S11L1

ESERCIZIO 1: Preparazione alle esercitazioni dei prossimi giorni

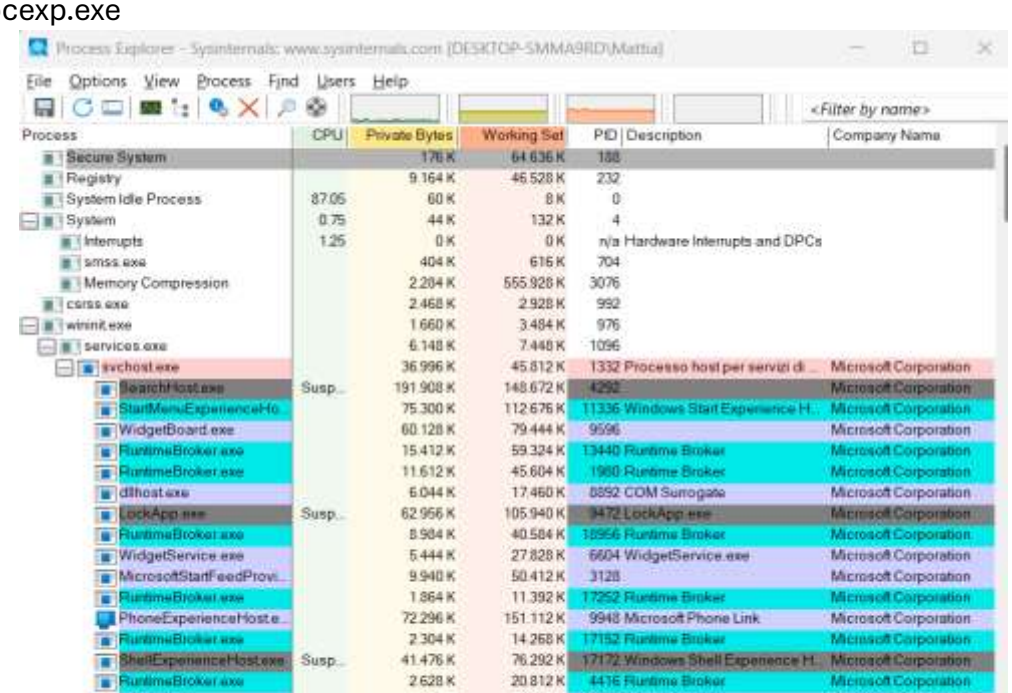
Scaricare e installare Per VirtualBox:

https://drive.google.com/file/d/1w9DG0erQ763XsJVOu7zH8RbZM2IkSob3/view?usp=drive_link
https://drive.google.com/file/d/1FSneSlqbyCD_dTo8F2NJMkE650y1UXZo/view?usp=sharing
Ho scaricato l'ova e importato su VM.

ESERCIZIO 2: Esplorazione di Processi, Thread, Handle e Registro di Windows

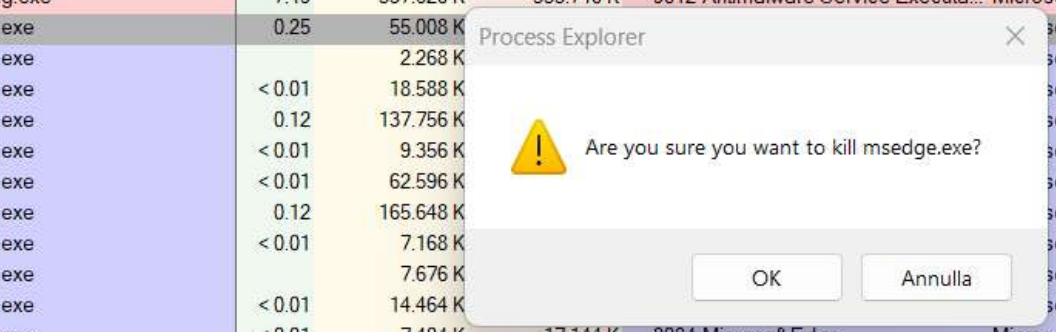
In questo laboratorio, esplorerai i processi, i thread e gli handle utilizzando Process Explorer della Suite SysInternals. Utilizzerai anche il Registro di Windows per modificare un'impostazione. ESERCIZIO 2: Esplorazione di Processi, Thread, Handle e Registro di Windows ESERCIZIO 2: Esplorazione di Processi, Thread, Handle e Registro di Windows ●Parte 1↵ Esplorazione dei Processi ● Parte 2↵ Esplorazione di Thread e Handle ● Parte 3 ↵ Esplorazione del Registro di Windows Risorse Richieste ● 1 PC Windows con accesso a internet

PASSO1
Apro procexp.exe



Da qui vado per killare:

NgcIso.exe		3.800 K	2.020 K	7224	
MsMpEng.exe	7.49	537.620 K	533.740 K	9012 Antimalware Service Executa...	Microsoft Corporation
msedge.exe	0.25	55.008 K			oft Corporation
msedge.exe		2.268 K			oft Corporation
msedge.exe	< 0.01	18.588 K			oft Corporation
msedge.exe	0.12	137.756 K			oft Corporation
msedge.exe	< 0.01	9.356 K			oft Corporation
msedge.exe	< 0.01	62.596 K			oft Corporation
msedge.exe	0.12	165.648 K			oft Corporation
msedge.exe	< 0.01	7.168 K			oft Corporation
msedge.exe		7.676 K			oft Corporation
msedge.exe	< 0.01	14.464 K			oft Corporation
msedge.exe	< 0.01	7.404 K	17.144 K	8084 Microsoft Edge	Microsoft Corporation
msedge.exe		7.480 K	17.304 K	10768 Microsoft Edge	Microsoft Corporation
MpDefenderCoreService.exe	< 0.01	14.452 K	13.560 K	4748 Antimalware Core Service	Microsoft Corporation
MicrosoftStartFeedProvider.exe		10.056 K	51.640 K	3128	Microsoft Corporation
Memory Compression	< 0.01	2.248 K	484.900 K	3076	
lsass.exe	< 0.01	13.828 K	21.660 K	1128 Local Security Authority Proc...	Microsoft Corporation



1 Cosa è successo alla finestra del browser web quando il processo è stato terminato?

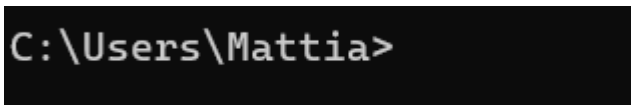
Appena ho killato si è chiusa pagina di Microsoft Edge.

NgcIso.exe		3.800 K	2.020 K	7224	
MsMpEng.exe	8.26	537.472 K	533.376 K	9012 Antimalware Service Executa...	Microsoft Corporation
msedge.exe	1.26	1.040 K	15.496 K	16880 Microsoft Edge	Microsoft Corporation
msedge.exe	< 0.01	2.368 K	9.996 K	9656 Microsoft Edge	Microsoft Corporation
msedge.exe	5.16	29.912 K	66.696 K	16116 Microsoft Edge	Microsoft Corporation
msedge.exe	0.63	31.796 K	71.076 K	11980 Microsoft Edge	Microsoft Corporation
MpDefenderCoreService.exe		14.452 K	13.560 K	4748 Antimalware Core Service	Microsoft Corporation
MicrosoftStartFeedProvider.exe		10.056 K	51.640 K	3128	Microsoft Corporation
Memory Compression	< 0.01	2.248 K	484.908 K	3076	
lsass.exe	< 0.01	13.796 K	21.628 K	1128 Local Security Authority Proc...	Microsoft Corporation

PASSO2

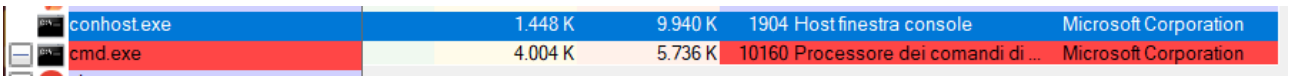
Cosa è successo durante il processo ping?

Apro il prompt, eseguo il ping e purtroppo non mi esce nulla...



Cosa è successo al processo figlio conhost.exe?

Appena ho killato cmd si è chiuso pure conhost.exe.



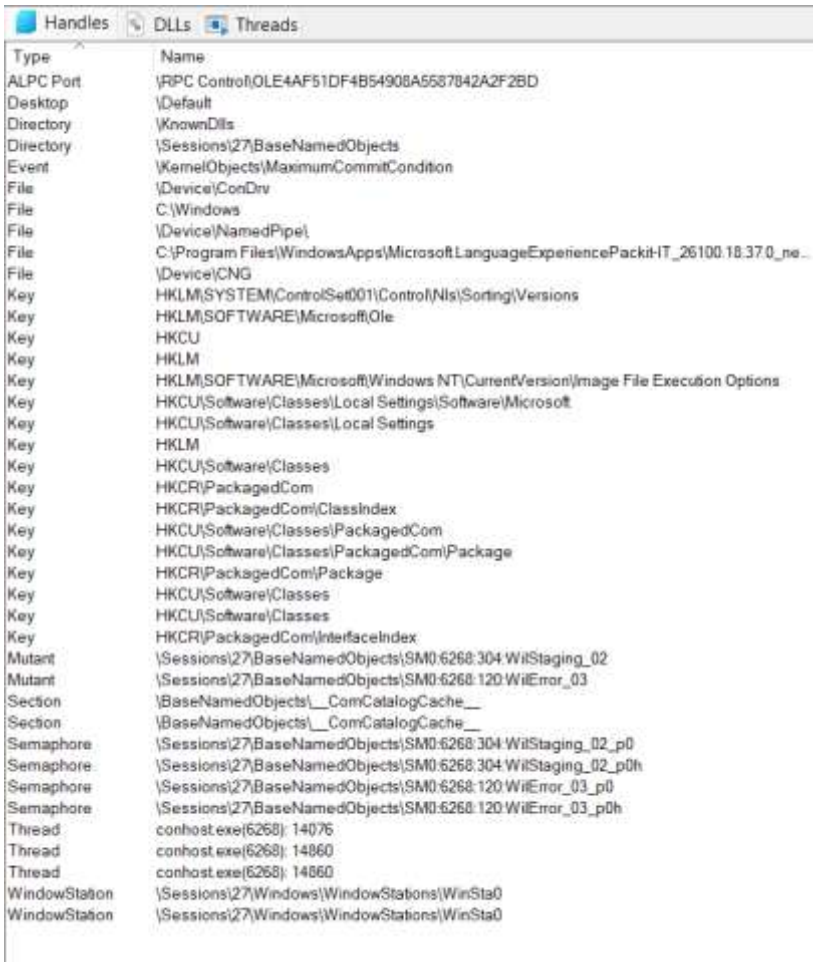
conhost.exe	1.448 K	9.940 K	1904 Host finestra console	Microsoft Corporation
cmd.exe	4.004 K	5.736 K	10160 Processore dei comandi di ...	Microsoft Corporation

Che tipo di informazioni sono disponibili nella finestra Proprietà?

Ci sono schede come TCP/IP, Security, Performance e altre che mostrano dettagli su come sta funzionando il processo, come l'utilizzo della CPU, l'ora di avvio, i thread e la priorità. Ci sono 3 processi in totale, e ognuno ha un suo ID, mi dice dove si trova il codice che il computer sta eseguendo per questo processo, quando è iniziato, quanto ha

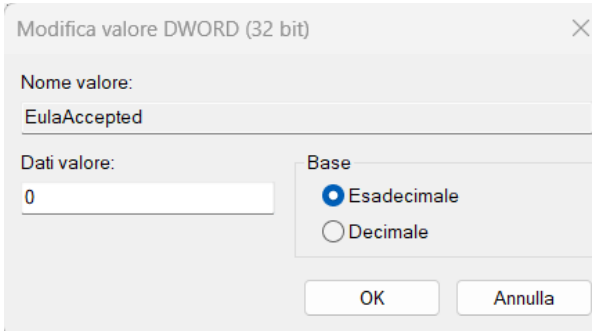
Esaminare gli handle. A cosa puntano gli handle?

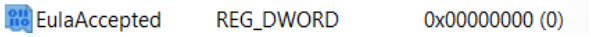
Gli "handle si usano per afferrare e controllare, come file, cartelle, o parti della memoria.



Qual è il valore per questa chiave di registro nella colonna Dati Data)?

Seguo prima i passaggi per arrivare a trovare la chiave di registro EulaAccepted, ho mofificato la chiave.





Quando apri Process Explorer, cosa vedi?

Dopo che ho messo 0 in EulaAccepted, mi dice che devo riaccettare.