Lab 6 – Analiza Registrului

**Scopul** acestui laborator este de a-i învăța pe studenți să extragă și să analize fișierele de Registru pentru orice artefacte relevante.

**Sarcina:**

1. Completați câmpurile libere de mai jos cu informația corespunzătoare, obținută în urma analizei fișierelor!

**Rezolvarea sarcinilor:**

Folosiți produsul din NTUSER.DAT pentru a răspunde la următoarele întrebări.

1. Din ce fus orar sunt datele și orele care apar pentru artefactele de registru?
2. Câte documente word au fost vizualizate recent prin Explorer? Care au fost numele de fișiere?
3. Au fost alte documente menționate în NTUSER.DAT? Dacă da, de ce acestea nu s-au regăsit în Registru?
4. Pe ce cale a fost accesat acesta și la ce oră? (Sugestie: adăugați în cronologie)
5. A fost instalat CCleaner și dacă da, când?
6. Ce a fost executat pe 8/1/17 la 17:56:12? În ce cheie s-a găsit acesta? (Sugestie: adăugați în cronologie)
7. Ce aplicații au fost setate la autorun? Având în vedere că este NTUSER.DAT, ce înseamnă acest lucru?

Folosiți produsul din SOFTWARE pentru a răspunde la următoarele întrebări.

1. Câte dispozitive USB au fost introduse în acest sistem? Care cheie v-a spus acest lucru?
2. Ce programe au fost setate la autorun?
3. Comparativ cu NTUSER.DAT, sunt aceleași programe? Dacă nu, de ce?
4. Ce versiune de Windows a fost instalată pe acest sistem? Când a fost instalată aceasta?

Folosiți produsul din SYSTEM pentru a răspunde la următoarele întrebări.

1. Care este numele gazdei sistemului victimă?
2. Care este dimensiunea maximă pentru Security Event log?
3. Ce adresă IP a fost atribuită ultima dată adaptorului de rețea?
4. La ce fus orar a fost configurat sistemul?

Folosiți instrumentul lui Eric Zimmerman AppCompatCacheParser pentru a răspunde la următoarele întrebări. Deschideți un prompt de comandă(cmd) și navigați către folderul unde ați salvat instumentul descărcat și tapați comanda “AppCompatCacheParser.exe –f SYSTEM --csv *filename*”.

1. Se afișează aici vreunul dintre programele setate la autorun? Care este marcajul temporal?
2. Are acest marcaj vreunul dintre alte programe?
3. Chiar dacă marcajul temporal este oprit, ce ar putea însemna faptul că au același marcaj temporal?
4. Există vreun artefact care ar arăta că PSEXEC a fost rulat? Care este marcajul temporal și posibila semnificație criminalistică? (Sugestie: PSEXEC este un instrument Sysinternals care permite utilizatorului să ruleze de la distanță aplicații pe un sistem. Atunci când este executat, numele fișierului nu este psexec.exe, dar este aproape de acesta.) (Sugestie: adăugați în cronologie)