S9L4

Conti Mirco

Data: 28/11/24

INFORMAZIONI PRINCIPALI

Traccia:: Analisi dei Log di Sicurezza di Windows

Obiettivo:
Condurre un'analisi dei log di sicurezza del'OS Windows, individuando eventi rilevanti e stilando una relazione tecnica che riassuma le principali scoperte.

Requirements* pip install -r requirements.txt (Recap)

Run (Esegui) è uno strumento integrato che consente agli utenti di avviare programmi, aprire file, directory o siti web e accedere a utility di sistema in modo fast, senza dover passare attraverso i menu tradizionali (Gui).

L'obiettivo di oggi era individuare attività rilevanti o potenzialmente sospette legate agli accessi al sistema, alla gestione degli account e alle modifiche di sicurezza.

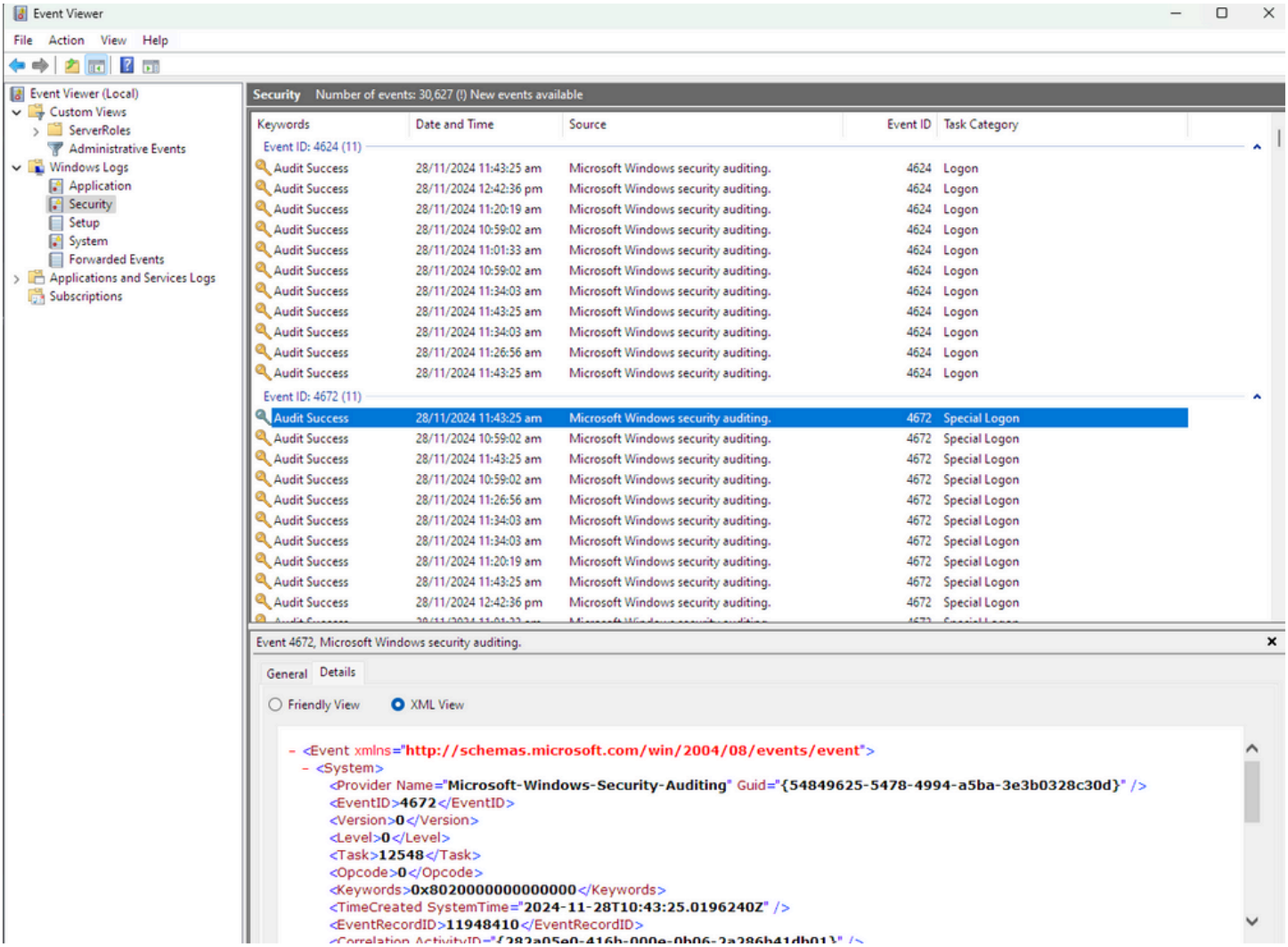
Warning: Ho Windows 11 Pro Eng* (Names will not match, currently doing the TryHackMe Course SEC level ½)

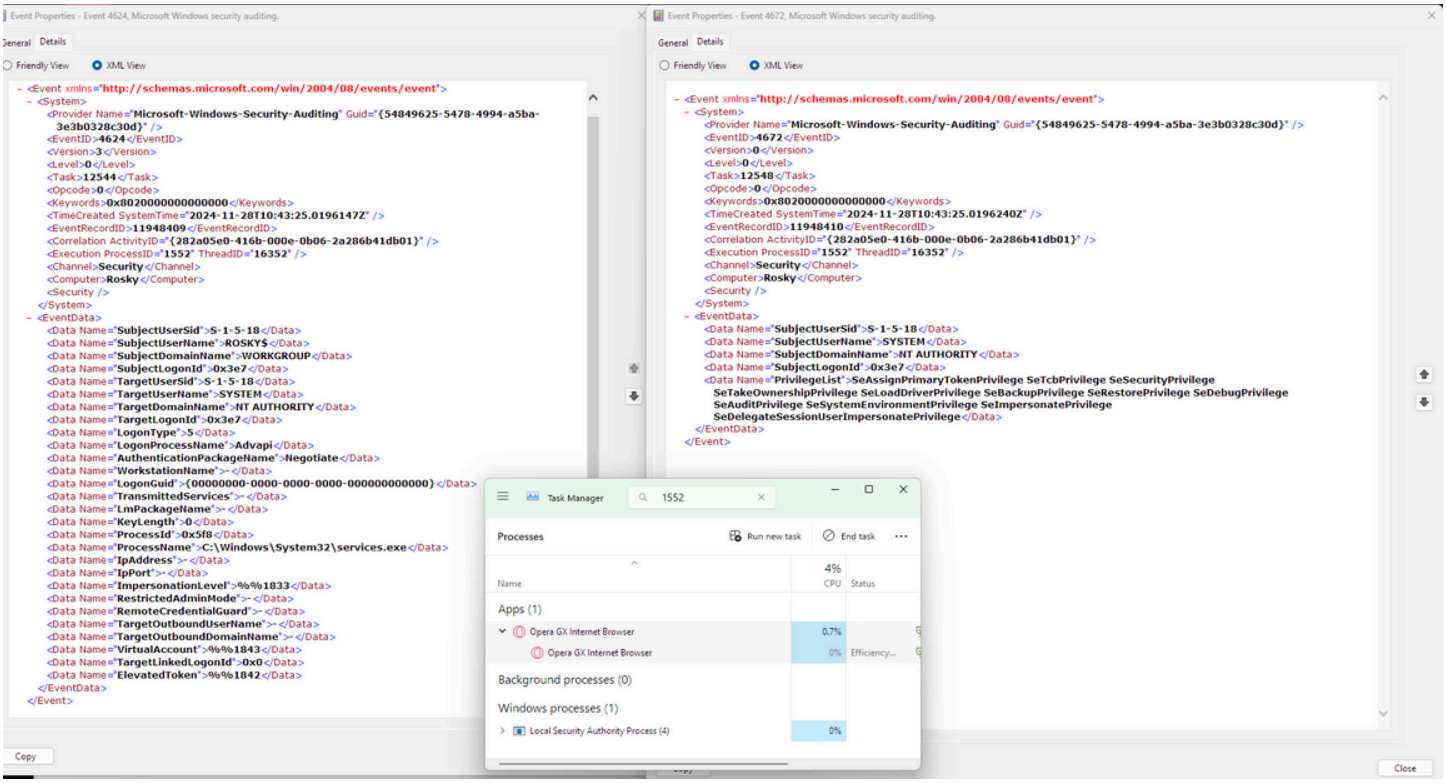
INIZIO ESERCIZIO

Sono entrato nel Visualizzatore eventi (EventViewer) avviandolo tramite lo strumento "Run" (Esegui) con lo shortcut Win+R e scrivendo “eventvwer”, ci permetterà di avviarlo che è il tool per vedere i log di sistema relativi alla sicurezza network. Procedo accedendo ai Registri di Windows(WindowsLogs) e poi su Sicurezza(Security). Qui ho provato a filtrare gli eventi per concentrarmi su quelli più significativi, come:

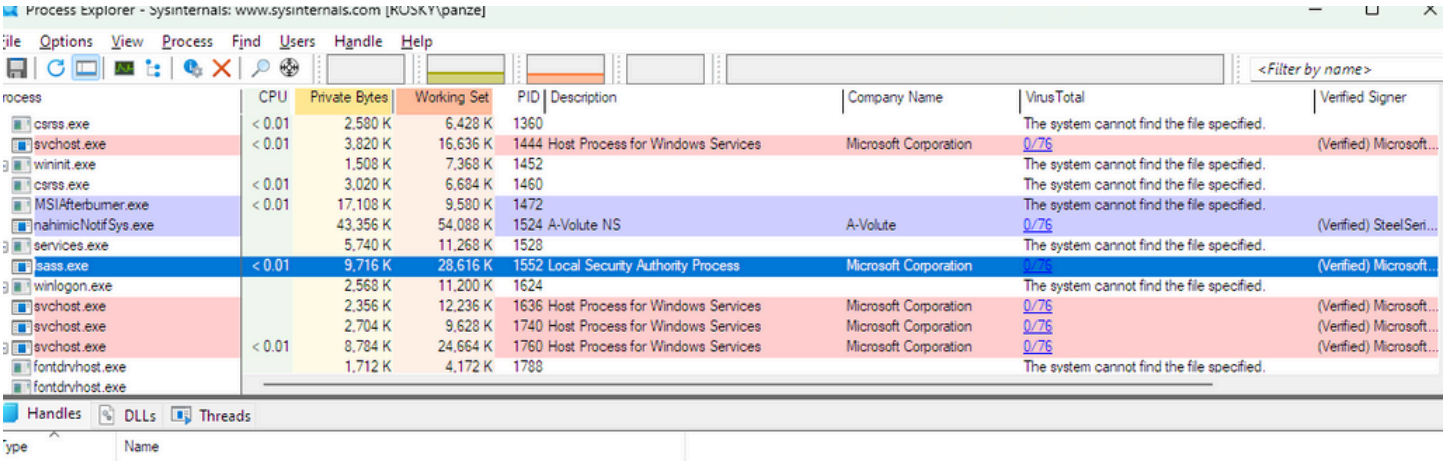
- **Accessi riusciti (ID evento 4624).**
- **Accessi falliti (ID evento 4625).**
- **Modifiche ai privilegi (ID evento 4670, 4672).**
- **Gestione degli account (ID evento 4720 e 4726).**

Filtrando con “View” and “Sort by” possiamo filtrare più a fondo insieme a “Group” per vedere gli gli eventi che ci interessano (sospetti)





Possiamo controllare anche il PID e il thread creato con il task manager.
(meglio procEXP/procMON)



Possiamo anche fare una scansione live con virustotal dei processi attivi in in quel momento di tutto il sistema operativo (Will return err. if it can't check (and send) the hash to Virustotal).

Controllerà anche il certificato e la firma se sarà da un vendor famoso. **(non tutti possiedono questo "dono", si può anche falsificare e non è un ottimo indicatore, comunque da tenere d'occhio)**

(options>virustotal>uknownexec>check virustot.)

ProcEXP

Gli eventi con ID 4624 registrano gli accessi riusciti al sistema. Ho individuato diversi log legati a questo evento, i quali confermano che l'utente ROSYKYS (Me), appartenente al dominio WORKGROUP, ha effettuato l’accesso correttamente. Non sono emersi accessi da account esterni o non autorizzati. Questi accessi si sono verificati in contesti operativi regolari, come il logon di servizio evidenziato dal "LogonType 5".

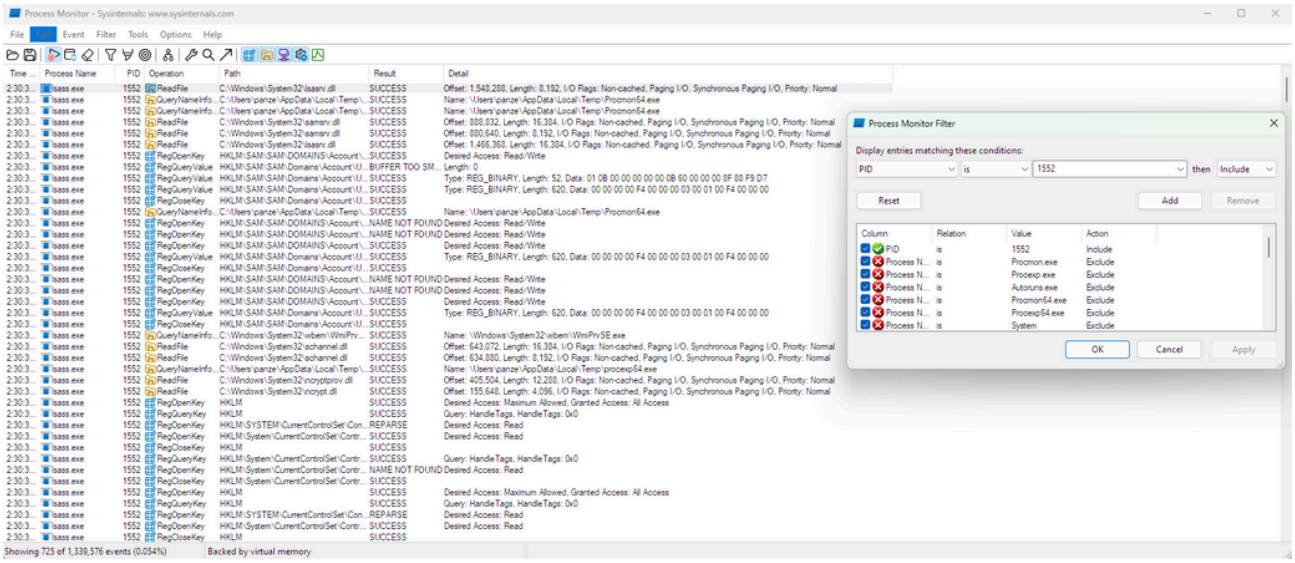
Ho poi verificato gli eventi con ID 4625, che registrano gli accessi falliti. Non è stato trovato alcun log associato a tentativi di accesso non autorizzati o falliti durante il periodo di monitoraggio (monitoring) . Questo suggerisce che non ci sono state attività sospette volte a compromettere l’autenticazione degli account.

Per quanto riguarda le modifiche ai privilegi, ho analizzato gli eventi con ID 4670 e 4672. L'evento 4672, come riportato in precedenza, rappresenta un "Special Logon" effettuato dall'account di sistema SYSTEM. Non sono stati trovati eventi 4670, che avrebbero indicato modifiche dirette ai privilegi di sicurezza o agli oggetti sensibili. I privilegi elencati per l’account SYSTEM (come SeDebugPrivilege e SeTakeOwnershipPrivilege) sono stati assegnati in modo previsto e non risultano alterati.

Ho esaminato inoltre la gestione degli account, controllando gli eventi con ID 4720 (creazione di un account) e 4726 (eliminazione di un account). Non è stato registrato alcun evento di creazione o rimozione di account durante il periodo analizzato, il che suggerisce che la configurazione degli utenti e degli account del sistema è rimasta invariata.

Infine, l'analisi ha incluso il processo identificato dal PID 1552, corrispondente al Local Security Authority Process (LSASS). Questo processo, essenziale per il sistema, gestisce autenticazioni e token di sicurezza, operando in conformità con i log 4624 e 4672. La presenza del browser Opera durante l'analisi è stata ricondotta ad attività legittime, come la consultazione di risorse, senza evidenze di comportamenti anomali.

ProcMON



Dopodiche ho analizzato con Procmon che ci permette di osservare le modifiche (o letture) del registro in modo più dettagliato, ma con alcune differenze rispetto ad altri strumenti (ad esempio, non è pensato per identificare virus o altre minacce specifiche). Permette di visualizzare in dettaglio le operazioni sul registro e altre dipendenze, come le librerie in uso dal programma. Se il processo fosse malevolo, sarebbe possibile rilevare chiamate sospette, come l'invocazione (invocation) di /t -cmd.exe, che potrebbe indicare l'avvio di una shell remota, o l'uso di strumenti per bindarsi a porte locali o remote. Inoltre, è possibile individuare modifiche critiche al sistema, come quelle relative a chiavi del registro come HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters, utilizzate per la configurazione di rete (e se il malware sfruttasse librerie come ws2_32.dll, queste potrebbero apparire su Procmon in caso di connessione remota). Altre chiavi sospette potrebbero essere HKCU\Software\Microsoft\Windows\CurrentVersion\Runutilizzate per impostare la persistenza del malware al riavvio del sistema o anche chiavi con errore “access denied”. (processo che tenta di accedere più volte alla chiave del registro ma senza accesso)

Detto questo, Ho osservato come il processo sospetto (1552) che corrisponde a LSASS, accedeva a chiavi di registro e risorse di sistema. Se ci fosse stato un malware, avrei potuto individuare attività sospette come la creazione di una shell remota o modifiche a configurazioni di rete critiche, ad esempio l’invocazione di cmd.exe con parametri che potrebbero legare una shell al processo LSASS. Inoltre, avrei potuto vedere i dettagli relativi ai privilegi elevati o altre operazioni anomale. Dal controllo non è emerso niente, no modifiche al registro insolite. dipendenze (library dependecies) strane, shell remote o process injection (thankfully). Potremo indagare oltre con CFF per vedere lo scheletro di LSASS, mi sembra di esagerare per questa situazione. Non andremo a fare “escalation” e chiuderemo il rapporto con un falso positivo (Ipotetical).

In conclusione, non sono stati trovati eventi che suggeriscano accessi non autorizzati, tentativi di intrusione, modifiche non previste ai privilegi o interventi sugli account. Tutti i log analizzati riflettono operazioni legittime e il corretto funzionamento del sistema.

TL:DR =

Gli eventi 4624 e 4672 che vedi nel Visualizzatore Eventi indicano un accesso riuscito a Windows (4624) e l'assegnazione di privilegi speciali (4672) per un utente con permessi amministrativi. Il PID 1552 corrisponde al processo LSASS, che è fondamentale per la gestione della sicurezza di sistema, come l'autenticazione degli utenti e la gestione dei privilegi. È normale che compaia nei log di accesso. Opera è semplicemente aperto perché stavo usando il browser durante la sessione. Tutto quello che vedo sembra rientrare nel comportamento previsto del sistema.