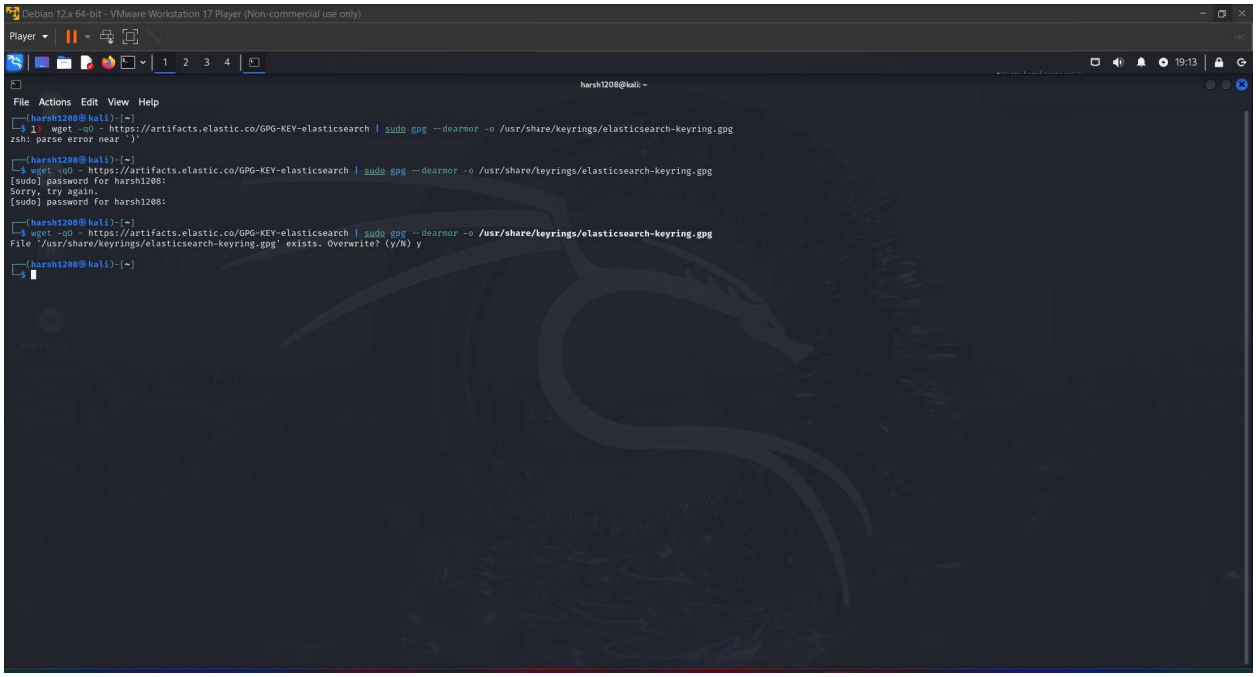
1. Install ElasticSearch (and Kibana), and install Nifi on a KALI VM

INSTALL ELASTICSEARCH

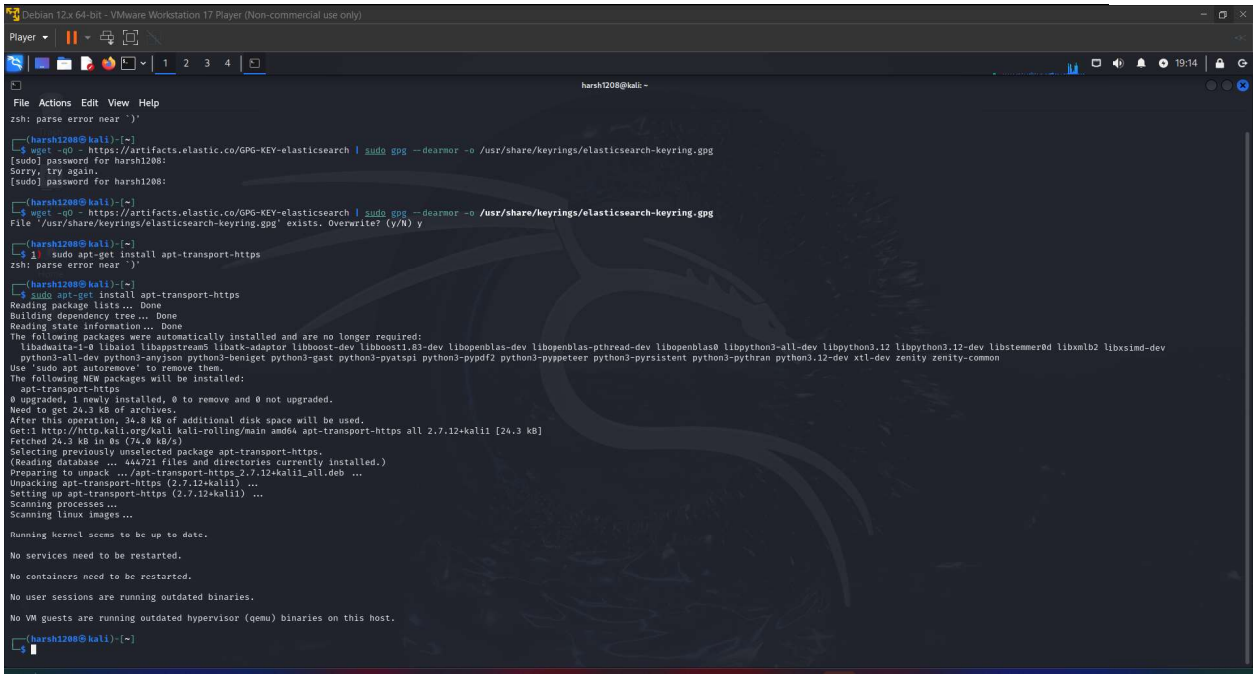
Import the Elasticsearch PGP Key

1) wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

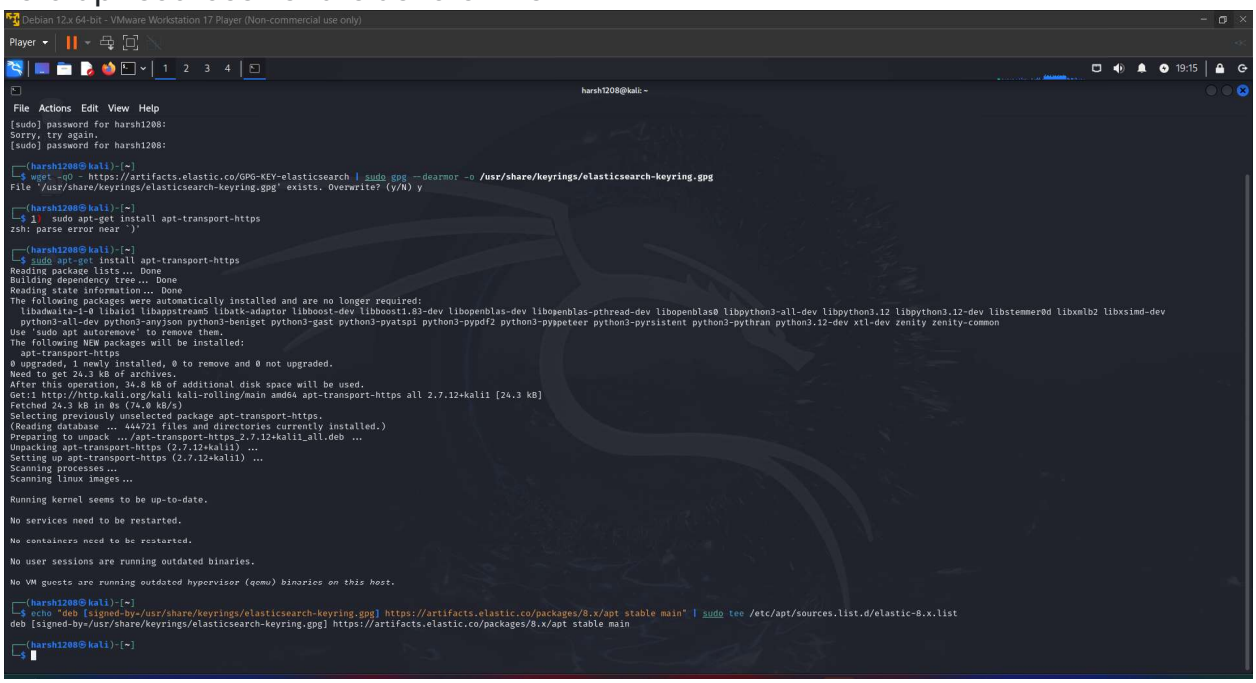


Installing from the APT repository

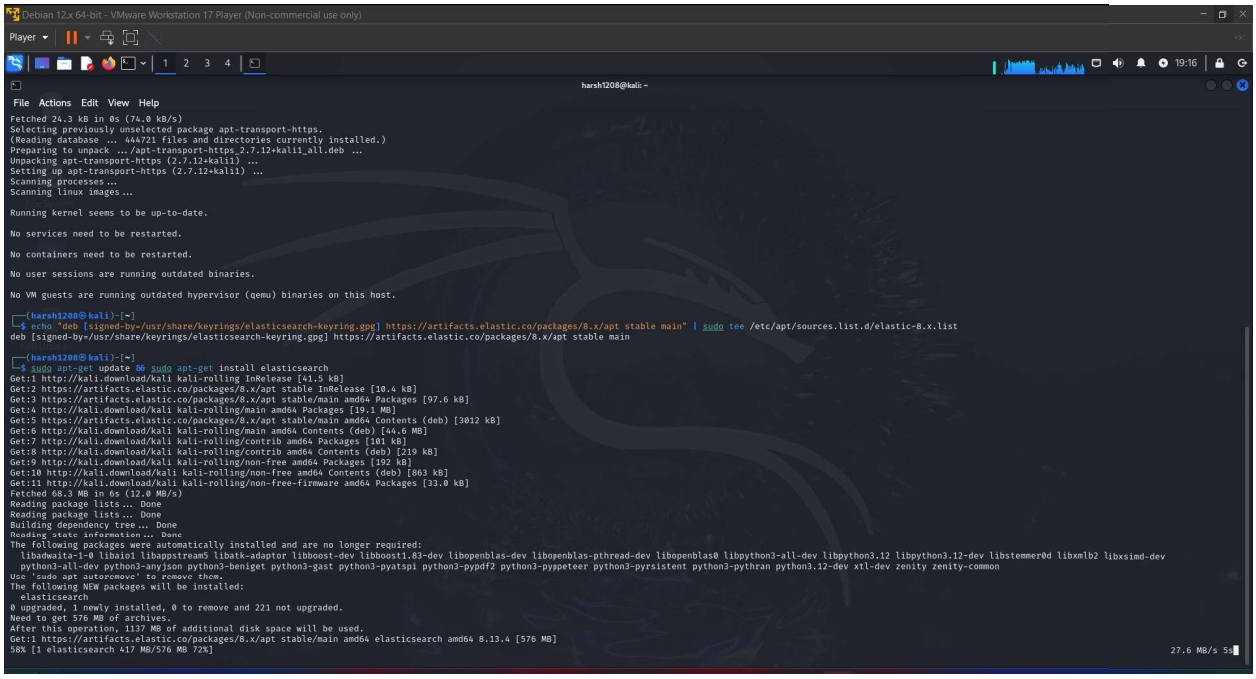
1) sudo apt-get install apt-transport-https



2) echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list



3) sudo apt-get update && sudo apt-get install elasticsearch



Running Elasticsearch with `systemd`

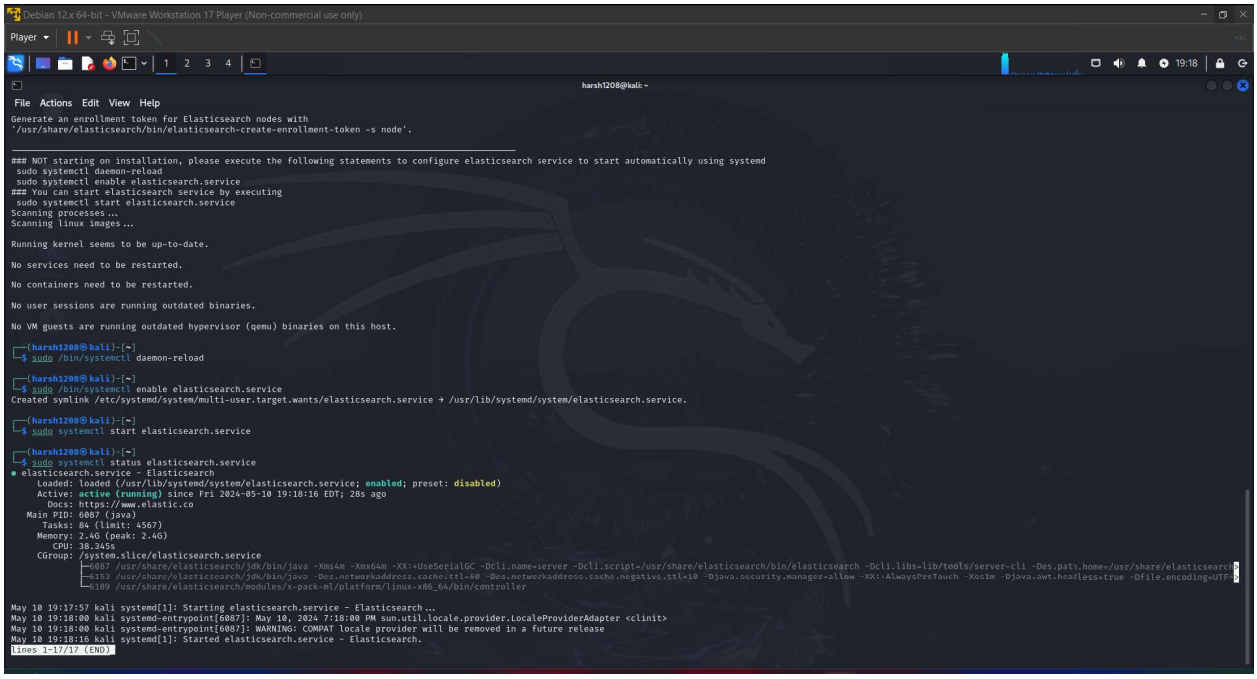
sudo /bin/systemctl daemon-reload

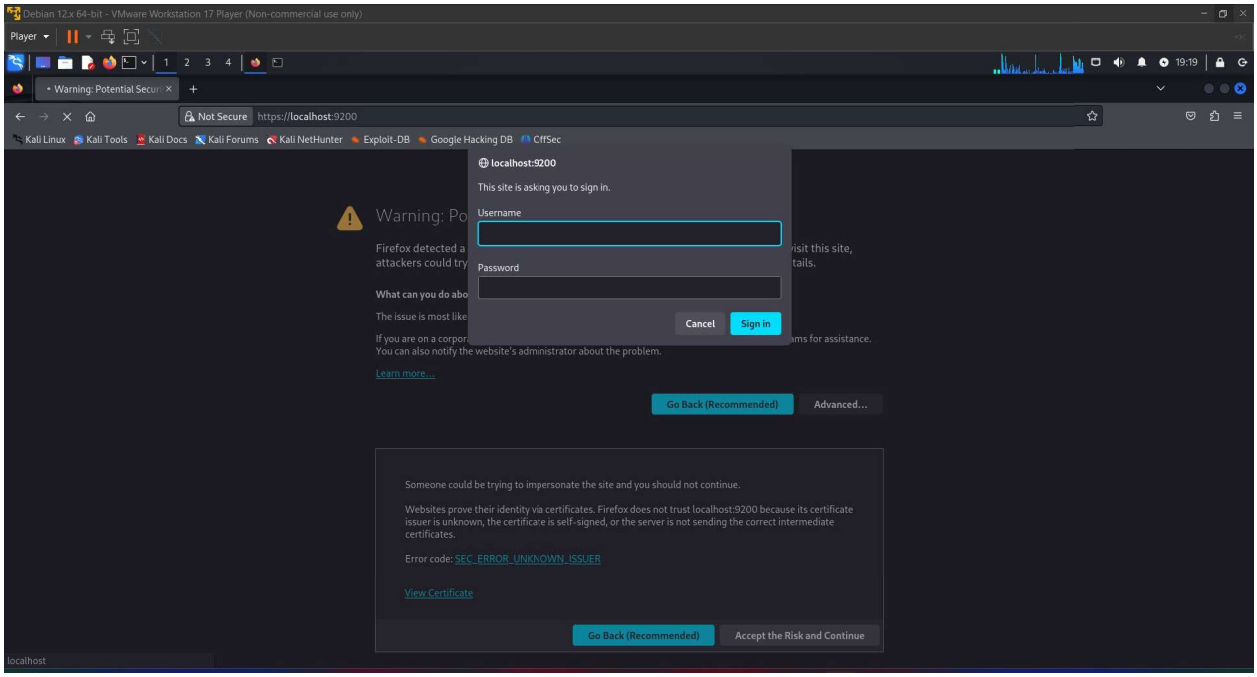
sudo /bin/systemctl enable elasticsearch.service

Elasticsearch can be started and stopped as follows:

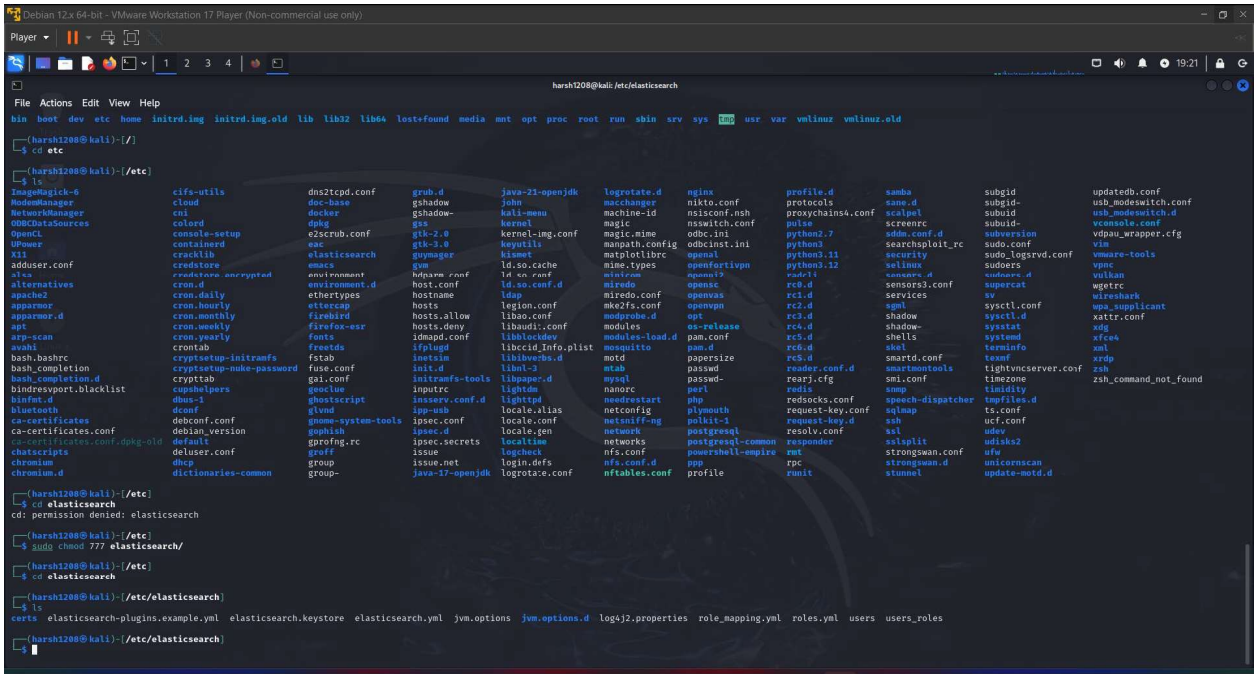
sudo systemctl start elasticsearch.service

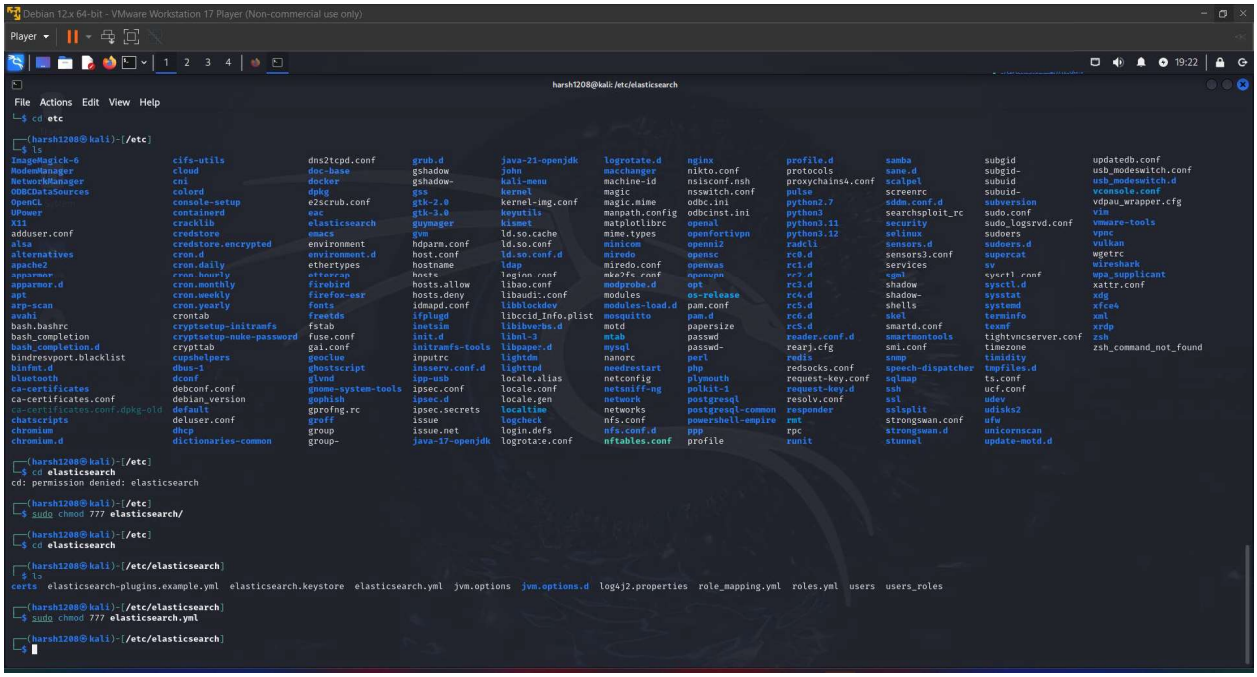
sudo systemctl stop elasticsearch.service



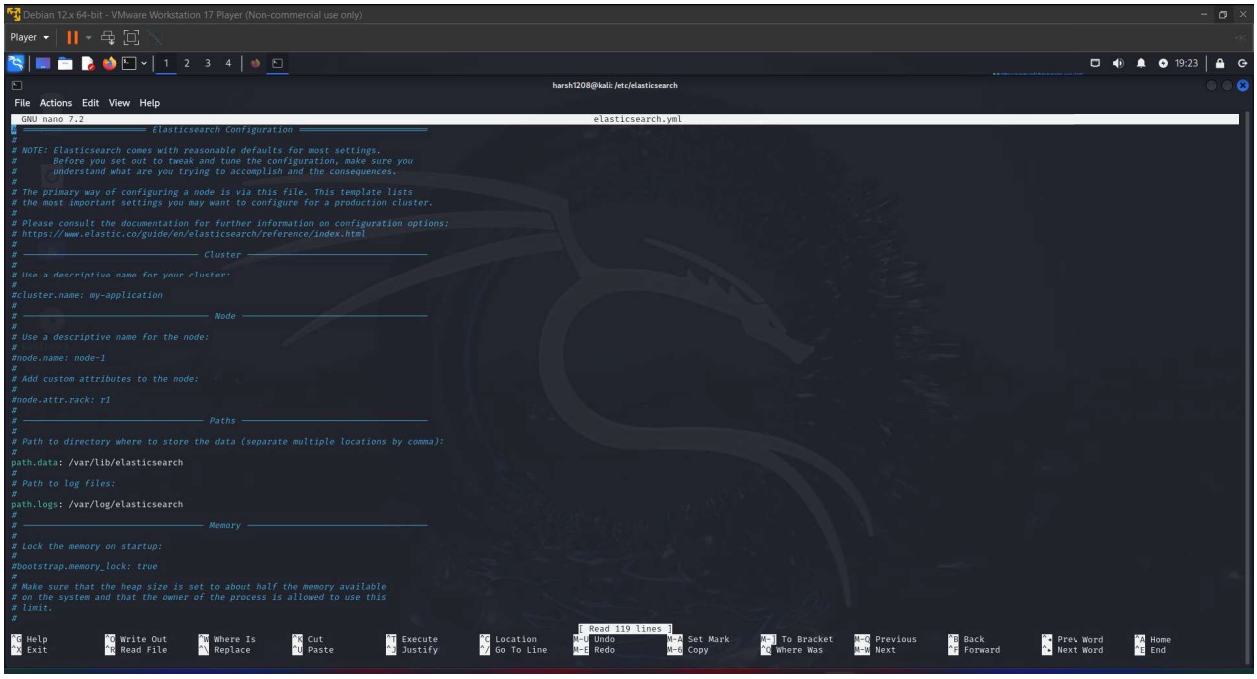


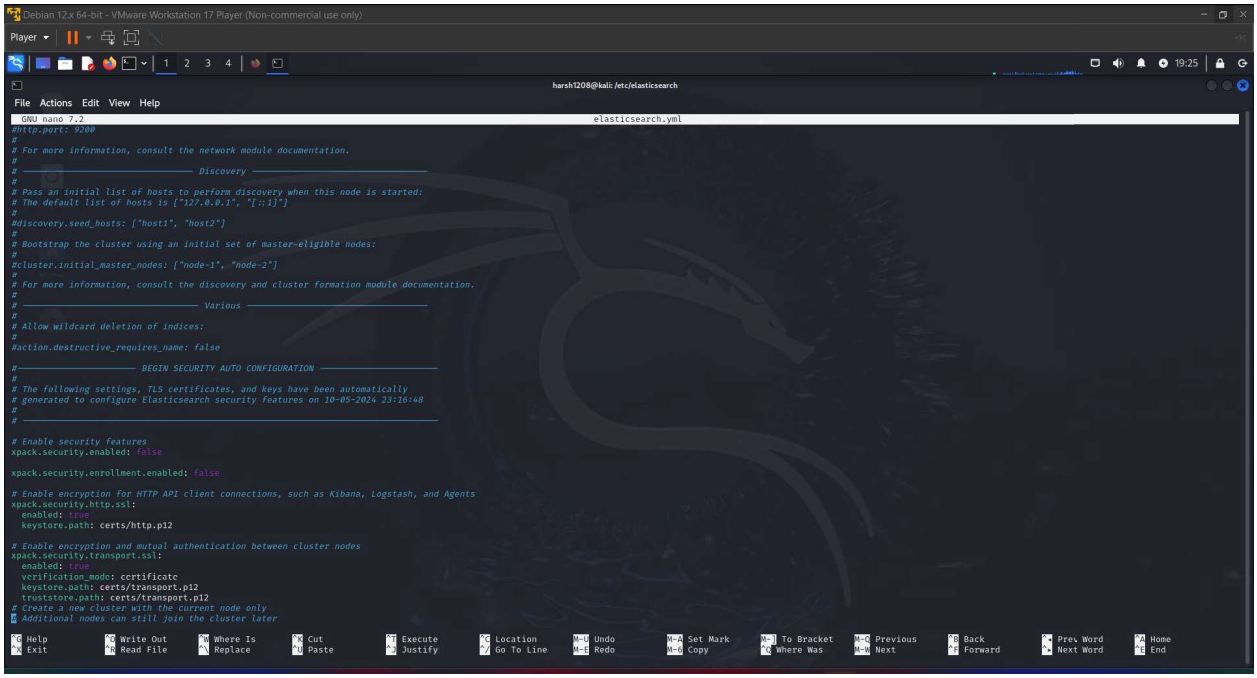
Start Elasticsearch without username and password (disable security settings):

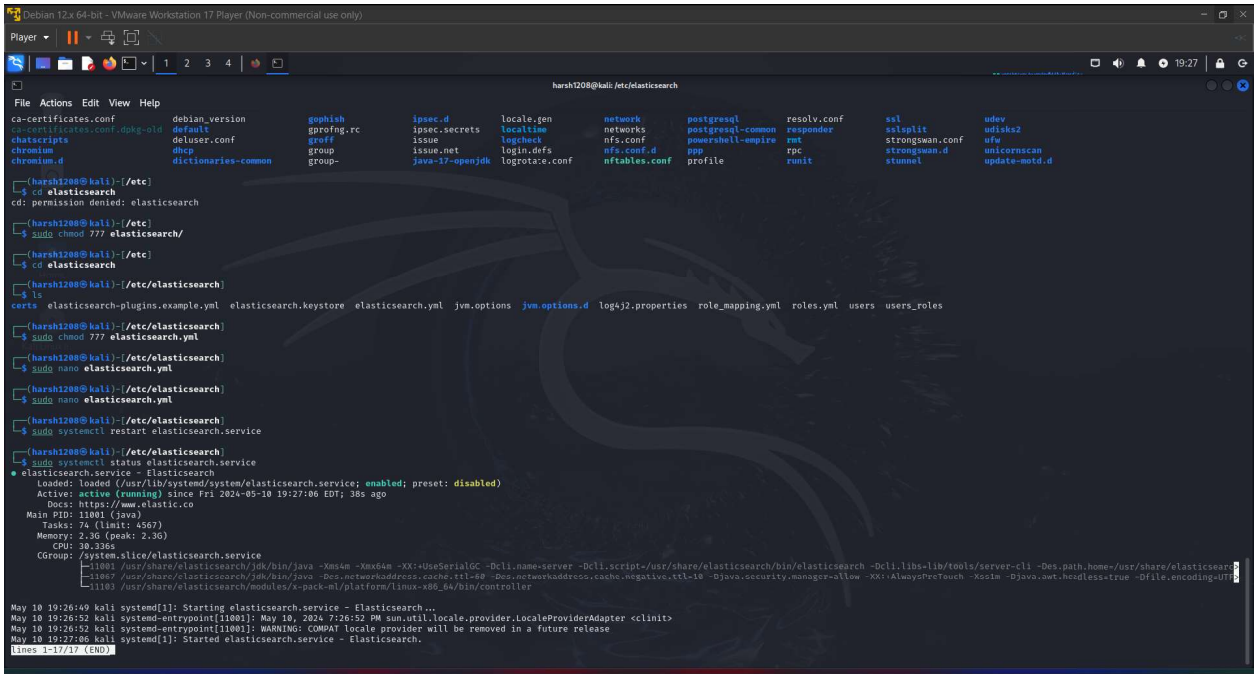


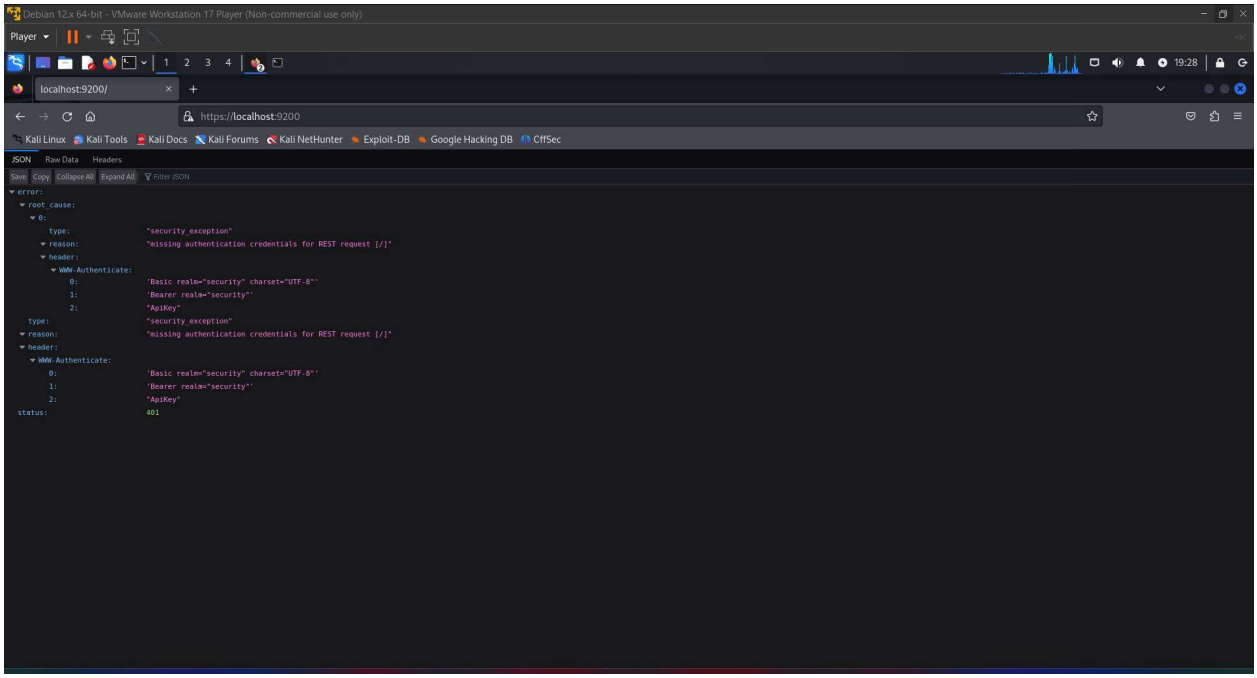


Open yml file


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
19:23
harsh1208@kali: /etc/elasticsearch
File Actions Edit View Help
GNU nano 7.2 elasticsearch.yml
======== Elasticsearch Configuration =========
NOTE: Elasticsearch comes with reasonable defaults for most settings.
Before you set out to tweak and tune the configuration, make sure you
understand what are you trying to accomplish and the consequences.
The primary way of configuring a node is via this file. This template lists
the most important settings you may want to configure for a production cluster.
Please consult the documentation for further information on configuration options:
https://www.elastic.co/guide/en/elasticsearch/reference/index.html
---------- Cluster -----------
#cluster.name: my-application
---------- Node -----------
Use a descriptive name for the node:
#node.name: node-1
Add custom attributes to the node:
#node.attr.rack: r1
---------- Paths -----------
Path to directory where to store the data (separate multiple locations by comma):
path.data: /var/lib/elasticsearch
Path to log files:
path.logs: /var/log/elasticsearch
---------- Memory -----------
Lock the memory on startup:
#bootstrap.memory_lock: true
Make sure that the heap size is set to about half the memory available
on the system and that the owner of the process is allowed to use this
limit.
[Read 119 lines]
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous M-B Back M-Left Prev Word M-/ Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward M-Right Next Word M-? End


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
19:25
harsh1208@kali: /etc/elasticsearch
File Actions Edit View Help
GNU nano 7.2 elasticsearch.yml
#http.port: 9200
For more information, consult the network module documentation.
---------- Discovery -----------
Pass an initial list of hosts to perform discovery when this node is started:
The default list of hosts is ["127.0.0.1", "[::1]"]
#discovery.seed_hosts: ["host1", "host2"]
Bootstrap the cluster using an initial set of master-eligible nodes:
#cluster.initial_master_nodes: ["node-1", "node-2"]
For more information, consult the discovery and cluster formation module documentation.
---------- Various -----------
Allow wildcard deletion of indices:
#action.destructive_requires_name: false
#---------------------- BEGIN SECURITY AUTO CONFIGURATION -----------------------
The following settings, TLS certificates, and keys have been automatically
generated to configure Elasticsearch security features on 10-05-2024 23:16:48
Enable security features
xpack.security.enabled: false
xpack.security.enrollment.enabled: false
Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
xpack.security.http.ssl:
enabled: true
keystore.path: certs/http.p12
Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
enabled: true
verification_mode: certificate
keystore.path: certs/transport.p12
truststore.path: certs/transport.p12
Create a new cluster with the current node only
Additional nodes can still join the cluster later
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-Q Previous M-B Back M-Left Prev Word M-/ Home
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^Q Where Was M-W Next ^F Forward M-Right Next Word M-? End


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
19:27
harsh1208@kali: /etc/elasticsearch
File Actions Edit View Help
ca-certificates.conf debian_version gophish ipsec.d locale.gen network postgresql resolv.conf ssl udev
ca-certificates.conf.dpkg-old default gprofng.rc ipsec.secrets localtime networks postgresql-common responder sslsplit udisks2
chatscripts deluser.conf groff issue logcheck nfs.conf powershell-empire rmt strongswan.conf ufw
chromium dhcp group issue.net login.defs nfs.conf.d ppp rpc strongswan.d unicornscan
chromium.d dictionaries-common group- java-17-openjdk logrotate.conf nftables.conf profile runit stunnel update-motd.d
(harsh1208㉿kali)-[/etc]
$ cd elasticsearch
cd: permission denied: elasticsearch
(harsh1208㉿kali)-[/etc]
$ sudo chmod 777 elasticsearch/
(harsh1208㉿kali)-[/etc]
$ cd elasticsearch
(harsh1208㉿kali)-[/etc/elasticsearch]
$ ls
certs elasticsearch-plugins.example.yml elasticsearch.keystore elasticsearch.yml jvm.options jvm.options.d log4j2.properties role_mapping.yml roles.yml users users_roles
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo chmod 777 elasticsearch.yml
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo nano elasticsearch.yml
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo nano elasticsearch.yml
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo systemctl restart elasticsearch.service
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: disabled)
Active: active (running) since Fri 2024-05-10 19:27:06 EDT; 38s ago
Docs: https://www.elastic.co
Main PID: 11001 (java)
Tasks: 74 (limit: 4567)
Memory: 2.3G (peak: 2.3G)
CPU: 30.336s
CGroup: /system.slice/elasticsearch.service
├─11001 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearch/bin/elasticsearch -Dcli.libs=lib/tools/server-cli -Des.path.home=/usr/share/elasticsearch
├─11067 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.cache.ttl=60 -Des.networkaddress.cache.negative.ttl=10 -Djava.security.manager=allow -XX:+AlwaysPreTouch -Xss1m -Djava.awt.headless=true -Dfile.encoding=UTF-8
└─11103 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x86_64/bin/controller
May 10 19:26:49 kali systemd[1]: Starting elasticsearch.service - Elasticsearch...
May 10 19:26:52 kali systemd-entrypoint[11001]: May 10, 2024 7:26:52 PM sun.util.locale.provider.LocaleProviderAdapter <clinit>
May 10 19:26:52 kali systemd-entrypoint[11001]: WARNING: COMPAT locale provider will be removed in a future release
May 10 19:27:06 kali systemd[1]: Started elasticsearch.service - Elasticsearch.
lines 1-17/17 (END)


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
19:28
localhost:9200/
https://localhost:9200
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
error:
root_cause:
0:
type: "security_exception"
reason: "missing authentication credentials for REST request [/]"
header:
WWW-Authenticate:
0: 'Basic realm="security" charset="UTF-8"'
1: 'Bearer realm="security"'
2: "ApiKey"
type: "security_exception"
reason: "missing authentication credentials for REST request [/]"
header:
WWW-Authenticate:
0: 'Basic realm="security" charset="UTF-8"'
1: 'Bearer realm="security"'
2: "ApiKey"
status: 401

INSTALL KIBINA

Download Kibana at:

Import the Elastic PGP key

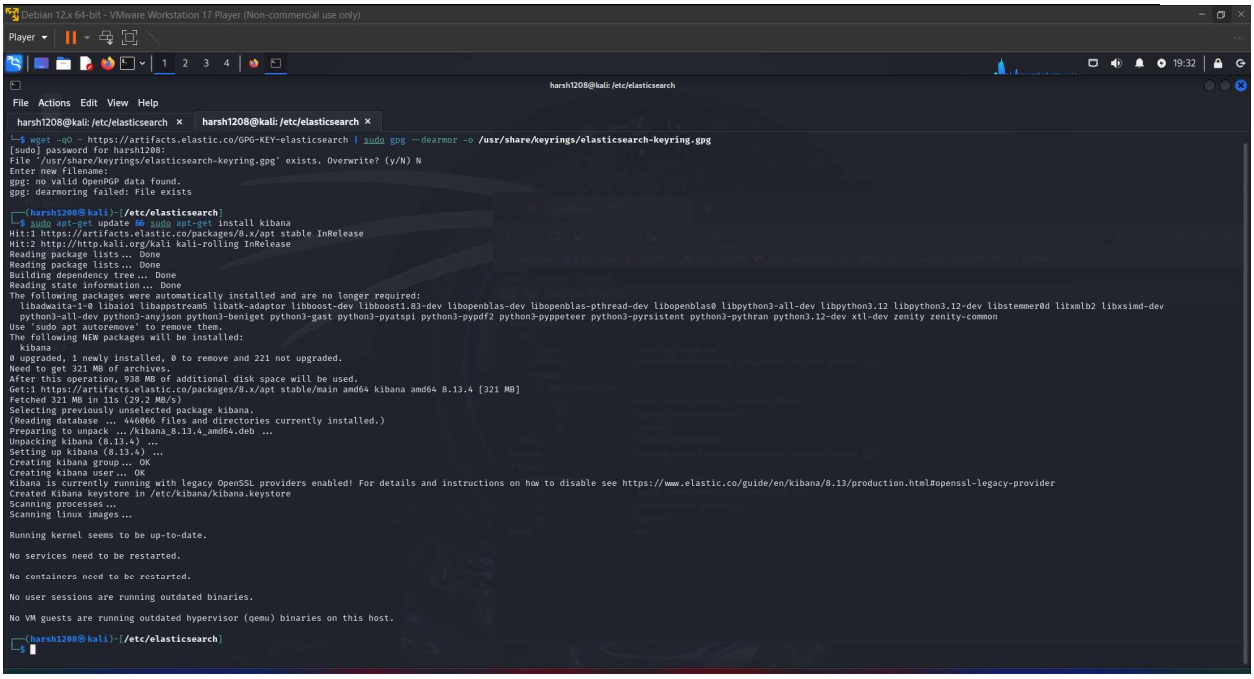
1) wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

Install from the APT repository

1)sudo apt-get install apt-transport-https
2)echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

You can install the Kibana Debian package with:

sudo apt-get update && sudo apt-get install kibana



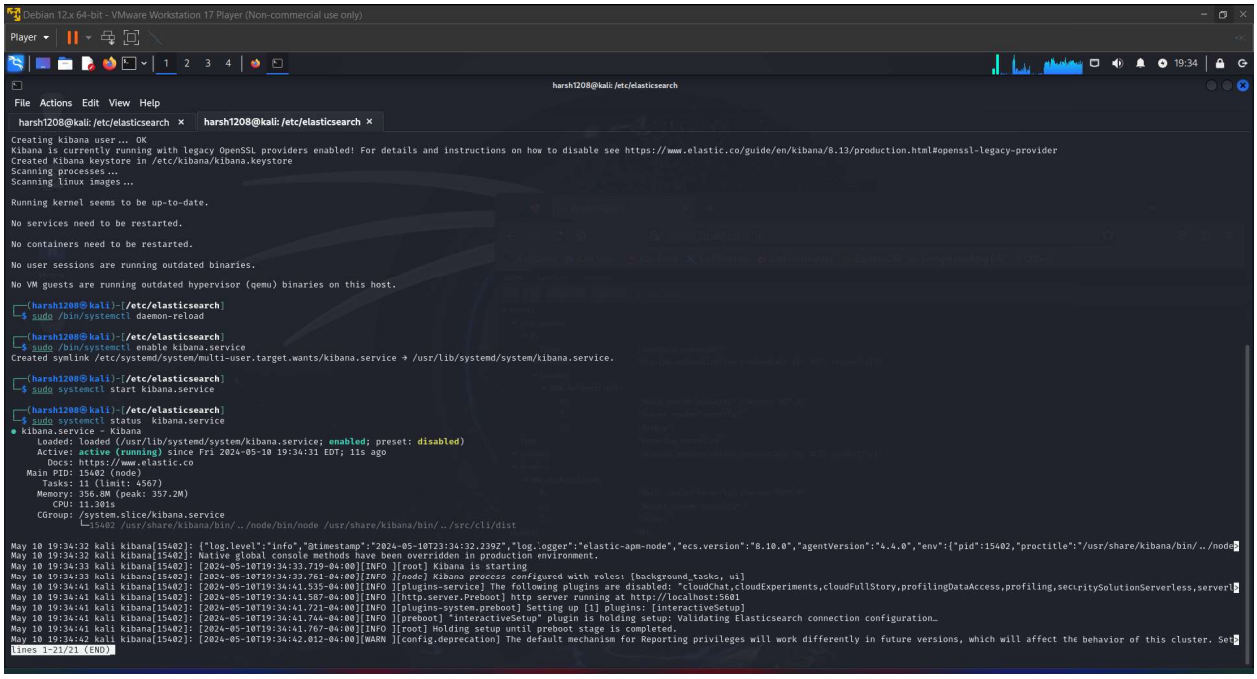
Run Kibana with `system`

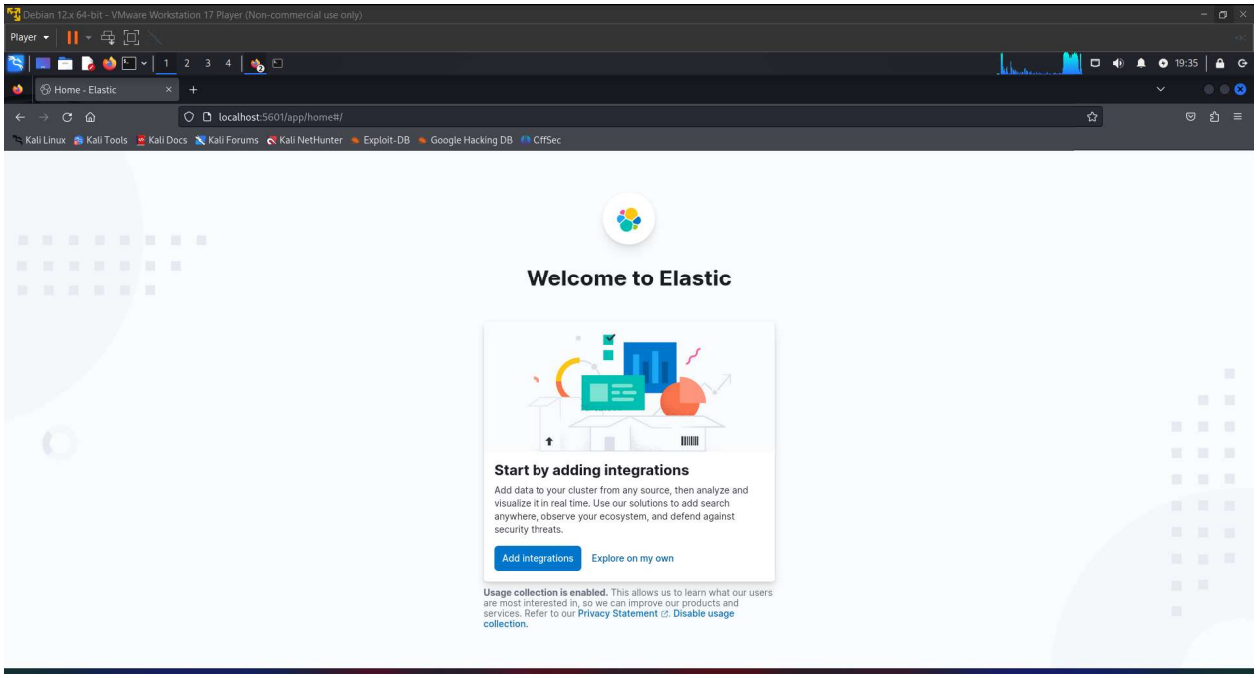
sudo /bin/systemctl daemon-reload

sudo /bin/systemctl enable kibana.service

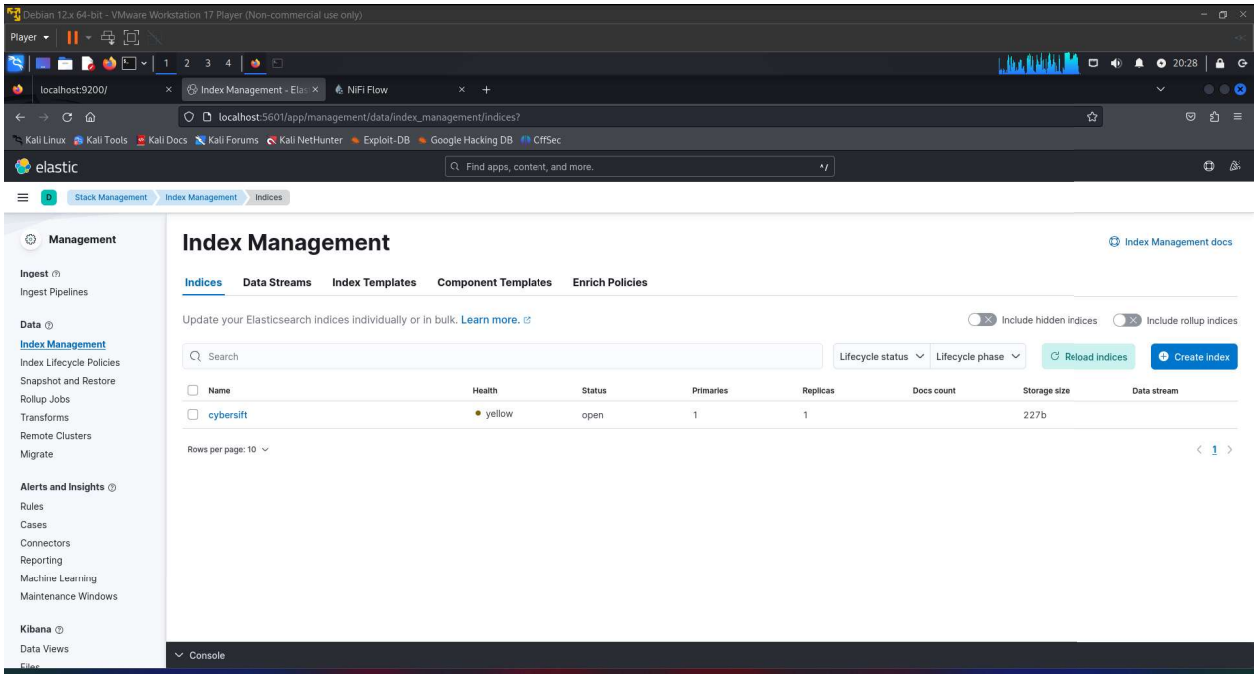
sudo systemctl start kibana.service

sudo systemctl stop kibana.service


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
harsh1208@kali: /etc/elasticsearch
File Actions Edit View Help
harsh1208@kali: /etc/elasticsearch
harsh1208@kali: /etc/elasticsearch
Creating kibana user ... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.13/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
Scanning processes ...
Scanning linux images ...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo /bin/systemctl daemon-reload
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo /bin/systemctl enable kibana.service
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /usr/lib/systemd/system/kibana.service.
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo systemctl start kibana.service
(harsh1208㉿kali)-[/etc/elasticsearch]
$ sudo systemctl status kibana.service
● kibana.service - Kibana
Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: disabled)
Active: active (running) since Fri 2024-05-10 19:34:31 EDT; 11s ago
Docs: https://www.elastic.co
Main PID: 15402 (node)
Tasks: 11 (limit: 4567)
Memory: 356.8M (peak: 357.2M)
CPU: 11.301s
CGroup: /system.slice/kibana.service
└─15402 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/../src/cli/dist
May 10 19:34:32 kali kibana[15402]: {"log.level":"info","@timestamp":"2024-05-10T23:34:32.239Z","log.logger":"elastic-apm-node","ecs.version":"8.10.0","agentVersion":"4.4.0","env":{"pid":15402,"proctitle":"/usr/share/kibana/bin/../node
May 10 19:34:32 kali kibana[15402]: Native global console methods have been overridden in production environment.
May 10 19:34:33 kali kibana[15402]: [2024-05-10T19:34:33.719-04:00][INFO][root] Kibana is starting
May 10 19:34:33 kali kibana[15402]: [2024-05-10T19:34:33.761-04:00][INFO][node] Kibana process configured with roles: [background_tasks, ui]
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.535-04:00][INFO][plugins-service] The following plugins are disabled: "cloudChat,cloudExperiments,cloudFullStory,profilingDataAccess,profiling,securitySolutionServerless,serverl
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.587-04:00][INFO][http.server.Preboot] http server running at http://localhost:5601
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.721-04:00][INFO][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup]
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.744-04:00][INFO][preboot] "interactiveSetup" plugin is holding setup: Validating Elasticsearch connection configuration…
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.767-04:00][INFO][root] Holding setup until preboot stage is completed.
May 10 19:34:42 kali kibana[15402]: [2024-05-10T19:34:42.012-04:00][WARN][config.deprecation] The default mechanism for Reporting privileges will work differently in future versions, which will affect the behavior of this cluster. Set
lines 1-21/21 (END)

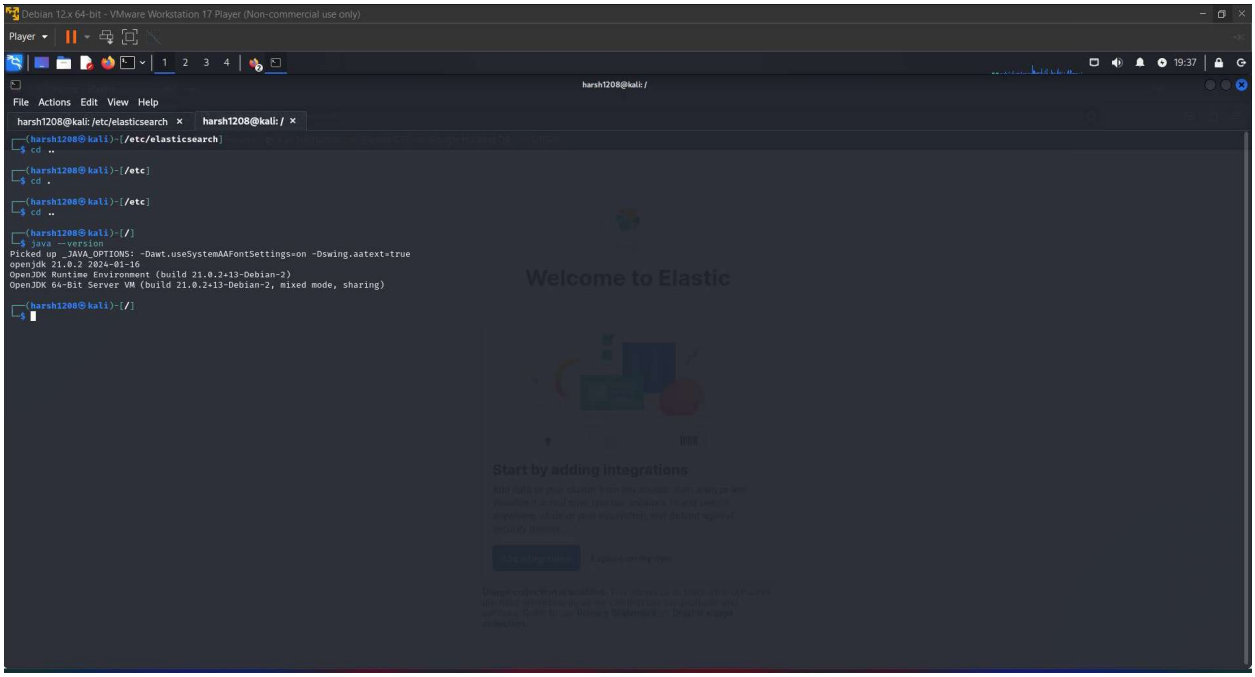

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Home - Elastic
localhost:5601/app/home#/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB CffSec
Welcome to Elastic
Start by adding integrations
Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.
Add integrations
Explore on my own
Usage collection is enabled. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our Privacy Statement. Disable usage collection.

Create Index

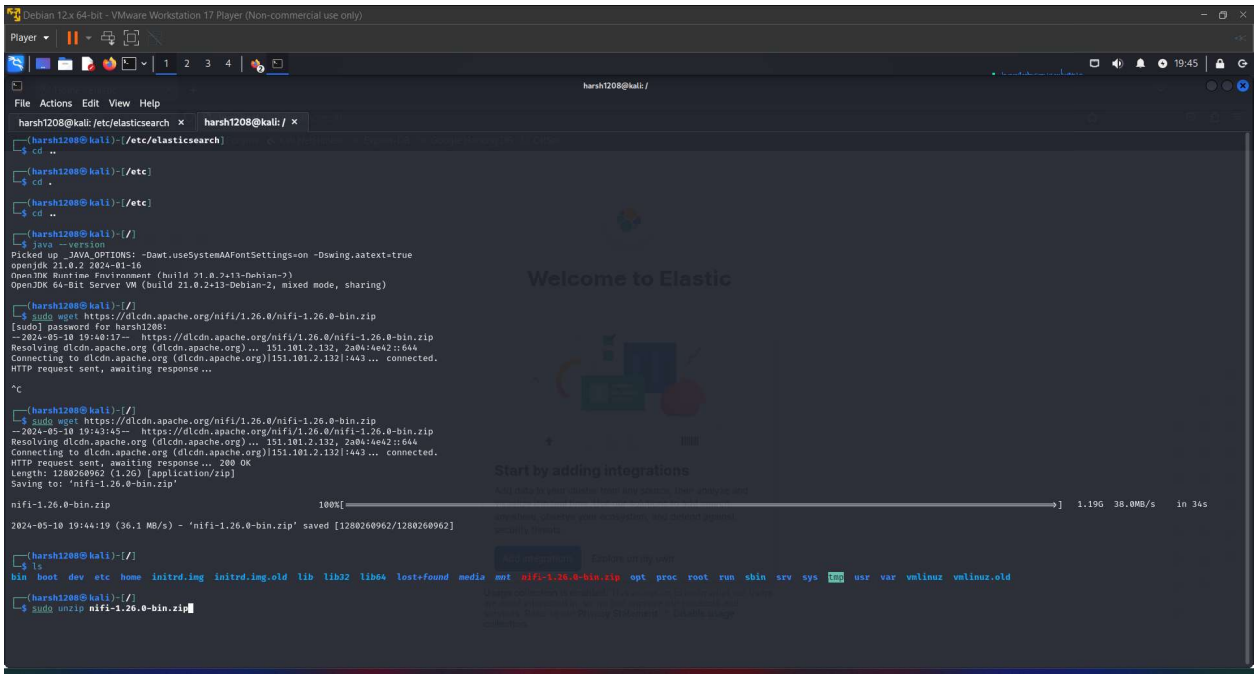


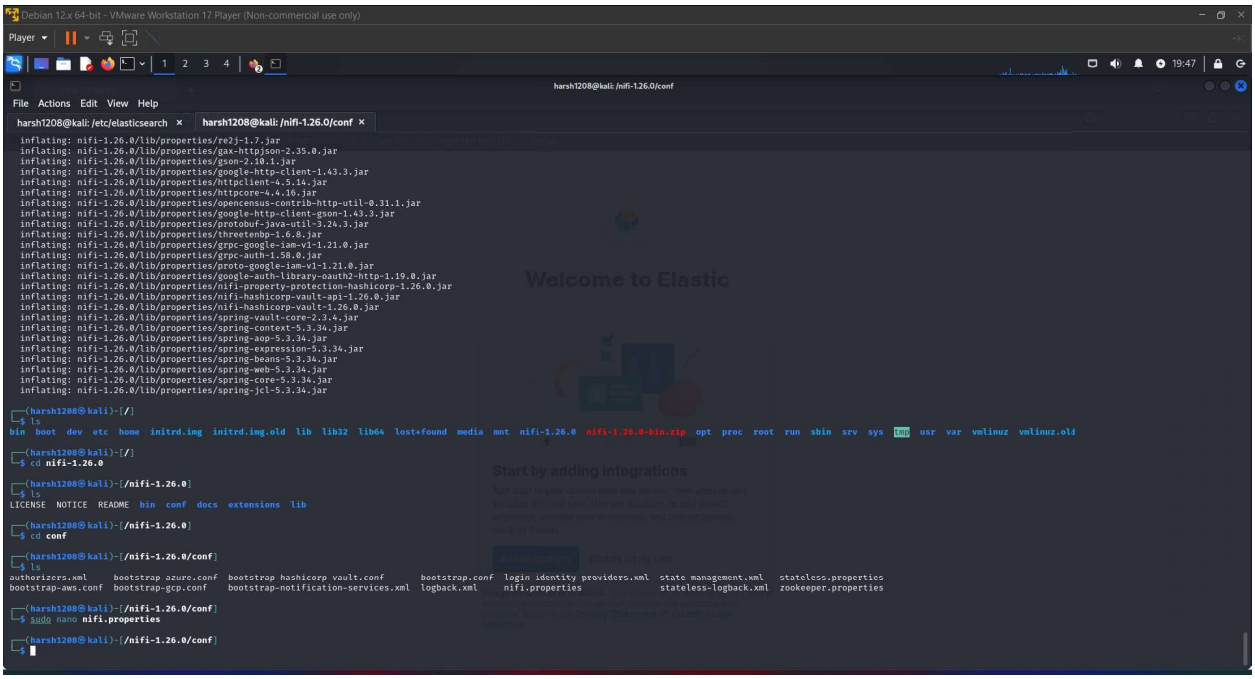
Install Apache Nifi

Install java:



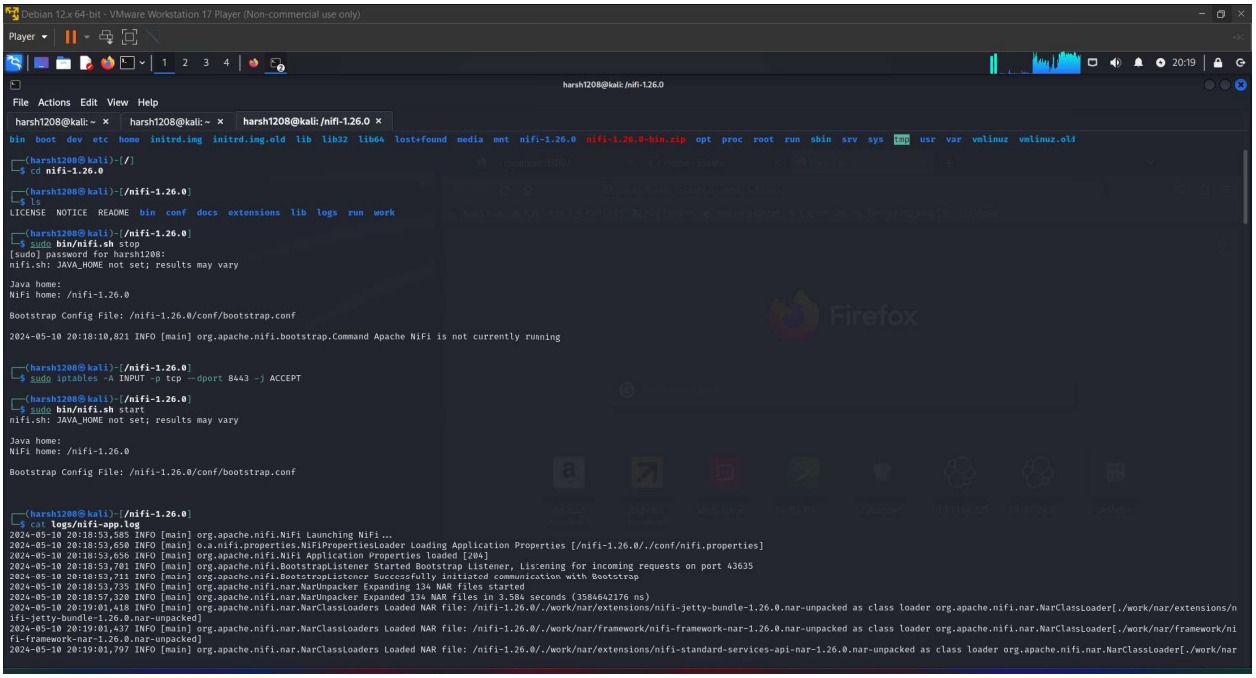
WGET NIFI

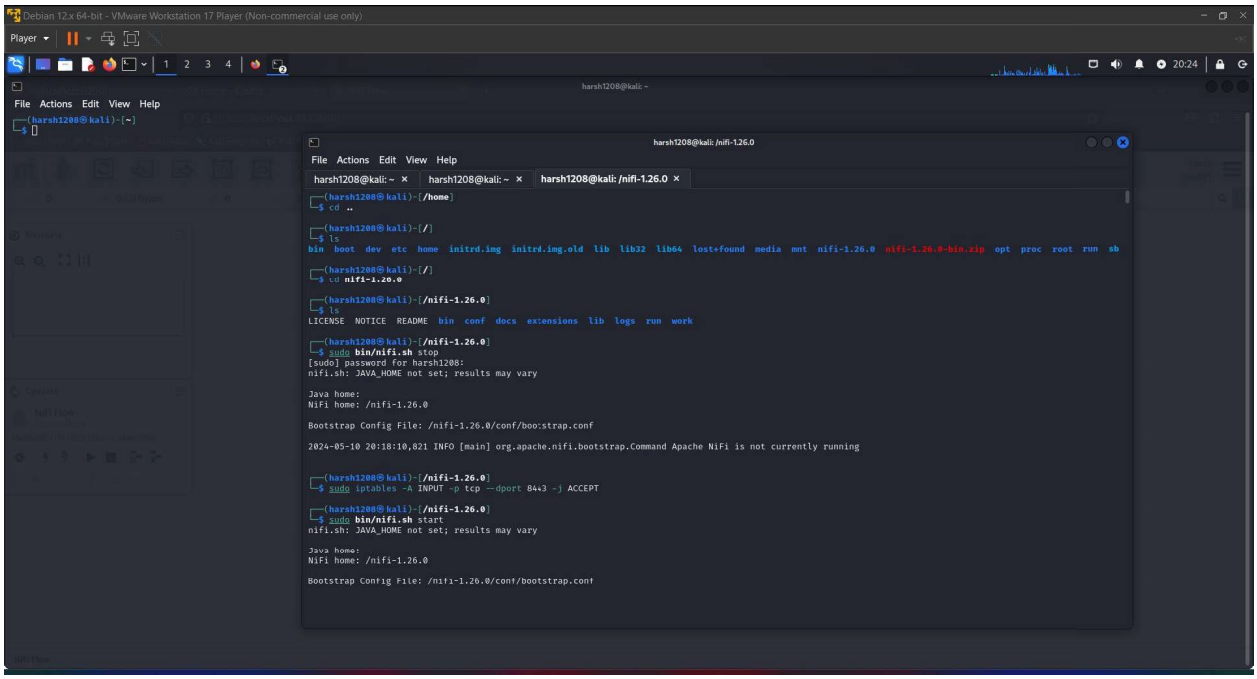

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
harsh1208@kali: /
File Actions Edit View Help
harsh1208@kali: /etc/elasticsearch
harsh1208@kali: /
(harsh1208㉿kali)-[/etc/elasticsearch]
$ cd ..
(harsh1208㉿kali)-[/etc]
$ cd .
(harsh1208㉿kali)-[/etc]
$ cd ..
(harsh1208㉿kali)-[/]
$ java --version
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true
openjdk 21.0.2 2024-01-16
OpenJDK Runtime Environment (build 21.0.2+13-Debian-2)
OpenJDK 64-Bit Server VM (build 21.0.2+13-Debian-2, mixed mode, sharing)
(harsh1208㉿kali)-[/]
$ sudo wget https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip
[sudo] password for harsh1208:
--2024-05-10 19:40:17-- https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip
Resolving dlcdn.apache.org (dlcdn.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to dlcdn.apache.org (dlcdn.apache.org)|151.101.2.132|:443... connected.
HTTP request sent, awaiting response...
^C
(harsh1208㉿kali)-[/]
$ sudo wget https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip
--2024-05-10 19:43:45-- https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip
Resolving dlcdn.apache.org (dlcdn.apache.org)... 151.101.2.132, 2a04:4e42::644
Connecting to dlcdn.apache.org (dlcdn.apache.org)|151.101.2.132|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1280260962 (1.2G) [application/zip]
Saving to: 'nifi-1.26.0-bin.zip'
nifi-1.26.0-bin.zip 100%[=====>] 1.19G 38.0MB/s in 34s
2024-05-10 19:44:19 (36.1 MB/s) - 'nifi-1.26.0-bin.zip' saved [1280260962/1280260962]
(harsh1208㉿kali)-[/]
$ ls
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 lost+found media mnt nifi-1.26.0-bin.zip opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
(harsh1208㉿kali)-[/]
$ sudo unzip nifi-1.26.0-bin.zip

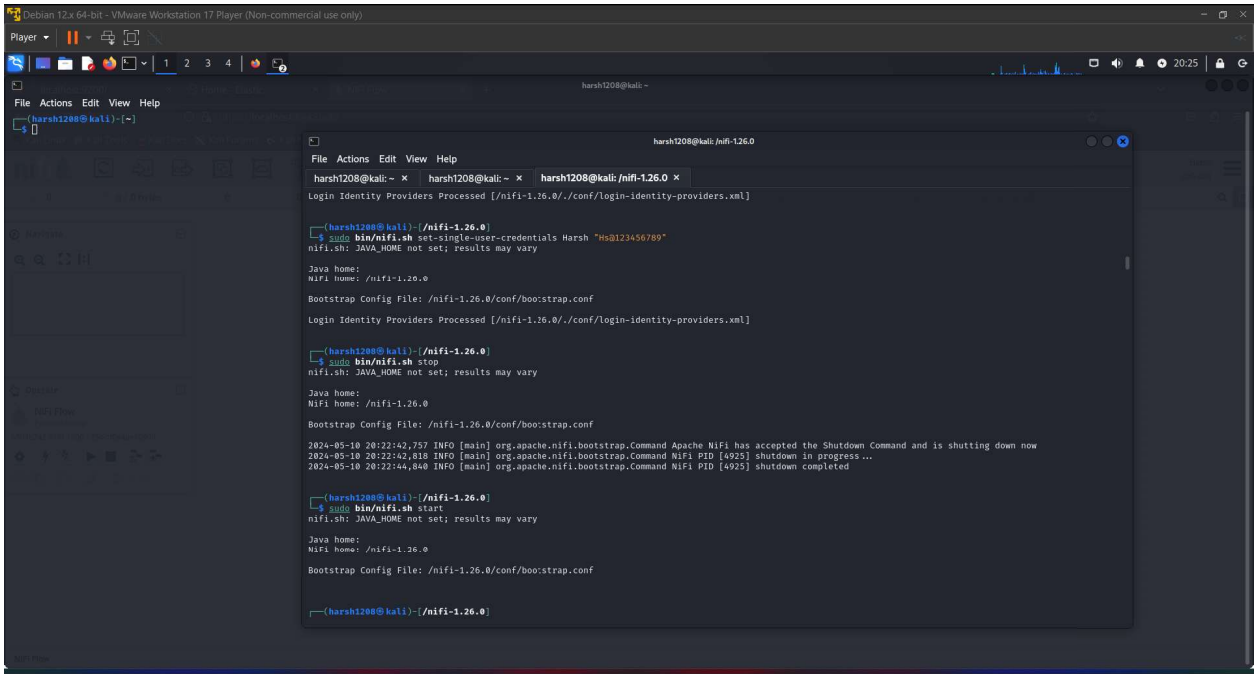

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
harsh1208@kali: /nifi-1.26.0/conf
File Actions Edit View Help
harsh1208@kali: /etc/elasticsearch
harsh1208@kali: /nifi-1.26.0/conf
inflating: nifi-1.26.0/lib/properties/re2j-1.7.jar
inflating: nifi-1.26.0/lib/properties/gax-httpjson-2.35.0.jar
inflating: nifi-1.26.0/lib/properties/gson-2.10.1.jar
inflating: nifi-1.26.0/lib/properties/google-http-client-1.43.3.jar
inflating: nifi-1.26.0/lib/properties/httpclient-4.5.14.jar
inflating: nifi-1.26.0/lib/properties/httpcore-4.4.16.jar
inflating: nifi-1.26.0/lib/properties/opencensus-contrib-http-util-0.31.1.jar
inflating: nifi-1.26.0/lib/properties/google-http-client-gson-1.43.3.jar
inflating: nifi-1.26.0/lib/properties/protobuf-java-util-3.24.3.jar
inflating: nifi-1.26.0/lib/properties/threeetenbp-1.6.8.jar
inflating: nifi-1.26.0/lib/properties/grpc-google-iam-v1-1.21.0.jar
inflating: nifi-1.26.0/lib/properties/grpc-auth-1.58.0.jar
inflating: nifi-1.26.0/lib/properties/proto-google-iam-v1-1.21.0.jar
inflating: nifi-1.26.0/lib/properties/google-auth-library-oauth2-http-1.19.0.jar
inflating: nifi-1.26.0/lib/properties/nifi-property-protection-hashicorp-1.26.0.jar
inflating: nifi-1.26.0/lib/properties/nifi-hashicorp-vault-api-1.26.0.jar
inflating: nifi-1.26.0/lib/properties/nifi-hashicorp-vault-1.26.0.jar
inflating: nifi-1.26.0/lib/properties/spring-vault-core-2.3.4.jar
inflating: nifi-1.26.0/lib/properties/spring-context-5.3.34.jar
inflating: nifi-1.26.0/lib/properties/spring-aop-5.3.34.jar
inflating: nifi-1.26.0/lib/properties/spring-expression-5.3.34.jar
inflating: nifi-1.26.0/lib/properties/spring-beans-5.3.34.jar
inflating: nifi-1.26.0/lib/properties/spring-web-5.3.34.jar
inflating: nifi-1.26.0/lib/properties/spring-core-5.3.34.jar
inflating: nifi-1.26.0/lib/properties/spring-jcl-5.3.34.jar
(harsh1208㉿kali)-[/]
$ ls
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 lost+found media mnt nifi-1.26.0 nifi-1.26.0-bin.zip opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old
(harsh1208㉿kali)-[/]
$ cd nifi-1.26.0
(harsh1208㉿kali)-[/nifi-1.26.0]
$ ls
LICENSE NOTICE README bin conf docs extensions lib
(harsh1208㉿kali)-[/nifi-1.26.0]
$ cd conf
(harsh1208㉿kali)-[/nifi-1.26.0/conf]
$ ls
authorizers.xml bootstrap azure.conf bootstrap hashicorp vault.conf bootstrap.conf login identity providers.xml state management.xml stateless.properties
bootstrap-aws.conf bootstrap-gcp.conf bootstrap-notification-services.xml logback.xml nifi.properties stateless-logback.xml zookeeper.properties
(harsh1208㉿kali)-[/nifi-1.26.0/conf]
$ sudo nano nifi.properties
(harsh1208㉿kali)-[/nifi-1.26.0/conf]

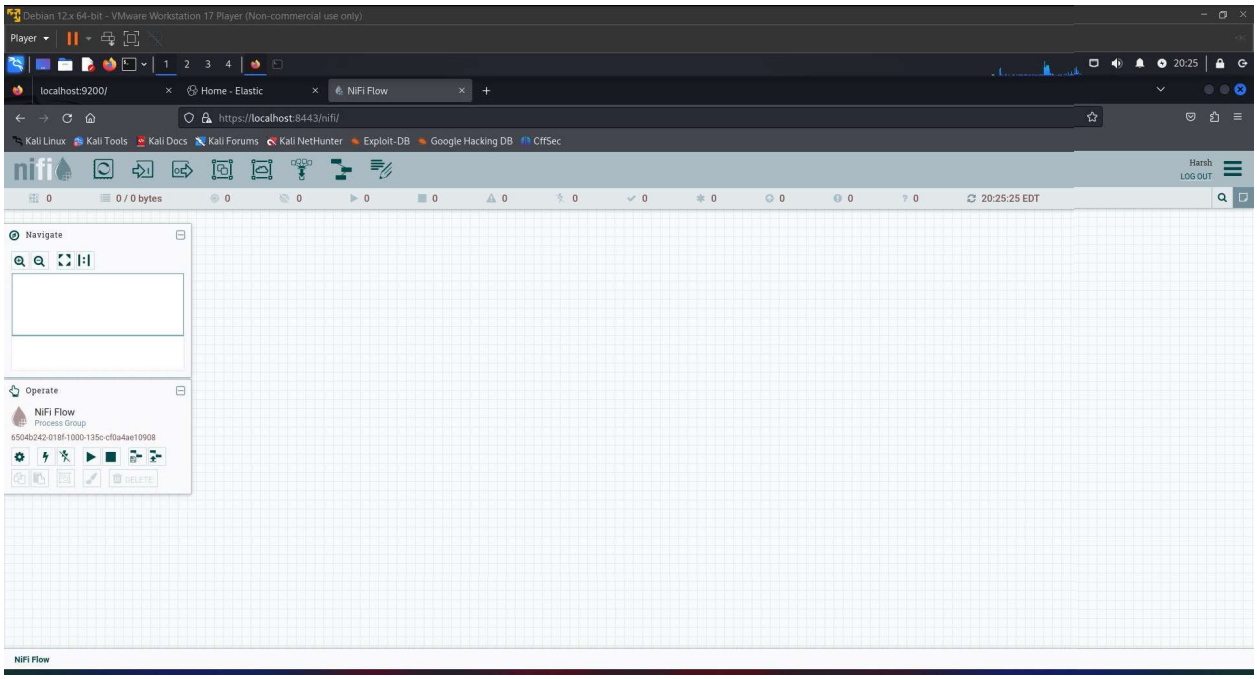
sudo bin/nifi.sh start

cat logs/nifi-app.log



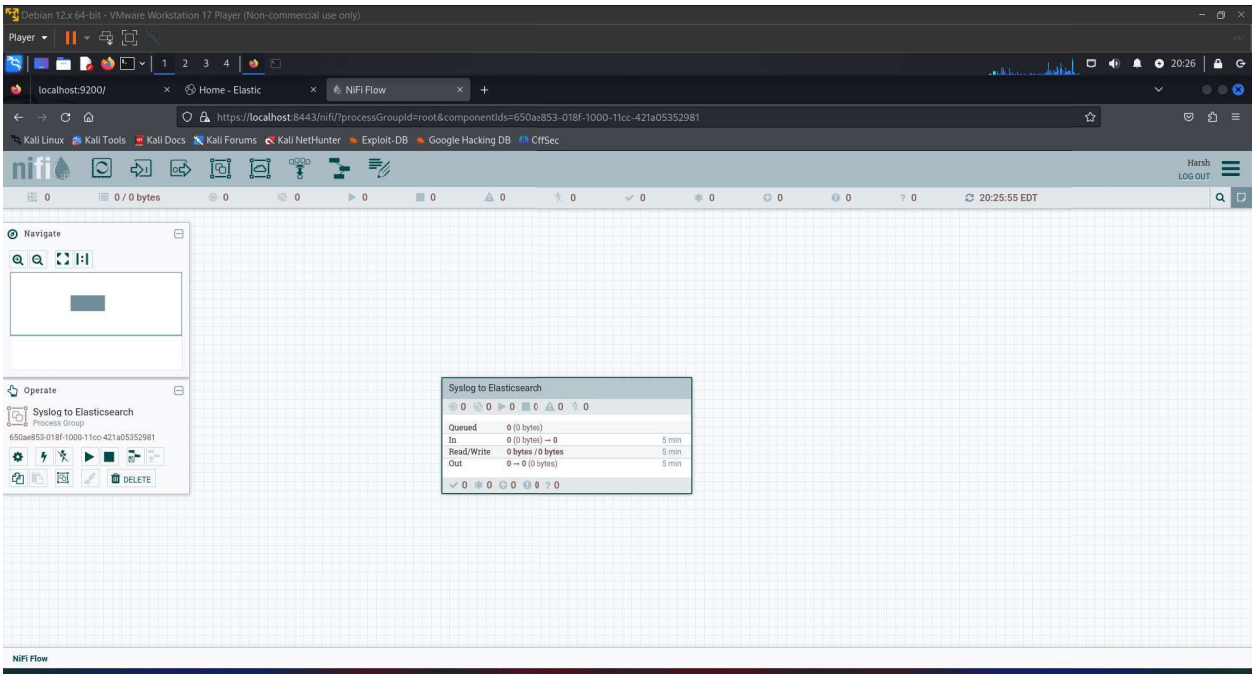






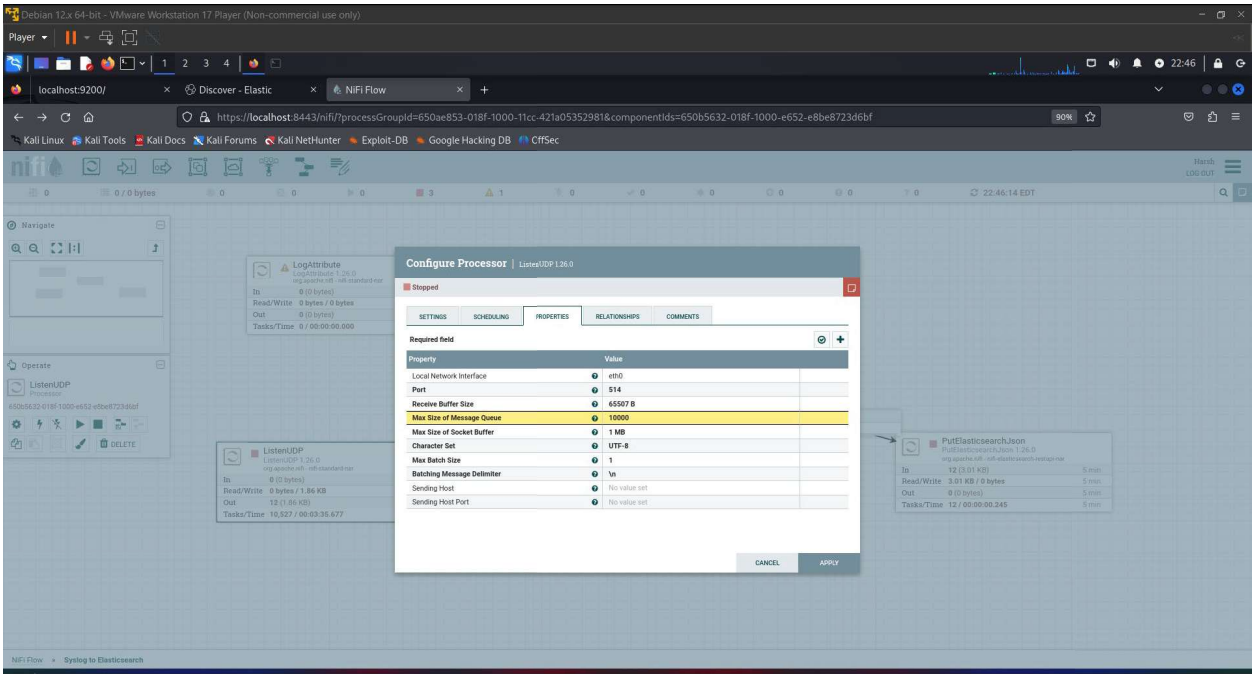
2. Build a simple NiFi pipeline which accept syslog on local port UDP 514 and send it on to ElasticSearch

Create a Process Group name Syslog to Elasticsearch:



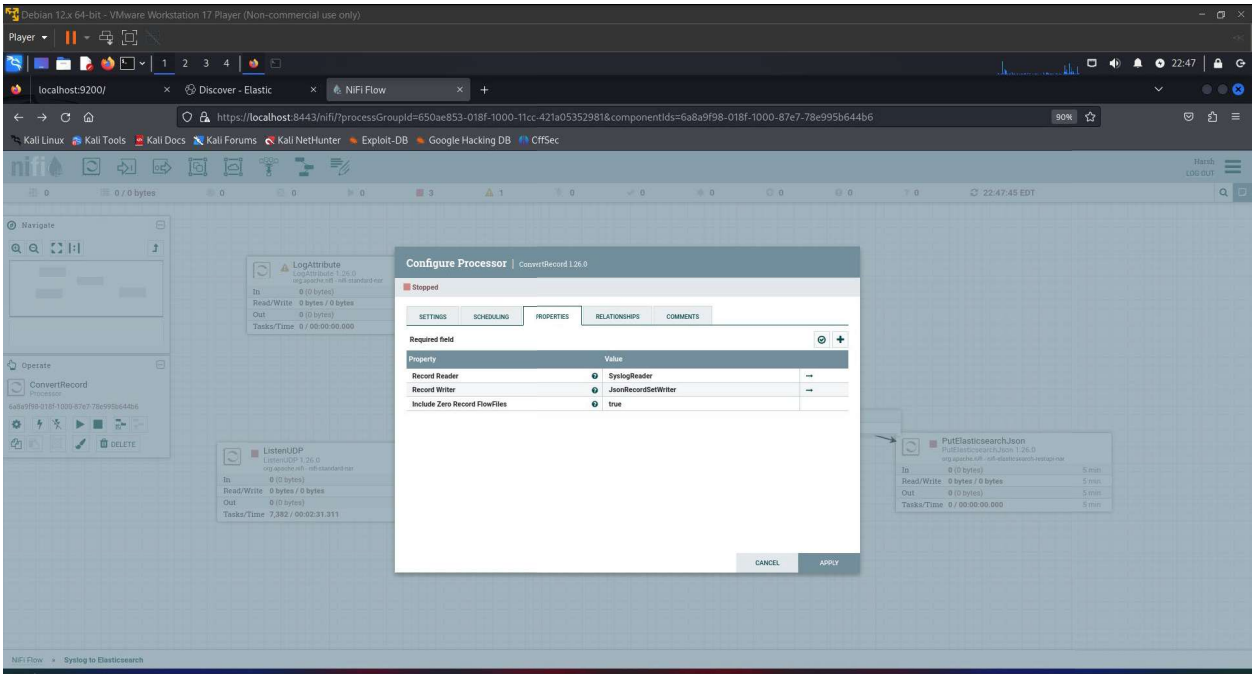
1. Set Up Syslog UDP Source
First, you need a processor to receive syslog messages:

Processor: ListenUDP
Properties:
Local Network Interface: Set to the local network interface IP or keep it blank for all interfaces.
Port: 514
Max Size of Message Queue: Depending on your expected traffic (e.g., 10000).



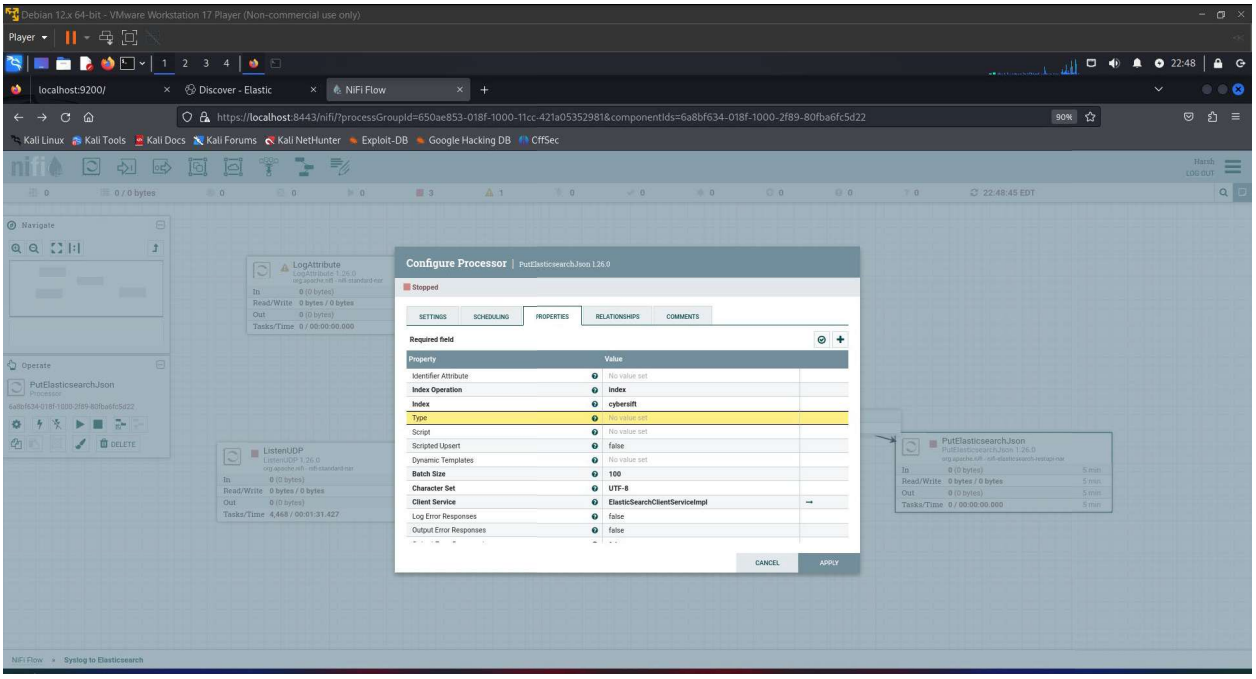
2. Convert Syslog to JSON
Syslog messages are generally not in JSON format, so you might want to convert them before sending to Elasticsearch:

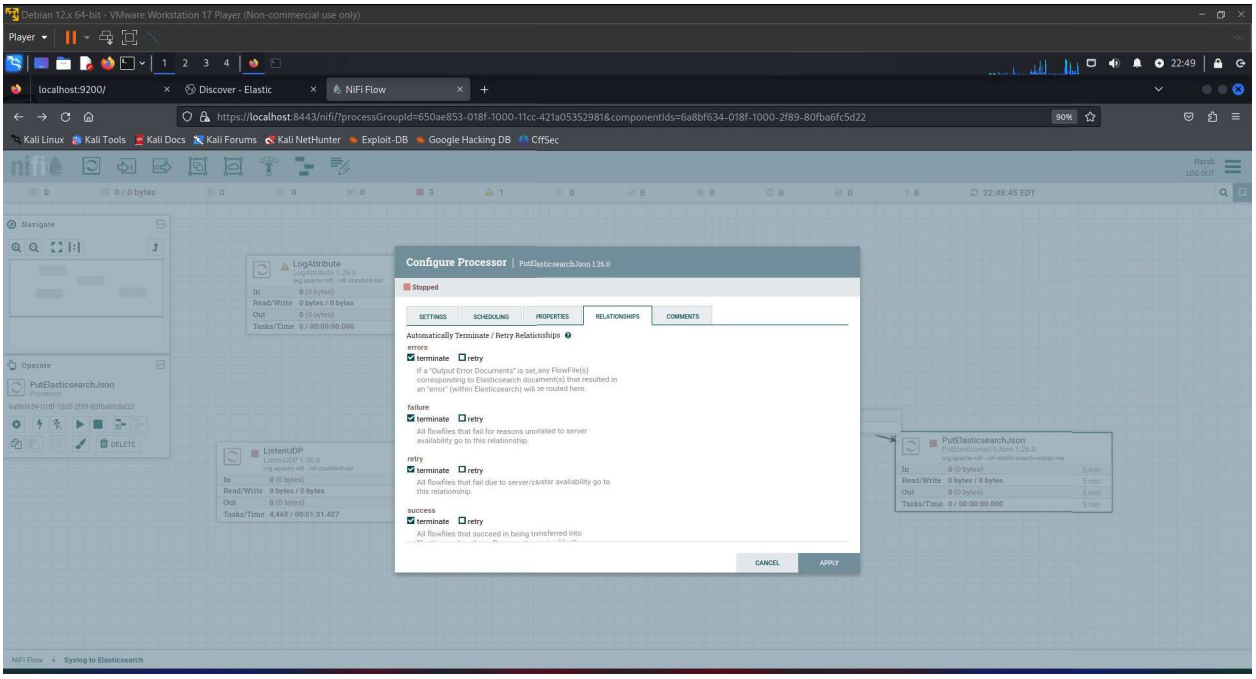
Processor: ConvertRecord
Properties:
Record Reader: Use SyslogReader to parse syslog messages.
Record Writer: Use JsonRecordSetWriter to convert records to JSON.

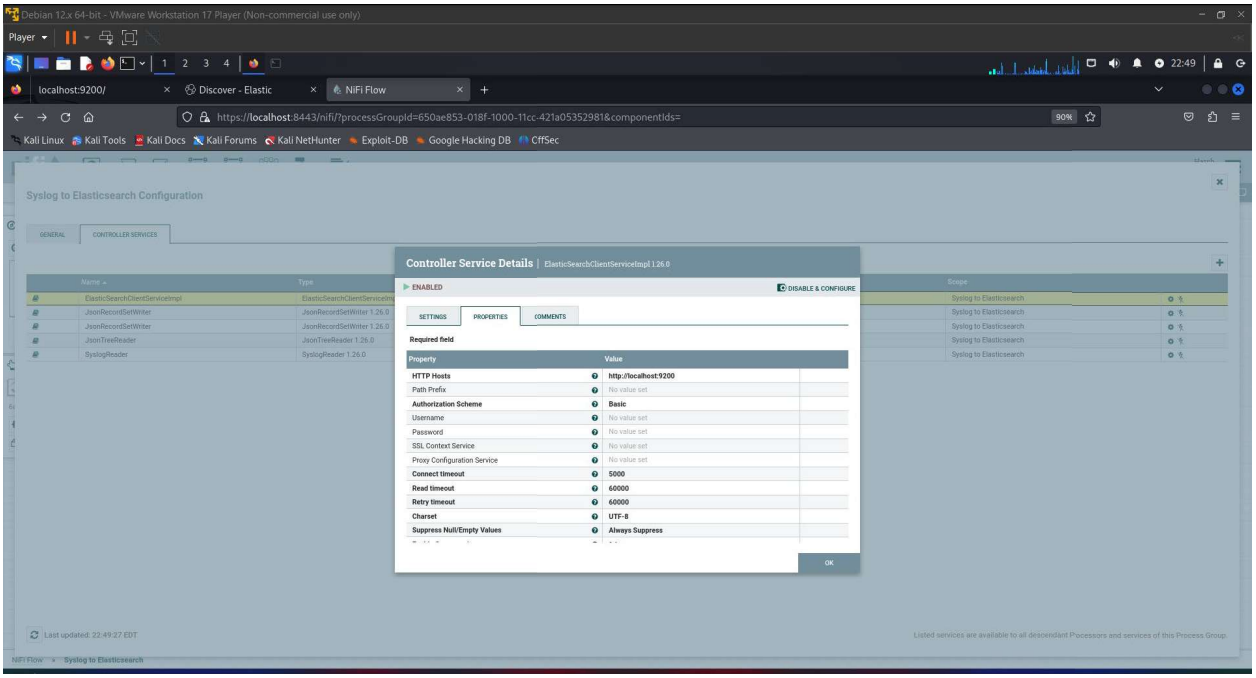


3. Send Data to Elasticsearch
Finally, use the PutElasticsearchJson processor to send the formatted syslog messages to your Elasticsearch cluster:

Processor: PutElasticsearchJson
Properties:
Elasticsearch Hosts: URL of the Elasticsearch host (e.g., http://localhost:9200).
Cluster Name: Name of your Elasticsearch cluster (if applicable).
Index: The name of the Elasticsearch index where data will be stored.
Type: The type of the index (as per Elasticsearch version).
Batch Size: Number of records to send in a batch.
ID Attribute: If you want Elasticsearch to use a specific attribute from the record as the document ID.


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
localhost:9200/
Discover - Elastic
NiFi Flow
https://localhost:8443/nifi/?processGroupId=650ae853-018f-1000-11cc-421a05352981&componentIds=6a8bf634-018f-1000-2f89-80fba6fc5d22
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
CffSec
Configure Processor
PutElasticsearchJson 1.26.0
Stopped
SETTINGS
SCHEDULING
PROPERTIES
RELATIONSHIPS
COMMENTS
Required field
Property
Value
Identifier Attribute
Index Operation
index
Index
cybersift
Type
Script
Scripted Upsert
false
Dynamic Templates
Batch Size
100
Character Set
UTF-8
Client Service
ElasticSearchClientServiceImpl
Log Error Responses
false
Output Error Responses
false
CANCEL
APPLY
LogAttribute
ListenUDP
PutElasticsearchJson
NiFi Flow
Syslog to Elasticsearch

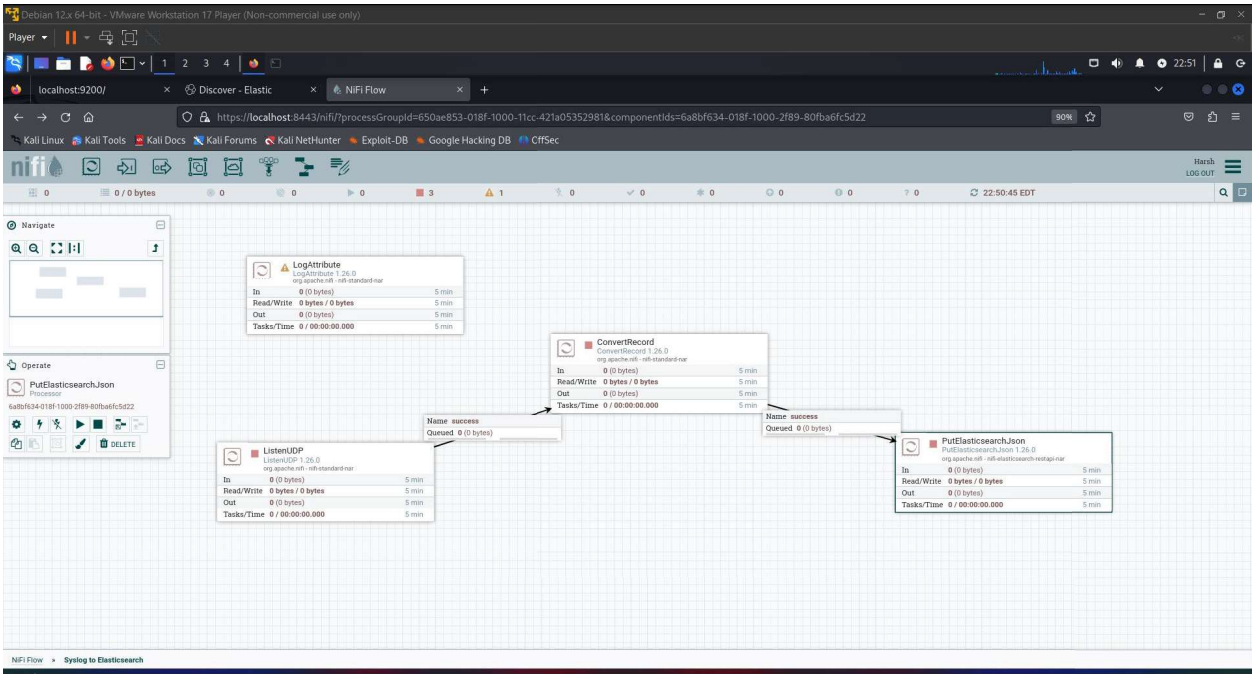

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
localhost:9200/
Discover - Elastic
NiFi Flow
https://localhost:8443/nifi/?processGroupId=650ae853-018f-1000-11cc-421a05352981&componentIds=6a8bf634-018f-1000-2f89-80fba6fc5d22
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
CffSec
Configure Processor
PutElasticsearchJson 1.26.0
Stopped
SETTINGS
SCHEDULING
PROPERTIES
RELATIONSHIPS
COMMENTS
Automatically Terminate / Retry Relationships
errors
terminate
retry
If a "Output Error Documents" is set,any FlowFile(s) corresponding to Elasticsearch document(s) that resulted in an "error" (within Elasticsearch) will be routed here.
failure
terminate
retry
All flowfiles that fail for reasons unrelated to server availability go to this relationship.
retry
terminate
retry
All flowfiles that fail due to server/cluster availability go to this relationship.
success
terminate
retry
All flowfiles that succeed in being transferred into
CANCEL
APPLY
LogAttribute
ListenUDP
PutElasticsearchJson
NiFi Flow
Syslog to Elasticsearch



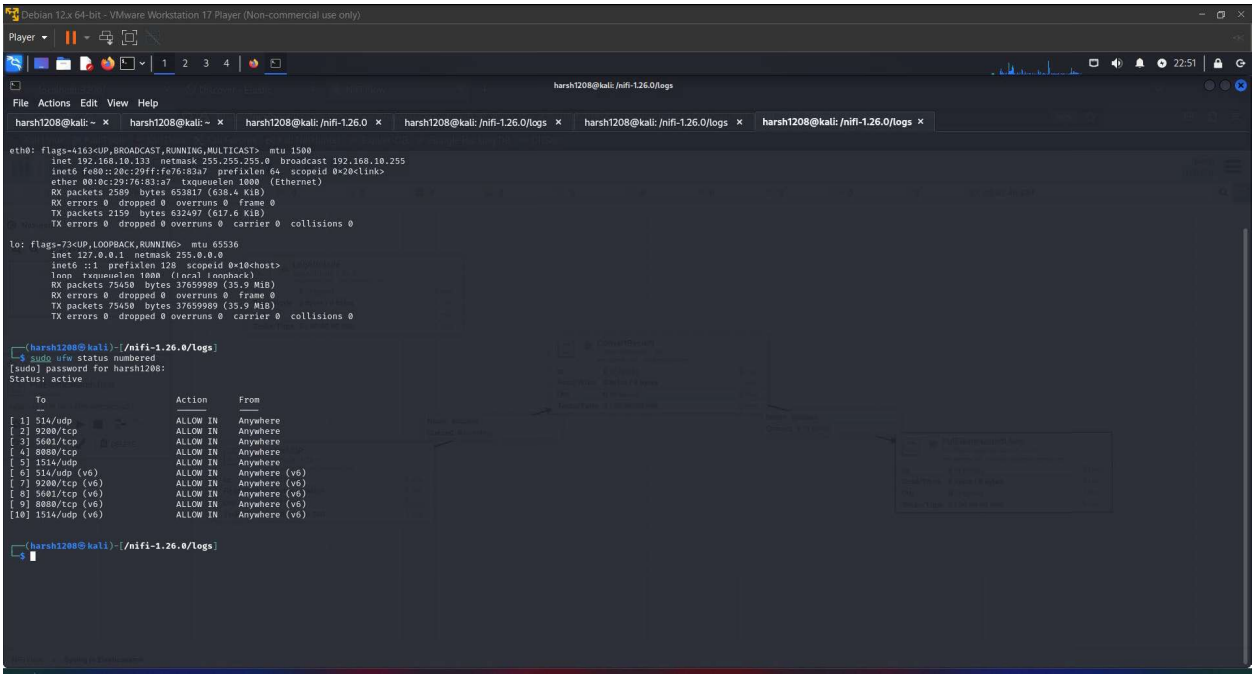
Connecting the Processors
Connect all processors:

Connect ListenUDP to ConvertRecord with a success relationship.
Connect ConvertRecord to PutElasticsearchJson with a success relationship.
Handle failure relationships according to your error-handling strategy (e.g., connect to a LogMessage processor for debugging).
Error Handling
It's good practice to add processors for handling possible errors or failed processing:

Processor: PutFile or LogMessage for debugging purposes.
Final Steps
Start the Processors: Once all configurations are done, start all the processors.
Monitor the Flow: Use NiFi's built-in data provenance and logging to monitor the data flow and troubleshoot any issues.

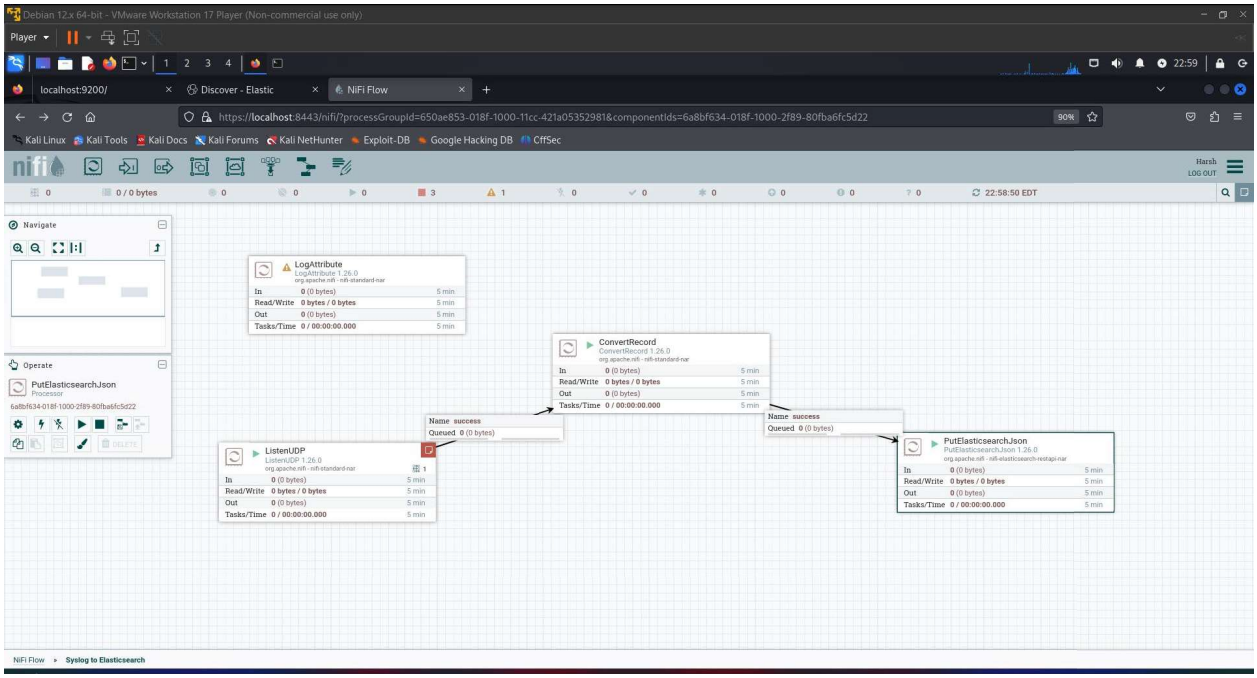


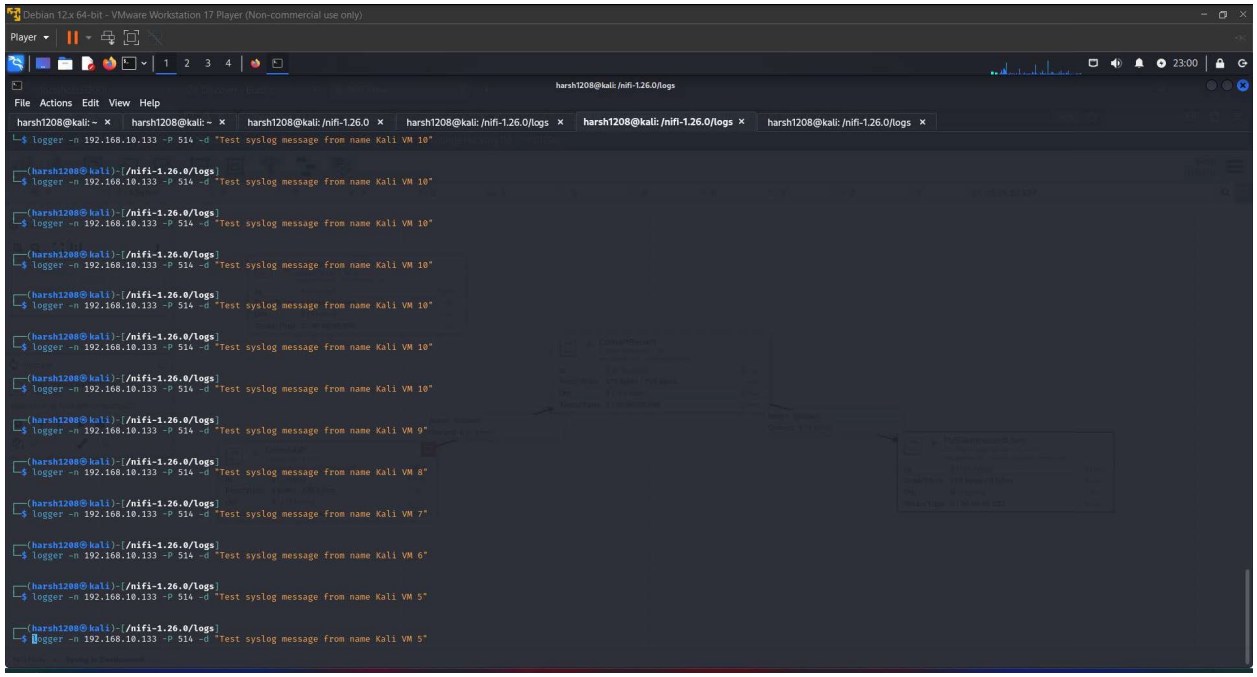
Firewall and Network Settings:



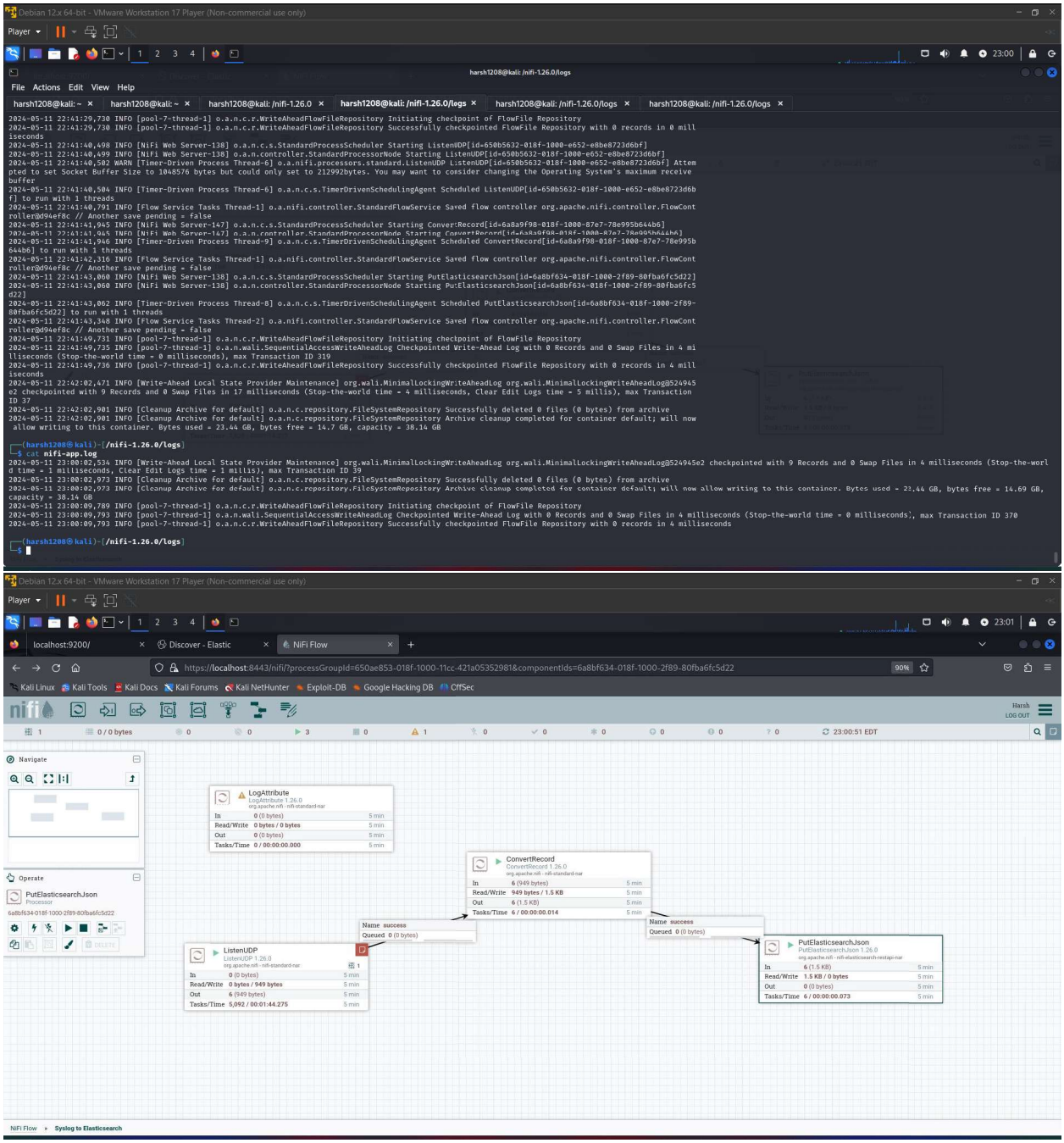
Next, Start all the Processors in NiFi and then send/generate multiple syslog messages like:

- logger -n 192.168.10.133 -P 514 -d "Test syslog message from name Kali VM"

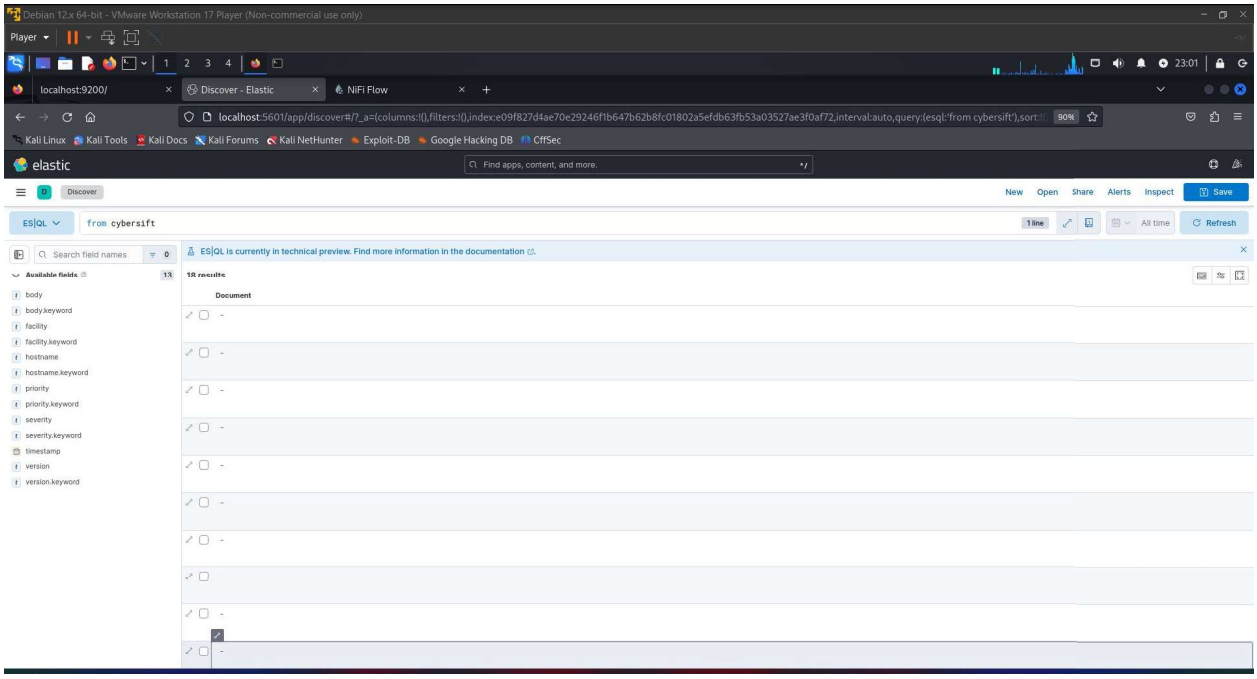


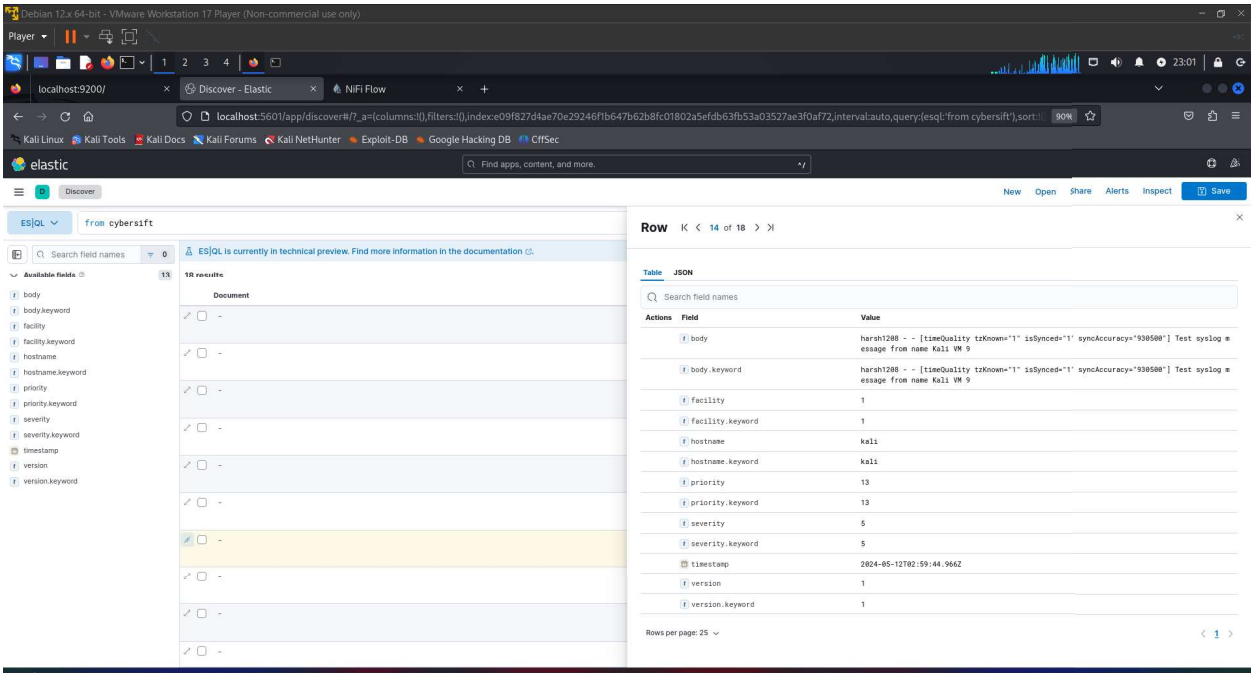


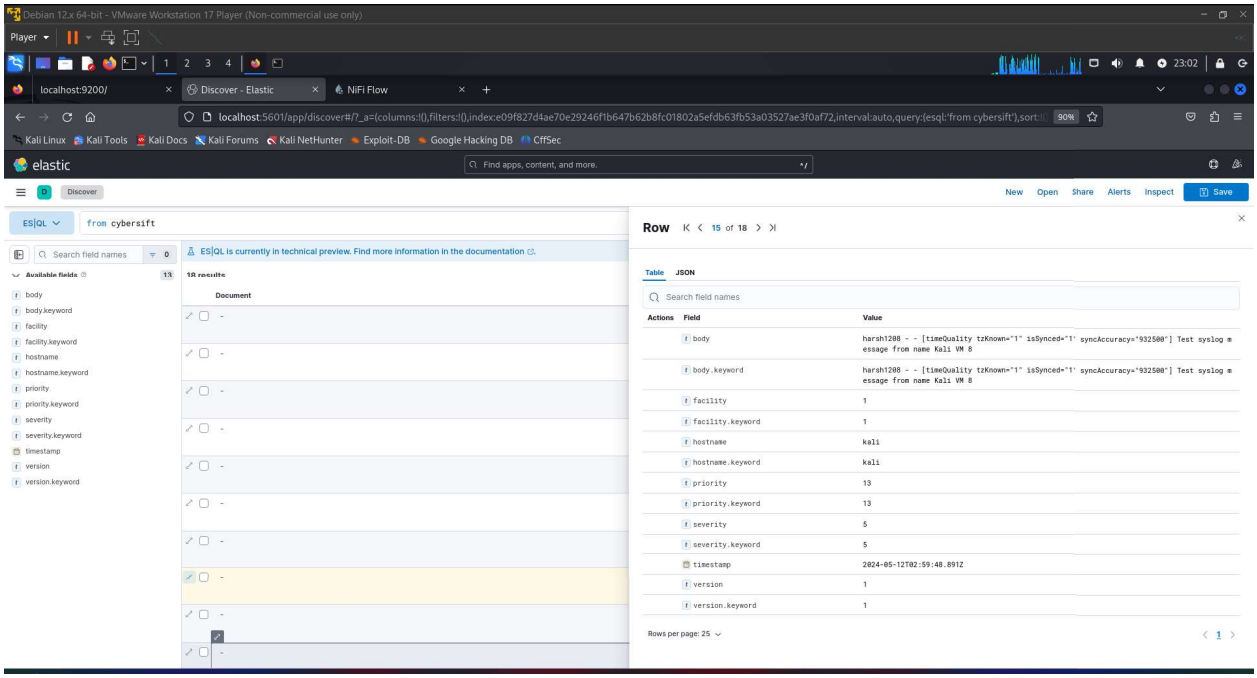
Open logs in nifi.logs and see for any errors:

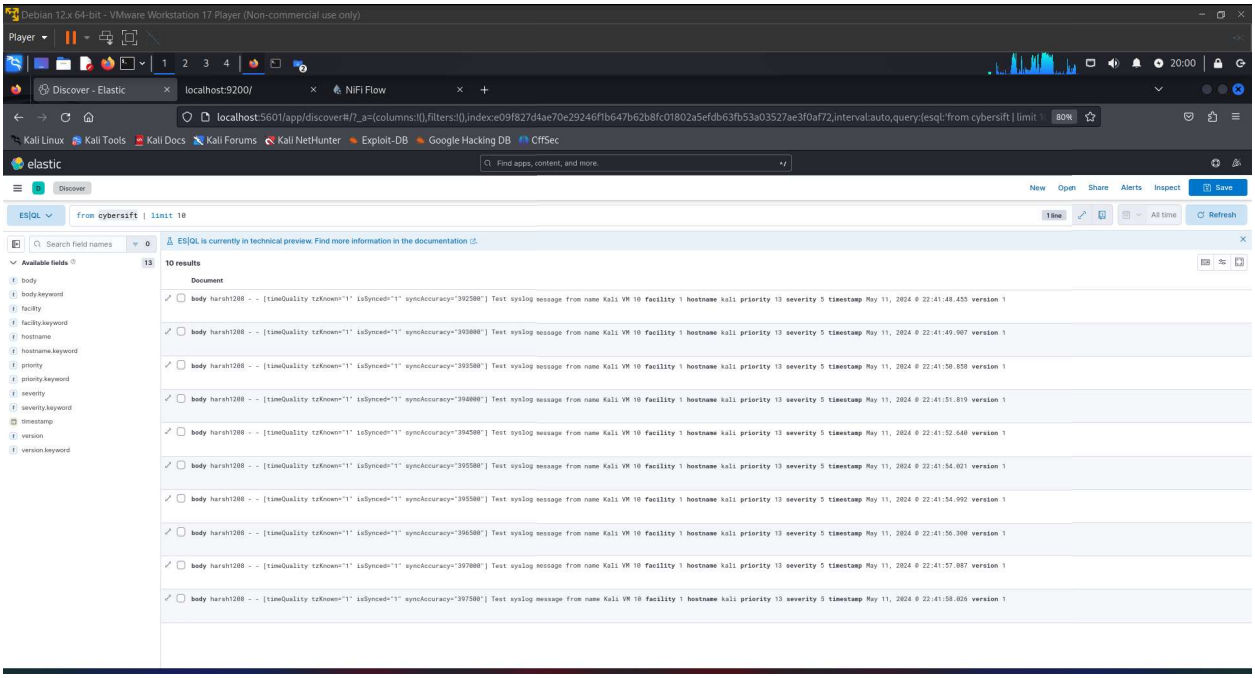


Open Kibana interface for data logs review.


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
localhost:9200/
Discover - Elastic
NiFi Flow
localhost:5601/app/discover#/?_a=(columns:!(),filters:!(),index:e09f827d4ae70e29246f1b647b62b8fc01802a5efdb63fb53a03527ae3f0af72,interval:auto,query:(esql:'from cybersift'),sort:!(
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
CffSec
elastic
Find apps, content, and more.
Discover
New
Open
Share
Alerts
Inspect
Save
ES|QL
from cybersift
Refresh
Search field names
ES|QL is currently in technical preview. Find more information in the documentation
Document
body
body.keyword
facility
facility.keyword
hostname
hostname.keyword
priority
priority.keyword
severity
severity.keyword
timestamp
version
version.keyword


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
localhost:9200/
Discover - Elastic
NiFi Flow
localhost:5601/app/discover#/?_a=(columns:!(),filters:!(),index:e09f827d4ae70e29246f1b647b62b8fc01802a5efdb63fb53a03527ae3f0af72,interval:auto,query:(esql:'from cybersift'),sort:!(
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
CffSec
elastic
Find apps, content, and more.
Discover
New
Open
Share
Alerts
Inspect
Save
ES|QL
from cybersift
Search field names
ES|QL is currently in technical preview. Find more information in the documentation
Document
Row
14 of 18
Table
JSON
Search field names
Actions
Field
Value
body
harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="930500"] Test syslog message from name Kali VM 9
body.keyword
harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="930500"] Test syslog message from name Kali VM 9
facility
1
facility.keyword
1
hostname
kali
hostname.keyword
kali
priority
13
priority.keyword
13
severity
5
severity.keyword
5
timestamp
2024-05-12T02:59:44.966Z
version
1
version.keyword
1
Rows per page: 25


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
localhost:9200/
Discover - Elastic
NiFi Flow
localhost:5601/app/discover#/?_a=(columns:!(),filters:!(),index:e09f827d4ae70e29246f1b647b62b8fc01802a5efdb63fb53a03527ae3f0af72,interval:auto,query:(esql:'from cybersift'),sort:!(
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
CffSec
elastic
Find apps, content, and more.
Discover
New
Open
Share
Alerts
Inspect
Save
ES|QL
from cybersift
Search field names
ES|QL is currently in technical preview. Find more information in the documentation
Document
Row
15 of 18
Table
JSON
Search field names
Actions
Field
Value
body
harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="932500"] Test syslog message from name Kali VM 8
body.keyword
harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="932500"] Test syslog message from name Kali VM 8
facility
1
facility.keyword
1
hostname
kali
hostname.keyword
kali
priority
13
priority.keyword
13
severity
5
severity.keyword
5
timestamp
2024-05-12T02:59:48.891Z
version
1
version.keyword
1
Rows per page: 25


Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player
Discover - Elastic
localhost:9200/
NiFi Flow
localhost:5601/app/discover#/?_a=(columns:!(),filters:!(),index:e09f827d4ae70e29246f1b647b62b8fc01802a5efdb63fb53a03527ae3f0af72,interval:auto,query:(esql:'from cybersift | limit
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
CffSec
elastic
Find apps, content, and more.
Discover
New
Open
Share
Alerts
Inspect
Save
ES|QL
from cybersift | limit 10
Refresh
Search field names
ES|QL is currently in technical preview. Find more information in the documentation
10 results
Document
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="392500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:48.455 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="393000"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:49.907 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="393500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:50.858 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="394000"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:51.819 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="394500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:52.640 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="395500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:54.021 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="395500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:54.992 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="396500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:56.300 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="397000"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:57.087 version 1
body harsh1208 - - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="397500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 @ 22:41:58.026 version 1