Stredná priemyselná škola elektrotechnická
Komenského 44, 040 01 Košice

Forenzná analýza operačnej pamäte
Teória

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

Obsah

1. Forenzná analýza

1.1. Vo všeobecnosti

Vo všeobecnosti môžeme forenznú analýzu definovať ako každú činnosť zameranú na hĺbkovú analýzu, vyšetrovanie, ktorého cieľom je objektívne určiť a zdokumentovať vinníkov, dôvody, priebeh a dôsledky bezpečnostného incidentu, priestupku alebo trestného činu. Cieľom forenznej analýzy je zozbierať čo najviac dôkazov o tom, kto, kedy a ako niečo zavinil. Často súvisí so súdnym dokazovaním, najmä v trestných záležitostiach. Zahŕňa využitie širokého spektra vyšetrovacích technológií, postupov a metód. Výsledkom forenznej analýzy je znalecký alebo technický posudok alebo vyjadrenie majúce dôkaznú hodnotu v súdnom konaní. Vychádza z odboru Forenzika (Forenzná veda).

1.2. V kyberbezpečnosti

Z hľadiska kyberbezpečnosti je forenzná analýza prostriedkom získavania dôkazov k bezpečnostným incidentom. Väčšina kyberbezpečnostných incidentov sa odohráva na serveroch, počítačoch a iných zariadeniach. Tie sú mnohokrát cieľom útoku. Dá sa povedať, že počítač alebo server je pri vyšetrovaní takýchto incidentov niečo ako miesto činu. Existuje mnoho podkategórií digitálnej forenznej analýzy, no my sa špecifikujeme len na jeden – forenzná analýza obsahu operačnej pamäte. Budeme sa teda sústrediť len na operačnú pamäť. Je to pamäť závislá od napätia (volatilná), teda je schopná uchovávať dáta len po dobu, kým je pod napätím. Uchováva dáta, s ktorými počítač aktuálne pracuje. Ak dôjde k nejakému kyberútoku alebo bezpečnostnému incidentu, všetko, čo sa na danom počítači alebo serveri odohrá, ostane v jeho operačnej pamäti. Z nej sa vyhotoví obraz, ktorý sa následne analyzuje nástrojom na forenznú analýzu pamäte.

2. Nástroje na forenznú analýzu

V súčasnosti existuje niekoľko populárnych nástrojov na forenznú analýzu obsahu operačnej pamäte. Medzi najpoužívanejšie patria: Varc, Rekall (od Google security teamu) a Volatility.

2.1. Volatility

Volatility je v súčasnosti najrozšírenejší a najpokročilejší nástroj pre forenznú analýzu obsahu operačnej pamäte. Používajú ho aj profesionálni forenzní analytici pri vyšetrovaní bezpečnostných incidentov. Je napísaný v programovacom jazyku Python. Poskytuje širokú škálu možností analýzy. Je dostupný ako open-source pre Windows, Linux aj Mac a taktiež umožňuje analýzu obsahu operačnej pamäte všetkých týchto operačných systémov. Volatility2 je dostupná aj ako standalone executable verzia aj ako zdrojový kód v .zip archíve. Volatility3 je dostupná už len ako zdrojový kód.

3. Rozdiel medzi Volatility2 a 3

Posledné vydanie Volatility2 bolo v decembri 2016, zatiaľčo najnovšia verzia Volatility3 bola vydaná v apríli 2023. Volatility3 poskytuje oproti Volatility2 novšie a lepšie pluginy ako pre Windows, tak aj pre Linux. Avšak čo sa týka analýzy obsahu operačnej pamäte s Linuxom, Volatility3 neposkytuje až také efektívne pluginy na analýzu. Čo sa týka verzií Pythonu, Volatility2 podporuje Python2.6 a novšie, no nie Python3. To prináša určitú nevýhodu, pretože Python2 od 1. januára 2020 už nie je upravovaný a nie sú v ňom opravované ani bezpečnostné chyby a zraniteľnosti. Volatility3 vyžaduje Python 3.7 a vyššie.

3.1. Čo je lepšie?

Na základe informácií spomenutých vyššie sa nedá povedať, ktorá verzia Volatility je lepšia, pretože každá má svoje výhody aj nevýhody. V nasledujúcich praktických učebných materiáloch si ukážeme ako pracovať s oboma verziami, keďže Volatility2 je aj napriek svojej zastaranosti stále široko používaná. Napriek tomu, že sa Python2 a spolu s ním aj Volatility2 postupne vytrácajú, kvôli širokej škále dostupných pluginov je Volatility2 stále užitočným nástrojom pre forenznú analýzu a je užitočné používať ich kombináciu. Keďže ale Volatility2 dosť často nefunguje, pretože je zastaralé a jeho používanie je v dnešnej dobe plné komplikácií a problémov s funkčnosťou, na analýzu Linuxu budeme používať Volatility3.

4. Praktické úlohy

V ďalších častiach tohto učebného materiálu si vyskúšate sprevádzanú analýzu dvoch obrazov operačnej pamäte s Windowsom a dvoch s Linuxom. Budete postupovať podľa návodov v materiáloch a postupne si osvojíte prácu s Volatility3. Na konci každého materiálu bude úloha k tretiemu obrazu operačnej pamäte aj pre Windows aj pre Linux, ktorú budete na základe nadobudnutých skúseností riešiť sami.

4.1. Rozdiel medzi analýzou Windowsu a Linuxu

Kým analýza pamäte s Windowsom sa pri prechode z verzie 2 na verziu 3 takmer nezmenila, pri Linuxe sú podstatné rozdiely. Verzia 2 používala na zistenie verzie operačného systému tzv. linuxový profil, čiže .zip archív, ktorý obsahuje údaje na identifikáciu operačného systému. Bez toho Volatility2 nie je schopné analyzovať obraz operačnej pamäte s Linuxom. Volatility3 už nepoužíva Linuxové profily, ale tzv. symbolové tabuľky. V niektorých ohľadoch sú podobné s profilmi. Taktiež obsahujú informácie potrebné na rozpoznanie verzie operačného systému, no už to nie je klasický .zip súbor, ale komprimovaný .json súbor s príponou .json.xz. Čo sa týka Windowsu, vo Volatility2 bolo potrebné ešte pred samotnou analýzou oskenovať obraz operačnej pamäte pomocou pluginu *imageinfo* a vyhodnotiť verziu operačného systému. Tento profil bolo nutné následne špecifikovať zakaždým keď sme používali nejaký plugin. Volatility3 to celé o niečo zjednodušila, pretože netreba vôbec riešiť verziu operačného systému. Pri behu prvého pluginu sa automaticky oskenuje celý obraz operačnej pamäte (preto aj vykonanie prvého pluginu trvá dlhšie) a profil operačného systému uloží do svojej vyrovnávacej pamäte.