Guida ai tools manuali

Guida approfondita sui vari tools manuali che si possono usare durante un controllo

Come descritto brevemente nella introduzione, per aiutarci nel controllo, vengono in aiuto diversi tool, automatici e manuali. Essendo i tool automatici comunque per definizione e design, semplici ed intuitivi da usare, in questo capitolo ci concentreremo solo ed esclusivamente sui tool manuali.

WinPrefetchView

WinPrefetchView è forse il uno dei tool più usati dagli staffer nei controlli. Permette di visualizzare tutti i file prefetch e le informazioni di essi con un interfaccia grafica abbastanza user friendly. Fa parte della suite di programmi NirSoft e funziona praticamente su ogni pc (anche quelli 32bit). Le informazioni sono tante ma non sono del tutto complete, per avere una overview piena delle informazioni di un file prefetch, bisognerà usare altri tool. Una cosa fondamentale da tenere a mente quando si usa winprefetchview, è quella di ordinare i file per modifica più recente, così che si può avere una timeline mediocre dei programmi eseguiti sul pc. Riassumendo, serve principalmente a vedere le informazioni principali dei file prefetch (index, dipendenze e risorse, path degli eseguibili etc.).

Process Hacker

Questo programma è forse il più conosciuto e il più utilizzato tra tutti i programmi. Fin dai primi giorni questo particolare tool è stato usato per aiutare lo staffer nei controlli ed ha sempre saputo fornire una quantità notevole di informazioni. Process hacker può essere considerata come una versione super avanzata di gestione attività. Ha tutte le funzioni di un normale gestione attività, ma appena andiamo a fare tasto destro su un processo notiamo perché questo tool è utilizzato da tutti gli staffer nel mondo. La quantità di opzioni che offre è quasi troppo, ogni informazione di un processo, ogni peculiarità, anche quelle apparentemente inutili, sono visualizzate da questo fantastico programma. La funzione più utilizzata è quella dell'esplorazione della memoria del processo, dove noi possiamo filtrare delle stringhe all'interno della memoria di un processo, una feature che verrà abusata nel tempo per creare nuovi metodi, a destra e a sinistra. Senza dubbio sono tutte informazioni utili quelle che si ricavano dai processi, ma non ci si dovrebbe mai basare su delle prove che sono, per loro stessa natura, volatili. A lungo, specialmente verso gli inizi, gli staffer si limitavano a controllare il .minecraft, qualche stringa su un processo qua e la e finivano il controllo. Ora queste funzionalità ci aiutano molto nei controlli, ma finalmente non sono l'unico modo per noi di dimostrare se un player sta cheattando o no. Di process hacker e delle funzioni legate alla memoria ne ho già parlato in modo esaustivo nella parte più teorica, sui processi e la memoria ram, perciò ora mi soffermo su altre due funzionalità molto utili su process hacker. La prima è quella di vedere gli handle di un processo. Questo significa che ogni risorsa caricata da quel processo in particolare viene elencata sul programma. Questo è molto utile per verificare l'esecuzione di metodi bypass come le mod unloaddate ma questo lo vedremmo nel capitolo successivo. Un altra feature, invece questa più per i cheater, è quella di avere la possibilità, con process hacker 2 (nel 3 è stata rimossa), di iniettare delle librerie .dll all'interno di un processo. Inoltre permette di vedere l'utilizzo che fanno i vari processi di tutte le risorse del pc, questo include dischi, network (con tutte le connessioni aperte dai vari processi) e tanto altro.

Everything

Santa sia voidtools, la società che ha sviluppato questo fantastico tool, che aiuta noi a trovare i file in tempo minimo, e con minimo sforzo. Il programma carica la master file table nella sua memoria e la interpreta, così che noi riusciamo a cercare in modo veloce all'interno di tutto il file system senza troppi problemi. É questione di scaricare l'installer, installarlo ed aprirlo e si riuscirà a trovare qualsiasi file o cartella in tempo zero.

USB Deview

USB Deview è un programma sviluppato da NirSoft, che ci permette di visualizzare tutti i dispositivi usb che sono stati collegati e che sono collegati. Questo ci potrebbe avvertire se l'utente usava due mouse, e ne ha disconnesso uno, oppure se ha cambiato mouse per evitare di trovare le macro impedendo l'accesso al software del mouse, insomma un tool molto utile per capire sempre, cosa è successo e quando, un tema ricorrente in tutti i tool che andremmo ad introdurre qui.

Fsutil

Essendo un programma incluso con windows, non c'è nessun bisogno di scaricarlo o altro. Fsutil è una command line utility che ci permette di esplorare il $USNJrnl:$J, ci lista tutte le sue entry e quindi cosa è stato registrato in quanto eventi, cambiamenti al file system e al disco.

WinLiveInfo

Windows 10 Live Information viewer, o meglio conosciuto come winliveinfo, è un tool open source, che si occupa di interpretari una vasta gamma di artefatti che indicano le più svariate cose. Questi artefatti vanno dalla lista completa di processi attuali, alle entry del registro BAM, alla MRU cache e così via. É un tool di estrema utilità e valore in quanto alle prove che egli ci fornisce, oltre a rendere più veloce il controllo.

PECmd

Una utility per command line, che permette di visualizzare ogni informazione di uno o più file prefetch.

OS Forensics

OS Forensics è un programma professionale (a pagamento) che offre in un solo tool, una vastissima gamma di sotto tool, tutti con lo scopo di ottenere informazioni riguardo il pc e cosa è successo, quando, dove e come. Si protrebbe considerare un tool a tutto tondo, offre davvero ogni funzionalità. Include un explorer della memoria dei processi, un parser per i file prefetch, un generatore di timeline dove analizza molti artefatti allo stesso tempo, per generare una timeline complessa ma sopratutto completa, un journal viewer, una ricerca di estensioni spoofate e così via. Insomma ogni tool immaginabile si trova all'interno di questo programma, il cui utilizzo è anche relativamente facile, grazie alla sua interfaccia user friendly.

FTK Imager

FTK Imager, fornito da access data, è un tool che permette l'analisi di immagini di dischi fissi. Montando al suo interno il disco del player controllato, abbiamo accesso ad ogni file, compresi quelli di sistema. Questo tool viene utilizzato per due scopi principali: L'estrazione di artefatti appartenenti al sistema operativo, quindi nasconsti e non accessibili normalmente; mentre l'altro è ottenere un dump intero della memoria ram.

NTFS Log Tracker

Un tool che ci permette di convertire i file raw della master file table, del journal e del $LogFile in file csv, leggibili da un umano e quindi interpretabili da programmi appositi per leggere file di quel genere.

Timeline Explorer

Un programma molto potente ma semplice, che ci permette di visualizzare e interpretare i file csv, che possono essere considerati un po' come la versione lite e primitiva dei file excel. Riesce ad aprire file di grandi dimensioni, molto importante per parsare artefatti complessi come quelli del journal e della master file table.

JD-Gui

Un programma che ci permette di visualizzare il contenuto degli archivi .jar, e quindi ci permette di decompilare tutti questi file java. Ci lascia dare un occhiata al codice sorgente, ammeno che esso non sia offuscato, ma comunque è fondamentale per capire se artefatti come le mod o altro sono legit o meno.

MemProcFS

Un programma che ci permette di trasformare un dump della memoria ram, in un file system esplorabile, con tutte le informazioni che potrebbero servirci, anche con delle feature già implementate per la conversione a csv e così via. Fondamentale per avere ogni aspetto di cosa contiene la memoria ram in quel preciso momento. Questo utlimo è una command line utility, ma solo un comando è già abbastanza per avere una serie di prove molto schiaccianti e affidabili

Registry (Windows)

L'explorer default per le chiavi di registro di windows, un tool fondamentale e incluso appunto con windows, che ci permette di visualizzare la gerarchia dei registri, insieme al valore delle loro chiavi

Programmi non menzionati

In questa guida ai vari tools fondamentali, abbiamo saltato molti altri tools che sono si utili, ma almeno io penso siano di seconda importanza rispetto a questi elencati. Una maestria dei programmi sopra elencati è necessaria per condurre dei controlli soddisfacenti. Detto questo lascio qua un elenco di programmi non elencati che potreste incontrare nel vostro viaggio nel mondo dei controlli:

- Hibernation recon
- Last Activity View
- User Assist View
- OpenSave File View
- Registry Explorer
- Kape
- EZ Viewer

- System Informer (Process hacker 3)
- …..

Questa lista come ho già specificato prima, potrà essere modificata in futuro, ci sono così tanti programmi ed è quasi impossibile listarli tutti, ma noi comunque ci proviamo.

Conclusioni

In questo capitolo abbiamo visto tutti i tool principali, insieme a delle informazioni riguardo a loro e alcune spiegazioni sul loro utilizzo. Come specificato in ogni capitolo, queste informazioni sono pensate per essere il più complete possibili ma niente è perfetto, perciò informatevi, e sopratutto rimanete interessati. Buon proseguimento.