

S11L2



Data: 10/12/24

INFORMAZIONI PRINCIPALI

Traccia:

1. Installazione e utilizzo degli strumenti per il monitoraggio dei processi:

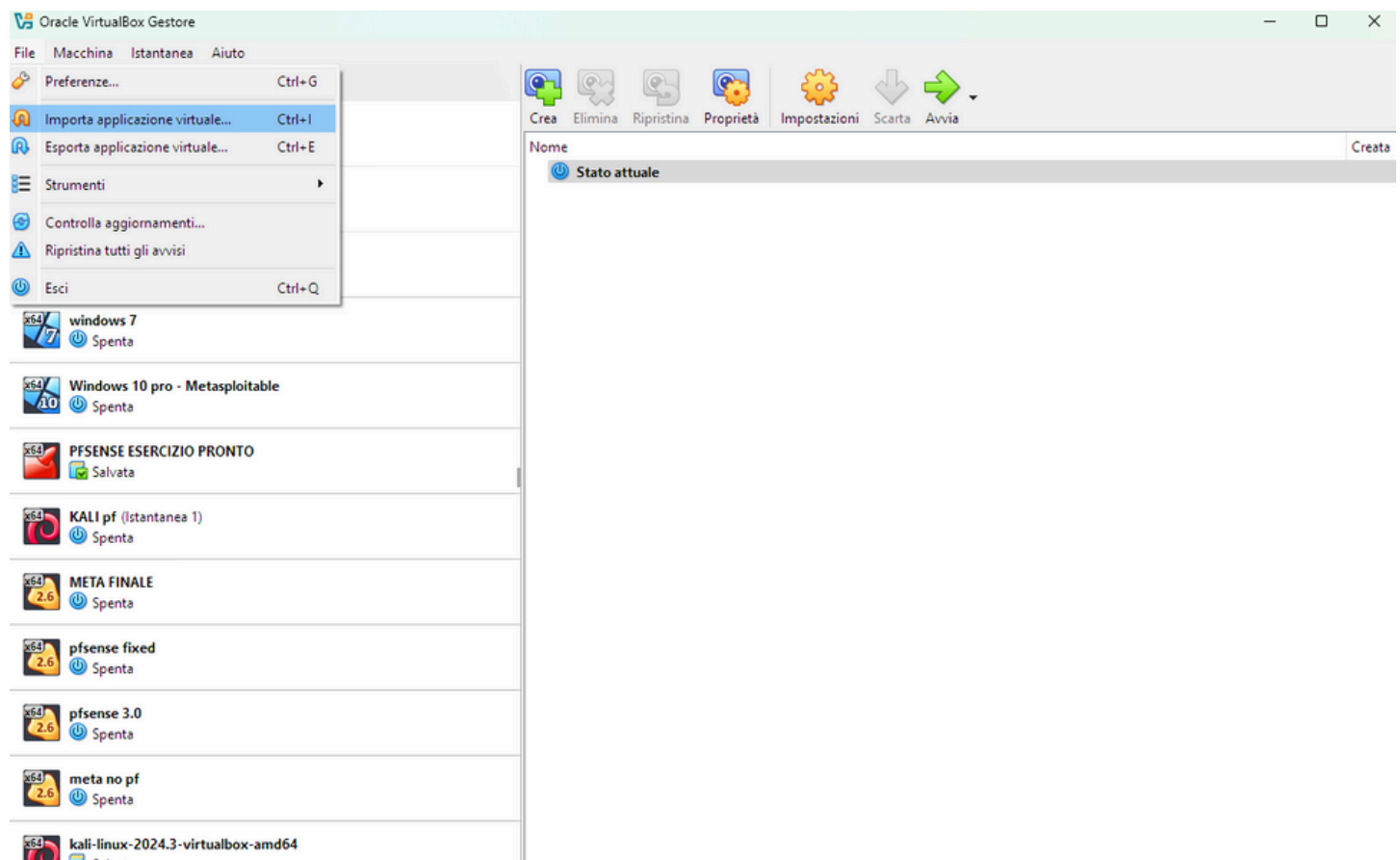
- Configurare due macchine virtuali: Cyberops Workstation e Security Onion.
- Una volta configurare ed installare le VM

2. Modifica delle impostazioni tramite il Registro di Windows:

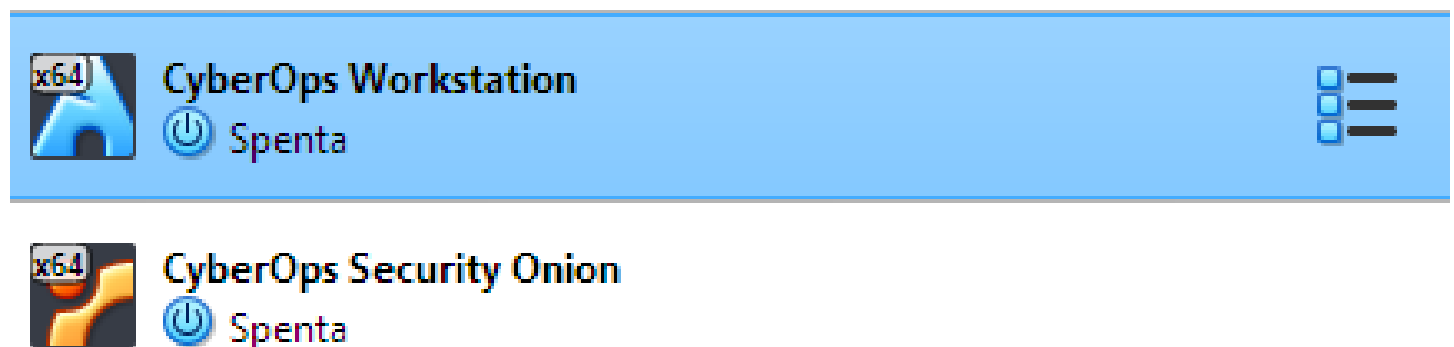
- Usare la macchina locale (Optional) per accedere al Registro di Windows.
- Modificare un'impostazione specifica usando l'editor del registro (Regedit).

INIZIO ESERCIZIO

Per iniziare installiamo le due macchine importandole.



Una volta importate, modifichiamo la schede di rete su NAT o Bridge (Per la connessione al mondo “esterno”)

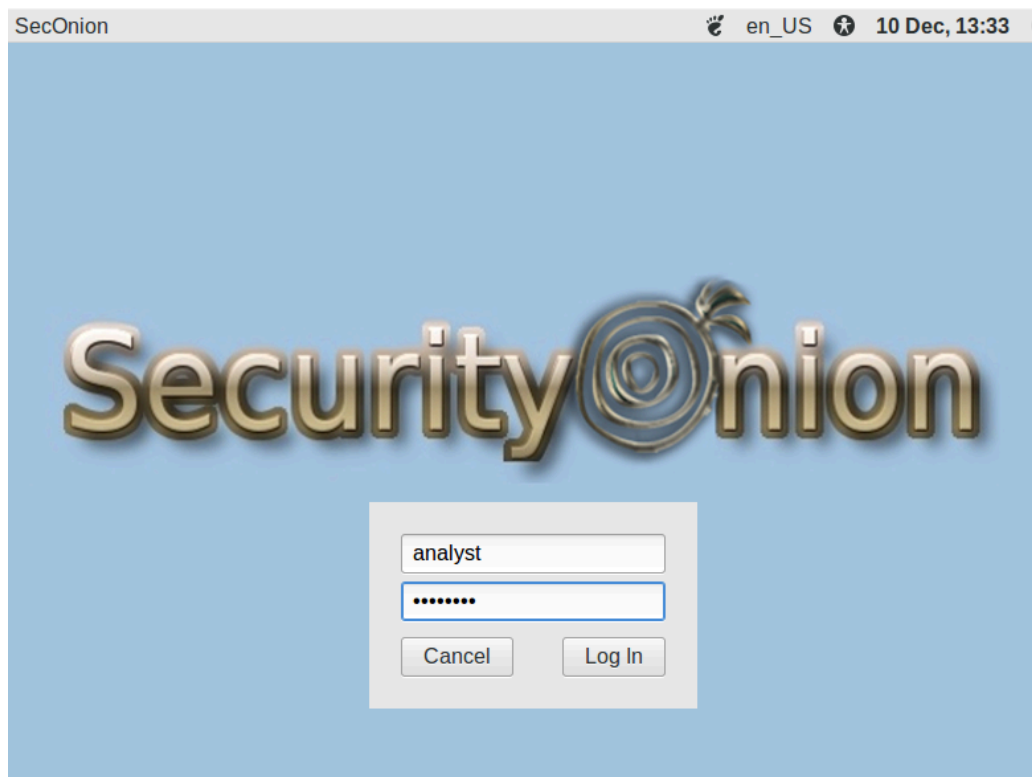


Una volta avviato accediamo con Analyst (user) e Cyberops (psw) Attualmente, Procmon for Linux non è disponibile nei repository ufficiali di Arch Linux.

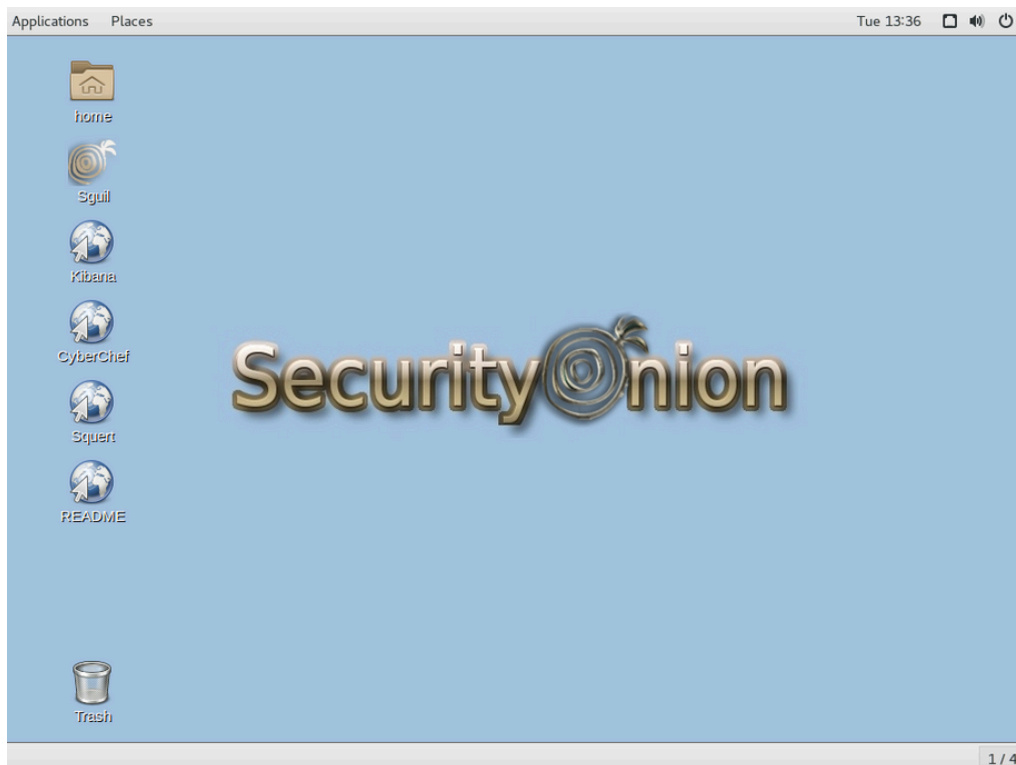


SECONDA MACCHINA

Allo stesso modo usiamo analyst (utente) e Cyberops (password)



Entrati dentro completiamo l'esercizio.



WINDOWS

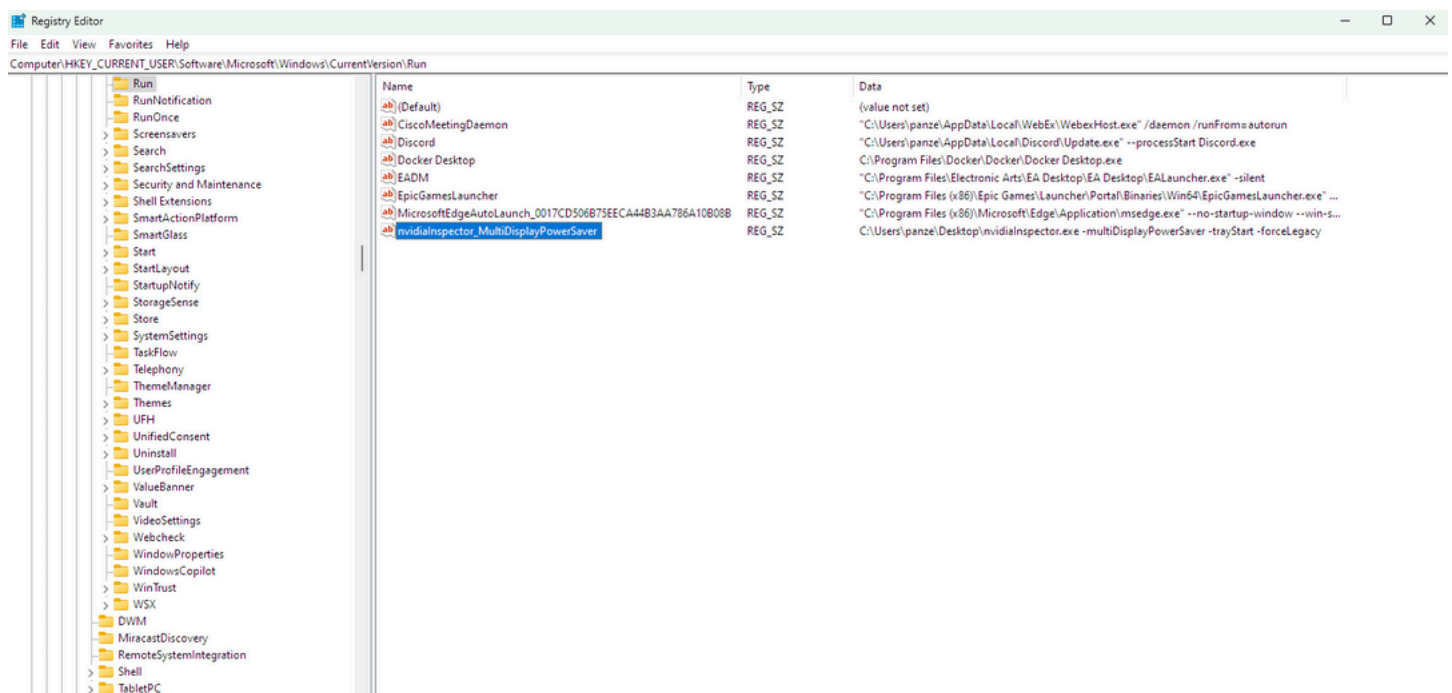
Apriamo process explorer e modificheremo che nvidiaDisplaysaver (mine) non partirà più all'avvio di windows. Procediamo poi con run Run e accediamo al registro con Regedit (scrivendolo o con Win+R per entrambi)

Troviamo la chiave e il percorso associato per l'avvio

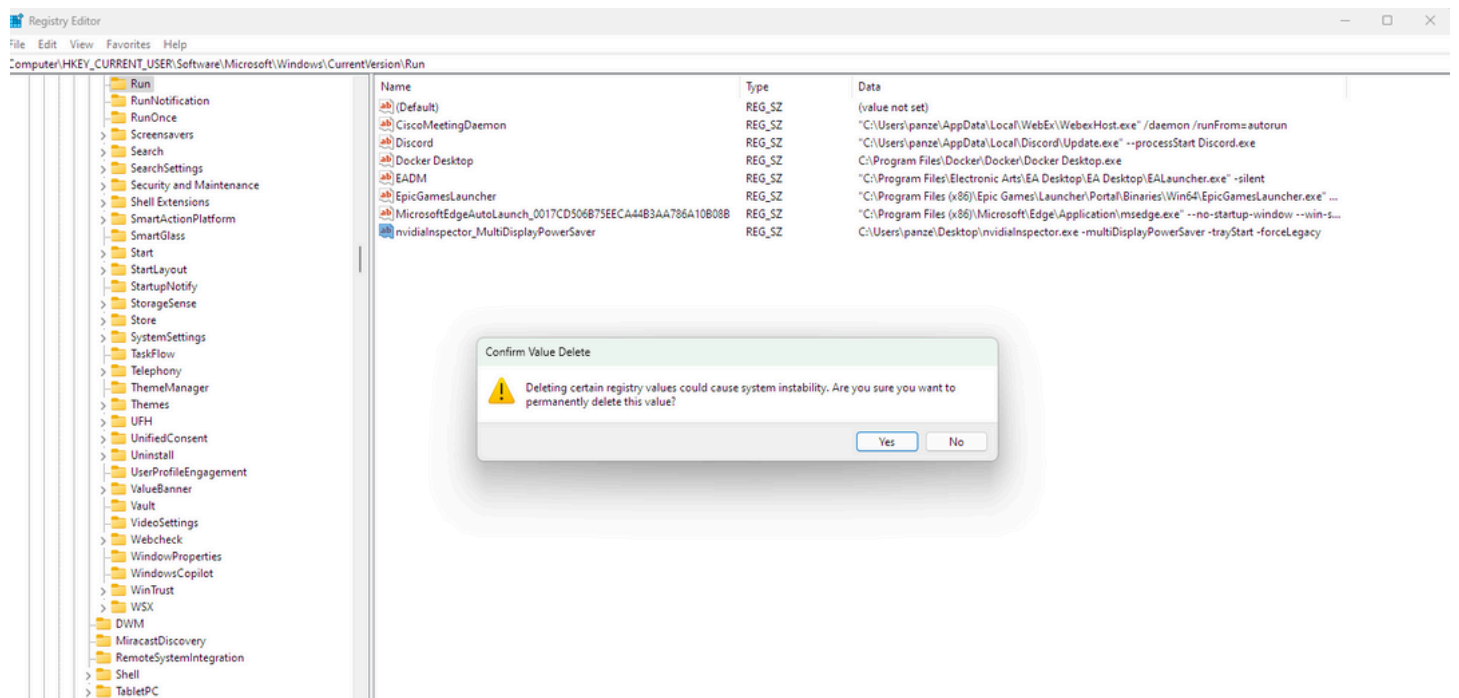
[HKLM\Software\Microsoft\Windows\CurrentVersion\Run per l'avvio di sistema]

e [HKCU\Software\Microsoft\Windows\CurrentVersion\Run per l'utente corrente]

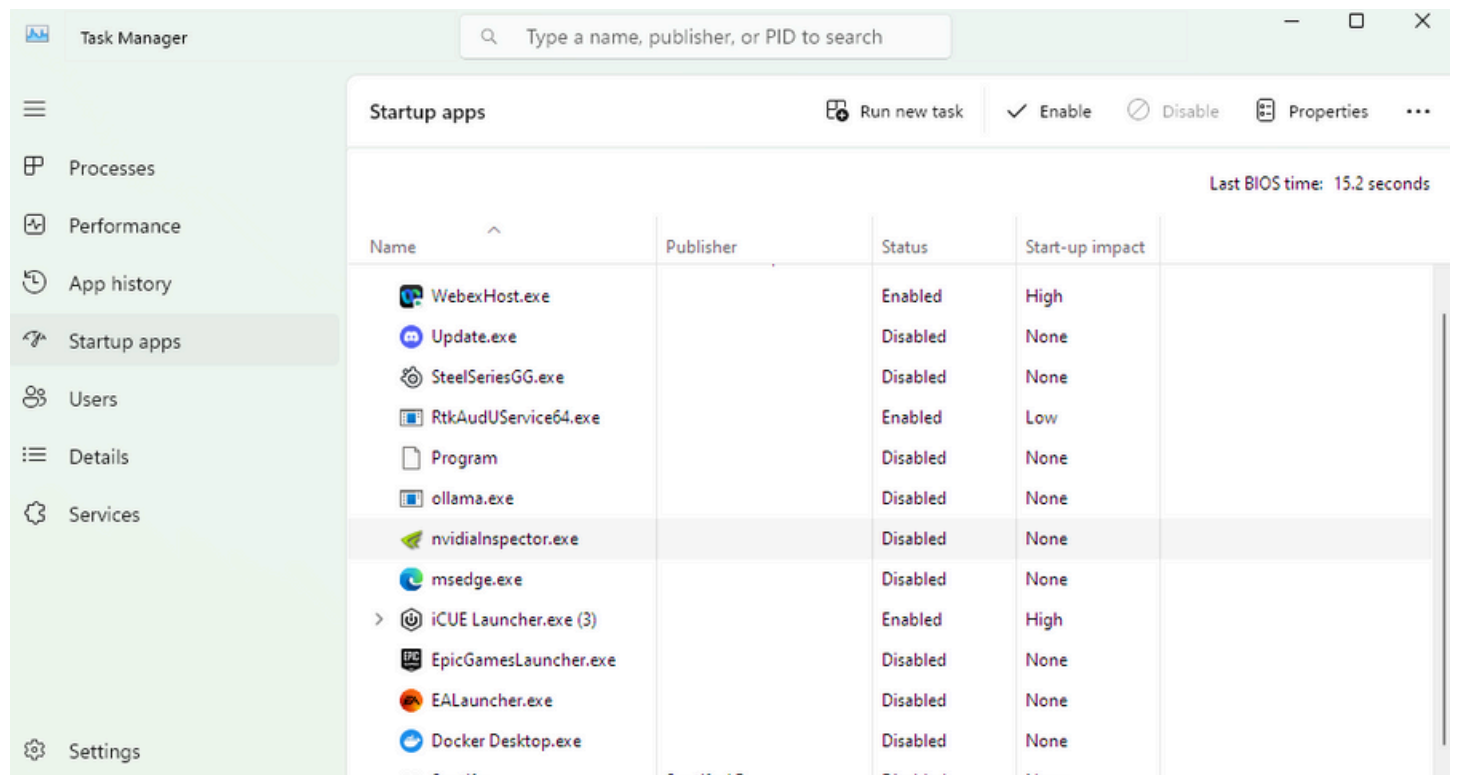
e cerchiamo voci con Nvidia "save"



La cancelliamo, per non avere più il process



Prima: (anche se era già disabilitata, la potevamo attivare modificando la chiave. o cancellandola, la rimuoviamo direttamente.



Task Manager

Type a name, publisher, or PID to search

Startup apps

Run new task Enable Disable Properties

Last BIOS time: 15.2 seconds

Name	Publisher	Status	Start-up impact
Xbox	Microsoft Corporation	Disabled	None
WebexHost.exe		Enabled	High
Update.exe		Disabled	None
SteelSeriesGG.exe		Disabled	None
RtkAudUService64.exe		Enabled	Low
Program		Disabled	None
ollama.exe		Disabled	None
msedge.exe		Disabled	None
> iCUE Launcher.exe (3)		Enabled	High
EpicGamesLauncher.exe		Disabled	None
EALauncher.exe		Disabled	None
Docker Desktop.exe		Disabled	None
Spotify	Spotify AB	Disabled	None

Completando l'esercizio (Program is docker don't worry.)