HORIZON
SECURED

Windows Advanced Auditing

Protecting cached Credentials

Procedure:

1. Configure an Advanced Auditing Policy Configuration
2. Configure a SACL on LSASS.EXE
3. Test the configuration with Mimikatz
4. Confirm Event ID 4663 in the Event Viewer Security log

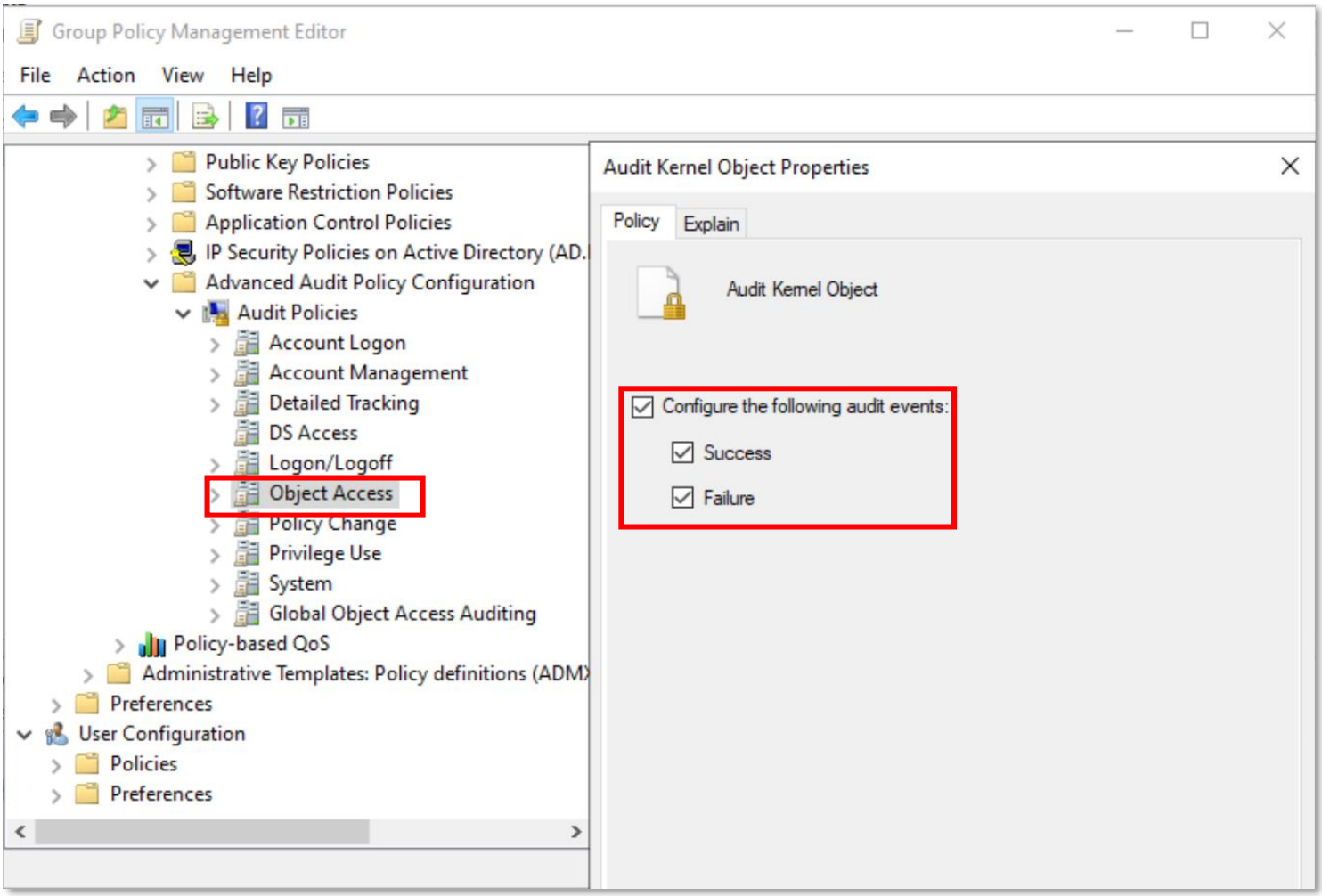
For more details

If you like this content, please make sure to follow our LinkedIn page, as we publish resources like this frequently.

https://www.linkedin.com/company/horizon-secured/

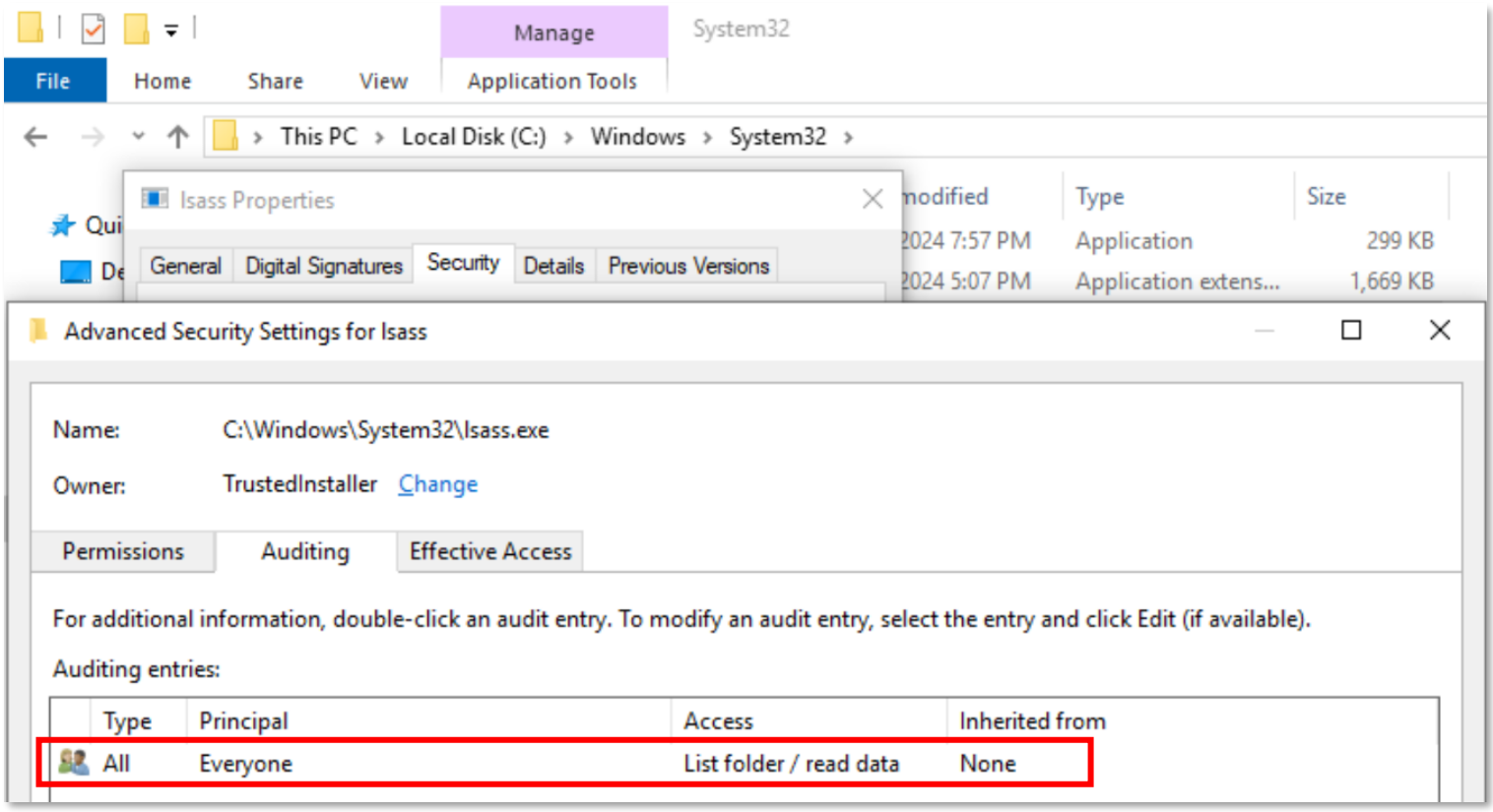
1. First you must configure Advanced Auditing Policy Configuration in Group Policy. You want to enable following:

- **Object Access > Audit Kernel Object**



2. You also must configure the auditing on the binary level. You can find it here: C:\Windows\System32**lsass.exe**. On this binary go to **Properties > Security > Advanced > Auditing.** Here you must add following:

   - **All > Everyone > List folder / read data**

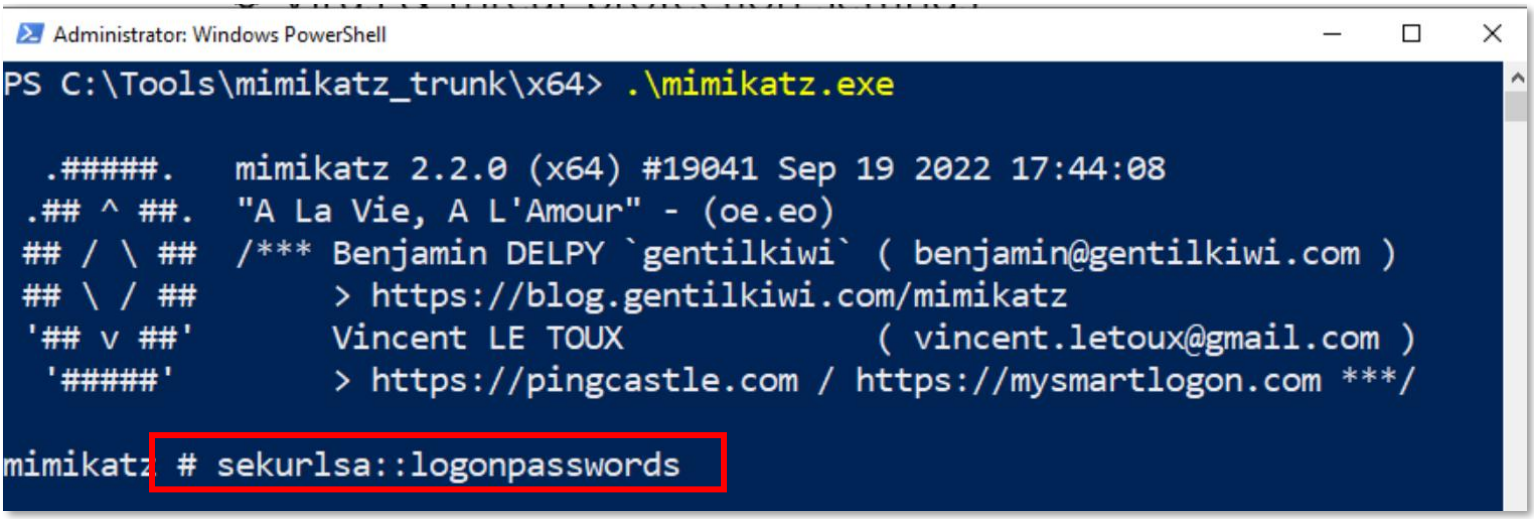


If you like this content, please make sure to follow our LinkedIn page, as we publish resources like this frequently.

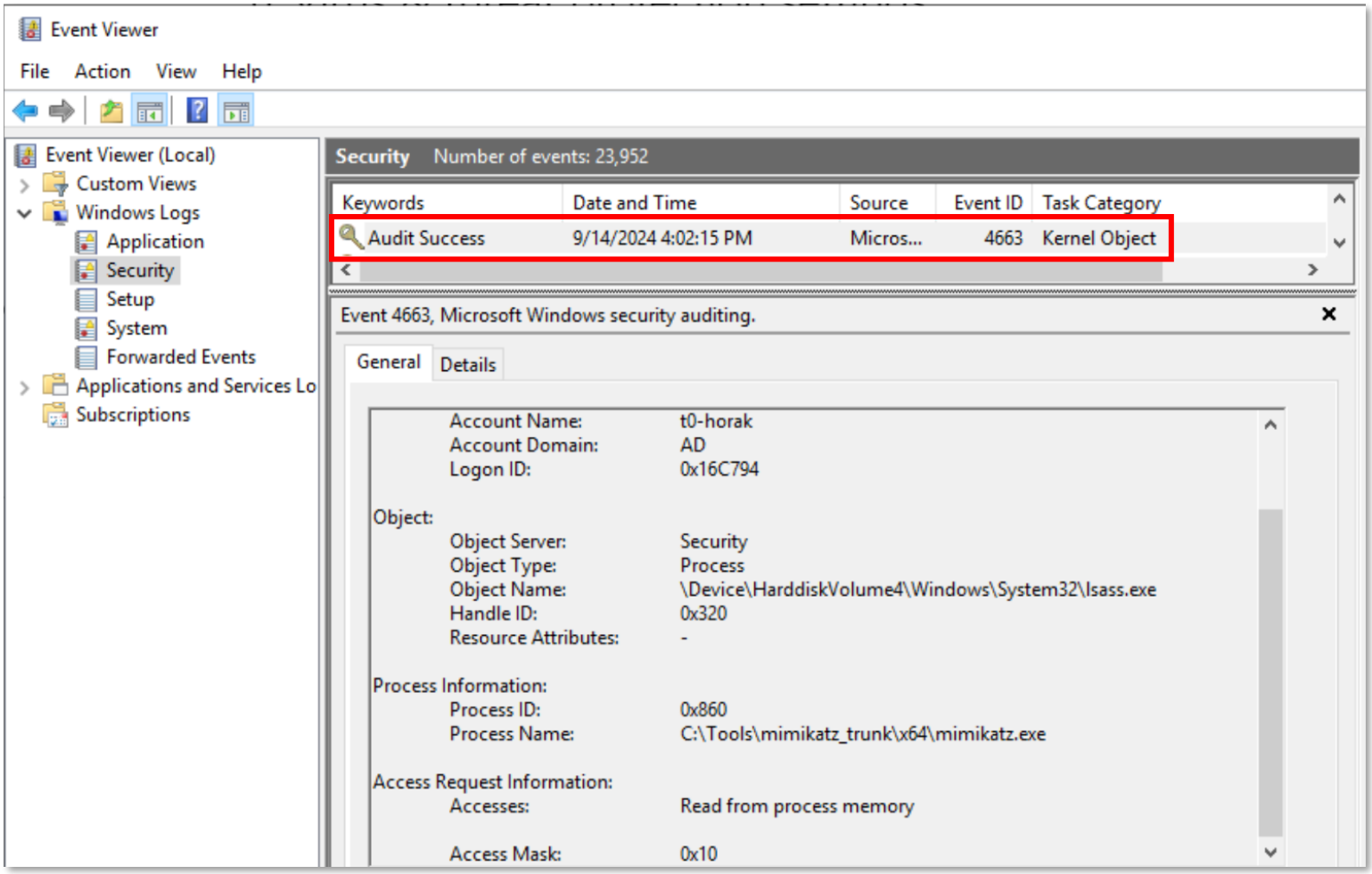
https://www.linkedin.com/company/horizon-secured/

3. Now let's test our configuration. You can use Mimikatz for this usecase. You must have antivirus disabled otherwise it gets blocked. In Mimikatz use following commandlet to test auditing configuration for our **lsass.exe:**

- **sekurlsa::logonpasswords**



4. Let's confirm our auditing works in Event Viewer. We are looking for **Event ID 4663** in **Security** log.

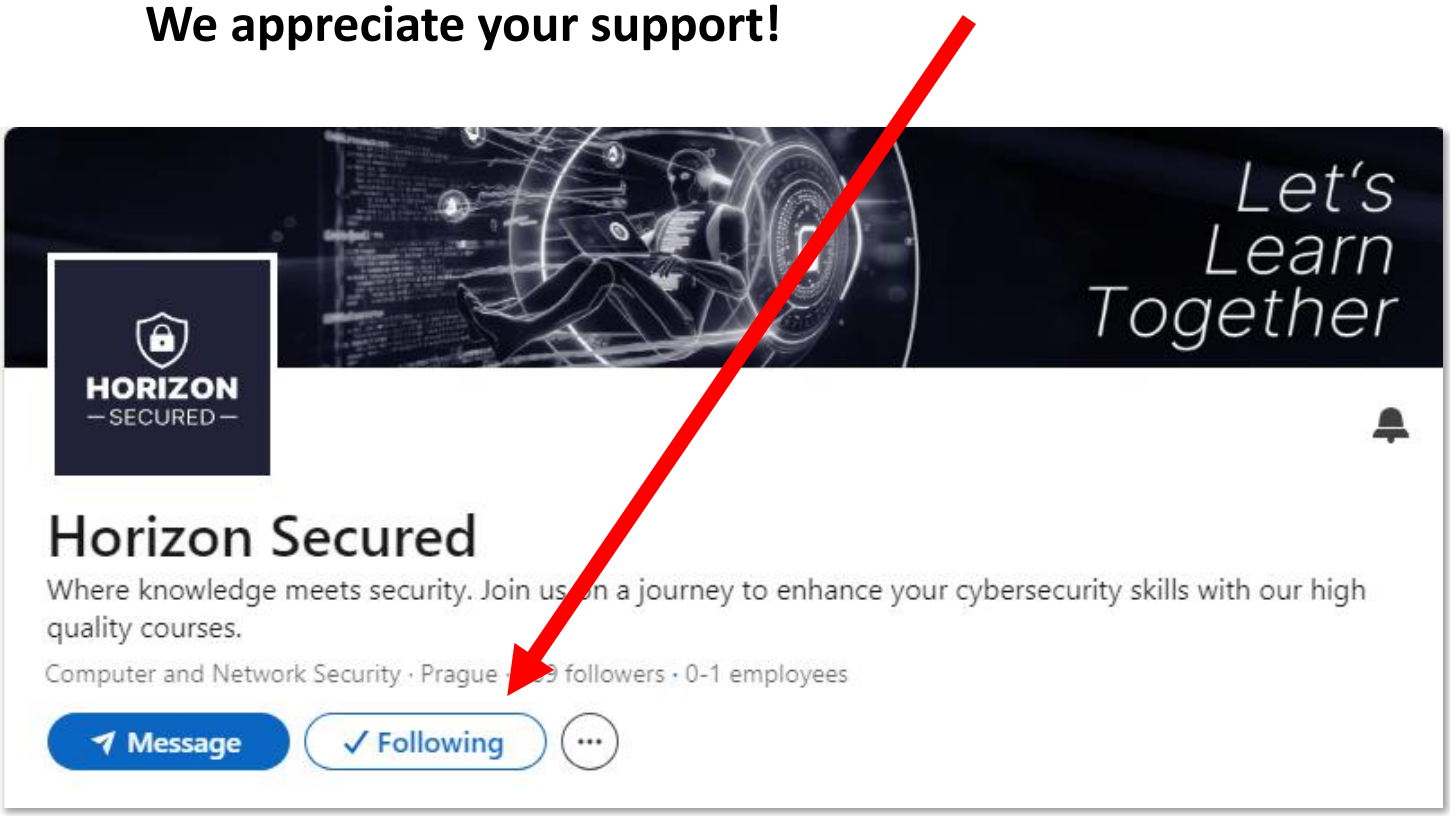


Enjoyed This Content?

We have courses with similar insights and some of them are **FREE**:

https://horizon-secured.com/courses/

Stay up to date with Horizon Alert Newsletter:

https://horizon-secured.com/newsletter/

We appreciate your support!