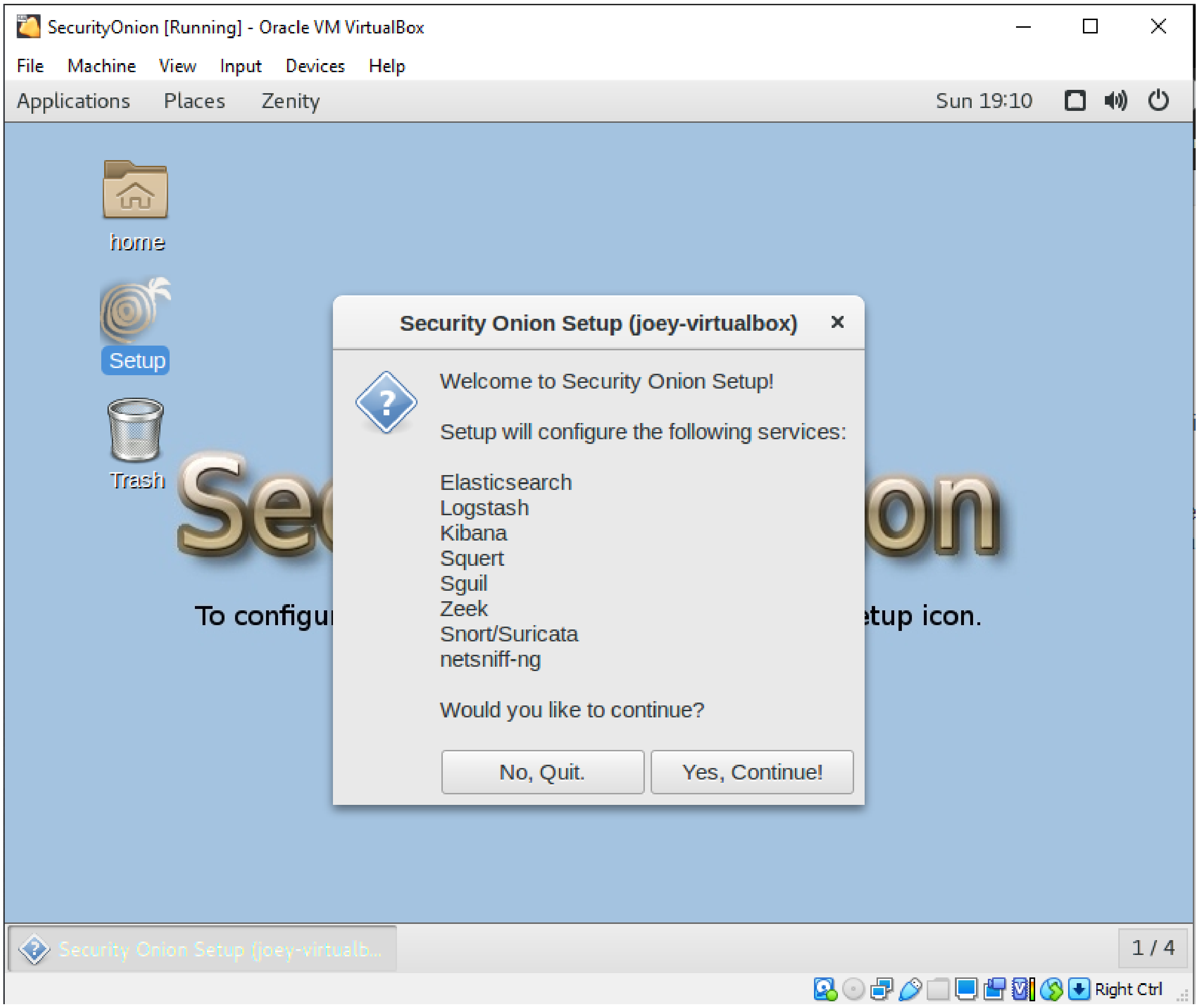
- **Testing of fundamental Sgiul operations**

1. Download ISO image (16.04.6.5 ISO image built on 2020/03/25)

   https://download.securityonion.net/file/Security-Onion-16/securityonion-16.04.6.5.iso

2. Install it in Virtual BOX.

3. Run Setup script on desktop and follow the prompts to configure and start the Sguil.



SecurityOnion [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Zenity
Sun 19:10
home
Setup
Trash
Sec on
To configu tup icon.

Security Onion Setup (joey-virtualbox)

Welcome to Security Onion Setup!

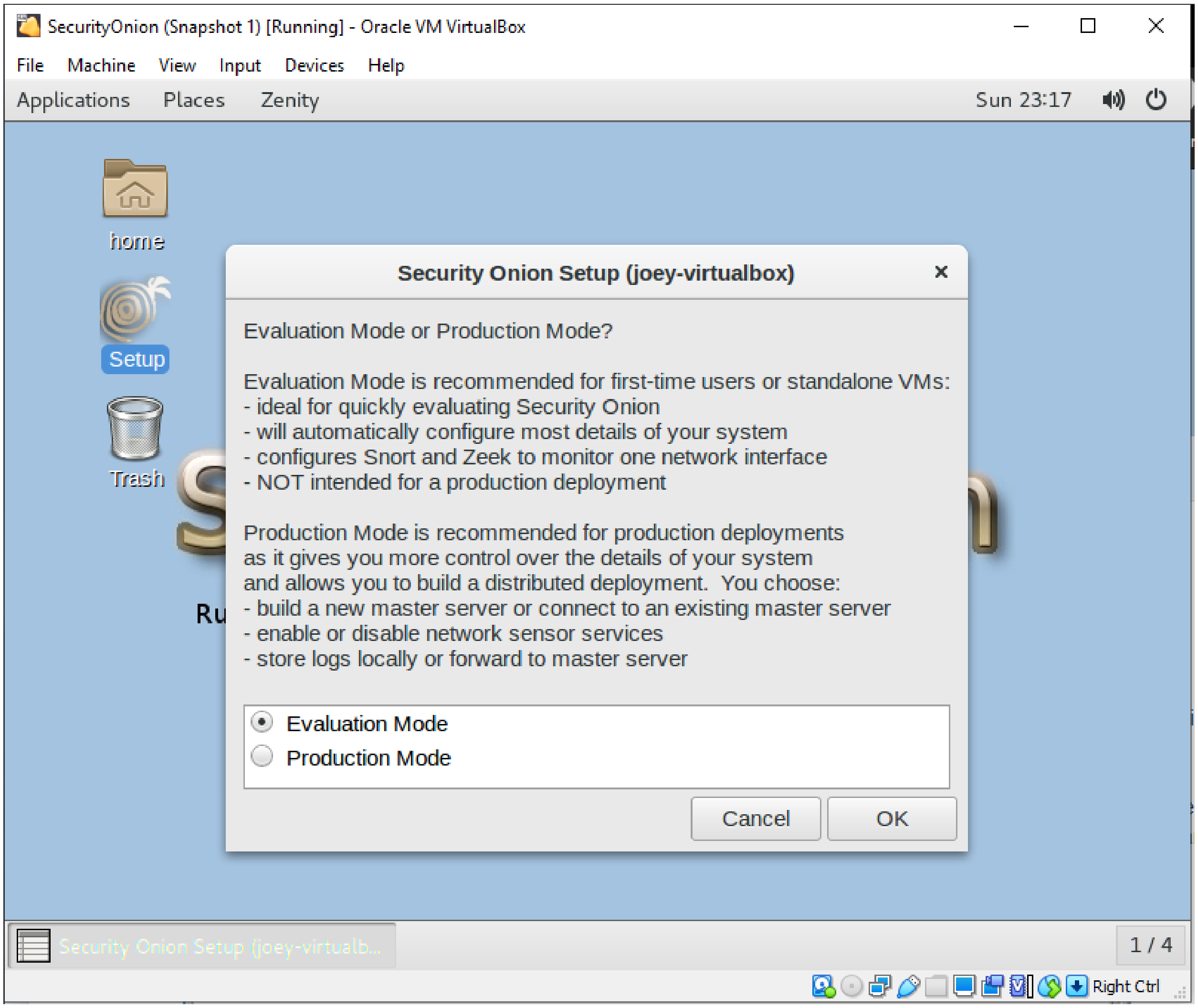
Setup will configure the following services:

Elasticsearch
Logstash
Kibana
Squert
Sguil
Zeek
Snort/Suricata
netsniff-ng

Would you like to continue?

No, Quit.
Yes, Continue!
Security Onion Setup (joey-virtualb...
1 / 4
Right Ctrl

4. After reboot, run setup again to continue, then select evaluation mode.


SecurityOnion (Snapshot 1) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
Applications
Places
Zenity
Sun 23:17
home
Setup
Trash
Security Onion Setup (joey-virtualb...
1 / 4
Right Ctrl

Security Onion Setup (joey-virtualbox)

Evaluation Mode or Production Mode?

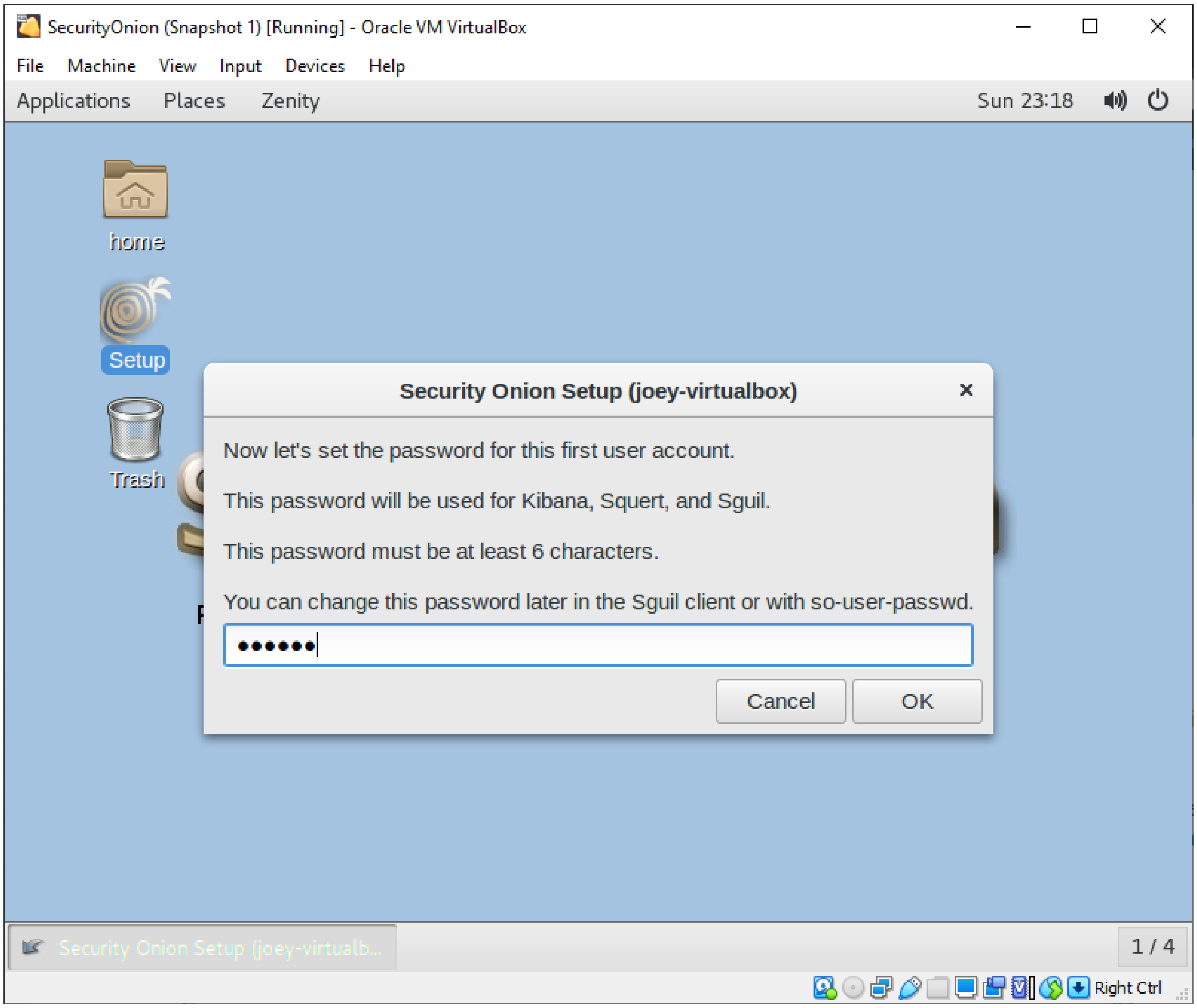
Evaluation Mode is recommended for first-time users or standalone VMs:
- ideal for quickly evaluating Security Onion
- will automatically configure most details of your system
- configures Snort and Zeek to monitor one network interface
- NOT intended for a production deployment

Production Mode is recommended for production deployments as it gives you more control over the details of your system and allows you to build a distributed deployment. You choose:
- build a new master server or connect to an existing master server
- enable or disable network sensor services
- store logs locally or forward to master server

● Evaluation Mode
○ Production Mode

Cancel | OK

5. Define username and password


SecurityOnion (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Zenity
Sun 23:18
home
Setup
Trash

Security Onion Setup (joey-virtualbox)

Now let's set the password for this first user account.

This password will be used for Kibana, Squert, and Sguil.

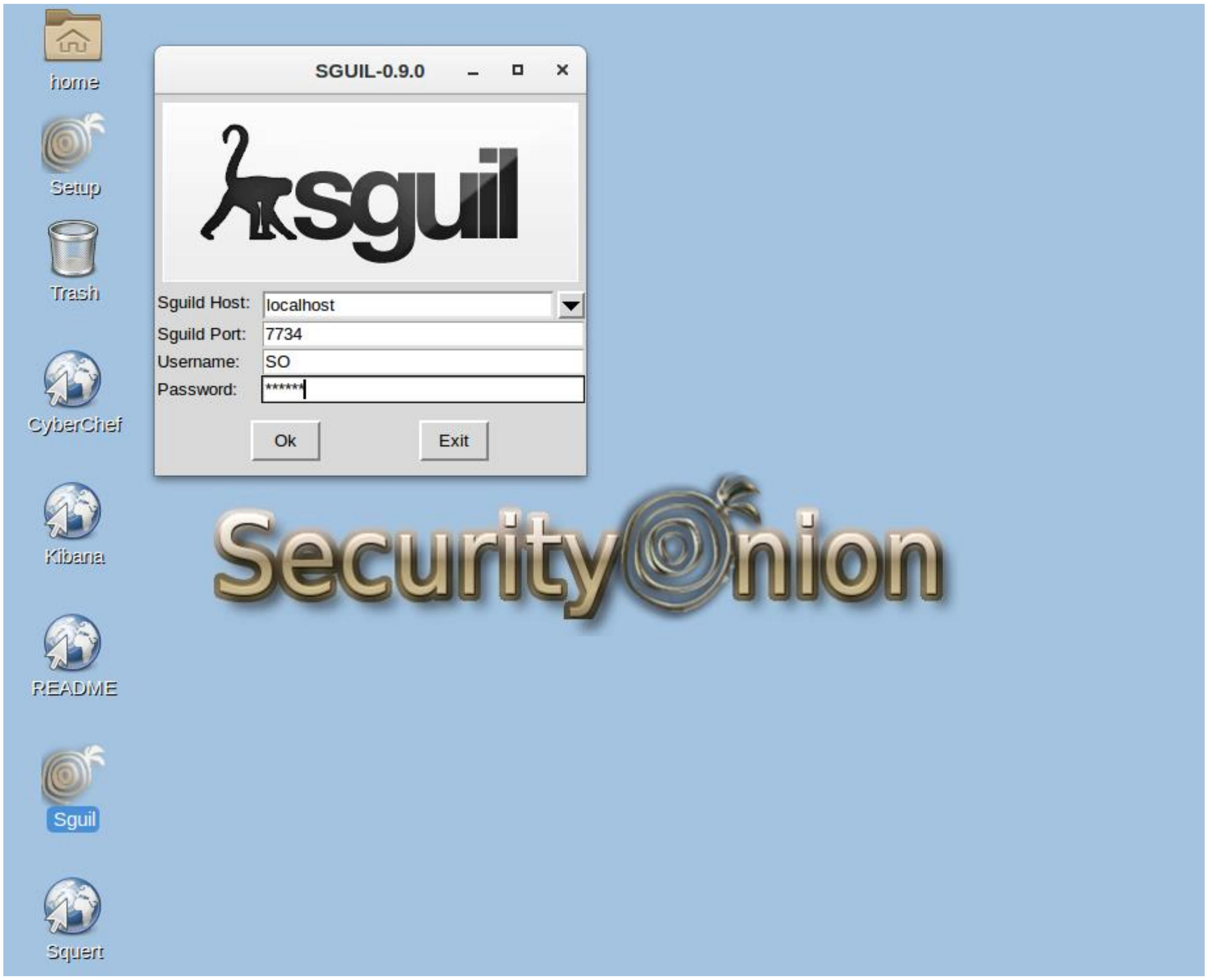
This password must be at least 6 characters.

You can change this password later in the Sguil client or with so-user-passwd.

••••••

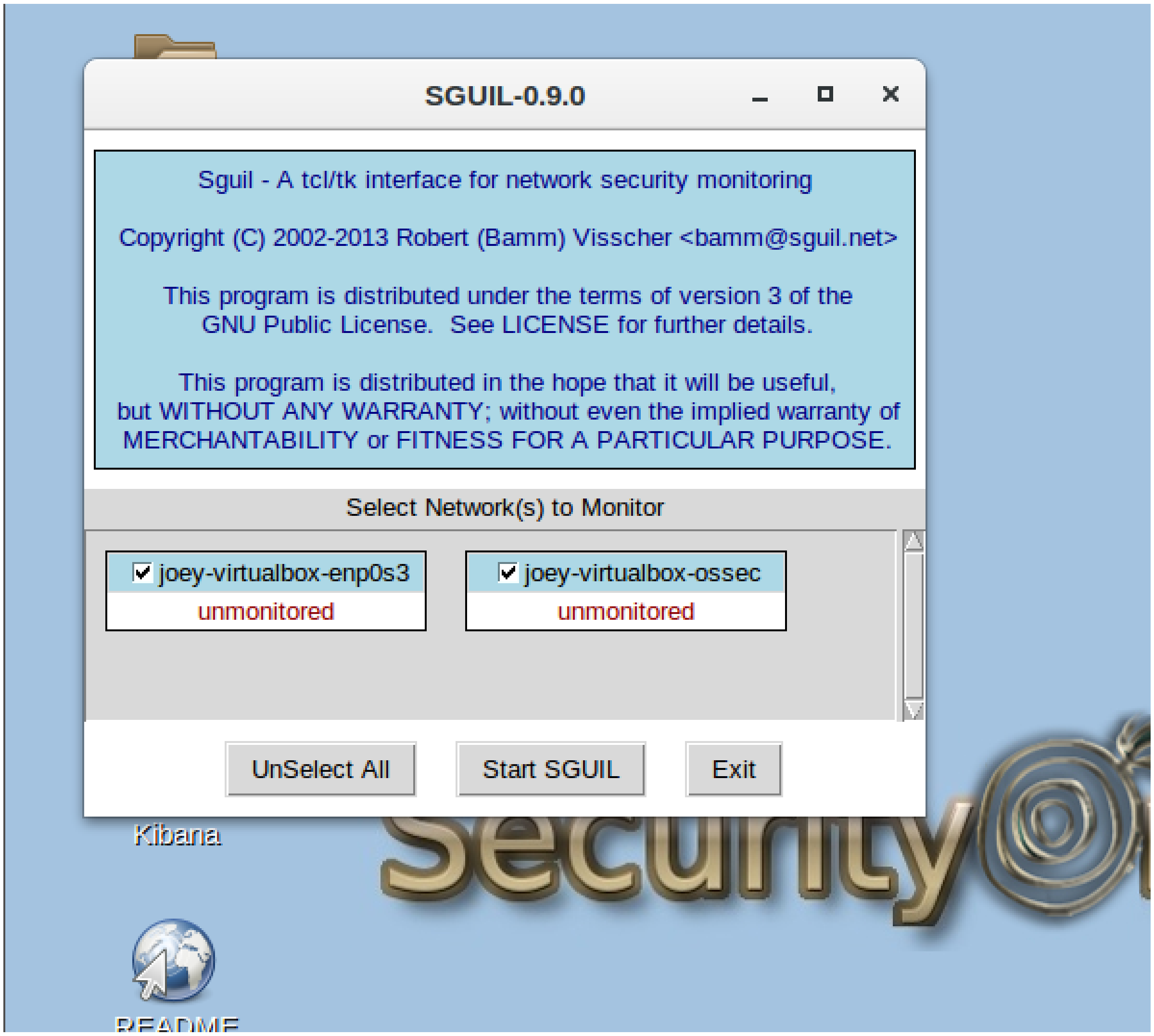
Cancel
OK
Security Onion Setup (joey-virtualb...
1 / 4
Right Ctrl

6. Run Sguil by desktop icon. Log into Sguil by using the username and password which is defined during previous step.



Sguild Host: localhost
Sguild Port: 7734
Username: SO
Password: ******

7. Select all the interfaces and click “Start SGUIL”



SGUIL-0.9.0

Sguil - A tcl/tk interface for network security monitoring

Copyright (C) 2002-2013 Robert (Bamm) Visscher <bamm@sguil.net>

This program is distributed under the terms of version 3 of the GNU Public License. See LICENSE for further details.

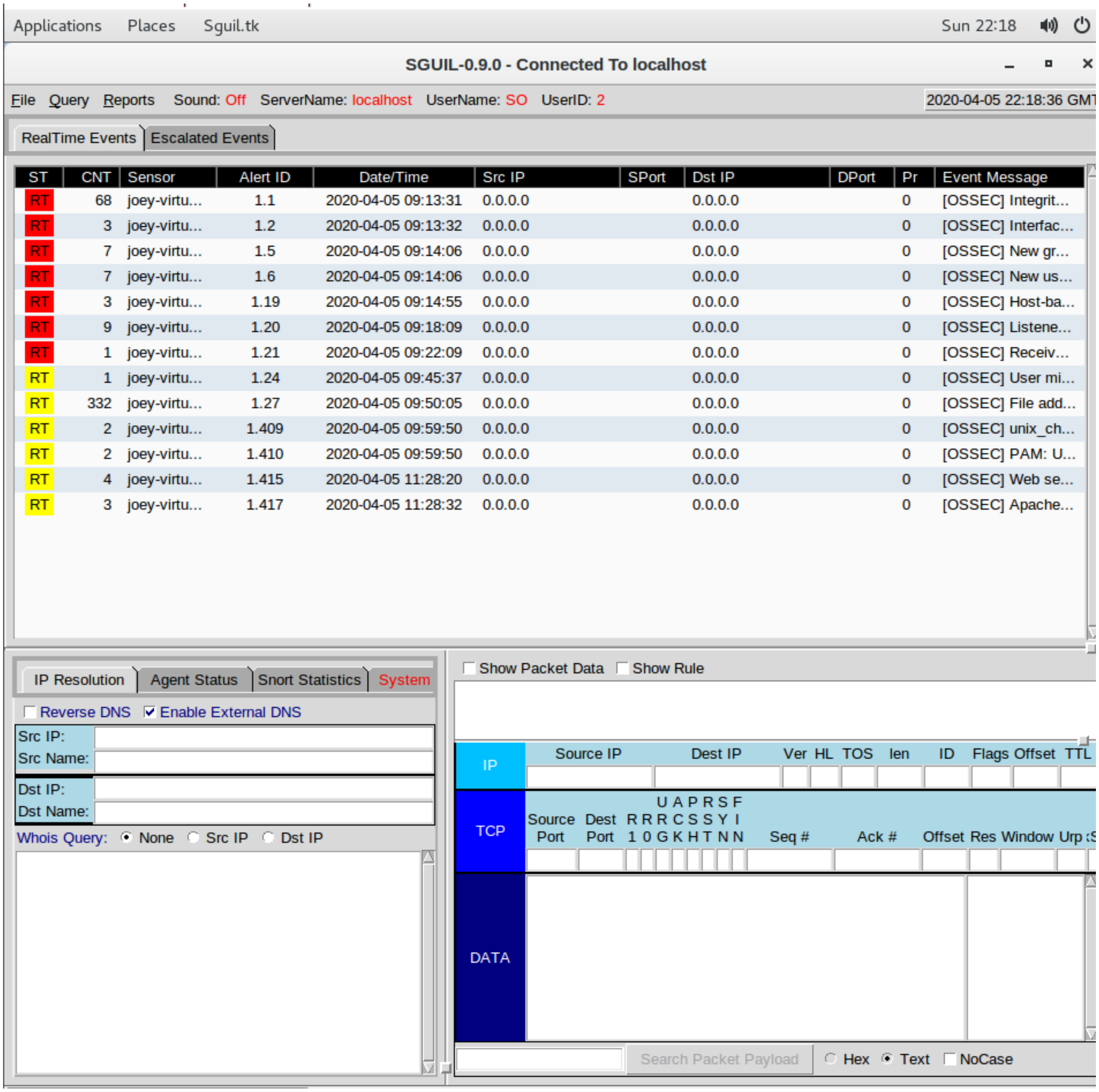
This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

Select Network(s) to Monitor

☑ joey-virtualbox-enp0s3
unmonitored

☑ joey-virtualbox-ossec
unmonitored

8. Logged into Sguil



SGUIL-0.9.0 - Connected To localhost

Sound: Off ServerName: localhost UserName: SO UserID: 2 2020-04-05 22:18:36 GMT

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	68	joey-virtu...	1.1	2020-04-05 09:13:31	0.0.0.0		0.0.0.0		0	[OSSEC] Integrit...
RT	3	joey-virtu...	1.2	2020-04-05 09:13:32	0.0.0.0		0.0.0.0		0	[OSSEC] Interfac...
RT	7	joey-virtu...	1.5	2020-04-05 09:14:06	0.0.0.0		0.0.0.0		0	[OSSEC] New gr...
RT	7	joey-virtu...	1.6	2020-04-05 09:14:06	0.0.0.0		0.0.0.0		0	[OSSEC] New us...
RT	3	joey-virtu...	1.19	2020-04-05 09:14:55	0.0.0.0		0.0.0.0		0	[OSSEC] Host-ba...
RT	9	joey-virtu...	1.20	2020-04-05 09:18:09	0.0.0.0		0.0.0.0		0	[OSSEC] Listene...
RT	1	joey-virtu...	1.21	2020-04-05 09:22:09	0.0.0.0		0.0.0.0		0	[OSSEC] Receiv...
RT	1	joey-virtu...	1.24	2020-04-05 09:45:37	0.0.0.0		0.0.0.0		0	[OSSEC] User mi...
RT	332	joey-virtu...	1.27	2020-04-05 09:50:05	0.0.0.0		0.0.0.0		0	[OSSEC] File add...
RT	2	joey-virtu...	1.409	2020-04-05 09:59:50	0.0.0.0		0.0.0.0		0	[OSSEC] unix_ch...
RT	2	joey-virtu...	1.410	2020-04-05 09:59:50	0.0.0.0		0.0.0.0		0	[OSSEC] PAM: U...
RT	4	joey-virtu...	1.415	2020-04-05 11:28:20	0.0.0.0		0.0.0.0		0	[OSSEC] Web se...
RT	3	joey-virtu...	1.417	2020-04-05 11:28:32	0.0.0.0		0.0.0.0		0	[OSSEC] Apache...

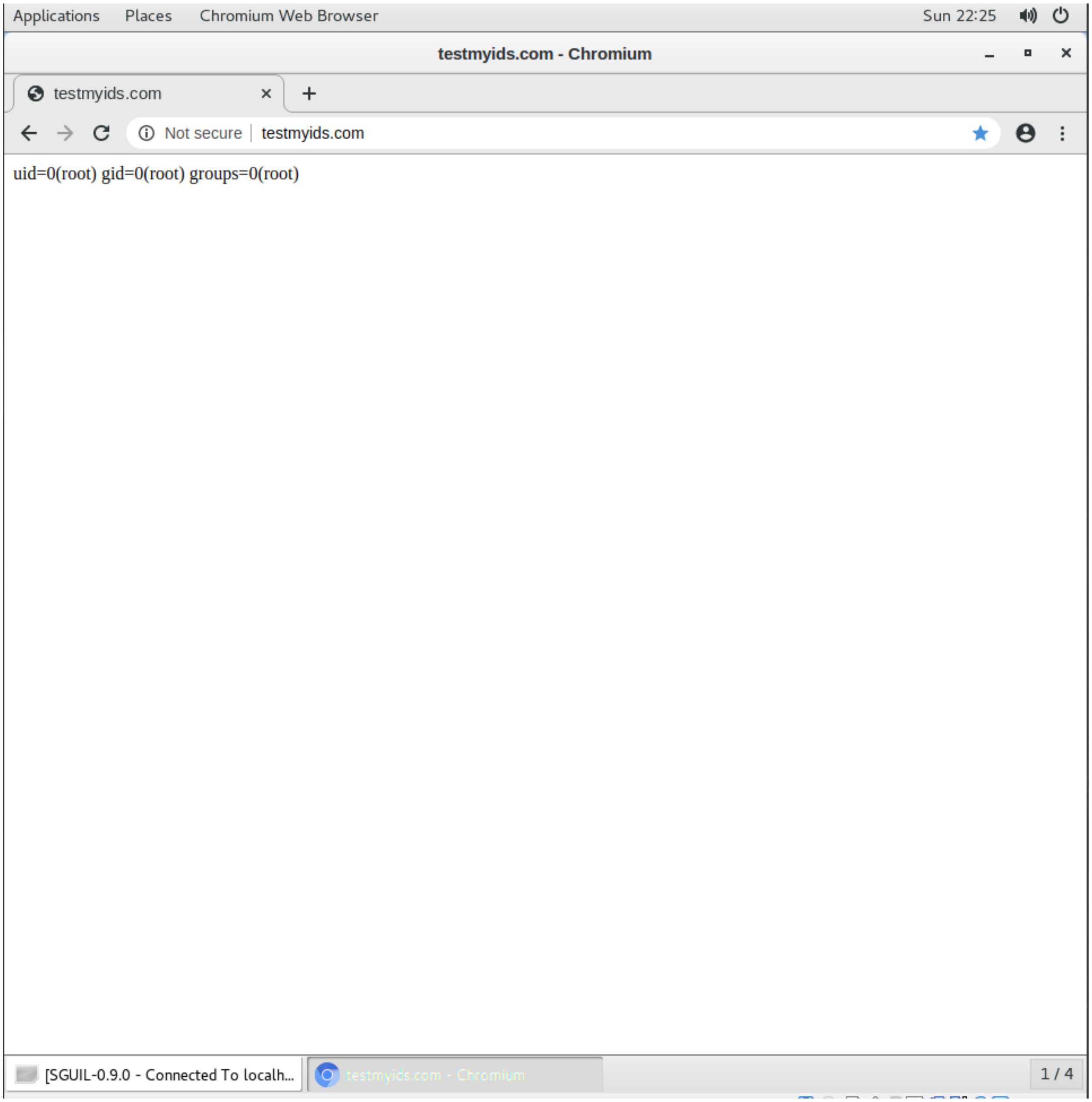
☐ Reverse DNS ☑ Enable External DNS

Whois Query: ● None ○ Src IP ○ Dst IP

☐ Show Packet Data ☐ Show Rule

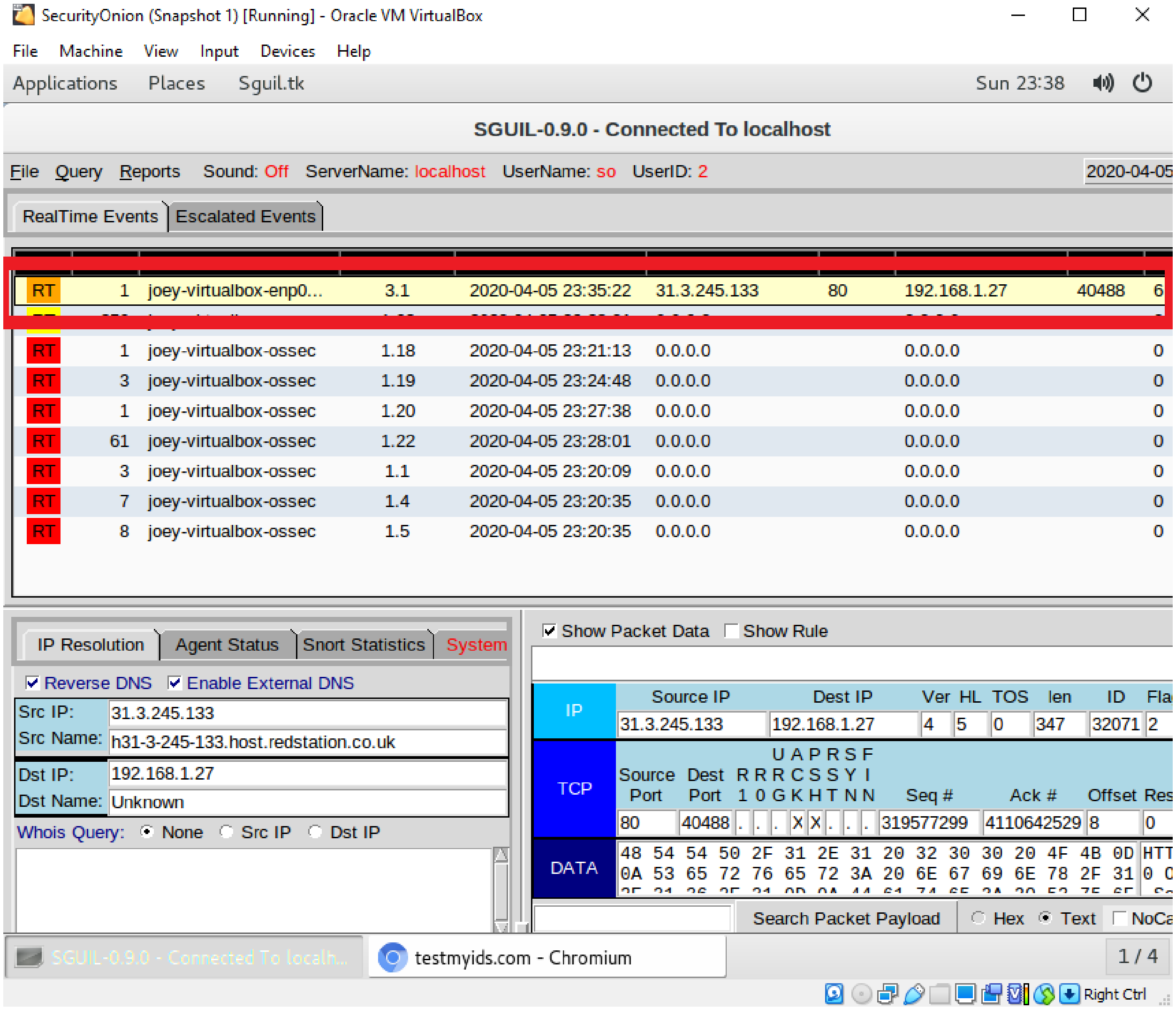
○ Hex ● Text ☐ NoCase

9. Open Chrome and visit testmyids.com



```
uid=0(root) gid=0(root) groups=0(root)
```

10. found one alert. (Alert ID 3.1)



SecurityOnion (Snapshot 1) [Running] - Oracle VM VirtualBox

SGUIL-0.9.0 - Connected To localhost

File Query Reports Sound: Off ServerName: localhost UserName: so UserID: 2 2020-04-05

RealTime Events | Escalated Events

RT	1	joey-virtualbox-enp0...	3.1	2020-04-05 23:35:22	31.3.245.133	80	192.168.1.27	40488	6
RT	1	joey-virtualbox-ossec	1.18	2020-04-05 23:21:13	0.0.0.0		0.0.0.0		0
RT	3	joey-virtualbox-ossec	1.19	2020-04-05 23:24:48	0.0.0.0		0.0.0.0		0
RT	1	joey-virtualbox-ossec	1.20	2020-04-05 23:27:38	0.0.0.0		0.0.0.0		0
RT	61	joey-virtualbox-ossec	1.22	2020-04-05 23:28:01	0.0.0.0		0.0.0.0		0
RT	3	joey-virtualbox-ossec	1.1	2020-04-05 23:20:09	0.0.0.0		0.0.0.0		0
RT	7	joey-virtualbox-ossec	1.4	2020-04-05 23:20:35	0.0.0.0		0.0.0.0		0
RT	8	joey-virtualbox-ossec	1.5	2020-04-05 23:20:35	0.0.0.0		0.0.0.0		0

IP Resolution | Agent Status | Snort Statistics | System

☑ Reverse DNS ☑ Enable External DNS

Src IP: 31.3.245.133
Src Name: h31-3-245-133.host.redstation.co.uk
Dst IP: 192.168.1.27
Dst Name: Unknown

Whois Query: ● None ○ Src IP ○ Dst IP

☑ Show Packet Data □ Show Rule

IP	Source IP	Dest IP	Ver	HL	TOS	len	ID	Fla
	31.3.245.133	192.168.1.27	4	5	0	347	32071	2

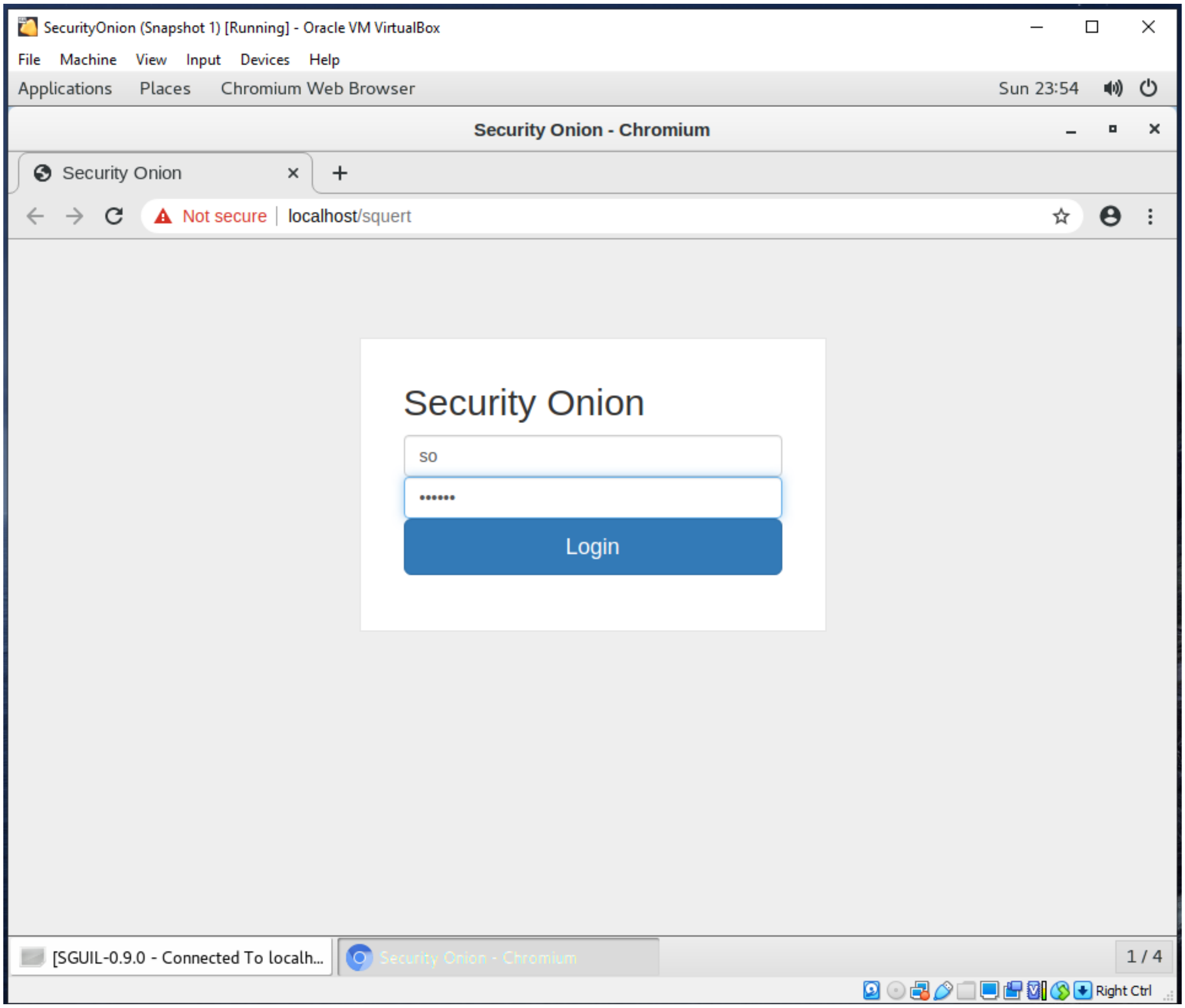
TCP	Source Port	Dest Port	R 1	R 0	U R G	A C K	P S H	R S T	S Y N	F I N	Seq #	Ack #	Offset	Res
	80	40488	.	.	.	X	X	.	.	.	319577299	4110642529	8	0

```
DATA  48 54 54 50 2F 31 2E 31 20 32 30 30 20 4F 4B 0D  HTT
      0A 53 65 72 76 65 72 3A 20 6E 67 69 6E 78 2F 31  0 C
```

Search Packet Payload ○ Hex ● Text □ NoCa

SGUIL-0.9.0 - Connected To localh... | testmyids.com - Chromium | 1 / 4

11. login Squert by Desktop icon



SecurityOnion (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications Places Chromium Web Browser
Sun 23:54
Security Onion - Chromium
Security Onion
Not secure
localhost/squert
[SGUIL-0.9.0 - Connected To localh...
Security Onion - Chromium
1 / 4
Right Ctrl

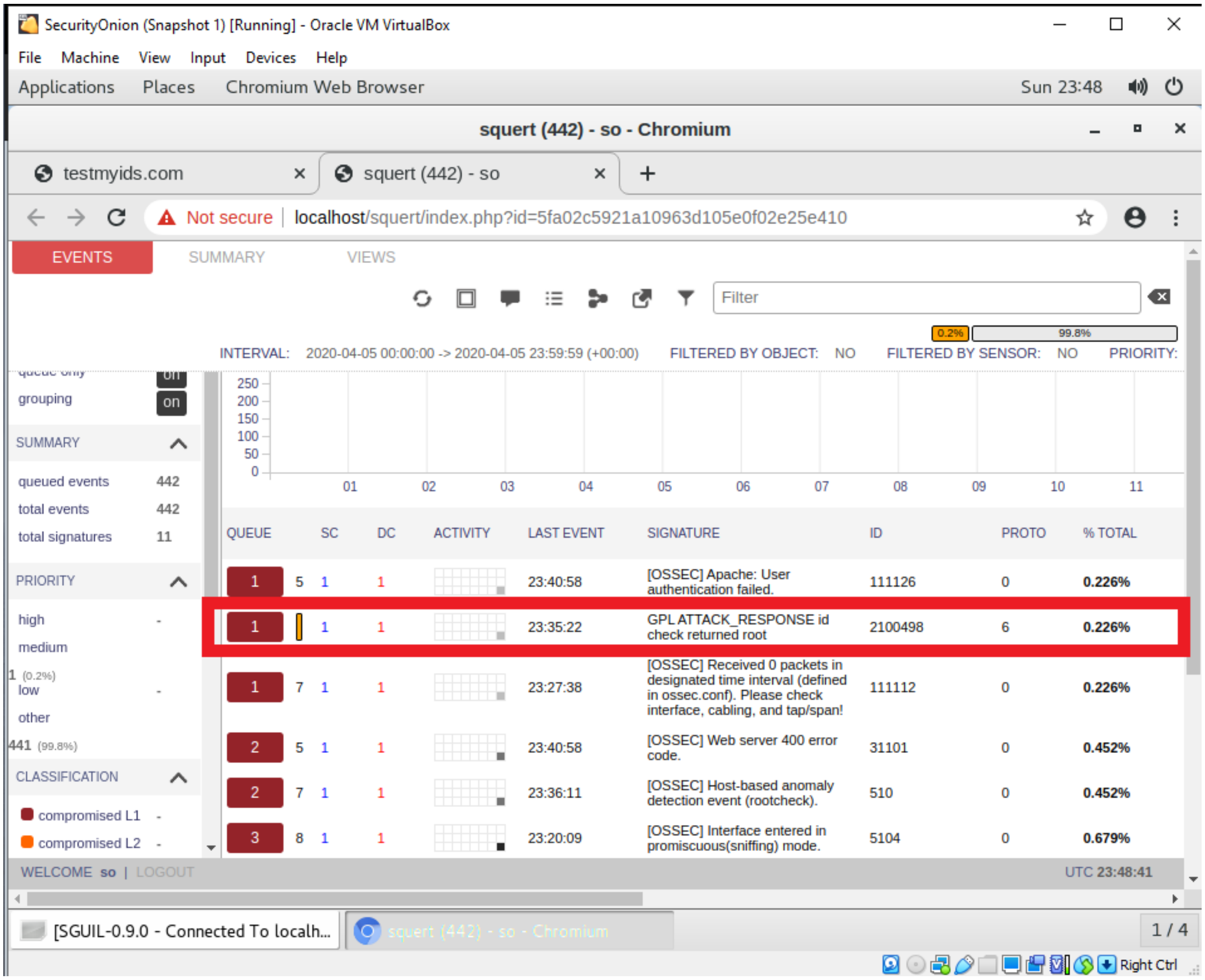
Security Onion

so

••••••

Login

12. Found the event which we visited the testmyids.com in the browser



SecurityOnion (Snapshot 1) [Running] - Oracle VM VirtualBox

squert (442) - so - Chromium

localhost/squert/index.php?id=5fa02c5921a10963d105e0f02e25e410

INTERVAL: 2020-04-05 00:00:00 -> 2020-04-05 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: NO PRIORITY:

SUMMARY	
queued events	442
total events	442
total signatures	11

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
1	5 1	1		23:40:58	[OSSEC] Apache: User authentication failed.	111126	0	0.226%
1	1	1		23:35:22	GPL ATTACK_RESPONSE id check returned root	2100498	6	0.226%
1	7 1	1		23:27:38	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	111112	0	0.226%
2	5 1	1		23:40:58	[OSSEC] Web server 400 error code.	31101	0	0.452%
2	7 1	1		23:36:11	[OSSEC] Host-based anomaly detection event (rootcheck).	510	0	0.452%
3	8 1	1		23:20:09	[OSSEC] Interface entered in promiscuous(sniffing) mode.	5104	0	0.679%

It conformed that Sguil using several probes to analyze the traffic from network. When the condition satisfied , it will send an alert to user. In this case, we visited a dummy website http://testmyids.com which has a suspicious behavior and Sguil successfully captured the action and report it to user interface (both Sguil and Squert).

Ref:

https://blog.securityonion.net/2011/01/introduction-to-sguil-and-squert-part-1.html