Lab 4 Security Onion

Cheng Xu Yu Qiu Minjie Fu

NIDS - Snort

1. Figure out what's the directory that stores the Snort rules and also the alert logs.

The following is the directory that stores the Snort rules: `/etc/nsm/rules/`

```
cxu@cxu-VirtualBox:/etc$ cd nsm/rules
cxu@cxu-VirtualBox:/etc/nsm/rules$ ls
app-layer-events.rules  files.rules            reference.config
backup                  gen-msg.map            sid-msg.map
black_list.rules        http-events.rules      smb-events.rules
bpf.conf                ipsec-events.rules     smtp-events.rules
classification.config   kerberos-events.rules  so_rules.rules
decoder-events.rules    local.rules            stream-events.rules
dnp3-events.rules       modbus-events.rules    threshold.conf
dns-events.rules        nfs-events.rules       tls-events.rules
downloaded.rules        ntp-events.rules       white_list.rules
```

The following is the directory that stores the Snort alert logs: `/var/log/nsm/cxu-virtualbox-enp0s8/`

```
root@cxu-VirtualBox:~# cd /var/log/nsm/cxu-virtualbox-enp0s8/
root@cxu-VirtualBox:/var/log/nsm/cxu-virtualbox-enp0s8# ls
barnyard2-1.log                  netsniff-ng.log.20190510204535
barnyard2-1.log.20190508025204   netsniff-ng.log.20190510214533
netsniff-ng.log                  pcap_agent.log
netsniff-ng.log.20190508025158   pcap_agent.log.20190508025159
netsniff-ng.log.20190508160530   snort_agent-1.log
netsniff-ng.log.20190508183939   snort_agent-1.log.20190508025200
netsniff-ng.log.20190508185243   snortu-1.log
netsniff-ng.log.20190508185351   snortu-1.log.20190508025203
netsniff-ng.log.20190509154334
root@cxu-VirtualBox:/var/log/nsm/cxu-virtualbox-enp0s8# ls
```

2. Generate the malicious traffic with the sample pcap files, and use the analysis tool "Squert" or "Sguil" to verify that the IDS is running. What's your observation? (Hint: "tcpreplay" is a tool for traffic replay. If you're not sure on how to do it, refer to the walkthrough doc or the youtube tutorial mentioned above.)

1) We use command `locate zeus` to find out the sample pcap files:

```
cxu@cxu-VirtualBox:~$ locate zeus
/opt/samples/zeus-sample-1.pcap
/opt/samples/zeus-sample-2.pcap
/opt/samples/zeus-sample-3.pcap
/usr/share/wireshark/radius/dictionary.zeus
```

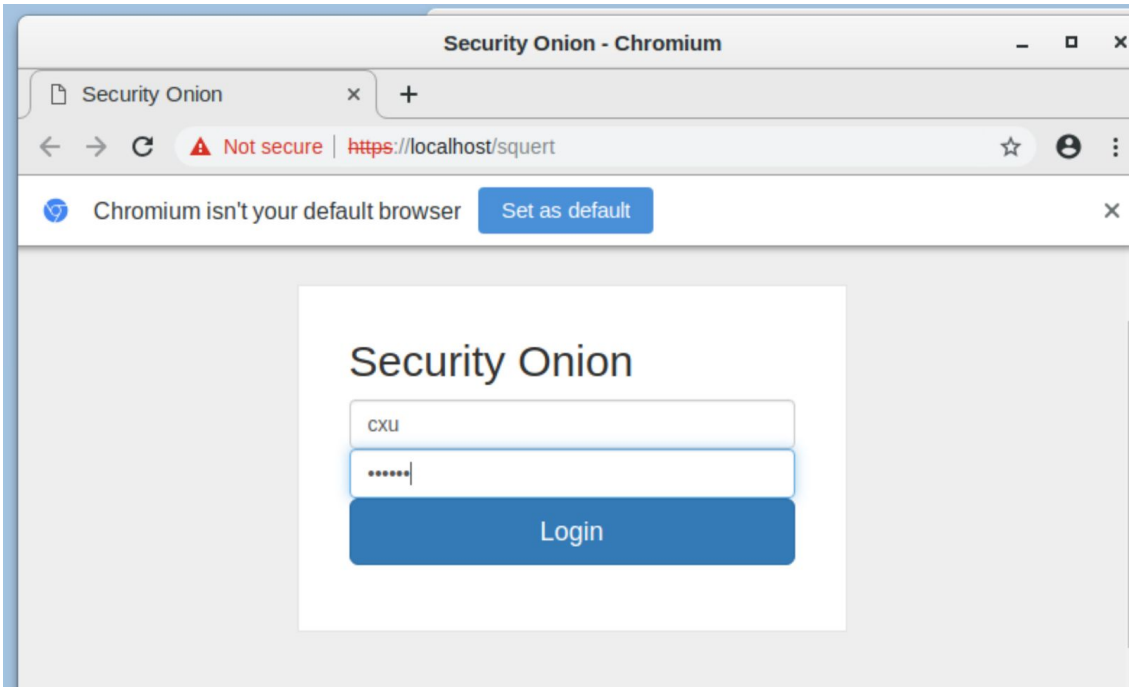
2) We use `tcpreplay` to generate malicious traffic. We chose the first sample pcap file and looped the following command 10 times on the host-only interface:

```
sudo tcpreplay -l 10 -i enp0s8 -t /opt/samples/zeus-sample-1.pcap
```

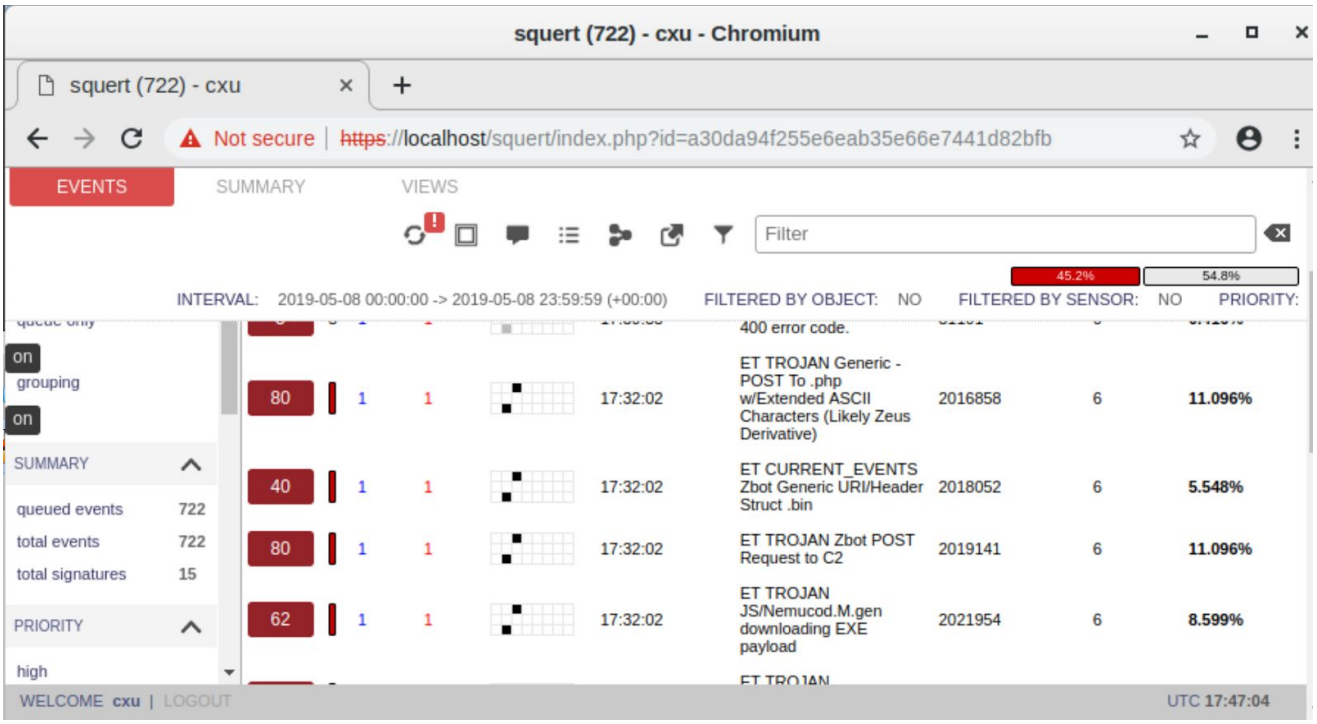
Regardless of error messages, the `tcpreplay` command functions properly.

```
Unable to send packet:
Warning in send_packets.c:send_packets() line 178:
Unable to send packet:
Warning in send_packets.c:send_packets() line 178:
Unable to send packet:
Warning in send_packets.c:send_packets() line 178:
Unable to send packet:
Warning in send_packets.c:send_packets() line 178:
Unable to send packet:
Warning in send_packets.c:send_packets() line 178:
Unable to send packet:
Warning in send_packets.c:send_packets() line 178:
Unable to send packet:
```

3) We double-clicked the Squert icon on the desktop and logged-in using our username and password:



4) Once logged-in, several alerts showed on the web page indicating Zeus Trojan activity is detected, which verified the IDSis running.



HIDS - Wazuh/Ossec

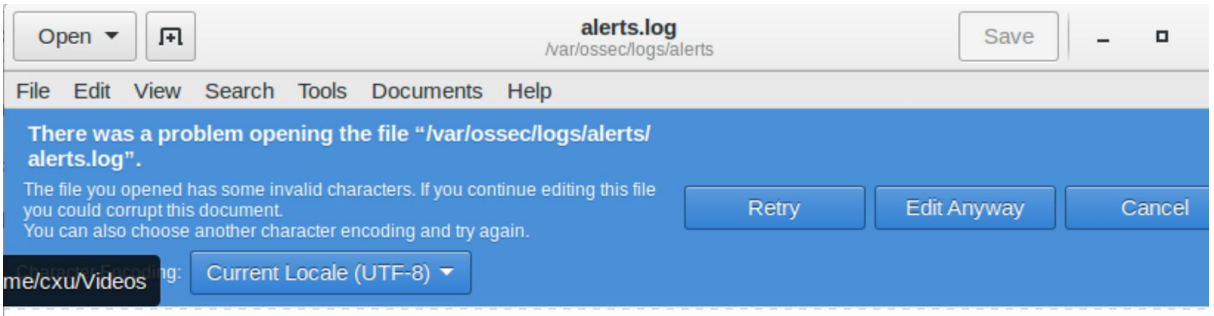
1. Find the location where stores the OSSEC alert logs. If there's no "login success", "login failure", or "access to root" alerts, try to generate them and provide the screenshots and explanations.

The following file stores the OSSEC alert logs:

`/var/ossec/logs/alerts/alerts.log`

We found all three kinds of alerts in alerts.log:

- “login success” alert:




```
** Alert 1557282885.647: -
pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,
2019 May 08 02:34:45 cxu-VirtualBox->/var/log/auth.log
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
User: cxu
May  8 02:34:45 cxu-VirtualBox systemd: pam_unix(systemd-user:session): session opened for
user cxu by (uid=0)
uid: 0
```

- "login failure" alerts are found:

```
** Alert 1557340865.427285: -
pam,syslog,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,gpg13_7.8,gdpr_IV_35.7.d,gdpr_IV_32.2,
2019 May 08 18:41:05 cxu-VirtualBox->/var/log/auth.log
Rule: 5503 (level 5) -> 'PAM: User login failed.'
User: cxu
May  8 18:41:05 cxu-VirtualBox sudo: pam_unix(sudo:auth): authentication failure; logname= uid=1000
euid=0 tty=/dev/pts/0 ruser=cxu rhost=  user=cxu
uid: 1000
euid: 0
tty: /dev/pts/0
```

The following is the authentication failure for Squert:

```
** Alert 1557284214.177466: -
securityonion,syslog,authentication_failed,pci_dss_10.2.4,pci_dss_10.2.5,gpg13_7.1,gdpr_IV_35.7.d,gdpr_
2019 May 08 02:56:54 cxu-VirtualBox->/var/log/apache2/error.log
Rule: 111126 (level 5) -> 'Apache: User authentication failed.'
Src IP: ::1
Src Port: 49808
User: cxu
[Wed May 08 02:56:53.037631 2019] [auth_form:error] [pid 20246] [client ::1:49808] AH01807: user
'cxu': authentication failure for "/squert": password Mismatch, referer: https://localhost/squert
```

- "access to root" alert:

```
** Alert 1557282943.17712: -
syslog,sudo,pci_dss_10.2.5,pci_dss_10.2.2,gpg13_7.6,gpg13_7.8,gpg13_7.13,gdpr_IV_32.2,
2019 May 08 02:35:43 cxu-VirtualBox->/var/log/auth.log
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed'
User: root
May  8 02:35:41 cxu-VirtualBox sudo:      cxu : TTY=unknown ; PWD=/home/cxu ; USER=root ;
COMMAND=/usr/sbin/sosetup
tty: unknown
pwd: /home/cxu
command: /usr/sbin/sosetup
```

2. Create your own OSSEC rules! Let OSSEC monitor any specific directory as you like, and generate the "real-time alerts" once you create, modify, and delete the files inside that directory.

* View and screenshot the alert log files from the terminal

* Use the visual analysis tool to view those alerts OR try to setup the email notifications regarding those alerts

We set up the OSSEC rules in the following file: `/var/ossec/etc/ossec.conf`

- By default, OSSEC does not alert on new files. To enable this functionlity, <alert_new_files> must be set to yes inside the <syscheck> section of the ossec.conf.

  We also changed directories to let OSSEC send real-time alerts:

```
<!-- File integrity monitoring -->
<syscheck>
  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <scan_on_start>yes</scan_on_start>

  <!-- Generate alert when new file detected -->
  <alert_new_files>yes</alert_new_files>

  <!-- Don't ignore files that change more than 'frequency' times -->
  <auto_ignore frequency="10" timeframe="3600">no</auto_ignore>

  <!-- Directories to check  (perform all possible verifications) -->
<directories report_changes="yes" realtime="yes" check_all="yes">/etc,/usr/bin,/usr/sbin</directorie
<directories report_changes="yes" realtime="yes" check_all="yes">/var/www,/bin,/sbin</directories>
```

- We modified the rules file: `/var/ossec/rules/local_rules.xml.` We added a new rule inside this file:

```
Open ▾   local_rules.xml   Save
         /var/ossec/rules
File  Edit  View  Search  Tools  Documents  Help
<!-- Local rules -->

<!-- Modify it at your will. -->
<rule id="554" level="10" overwrite="yes">
    <category>ossec</category>
    <decoded_as>syscheck_new_entry</decoded_as>
    <description>File added to the system</description>
    <group>syscheck,</group>
  </rule>
```

- We restarted OSSEC with the following command: `/var/ossec/bin/ossec-control restart`

- To see whether our new rule works, we created a new file called `new_file.txt` under /etc directory, and added a word “test” in that file:

```
** Alert 1557436040.93312: mail  - local,syslog,sshd,syscheck,
2019 May 09 21:07:20 cxu-VirtualBox->syscheck
Rule: 554 (level 7) -> 'File added to the system.'
File '/etc/new_file.txt' was added.
```

The above screenshot shows that the alert was sent.

- Then we change the content of that file from “test” to “change 1”. After modification, we got the alert indicates that the file was changed.

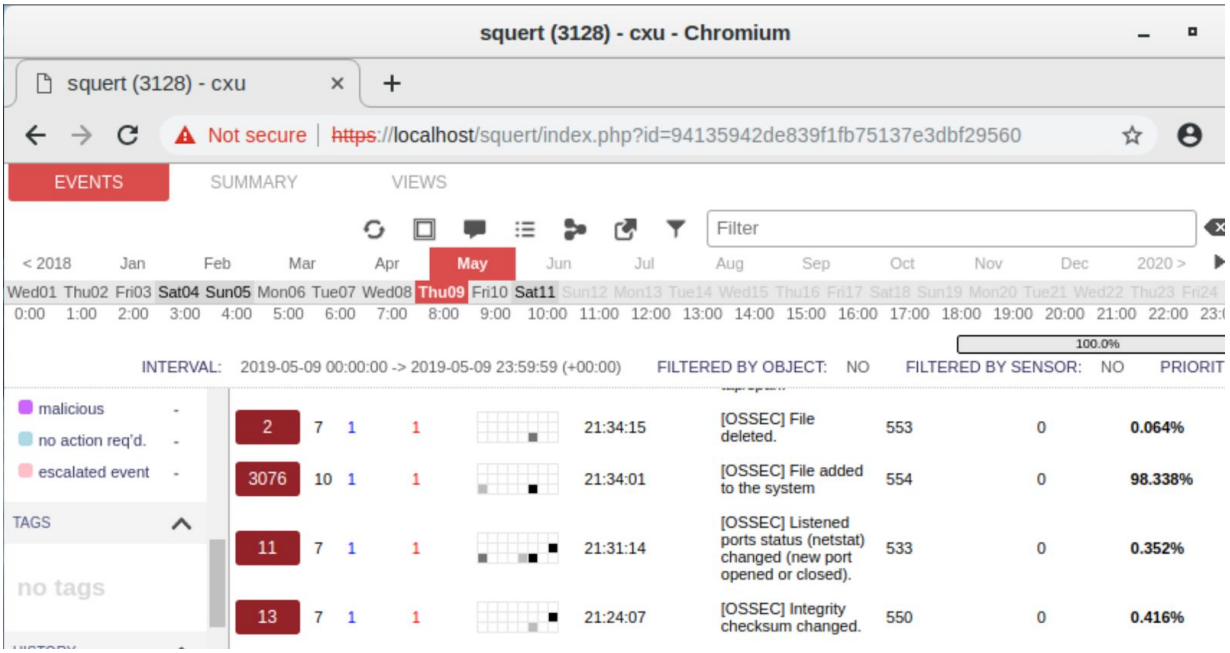
```
Open ▾   alerts.log
/var/ossec/logs/alerts   Save
File  Edit  View  Search  Tools  Documents  Help
** Alert 1557437047.1715310: mail  - ossec,syscheck,pci_dss_11.5,gpg13_4.11,gdpr_II_5.1.f,
2019 May 09 21:24:07 cxu-VirtualBox->syscheck
Rule: 550 (level 7) -> 'Integrity checksum changed.'
File '/etc/new_file.txt' checksum changed.
Size changed from '5' to '9'
Old md5sum was: 'd8e8fca2dc0f896fd7cb4cb0031ba249'
New md5sum is : '58cdc472c804dac66bd9399c7f082e9e'
Old sha1sum was: '4e1243bd22c66e76c2ba9eddc1f91394e57f9f83'
New sha1sum is : '42a545badb631cb713c37adc3bc73bb0ef335578'
Old sha256sum was: 'f2ca1bb6c7e907d06dafe4687e579fce76b37e4e93b7605022da52e6ccc26fd2'
New sha256sum is : '14a32a460151b3cbde3901f6838c10b8e12e0de178ab56c656f21d0724c56f49'
Old modification time was: 'Thu May  9 20:50:37 2019', now it is 'Thu May  9 21:23:44 2019'
Old inode was: '819086', now it is '819790'
What changed:
1c1
< test
---
> change 1

Attributes:
 - Size: 9
 - Date: Thu May  9 21:23:44 2019
 - Inode: 819790
 - User: root (0)
```

- We deleted the file “new_file.txt” and we got the alert says the file was deleted.

```
** Alert 1557437655.1729054: mail  - ossec,syscheck,pci_dss_11.5,gpg13_4.11,gdpr_II_5.1.f,
2019 May 09 21:34:15 cxu-VirtualBox->syscheck
Rule: 553 (level 7) -> 'File deleted.'
File '/etc/new_file.txt' was deleted.
```

- At last, we used Squert to view 3 three alerts:


squert (3128) - cxu - Chromium
squert (3128) - cxu
Not secure
https://localhost/squert/index.php?id=94135942de839f1fb75137e3dbf29560
EVENTS
SUMMARY
VIEWS
Filter
< 2018 Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec 2020 >
Wed01 Thu02 Fri03 Sat04 Sun05 Mon06 Tue07 Wed08 Thu09 Fri10 Sat11 Sun12 Mon13 Tue14 Wed15 Thu16 Fri17 Sat18 Sun19 Mon20 Tue21 Wed22 Thu23 Fri24
0:00 1:00 2:00 3:00 4:00 5:00 6:00 7:00 8:00 9:00 10:00 11:00 12:00 13:00 14:00 15:00 16:00 17:00 18:00 19:00 20:00 21:00 22:00
100.0%
INTERVAL: 2019-05-09 00:00:00 -> 2019-05-09 23:59:59 (+00:00)
FILTERED BY OBJECT: NO
FILTERED BY SENSOR: NO
PRIORIT
malicious -
no action req'd. -
escalated event -
TAGS
no tags
2 7 1 1 21:34:15 [OSSEC] File deleted. 553 0 0.064%
3076 10 1 1 21:34:01 [OSSEC] File added to the system 554 0 98.338%
11 7 1 1 21:31:14 [OSSEC] Listened ports status (netstat) changed (new port opened or closed). 533 0 0.352%
13 7 1 1 21:24:07 [OSSEC] Integrity checksum changed. 550 0 0.416%