2021-10-26 05:46:20
52.37022
latitude:52.37022,longitude:4.89517,destinationhost:samplehost,username:CSNYDER,sourcehost:89.248.165.74,state:North Holland,country:Netherlands,label:Netherlands - 89.248.165.74,timestamp:2021-10-26 06:12:56
40.71455
latitude:40.71455,longitude:-74.00714,destinationhost:samplehost,username:ADMINISTRATOR,sourcehost:72.45.247.218,state:New York,country:United States,label:United States - 72.45.247.218,timestamp:2021-10-26 10:4
SUMMARY
[-] hide tips
Condition
FAILED_RDP_WITH_GEO_CL | limit 100
latitude_CF (12 values)
47.91542 (1 matches)
-22.90906 (1 matches)
52.37022 (1 matches)
40.71455 (1 matches)
33.99762 (1 matches)
-5.32558 (1 matches)
41.05722 (1 matches)
55.87925 (1 matches)
52.37018 (1 matches)
Save extraction
Cancel
35°C
Smoke
Search
ENG
IN
13:42
26-02-2023

Logs - Microsoft Azure | IPGeolocation API - Dashboard | WhatsApp | New workbook - Microsoft Azure

portal.azure.com/?Microsoft_Azure_Education_correlationId=a0dfeace9b0f4dd7bedeee5d9f794378#view/AppInsightsExtension/UsageNoteboo...

Microsoft Azure | Search resources, services, and docs (G+/) | prerna.madan@somaiy... SOMAIYA.EDU (SOMAIYA.EDU)

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

New workbook

law-honeypot1

Edit | Open | Help | Auto refresh: Off

India - 106.193.164.102

19.4

27°C Haze | Search | ENG IN | 22:40 23-03-2023

FAILED_RDP_LOG - Microsoft Azu

portal.azure.com/?Microsoft_Azure_Education_correlationId=a3a12c93-38da-4f17-8373-58c7cb2b3a49#view/AppInsightsExtension/UsageNote...

Microsoft Azure | Search resources, services, and docs (G+/) | prerna.madan@somaiy... SOMAIYA.EDU (SOMAIYA.EDU)

Home > Microsoft Sentinel > Microsoft Sentinel | Workbooks >

FAILED_RDP_LOG

law-honeypot1

Edit | Open | Help | Auto refresh: Off

1/2

Seychelles - 5.181.86.122	Islands - 185.190.24.15	Netherlands - 185.170.144.3	Palestine - 213.6.148.83	India - 106.193.164.102	States - 20.97.165.84	States - 20.25.7.132	States - 20.9.74.54
10.8 K	1.53 K	180	94	3	2	2	2

Search | ENG IN | 08:58 24-03-2023