

Отчет

1. Установка стека ELK.....	2
2. Особенности работы данного стека.....	16
3. Сбор логов Windows и их анализ.....	23
4. Сбор логов локальной машины (Lubuntu 20.04 LTS) и их анализ.....	28
1. Шаблоны Grok для фильтрации подозрительных событий в auth.log..	28
2. Syslog: скрытая угроза безопасности.....	30

1. Установка стека ELK

В Oracle VM VirtualBox была создана виртуальная машина (выделено 5 Гб RAM, адаптер – сетевой мост). На ней установлена Ubuntu 20.04 LTS.



Стек Elastic — ранее известный как стек ELK — представляет собой набор программного обеспечения с открытым исходным кодом, созданного Elastic, который позволяет искать, анализировать и визуализировать журналы, вести их как централизованный журнал. Централизованное ведение журнала может быть полезно при попытке выявить проблемы с серверами или приложениями, поскольку оно позволяет выполнять поиск по всем вашим журналам в одном месте.

Эластичный стек состоит из четырех основных компонентов:

- Elasticsearch: распределенная поисковая система RESTful, в которой хранятся все собранные данные.
- Logstash: компонент обработки данных Elastic Stack, который отправляет входящие данные в Elasticsearch.
- Kibana: веб-интерфейс для поиска и визуализации логов.
- Beats: легкие одноцелевые поставщики данных, которые могут отправлять данные с сотен или тысяч компьютеров либо в Logstash, либо в Elasticsearch.

Важное №1: при установке Elastic Stack необходимо использовать одну и ту же версию для всего стека. В данной работе будут установлены последние версии всего стека, которыми на момент написания, а именно Elasticsearch 7.17.1, Kibana 7.17.1, Logstash 7.17.1 и Filebeat 7.17.1 (см. “number”).

```
elk@vm: /etc
File Actions Edit View Help
elk@vm: /etc
elk@vm:/etc$ sudo vim /etc/systemd/system/elasticsearch.service.d
elk@vm:/etc$ sudo systemctl start elasticsearch
elk@vm:/etc$ sudo systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /l
ib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
elk@vm:/etc$ curl -XGET 'http://localhost:9200'
{
  "name" : "vm",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "gbvyqmLEQmCa3a2B4bRt1A",
  "version" : {
    "number" : "7.17.1",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "e5acb99f822233d62d6444ce45a4543dc1c8059a",
    "build_date" : "2022-02-23T22:20:54.153567231Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Важное №2: перед установкой стека ELK обязательно должны быть установлены Nginx и OpenJDK 11.

Важное №3: скачивание компонентов, а также установка стека ELK в России с весны 2022 должна производиться с использованием VPN или прокси.

Процесс установки Elasticsearch:

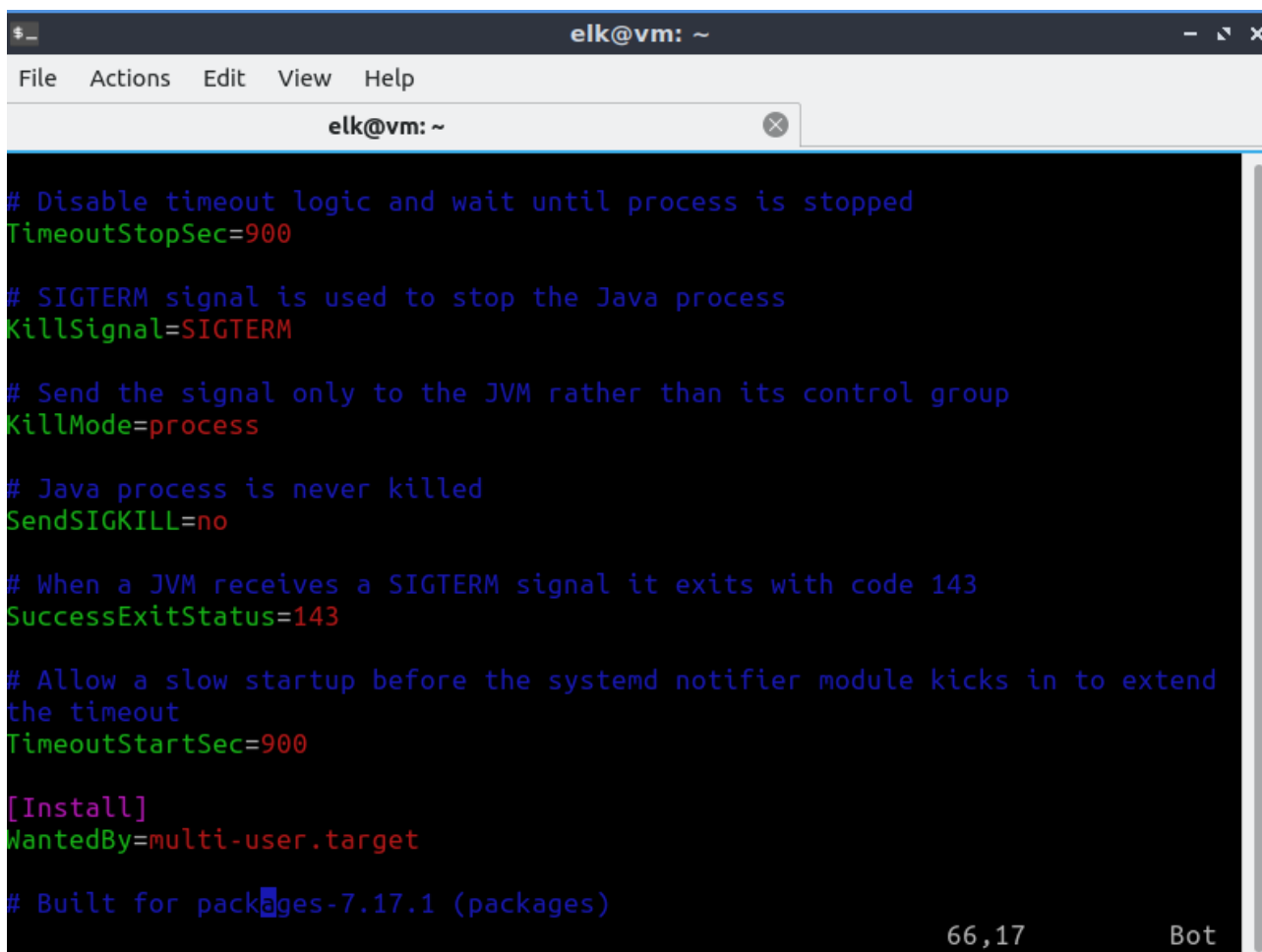
- `curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch |sudo gpg --dearmor -o /usr/share/keyrings/elastic.gpg`
- `echo "deb [signed-by=/usr/share/keyrings/elastic.gpg] https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list`
- `sudo apt update`
- `sudo apt install elasticsearch`
- `sudo nano /etc/elasticsearch/elasticsearch.yml`

Настройка файла `elasticsearch.yml` включает в себя:

```
elk@vm: ~  
File Actions Edit View Help  
elk@vm: ~  
#  
# By default Elasticsearch is only accessible on localhost. Set a different  
# address here to expose this node on the network:  
#  
network.host: localhost  
#  
# By default Elasticsearch listens for HTTP traffic on the first free port it  
# finds starting at 9200. Set a specific HTTP port here:  
#  
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: ["127.0.0.1"]  
#  
# Bootstrap the cluster using an initial set of master-eligible nodes:  
#
```

```
#  
#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
```

Кроме того, для корректной работы необходимо настроить параметры `timelstartsec`, `timelstopsec` в файле `/usr/lib/systemd/system/elasticsearch.service` :



```
# Disable timeout logic and wait until process is stopped
TimeoutStopSec=900

# SIGTERM signal is used to stop the Java process
KillSignal=SIGTERM

# Send the signal only to the JVM rather than its control group
KillMode=process

# Java process is never killed
SendSIGKILL=no

# When a JVM receives a SIGTERM signal it exits with code 143
SuccessExitStatus=143

# Allow a slow startup before the systemd notifier module kicks in to extend
the timeout
TimeoutStartSec=900

[Install]
WantedBy=multi-user.target

# Built for packages-7.17.1 (packages)
```

Для быстрой работы стека также можно прописать ограничения по использованию оперативной памяти:

В файле `/etc/default/elasticsearch` указать `ES_JAVA_OPTS="-Xms4g -Xmx4g"`, `MAX_LOCKED_MEMORY=unlimited`. В файле `/etc/security/limits.conf` указать `elasticsearch soft memlock unlimited, elasticsearch hard memlock unlimited`. В файле `/usr/lib/systemd/system/elasticsearch.service` указать `LimitMEMLOCK=infinity` и запустить: `sudo systemctl daemon-reload`. В файле `/etc/elasticsearch/elasticsearch.yml` указать `bootstrap.memory_lock: true`. В файле `/etc/elasticsearch/jvm.options` выделить 4 Гб RAM:

```
-Xms4g
-Xmx4g
```

После всех настроек: `sudo systemctl restart elasticsearch`.

Запуск Elasticsearch и проверка работы включают в себя:

- `sudo systemctl start elasticsearch`
- `sudo systemctl enable elasticsearch`
- `curl -X GET "localhost:9200"`

Если на экране вам высветилось похожее сообщение, значит, установка elasticsearch была успешной:

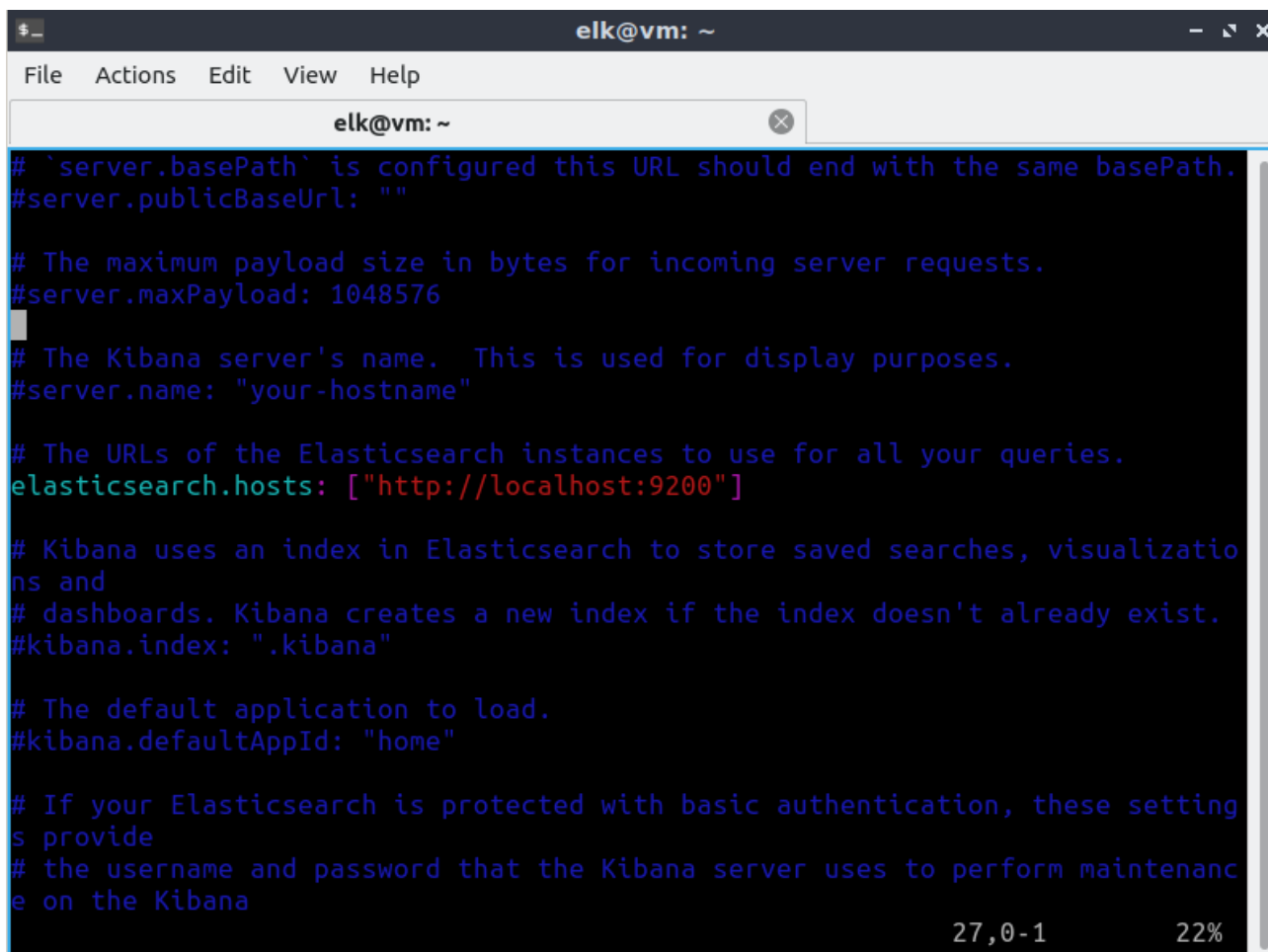
```
elk@vm: /etc
File Actions Edit View Help
elk@vm: /etc
elk@vm:/etc$ sudo vim /etc/systemd/system/elasticsearch.service.d
elk@vm:/etc$ sudo systemctl start elasticsearch
elk@vm:/etc$ sudo systemctl enable elasticsearch
Synchronizing state of elasticsearch.service with SysV service script with /l
ib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable elasticsearch
elk@vm:/etc$ curl -XGET 'http://localhost:9200'
{
  "name" : "vm",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "gbvyqmLEQmCa3a2B4bRt1A",
  "version" : {
    "number" : "7.17.1",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "e5acb99f822233d62d6444ce45a4543dc1c8059a",
    "build_date" : "2022-02-23T22:20:54.153567231Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.1",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
```

Процесс установки Kibana:

- `sudo apt install kibana`
- `sudo nano /etc/kibana/kibana.yml`

Настройка файла `kibana.yml` включает в себя:

```
elk@vm: ~  
File Actions Edit View Help  
elk@vm: ~  
# Kibana is served by a back end server. This setting specifies the port to use.  
server.port: 5601  
  
# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.  
# The default is 'localhost', which usually means remote machines will not be able to connect.  
# To allow connections from remote users, set this parameter to a non-loopback address.  
server.host: "localhost"  
  
# Enables you to specify a path to mount Kibana at if you are running behind a proxy.  
# Use the `server.rewriteBasePath` setting to tell Kibana if it should remove the basePath  
# from requests it receives, and to prevent a deprecation warning at startup.  
# This setting cannot end in a slash.  
server.basePath: ""  
  
# Specifies whether Kibana should rewrite requests that are prefixed with `server.basePath` or require that they are rewritten by your reverse proxy.  
# This setting was effectively always `false` before Kibana 6.3 and will default to `true` starting in Kibana 7.0
```



```
elk@vm: ~
File Actions Edit View Help
elk@vm: ~
# `server.basePath` is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"

# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]

# Kibana uses an index in Elasticsearch to store saved searches, visualizations and
# dashboards. Kibana creates a new index if the index doesn't already exist.
#kibana.index: ".kibana"

# The default application to load.
#kibana.defaultAppId: "home"

# If your Elasticsearch is protected with basic authentication, these settings provide
# the username and password that the Kibana server uses to perform maintenance on the Kibana

27,0-1 22%
```

Запуск Kibana:

- `sudo systemctl enable kibana`
- `sudo systemctl start kibana`


Поскольку Kibana настроен на прослушивание только на локальном хосте, мы должны настроить обратный прокси-сервер, чтобы разрешить внешний доступ к нему. Для этого мы будем использовать Nginx, который уже должен быть установлен на вашем сервере.

Следующая команда создаст административного пользователя и пароль Kibana и сохранит их в файле `htpasswd.users`. Бдтеу настроен Nginx на запрос этого имени пользователя и пароля и прочитан этот файл:

- `echo "kibanaadmin:`openssl passwd -apr1`" | sudo tee -a /etc/nginx/htpasswd.users`

Создайте файл блока сервера Nginx с названием "default":

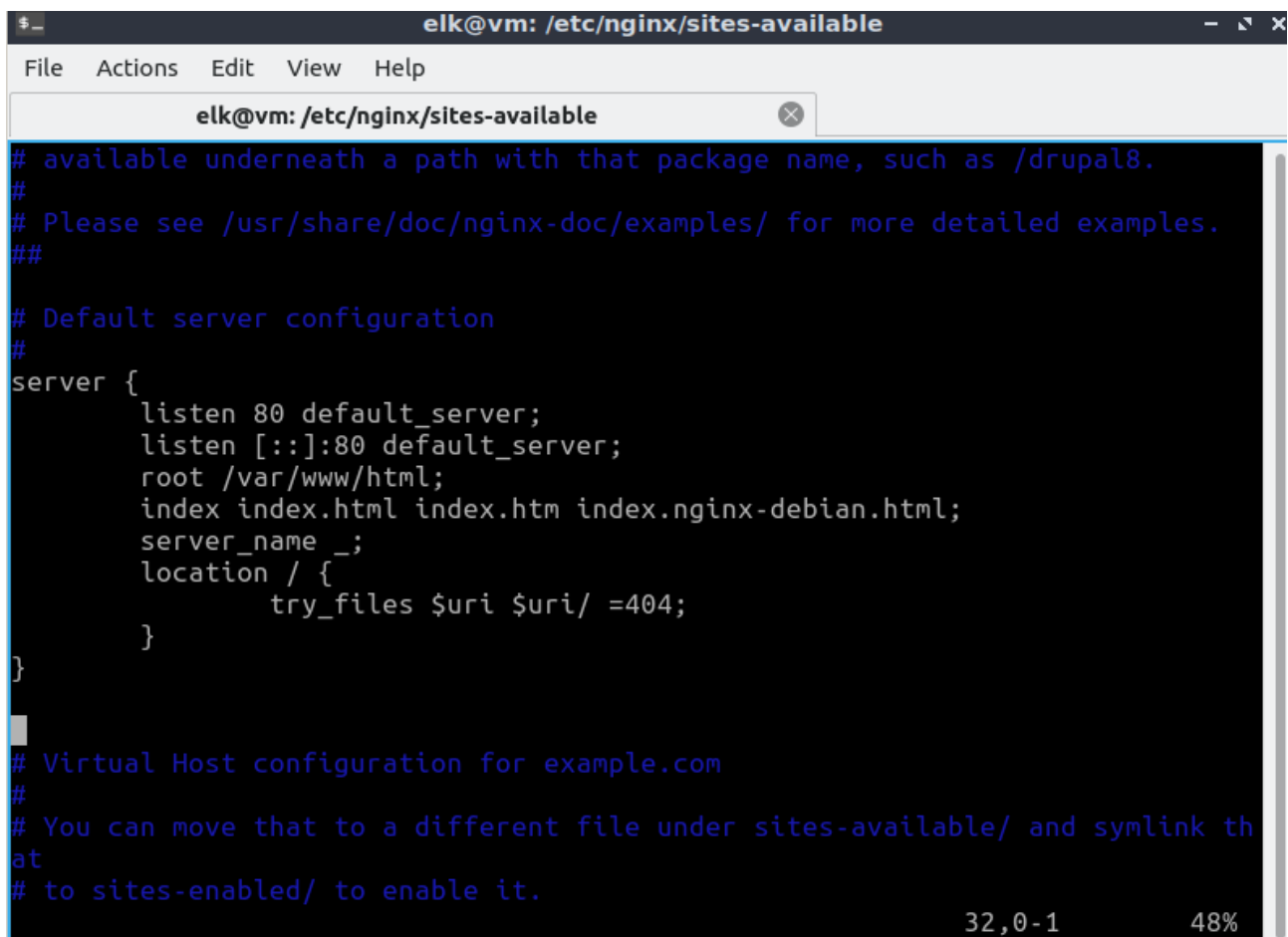
- `sudo nano /etc/nginx/sites-available/default`



```
elk@vm:/etc/nginx/sites-available$ ls
default
```

В данный файл добавляется следующий блок кода. Этот код настраивает Nginx для направления HTTP-трафика вашего сервера в приложение Kibana,

которое прослушивает localhost:5601. Кроме того, он настраивает Nginx для чтения файла htpasswd.users и требует базовой аутентификации:



```
# available underneath a path with that package name, such as /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##

# Default server configuration
#
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    root /var/www/html;
    index index.html index.htm index.nginx-debian.html;
    server_name _;
    location / {
        try_files $uri $uri/ =404;
    }
}

# Virtual Host configuration for example.com
#
# You can move that to a different file under sites-available/ and symlink th
at
# to sites-enabled/ to enable it.
```

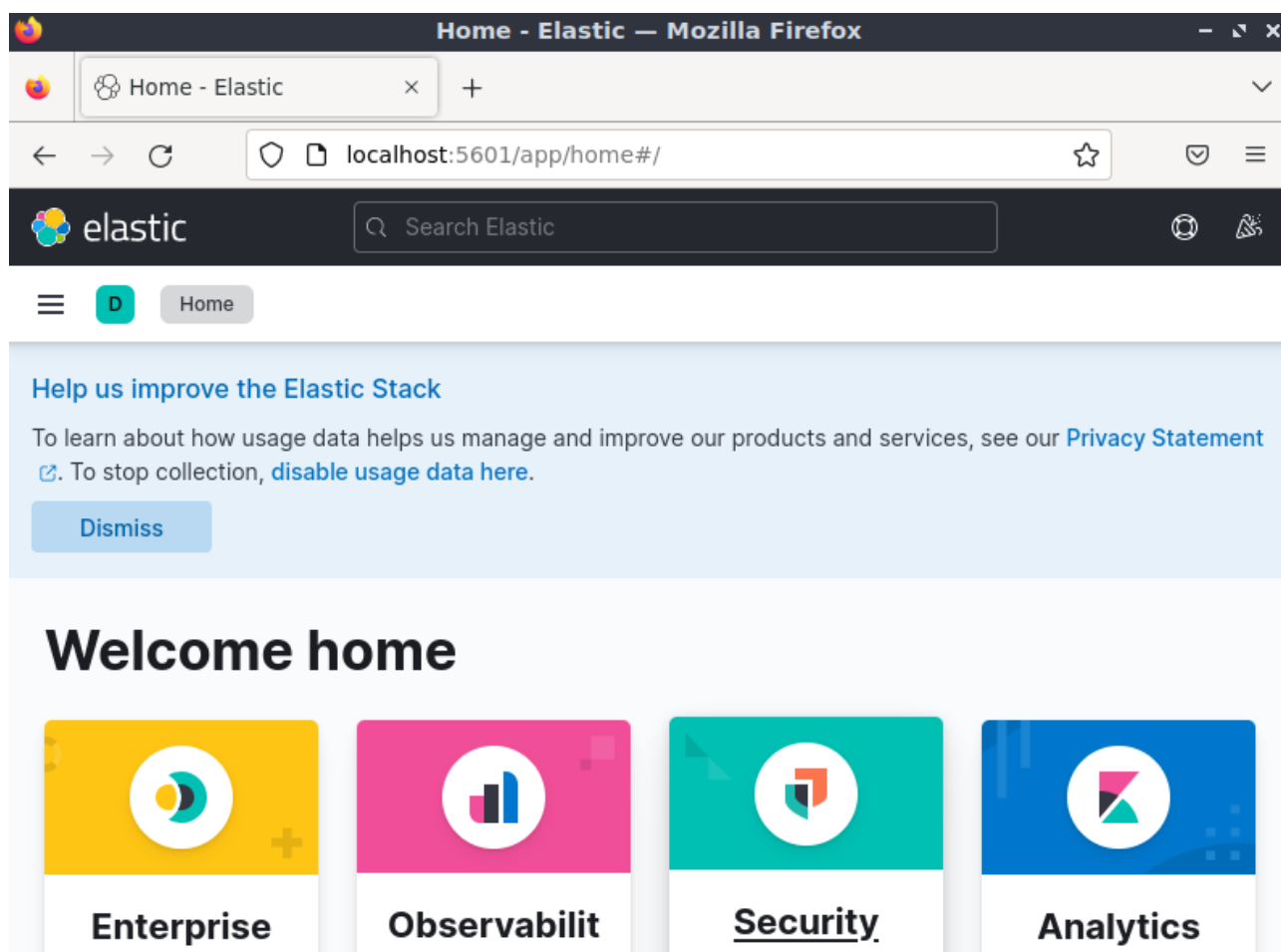
Затем включите новую конфигурацию, создав символическую ссылку на каталог с поддержкой сайтов:

- `sudo ln -s /etc/nginx/sites-available/default /etc/nginx/sites-enabled/default`
- `sudo nginx -t`
- `sudo systemctl reload nginx`

Для проверки работы Kibana введите в браузере:

- `localhost:5601`

Таким образом, откроется сайт Elastic:



Процесс установки Logstash:

- `sudo apt install logstash`
- `sudo nano /etc/logstash/conf.d/logstash.conf`

Настройка конфигурационного файла `logstash.conf` для сбора логов Windows 7 Professional по порту 5044 включает в себя:

```
input {
  beats {
    port => 5044
  }
}
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "windows"
  }
}
```

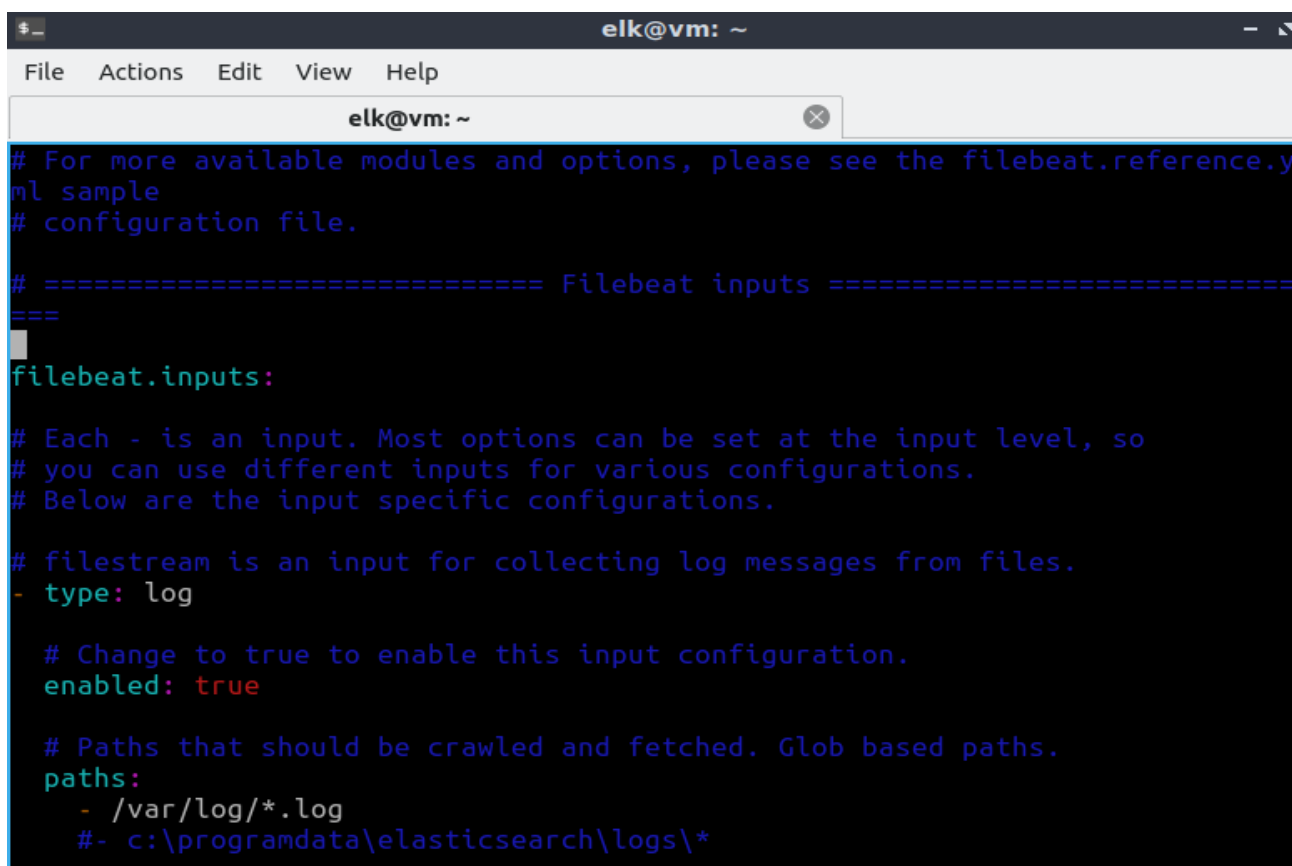
Запуск Logstash:

- `sudo systemctl start logstash`
- `sudo systemctl enable logstash`

Процесс установки Filebeat:

- `sudo apt install filebeat`
- `sudo nano /etc/filebeat/filebeat.yml`

Настройка конфигурационного файла на сбор файлов `auth.log` и `syslog` имеет вид:



```
# For more available modules and options, please see the filebeat.reference.y
ml sample
# configuration file.

# ===== Filebeat inputs =====
#
# filebeat.inputs:
#
# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input specific configurations.
#
# filestream is an input for collecting log messages from files.
- type: log

# Change to true to enable this input configuration.
enabled: true

# Paths that should be crawled and fetched. Glob based paths.
paths:
  - /var/log/*.log
  #- c:\programdata\elasticsearch\logs\*
```

```
elk@vm: ~
File Actions Edit View Help
elk@vm: ~

filebeat.config.modules:
  # Glob pattern for configuration loading
  path: ${path.config}/modules.d/*.yaml

  # Set to true to enable config reloading
  reload.enabled: true

  # Period on which files under path should be checked for changes
  #reload.period: 10s

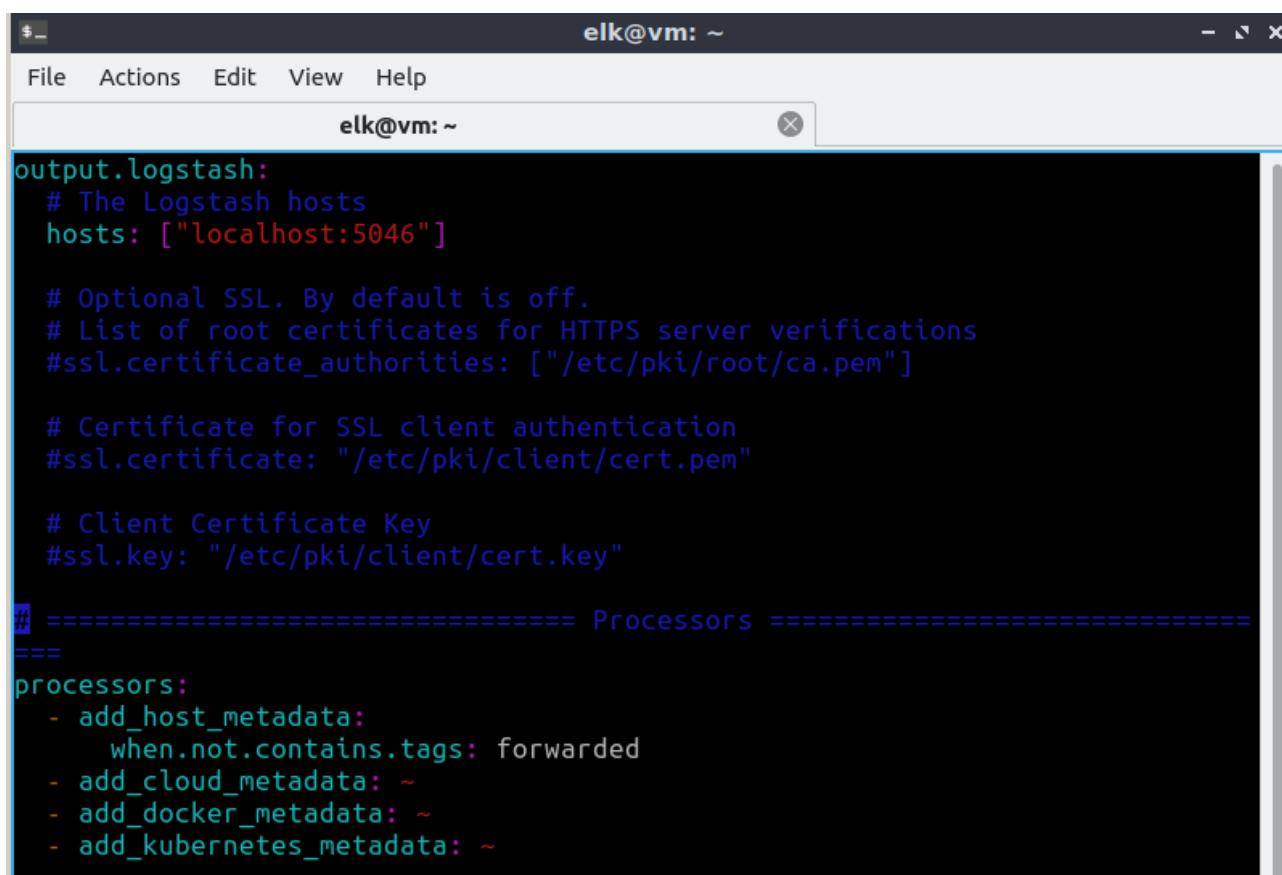
# ===== Elasticsearch template setting =====
===

setup.template.settings:
  index.number_of_shards: 1
  #index.codec: best_compression
  #_source.enabled: false

# ===== General =====
===
```

```
elk@vm: ~
File Actions Edit View Help
elk@vm: ~

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana
API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "http://localhost:5601"
```



```
output.logstash:
  # The Logstash hosts
  hosts: ["localhost:5046"]

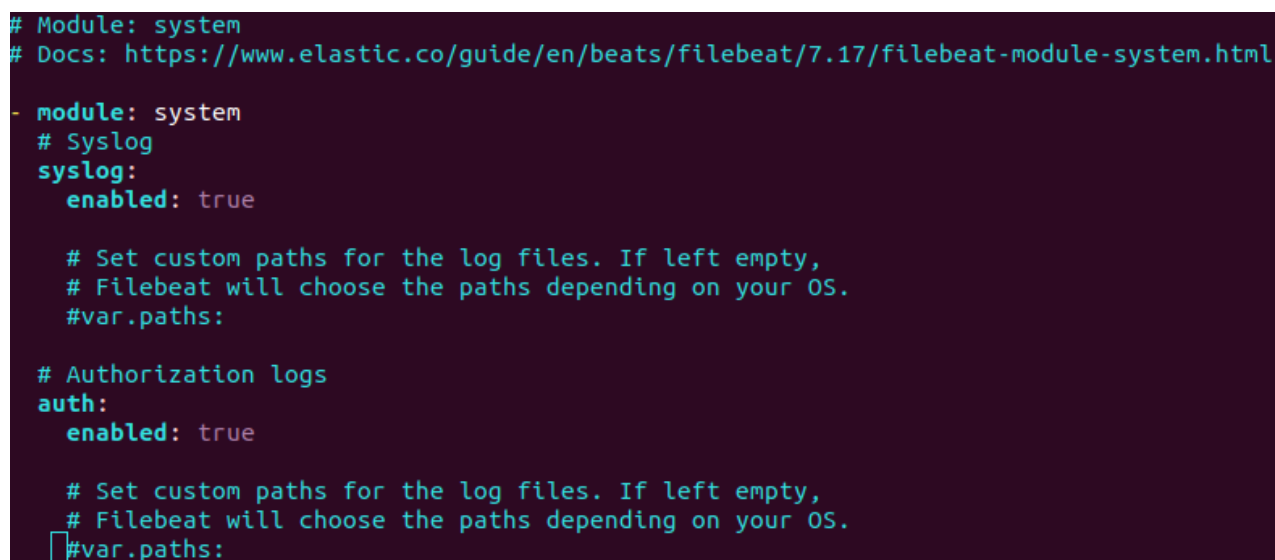
  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

# ===== Processors =====
processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
  - add_cloud_metadata: ~
  - add_docker_metadata: ~
  - add_kubernetes_metadata: ~
```

Кроме того, для сбора auth.log и syslog важно проконтролировать то, какие модули подключены (файл /etc/filebeat/modules.d/system.yml) . Это же касается и сбора любых других логов:



```
# Module: system
# Docs: https://www.elastic.co/guide/en/beats/filebeat/7.17/filebeat-module-system.html

- module: system
  # Syslog
  syslog:
    enabled: true

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:

  # Authorization logs
  auth:
    enabled: true

    # Set custom paths for the log files. If left empty,
    # Filebeat will choose the paths depending on your OS.
    #var.paths:
```

Запуск Filebeat:

- `sudo systemctl start filebeat`
- `sudo systemctl enable filebeat`

Процесс установки Winlogbeat:

Для сбора логов с машины Windows необходимо установить Winlogbeat. Для этого в PowerShell с правами администратора следует:

- `cd 'C:\Program Files\Winlogbeat'`
- `.\install-service-winlogbeat.ps1`

Настройка файла `winlogbeat.yml` включает в себя (192.168.1.71 – ip Lubuntu, на которой установлен стек ELK, 5044 – используемый порт):

```
winlogbeat.event_logs:
  - name: Application
    ignore_older: 72h

  - name: System

  - name: Security
    processors:
      - script:
        lang: javascript
        id: security
        file: ${path.home}/module/security/config/winlogbeat-security-js

  - name: ForwardedEvents
    tags: [forwarded]

  - name: Windows PowerShell
    event_id: 400, 403, 600, 800

  - name: Microsoft-Windows-PowerShell/Operational
    event_id: 4103, 4104, 4105, 4106

# ===== Elasticsearch template settings =====

setup.template.settings:
  index.number_of_shards: 1
```

```

..
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.1.71:5044"]
loadbalance: true
ssl.enabled: true
  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"

# ===== Processors =====
processors:
  - add_host_metadata:
      when.not.contains.tags: forwarded
  - add_cloud_metadata: ~

```

Для запуска Winlogbeat следует ввести команды:

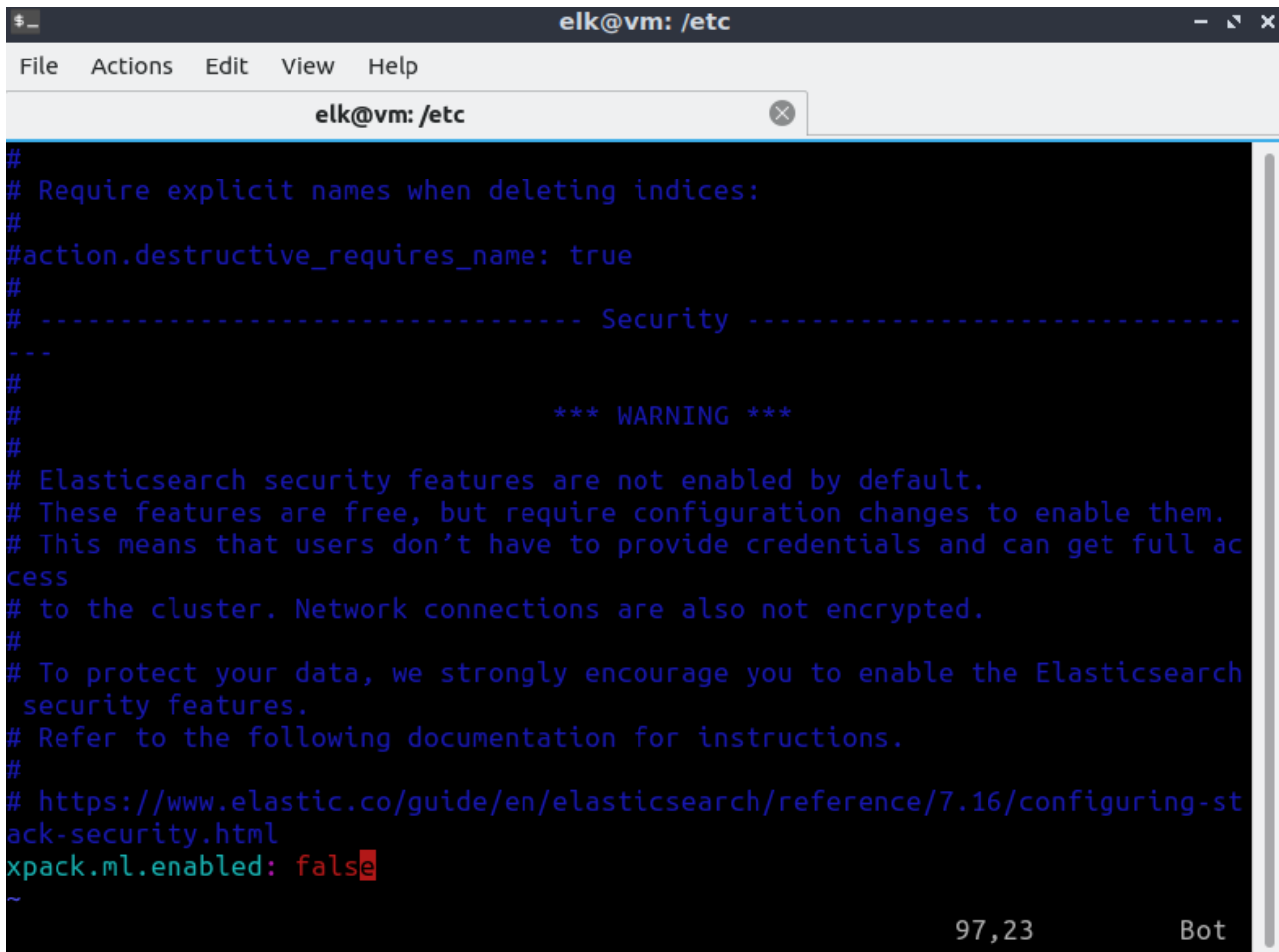
- Start-Service winlogbeat
- services.msc

Для приостановки работы:

- Stop-Service winlogbeat

2. Особенности работы данного стека

Особенность №1. Конфигурационный файл `elasticsearch.yml` содержит строку: `xpack.ml.enabled: false`. Без нее работа на используемом в этой работе оборудовании невозможна, т.к. процессор данной машины старый.



```
elk@vm: /etc
File Actions Edit View Help
elk@vm: /etc

#
# Require explicit names when deleting indices:
#
#action.destructive_requires_name: true
#
# ----- Security -----
#
# *** WARNING ***
#
# Elasticsearch security features are not enabled by default.
# These features are free, but require configuration changes to enable them.
# This means that users don't have to provide credentials and can get full access
# to the cluster. Network connections are also not encrypted.
#
# To protect your data, we strongly encourage you to enable the Elasticsearch
# security features.
# Refer to the following documentation for instructions.
# https://www.elastic.co/guide/en/elasticsearch/reference/7.16/configuring-stack-security.html
xpack.ml.enabled: false
~
97,23 Bot
```


Windows 7 Максимальная

© Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

Service Pack 1



Система

Оценка:	Получение оценки
Процессор:	AMD Athlon(tm) II X3 440 Processor 3.00 GHz
Установленная память (ОЗУ):	8,00 ГБ
Тип системы:	64-разрядная операционная система
Перо и сенсорный ввод:	Перо и сенсорный ввод недоступны для этого экрана

Комментарий Elastic: “Машинное обучение использует инструкции SSE4.2, поэтому оно работает только на машинах, процессоры которых поддерживают SSE4.2. Если вы запускаете Elasticsearch на старом оборудовании, вы должны отключить машинное обучение (установив для `xpack.ml.enabled` значение `false`)”.

Примечание: SSE4 — набор команд микроархитектуры Intel Core, впервые реализованный в процессорах серии Penryn (не следует путать с SSE4A от AMD).

Особенность №2. Установленный стек ELK может работать некорректно, а именно — переставать собирать логи. Изменение конфигурационных файлов (`winlogbeat.yml`, `logstash.conf`, `filebeat.yml`) не приносит результатов. Была произведена проверка используемых портов (для `winlogbeat` — 5044, для `filebeat` — 5046) с помощью `tcpdump` (например, `sudo tcpdump port 5044`). Пакеты

действительно получаются фильтром (received by filter), но не “захватываются” (captured). Но сам сетевой адаптер работает:

```
elk@vm:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.71 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::7d96:32f9:e1cd:557e prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:09:c1:06 txqueuelen 1000 (Ethernet)
    RX packets 8879 bytes 1071253 (1.0 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2711 bytes 493876 (493.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 91986 bytes 14109663 (14.1 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 91986 bytes 14109663 (14.1 MB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

elk@vm:~$ sudo tcpdump -Xi enp0s3
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
13:34:15.870860 IP vm.37506 > 93.184.220.29.http: Flags [.], ack 915150799, w
in 501, options [nop,nop,TS val 2940558213 ecr 4141776499], length 0
    0x0000: 4500 0034 28e1 4000 4006 161e c0a8 0147 E..4(.@.@.....G
```

```
elk@vm: ~
File Actions Edit View Help
elk@vm: ~
0x0000: 4500 0076 1202 4000 4011 a4dc c0a8 0101 E..v..@.@.....
0x0010: c0a8 0147 0035 911e 0062 e48d 10a7 8183 ...G.5...b.....
0x0020: 0001 0000 0000 0000 0165 0137 0135 0135 .....e.7.5.5
0x0030: 0138 0162 0164 0135 0166 0137 0132 0163 .8.b.d.5.f.7.2.c
0x0040: 0130 0161 0134 0163 0130 0130 0130 0130 .0.a.4.c.0.0.0.0
0x0050: 0130 0130 0130 0130 0130 0130 0130 0130 .0.0.0.0.0.0.0.0
0x0060: 0130 0138 0165 0166 0369 7036 0461 7270 .0.8.e.f.ip6.arp
0x0070: 6100 000c 0001 a.....
13:35:28.318893 IP vm.41082 > lo-in-f94.1e100.net.http: Flags [.], ack 576542
580, win 501, options [nop,nop,TS val 4086785989 ecr 3178749523], length 0
0x0000: 4500 0034 2f19 4000 4006 bd9a c0a8 0147 E..4/.@.@.....G
0x0010: adc2 de5e a07a 0050 321a 67f8 225d 5774 ...^.z.P2.g."]Wt
0x0020: 8010 01f5 4e37 0000 0101 080a f397 67c5 ....N7.....g.
0x0030: bd77 de53 .w.S
13:35:28.337319 IP lo-in-f94.1e100.net.http > vm.41082: Flags [.], ack 1, win
290, options [nop,nop,TS val 3178759762 ecr 4086683667], length 0
0x0000: 4500 0034 8a72 0000 7c06 6641 adc2 de5e E..4.r...|.fA...^
0x0010: c0a8 0147 0050 a07a 225d 5774 321a 67f9 ...G.P.z"]Wt2.g.
0x0020: 8010 0122 e366 0000 0101 080a bd78 0652 ...".f.....x.R
0x0030: f395 d813 ....
^C
60 packets captured
60 packets received by filter
0 packets dropped by kernel
elk@vm:~$
```

Отключение файрвола (sudo ufw disable) не дало результатов.

Важно отметить, что указанные выше порты были доступны (sudo ufw enable 5044 и sudo ufw enable 5044/tcp) и через них некоторое время удавалось получать пакеты. Посмотреть полученные логи, а также их анализ можно в Главах 3,4 данного отчета.

Особенность №3. При проверке статуса работы logstash.service (sudo systemctl status logstash.service) можно наблюдать появление строки: “-Dlog4j2.isThreadContextMapInheritable=true”

```
elk@vm: ~
File Actions Edit View Help

elk@vm: ~
● logstash.service - logstash
   Loaded: loaded (/etc/systemd/system/logstash.service; enabled; vendor p>
   Active: active (running) since Mon 2023-01-02 16:35:50 MSK; 10min ago
 Main PID: 575 (java)
   Tasks: 31 (limit: 6968)
  Memory: 585.7M
   CGroup: /system.slice/logstash.service
           └─575 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -XX:+UseCo>

январь 02 16:43:18 vm logstash[575]: [2023-01-02T16:43:18,652][INFO ][logstash.>
январь 02 16:43:19 vm logstash[575]: [2023-01-02T16:43:19,714][INFO ][logstash.>
январь 02 16:43:20 vm logstash[575]: [2023-01-02T16:43:19,786][INFO ][logstash.>
январь 02 16:43:24 vm logstash[575]: [2023-01-02T16:43:24,114][INFO ][logstash.>
январь 02 16:43:24 vm logstash[575]: [2023-01-02T16:43:24,750][INFO ][logstash.>
январь 02 16:43:34 vm logstash[575]: [2023-01-02T16:43:34,228][INFO ][logstash.>
январь 02 16:43:34 vm logstash[575]: [2023-01-02T16:43:34,381][INFO ][logstash.>
январь 02 16:43:34 vm logstash[575]: [2023-01-02T16:43:34,501][INFO ][logstash.>
январь 02 16:43:35 vm logstash[575]: [2023-01-02T16:43:35,085][INFO ][logstash.>
январь 02 16:43:36 vm logstash[575]: [2023-01-02T16:43:36,572][INFO ][org.logst>
~
~
~
~
lines 1-19/19 (END)
```

```
elk@vm: ~
File Actions Edit View Help

elk@vm: ~

security.egd=file:/dev/urandom -Dlog4j2.isThreadContextMapInheritable=true ->

>"}

~
~
~
~
lines 1-19/19 (END)
```

Если приложение создает дополнительные потоки для выполнения пользовательской операции, тогда контекст может быть передан из родительского потока в дочерние потоки путем выполнения определенной конфигурации в рамках запуска приложения/log4j2. Это делается путем установки для isThreadContextMapInheritable значения «true».

Log4j — библиотека журналирования (логирования) Java-программ, часть общего проекта «Apache Logging Project». Log4j первоначально развивался в рамках зонтичного «Apache Jakarta Project», ответственного за все Java-проекты Apache, но впоследствии выделился в отдельный, очень популярный проект журналирования. Используется часто при написании программ на Java, для ведения логов.

9 декабря 2021 года в Log4j 2 была выявлена критическая уязвимость (CVE-2021-44228), позволяющая выполнить произвольный код. Подверженные проблеме проекты включают Steam, Apple iCloud, Minecraft.

Уязвимость существует в действии интерфейса именования и каталогов Java (JNDI) для разрешения переменных. Затронутые версии Log4j содержат функции JNDI, такие как подстановка поиска сообщений, не защищают от злоумышленников контролируемый облегченный протокол доступа к каталогам (LDAP), систему доменных имен (DNS) и другие конечные точки, связанные с JNDI.

Злоумышленник может использовать Log4Shell, отправив специально созданный запрос в уязвимую систему. Это заставляет систему выполнять произвольный код. Запрос позволяет противнику полностью контроль над системой. Затем злоумышленник может украсть информацию, запустить программу-вымогатель или провести другие вредоносные действия.

Выходящие в Интернет устройства, а также ноутбуки, настольные компьютеры и планшеты особенно подвержены эксплуатации этих уязвимостей.

Рекомендации по устранению уязвимостей Log4J были опубликованы на сайте Национального Агентства Безопасности 22 декабря 2021 года:



National Security Agency/Central Security Service

HOME › PRESS ROOM › NEWS & HIGHLIGHTS › ARTICLE

Mitigating Log4Shell and Other Log4j Related Vulnerabilities

certnz ACSC Canadian Centre for Cyber Security National Cyber Security Centre

GOVERNMENT COMMUNICATIONS SECURITY BUREAU

Log4j Example:

```
import org.apache.logging.log4j.LogManager;
import org.apache.logging.log4j.Logger;

public class Log4jExample {
    // Create a logger instance
    Logger log = LogManager.getLogger(Log4jExample.class);

    // Log a message at the debug level
    log.debug("Hello this is a debug message");

    // Log a message at the info level
    log.info("Hello this is an info message");
}
```

PRESS RELEASE | Dec. 22, 2021

**CISA, FBI, NSA, and International
Partners Issue Advisory to Mitigate
Apache Log4J Vulnerabilities**

Учитывая это, необходимо использовать ELK, предварительно обезопасив себя от уязвимостей Log4J.

Данный отчет содержит перевод статьи “CISA, FBI, NSA, and International Partners Issue Advisory to Mitigate Apache Log4J Vulnerabilities (CISA, ФБР, АНБ и международные партнеры выпускают рекомендации по устранению уязвимостей Apache Log4J)”, а также сами рекомендации по устранению уязвимости.

Основная работа по устранению уязвимости лежит на поставщике продукта (Elastic). Но есть некоторые меры по снижению риска, которые может сделать пользователь, чтобы дополнительно обезопасить себя:

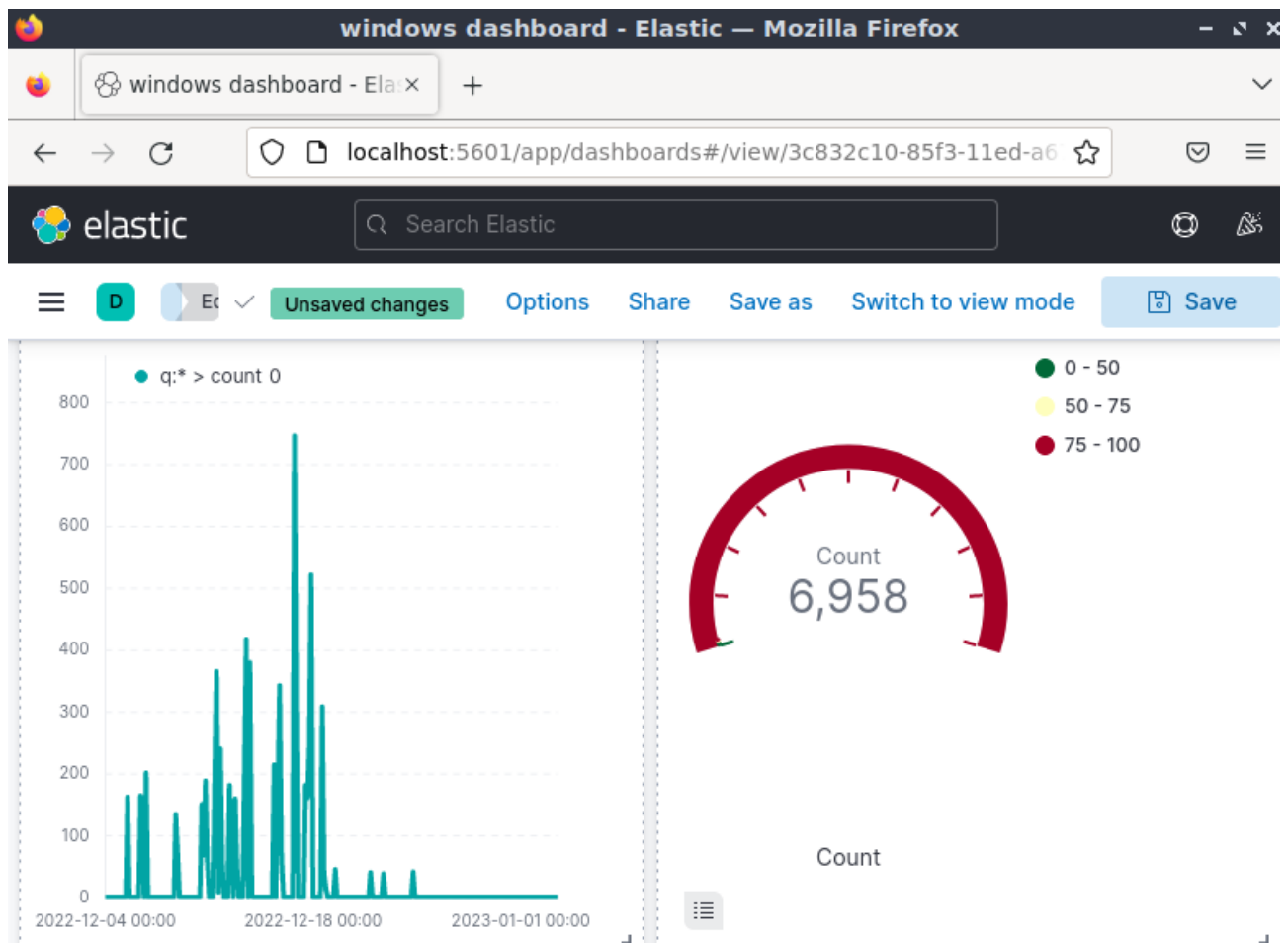
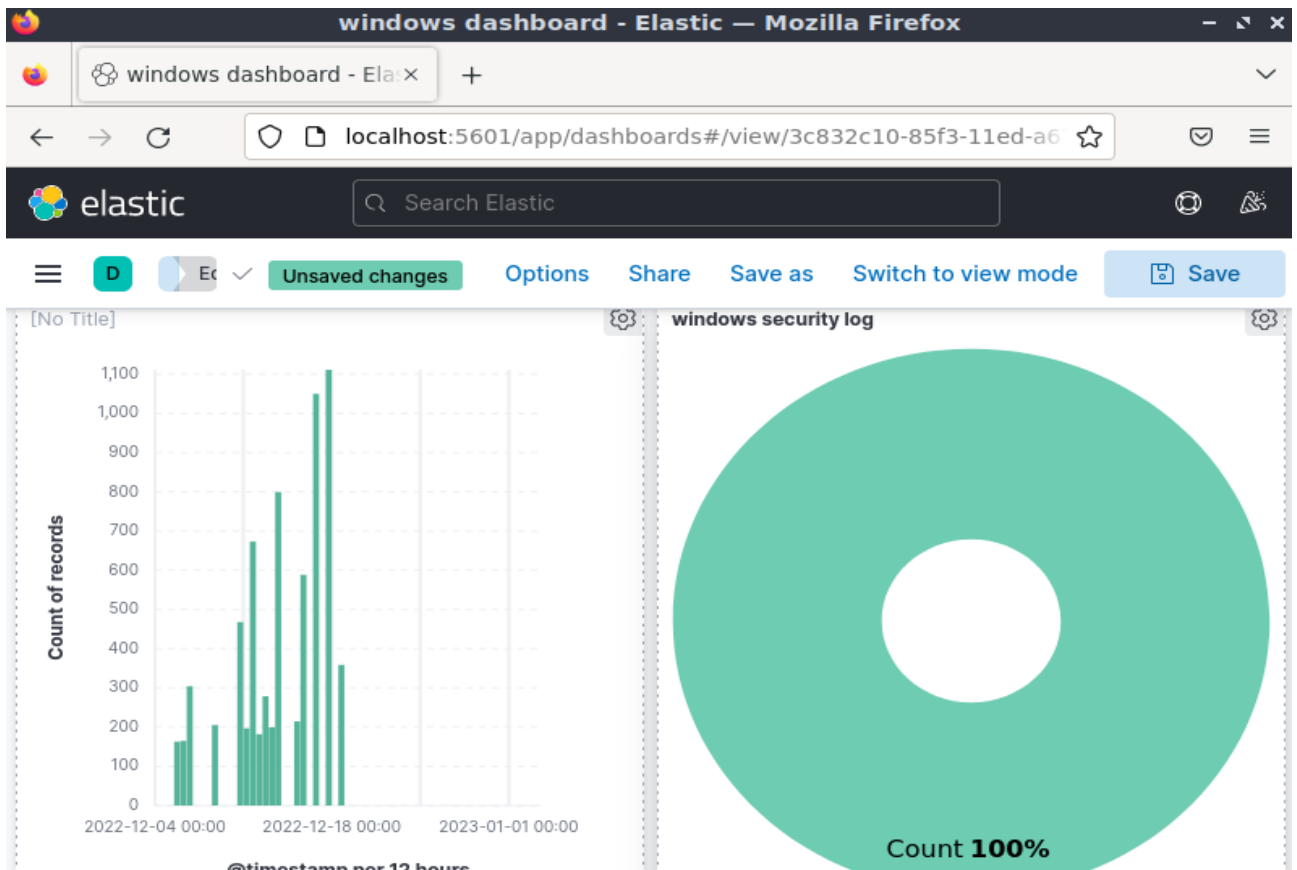
- Обновить Log4j и другие уязвимые продукты до последней версии (например, использовать JDK последней версии). Будьте внимательны к изменениям от поставщиков программного обеспечения в активе и немедленно применяйте обновления к активам, когда поставщик уведомляет о том, что в его продукте есть исправление для этой уязвимости.
- Продолжайте отслеживать веб-страницу уязвимостей безопасности Apache Log4j(<https://logging.apache.org/log4j/2.x/security.html>) на наличие новых обновлений.
- Блокировать конкретный исходящий протокол управления передачей (TCP) и UDP сетевого трафика (исходящий LDAP, удаленный вызов метода (RMI), исходящий DNS).
- Когда требуется удаленный доступ, используйте безопасные методы, такие как виртуальные частные сети (VPN), признайте, что VPN могут иметь уязвимости и должны быть обновлены до самой последней версии, что имеется в наличии.

3. Сбор логов Windows и их анализ

С Windows 7 Professional были собраны Windows Security Log:

The screenshot shows the Elastic Discover interface in a Mozilla Firefox browser. The address bar shows the URL `localhost:5601/app/discover#/?_g=(filters:!(),refreshInterval:(p`. The Elastic logo is visible in the top left, and a search bar labeled "Search Elastic" is in the top center. The interface includes a navigation bar with buttons like "Discover", "Options", "New", "Open", "Share", "Inspect", and "Save". Below this, there's a search bar with a dropdown menu, a "KQL" button, a date range selector set to "Last 30 days", a "Show dates" button, and a "Refresh" button. The main content area shows "6,958 hits" and a "Chart options" button. The search results are displayed in a table with two columns: "Time" and "Document". The first document entry shows a timestamp of "Dec 24, 2022 @ 19:20:03.204" and a version of "1". The document fields include `agent.ephemeral_id`, `agent.id`, `agent.name` (Админ-ПК), `agent.type` (winlogbeat), `agent.version` (8.5.3), `ecs.version` (8.0.0), `event.action` (Вход в систему), `event.code` (4624), and `event.created` (Dec 24, 2022 @ 19:20:03.204).

А также на основе этого создан dashboard:



Категории событий, которые могут быть зарегистрированы в Windows Security Log:

- События входа в учетную запись
- Управление аккаунтом
- Доступ к службе каталогов
- События входа
- Доступ к объекту
- Изменение политики
- Привилегированное использование
- Отслеживание процессов
- Системные события

Можно провести поиск угроз с помощью журнала безопасности Windows. Для этого проверим event.code каждого события. Логи, представляющие опасность, представлены в переводе статьи “Threat Hunting Using Windows Security Log (Поиск угроз с помощью журнала безопасности Windows)”.

Успешному входу в операционную систему соответствует номер 4624.

Пример:

The screenshot shows the Elastic Discover interface in a Mozilla Firefox browser. The address bar shows the URL `localhost:5601/app/discover#/?_g=(filters:!(),refreshInterval:(p`. The Elastic logo is visible in the top left. The search bar contains the query `event.code : 4624`. Below the search bar, there are buttons for "Options", "New", "Open", "Share", "Inspect", and "Save". The search results show 441 hits. The first two hits are displayed in a table with columns "Time" and "Document".

Time	Document
Dec 18, 2022 @ 21:46:34.189	<pre>@timestamp: Dec 18, 2022 @ 21:46:34.189 @version: 1 agent.ephemeral_id: 6c8d3a01-b60a-489f-9001-32c8f00702b1 agent.id: 3a44c9c0-ebf7-4983-91fc-eed9a1761023 agent.name: Админ-ПК agent.type: winlogbeat agent.version: 8.5.3 ecs.version: 8.0.0 event.action: None event.code: 7036 event.created: Dec 18, 2022 @</pre>
Dec 18, 2022 @ 21:44:30.870	<pre>@timestamp: Dec 18, 2022 @ 21:44:30.870 @version: 1 agent.ephemeral_id: 6c8d3a01-b60a-489f-9001-32c8f00702b1</pre>

Номера событий, представляющих угрозу: 4771, 4625, 4794, 4793, 4713, 4719, 4728, 4732, 4756, 4697, 4672, 4688, 4724, 4723, 4798, 4720, 4698, 4702, 4648, 4735, 4737, 4755, 1102, 4765, 4766.

На основе списка, представленного выше, были найдены события, представляющие опасность, а именно 4625, 4672, 4648:

event.code : 4625 KQL Last 30 days Show dates Refresh

+ Add filter

10 hits Chart options

log.level	сведения
message	Подсистема EventSystem подавляет повторяющиеся элементы журнала событий в течение 86400 сек. Таймаут подавления управляется значением REG_DWORD с именем SuppressDuplicateDuration в следующем разделе реестра: HKLM\Software\Microsoft\EventSystem\EventLog.
tags	beats_input_codec_plain_applied, _grokparsefailure
winlog.api	wineventlog
winlog_channel	Application

Идентификатор события 4625 — неудачные попытки входа в систему.
Описание:

- Если попытка входа в учетную запись не удалась, когда учетная запись уже заблокирована, запускается это событие. Он также генерируется при неудачной попытке входа в систему, что приводит к блокировке учетной записи.
- Он появляется на машине, на которой была предпринята попытка входа в систему; например, если попытка входа была предпринята на рабочей станции пользователя, событие появится на этой рабочей станции.
- Это событие произойдет на контроллерах домена, рядовых серверах и рабочих станциях.

event.code : 4672 KQL Last 30 days Show dates Refresh

+ Add filter

357 hits Chart options

Новому сеансу входа назначены специальные привилегии.	
Субъект:	
ИД безопасности:	S-1-5-18
Имя учетной записи:	система
Домен учетной записи:	NT AUTHORITY
У	
Код входа:	0x3e7
Привилегии:	SeAssignPrimaryTokenPrivilege
ge	SeTcbPrivilege

Идентификатор события — 4672 — специальные привилегии, назначенные новому входу в систему.

Описание:

Это событие создает новые входы в учетную запись, если новому сеансу входа назначены какие-либо из конфиденциальных привилегий.

event.code : 4648 KQL Last 30 days Show dates Refresh

+ Add filter

28 hits Chart options

Выполнена попытка входа в систему с явным указанием учетных данных.

Субъект:

ИД безопасности:	S-1-5-18
Имя учетной записи:	АДМИН-ПК\$
Домен учетной записи:	WORKGROUP
Код входа:	0x3e7
GUID входа:	{00000000-0000-0000-0000-000000000000}

Были использованы учетные данные следующей учетной записи:

Идентификатор события — 4648 — попытка входа в систему с использованием явных учетных данных.

Описание:

Это событие генерируется, когда процесс пытается войти в систему с помощью явного указания учетных данных этой учетной записи. Чаще всего это происходит в конфигурациях пакетного типа, таких как запланированные задачи, или при использовании команды «RUNAS». Это также обычное событие, которое периодически происходит во время нормальной работы операционной системы.

4. Сбор логов локальной машины (Lubuntu 20.04 LTS) и их анализ

Учитывая конфигурацию Filebeat, представленную в разделе 1, можно собрать логи с локальной машины, а именно логи, находящиеся по адресу `/var/log/*.log`

В данном случае, нас интересуют логи SSH (`auth.log`) и `syslog`.

4.1. Шаблоны Grok для фильтрации подозрительных событий в `auth.log`

Grokking – это извлечение структурированных полей из одного текстового поля в документе. Вы выбираете, из какого поля извлекать совпадающие поля, а также шаблон grok, который, как вы ожидаете, будет совпадать. Шаблон grok похож на регулярное выражение, которое поддерживает выражения с псевдонимами, которые можно использовать повторно.

Журналы авторизации, которые обычно находятся либо в `/var/log/auth.log` (для систем на основе Debian), либо в `/var/log/secure` (для систем на основе RedHat), содержат много интересной информации, связанной с безопасностью, например неудачные и успешные Входы по SSH, попытки `sudo` или создание пользователей и групп. Давайте рассмотрим эти журналы поближе и посмотрим, как мы можем их анализировать и визуализировать.

Файлы журнала авторизации обычно создаются локальным сервером Syslog, который направляет к ним средства AUTH и AUTHPRIV. Это означает, что любая программа, работающая в системе, может записывать в эти файлы журналов через протокол системного журнала. Это также означает, что формат, используемый журналами авторизации, является форматом системного журнала, но часть сообщений в них отличается в зависимости от того, какая программа записывает каждую конкретную строку.

Авторизованные пользователи

Два примера шаблонов Grok, используемых для фильтрации авторизованных пользователей:

- `%{SYSLOGTIMESTAMP:system.auth.timestamp}`
`%{SYSLOGHOST:system.auth.hostname}`
`sshd(?:\\[%{POSINT:system.auth.pid}\\])?: %{DATA:system.auth.ssh.event}`
`%{DATA:system.auth.ssh.method} for (invalid user`
`)?%{DATA:system.auth.user} from %{IPORHOST:system.auth.ip} port`
`%{NUMBER:system.auth.port} ssh2(:`
`%{GREEDYDATA:system.auth.ssh.signature}))?`
- `%{SYSLOGTIMESTAMP:system.auth.timestamp}`
`%{SYSLOGHOST:system.auth.hostname}`
`sshd(?:\\[%{POSINT:system.auth.pid}\\])?: %{DATA:system.auth.ssh.event}`
`user %{DATA:system.auth.user} from %{IPORHOST:system.auth.ip}`

Если вы делаете это на машине, на которой сервер SSH открыт для Интернета и прослушивает порт по умолчанию, вы, вероятно, увидите массу

неудачных попыток. Такая атака грубой силы пытается перепробовать множество комбинаций имени пользователя и пароля. Используемых паролей нет в журналах, но можно посмотреть, какие имена пользователей используются чаще всего. Так, root является наиболее целевой учетной записью. После этого идет длинный список имен пользователей, которые часто встречаются в системах Linux, таких как ubuntu, wordpress, postgres, oracle, admin, а также общие имена, такие как alex, daniel, andrew и так далее.

Хотя эти атаки могут показаться простыми и с низкими шансами на успех, помните, что достаточно, чтобы один пользователь в системе имел слабый пароль, и он, вероятно, в конечном итоге будет использован. Методы снижения этого риска включают отключение аутентификации по паролю для SSH, отключение входа в систему с правами root через SSH и изменение порта SSH по умолчанию.

Говоря об аутентификации по паролю, после анализа логов таким образом легко проверить, были ли какие-либо успешные входы в систему с использованием паролей, когда вы ожидаете только входы с использованием закрытых ключей.

Sudo

Другой набор журналов, который может вас заинтересовать, — это журналы, созданные командой sudo. Любая команда, выполненная с помощью sudo, а также неудачные попытки регистрируются в журналах авторизации. Вот несколько примеров:

```
Feb 23 00:08:48 localhost sudo: vagrant : TTY=pts/1 ; PWD=/home/vagrant ; USER=root ;  
COMMAND=/bin/cat /var/log/secure  
Feb 24 00:13:02 precise32 sudo:      tsg : user NOT in sudoers ; TTY=pts/1 ; PWD=/home/vagrant ;  
USER=root ; COMMAND=/bin/ls
```

Следующий шаблон Grok может сопоставлять как успешные, так и неудачные команды sudo. В случае ошибок ошибка сохраняется в поле system.auth.sudo.error:

- `%{SYSLOGTIMESTAMP:system.auth.timestamp}`
`%{SYSLOGHOST:system.auth.hostname}`
`sudo(?:\\[\\%{POSINT:system.auth.pid}\\])?: \\s*%{DATA:system.auth.user} :(`
`%{DATA:system.auth.sudo.error} ;)? TTY=%{DATA:system.auth.sudo.tty} ;`
`PWD=%{DATA:system.auth.sudo.pwd} ;`
`USER=%{DATA:system.auth.sudo.user} ;`
`COMMAND=%{GREEDYDATA:system.auth.sudo.command}`

Таким образом, мы можем легко увидеть, какие команды чаще всего выполняются через sudo, какие пользователи выполняют команды с помощью sudo и когда, и о каких ошибках сообщил sudo. Эти данные могут быть полезны для обнаружения нарушений безопасности до их эскалации, поскольку, если злоумышленник завладеет непривилегированной учетной записью, скорее

всего, он сначала попытается использовать `sudo`, чтобы получить права суперпользователя.

Новые пользователи и группы

Еще одна вещь, за которой нужно следить в журналах авторизации, — это создание новых пользователей и групп. Пользователи часто создаются автоматически при установке пакетов, и важно убедиться, что они созданы с правильными привилегиями.

Вот как выглядят строки журнала, созданные программами `adduser` и `addgroup`:

```
Feb 22 11:47:05 localhost groupadd[6991]: new group: name=apache, GID=48
Feb 22 11:47:05 localhost useradd[6995]: new user: name=apache, UID=48, GID=48,
home=/usr/share/httpd, shell=/sbin/nologin
```

Необходимый Grok шаблон в таком случае выглядит следующим образом:

- `%{SYSLOGTIMESTAMP:system.auth.timestamp}`
`%{SYSLOGHOST:system.auth.hostname}`
`groupadd(?:\\[%{POSINT:system.auth.pid}\\])?: new group:`
`name=%{DATA:system.auth.groupadd.name},`
`GID=%{NUMBER:system.auth.groupadd.gid}`
`%{SYSLOGTIMESTAMP:system.auth.timestamp}`
`%{SYSLOGHOST:system.auth.hostname}`
`useradd(?:\\[%{POSINT:system.auth.pid}\\])?: new user:`
`name=%{DATA:system.auth.useradd.name},`
`UID=%{NUMBER:system.auth.useradd.uid},`
`GID=%{NUMBER:system.auth.useradd.gid},`
`home=%{DATA:system.auth.useradd.home},`
`shell=%{DATA:system.auth.useradd.shell}$`

Этот шаблон поможет получить обзор новых пользователей и когда они были созданы.

4.2. Syslog: скрытая угроза безопасности

Люди иногда забывают, что существует также ряд сервисов на основе UDP, которые могут представлять угрозу безопасности ваших систем. SNMP — это хорошо известная служба, печально известная тем, что для нее настроен пароль по умолчанию (или строка сообщества).

Но есть еще одна услуга, которая часто не рассматривается как риск. Это служба системного журнала (`syslog`). Системный журнал используется практически на всех UNIX-подобных платформах для записи сообщений системы в один или несколько файлов журнала на диск. Служба `syslog` часто слушает в сети UDP-порт 514. Обратите внимание, что `syslog` не выполняет никакой аутентификации данных, которые ему отправляются. Это значит, что злоумышленник может:

- Создать условие отказа в обслуживании (DoS), отправив большие объемы данных в службу системного журнала, заполнив дисковое пространство.
- Когда диск заполнен, журналы больше не могут быть сохранены, поэтому любая атака, оставляющая след в журналах, останется незамеченной.
- Отправляя большое количество специально созданных сообщений, злоумышленник может вызвать хаос, если журналы отслеживаются системами обнаружения вторжений или другими системами, создающими предупреждения.

Как атаковать? Просто использовать netcat: nc -u [IP-адрес] 514. Как только вы подключитесь, все, что вы наберете, будет зарегистрировано в файле журнала.

Как смягчить эту проблему? Ответ: изменить доступ брандмауэра к UDP-порту 514. Кроме того, необходимо убедиться, что служба syslog не прослушивает сеть, если это не требуется, только на локальном хосте.