Please walk through these checks on your Zeek and AC-Hunter systems. If any of them fail or you're getting errors of some form, please get in touch with support at https://portal.activecountermeasures.com/support/support-request/ . Please describe the check that failed and include the program output and errors (if any).

The steps below are generally organized starting at the source of the data (the packet capture) and go through to the final stages of importing the data into AC-Hunter. With that said, you're welcome to do these in a different order if you suspect your issue is at a particular stage. If these don't find the source of the problem, it's worth starting at the beginning and working your way through.

Text below in italics, such as "*eth99*" is intended to be replaced with the appropriate value for your system.

Checks

On the Zeek sensor

1. On what OS are you running?

```
cat /etc/*release*
```

will show the name and version of the Linux distribution you're using. Please include this if you contact support.

2. Is selinux enabled?

```
getenforce
```

If you get an error that says "getenforce is not installed" or "not found", this is actually not a problem (consider this "disabled", which is good.) If you get "Enforcing" or "Current mode: enforcing", this is an issue. You'll need to a) change the selinux mode to Permissive with:

```
setenforce Permissive
```

, b) edit /etc/selinux/config as root, c) change the uncommented "SELINUX=" line to SELINUX=permissive

and d) reboot. ("SELINUX=disabled" is acceptable as well.)

3. Identify the interface on which you're capturing packets. See https://www.activecountermeasures.com/on-which-interface-should-i-capture-packets/ if you're not sure which one to use. In the following instructions we'll use "*eth99*"; please substitute the name of your interface.

4. Do you have available drive space?

```
df -h /opt/
```

This should have at least 20GB of disk space, preferably more. If you're out of drive space, please see https://portal.activecountermeasures.com/support/faq/?Display_FAQ=4970 for the steps to manually and/or automatically prune old data.

5. See that packets are arriving on it by running either:

```
ip -s addr
```

or

```
ifconfig eth99
```

Both display the number of bytes received (RX) and the number of bytes transmitted (TX) on that interface since boot. The number of bytes received on an interface connected to a span/copy/mirror/tap should be at least hundreds of times larger than the number of bytes transmitted. If it isn't, this may not be the correct interface to use or you may not be receiving traffic from a span/copy/mirror/tap port.

6. Is the interface in "promiscuous" mode? Run

```
ip -s addr
```

or

```
ifconfig eth99
```

You should see "PROMISC" in the list of flags for that interface. Zeek should - in most cases - enable this automatically when it starts. In recent versions of Centos or RHEL Linux you may run into an issue where it does not. Please refer to the following for potential fixes:
https://access.redhat.com/solutions/3525641
https://www.thegeekdiary.com/how-to-configure-interface-in-promiscuous-mode-in-centos-rhel/
https://www.thegeekdiary.com/how-to-configure-interfaces-in-promiscuous-mode-on-centos-rhel-7-persistently/
https://unix.stackexchange.com/questions/198076/enable-promiscous-mode-in-centos-7

For Ubuntu 20.04, see:
https://askubuntu.com/questions/1355974/how-to-enable-promiscuous-mode-permanently-on-a-nic-managed-by-networkmanager
https://copyprogramming.com/howto/how-to-properly-put-network-interface-into-promiscuous-mode-on-linux (in particular, see "Method 2").

7. Confirm that you have packets arriving on that interface with:

```
sudo tcpdump -qtnp -i eth99 'not tcp port 22'
```

You should see a flood of traffic coming across your screen, including traffic to and from other systems on this network. If you don't, you may have the wrong interface on the Zeek sensor or what you think is a span/copy/mirror port on the switch (or tap) may not be correctly configured.

Press `ctrl-c` to stop the program.

8. Is Zeek listening on the right interface?

```
cat /opt/zeek/etc/node.cfg | egrep '(worker-|interface)'
```

Both output lines should show the interface you found in step 1. If not (or if this file doesn't exist at all), please see https://portal.activecountermeasures.com/support/faq/?Display_FAQ=3914 for the steps to enter the right interface. (Note: it's fine if these lines show up multiple times when you have multiple interfaces accepting traffic.)

9. Do you use vlans on your network? If you do, and if there's any chance that you may have vlan-tagged traffic arriving at the capture interface, make sure that the "8021q" kernel module is loaded by running:

```
lsmod | grep -i 8021q
```

You should see a line of output with "8021q" in it. If you don't, run:

```
sudo modprobe 8021q
```

and append the line

```
8021q
```

to `/etc/modules` if it exists, and `/etc/modules-load.d/8021q.conf` if /etc/modules doesn't exist.

The above steps simply tell the kernel to capture vlan-tagged traffic on the capture interface and pass it up to Zeek. Zeek will recognize and parse that traffic with no additional configuration.

10. Is Zeek running? Check with:

```
sudo zeek status
```

In particular, does it show "restarting", or is the time up in the STATUS column under a minute or two? Both of these may point to Zeek crashing and restarting. Ideally the time under STATUS should be approximately equal to the time under CREATED for the Zeek container.

11. Does the Zeek log output show problems or issues related to crashing? Run:

```
sudo docker logs zeek
```

If docker complains that it can't find the container (or something similar) you may need to run this multiple times to catch Zeek while it's up.

12. How much drive space is taken by Zeek logs on the Zeek sensor? We'll look at yesterday as that should be a complete day's worth of logs:

```
du -sh /opt/zeek/logs/`date +%Y-%m-%d --date=yesterday`
```

This should be well into the megabytes on a lightly loaded network or gigabytes on a heavily loaded network. If not, you may not be capturing the traffic headed to the Internet.

13. In particular, do you have 24 logs whose names start with "conn"? In particular, these have to be files starting with "conn**.**" or "conn_"; "conn-summary" files don't count for this. To check, run:

```
ls -al /opt/zeek/logs/`date +%Y-%m-%d --date=yesterday`/conn[._]*
```

There should be 24 of them; their starting hour should range from 00 to 23. If you don't have these or they're terribly small (less than 1000000 bytes), it's a sign that something may be wrong in the packet capture.

14. Do all the systems on this network use (only) reserved/private/RFC1918 addresses (10.x.y.z, 192.168.y.z, and/or 172.16.y.z-172.31.y.x addresses)? If not, have you told Zeek what address blocks to use by editing networks.cfg? Steps to do this are at https://portal.activecountermeasures.com/support/faq/?Display_FAQ=3132 . If you contact support, please let us know the address blocks you've added to this file. Remember that it will take a few hours for this to take effect.

15. Is the operating system reporting problems?

```
sudo dmesg -T | tail --lines=50
```

or

```
sudo tail --lines=50 /var/log/dmesg
```

The output includes a mix of messages from the Linux kernel, including status and state reports as well as hardware or other errors. In particular, is your system so low on memory that it had to kill one or more running process(es)? To check, run:

```
sudo dmesg -T | grep -i '(oom-kill|Out of memory|Killed process|oom_reaper|oom_kill)'
```

If this returns no output at all, that's good - it means that this hasn't happened recently. If you *do* get lines of output, please include these in an email to support@activecountermeasures.com .

16. When logged in as the user under which you installed Zeek on this system, can you ssh to the AC-Hunter system with the following command (replacing ACH.IP.ADDRESS with the AC-Hunter system IP address)?

```
ssh dataimport@ACH.IP.ADDRESS -i "$HOME/.ssh/id_rsa_dataimport" 'echo Successfully connected.'
```

You should **not** be asked for a password - if you are, that means the keys are not set up correctly between Zeek and AC-Hunter. Please follow the steps under "Automated approach" in https://portal.activecountermeasures.com/support/faq/?Display_FAQ=863 to re-establish the link to AC-Hunter.

On the AC-Hunter system

17. On what OS are you running?

```
cat /etc/*release*
```

will show the name and version of the Linux distribution you're using. Please include this if you contact support.

18. Is selinux enabled?

```
getenforce
```

If you get an error that says "getenforce is not installed" or "not found", this is actually not a problem (consider this "disabled", which is good.) If you get "Enforcing" or "Current mode: enforcing", this is an issue. You'll need to change the selinux mode to Permissive with:
setenforce Permissive
, edit /etc/selinux/config as root and change the "SELINUX=" line to
SELINUX=permissive
and reboot.

19. Do you have available drive space?

```
df -h /opt/ /var/lib/docker/
```

Both of these should have at least 20GB of disk space, preferably more. If you're out of drive space, please see https://portal.activecountermeasures.com/support/faq/?Display_FAQ=4970 for the steps to manually and/or automatically prune old data.

20. Are the logs making it across to the AC-Hunter system?

```
du -sh /opt/zeek/remotelogs/*/`date +%Y-%m-%d --date=yesterday`
```

(If you have multiple sensors feeding this AC-Hunter system, you'll see drive usage for all of them - focus on the sensor in question.)

The amount of drive space should be a little smaller than (possibly around ½) the drive usage for the logs stored on the Zeek system. If it isn't, it's possible that the log transfer isn't working. In particular, if the amount of drive space used is 0, 4KB, or some other miniscule amount of storage, it may be that no logs are being transferred at all.

21. Are the logs readable by any process on the system?

```
ls -al /opt/zeek/remotelogs/*/`date +%Y-%m-%d --date=yesterday`
```

On the left of each line will be the permissions for that file. These should all have 3 r's, like:

```
-rw-r--r--   2 dataimport dataimport   2622 Sep 30 23:45 x509.22:00:00-23:00:00.log.gz
```

or

```
-rw-rw-r--   2 dataimport dataimport   2622 Sep 30 23:45 x509.22:00:00-23:00:00.log.gz
```

In particular, the last "r" says that the file is readable by any process on the system, which is needed for AC-Hunter to import the logs.

22. Is AC-Hunter running?

```
sudo docker ps
```

This should show 4 or 5 containers whose names (at the end of each line) start with "achunter_". (If you also installed beaker, active-flow, or Zeek on this system, you'll see other containers whose names start with something else - we can ignore those at the moment.) Is the uptime (in the STATUS column) about equal to the time in the CREATED column? (If not, AC-Hunter may be crashing for some reason.)

23. Are you getting a database named "*sensorname__ipaddress*-rolling" in the list of AC-Hunter databases at all (the list can be found on the Dashboard tab; click the gear icon)? If so, is it there but with totally empty screens for all modules? In particular, does

the DNS module contain any records at all? If a database exists for a given sensor but most or all of the modules are empty, this may be because Zeek doesn't have a complete list of the internal address ranges. See the entry above referring to "networks.cfg".

24. In that list of databases, take a look at the timestamp range of any -rolling databases. Do any of them show a date of 12/31/1969 or 1/1/1970? Computers commonly use these dates as placeholders for "the start of computing time", aka "epoch". If these show up as one of the dates for a database, that may indicate that these are at their default and no data could be imported. This could point to missing or unreadable logs, a mirror port that's not getting copies of all packets, or other issues with the import. Please mention this problem to support when you write in with any other symptoms.

25. Please open up the "-rolling" database for the sensor in question. Please switch to the "Beacons Web" tab. In the upper left, there's a filter (">50%") that discards any results where the certainty that this is a beacon is 49% or less (you can find this under "cumulative metric conformity".) If you get no results, please adjust the filter in the upper left to ">0%". Now look at the "cumulative metric conformity" for the first few results. Are they all small percentages under or around 20%? This may point to a problem getting data into Zeek. Please mention this in your note to support.

26. Are there problems with the import?

```
sudo hunt logs api | tail –lines=100
```

Please look for any error messages.

27. Is the operating system reporting problems?

```
sudo dmesg -T | tail --lines=50
```

or

```
sudo tail --lines=50 /var/log/dmesg
```

The output includes a mix of messages from the Linux kernel, including status and state reports as well as hardware or other errors. In particular, is your system so low on memory that it had to kill one or more running process(es)? To check, run:

```
sudo dmesg -T | grep -i '(oom-kill|Out of memory|Killed process|oom_reaper|oom_kill)'
```

If this returns no output at all, that's good - it means that this hasn't happened recently. If you *do* get lines of output, please include these in an email to support@activecountermeasures.com .

28. If you've reached this point and haven't seen any obvious issues, please contact Active Countermeasures support .

This is a document in progress. Please send feedback on errors, omissions, or improvements to support@activecountermeasures.com .

Document date: 2024-01-18, 12:16