Solution Installation and Operations

LET'S START WITH ELASTIC SEARCH AS A "NETWORK MONITORING SYSTEM".

Requirements

Ubuntu Server 20.04

Elastic-Search

Kibana

Filebeat

Zeek || Suricata

System Requirements

1. RAM 128GB
2. Minimum 1TB SSD
3. Two(2) NIC cards

An Efficient Operator Skillset

1. Understand TCP/OSI Model
2. Understand Infrastructure, Ports, Protocols, and their working
3. Understand the mechanisms used by tools
4. Understand the concept to remove installation errors of this setup

A Network Detection and Response is an application or set of applications that allows us to monitor network traffic for malicious actors and suspicious behaviour, react and respond to the detection of cyber threats to the network.

SENSOR SYSTEM REQUIREMENTS

- Ubuntu server 20.04
- RAM 128GB
- Minimum 1TB SSD
- 2 NIC cards

PRE-REQUISITES

1. During Installation of Ubuntu Server the "mirror address should be: http://mirror.sg.gs/ubuntu/"
2. Once installed, change time to IST using below command
    a. timedatectl list-timezones
    b. sudo timedatectl set-timezone "Asia Kolkata"
3. Disable UFW – pre-built firewall of ubuntu server
    a. ufw disable
    b. Check using ufw status
4. Install Net-tools – network level utilities, *if don't want to work with ubuntu server commands*
    a. sudo apt install net-tools
        i. Start using ifconfig lol
5. Configure the ethernet port now using below commands – for now consider you have two ethernet port ens1 and ens2 (change the port name according to yours)
    a. To check ethernet port name – ip addr sh

    These ethernet ports must have IP assigned by default. Make sure both the Ips are static. In case of VM environment, you must set static ip else every reboot will change the ip.

    b. Consider ens1 has IP 10.10.10.2, set ip to other port as well
    c. ifconfig ens2 up 10.10.10.3
    d. ifconfig ens2 promisc – All traffic will be routed to this port as other port is used for management
        i. Even after these things if the reboot is changing the IP, you must mention below setting in /etc/netplan/00_*_*.yml file
        ii. nano /etc/netplan/00_*_*.yml
            1. paste below line – without syntax error.
        iii. sudo netplan apply
        iv. reboot
        v. ifconfig ens1 up 10.10.10.2
        vi. ifconfig ens2 up 10.10.10.3
        vii. ifconfig ens2 promisc
        viii. sudo dhclient ens1

DEFINITIONS OF INTEGRATED PLATFORMS

1. **Elasticsearch:** Elasticsearch is a distributed, free and open search and analytics engine for all types of data, including textual, numerical, geospatial, structured, and unstructured.

Solution Installation and Operations

2. **Kibana:** Kibana is a free and open user interface that lets you visualize your Elasticsearch data and navigate the Elastic Stack. Do anything from tracking query load to understanding the way requests flow through your apps.
3. **Zeek:** Zeek is a passive, open-source network traffic analyser tool used by many operators. It analyses network traffic packets and creates "Zeek logs" which can be used to detect malicious activity within a network.
4. **Suricata:** Suricata is a high performance, open-source network analysis and threat detection software
5. **Filebeat:** Filebeat is a lightweight shipper for forwarding and centralizing log data. Installed as an agent on your servers, Filebeat monitors the log files or locations that you specify, collects log events, and forwards them either to Elasticsearch or Logstash for indexing.

ZEEK

Note: Below commands and installation is for Ubuntu - 20.04

A. Installation Commands

1. sudo apt-get update // sudo apt update
2. echo 'deb http://download.opensuse.org/repositories/security:/zeek/xUbuntu_20.04/ /' | sudo tee /etc/apt/sources.list.d/security:zeek.list
3. curl -fsSL https://download.opensuse.org/repositories/security:zeek/xUbuntu_20.04/Release.key | gpg --dearmor | sudo tee /etc/apt/trusted.gpg.d/security_zeek.gpg > /dev/null
4. sudo apt update
5. sudo apt install zeek

B. Let us configure Zeek - You must find four **"*.cfg"** files under directory /opt/zeek/etc/ post installation. (Here, I just introduced the configuration, you must follow the other configurations files attached under this repository)

1. **networks.cfg -** contains IP addresses/subnet which are required to be sniffed. Since the list is by-default in line with local IP ranges. But see if the required IP falls under the list or not. If not, then simply add in the same format in which other IPs are mentioned i.e., subnet format.
2. **node.cfg** - contains information about network interface that needs to be sniffed and about zeek's host IP details.
   Configuration
   1. vim node.cfg
      a. add, host: 10.10.10.3
      b. add, interface: ens2
   2. save it.

3. **Zeekctl.cfg→** contains actual configurations of zeek.
   Configuration: Make sure all lines present in this file are same as mentioned in sample files attached below or you can refer either note attached to point 3 attached .txt file for raw comments.

4. Now, open below file and add **@load policy/tuning/json-logs.zeek** at the end of it. Same can be seen in .txt file attached above. Below are the commands that can be followed.
   a. vim /opt/zeek/share/zeek/site/local.zeek
   b. refer guide - https://docs.zeek.org/en/master/scripts/policy/tuning/json-logs.zeek.html
   c. Write/Paste this to last line "@load policy/tuning/json-logs.zeek"
   d. This line is required to create logs in json format as this format is structured and filebeat can easily read it.

C. Post Configuration, it's time to create binaries, install, deploy and test the zeek

1. echo "export PATH=$PATH:/opt/zeek/bin" >> ~/.bashrc
2. source ~/.bashrc
3. cat ~/.bashrc
4. zeekctl
   a. zeekctl> install
   b. zeekctl> start
   c. zeekctl> deploy
   d. zeekctl> top (tell the status whether zeek is running or not)
   e. exit
5. ls -la ./logs/current (check zeek logs – you should do cd /opt/zeek/ to run this command)
6. ./zeekctl top (zeek status – open /opt/zeek/bin/ then run this command)
7. Similarly, zeek services can be started using systemctl enable zeek // systemctl start zeek // systemctl status zeek // systemctl stop zeek // service zeek enable/start/status

Suricata Installation:

Solution Installation and Operations

A. **Installation**

1. sudo add-apt-repository ppa:oisf/suricata-stable
2. sudo apt-get update && sudo apt-get install suricata -y

Note: if any error related to tmp directory means suricata enable to create files there - chmod -R 777 /tmp

B. **Configuration**

1. Vim /etc/suricata/suricata.yml → refer attached sample file and txt file attached previously.
2. Save the file and then test suricata using below commands
    a. suricata -T /etc/suricata/suricata.yml (remove error if any – run this command under /etc/suricata/)
    b. suricata-update (to remove - error - No rule files match the pattern /var/lib/suricata/rules/suricata.rules, run this command under /etc/suricata/)
    c. suricata -T /etc/suricata/suricata.yml (run this command under /etc/suricata/)
3. systemctl enable suricata // systemctl start suricata // systemctl status suricata

Filebeat Installation

A. Installation

1. wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
2. sudo apt-get install apt-transport-https
3. echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list
4. echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-7.x.list
5. apt get install filebeat

B. Configuration

1. vim /etc/filebeat/filebeat.yml
2. add
    a. hosts: ["192.168.112.170:9200"] → elasticsearch access
    b. host: "192.168.112.170:5601" → kibana access
3. save.

Now to enable filebeat to communicate with zeek and suricata.

4. Go to vim /etc/filebeat/modules.d/suricata.yml
    a. enabled: true
    b. var.paths: ["/var/log/suricata/eve.json"]
5. save. Attached is sample suricata.yml which will be used by filebeat, under this repository.

Now for zeek, https://www.elastic.co/guide/en/beats/filebeat/7.9/filebeat-module-zeek.html

6. Go to vim /etc/filebeat/modules.d/zeek.yml
    a. Add line on this link https://gist.github.com/CarlosLannister/7bfb5db332538e513ae2b963f8665e31
    b. Sample file attached for reference. First open file then visit link, you will understand what needs to be added into zeek.yml
7. Save.
8. Enable zeek module in filebeat - sudo filebeat modules enable zeek
9. Enable suricata module in filebeat - sudo filebeat modules enable suricata
10. It's time to test filebeat, Filebeat setup command - filebeat setup -e -v -c ./filebeat.yml
    a. filebeat test config - output will be ok
    b. filebeat test output -v - Output should be ok
    c. filebeat --help
    d. filebeat setup
11. systemctl enable filebeat
12. systemctl start filebeat
13. systemctl status filebeat

Elasticsearch Installation (Script-make sure you install unzip first, and script tags can be ignored if wanted to install manually)

#Install Java#

Solution Installation and Operations

```
read -p "Enter username:  " username
read -p "Enter Machine IP:  " machineIP
sudo apt update
sudo apt-get install openjdk-8-jdk -y

#Add Elastic Repo#
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee –a /etc/apt/sources.list.d/elastic-7.x.list

#Install apt-transport-https package#
sudo apt-get install apt-transport-https unzip
sudo apt-get update

#Install Elasticsearch
sudo apt-get install elasticsearch -y
sudo systemctl enable elasticsearch

#Ask Elasticsearch cluster name#
read -p "Enter cluster name: " cluster_name

# Elasticsearch configuration#
#cat > /usr/share/elasticsearch/instances.yml
sudo cat >> /usr/share/elasticsearch/instances.yml <<EOF
instances:
  - name: "elasticsearch"
    ip:
      - "$machineIP"
  - name: "kibana"
    ip:
      - "$machineIP"
EOF

sudo echo "cluster.name: "$cluster_name"" >> /etc/elasticsearch/elasticsearch.yml
sudo echo "network.host: "$machineIP"" >> /etc/elasticsearch/elasticsearch.yml
sudo cat >> /etc/elasticsearch/elasticsearch.yml <<EOF
http.port: 9200
discovery.type: single-node
xpack.security.enabled: true
xpack.security.authc.api_key.enabled: true

#xpack.security.transport.ssl#
xpack.security.transport.ssl.enabled: true
xpack.security.transport.ssl.verification_mode: certificate
xpack.security.transport.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
xpack.security.transport.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt
xpack.security.transport.ssl.certificate_authorities: ["/etc/elasticsearch/certs/ca/ca.crt"]

#xpack.security.http.ssl#

xpack.security.http.ssl.enabled: true
xpack.security.http.ssl.verification_mode: certificate
xpack.security.http.ssl.key: /etc/elasticsearch/certs/elasticsearch.key
xpack.security.http.ssl.certificate: /etc/elasticsearch/certs/elasticsearch.crt
xpack.security.http.ssl.certificate_authorities: ["/etc/elasticsearch/certs/ca/ca.crt"]

EOF

cat >> /etc/elasticsearch/jvm.options <<EOF
```

Solution Installation and Operations

```
-Xms2g
-Xmx2g
EOF


#create certificates#
#cd /usr/share/elasticsearch/
#sudo mkdir -p /usr/share/elasticsearch/ca/
#sudo /usr/share/elasticsearch/bin/elasticsearch-certutil ca --pem --out ./elastic-stack-ca.zip
#sudo unzip /usr/share/elasticsearch/elastic-stack-ca.zip
#sudo /usr/share/elasticsearch/bin/elasticsearch-certutil cert --ca-cert ca/ca.crt --ca-key ca/ca.key --pem --in instances.yml  --out certs.zip

#unzip certs#
sudo unzip /usr/share/elasticsearch/certs.zip
sudo mkdir -p ./certs/
sudo mv /usr/share/elasticsearch/elasticsearch/* ./certs/
sudo mv /usr/share/elasticsearch/kibana/* ./certs/
sudo mkdir -p /etc/kibana/certs/ca/
sudo mkdir -p /etc/elasticsearch/certs/ca/

#Copy certificates#
sudo cp /usr/share/elasticsearch/ca/ca.* /etc/elasticsearch/certs/ca/
sudo cp /usr/share/elasticsearch/ca/ca.* /etc/kibana/certs/ca/
sudo cp /usr/share/elasticsearch/certs/elasticsearch.* /etc/elasticsearch/certs/
sudo cp /usr/share/elasticsearch/certs/kibana.* /etc/kibana/certs/
sudo cp /usr/share/elasticsearch/ca/ca.crt /
sudo rm -r /usr/share/elasticsearch/elasticsearch/ /usr/share/elasticsearch/kibana/

#Change ownership#
cd /usr/share/
sudo chown -R elasticsearch:elasticsearch elasticsearch/
sudo chown -R elasticsearch:elasticsearch /etc/elasticsearch/
cd /usr/share/elasticsearch/
sudo chown -R elasticsearch:elasticsearch certs/
sudo chown -R elasticsearch:elasticsearch ca/

#Elasticsearch service#
sudo systemctl start elasticsearch
sudo systemctl status elasticsearch

#Create passwords
cd /usr/share/elasticsearch/
#sudo touch /home/$username/passwords.txt
#read -p "Press y to create password" password
#echo $password
#sudo ./bin/elasticsearch-setup-passwords auto 1> /home/$username/passwords.txt
#kibana_password = `cat /home/$username/passwords.txt | grep "PASSWORD kibana_system" | cut -d '=' -f 2`



#Install Kibana
sudo apt-get install kibana -y

cat >> /etc/kibana/kibana.yml <<EOF
server.host: $machineIP
server.port: 5601
server.publicBaseUrl: https://$machineIP
elasticsearch.hosts: ["https://$machineIP:9200"]

elasticsearch.username: "kibana_system"
```

elasticsearch.password: "$kibana_password"

server.ssl.enabled: true
server.ssl.certificate: "/etc/kibana/certs/kibana.crt"
server.ssl.key: "/etc/kibana/certs/kibana.key"

xpack.encryptedSavedObjects.encryptionKey: 3c7cd13abcc677fff24c49755a3883ce
xpack.reporting.encryptionKey: a74e79eb9b8b3ac83acc4ae6091b1689
xpack.security.encryptionKey: 18856156b26c268d3800a60961e10817
xpack.security.session.idleTimeout: "30m"

elasticsearch.ssl.certificateAuthorities: ["/etc/kibana/certs/ca/ca.crt"]
elasticsearch.ssl.certificate: "/etc/kibana/certs/kibana.crt"
elasticsearch.ssl.key: "/etc/kibana/certs/kibana.key"

EOF

#Kibana service#
sudo systemctl enable kibana
sudo systemctl start kibana
sudo systemctl status kibana

script ends here….
**********Now commands related to password generation, needs to be executed manually**********
Stop kibana service – systemctl stop kibana
sudo ./bin/elasticsearch-setup-passwords auto 1> /home/passwords.txt
press “q” and hit enter. Password file will be generated. And add kibana_system password in kibana.yml file and restart services.

Logstash Installation (If Required)

Definition: An open source, server-side data processing pipeline.
Guide: Visit Elasticsearch official web pages

Installation

1. apt install logstash (check if logstash is running or not - ps -ef|grep logstash)
2. apt-get install logstash
3. Note: cd /etc/logstash/conf.d/ → create filters here, watch youtube videos or web links for guide.
4. sudo systemctl enable logstash
5. sudo systemctl start logstash
6. sudo systemctl status logstash
7. run grok filter file using below command /usr/share/logstash/bin/logstash -f /etc/logstash/conf.d/apache.conf

---

For Multi Sensor at one location (need to configure below line before filebeat setup)

1. output.elasticsearch.index: "bb-network-%{[agent.version]}-%{+yyyy.MM.dd}"
2. setup.ilm.enabled: false
3. #setup.ilm.overwrite: true
4. setup.template.name: "bb-network"
5. setup.template.pattern: "bb-network-*"

Then visit kibana and create index pattern. Successful creation of pattern will results visibility of new Index.

Errors Observed and commands to resolve them

1. run pcap for demo over zeek
   tcpreplay -v -i ens38 "pcaplocation"

Solution Installation and Operations

2. Error of suricata on kibana dashboard.

   "Elastic search > discover > search "event.module" to check whether zeek or suricata added or not" if not then run below for suricata

   suricata -c /etc/suricata/suricata.yaml -i ens38 -v (manually feed or supply pcap/traffic)

3. Unable to create actions client because the Encrypted Saved Objects plugin is missing encryption key.
   Please set xpack.encryptedSavedObjects.encryptionKey in the kibana.yml or use the bin/kibana-encryption-keys command.
   cd /usr/share/kibana -→ Run below command if any error related to above lines
   ./bin/kibana-encryption-keys

   output will be similar to below
   xpack.encryptedSavedObjects.encryptionKey: 4555f3603ea947d2858798334b5aac1d
   xpack.reporting.encryptionKey: 40b8d7c4d9accf11702c275c38179d01
   xpack.security.encryptionKey: 0febf74da25b30fcadf9c70e3412f3db

   paste all in kibana.yml

   go to kibana > security > rules > select all > bulk action > activate (some may fail as require ML etc)

4. Convert security keys using below commands
   openssl pkcs12 -in ./elastic-certificates.p12 -out elastic.crt -nokeys
   openssl pkcs12 -in ./elastic-certificates.p12 -out elastic.key -nocerts

5. Use this curl on the host on which Elasticsearch is installed to get a list of all Elasticsearch indices:
   curl -XGET 'localhost:9200/_cat/indices?v&pretty'

6. Failed to start elasticsearch.service: Unit elasticsearch.service failed to load: No such file or directory.

   Solution:
   sudo /bin/systemctl daemon-reload
   sudo /bin/systemctl enable elasticsearch.service
   sudo systemctl start elasticsearch.service

7. Job for elasticsearch.service failed because the control process exited with error code.

   Solution:
   visit configuration file and check unessessary "space"
   check error using - systemctl status elasticsearch.service" and "journalctl -xeu elasticsearch.service
   enable the service and start again

==========