PV210 Bezpečnostní analýza síťového provozu

Analýza probíhajícího incidentu, ex-post analýza

Daniel Kouřil, Michal Procházka

10. 12. 2014

Shrnutí z minula

Analýza probíhajícího incidentu

Analýza artefaktů

Zadání domácího úkolu

Shrnutí

Shrnutí minulé přednášky

- Forenzní analýza odhaluje fakta o útoku a přispívá k rekonstrukci původního stavu
- Tři fáze forenzní analýzy
- Důležitost netechnických aspektů
  - výhoda týmové spolupráce

Příklady incidentů

- Změna webových stránek
  - Zadání pro FA: ?
- Úmyslně smazané soubory z disku
  - Zadání pro FA: ?
- Služba pod DDoS útokem
  - Zadání pro FA: ?
- Ransomware
  - Zadání pro FA: ?

Typy incidentů podle „živosti“

- Incident může stále probíhat, tj. aktivitu lze sledovat
- Aktivity útočníka skončily, jiné stopy nebudou
- K dispozici jsou pouze artefakty z incidentu

- V praxi se řeší kombinace všech tří oblastí

Fáze forenzní analýzy

0. Počáteční příprava

1. Sběr primárních dat
2. Vyhodnocení a analýza
3. Reporting

Počáteční příprava

- Zajištění kompetence a podpory
  - Nelze soupeřit s lokálními správci
  - Důvěryhodost CSIRTu
- Pravidla
  - Check list
  - Školení
- Technické nástroje
- Nástroje pro spolupráci
  - Bezpečné sdílení (velkých) dat
- Kontakty

Typické otázky

- Jak se útočník dostal do systému?
  - tj. identifikace *vstupního vektoru*
- Co útočník dělal po napadení systému?
- Které další systémy mohou být napadeny?

Detekce incidentu

- Upozornění, monitoring
- Co nachystat před/pro triage
- Formulace otázek, zadání pro řešení incidentu
  - obnovení služby vs. dohledání útočníka
  - lze měnit v průběhu vyšetřování

Incident triage

- Prvotní ohledání situace
  - všechny kroky mohou ničit důkazy!
- Systém neměníme
  - reinstalace ničí téměř vše a neodhalíme detaily
- Vhodné zacházení s artefakty již od počátku
- Komunikace

Analýza probíhajícího incidentu

- Útočník má otevřená spojení nebo se vrací do systému
- Větší příležitost pro zjištění informací
- Nebezpečí ponechání útočníka v systému
  - možnost odklonění do chráněného prostředí

Zásady pro sběr dat z živého systému

- Každý zásah ponechává stopy a mění zkoumaný systém
- Mezivýsledky posílat po síti, ukládat do ram disku nebo cut&paste z terminálu
- Audit prováděných příkazů
  - Automatizace

Sběr dat z probíhajícího incidentu

- Různé úrovně volatility
  - Síťová konfigurace
  - Paměť
  - Seznam procesů
  - Aktivní struktury OS
  - Systémy souborů

Využití dat z paměti RAM

- Různé paměťové oblasti
  - celá RAM, paměť procesu, swap
- Malware často běží pouze v paměti
  - po skončení procesu nelze zrekonstruovat text
- V paměti jsou cenné informace, které nelze nalézt jinde
  - Historie příkazů, šifrovací klíče - TrueCrypt
  - Specializované nástroje, vyhledávání řetezců

Získání dat z paměti

- Obraz celé paměti RAM
  - HW podpora FireWire, Thunderbolt
  - Pomocí SW - podpora OS
  - Složitější, může ukázat i skryté procesy, apod.
- Výpis vybraných procesů
  - Pomocí nástrojů OS
  - Obsahuje pouze data konkrétního procesu, snadnější pro analýzu
- Přístup do virtuálních strojů

Analýza struktur OS

- Meziprocesová komunikace (IPC)
- Porovnávání seznamu aktivních procesů, síťových spojení
  - systémový příkaz vs. “čistá” kopie (nemusí fungovat pro rootkity!)
- Otevřené popisovače souborů, smazané soubory
- Síťová spojení, tabulky

Ex-post Analýza

- Zkoumání artefaktů
  - pořízených z online analýzy
  - předaných jako zadání
- Analýza disků apod. zařízení
- Analýza souborů

Analýza disku

- Rozložení, partitions, skrytá místa
  - TrueCrypt
- Analýza systémů souborů na partitions
  - včetně metadat (mount, journal)
- Vždy práce s kopií
  - Důvěryhodné pořízení kopie disku/partition

Analýza systému souborů

- Smazané soubory – file carving
- Skrytá data
- Metadata
- Obsah souborů

Časová razítka

- Jedna z nejpřínosnějších informací
  - mtime (modification time) – Změna obsahu.
  - atime (access time) – Čas posledního přístupu.
  - ctime (change time) – Čas změny metadat.

  - dtime (deletion time) – čas smazání.
  - btime (creation time) – čas vytvoření.
- Časová razítka usnadňují výměnu dat, není potřeba žádat o obraz

Časová razítka – příklad

```
Tue Aug 16 2011 14:03:15 .a. r-xr-xr-x root root /usr/bin/w
Tue Aug 16 2011 14:03:28 .a. rwxr-xr-x root root /usr/bin/curl
Tue Aug 16 2011 14:03:36 .a. rwxr-xr-x root root /usr/bin/bzip2
Tue Aug 16 2011 14:04:41 .a. rwxr-xr-x root root /usr/bin/shred
Tue Aug 16 2011 14:06:26 .a. rw-r-r- root root /usr/include/crypt.h
Tue Aug 16 2011 14:07:25 m.. rwxrwxr-x x_lenix x_lenix /var/tmp/...
Tue Aug 16 2011 14:08:01 m.c rw-r-r- root root /var/tmp/.../openssh-5.2p1.tar.bz2 (deleted-rea
```

Courtesy to Leif Nixon

Obsah souborů

- Historie a dočasné soubory programů
  - bash_history, viminfo, lesshst, ...
- Analýza logů
  - Lokální logy mohou být zničené

- Pohybujeme se v řádech GB, TB
- Souborové systémy, záznamová média
- Problematické při hledání smazaných souborů, je nutné projít celé záznamové médium
- Nutné filtrovat a indexovat
- Nejenom soubory, ale i síťová data apod.

Analýza podezřelých souborů

- Identifikace škodlivého, podezřelého chování
  - Spustitelné soubory se škodlivým kódem
  - Dokumenty zneužívající zranitelnosti (MS Office, PDF, obrázky)
- Statická analýza
  - Vyhledání řetězců
  - Reverzní inženýrství
- Dynamická analýza
  - Řízené spouštění
  - Využití sandboxů

Zadání úkolu

Viz interaktivní osnova v ISu:
`https://is.muni.cz/auth/el/1433/podzim2014/PV210/index.qwarp`
Úkol – hledání útoku v PCAPu a logu.

Shrnutí

- Pozor na poškození stop sběru dat
- Nástroje a expertíza pro sběr dat
- Různá místa, kde hledat důkazy
  - Systém souborů – časová razítka
  - Paměť
  - Logy
  - Struktury OS
- Cílené a zdokumentované shromáždění stop a jejich vyhodnocení