SUTMS Supplementary Descriptions and Evaluation Results

Asif Siddiqui, Bhaskar P. Rimal, Martin Reisslein, and Deepak GC, and Yong Wang

March 2024

I. Purpose

This supplementary document accompanies the article [1] by providing additional descriptions and evaluation results that could not be accommodated in [1].

II. SUTMS Configuration

A. Suricata Configuration

Listing 1. Suricata Installation Log Showing 37075 enabled rules

```
asif@SUTMS:~$ sudo suricata-update
26/3/2024 -- 22:10:45 - <Info> -- Found Suricata version 6.0.4 at /usr/bin/suricata.
26/3/2024 -- 22:10:45 - <Info> -- Backing up current rules.
26/3/2024 -- 22:10:66 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 48388; enabled: 37075; added: 0; removed 0; modified: 0
```

Listing 2. Suricata rule generation based on relevant protocols

```
root@SUTMS:/var/lib/suricata/rules# suricata-update
26/3/2024 -- 23:29:06 - <Info> -- Loading /etc/suricata/disable.conf.
26/3/2024 -- 23:29:06 - <Info> -- Loading /etc/suricata/enable.conf.
26/3/2024 -- 23:29:08 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total:48388; enabled: 5565; added: 0; removed 0; modified: 0
```

B. Suricata IDS Management

The Suricata rule:

```
alert http $HOME_NET any ->
$EXTERNAL_NET 80 (msg:"TROJAN";
flow:established,to_server;
flowbits:isset; content:"trojan"
; pcre:"/trojan .*[0-9]3,/i";
classtype:trojan-activity; sid:200;
rev:2;)
```

has the following key components [2]: alert → action is set to alert, protocol → http, destination port → 80, direction → Home Net (private) networks to External (internet), State → Established connections

(flowbits:isset), pcre → regex search set to trojan .*[0-9]3,/i, malicious content → trojan, sid → unique identifier.

We conducted an initial verification of the correct operation of the Suricate IDS engine as follows. We created a test signature `suricata_test_rule.rules` and generated traffic from a remote system to simulate an attacker. The test signature basically detects the SSH traffic in the network over port 22 to ensure that the IDS engine detection is working as expected. Logs were observed in `fast.log` file for matching signature description `\This is SUTMS test signature"` as shown below.

```
root@SUTMS:/var/log/suricata# suricata
-S suricata_test_rule.rules -i wlan0
root@SUTMS:/var/log/suricata# more
fast.log
08/10/2022-21:53:01.707410 [**]
[1:2008124:0] This is SUTMS test
signature [**] [Classification:(null)]
[Priority:3] TCP 192.168.200.155:56314
→ 192.168.200.156:22
```

C. iptables Firewall Management

The actual firewall rule enforcement of SUMTS can be verified via the command line as illustrated in Fig. 1.

```
root@sutms:/etc/iptables# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     udp  --  192.168.200.0/24     anywhere             udp dpt:domain
ACCEPT     all  --  192.168.200.156      anywhere
ACCEPT     udp  --  192.168.0.0/16       8.8.8.8              udp dpt:domain
ACCEPT     udp  --  10.0.0.0/8           8.8.8.8              udp dpt:domain
ACCEPT     udp  --  172.16.0.0/12        8.8.8.8              udp dpt:domain
ACCEPT     tcp  --  192.168.0.0/16       anywhere             tcp multiport dports http,https
ACCEPT     tcp  --  10.0.0.0/8           anywhere             tcp multiport dports http,https
ACCEPT     tcp  --  172.16.0.0/12        anywhere             tcp multiport dports http,https
ACCEPT     tcp  --  192.168.0.0/16       anywhere             tcp multiport dports ssh,webmin
ACCEPT     tcp  --  10.0.0.0/8           anywhere             tcp multiport dports ssh,webmin
ACCEPT     tcp  --  172.16.0.0/12        anywhere             tcp multiport dports ssh,webmin
ACCEPT     tcp  --  192.168.0.0/16       anywhere             tcp dpt:3000
ACCEPT     tcp  --  10.0.0.0/8           anywhere             tcp dpt:3000
ACCEPT     tcp  --  172.16.0.0/12        anywhere             tcp dpt:3000
DROP       all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination

Chain LOG_AND_DROP (0 references)
target     prot opt source               destination
root@sutms:/etc/iptables#
```

Fig. 1. Output of SUTMS Iptable rules.

D. IoC Feed Management

SUTMS ingests feeds via an API call provided by ANAMOLI [3], as shown below.

```
curl -kv -o 'ioc_updates' -H 'Content-
Type:application/json' 'https://192.168.
200.160:8080/api/v1/intelligence' -d'
{"token":"797d09613cbf91bd6d48aad
b8bc1a66e", "query":"confidence>50
AND severity=very-high AND
date_last>-1d", "type":"csv",
"size":100 }'
```

To secure the HTTPS transactions, the token can be retrieved by using the curl command in our evaluation network. Specifically, `IP = 192.168.200.160` is the IP address of the server, and it requires a username/password for retrieving the data. SSL handshake will be completed, followed by key exchange and certificate validation. The token acquired, i.e., `364d56025538c3dc193676cde8dd8ae9` will be used in the original API call.

Downloaded IoC feeds can be accessed by using Linux commands, such as `more` or `cat` as indicated below

```
root@SUTMS:/home/asif/Downloads# ls
ioc_updates
root@SUTMS:/home/asif/# more ioc_updates
indicator,classification,confidence,itype,type,
severity,source,feed _site_netloc,
feed_name,detail,date_last,actor,
campaign,id,tlp 194.104.136.155,private,75,
mal_ip,ip,very-high,limo.anomali.com:TAXII
feeds:Emerging Threats C&C Server,limo.
anomali.com,Emerging Threats C&C
Server,"mal_ip:
-194.104.136.155,malicious-activity",2022-06
-22 04:02:48 PM,indicator--8dc28cca-34bf-
4904-951e-eda05551551a,
TLP:AMBER 154.56.0.108,private
,92,mal_ip,ip,very-high,
limo.anomali.com: TAXII feeds:Emerging
Threats C&C Server,limo.anomali.com,
Emerging
Threats C&C Server,
"mal_ip:-154.56.0.108,malicious
-activity", 2022-06-22 04:02:40
PM,indicator
--c73e43c4-9f2a-4282-97fe-a4da3847a832,
TLP:AMBER
```

The `ioc_updates` fetched two malicious IP addresses that met the criteria, i.e., `194.104.136.155` and `154.56.0.108`.

III. SUTMS Evaluation

A. Phase II Accuracy Evaluation

$$\begin{aligned} TP &= HTTP + HTTPS + FTP + FTP\_data + SSH && (1)\\ &= 1194 + 2278 + 25 + 13 + 196 && (2)\\ &= 3706. && (3)\end{aligned}$$

$$FP = \text{Miscategorized email events} = 2199 \quad (4)$$

FN is 0 for both phase I and II.

$$\begin{aligned} TN &= Total - (TP + FP + FN) && (5)\\ &= 229341 - (3706 + 2199 + 0) && (6)\\ &= 223436. && (7)\end{aligned}$$

$$\begin{aligned} Accuracy &= \frac{TP + TN}{TP + TN + FP + FN} && (8)\\ &= \frac{3706 + 223436}{3706 + 223436 + 2199 + 0} && (9)\\ &= 0.9904 \approx 99\%. && (10)\end{aligned}$$

B. Resource Utilization

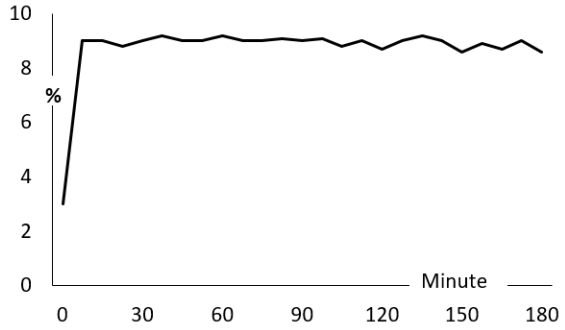

Fig. 2. SUTMS CPU usage - firewall & NTOP engine.

References

[1] A. Siddiqui, B. P. Rimal, M. Reisslein, D. Gc, and Y. Wang, "SUTMS: Designing a unified threat management system for home networks," *Under Review*, 2024.

[2] (2022) Suricata 6.0.4 documentation. [Online]. Available: https://suricata.readthedocs.io/en/suricata-6.0.4/configuration/suricata-yaml.html?highlight=thread

[3] (2012) Anomali Threat Feeds. [Online]. Available: https://www.anomali.com/resources/what-are-stix-taxii

TABLE I
PHASE I AND II - CPU USAGE OBSERVED IN 3HR.

Time-min	**CPU(%)-Phase I**	**CPU(%)-Phase II**
10	22	20.5
20	23	20.5
30	22	20.9
40	23	20.4
50	23	20.01
60	25	21.3
70	23	20.1
80	23.1	20.7
90	24	20.1
100	23	20.6
110	23	20.7
120	24	20.3
130	26	20.3
140	23	20.1
150	23	20.3
160	22	20.02
170	22	20.01
180	21.5	20.4

TABLE II
PHASE I AND II - MEMORY USAGE OBSERVED IN 3HR.

Time-min	**Mem(GB)-Phase I**	**Mem(GB)-Phase II**
10	2.34	0.98
20	2.31	0.99
30	2.2	1.01
40	2.1	1
50	2.3	0.85
60	1.9	0.99
70	1.8	0.86
80	2	0.93
90	1.8	0.85
100	2	0.9
110	2.2	0.98
120	2	0.94
130	1.8	0.93
140	2	0.92
150	2	0.86
160	2	0.9
170	1.99	0.8
180	1.87	0.89

TABLE III
LOAD IN PHASE I AND II - LOAD OBSERVED IN 3HR.

Time-min	**Load-Phase I**	**Load-Phase II**
10	2.5	1.1
20	2.52	1.1
30	2.52	1.2
40	2.2	1.23
50	2.1	1.39
60	2.3	1.5
70	2.3	1.2
80	2.5	1.2
90	1.8	1.5
100	2.1	1.2
110	1.8	1.39
120	1.8	1.4
130	2	1.2
140	2.2	1.2
150	2.1	1.3
160	1.3	1.2
170	1.2	1.2
180	1.4	1.25

TABLE IV
DISK I/O IN PHASE I AND II - DISK USAGE OBSERVED IN 3HR.

Time-min	**Disk(I/O)-Phase I**	**Disk(I/O)-Phase II**
10	0.08	0.01
20	0.06	0.01
30	0.01	0.01
40	0.09	0.01
50	0.01	0.02
60	6	0.01
70	5.9	0.03
80	5	0.01
90	0.08	0.01
100	0.01	0.03
110	0.01	0.04
120	0.03	0.01
130	0.03	0.01
140	0.05	6
150	0.01	5.9
160	5.1	0.003
170	4.9	0.01
180	0.01	0.01

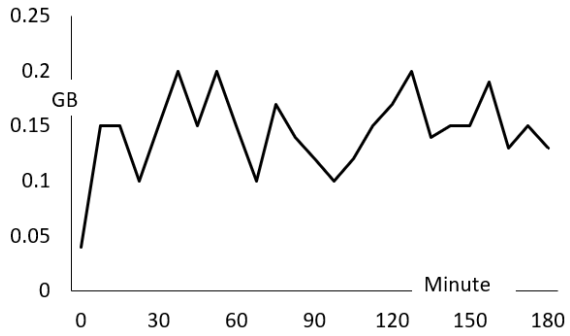

Fig. 3. SUTMS Memory usage - firewall & NTOP Engine.

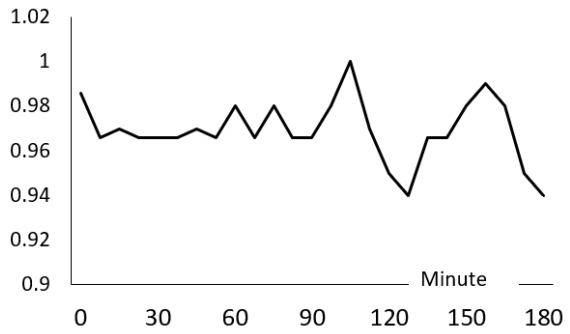

Fig. 4. SUTMS system load - firewall & NTOP Engine.