

S11L1

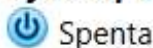
ESERCIZIO 1: Preparazione alle esercitazioni dei prossimi giorni

Scaricare e installare Per VirtualBox:

https://drive.google.com/file/d/1w9DG0erQ763XsJVou7zH8RbZM2lkSob3/view?usp=drive_link
https://drive.google.com/file/d/1FSneSlqbyCD_dTo8F2NJMkE650y1UXZo/view?usp=sharing
Ho scaricato l'ova e importato su VM.



CyberOps Workstation



CyberOps Security Onion

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

● 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

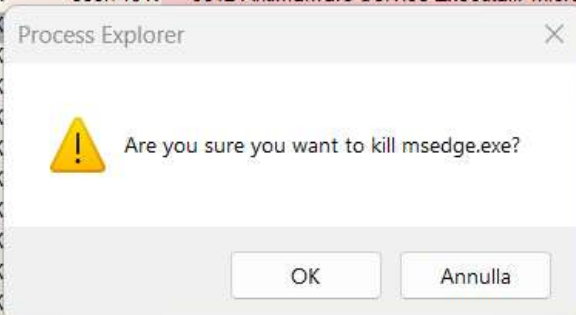
PASSO1

Apro procexp.exe

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Secure System		176 K	64.636 K	188		
Registry		9.164 K	46.528 K	232		
System Idle Process	87.05	60 K	8 K	0		
System	0.75	44 K	132 K	4		
Interrupts	1.25	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		404 K	616 K	704		
Memory Compression		2.204 K	555.928 K	3076		
csrss.exe		2.468 K	2.928 K	992		
wininit.exe		1.660 K	3.484 K	976		
services.exe		6.148 K	7.448 K	1096		
svchost.exe		36.996 K	45.812 K	1332	Processo host per servizi di	Microsoft Corporation
SearchIndexing.exe	Susp...	191.908 K	148.672 K	4292		Microsoft Corporation
StartMenuExperienceHost.exe		75.300 K	112.676 K	11336	Windows Start Experience H...	Microsoft Corporation
WidgetBoard.exe		60.128 K	79.444 K	9596		Microsoft Corporation
RuntimeBroker.exe		15.412 K	59.324 K	13440	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		11.612 K	45.604 K	1980	Runtime Broker	Microsoft Corporation
cdllhost.exe		6.044 K	17.460 K	8892	COM Surrogate	Microsoft Corporation
LockApp.exe	Susp...	62.956 K	105.940 K	3472	LockApp.exe	Microsoft Corporation
RuntimeBroker.exe		8.984 K	40.584 K	18956	Runtime Broker	Microsoft Corporation
WidgetService.exe		5.444 K	27.828 K	6604	WidgetService.exe	Microsoft Corporation
MicrosoftStartFeedProvi...		9.940 K	50.412 K	3128		Microsoft Corporation
RuntimeBroker.exe		1.864 K	11.392 K	17252	Runtime Broker	Microsoft Corporation
PhoneExperienceHost.exe		72.296 K	151.112 K	9948	Microsoft Phone Link	Microsoft Corporation
RuntimeBroker.exe		2.304 K	14.268 K	17152	Runtime Broker	Microsoft Corporation
ShellExperienceHost.exe	Susp...	41.476 K	76.292 K	17172	Windows Shell Experience H...	Microsoft Corporation
RuntimeBroker.exe		2.628 K	20.812 K	4416	Runtime Broker	Microsoft Corporation

Da qui vado per killare:

Ngclso.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			Microsoft Corporation
msedge.exe		2.268 K			Microsoft Corporation
msedge.exe	< 0.01	18.588 K			Microsoft Corporation
msedge.exe	0.12	137.756 K			Microsoft Corporation
msedge.exe	< 0.01	9.356 K			Microsoft Corporation
msedge.exe	< 0.01	62.596 K			Microsoft Corporation
msedge.exe	0.12	165.648 K			Microsoft Corporation
msedge.exe	< 0.01	7.168 K			Microsoft Corporation
msedge.exe		7.676 K			Microsoft Corporation
msedge.exe	< 0.01	14.464 K			Microsoft 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.

Ngclso.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...

```
C:\Users\Mattia>
```

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.

Type	Name
ALPC Port	\RPC Control\OLE4AF51DF4B54908A5587842A2F2BD
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\27\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	\Device\NamedPipe\
File	C:\Program Files\WindowsApps\MicrosoftLanguageExperiencePack\it-IT_26100.18.37.0_ne...
File	\Device\CNG
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKLM
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom
Key	HKCR\PackagedCom\ClassIndex
Key	HKCU\Software\Classes\PackagedCom
Key	HKCU\Software\Classes\PackagedCom\Package
Key	HKCR\PackagedCom\Package
Key	HKCU\Software\Classes
Key	HKCU\Software\Classes
Key	HKCR\PackagedCom\InterfaceIndex
Mutant	\Sessions\27\BaseNamedObjects\SM0:6268:304:WinStaging_02
Mutant	\Sessions\27\BaseNamedObjects\SM0:6268:120:WinError_03
Section	\BaseNamedObjects__ComCatalogCache__
Section	\BaseNamedObjects__ComCatalogCache__
Semaphore	\Sessions\27\BaseNamedObjects\SM0:6268:304:WinStaging_02_p0
Semaphore	\Sessions\27\BaseNamedObjects\SM0:6268:304:WinStaging_02_p0h
Semaphore	\Sessions\27\BaseNamedObjects\SM0:6268:120:WinError_03_p0
Semaphore	\Sessions\27\BaseNamedObjects\SM0:6268:120:WinError_03_p0h
Thread	conhost.exe(6268): 14076
Thread	conhost.exe(6268): 14860
Thread	conhost.exe(6268): 14860
WindowStation	\Sessions\27\Windows\WindowStations\WinSta0
WindowStation	\Sessions\27\Windows\WindowStations\WinSta0

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 modificato la chiave.

Modifica valore DWORD (32 bit)

Nome valore:
EulaAccepted

Dati valore:
0

Base
☒ Esadecimale
☐ Decimale

OK Annulla

EulaAccepted REG_DWORD 0x00000000 (0)

Quando apri Process Explorer, cosa vedi?

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

