Stredná priemyslená škola elektrotechnická
Komenského 44, 040 01 Košice

Forenzná analýza operačnej pamäte
Volatility setup

Autor: Marek Horňak
Trieda: 4.B
Školský rok: 2023/2024
Odbor: 2561M – Informačné a sieťové technológie

Obsah

0. Úvod

Otvorte si svoj virtuálny analytický počítač s Ubuntu. Na tomto počítači budete analyzovať všetky obrazy, ktoré tento učebný materiál obsahuje, a preto na ňom treba urobiť nejaké úpravy a nastavenia. Hlavnou úlohou je nainštalovať program Volatility3, v ktorom budete obrazy analyzovať a nastaviť ho tak, aby všetko fungovalo.

1. Inštalácia potrebných balíčkov

Skôr ako začneme inštalovať Volatility3, musíme nainštalovať niekoľko balíčkov potrebných pre inštaláciu a chod Volatility3. Presuňte sa do svojho domovského priečinka.

Najprv si aktualizujte systém a nainštalujte balíčky git, python3 a pip3:
- sudo apt update
- sudo apt install git python3 pip3

2. Inštalácia Volatility3

Volatility3 budete inštalovať z oficiálnej Github stránky Volatilityfoundation, pretože tam sa nachádzajú všetky priebežné vydania, ktoré obsahujú najnovšie opravy chýb a najnovšie funkcie.

Stiahnite si z Githubu Volatility3 repozitár, vytvorí sa vám nový priečinok s názvom volatility3:
- git clone https://github.com/volatilityfoundation/volatility3.git

Presuňte sa do priečinka volatility3 a spustite nasledujúci príkaz:
- pip3 install -r requirements.txt

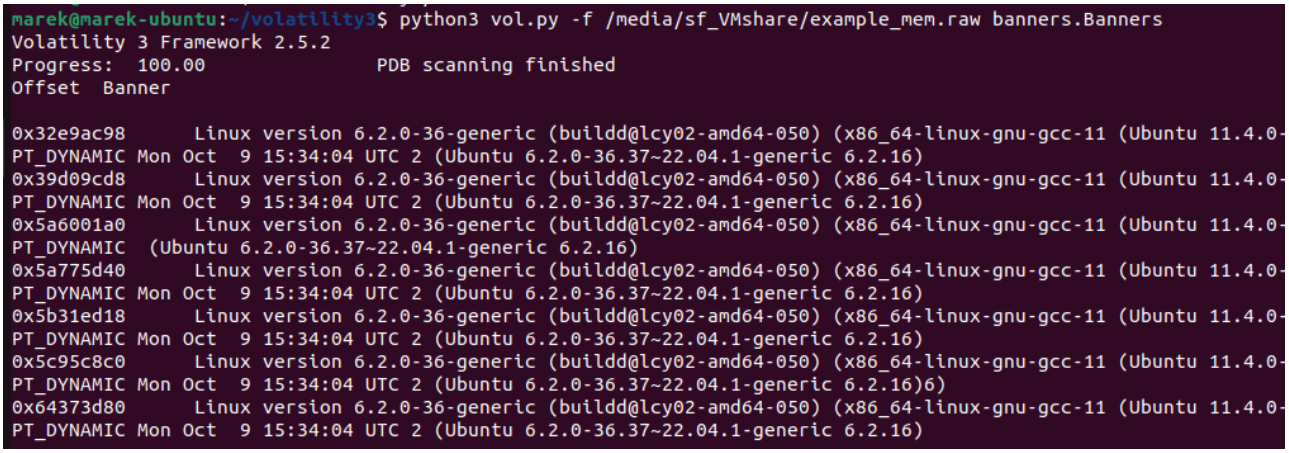
Teraz by Volatility3 malo byť nainštalované a plne funkčné.

3. Pridanie symbolovej tabuľky

Najdôležitejšou vecou, ktorú treba mať na pamäti je, že symbolová tabuľka musí byť vytvorená z kernelu, ktorý je zhodný s kernelom obrazu, ktorý chceme analyzovať. Ak nevieme, aký kernel používal počítač, z ktorého daný obraz pochádza, môžeme si kernelové informácie zobraziť pomocou Volatility3 pluginu *banners.Banners*. Na tento krok je vytvorený samostatný obraz operačnej pamäte, na ktorom tento plugin spustíte. Stiahnite si do svojho virtuálneho počítača s Ubuntu obraz example_mem.raw a presuňte si ho do priečinka s Volatility3, aby ste nemuseli zadávať absolútnu cestu k nemu a sputite tento príkaz:

python3 vol.py -f example_mem.raw banners.Banners

Výstup by mal vyzerať ako na Obrázku 1:



Obrázok 1: Výstup pluginu banners.Banners

Z tohto výstupu zistíme, že počítač, z ktorého pochádza tento obraz, používal kernel 6.2.0-36-generic. Symbolové tabuľky pre väčšinu kernelov nájdete na stránke https://isf-server.techanarchy.net/. Táto stránka je ISF server Volatility. Tento kernel sa tam ale nenachádza. Stiahnite si ho teda z Githubu, z repozitára, odkiaľ sú aj obrazy, ktoré budete analyzovať a premiestnite ho do priečinka ***volatility3/volatility3/symbols/linux***. Ak priečinok linux neexistuje, vytvorte ho.

Teraz musíme povedať Volatility3, že sme pridali novú symbolovú tabuľku. Spustite vo svojom domovskom priečinku príkaz ls -la a zobrazte si aj skryté priečinky a súbory. Okrem bežných priečinkov, priečinka s Volatility3 a poprípade iných súborov by sa tam mal nachádzať aj súbor s názvom .volatilityrc. Je to konfiguračný súbor pre Volatility3. Ak ho tam nemáte, vytvorte ho a zeditujte. Dopíšte tam tento text:

[symboltable]

linux = /path/to/volatility3/volatility3/symbols/linux/ubuntu-6.2.0-36-generic.json.xz

Teraz sme Volatility povedali, že sme pridali novú symbolovú tabuľku a uviedli sme, kde ju má hľadať. Po týchto nastaveniach vy už Volatility3 malo bez problémov fungovať a malo by byť schopné analyzovať obrazy s Linuxom.