

Esercitazione S11/L2

In questa esercitazione andrò a vedere alcune funzionalità del programma Process explorer.

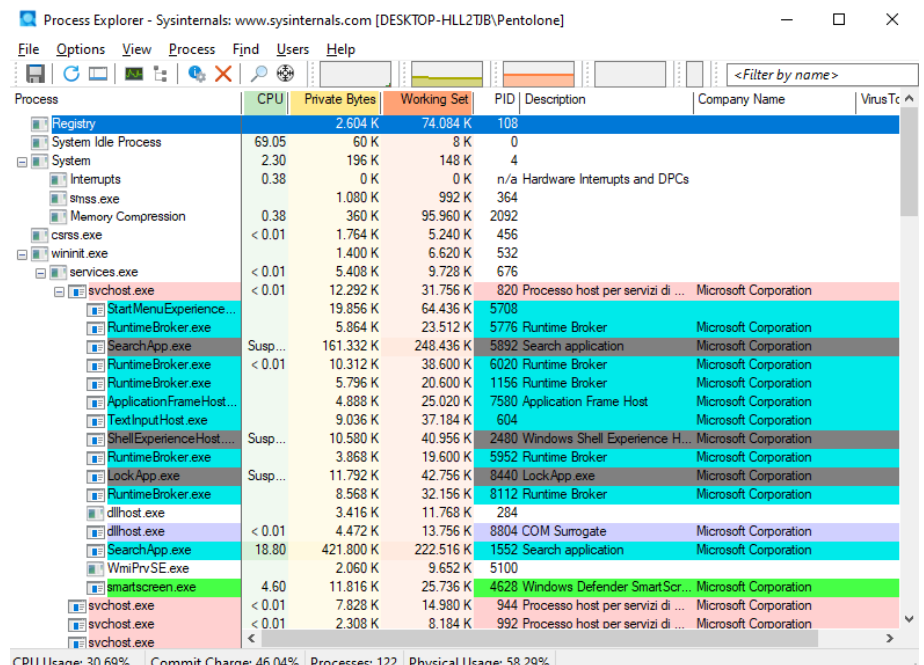
Process explorer

Process explorer è un software utile per controllare file, DLL e processi attivi sul sistema operativo. Si può paragonare ad un Task Manager più completo. Selezionando un processo è possibile visualizzare le librerie e i file collegati, sospenderlo, interromperlo, cambiargli di priorità o fare una ricerca su Internet per ottenere maggiori informazioni. Process Explorer è anche in grado di visualizzare ulteriori informazioni sul sistema, come l'uso della memoria, del processore e altro ancora.

Procedimento

Come primo step andrò a scaricare il software, si troverà nella suite di Sysinternals. Andrò ad avviarlo e mi troverò questa schermata:

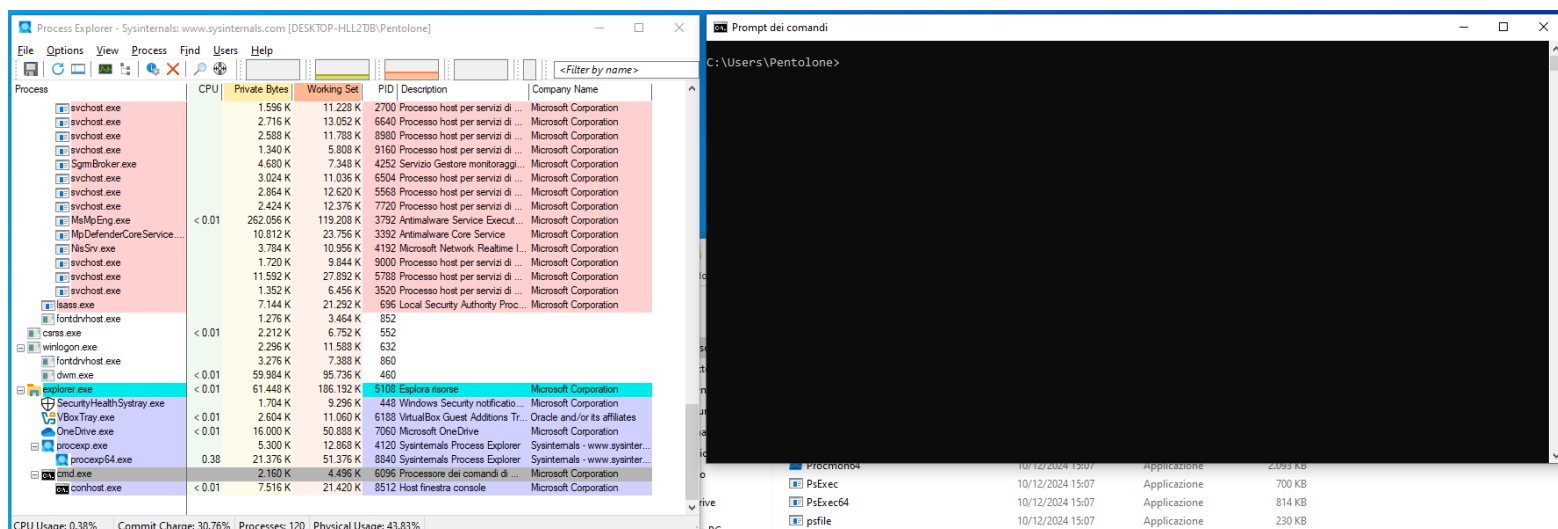
Si può notare la lista dei processi e sottoprocessi attivi sul sistema operativo. Si potranno andare a fare diverse opzioni e si vedono anche in basso la % di CPU utilizzata, numero di processi attivi ed altro.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTr
Registry		2.604 K	74.084 K	108			
System Idle Process		60 K	8 K	0			
System	2.30	196 K	148 K	4			
Interrupts	0.38	0 K	0 K	n/a	Hardware Interrupts and DPCs		
smss.exe		1.080 K	992 K	364			
Memory Compression	0.38	360 K	95.960 K	2092			
csrss.exe	< 0.01	1.764 K	5.240 K	456			
wininit.exe		1.400 K	6.620 K	532			
services.exe	< 0.01	5.408 K	9.728 K	676			
svchost.exe	< 0.01	12.292 K	31.756 K	820	Processo host per servizi di ...	Microsoft Corporation	
StartMenuExperienceHost.exe		19.856 K	64.436 K	5708			
RuntimeBroker.exe		5.864 K	23.512 K	5776	Runtime Broker	Microsoft Corporation	
SearchApp.exe	Susp...	161.332 K	248.436 K	5892	Search application	Microsoft Corporation	
RuntimeBroker.exe	< 0.01	10.312 K	38.600 K	6020	Runtime Broker	Microsoft Corporation	
RuntimeBroker.exe		5.796 K	20.600 K	1156	Runtime Broker	Microsoft Corporation	
ApplicationFrameHost.exe		4.888 K	25.020 K	7580	Application Frame Host	Microsoft Corporation	
TextInputHost.exe		9.036 K	37.184 K	604		Microsoft Corporation	
ShellExperienceHost.exe	Susp...	10.580 K	40.956 K	2480	Windows Shell Experience H...	Microsoft Corporation	
RuntimeBroker.exe		3.868 K	19.600 K	5952	Runtime Broker	Microsoft Corporation	
LockApp.exe	Susp...	11.792 K	42.756 K	8440	LockApp.exe	Microsoft Corporation	
RuntimeBroker.exe		8.568 K	32.156 K	8112	Runtime Broker	Microsoft Corporation	
dllhost.exe		3.416 K	11.768 K	284			
dllhost.exe	< 0.01	4.472 K	13.756 K	8804	COM Surrogate	Microsoft Corporation	
SearchApp.exe	18.80	421.800 K	222.516 K	1552	Search application	Microsoft Corporation	
WmiPrvSE.exe		2.060 K	9.652 K	5100			
smartscreen.exe	4.60	11.816 K	25.736 K	4628	Windows Defender SmartScr...	Microsoft Corporation	
svchost.exe	< 0.01	7.828 K	14.980 K	944	Processo host per servizi di ...	Microsoft Corporation	
svchost.exe	< 0.01	2.308 K	8.184 K	992	Processo host per servizi di ...	Microsoft Corporation	

CPU Usage: 30.69% | Commit Charge: 46.04% | Processes: 122 | Physical Usage: 58.29%

Andrò ora ad avviare il prompt dei comandi (cmd.exe) e proverò a fare un'azione per vedere eventuali cambi sul Process Explorer. Effettuerò un ping. Prima:



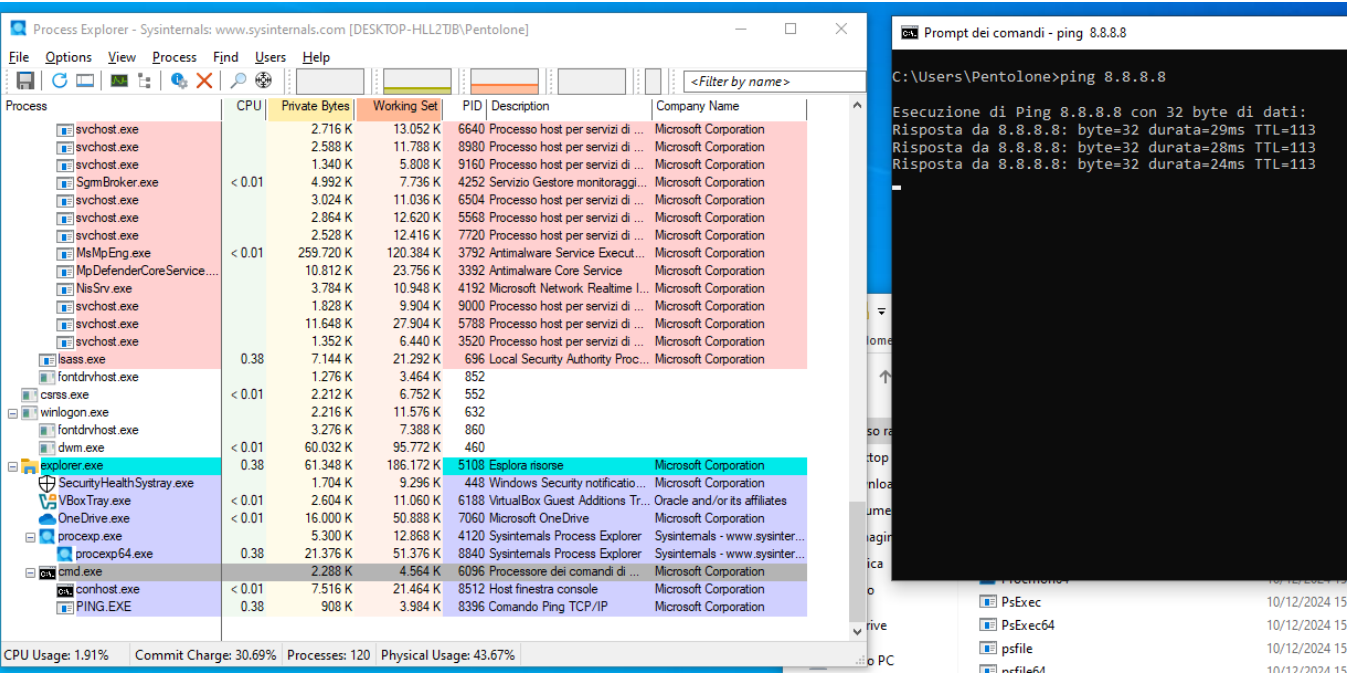
Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
svchost.exe		1.596 K	11.228 K	2700	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		2.716 K	13.052 K	6640	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		2.588 K	11.788 K	8900	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		1.340 K	5.808 K	9160	Processo host per servizi di ...	Microsoft Corporation
SgmBroker.exe		4.680 K	7.348 K	4252	Servizio Gestore monitoraggio...	Microsoft Corporation
svchost.exe		3.024 K	11.036 K	6504	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		2.864 K	12.620 K	5568	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		2.424 K	12.376 K	7720	Processo host per servizi di ...	Microsoft Corporation
MsMpEng.exe	< 0.01	262.056 K	119.208 K	3792	Antimalware Service Execut...	Microsoft Corporation
MsDefenderCoreService...		10.812 K	23.756 K	3392	Antimalware Core Service	Microsoft Corporation
NlsSvc.exe		3.704 K	10.556 K	4192	Microsoft Network Realtime L...	Microsoft Corporation
svchost.exe		1.720 K	9.844 K	9000	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		11.592 K	27.832 K	5788	Processo host per servizi di ...	Microsoft Corporation
svchost.exe		1.352 K	6.456 K	3520	Processo host per servizi di ...	Microsoft Corporation
lsass.exe		7.144 K	21.292 K	696	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1.276 K	3.464 K	852		
csrss.exe	< 0.01	2.212 K	6.752 K	552		
winlogon.exe		2.296 K	11.588 K	632		
fontdrvhost.exe	< 0.01	3.276 K	7.388 K	860		
dim.exe	< 0.01	59.984 K	95.736 K	460		
explorer.exe	< 0.01	61.448 K	186.192 K	5108	Esplora risorse	Microsoft Corporation
SecurityHealthSystray.exe	< 0.01	1.704 K	9.296 K	448	Windows Security notificazio...	Microsoft Corporation
VBoxTray.exe	< 0.01	2.604 K	11.060 K	6188	VirtualBox Guest Additions Tr...	Oracle and/or its affiliates
OneDrive.exe	< 0.01	16.000 K	50.888 K	7060	Microsoft OneDrive	Microsoft Corporation
process.exe		5.300 K	12.860 K	4120	Sysinternals Process Explorer	Sysinternals - www.sysinter...
process64.exe	0.38	21.376 K	51.376 K	8840	Sysinternals Process Explorer	Sysinternals - www.sysinter...
cmd.exe		2.160 K	4.496 K	6096	Processore dei comandi di ...	Microsoft Corporation
conhost.exe	< 0.01	7.516 K	21.420 K	8512	Host finestra console	Microsoft Corporation

CPU Usage: 0.38% | Commit Charge: 30.76% | Processes: 120 | Physical Usage: 43.83%

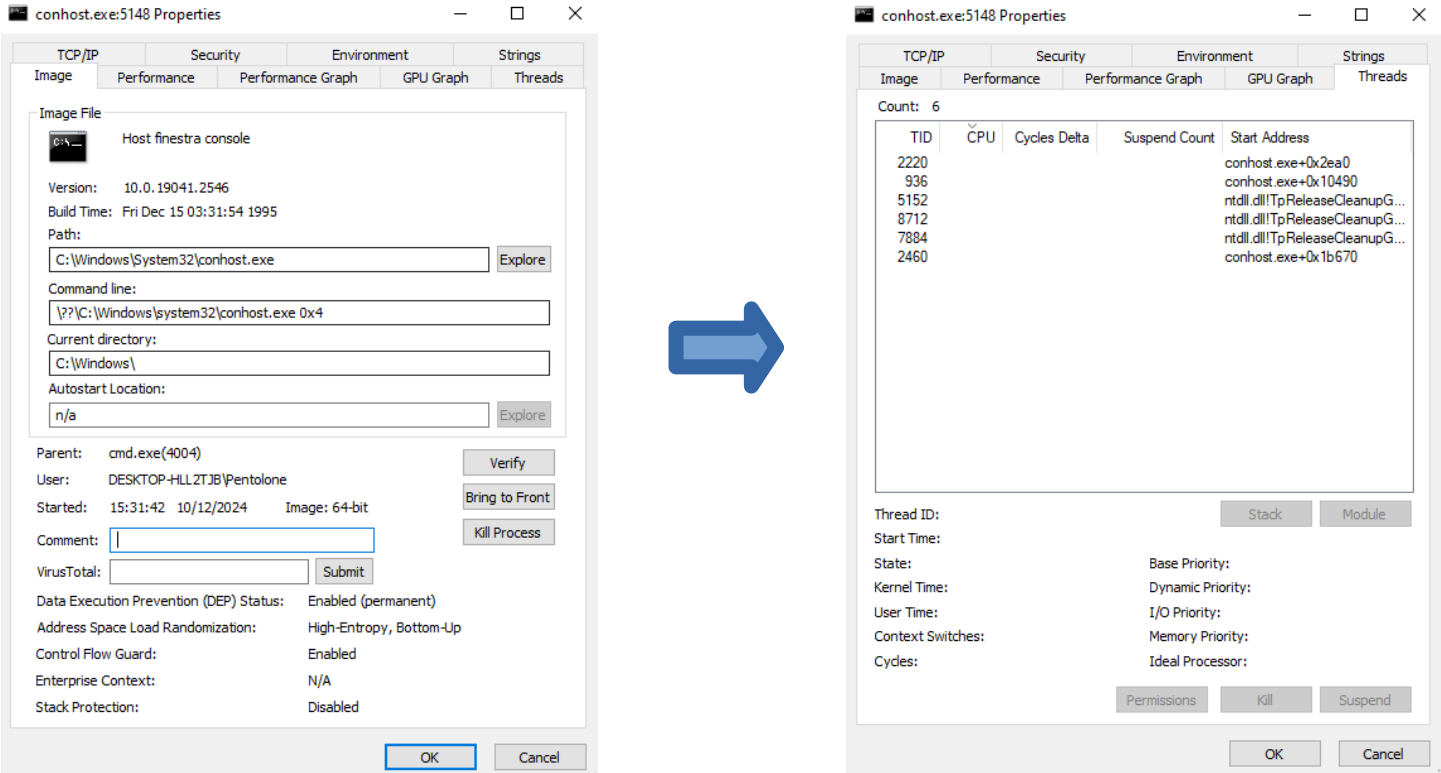
Command Prompt: C:\Users\Pentolone> ping 10.12.2024.1507

Processo	10/12/2024 15:07	Applicazione	2.059 KB
PsExec	10/12/2024 15:07	Applicazione	700 KB
PsExec64	10/12/2024 15:07	Applicazione	814 KB
psfile	10/12/2024 15:07	Applicazione	230 KB

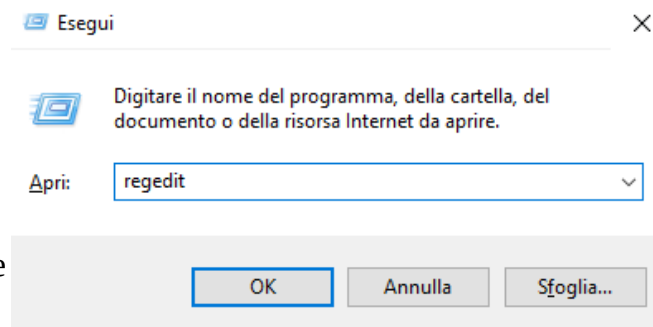
Dopo:



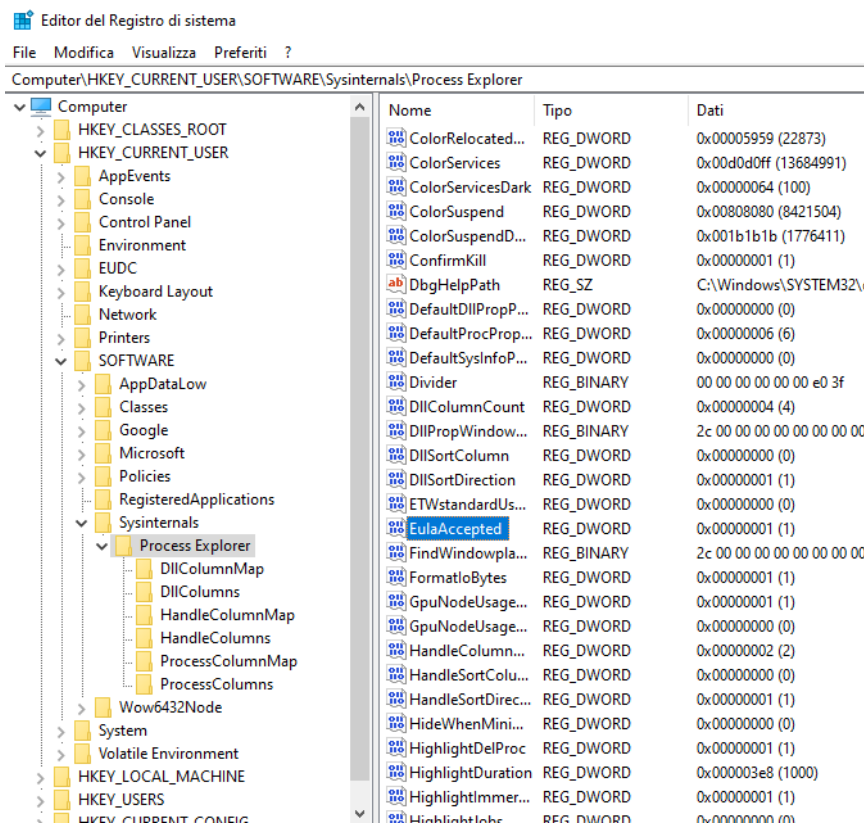
Si può notare, in fase di svolgimento del ping, il sottoprocesso PING.EXE.
Si possono anche vedere i thread legati al processo:



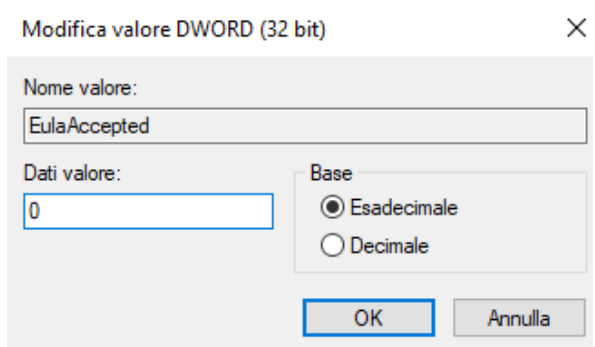
Con il comando regedit andrò ad aprire l'Editor di registro del sistema, uno strumento in grado di visualizzare e modificare il Registro di sistema. Questo viene utilizzato per gestire e modificare le impostazioni relative alle preferenze dell'utente e alla configurazione del sistema.



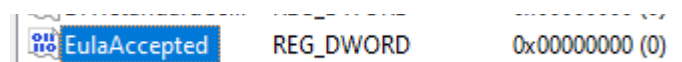
Andrò quindi a cercare in HKEY_CURRENT_USER il Process Explorer. Andrò a modificare l'EulaAccepted, quella regola che fa apparire l'accettazione dell'accordo di licenza con l'utente finale (EULA). Andrò a modificare



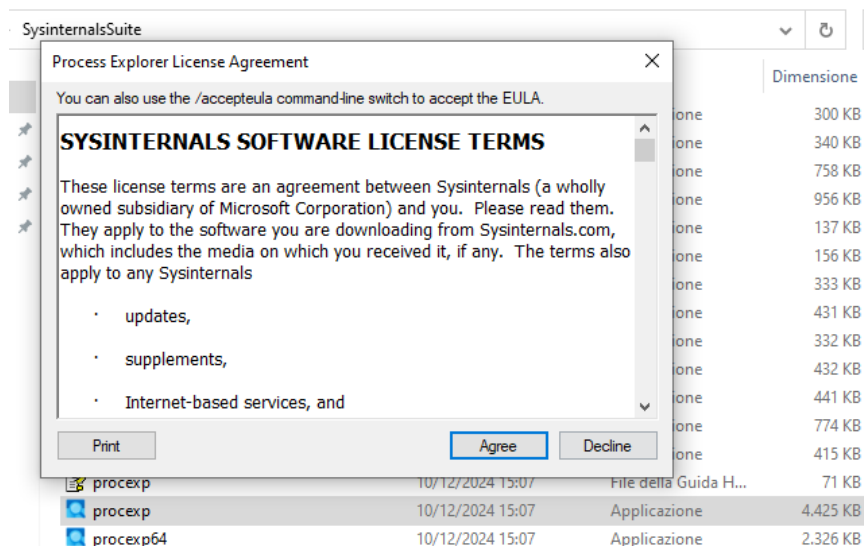
Andrò a modificare il valore poiché ho avviato il Process Explorer in precedenza e avevo già accettato l'EULA. Il valore sarà 1 se accettato, con 0 andiamo a ripristinare l'EULA.



Si vedrà infatti lo 0 allafine della riga



Andando a riaprire il software ci richiederà correttamente l'EULA.



Come ultima funzionalità con Process Explorer si può andare a scansionare un processo con VirusTotal. Cliccando con il pulsante destro, nel menù a tendina, comparirà lo scan direttamente con VirusTotal. Ci sarà quindi il riscontro nella tabella VirusTotal. Per l'esempio ho scansionando il processo conhost.exe e comparirà la scansione ottenuta (0/76).

