Appendix F – Local Tests

LOCAL TESTS

Lab:

```
JP-OLD (SERVER + AGENT) - 2013
Sony Vaio E11 (SVE1113M1EW)
Processor: 1.75GHz Dual Core
Memory: 8GB
WLAN

RPI4 (AGENT) - Q2 2019
Raspberry Pi 4 Model B Rev 1.2
Processor: 1.5GHz Quad Core
Memory: 2GB
Ethernet / WLAN

pi@raspberrypi:~ $ cat /proc/cpuinfo
(...)
Hardware        : BCM2835
Revision        : b03112
Serial          : 10000000dbb5bbc1
Model           : Raspberry Pi 4 Model B Rev 1.2

RPI1 (AGENT) - Q3 2012
Raspberry Pi Model B Rev 1
Processor: 700MHz Single Core
Memory: 256MB
Ethernet

pi@raspberrypi:~ $ cat /proc/cpuinfo
(...)
Hardware        : BCM2835
Revision        : 0003
Serial          : 000000007ab1b3b3
Model           : Raspberry Pi Model B Rev 1

SIAAS (VM) (SERVER + AGENT + CLI)
Processor: 1.8GHz Quad Core
```

```
Memory: 8GB
Ethernet / WLAN

Set up November 2022.
```

Nmap commands run by python3-nmap:

```
OS detection:

#TCP
nmap.nmap_os_detection(target, args="-%s -sV -Pn --host-timeout %s" % (ipv, timeout))
/usr/bin/nmap -v -oX - -O -4 -sV -Pn --host-timeout 600 sapo.pt

#UDP
nmap.scan_top_ports(scanned_ip, args="-%s -sU --top-ports 10 -Pn --host-timeout %s" % (ipv, timeout))
/usr/bin/nmap -v -oX - --top-ports 10 -4 -sU --top-ports 10 -Pn --host-timeout 600 sapo.pt

Vulnerability scan:

nmap.nmap_version_detection(target, args="-%s -p%s:%s --script %s -Pn --host-timeout %s" % (ipv, prot_flag, port, nmap_script, timeout))
/usr/bin/nmap -v -oX - -sV -4 -pT:443 --script vuln -Pn --host-timeout 600 sapo.pt
/usr/bin/nmap -v -oX - -sV -4 -pU:445 --script vuln -Pn --host-timeout 600 sapo.pt

# -O: Enable OS detection
# --top-ports: most famous ports for this service (UDP is very slow when scanning ports, so we just scan the 10 most famous ones)
# -sV: Probe open ports to determine service/version info
# -sU: UDP scan
# -Pn: Treat all hosts as online -- skip host discovery
```

Reliability tests:

```
Uptime agent @ RPI4:

pi@raspberrypi:~ $ journalctl -u siaas-agent | grep -Ei 'Started|Stopped'
(...)
Jan 26 15:42:29 raspberrypi systemd[1]: Started SIAAS Agent.
Feb 10 14:33:14 raspberrypi systemd[1]: Stopped SIAAS Agent. # 15 days
(...)
Feb 26 16:17:33 raspberrypi systemd[1]: Started SIAAS Agent.
Mar 15 14:22:31 raspberrypi systemd[1]: Stopped SIAAS Agent. # 17 days

Uptime server @ JP-OLD:

jpseara@JP-OLD:~$ journalctl -u siaas-server | grep -Ei 'Started|Stopped'
```

```
(...)
jan 24 19:30:56 JP-OLD systemd[1]: Started SIAAS Server.
fev 03 14:04:16 JP-OLD systemd[1]: Stopped SIAAS Server. # 10 days
(...)
fev 24 02:24:30 JP-OLD systemd[1]: Started SIAAS Server.
mar 10 00:05:17 JP-OLD systemd[1]: Stopped SIAAS Server. # 14 days

RPI4 and RPI1 customized configs for stress test:

enable_internal_api: true
log_level: debug
manual_hosts: google.com,sapo.pt
neighborhood_loop_interval_sec: 5
nmap_scripts: vuln,vulscan,discovery
platform_loop_interval_sec: 5
portscanner_loop_interval_sec: 5

RPI1 modified configs for stress test (check MULTIPROC/MULTITHREAD ANALYSIS):

enable_internal_api: true
log_level: debug
manual_hosts: google.com,sapo.pt
neighborhood_loop_interval_sec: 5
nmap_scripts: vuln
platform_loop_interval_sec: 5
portscanner_loop_interval_sec: 5
portscanner_max_parallel_workers: 1

JP-OLD customized configs for stress test:

disable_wifi_auto_discovery: true # problematic Sony Vaio WLAN card...
log_level: debug
manual_hosts: google.com,sapo.pt
neighborhood_loop_interval_sec: 5
nmap_scripts: vuln,vulscan,discovery
platform_loop_interval_sec: 5
portscanner_loop_interval_sec: 5
```

Multiproc/Multithread analysis:

```
Scripts: vuln,vulscan,discovery

$ cat /var/log/siaas-agent/siaas-agent.log | grep portscanner.py | grep -Ei 'running|sleeping'

SIAAS (VM)

4 cores:
```

```
(target                                                                                             -
num_scanned_ports/num_valid_scripts/total_num_vulnerabilities/total_num_exploits/time_taken_sec_with
_multiprocs | time_taken_sec_with_multithreads)

192.4.5.5 - 10/0/0/0/320 | 321
192.168.122.1 - 3/1/21/0/75 | 72
192.168.123.3 - 6/1/105/16/414 | 499
2a00:1450:4003:80f::500e - 0 | 1
aisense-qas.aitecservdevenv.local - 6/1/105/16/205 | 287
cgsa-dev.aitecservdevenv.local - 6/1/105/16/305 | 507
focal62 - 6/1/105/16/281 | 431
google.com - 12/1/0/0/828 | 834
sapo.pt - 12/1/0/0/269 | 277

# Multiproc

2023-03-26 20:28:49.610 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 20:42:38.092 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 14 min with multiprocs

2023-03-26 23:37:25.729 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 23:53:00.522 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 16 min with multiprocs

2023-03-27 00:30:38.661 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-27 00:44:21.775 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 14 min with multiprocs

# Multithread

2023-03-26 20:53:22.372 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 21:07:16.836 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 14 min with multithreads

2023-03-26 23:55:42.821 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-27 00:12:06.655 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 17 min with multithreads

2023-03-27 00:13:06.681 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-27 00:26:54.418 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 13 min with multithreads

1 core:
```

```
(target -
num_scanned_ports/num_valid_scripts/total_num_vulnerabilities/total_num_exploits/time_taken_sec_with
_multiprocs | time_taken_sec_with_multithreads)

192.4.5.5 - 10/0/0/0/319 | 321
192.168.122.1 - 3/1/21/0/76 | 77
192.168.123.3 - 6/1/105/16/291 | 288
2a00:1450:4003:80f::500e - 0 | 0
aisense-qas.aitecservdevenv.local - 6/1/105/16/191 | 219
cgsa-dev.aitecservdevenv.local - 6/1/105/16/241 | 390
focal62 - 6/1/105/16/258 | 250
google.com - 12/1/0/0/837 | 822
sapo.pt - 12/1/0/0/403 | 333

# Multiproc

2023-03-26 21:16:35.895 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 22:00:15.958 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 44 min with multiprocs

2023-03-26 22:25:07.402 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 23:07:10.023 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 42 min with multiprocs

# Multithread

2023-03-26 22:07:57.615 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 22:21:40.491 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 14 min with multithreads

2023-03-26 23:16:51.694 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 23:30:33.042 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 60 seconds
before next loop ...
^ 14 min with multithreads

***

JP-OLD (2 cores):

# Multiproc

2023-03-26 20:26:37.423 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 21:11:35.644 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds
before next loop ...
^ 45 min
```

```
2023-03-26 22:49:22.629 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 23:39:44.293 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 50 min

2023-03-27 09:09:23.603 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-27 09:52:51.857 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 43 min

# Multithread

2023-03-27 14:14:54.371 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-27 14:49:05.507 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 35 min

2023-03-27 23:39:46.666 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-28 00:12:47.279 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 33 min

2023-03-29 21:28:20.767 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-29 22:06:56.988 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 38 min

***

RPI4 (4 cores):

# Multiproc

2023-03-26 21:07:50.915 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 21:41:47.588 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 34 min

2023-03-26 22:52:43.420 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-26 23:32:21.365 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 40 min

2023-03-27 09:11:46.586 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-27 09:45:00.430 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 34 min
```

```
# Multithread

2023-03-27 15:44:48.612 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-27 16:18:19.489 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds
before next loop ...
^ 34 min

2023-03-27 23:45:25.392 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-28 00:23:52.301 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds
before next loop ...
^ 38 min

2023-03-29 22:03:27.798 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-29 22:39:06.373 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds
before next loop ...
^ 36 min

***

RPI1 (1 core):

# Multiproc

2023-03-26 18:53:47.131 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
(Still stuck on discovery script at 10:23 next day (observed in two consecutive days))

# Multithread (auto=5)

2023-03-27 10:44:05.352 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
Mar 27 10:58:00 raspberrypi kernel: [251173.162310] Out of memory: Killed process 12525 (nmap) total-
vm:49200kB, anon-rss:24476kB, file-rss:0kB, shmem-rss:0kB, UID:0 pgtables:56kB oom_score_adj:0

# Multithread (3)

2023-03-28 02:07:05.455 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
Mar 28 02:30:10 raspberrypi kernel: [307127.505793] Out of memory: Killed process 3296 (nmap) total-
vm:49272kB, anon-rss:20656kB, file-rss:0kB, shmem-rss:0kB, UID:0 pgtables:56kB oom_score_adj:0

# Multithread (1)

2023-03-28 02:43:58.575 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
(Still stuck on discovery script at 11:15 next day)

# Multithread (3, just vuln+vulscan)

2023-03-28 11:19:17.734 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
Mar 28 12:28:56 raspberrypi kernel: [343049.420355] Out of memory: Killed process 21494 (nmap) total-
vm:93968kB, anon-rss:38344kB, file-rss:0kB, shmem-rss:0kB, UID:0 pgtables:98kB oom_score_adj:0
```

```
# Multithread (3, just vuln)

2023-03-28 12:42:47.256 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-28 14:10:23.094 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 1 hr 28 min

2023-03-28 14:10:28.110 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-28 15:32:47.064 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 1 hr 22 min

(Works, but under very intense load (Munin fails, SSH fails):
top - 14:55:47 up 4 days,  1:44,  1 user,  load average: 10.47, 7.24, 7.68)

# Multithread (2, just vuln)

2023-03-28 17:00:39.340 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-28 17:56:55.046 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 56 min

2023-03-28 17:57:00.054 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-28 18:53:34.851 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 56 min

(Less load but still high:
top - 17:22:22 up 4 days,  4:11,  1 user,  load average: 5.36, 4.20, 4.50)

# Multithread (1, just vuln)

2023-03-28 19:55:54.036 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-28 21:27:22.010 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 1 hr 32 min

2023-03-29 14:25:23.225 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-29 15:47:50.464 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 1 hr 22 min

2023-03-29 21:16:40.642 DEBUG siaas_portscanner.py [Process-3|MainThread] Loop running ...
2023-03-29 22:31:19.090 DEBUG siaas_portscanner.py [Process-3|MainThread] Sleeping for 5 seconds before next loop ...
^ 1 hr 15 min

(Even less load (much more acceptable now):
top - 21:34:52 up 4 days,  8:23,  1 user,  load average: 2.08, 2.14, 2.03)
```

```
***

Peak memory usage observations (per script category):

(at RPI4)

$ watch sudo ps -C "nmap" -o vsz,rss,cmd

106548 98220 /usr/bin/nmap -v -oX - google.com -sV -4 -pT:443 --script vuln -Pn --host-timeout 600
^ 98MB

141912 133492 /usr/bin/nmap -v -oX - google.com -sV -4 -pT:443 --script discovery -Pn --host-timeout
600
^ 133MB

135132 127136 /usr/bin/nmap -v -oX - google.com -sV -4 -pT:443 --script vulscan -Pn --host-timeout 600
^ 127MB
```

Accuracy tests:

```
ubuntu@target:~$ uname -a
Linux target 5.4.0-131-generic #147-Ubuntu SMP Fri Oct 14 17:07:22 UTC 2022 x86_64 x86_64 x86_64
GNU/Linux

ubuntu@target:~$ sudo dpkg -l | grep -Eiw 'apache2|openssh'
ii  apache2                           2.4.41-4ubuntu3.12                                    amd64
Apache HTTP Server
ii  openssh-server                    1:8.2p1-4ubuntu0.3                                    amd64
secure shell (SSH) server, for secure access from remote machines

https://ubuntu.com/security/cves?q=&package=openssh
https://ubuntu.com/security/CVE-2021-28041 # Fixed in 20.04, no issue in 22.04

https://ubuntu.com/security/cves?q=&package=apache2
https://ubuntu.com/security/CVE-2020-9490 # Fixed in 20.04, no issue in 22.04

ubuntu@siaas:~$ siaas-cli vuln-report -h 192.168.122.51 -t vuln_only | grep -Ei 'CVE-2021-28041|CVE-
2020-9490'
'CVE-2021-28041': ['4.6', 'https://vulners.com/cve/CVE-2021-28041'],
'CVE-2020-9490': ['5.0', 'https://vulners.com/cve/CVE-2020-9490'],

^ OK!

ubuntu@siaas:~$ siaas-cli vuln-report -h 192.168.122.51 -t all | grep -i apache
'product': 'Apache httpd 2.4.41 (Ubuntu)',
'http-server-header': {'raw_lines': ['Apache/2.4.41 (Ubuntu)']},
^ OK!

ubuntu@siaas:~$ siaas-cli vuln-report -h 192.168.122.51 -t all | grep -i openssh
'product': 'OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)',

^ OK!

ubuntu@siaas:~$ siaas-cli vuln-report -h 192.168.122.51 -t all | grep -i linux
{'0924aa8b-6dc9-4fec-9716-d1601fc8b6c6': {'portscanner': {'192.168.122.51': {'system_info':
{'hostname': 'target.local', 'mac_address': '52:54:00:59:A5:04', 'nic_vendor': 'QEMU virtual NIC',
'os_name': 'Linux 3.2 - 4.9', 'os_family': 'Linux', 'os_gen': '4.X', 'os_vendor': 'Linux', 'os_type':
'general purpose', 'scanned_ip': '192.168.122.51'},

^ Linux OK! Kernel info NOK...

ubuntu@target:~$ sudo apt update
ubuntu@target:~$ sudo apt-get dist-upgrade -y
ubuntu@target:~$ sudo do-release-upgrade

ubuntu@target:~$ uname -a
Linux target 5.15.0-40-generic #43-Ubuntu SMP Wed Jun 15 12:54:21 UTC 2022 x86_64 x86_64 x86_64
GNU/Linux

ubuntu@target:~$ sudo dpkg -l | grep -Eiw 'apache2|openssh'
ii  apache2                              2.4.52-1ubuntu4.4                       amd64        Apache
HTTP Server
ii  openssh-server                       1:8.9p1-3ubuntu0.1                      amd64        secure
shell (SSH) server, for secure access from remote machines

ubuntu@siaas:~$ siaas-cli vuln-report -h 192.168.122.51 -t vuln_only | grep -Ei 'CVE-2021-28041|CVE-
2020-9490'
(No output.)

^ OK!

ubuntu@siaas:~$ siaas-cli vuln-report -h 192.168.122.51 -t all | grep -i apache
'product': 'Apache httpd 2.4.52 (Ubuntu)',
'http-server-header': {'raw_lines': ['Apache/2.4.52 (Ubuntu)']},

^ OK!

ubuntu@siaas:~$ siaas-cli vuln-report -h 192.168.122.51 -t all | grep -i openssh
'product': 'OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)'

^ OK!

ubuntu@siaas:/opt/siaas-cli$ siaas-cli vuln-report -h 192.168.122.51 -t all | grep -i linux
{'0924aa8b-6dc9-4fec-9716-d1601fc8b6c6': {'portscanner': {'192.168.122.51': {'system_info':
{'hostname': 'target.local', 'mac_address': '52:54:00:59:A5:04', 'nic_vendor': 'QEMU virtual NIC',
'os_name': 'Linux 3.2 - 4.9', 'os_family': 'Linux', 'os_gen': '4.X', 'os_vendor': 'Linux', 'os_type':
'general purpose', 'scanned_ip': '192.168.122.51'},

^ Linux OK! Kernel info NOK...
```

Security tests:

```
CLI (SIAAS (VM)) -> SERVER (JP-OLD)

-L: follow redirects
-X: method (GET)
--location-trusted: use the same authentication when redirected
--user: user/password auth
--insecure: don't check the CA validity
--cacert: local CA bundle to verify the endpoint against
-v: verbose (confirm redirection to https)

ubuntu@siaas:/opt/siaas-cli$ curl -LX GET https://192.168.1.69/api --user siaas:siaas
curl: (60) SSL certificate problem: self signed certificate
More details here: https://curl.haxx.se/docs/sslcerts.html
curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.

ubuntu@siaas:/opt/siaas-cli$ curl -LX GET https://192.168.1.69/api --user siaas:siaas --insecure
{"output":{"name":"Intelligent System for Automation of Security Audits
(SIAAS)","module":"Server","api":"v1","author":"João Pedro Seara","supervisor":"Carlos
Serrão"},"status":"success","total_entries":5,"time":"2023-04-04T18:43:25Z"}

ubuntu@siaas:/opt/siaas-cli$ curl -LX GET https://192.168.1.69/api --user siaas:siaas --cacert
./ssl/jp-old.crt
curl: (60) SSL: no alternative certificate subject name matches target host name '192.168.1.69'
More details here: https://curl.haxx.se/docs/sslcerts.html
curl failed to verify the legitimacy of the server and therefore could not
establish a secure connection to it. To learn more about this situation and
how to fix it, please visit the web page mentioned above.

ubuntu@siaas:/opt/siaas-cli$ curl -LX GET https://jp-old/api --user baduser:badpassword --cacert
./ssl/jp-old.crt
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>401 Unauthorized</title>
</head><body>
<h1>Unauthorized</h1>
<p>This server could not verify that you
are authorized to access the document
requested.  Either you supplied the wrong
credentials (e.g., bad password), or your
```

```
browser doesn't understand how to supply
the credentials required.</p>
<hr>
<address>Apache/2.4.41 (Ubuntu) Server at jp-old Port 443</address>
</body></html>

ubuntu@siaas:/opt/siaas-cli$ curl -L -X GET https://jp-old/api --user siaas:siaas --cacert ./ssl/jp-
old.crt
{"output":{"name":"Intelligent System for Automation of Security Audits
(SIAAS)","module":"Server","api":"v1","author":"João Pedro Seara","supervisor":"Carlos
Serrão"},"status":"success","total_entries":5,"time":"2023-04-04T18:45:37Z"}

ubuntu@siaas:/opt/siaas-cli$ curl -L -X GET http://jp-old/api --user siaas:siaas --location-trusted -
-cacert ./ssl/jp-old.crt -v
Note: Unnecessary use of -X or --request, GET is already inferred.
*   Trying 192.168.1.69:80...
* TCP_NODELAY set
* Connected to jp-old (192.168.1.69) port 80 (#0)
* Server auth using Basic with user 'siaas'
> GET /api HTTP/1.1
> Host: jp-old
> Authorization: Basic c2lhYXM6c2lhYXM=
> User-Agent: curl/7.68.0
> Accept: */*
>
* Mark bundle as not supporting multiuse
< HTTP/1.1 301 Moved Permanently
< Date: Tue, 04 Apr 2023 18:45:45 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Location: https://jp-old/api
< Content-Length: 298
< Content-Type: text/html; charset=iso-8859-1
<
* Ignoring the response-body
* Connection #0 to host jp-old left intact
* Issue another request to this URL: 'https://jp-old/api'
*   Trying 192.168.1.69:443...
* TCP_NODELAY set
* Connected to jp-old (192.168.1.69) port 443 (#1)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: ./ssl/jp-old.crt
  CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
```

```
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: C=PT; ST=Lisbon; L=Lisbon; O=ISCTE; OU=METI; CN=jp-old
*  start date: Oct 30 23:52:16 2022 GMT
*  expire date: Oct 27 23:52:16 2032 GMT
*  subjectAltName: host "jp-old" matched cert's "jp-old"
*  issuer: C=PT; ST=Lisbon; L=Lisbon; O=ISCTE; OU=METI; CN=jp-old
*  SSL certificate verify ok.
* Server auth using Basic with user 'siaas'
> GET /api HTTP/1.1
> Host: jp-old
> Authorization: Basic c2lhYXM6c2lhYXM=
> User-Agent: curl/7.68.0
> Accept: */*
>
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Tue, 04 Apr 2023 18:45:45 GMT
< Server: waitress
< Content-Length: 238
< Content-Type: application/json
<
{"output":{"name":"Intelligent System for Automation of Security Audits
(SIAAS)","module":"Server","api":"v1","author":"João Pedro Seara","supervisor":"Carlos
Serrão"},"status":"success","total_entries":5,"time":"2023-04-04T18:45:45Z"}
* Connection #1 to host jp-old left intact
```

Max BSON size limitation:

```
2023-03-14 04:33:04.090 ERROR siaas_aux.py [MainProcess|waitress-3] Can't insert data in the DB server:
BSON document too large (71625954 bytes) - the connected server supports BSON document sizes up to
16793598 bytes.

Ports 21, 22, 80, 111, 2049, 8080

- FTP
- NFS
- HTTP
- SSH

discovery,vuln,vulscan:
```

```
~ 140.8 KB (~119 hosts)

ubuntu@siaas:/opt/siaas-agent/var$ du -b
140842  .
ubuntu@siaas:/opt/siaas-agent/var$ ls -lrta
total 160
-rw-r--r--  1 root   root      577 Mar 15 02:24 config_local.db
-rw-r--r--  1 root   root       36 Mar 15 02:24 uid
drwxr-xr-x  2 root   root     4096 Mar 15 02:24 .
drwxrwxr-x 11 ubuntu ubuntu   4096 Mar 15 02:25 ..
-rw-r--r--  1 root   root   133767 Mar 15 02:36 portscanner.db
-rw-r--r--  1 root   root      577 Mar 15 02:42 config.db
-rw-r--r--  1 root   root      265 Mar 15 02:43 neighborhood.db
-rw-r--r--  1 root   root     1524 Mar 15 02:44 platform.db

discovery,vuln:

~ 75 KB

ubuntu@siaas:/opt/siaas-agent/var$ du -b
75039   . (~223 hosts)
ubuntu@siaas:/opt/siaas-agent/var$ ls -lrta
total 96
drwxrwxr-x 11 ubuntu ubuntu  4096 Mar 15 01:55 ..
-rw-r--r--  1 root   root     569 Mar 15 02:10 config_local.db
-rw-r--r--  1 root   root      36 Mar 15 02:10 uid
drwxr-xr-x  2 root   root    4096 Mar 15 02:10 .
-rw-r--r--  1 root   root   67898 Mar 15 02:21 portscanner.db
-rw-r--r--  1 root   root     569 Mar 15 02:22 config.db
-rw-r--r--  1 root   root     265 Mar 15 02:23 neighborhood.db
-rw-r--r--  1 root   root    1606 Mar 15 02:23 platform.db

vuln:

~ 26.2 KB

ubuntu@siaas:/opt/siaas-agent/var$ du -b
26234   . (~640 hosts)
ubuntu@siaas:/opt/siaas-agent/var$ ls -lrta
total 48
drwxrwxr-x 11 ubuntu ubuntu  4096 Mar 15 01:55 ..
-rw-r--r--  1 root   root     559 Mar 15 02:02 config_local.db
-rw-r--r--  1 root   root      36 Mar 15 02:02 uid
drwxr-xr-x  2 root   root    4096 Mar 15 02:02 .
-rw-r--r--  1 root   root   19198 Mar 15 02:07 portscanner.db
-rw-r--r--  1 root   root     265 Mar 15 02:08 neighborhood.db
-rw-r--r--  1 root   root     559 Mar 15 02:08 config.db
-rw-r--r--  1 root   root    1521 Mar 15 02:09 platform.db
```

```
vulscan: 65803 (~65.8K) - 46.7%
discovery: 48805 (~48.8K) - 34.7%
vuln: 26234 (~26.2K) - 18.6%
```

Technical Note F1 - Raw notes from the local tests