Esercizio.

Preparazione alla certificazione Cisco CyberOps.

Rispondi alle seguenti domande:

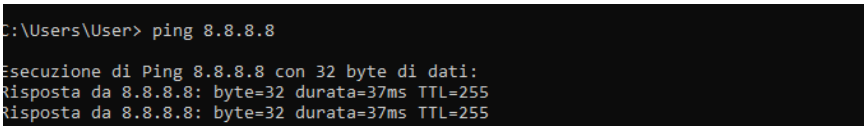
PARTE 1: Esplorazione dei Processi

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

   Quando il processo è stato terminato, la finestra del browser si è chiusa.

2) Cosa è successo durante il processo ping?

   Durante un comando ping nel Prompt dei Comandi, il processo cmd.exe ha creato un processo figlio conhost.exe. Il comando ping è stato eseguito dal processo conhost.exe.



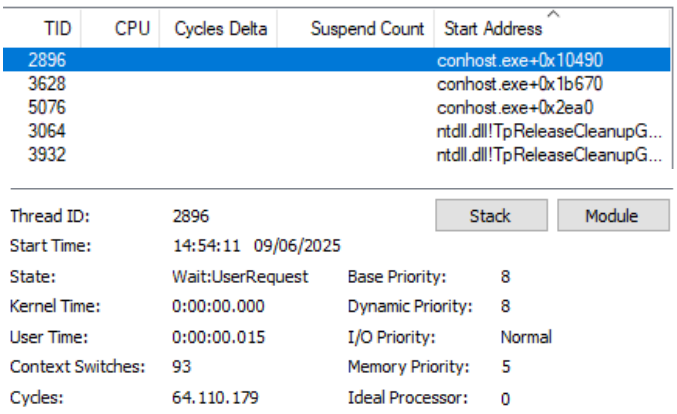
3) Cosa è successo al processo figlio conhost.exe?

   Quando il processo padre è stato terminato, anche il processo figlio conhost.exe è stato terminato.

PARTE 2: Esplorazione di Thread e Handle

4) Che tipo di informazioni sono disponibili nella finestra Proprietà?

   Nella finestra proprietà sono disponibili: l'ID del Thread, lo start time, lo stato, la priorità base, dinamica, di I/O della memoria, i cicli, i Context Switches.



5) Esaminare gli handle. A cosa puntano gli handle?

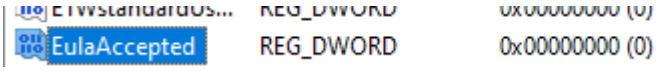
Gli handle puntano a un ALPC port, Desktop, a due directory, ad un Evento, a 7 files, a varie componenti di sistema (HKLM e HKCU), a 3 sessions, un processo e due Sezioni.

ALPC Port	\BaseNamedObjects\[CoreUI]-PID(5472)-TID(5076)f76de382-9801-4421-9f39-46ba530679...
Desktop	\Default
Directory	\KnownDlls
Directory	\Sessions\1\BaseNamedObjects
Event	\KernelObjects\MaximumCommitCondition
File	\Device\ConDrv
File	C:\Windows
File	C:\Windows\System32\it-IT\Conhost.exe.mui
File	C:\Windows\Fonts\StaticCache.dat
File	C:\Windows\System32\it-IT\user32.dll.mui
File	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0....
File	\Device\CNG
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Versions
Key	HKLM
Key	HKLM
Key	HKLM\SOFTWARE\Microsoft\Ole
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft
Key	HKCU\Software\Classes\Local Settings
Key	HKCU
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager
Key	HKLM\SYSTEM\ControlSet001\Control\Nls\Sorting\Ids
Key	HKCU\Software\Classes
Key	HKCU\Software\Classes
Mutant	\Sessions\1\BaseNamedObjects\SM0:5472:304:WilStaging_02
Mutant	\Sessions\1\BaseNamedObjects\SM0:5472:120:WilError_03
Mutant	\Sessions\1\BaseNamedObjects\SessionImmersiveColorMutex
Process	cmd.exe(4464)
Section	\Windows\Theme2581317009
Section	\Sessions\1\Windows\Theme1001625499
Section	\Sessions\1\BaseNamedObjects\SessionImmersiveColorPreference
Section	\BaseNamedObjects__ComCatalogCache__
Section	\BaseNamedObjects__ComCatalogCache__
Section	\Sessions\1\BaseNamedObjects\windows_shell_global_counters
Semaphore	\Sessions\1\BaseNamedObjects\SM0:5472:304:WilStaging_02_p0
Semaphore	\Sessions\1\BaseNamedObjects\SM0:5472:304:WilStaging_02_p0h
Semaphore	\Sessions\1\BaseNamedObjects\SM0:5472:120:WilError_03_p0
Semaphore	\Sessions\1\BaseNamedObjects\SM0:5472:120:WilError_03_p0h
Thread	conhost.exe(5472): 3628
Thread	conhost.exe(5472): 5076
Thread	conhost.exe(5472): 5076
Thread	conhost.exe(5472): 5076
Thread	conhost.exe(5472): 5076
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0
WindowStation	\Sessions\1\Windows\WindowStations\WinSta0

PARTE 3: Esplorazione del Registro di Windows

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

Dopo la modifica il valore per la chiave di registro è 0.



7) Quando apri Process Explorer, cosa vedi?

Vedo di nuovo l'avviso di sicurezza per Process Explorer.