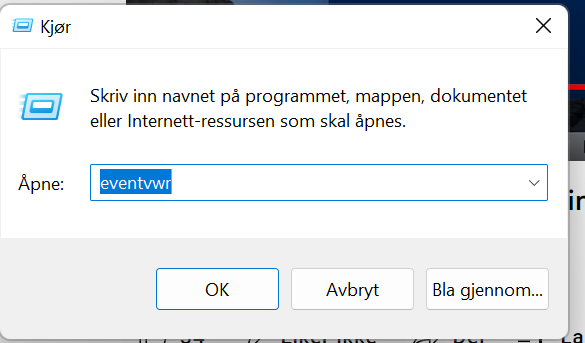
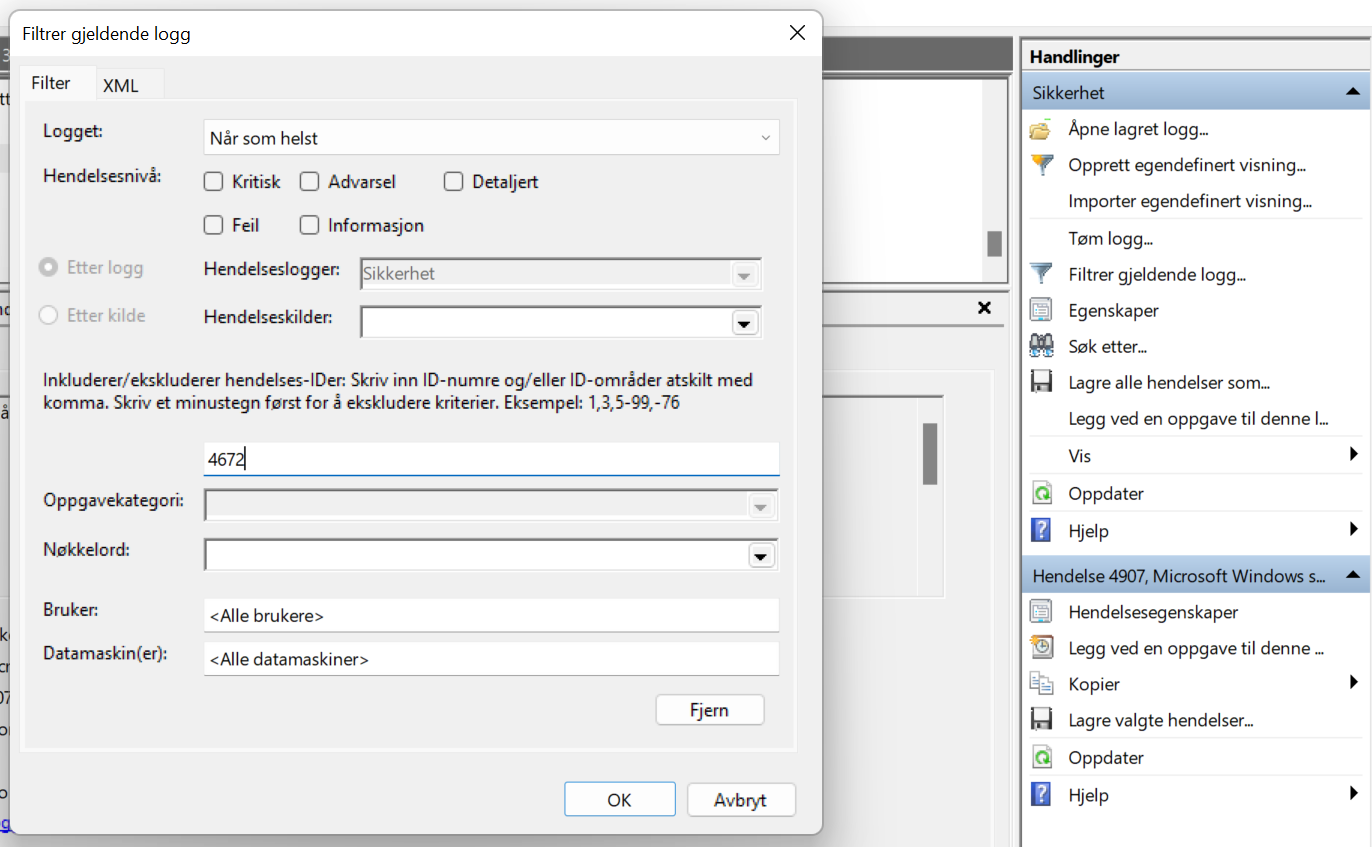
Lab 4 Cyberforsvar:

**Oppgave 1:**

**- Start Windows Event Viewer (har du Windows som VM, bruk gjerne den)**

**Åpner kjør skriver inn eventvwr**

****

****

**- Bruk søke funksjonen i Event Viewer for å lete etter kodene:**

**• 4672**

Denne eventen eller hendelsen gir beskjed når en konto er tildelt noen brukerrettigheter ved pålogging

**• 4608/4609**

4608: Denne hendelsen logges inn når Lsass.eze programmet starter og overvåkingsdelsystemet initialiseres.

**• 4720**

Fant ikke event info med denne id-en på windows event logger

**• 4800/4801**

**Fant ikke denne heller søkte på nettet:**

Denne eventen brukes når en bruker låser arbeidsstasjonen manuelt eller automatisk, låser konsollen etter en inaktiv periode logges denne hendelsen

Med id 4801 kan man sjekke når brukeren kom tilbake og låste opp arbeidsstasjonen

**• 4956 ikke funnet:**

Denne hendelsen logges når windows-brannmuren endrer domene og offentlige profiler og kan oppdages hver gang brannmuren startes opp i offentlig etter initialisering og bytter domene hvis det er aktuelt.

**• Hva betyr disse kodene? Fant du noen av de?**

**Oppgave 2:**

**• Trykk på “Emtpy log”. Hvilken kode generer dette?**

**Oppgave 3:**

**- Start powershell som Administrator**

**Prøv å svare på disse oppgavene ved å utføre de i powershell;**

**- Hva heter powershell kommandoen for å skrive ut security event loggen?**

Powershell komandoen for å skrive ut security event loggen heter (Get-eventLog security)

**- Hva er syntaxen for å sepsifisere hvilken fil du vil se på fra kommandolinje?**

Du bruker Get-Content

Et bilde som inneholder tekst

Automatisk generert beskrivelse

**- Hva er parameteret til kommandolinjen for å liste ut kun ID 1102? (Kommer an på hvor den er lokalisert**

**Parameter: InstanceId**

Get-EventLog -LogName Security -InstanceId 1102 -Source EventLog

**- Hva er syntaxen for å hente evnter fra andre maskiner? (bruk localhost for denne , tester på min egen pc)**

**Get-EventLog -LogName System -ComputerName localhost**

**Et bilde som inneholder tekst, svart, plakett, skjermbilde

Automatisk generert beskrivelse**

**- Hint: Denne linken er bra hjelp: https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-eventlog?view=powershell-5.1**