Volatility ile Ram Analizi

Komutlar

- `volatility_2.6_win64_standalone.exe -h` :Yardım komutu
- `volatility_2.6_win64_standalone.exe imageinfo -f cridex.vmem`
  - İmage işlemleri ve ilgili makine ile ilgili temel bilgileri gösterir.
- `volatility_2.6_win64_standalone.exe pslist —profile=WinXPS3×86 -f cridex.vmem`
  - Ram görüntüsü oluştuğunda makinede çalışan işlemleri gösterir.

➢ **Ofset :** İşlemin RAM'deki konumu, onaltılık
➢ **Ad :** Görev Yöneticisi'nde gösterildiği şekliyle işlem adı
➢ **PID :** İşlem kimliği
➢ **PPID :** Üst işlem kimliği - yani bu işlemi başlatan işlem. Yukarıdaki örnekte, "Sistem" işlemi 4. işlemdir ve **"smss.exe"** işleminin üst öğesidir.

- `volatility_2.6_win64_standalone.exe pstree —profile=WinXPS3×86 -f cridex.vmem`
  - Ram görüntüsü oluştuğunda çalışan işlemleri ağaç yapısında gösterir.
- `volatility_2.6_win64_standalone.exe —profile=WinXPS3×86 -f memdump.mem dlllist`
  - Ram görüntüsü oluştuğunda çalışan dll dosyalarını gösterir.
- `volatility_2.6_win64_standalone.exe netscan —profile=WinXPS3×86 -f memdump.mem`

    - Windows makinesindeki ağ bağlantılarını gösterir.
- `volatility_2.6_win64_standalone.exe connscan —profile=WinXPS3×86 -f cridex.vmem`
    - Windows makinesindeki tcp ağ bağlantılarını gösterir.
- `volatility_2.6_win64_standalone.exe sockets —profile=WinXPS3×86 -f cridex.vmem`
    - Açık soketleri listeler.
- `volatility_2.6_win64_standalone.exe psxview —profile=WinXPS3×86 -f cridex.vmem`
    - Bilgisayarda çalışırken kendini gizlemeye çalışan programları listeler.
- `volatility_2.6_win64_standalone.exe cmdlines —profile=WinXPS3×86 -f cridex.vmem`
    - Çalıştırılan son komutlara göz atmaya yarar.
- `volatility_2.6_win64_standalone.exe —profile=WinXPS3×86 -f cridex.vmem procdump -p <pid> -dump-dir <dizin>`
    - Process dökümlerini ayıklar.

🖋Ömer Faruk Baysal