

EVENT LOG

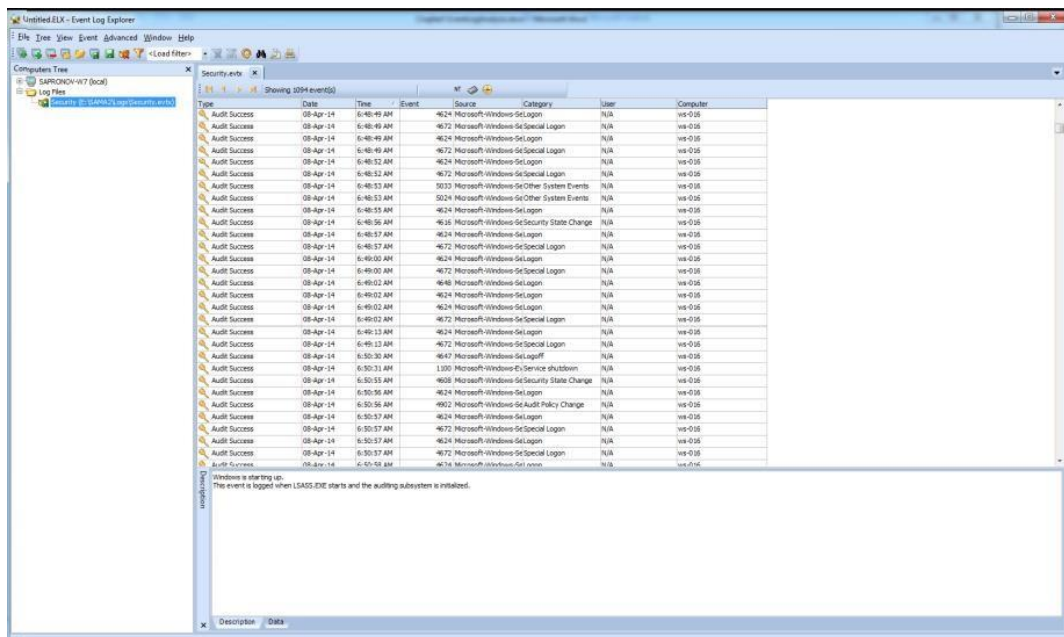
Цел: Да се анализираат логовите на даден корисник

Примена: Осознавање информации за корисникот, преку неговите логови

Потребни алатки: [Event Log Explorer](#)

Чекори:

1. Инсталирајте ја алатката
2. Отворете ја Event Log Explorer алатката
3. Изгледот на прозорецот треба да е како на сликата



4. Може да се зададе ново филтрирање на логовите базирано на user accounts, опис, датум, итн. Прозорецот за филтер е прикажан на сликата подолу.

Filter

Apply filter to:

☒ Active event log view (File: E:\SAMA2\Logs\Security.evtx)

☐ Event log view(s) on your choice

Event types

☒ Information

☒ Warning

☒ Error

☒ Critical

☒ Audit Success

☒ Audit Failure

Source:

☐ Exclude

Category:

☐ Exclude

User:

☐ Exclude

Computer:

☐ Exclude

Event ID(s):

☐ Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450! 10,255)

Text in description:

SYSTEMSERVICE

☐ RegExp

☐ Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elex.exe)

New conditionDelete conditionClear list

Name	Operator	Value

☐ Date☐ Time☐ Separately

From:02-Mar-1512:00:00 AMTo:02-Mar-1512:00:00 AM

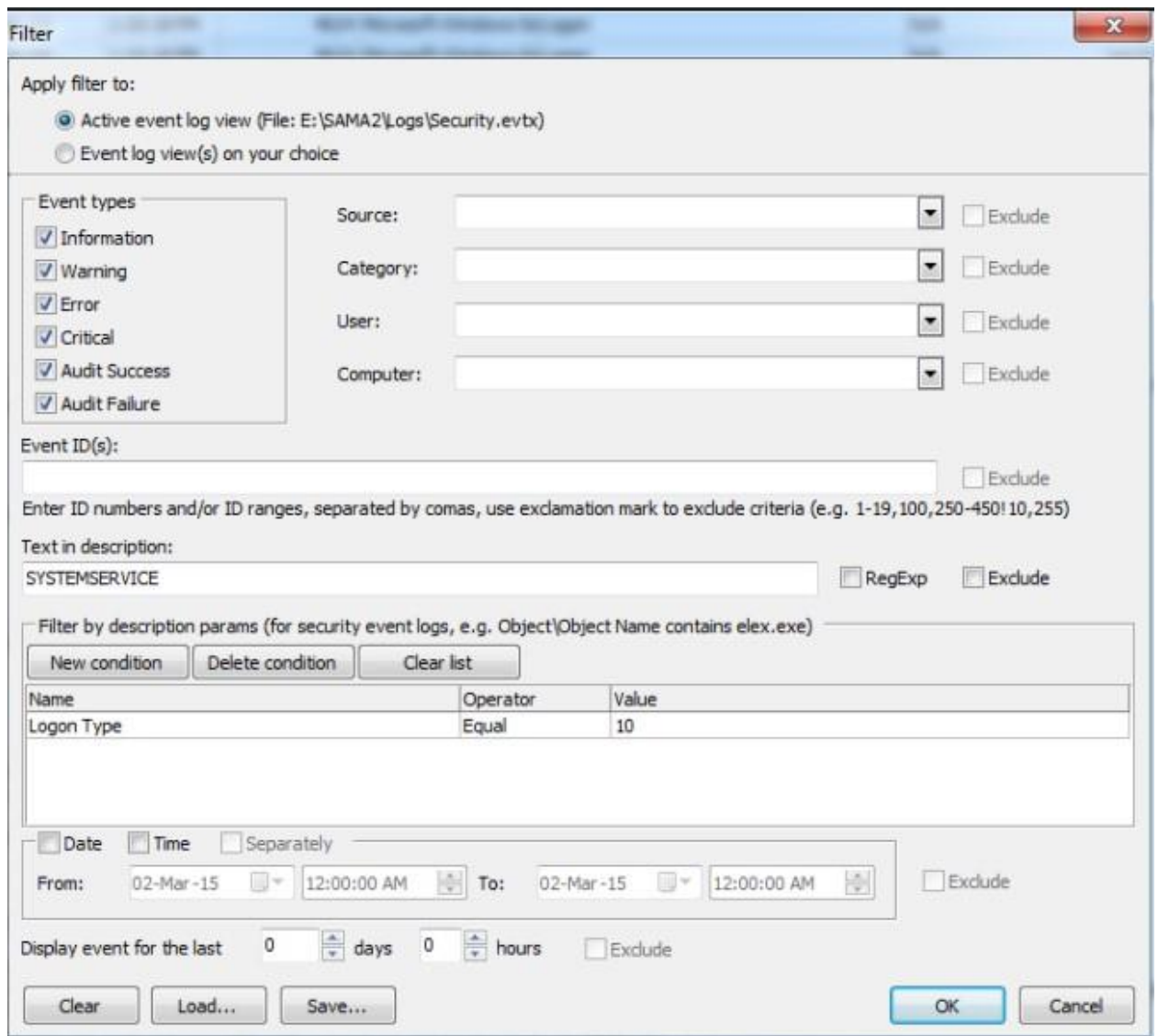
☐ Exclude

Display event for the last0 days0 hours

☐ Exclude

ClearLoad...Save...OKCancel

5. Исто така на самиот филтер може и да зададеме тип на лог, како што е RDP или тип 10.



Filter

Apply filter to:

☒ Active event log view (File: E:\SAMA2\Logs\Security.evbx)

☐ Event log view(s) on your choice

Event types

☒ Information

☒ Warning

☒ Error

☒ Critical

☒ Audit Success

☒ Audit Failure

Source: ☐ Exclude

Category: ☐ Exclude

User: ☐ Exclude

Computer: ☐ Exclude

Event ID(s): ☐ Exclude

Enter ID numbers and/or ID ranges, separated by comas, use exclamation mark to exclude criteria (e.g. 1-19,100,250-450!10,255)

Text in description: ☐ RegExp ☐ Exclude

Filter by description params (for security event logs, e.g. Object\Object Name contains elcx.exe)

New condition Delete condition Clear list

Name	Operator	Value
Logon Type	Equal	10

☐ Date ☐ Time ☐ Separately

From: To: ☐ Exclude

Display event for the last days hours ☐ Exclude

Clear Load... Save... OK Cancel