Analiza skupljenih podataka

Analiza podataka je dijelom znanost, a dijelom umjetnost. Znanstveni dio analize nalaže dobru pripremu, detaljno ispitivanje klijenta te poznavanje alata kojima će se provoditi istraga. Umjetnički dio znači da istražitelj treba imati "osjećaj" za istragu - što je bitno i gdje to naći.

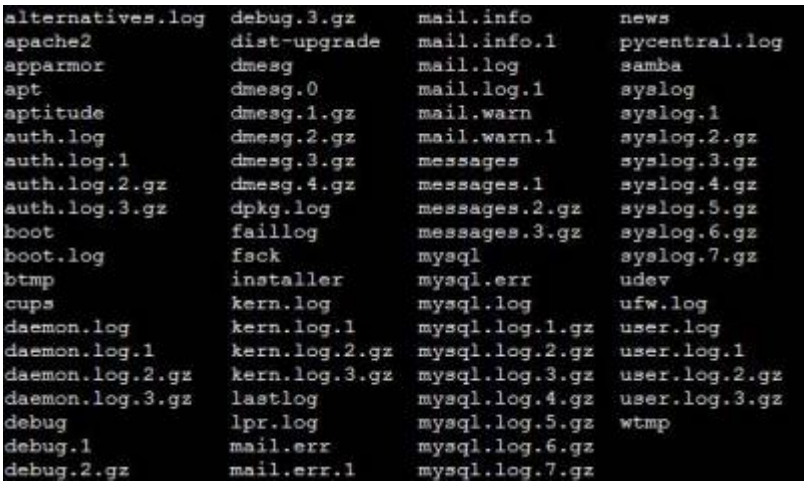
Procjena situacije

Prije početka analize, istražitelj treba biti upoznat sa sljedećim podacima kako bi bio siguran da potpuno razumije incident te da ga može riješiti efikasno i efektivno.

1. **Vremenski slijed događaja**
   Ako je moguće, pokušati staviti incident u određeni vremenski okvir.
2. **Topografiju mreže**
3. **Tok podataka**
4. **Sigurnosne aplikacije**
   Što klijent ima u mreži i da li se drže zapisničke datoteke.
5. **Stanje napadnutih sustava**
6. **Normalno stanje poslovanja**
   Što je "normalno" za klijenta? Način na koji dodjeljuju imena, procesi koji se standardno vrte, kakav im je svakodnevni promet, koji sustavi normalno komuniciraju i još mnogo mogućih varijabli koje će omogućiti istražitelju da dobro obavi posao.

Analiza zapisničkih datoteka

Sve zapisničke datoteke (eng. *log files*) na Linux sustavu se pohranjuju u `/var/log` direktoriju. Tu su i datoteke sustava i dodatnih programskih aplikacija instaliranih na računalu.



alternatives.log	debug.3.gz	mail.info	news
apache2	dist-upgrade	mail.info.1	pycentral.log
apparmor	dmesg	mail.log	samba
apt	dmesg.0	mail.log.1	syslog
aptitude	dmesg.1.gz	mail.warn	syslog.1
auth.log	dmesg.2.gz	mail.warn.1	syslog.2.gz
auth.log.1	dmesg.3.gz	messages	syslog.3.gz
auth.log.2.gz	dmesg.4.gz	messages.1	syslog.4.gz
auth.log.3.gz	dpkg.log	messages.2.gz	syslog.5.gz
boot	faillog	messages.3.gz	syslog.6.gz
boot.log	fsck	mysql	syslog.7.gz
btmp	installer	mysql.err	udev
cups	kern.log	mysql.log	ufw.log
daemon.log	kern.log.1	mysql.log.1.gz	user.log
daemon.log.1	kern.log.2.gz	mysql.log.2.gz	user.log.1
daemon.log.2.gz	kern.log.3.gz	mysql.log.3.gz	user.log.2.gz
daemon.log.3.gz	lastlog	mysql.log.4.gz	user.log.3.gz
debug	lpr.log	mysql.log.5.gz	wtmp
debug.1	mail.err	mysql.log.6.gz	
debug.2.gz	mail.err.1	mysql.log.7.gz	

Na slici ispisa `/var/log` direktorija desno se mogu primijetiti datoteke s brojevima na kraju. To su tzv. "rotirani arhivi". Trenutna verzija datoteke, npr. `dmesg`, nema nikakvih dodataka na ime. Prethodna inačica se zove `dmesg.0`, ona prije nje `dmesg.1.gz` i tako dalje. Najstarija datoteka ima najveći broj. To omogućuje alat `logrotate` koji, obično jednom dnevno (detalji u `/etc/cron.daily`), "zarotira" datoteke, odnosno otvori novu, a ostalima poveća indeks i po potrebi ih komprimira. Podaci o ovom postupku se mogu vidjeti i promijeniti u `/etc/logrotate.conf` datoteci.

Prilikom pregledavanja datoteka, korisne su naredbe:

Naredba	**Opis**
`zgrep <parametar_pretrage>`	Pretražuje komprimirane datoteke za određenim parametrom (riječ, izraz).
`tail -<broj> <filename>`, `tail -f /var/log/messages`	Ispisuje posljednjih `<broj>` redaka datoteke. Slučaj s opcijom `-f` ispisuje sadržaj zapisničke datoteke dok skuplja podatke u stvarnom vremenu.
`more <filename>`	Ispisuje sadržaj datoteke na zaslon stranicu po stranicu uz napomenu o tome koliki postotak datoteke preostaje: `–More–(x%)`. Tipka `b` vraća ispis unatrag jednu stranicu. Opcija `/<parametar_pretrage>` omogućuje pretraživanje datoteke - u slučaju višestrukog pojavljivanja traženog pojma, tipkom `n` se preskače na sljedeći, a tipkom `p` na prethodni. Tipkom `q` se izlazi iz ispisa.
`less <filename>`	Slično kao i `more`, ali brže i pruža više kontrole korisniku.
`grep <pattern> <filename>`	Traži dani pojam u danoj datoteci.

Prilikom analize uzetih podataka, dobra praksa je imati popis ključnih riječi koje bi se mogle pojaviti u dokazima. Taj popis će biti specifičan za svaku pretragu i mijenjati će se kako istražitelj bude dolazio do novih spoznaja.

Popis ključnih riječi za početak po preporuci autora knjige Unix and Linux Forensics Analysis

Aktivnosti korisnika

Shell History

Linux pohranjuje aktivnosti korisnika u *shell history* datoteci lociranoj u direktoriju `/home/<user>`. Većina Linux distribucija pohranjuje posljednjih 500 linija upisanih u komandnu liniju. No tu su pohranjene samo naredbe koje je korisnik utipkao, ne i odziv sustava na naredbe. Ovi podaci se trebaju koristiti u kombinaciji s ostalim podacima iz istrage kako bi se dobila smislena slika. Pregled datoteke `.bash_history` se može dobiti naredbom `$ cat .bash_history` ili jednostavno `$ history`.

Neke od najpopularnijih ljuski su:

- **BASH** - `.bash_history`
- **C-Shell** - `history.csh`
- **Korn** - `.sh_history`
- **POSIX** - `.sh_history`
- **Z-Shell** - `.history`

Ulogirani korisnici

Naredbama `$ who` i `$ w` se dobivaju podaci o trenutno ulogiranim

```
ikukina@marta:~$ who
ikukina  pts/0        2011-04-23 15:45 (cpe-109-60-83-17.zg3.cable.xnet.hr)
ikukina@marta:~$ w
 23:02:02 up 13 days,  6:32,  1 user,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
ikukina  pts/0    cpe-109-60-83-17 15:45    0.00s  0.77s  0.00s w
ikukina@marta:~$
```

korisnicima.
Polja u ispisu naredbe `$ w` su:

- **User**
  Ime korisnika.
- **TTY Teletype**
  `tty#` znači da je korisnik ulogiran u lokalnu konzolu. `pts#` i `ttyp#` znači da je ulogiran preko mreže. Na slici je korisnik dakle ulogiran preko mreže.
- **From**
  Lokacija ulogiranog korisnika. U slučaju lokalnog korisnika će biti ":0" ili ":0.0". U slučaju udaljenog korisnika će biti njegova IP adresa.
- **Idle**
  Koliko je vremena prošlo od posljednje aktivnosti korisnika.
- **JCPU**
  Ukupno vrijeme koliko su procesi korisnika koristili procesor od posljednjeg logina.
- **PCPU**
  Procesorsko vrijeme trenutnog procesa (onog u polju **What**)
- **What**
  Proces kojeg korisnik trenutno vrti.

Mrežne veze

```
netstat -an
```

```
netstat -rn
```

Pokrenuti procesi

```
ps aux
```

```
top
```

Open File Handlers

`lsof` - *List Open Files* pokazuje koje datoteke su (bile) otvorene i kojim procesima. Dodatne opcije su navedene u tablici:

`lsof -i -U`	Popisuje sve datoteke otvorenih Internet, x.25 (HP-UX) i Unix domena.
`lsof -i 4 -a -p 1234`	Popisuje sve otvorene IPv4 mrežne datoteke koje koristi proces s ID brojem 1234.
`lsof -i 6`	Popisuje sve otvorene IPv6 mrežne datoteke.
`lsof -i @wonderland.cc.purdue.edu:513-515`	Popisuje sve datoteke koje koriste bilo koji protokol na portovima 513, 514, 515 na računalu wonderland.cc.purdue.edu

`lsof -i @mace`	Popisuje sve datoteke koje koriste bilo koji protokol na bilo kojem portu računala mace.cc.purdue.edu (cc.purdue.edu je standardna domena).
`lsof -p 456,123,789 -u 1234,abe`	Popisuje sve datoteke za login ime “abe” ili korisnički ID 1234 ili proces 456 ili 123 ili 789
`lsof /dev/hd4`	Popisuje sve otvorene datoteke na uređaju `/dev/hd4`.
`lsof /u/abe/foo`	Traži proces koji koristi datoteku `/u/abe/foo`.
`+L1`	Označava sve odbačene (eng. *unlinked*) datoteke ili koje su označene za brisanje.