

Rajasploit Defensive Monitoring Report

Client: alan **Creator:** anit **Owner:** alan

Timestamp: 2025-10-02T06:16:43.317467Z

Executive Summary

- Network Capture: (file too large to include inline: run6_network_summary.txt, 56753901 bytes)
- Port & Service Scan (nmap): # Nmap 7.95 scan initiated Thu Oct 2 02:11:27 2025 as: /usr/lib/nmap/nmap --privileged -sV -T4 -oN results/defensive_monitoring/run6/run6_nmap.txt 10.239.252.221
- Process Snapshot: === ps_aux.txt ===
- File Integrity (sha256): (no file integrity results)
- Logs: === journal_recent.txt ===
- IDS Check: (no IDS detected or no IDS output)
- System Resources: === disk_usage.txt ===

Network Capture

(file too large to include inline: run6_network_summary.txt, 56753901 bytes)

Port & Service Scan (nmap)

```
# Nmap 7.95 scan initiated Thu Oct 2 02:11:27 2025 as: /usr/lib/nmap/nmap --privileged -sV -T4 -oN
results/defensive_monitoring/run6/run6_nmap.txt 10.239.252.221
Nmap scan report for 10.239.252.221
Host is up (0.0000070s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.65
Service Info: Host: 127.0.1.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Oct 2 02:11:50 2025 -- 1 IP address (1 host up) scanned in 22.95 seconds
```

Process Snapshot

```
==== ps_aux.txt ====
(file too large to include inline: ps_aux.txt, 23558 bytes)

==== top.txt ====
top - 02:12:49 up 1:16, 1 user, load average: 0.00, 0.03, 0.05
Tasks: 228 total, 3 running, 225 sleeping, 0 stopped, 0 zombie
%Cpu(s): 0.0 us, 1.1 sy, 0.0 ni, 98.9 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
MiB Mem : 8438.6 total, 5124.5 free, 1735.8 used, 1932.9 buff/cache
MiB Swap: 953.7 total, 953.7 free, 0.0 used. 6702.7 avail Mem

 PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 4151 kali      20   0 10420  5276  3228 R  9.1  0.1  0:00.01 top
    1 root      20   0 23976 14280 10404 S  0.0  0.2  0:01.82 systemd
    2 root      20   0      0    0      0 S  0.0  0.0  0:00.05 kthreadd
    3 root      20   0      0    0      0 S  0.0  0.0  0:00.00 pool_wo+
    4 root      0 -20     0    0      0 I  0.0  0.0  0:00.00 kworker+
    5 root      0 -20     0    0      0 I  0.0  0.0  0:00.00 kworker+
    6 root      0 -20     0    0      0 I  0.0  0.0  0:00.00 kworker+
    7 root      0 -20     0    0      0 T  0.0  0.0  0:00.00 kworker+
```

File Integrity (sha256)

(no file integrity results)

Logs

```
==== journal_recent.txt ====
(file too large to include inline: journal_recent.txt, 37628 bytes)
```

IDS Check

(no IDS detected or no IDS output)

System Resources

```
==== disk_usage.txt ====
Filesystem      Size  Used Avail Use% Mounted on
udev            4.1G   0    4.1G  0% /dev
tmpfs           844M  1.1M  843M  1% /run
/dev/sda1        79G   38G   38G  50% /
tmpfs           4.2G  3.1M  4.2G  1% /dev/shm
tmpfs           5.0M   0    5.0M  0% /run/lock
tmpfs           1.0M   0    1.0M  0% /run/credentials/systemd-journald.service
tmpfs           4.2G  8.0K  4.2G  1% /tmp
kali-linux       448G  297G  152G  67% /media/sf_kali-linux
tmpfs           1.0M   0    1.0M  0% /run/credentials/getty@tty1.service
tmpfs           844M  128K  844M  1% /run/user/1000

==== memory.txt ====
              total        used         free      shared  buff/cache   available
Mem:       8.2Gi     1.7Gi      5.0Gi      68Mi     1.9Gi     6.6Gi
Swap:      953Mi        0B     953Mi
```