Hledáme nezvané hosty

Pavel Kácha
CESNET, z. s. p. o.

Pomoc!

- Neznámé soubory na podivných místech
- Server komunikuje kdy či s kým nemá
- Neobvyklé procesy
- Nečekaný/neplánovaný restart důležitých démonů
- Otevřené porty
- Křičí Nagios
- Dupe po mně bezpečák

…

Čeho chci dosáhnout?

- Nahodit zpátky službu?
- Nahodit zpátky bezpečnou službu?
- Kolik mám času?
- Jak je služba kritická?
- Jaké mám možnosti přístupu?
- Jaké mám možnosti omezit dopad a ne službu?

Ukládání informací

- Stopař si může pošlapat stopy
  - atime
  - přepis smazaných souborů
  - relokace sektorů na disku, wear-leveling u SSD

  Je vhodné dělat si obrazy (paměti, disku, terminálu).
- Jak?
  - copy-paste z terminálu, ukládání ze screenu/tmuxu
  - rourování výstupů přes ssh na jiný stroj
  - externí USB disk
  - mount vzdáleného disku (ale pozor na cryptolocker :))

Kde začít: časová osa

- ```
  find / -xdev -printf \
  '%TY-%Tm-%TdT%TH:%TM:%TS %10i modify %M %u %g %p\n'\
  '%AY-%Am-%AdT%AH:%AM:%AS %10i access %M %u %g %p\n'\
  '%CY-%Cm-%CdT%CH:%CM:%CS %10i change %M %u %g %p\n'\
  | sort | awk '{$2=""; print}'
  ```

```
2017-10-06T12:50:50  access drwx------ root root /tmp/aptitude-root.5405:3MLP1m
2017-10-06T12:50:50  change drwx------ root root /tmp/aptitude-root.5405:3MLP1m
2017-10-06T12:50:50  modify drwx------ root root /tmp/aptitude-root.5405:3MLP1m
2017-10-06T12:51:43  access -rw-r--r-- root root /etc/ld.so.conf
2017-10-06T12:51:44  change drwxr-xr-x root root /etc
2017-10-06T12:51:44  modify drwxr-xr-x root root /etc
2017-10-06T13:24:25  change drwxrwxrwt root root /tmp
2017-10-06T13:24:25  modify drwxrwxrwt root root /tmp
```

(Ničí atime – je třeba provést jako první, nebo na image.)

- ```
  fls -r -m / /dev/XXX > fs.filelist
  mactime -b fs.filelist
  ```

(Obchází kernel, získá i smazané soubory.)

Image

- HW write blocker nemá každý
  - `blockdev –setro`
  - `hdparm –r1`
  - `hdparm –D`
  - `mount –o remount,ro`

  Kopie parcely/disku
  - `dd if=/dev/XXX of=XXX.dd bs=512k`
  - `ddrescue /dev/XXX XXX.dd`

Stav živého systému

- ps aux, netstat --all --program, lsof
- procesy s podivnými názvy (mezery, tečky, lomítka)
  - neobvyklé podprocesy
  - systémové/kernelové procesy s vysokým PID
- gcore -o PID.dump PID
  - `strings -a PID.dump`
  - `strace -p PID -o processname`
    - `grep "open" processname; …`
  - /proc/PID/exe, cwd, cmdline

Systém souborů

- mount -o loop,ro
  - `grep –r pattern /mountpoint`
  - `find /mountpoint –iname shpattern`
- smazaná data, carving
  - `grep --only-matching --byte-offset --text pattern image.bin`

    (výkon grepů může zlepšit --mmap, LANG=C)
  - `strings image.bin | grep – bez vazby na soubor`
  - SleuthKit, foremost, sfdumper, Scalpel, TestDisk, PhotoRec, extundelete, …

Časové známky

- mtime
  - modifikace dat souboru či obsahu adresáře
    (často zachovávají kopírovací utility)
- ctime
  - změna atributů (jméno, vlastník, práva, link)
    (často zde vydrží čas vytvoření)
    (na rozdíl od ostatních jde explicitně změnit jen zásahem na device)
- atime
  - poslední přístup (čtení, spuštění) souboru
    (s noatime pešek, s relatime jen pokud se změnilo i něco jiného)

(Zvažte **ne**používání noatime/relatime alespoň na systémových parcelách, jsou-li oddělené od datových s častým přístupem.)

Integrita

- `debsums`
- `rpm –verify`
- porovnání se zálohami
  - ale pozor, kompromitace může být už i tam

(Jsme-li prozíraví, máme Tripwire, Aide, Samhain.)

Anomálie

- Low-hanging fruit
  - chkrootkit, rkhunter, fslint
- /etc – podezřelé konfigurace a pohyby
  - init.d, apm, udev, UPower, NetworkManager, (ana)cron, hibernate, pmode, ifplugd, ifup, profile.d...
- soubory a jejich pohyb
  - `mount | grep tmp` (sem patří i /dev)
  - adresáře vlastněné démony (/var/www, …)
  - tečkové soubory v nedomovských adresářích

Anomálie II

- práva
  - soubory bez vlastníka, bez skupiny
  - uživatelská práva v etc, bin, sbin, usr, lib, root
  - neobvyklá elevovaná práva (s-bit)
  - spustitelné soubory v neobvyklých adresářích
    (znamená i nespustitelné, ale s shebangem)
  - soubory s neuživatelským vlastníkem v uživatelských adresářích
- časové známky
  - příliš nové, příliš staré, „mimo“ okolí

Logy

- /var/log/{w,b}tmp, /var/run/utmp, /var/log/lastlog
  - `last -f ?tmp`
  - `lastlog`
- /var/log/syslog, daemon.log, secure, …
- apache a ostatní internetoví démoni
- logy specifických (webových) aplikací
- .bash_history
  - neobjevila se .bash_history i jinde než v /home/*/?

Vyřešeno?

- Jaké jsou souvislosti?
- Nemohl se útočník dostat i jinam?
- Nemohl využít jako přeskok?
- Co mohu udělat, aby se to znovu nestalo?
- Co mohu monitorovat, abych na to přišel dříve?

Jak se poučím?

Odkazy

- The Sleuth Kit
  - http://www.sleuthkit.org/
- SFDumper
  - http://sfdumper.sourceforge.net/index.html#c
- Foremost
  - http://foremost.sourceforge.net/
- TestDisk, PhotoRec
  - http://www.cgsecurity.org/
- Scalpel
  - http://www.digitalforensicssolutions.com/Scalpel/

Odkazy

- Tripwire
  - https://sourceforge.net/projects/tripwire/
- Aide
  - http://aide.sourceforge.net/
- Samhain
  - http://www.la-samhna.de/samhain/index.html

Paměť

- Volatility Framework
  - https://www.volatilesystems.com/default/volatility
- Volatilitux (ARM, PAE)
  - http://code.google.com/p/volatilitux/

Pozvánky

Zájemci o práci na projektech kolem bezpečnosti: **https://csirt.cesnet.cz/**

Ne 10:00 / 105 - Ondřej Caletka - IPv6 tunely pomocí OpenVPN

Ne 11:00 / 107 - Tomáš Čejka - Monitorování sítě pomocí flow

Stánek CESNET – dema:

- L0 SDN a železniční doprava
- Flexibilní zpracování paketů rychlostí 100 Gb/s

Stánek Bastlíři SH:

- indoor LoRaWAN gateway (s podporou CESNET)

Měsíc kybernetické bezpečnosti (http://mkb.cesnet.cz)

- Hacking soutěž **„The Catch“** (8. 10. – 5. 11. 2017)
- Seminář **Security Fest** (31. 10. 2017, Masarykova kolej ČVUT)