EVENTS ARE IMPORTANT – CHALLENGE

SCENARIO

You were hired by the CEO of Alex's HighT to investigate unusual activity on the network.
All you receive to work with is a log file.

OBJECTIVES

- Find the user account that logged in.
- Find the login date.
- Find the IP of the account used to log in.

PROGRAM USED

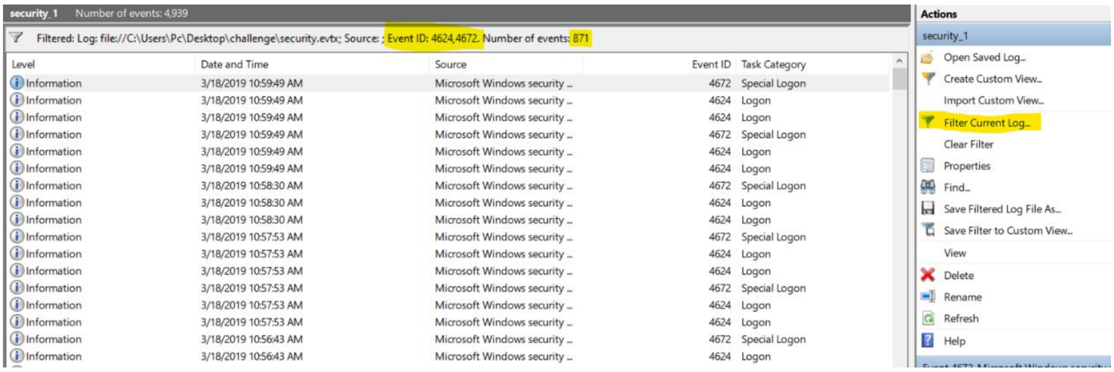
Windows Event Viewer.

Splunk.

First of all I entered the event viewer and attached the given file in. “security.evtx”

To detect any suspicious activity first of all we need to start looking for logged in accounts:

I filtered the log typing EventID “4624,4672” checking all kind of logged in accounts (4624 Logon, 4672 Special Logon). Special logon means logon with privileged account.



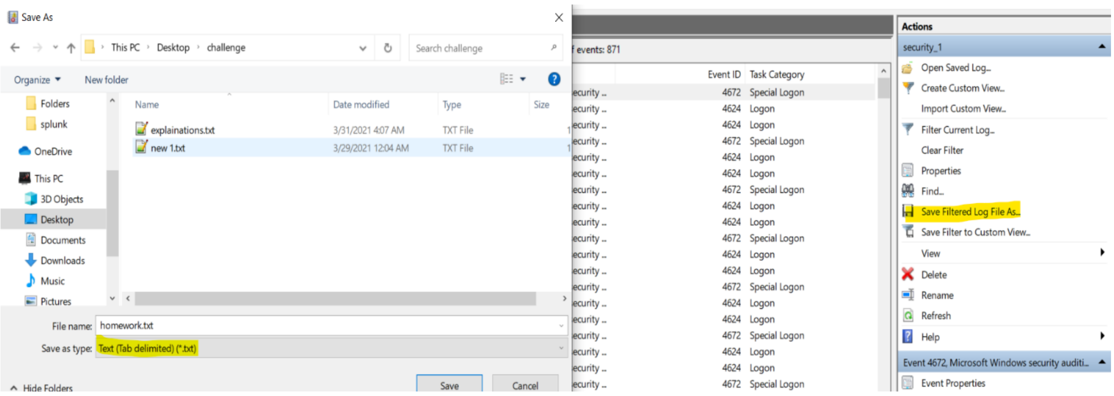
security_1 Number of events: 4,939

Filtered: Log: file://C:\Users\Pc\Desktop\challenge\security.evtx; Source: ; Event ID: 4624,4672. Number of events: 871

Level	Date and Time	Source	Event ID	Task Category
Information	3/18/2019 10:59:49 AM	Microsoft Windows security ...	4672	Special Logon
Information	3/18/2019 10:59:49 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:59:49 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:59:49 AM	Microsoft Windows security ...	4672	Special Logon
Information	3/18/2019 10:59:49 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:59:49 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:58:30 AM	Microsoft Windows security ...	4672	Special Logon
Information	3/18/2019 10:58:30 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:58:30 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:57:53 AM	Microsoft Windows security ...	4672	Special Logon
Information	3/18/2019 10:57:53 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:57:53 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:57:53 AM	Microsoft Windows security ...	4672	Special Logon
Information	3/18/2019 10:57:53 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:57:53 AM	Microsoft Windows security ...	4624	Logon
Information	3/18/2019 10:56:43 AM	Microsoft Windows security ...	4672	Special Logon
Information	3/18/2019 10:56:43 AM	Microsoft Windows security ...	4624	Logon

EVENTS ARE IMPORTANT – CHALLENGE

As you can see in the image we have a lot of events (871), and it would be hard to start digging and searching one by one, so I uploaded the file to Splunk (used 'Save Filtered Log File As' then saved as '.txt file').



Name	Date modified	Type
explainations.txt	3/31/2021 4:07 AM	TXT File
new 1.txt	3/29/2021 12:04 AM	TXT File

File name: homework.txt

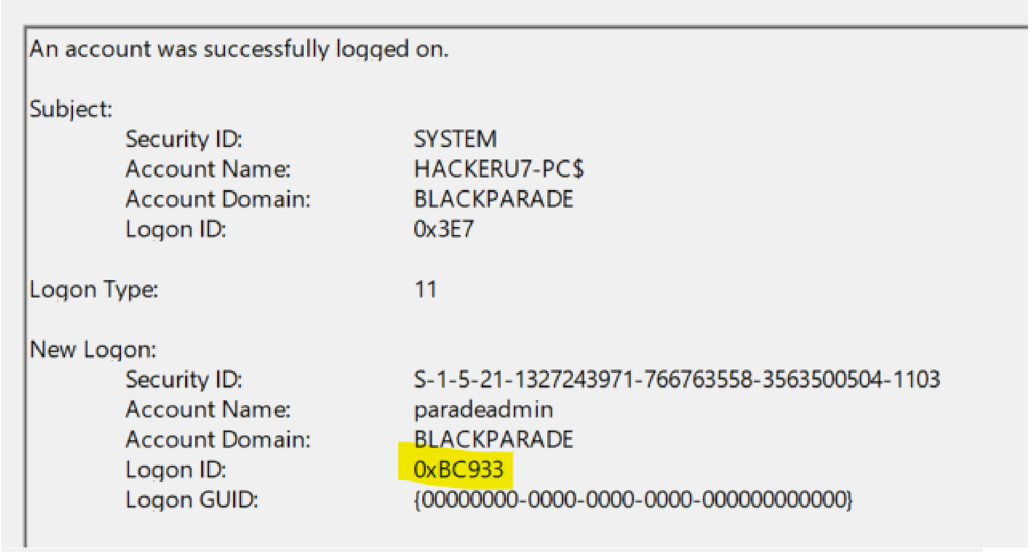
Save as type: Text (Tab delimited) (*.txt)

f events: 871

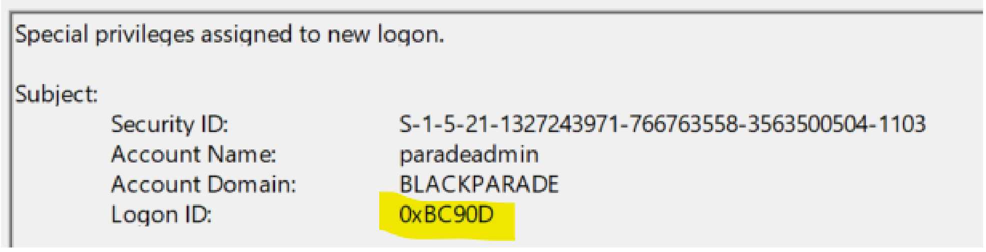
	Event ID	Task Category
ecurity ...	4672	Special Logon
ecurity ...	4624	Logon
ecurity ...	4624	Logon
ecurity ...	4672	Special Logon
ecurity ...	4624	Logon
ecurity ...	4624	Logon
ecurity ...	4672	Special Logon
ecurity ...	4624	Logon
ecurity ...	4624	Logon
ecurity ...	4672	Special Logon
ecurity ...	4624	Logon
ecurity ...	4624	Logon
ecurity ...	4672	Special Logon
ecurity ...	4624	Logon
ecurity ...	4624	Logon
ecurity ...	4672	Special Logon
ecurity ...	4624	Logon
ecurity ...	4624	Logon
ecurity ...	4672	Special Logon

detecting suspicious activity:

1) Usually it would be suspicious to see Logon and Special Logon after with the same LogonID. (LogonID is unique number that defines the logon session).



```
An account was successfully logged on.

Subject:
        Security ID:            SYSTEM
        Account Name:           HACKERU7-PC$
        Account Domain:         BLACKPARADE
        Logon ID:               0x3E7

Logon Type:                     11

New Logon:
        Security ID:            S-1-5-21-1327243971-766763558-3563500504-1103
        Account Name:           paradeadmin
        Account Domain:         BLACKPARADE
        Logon ID:               0xBC933
        Logon GUID:             {00000000-0000-0000-0000-000000000000}
```

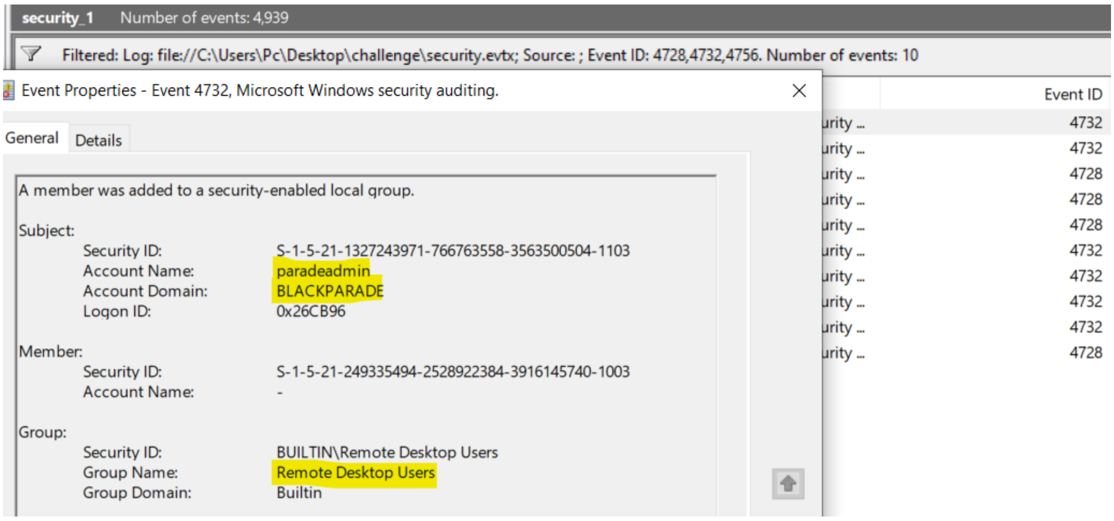


```
Special privileges assigned to new logon.

Subject:
        Security ID:            S-1-5-21-1327243971-766763558-3563500504-1103
        Account Name:           paradeadmin
        Account Domain:         BLACKPARADE
        Logon ID:               0xBC90D
```

EVENTS ARE IMPORTANT – CHALLENGE

2) Based on a search I've done checking what accounts were added to security groups:
   EventID "4728,4728": added to security-enabled local/global group.

We can see that the account BLACKPARADE/paradmin was enabled under "Remote Desktop Users"



security_1 Number of events: 4,939

Filtered: Log: file://C:\Users\Pc\Desktop\challenge\security.evtx; Source: ; Event ID: 4728,4732,4756. Number of events: 10

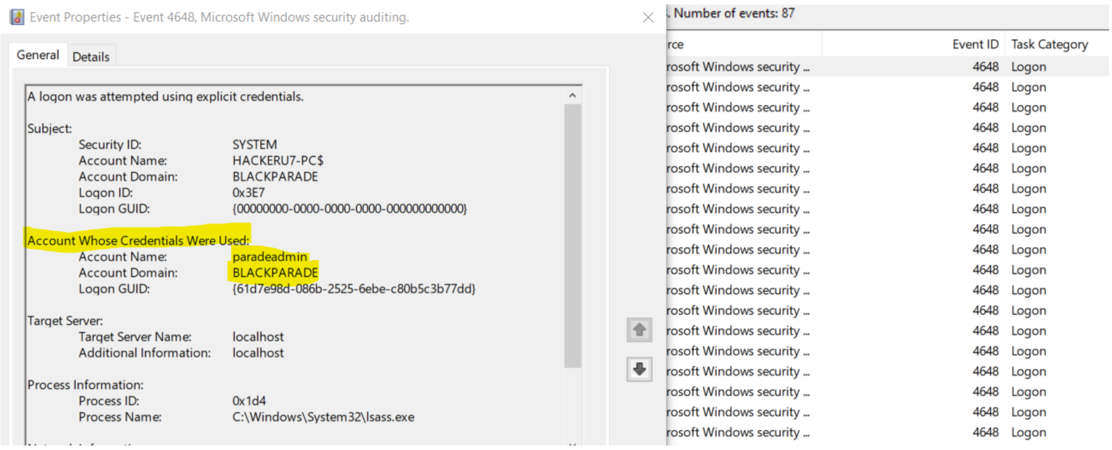
Event Properties - Event 4732, Microsoft Windows security auditing.

```
A member was added to a security-enabled local group.

Subject:
        Security ID:            S-1-5-21-1327243971-766763558-3563500504-1103
        Account Name:           paradeadmin
        Account Domain:         BLACKPARADE
        Logon ID:               0x26CB96

Member:
        Security ID:            S-1-5-21-249335494-2528922384-3916145740-1003
        Account Name:           -

Group:
        Security ID:            BUILTIN\Remote Desktop Users
        Group Name:             Remote Desktop Users
        Group Domain:           Builtin
```

	Event ID
urity ...	4732
urity ...	4732
urity ...	4728
urity ...	4728
urity ...	4728
urity ...	4732
urity ...	4732
urity ...	4732
urity ...	4732
urity ...	4728

3) Checking which account were logged remotely / with another credentials:
   EventID: "4648: logon was attempted using explicit credentials."

We can see that the credentials of BLACKPARADE/paradmin was used the most.



Event Properties - Event 4648, Microsoft Windows security auditing.

```
A logon was attempted using explicit credentials.

Subject:
        Security ID:            SYSTEM
        Account Name:           HACKERU7-PC$
        Account Domain:         BLACKPARADE
        Logon ID:               0x3E7
        Logon GUID:             {00000000-0000-0000-0000-000000000000}

Account Whose Credentials Were Used:
        Account Name:           paradeadmin
        Account Domain:         BLACKPARADE
        Logon GUID:             {61d7e98d-086b-2525-6ebe-c80b5c3b77dd}

Target Server:
        Target Server Name:     localhost
        Additional Information: localhost

Process Information:
        Process ID:             0x1d4
        Process Name:           C:\Windows\System32\lsass.exe
```

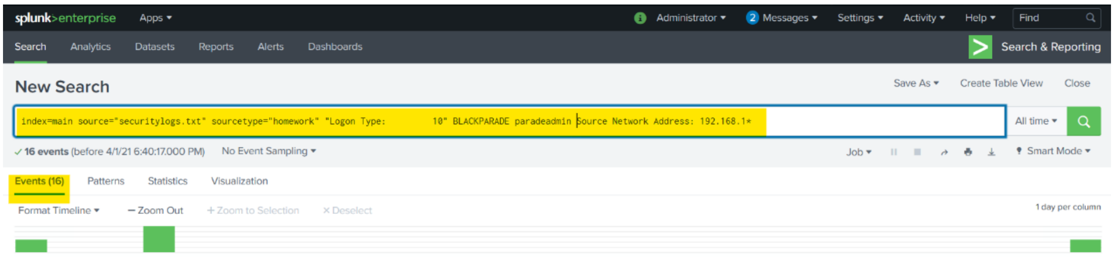
. Number of events: 87

rce	Event ID	Task Category
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon
rosoft Windows security ...	4648	Logon

EVENTS ARE IMPORTANT – CHALLENGE

Now after having the file in Splunk, and the suspicious DOMAIN/ACCOUNT, I start searching for suspicious Logon Type (Logon type indicates the kind of logon that occurred).

Suspicious Logon Type that found in the log was Logon Type 10 (connecting from a remote machine via RDP (using Remote Desktop, Terminal Services or Remote Assistance).

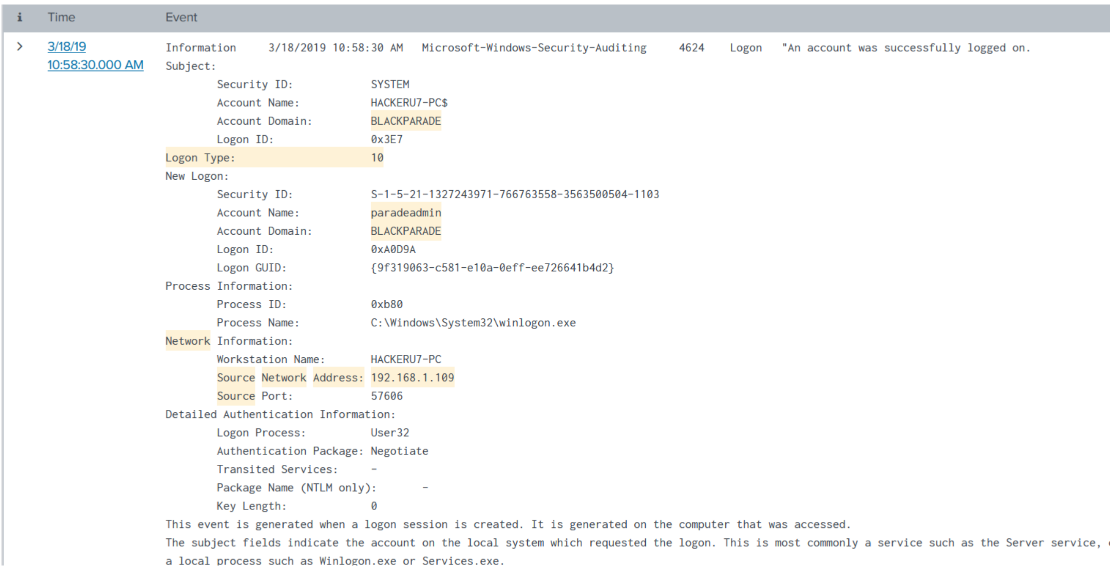


New Search

```
index=main source="securitylogs.txt" sourcetype="homework" "Logon Type:        10" BLACKPARADE paradeadmin Source Network Address: 192.168.1*
```

✓ 16 events (before 4/1/21 6:40:17.000 PM) No Event Sampling

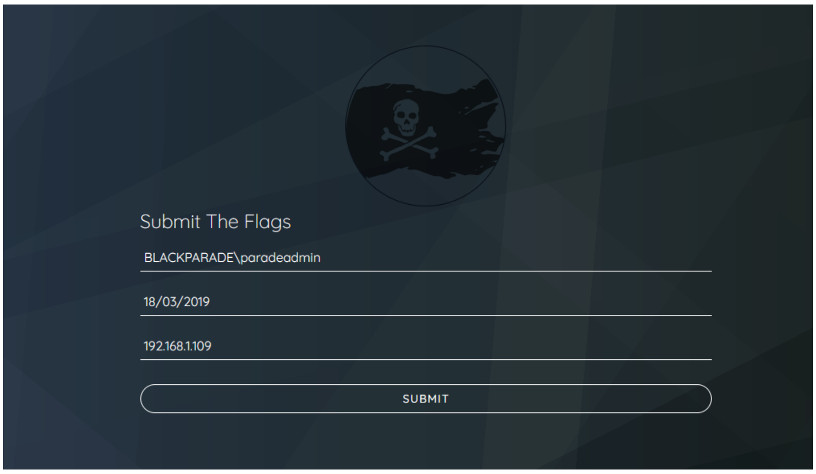
Suspicious account located:



3/18/19 10:58:30.000 AM

```
Information    3/18/2019 10:58:30 AM   Microsoft-Windows-Security-Auditing    4624    Logon    "An account was successfully logged on.
Subject:
        Security ID:            SYSTEM
        Account Name:           HACKERU7-PC$
        Account Domain:         BLACKPARADE
        Logon ID:               0x3E7
Logon Type:                     10
New Logon:
        Security ID:            S-1-5-21-1327243971-766763558-3563500504-1103
        Account Name:           paradeadmin
        Account Domain:         BLACKPARADE
        Logon ID:               0xA0D9A
        Logon GUID:             {9f319063-c581-e10a-0eff-ee726641b4d2}
Process Information:
        Process ID:             0xb80
        Process Name:           C:\Windows\System32\winlogon.exe
Network Information:
        Workstation Name:       HACKERU7-PC
        Source Network Address: 192.168.1.109
        Source Port:            57606
Detailed Authentication Information:
        Logon Process:          User32
        Authentication Package: Negotiate
        Transited Services:     -
        Package Name (NTLM only):       -
        Key Length:             0
This event is generated when a logon session is created. It is generated on the computer that was accessed.
The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service,
a local process such as Winlogon.exe or Services.exe.
```

Challenge completed:



Submit The Flags

BLACKPARADE\paradeadmin

18/03/2019

192.168.1.109