

UT3 - Ejercicio 3: ACTIVIDAD Stack ELK Siem



UT3 - Ejercicio 3: ACTIVIDAD Stack ELK Siem

Victoria Eugenia Pérez González
02/02/2023

ÍNDICE

UT3 - Ejercicio 3: ACTIVIDAD Stack ELK Siem	1
1.- Configurar varias reglas de detección en el IDS Suricata:	3
a) Crear una regla que detecte si se visita sitios web (HTTP o HTTPS) cuyo nombre de dominio contenga la palabra prohibida hack:	3
b) Crear una regla que detecte si se establece cualquier tipo de comunicación con un equipo ubicado en un país prohibido.	6
2.- Instalar el servidor SSH en el equipo Linux ELK y configurar Logstash para que acceda al archivo de log del servicio SSH y pueda capturar sus eventos.	11
3.- Crear un nuevo dashboard en el SIEM ELK que muestre las siguientes gráficas a partir de los eventos recibidos: a) Un gráfico circular con el porcentaje de tráfico de cada tipo de protocolo (TCP, UDP, ICMP): Accederemos a la opción de menú Analytics->Dashboard y crearemos un nuevo dashboard:	19

Para el desarrollo de esta actividad se debe partir de una máquina virtual Linux Ubuntu desktop 20.04.3 (adaptador de red en modo puente) para instalar el stack ELK.

En este caso la máquina tendrá una dirección de ip de la red del aula. Comenzaremos por instalar el IDS Suricata en el equipo Linux ELK para que tenga al menos una fuente de eventos de seguridad que pueda procesar el SIEM ELK.

1.- Configurar varias reglas de detección en el IDS Suricata:

a) Crear una regla que detecte si se visita sitios web (HTTP o HTTPS) cuyo nombre de dominio contenga la palabra prohibida hack:

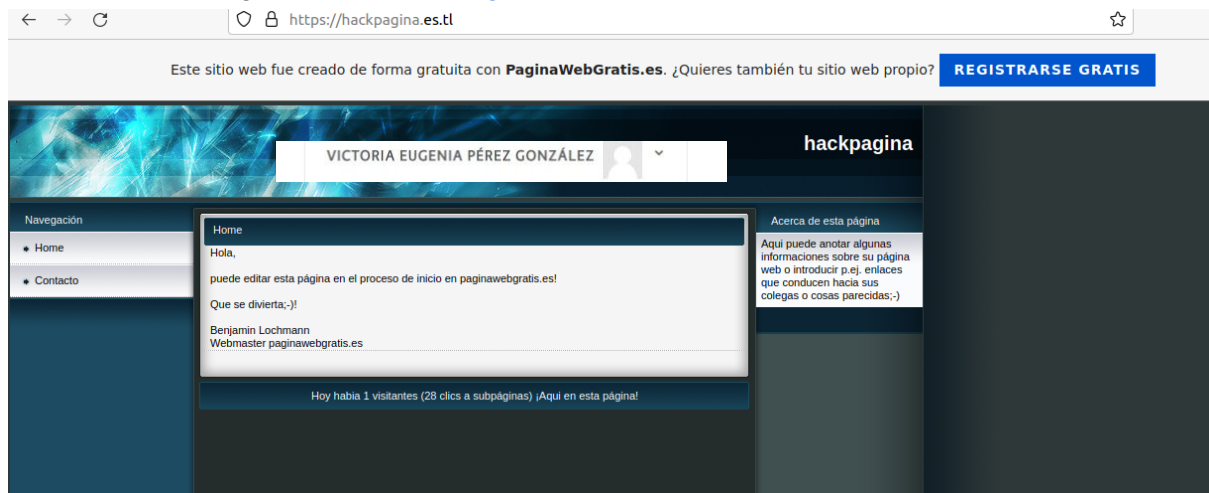
Se añade una nueva regla en el archivo suricata.rules para el puerto https

```
GNU nano 4.8 suricata.rules
alert icmp any any -> any any (msg:"Ping detectado"; sid:200001;)
alert dns any any -> any 53 (msg:"Petición dns a google detectada"; sid:200002;)
alert tcp any any -> any 22 (msg:"Conexión a SSH detectada"; sid:200003;)
alert tcp any any -> any 443 (msg:"Alerta puerto 8080 pagina con contenido hack";content:"hack"; sid:200004;)
VICTORIA EUGENIA PÉREZ GONZÁLEZ
```

Se reinicia el servicio:

```
victoriap@victoriap:/var/lib/suricata/rules$ sudo systemctl restart suricata.service
victoriap@victoriap:/var/lib/suricata/rules$
VICTORIA EUGENIA PÉREZ GONZÁLEZ
```

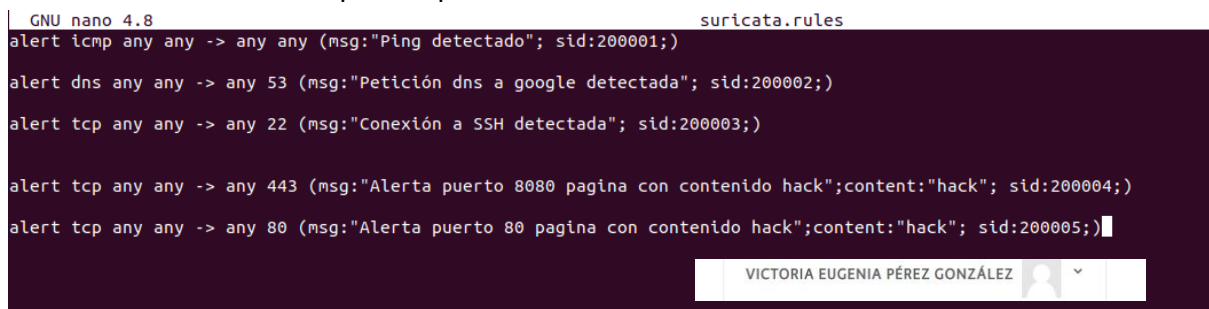
Se accede a la página <https://hackpagina.es.tl>



y detecta la alerta.

```
01/28/2023-16:52:00.164352  [**] [1:200004:0] Alerta puerto 8080 pagina con contenido hack [**] [Classification: (null)] [Priority: 3] (TCP) 192.168.0.28:37022 -> 193.238.27.26:443
```

Se crea una nueva alerta para el puerto 80:



Se entra en la página <http://www.hackerproducciones.com>



y detecta la alerta.

```
-> 212.166.132.104:53
01/28/2023-16:55:39.007222  [**] [1:200005:0] Alerta puerto 80 pagina con contenido hack [**] [Classification: (null)] [Priority: 3] {TCP} 192.168
.0.28:45034 -> 217.160.0.67:80
01/28/2023-16:55:39.020783  [**] [1:200005:0] Alerta puerto 80 pagina con contenido hack [**] [Classification: (null)] [Priority: 3] {TCP} 192.168
.0.28:45022 -> 217.160.0.67:80
```

Se comprueba accediendo vía web.

Table

VICTORIA EUGENIA PÉREZ GONZÁLEZ

Top values of evento.keyword	@timestamp per 30 minutes	Cantidad registros
Alerta puerto 80 pagina con contenido hack [**] [Classification: (null)] [Priority: 3]	16:30	31
Alerta puerto 8080 pagina con contenido hack [**] [Classification: (null)] [Priority: ...]	16:30	1
Petición dns a google detectada [**] [Classification: (null)] [Priority: 3]	16:30	117
Other	16:30	3

b) Crear una regla que detecte si se establece cualquier tipo de comunicación con un equipo ubicado en un país prohibido.

Es posible saber desde qué país se conecta un equipo a Internet a través de su dirección IP pública. La organización IANA reparte las direcciones IP públicas asignando rangos de direcciones a cada continente y país. De esta forma, dada una dirección IP pública, podemos determinar su país de procedencia sin más que consultar una BBDD de geolocalización de direcciones IP (GeoIP) como <https://www.maxmind.com/en/solutions/geoip2-enterprise-product-suite/anonymous-ip-database>.

Para poder descargar la BBDD de direcciones IP públicas junto con sus países, debemos registrarnos en: <https://www.maxmind.com/en/geolite2/signup?lang=en> (podemos usar una cuenta de temp-mail.org para registrarnos) Una vez recibido el enlace de acceso, indicaremos una password e iniciaremos sesión con la cuenta de correo que especificamos anteriormente. Debemos descargar del archivo GZIP que contiene la BBDD GeoLite2 Country en formato mmdb.




Entorno Virtual de Apre...991NTA - IHC - 22-23: UT...Account Summary | MaxMindGeoLite2 Sign Up | MaxMind

https://www.maxmind.com/en/accounts/819387/people/dea1dc01-312f-47bd-b6c3-c1d4d8577274

You're using our free data. Upgrade to GeoIP2 for more accurate data.

MAXMIND

ProductsSupportDevelopersCompanyBlogContact



VICTORIA EUGENIA PÉREZ GONZÁLEZ

Account Summary

Account

Account Summary

Account Information

Manage License Keys

Manage Account Services

Manage Users

Account Activity

Edit My Info

Change Password

Two-Factor Authentication

Billing

Payment Method

Payment History

Purchase or Manage Databases

Query Usage Report

To comply with data privacy regulations, please monitor our [Do Not Sell My Personal Information Requests page](#) for IP addresses and networks that should not be used for advertising or marketing purposes.

Thank you for using MaxMind's services. Please take a moment to review our [privacy policy](#).


Resources

- Learn how to Manage your Account
- MaxMind Knowledge Base
- Developer Portal
- minFraud Release Notes and GeoIP2 Release Notes

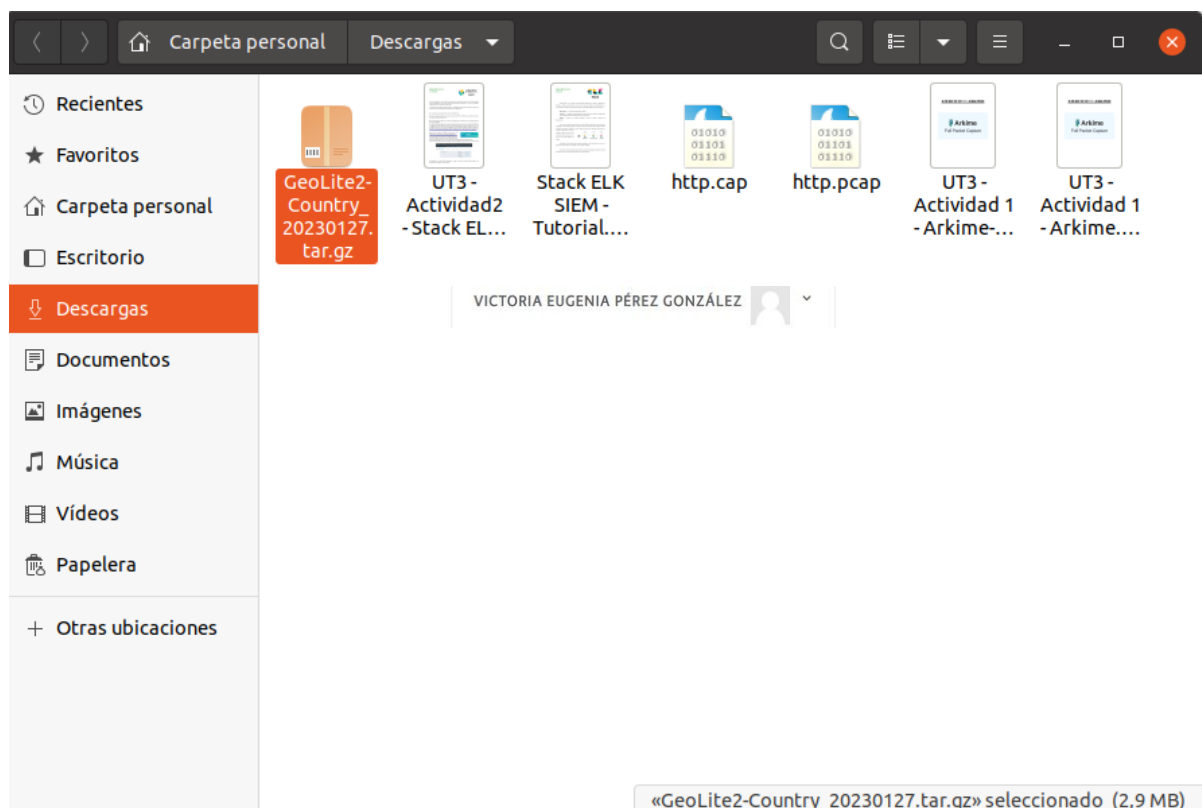
Database Products and Subscriptions

[Download Databases](#)
[View Your Download History](#)

Databases	Access Starts	Access Ends
GeoLite2 Country	2023-01-29	No end date

	2023-01-27	
<div>GeoLite2 Country</div> <div><div>VICTORIA EUGENIA PÉREZ GONZÁLEZ</div><div></div></div>	<div>Edition ID: GeoLite2-Country</div> <div>Format: GeoIP2 Binary (.mmdb) (APIs)</div> <div>Updated: 2023-01-27</div>	<ul style="list-style-type: none">Download GZIPDownload SHA256Get Permalinks

Página 7 de 20



Descomprimir el archivo GZIP descargado y copiar el archivo GeoLite2-Country.mmdb en el directorio de Suricata (/var/lib/suricata):

```
victoriap@victoriap:~/Descargas$ tar -xvf GeoLite2-Country_20230127.tar.gz
GeoLite2-Country_20230127/
GeoLite2-Country_20230127/LICENSE.txt
GeoLite2-Country_20230127/COPYRIGHT.txt
GeoLite2-Country_20230127/GeoLite2-Country.mmdb
victoriap@victoriap:~/Descargas$

victoriap@victoriap:~/Descargas/GeoLite2-Country_20230127$ ls
COPYRIGHT.txt  GeoLite2-Country.mmdb  LICENSE.txt
victoriap@victoriap:~/Descargas/GeoLite2-Country_20230127$ sudo cp GeoLite2-Country.mmdb /var/lib/suricata
victoriap@victoriap:~/Descargas/GeoLite2-Country_20230127$
```

Editar el archivo de configuración de Suricata /etc/suricata/suricata.yaml y ajustar esta directiva: geoip-database: /var/lib/suricata/GeoLite2-Country.mmdb


```
GNU nano 4.8 /etc/suricata/suricata.yaml
#
# hash - Flow assigned to threads using the 5-7 tuple hash.
# ippair - Flow assigned to threads using addresses only.
#
#autofp-scheduler: hash

# Preallocated size for each packet. Default is 1514 which is the classical
# size for pcap on Ethernet. You should adjust this value to the highest
# packet size (MTU + hardware header) on your system.
#default-packet-size: 1514

# Unix command socket that can be used to pass commands to Suricata.
# An external tool can then connect to get information from Suricata
# or trigger some modifications of the engine. Set enabled to yes
# to activate the feature. In auto mode, the feature will only be
# activated in live capture mode. You can use the filename variable to set
# the file name of the socket.
unix-command:
  enabled: auto
  #filename: custom.socket

# Magic file. The extension .mgc is added to the value here.
#magic-file: /usr/share/file/magic
#magic-file:

# GeoIP2 database file. Specify path and filename of GeoIP2 database
# if using rules with "geoip" rule option.
geoip-database: /var/lib/suricata/GeoLite2-Country.mmdb

legacy:
  uricontent: enabled
```

Seguidamente editar el archivo de reglas `/var/lib/suricata/rules/suricata.rules` y añadir la siguiente regla para detectar cualquier tráfico hacia/desde un equipo con una dirección IP ubicada en algún país prohibido. En este caso, detectará si hay comunicación con algún equipo de Rusia (RU), China (CN) o Corea del Norte (KP):

```
alert ip any any <> any any (msg:"Detectado tráfico con un país prohibido";
geoip:RU,CN,KP; sid:2000005;)
```

```
GNU nano 4.8 suricata.rules
#alert icmp any any -> any any (msg:"Ping detectado"; sid:2000001;)

#alert dns any any -> any 53 (msg:"Petición dns a google detectada"; sid:2000002;)

alert tcp any any -> any 22 (msg:"Conexión a SSH detectada"; sid:2000003;)

alert tcp any any -> any 443 (msg:"Alerta puerto 8080 página con contenido hack";content:"hack"; sid:2000004;)
alert tcp any any -> any 80 (msg:"Alerta puerto 80 página con contenido hack";content:"hack"; sid:2000005;)
alert ip any any <> any any(msg:"Detectado tráfico país prohibido";geoip:RU,CN,KP; sid:2000006;)
|
```

Luego reiniciamos Suricata para que aplique los cambios realizados en la configuración:

```
#suricata -T && systemctl restart suricata
```

Seguidamente probar la primera regla de detección visitando sitios web con la palabra hack:

```
#curl -L http://www.hacking.es https://elhacker.net
```


Y probar la segunda regla enviando pings o visitando sitios web alojados en países prohibidos:

```
#ping www.game.ru
#ping www.amazon.cn
#ping kcna.kp
```

```
01/29/2023-10:59:11.317680  [**] [1:200006:0] Detectado tráfico pais prohibido [
**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.28:8 -> 175.45.176.7
1:0
01/29/2023-10:59:12.340785  [**] [1:200006:0] Detectado tráfico pais prohibido [
**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.28:8 -> 175.45.176.7
1:0
01/29/2023-10:59:13.365096  [**] [1:200006:0] Detectado tráfico pais prohibido [
**] [Classification: (null)] [Priority: 3] {ICMP} 192.168.0.28:8 -> 175.45.176.7
1:0
01/29/2023-11:00:05.573786  [**] [1:200004:0] Alerta puerto 8080 pagina con cont
enido hack [**] [Classification: (null)] [Priority: 3] {TCP} 192.168.0.28:38532
-> 172.67.69.232:443
```

Top values of evento.keyword	@timestamp pei	Cantidad registr
Alerta puerto 80 pagina con contenido hack [**] [Classification: (null)] [Priority: 3]	10:30	3
Alerta puerto 80 pagina con contenido hack [**] [Classification: (null)] [Priority: 3]	11:00	1
Alerta puerto 8080 pagina con contenido hack [**] [Classification: (null)] [Priority: 3]	10:30	3
Alerta puerto 8080 pagina con contenido hack [**] [Classification: (null)] [Priority: 3]	11:00	1
Detectado tráfico pais prohibido [**] [Classification: (null)] [Priority: 3]	10:30	77
Detectado tráfico pais prohibido [**] [Classification: (null)] [Priority: 3]	11:00	12
Other	10:30	129
Other	11:00	8

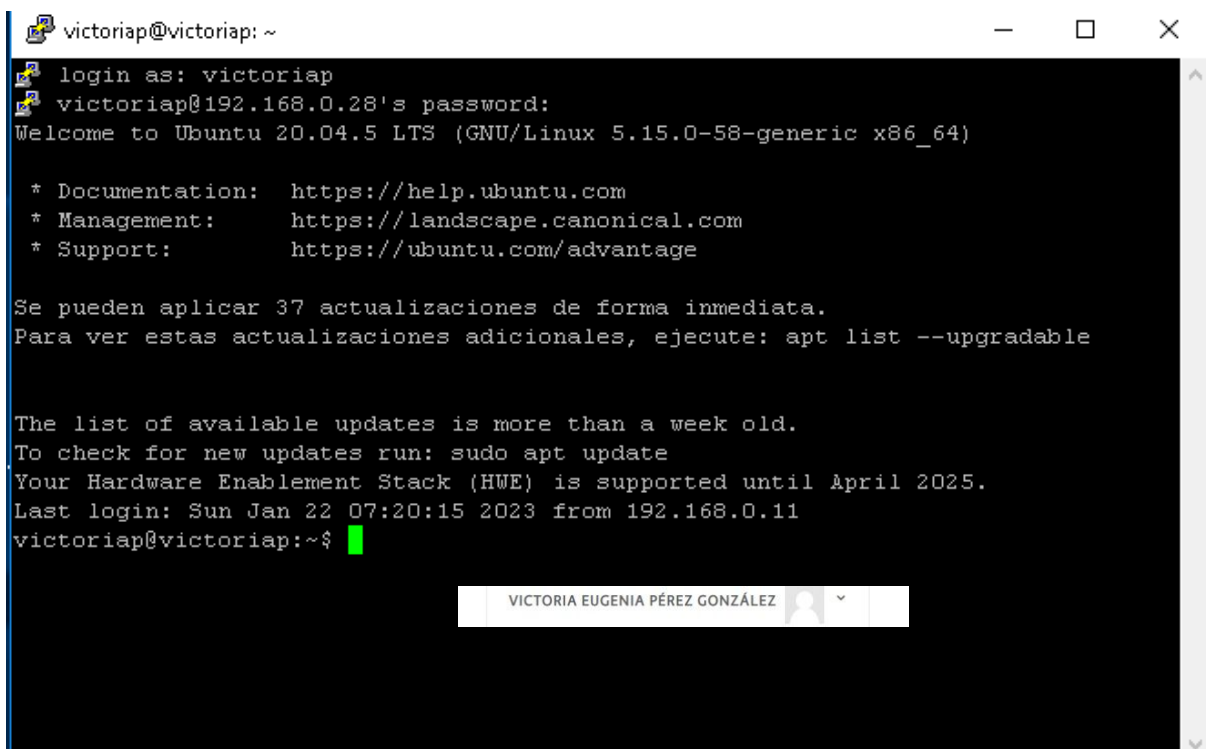
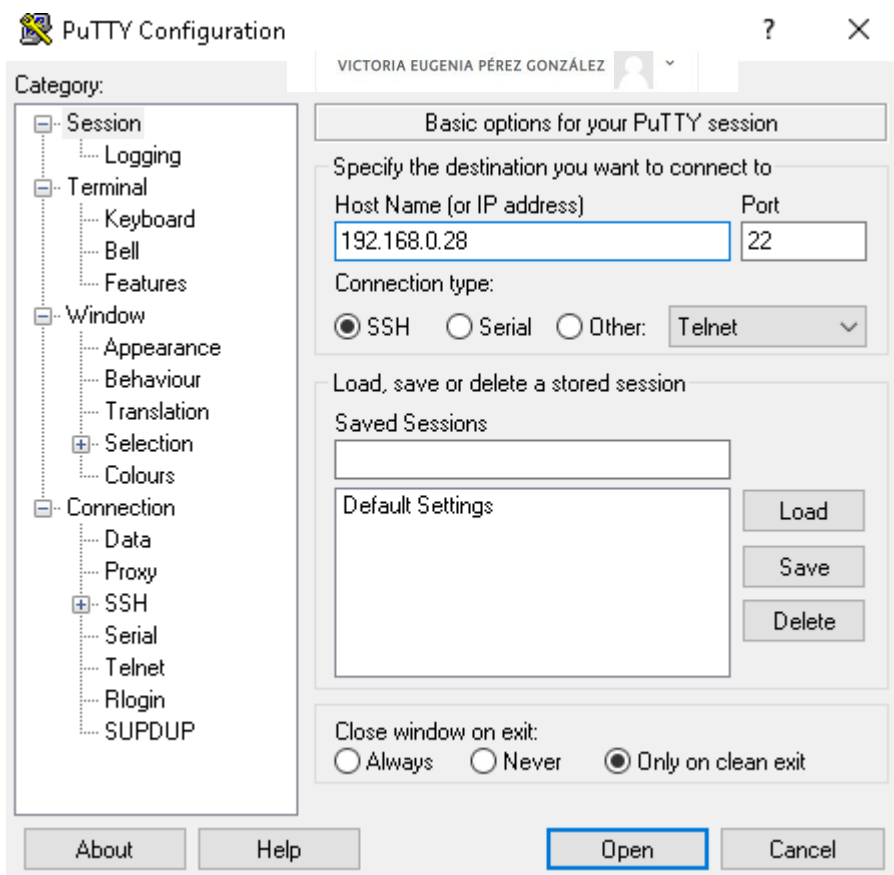
2.- Instalar el servidor SSH en el equipo Linux ELK y configurar Logstash para que acceda al archivo de log del servicio SSH y pueda capturar sus eventos.

A terminal window titled 'victoriap@victoriap: /' with standard window controls. The user runs 'sudo systemctl status ssh'. The output shows the 'ssh.service' is 'active (running)' since Sun 2023-01-29 10:30:28 WET. It lists details like the process (sshd), main PID (767), tasks, memory, and CGroup. At the bottom, there are three log entries: 'Starting OpenBSD Secure Shell server...', 'Server listening on 0.0.0.0 port 22.', and 'Started OpenBSD Secure Shell server.' The terminal also shows 'lines 1-15/15 (END)' and a user bar at the bottom with the name 'VICTORIA EUGENIA PÉREZ GONZÁLEZ' and a profile icon.

```
victoriap@victoriap:/$ sudo systemctl status ssh
[sudo] contraseña para victoriap:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: en
   Active: active (running) since Sun 2023-01-29 10:30:28 WET; 33min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 718 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 767 (sshd)
       Tasks: 1 (limit: 6426)
      Memory: 2.3M
         CGroup: /system.slice/ssh.service
                └─767 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

ene 29 10:30:25 victoriap systemd[1]: Starting OpenBSD Secure Shell server...
ene 29 10:30:28 victoriap sshd[767]: Server listening on 0.0.0.0 port 22.
ene 29 10:30:28 victoriap systemd[1]: Started OpenBSD Secure Shell server.
lines 1-15/15 (END)
```

Realizaremos alguna conexión de prueba para generar eventos en el log del servicio SSH:



Luego consultaremos cuál es el formato de las líneas del archivo de log de SSH ubicado en `/var/log/auth.log`

```
victoriap@victoriap:/$ tail -f /var/log/auth.log
Jan 29 11:05:45 victoriap sshd[3745]: Failed password for invalid user vitoriap
from 127.0.0.1 port 47222 ssh2
Jan 29 11:05:50 victoriap sshd[3745]: pam_unix(sshd:auth): check pass; user unkn
own
Jan 29 11:05:53 victoriap sshd[3745]: Failed password for invalid user vitoriap
from 127.0.0.1 port 47222 ssh2
Jan 29 11:05:56 victoriap sshd[3745]: Connection closed by invalid user vitoriap
127.0.0.1 port 47222 [preauth]
Jan 29 11:05:56 victoriap sshd[3745]: PAM 1 more authentication failure; logname
= uid=0 euid=0 tty=ssh ruser= rhost=127.0.0.1
Jan 29 11:05:56 victoriap sudo: pam_unix(sudo:session): session closed for user
root
Jan 29 11:11:12 victoriap gdm-password]: gkr-pam: unlocked login keyring
Jan 29 11:13:20 victoriap sshd[3822]: Accepted password for victoriap from 192.1
68.0.11 port 49757 ssh2
Jan 29 11:13:20 victoriap sshd[3822]: pam_unix(sshd:session): session opened for
user victoriap by (uid=0)
Jan 29 11:13:20 victoriap systemd-logind[603]: New session 4 of user victoriap.
```

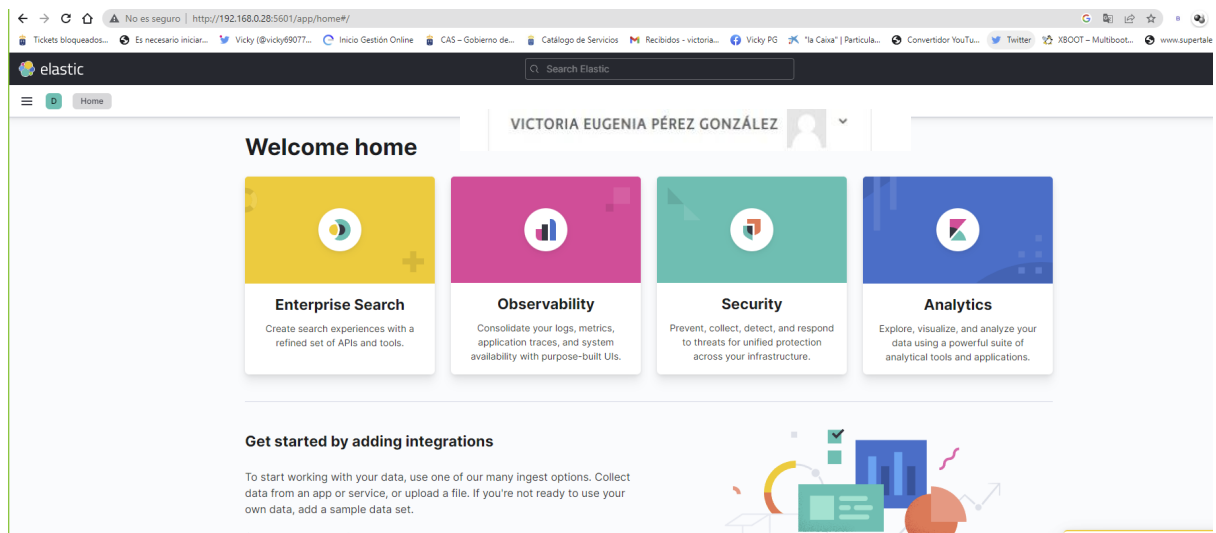
VICTORIA EUGENIA PÉREZ GONZÁLEZ

Ahora debemos configurar Logstash creando un patrón o filtro que le permita procesar las líneas del log para reconocer los eventos del servidor SSH y poder gestionarlos en ELK.

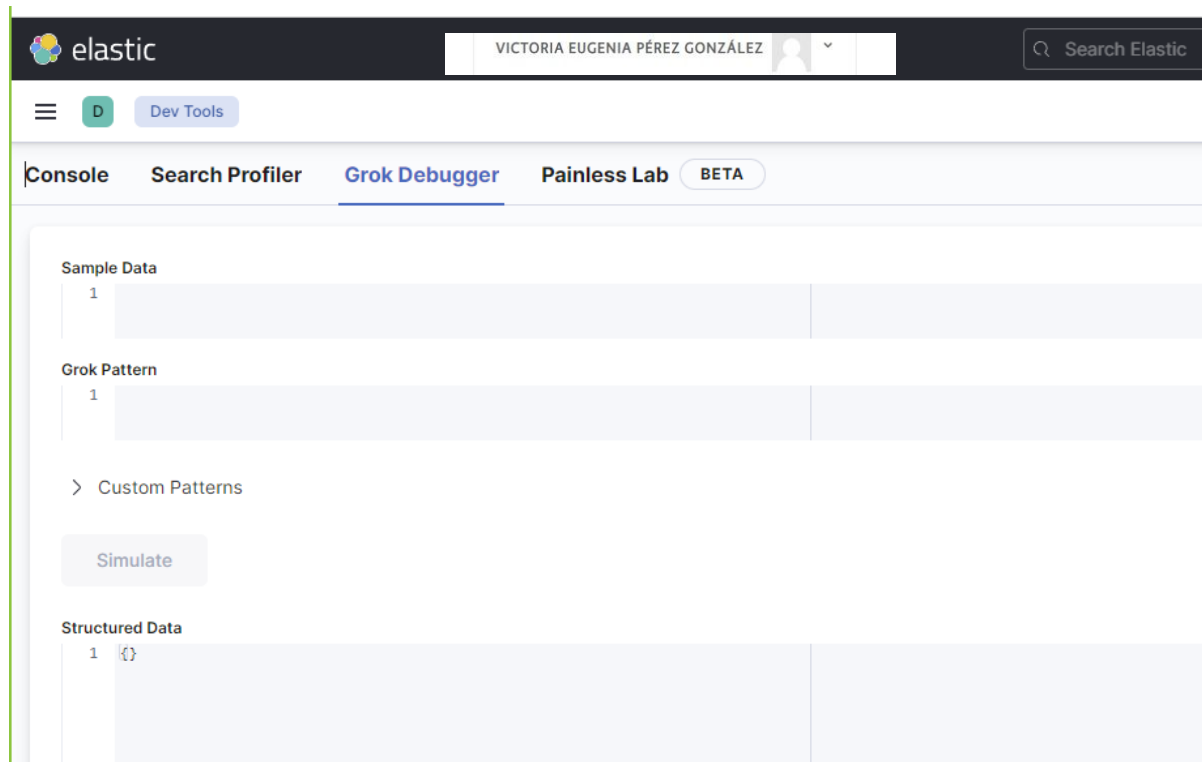
Para crear cómodamente el patrón, accederemos a la web de ELK:

<http://IPelk:5601>

En caso de que no cargue la web de ELK (Kibana server is not ready yet), debemos comprobar el estado de elasticsearch y reiniciarlo si fuese preciso:



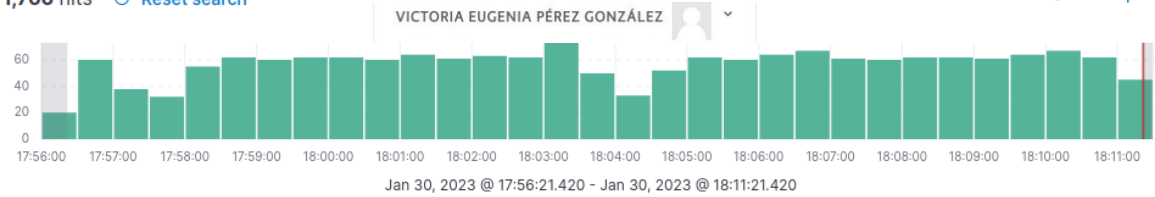
En la web de Kibana elegiremos la opción de menú Management->Dev Tools->Grok Debugger



Luego pegaremos en la sección Sample Data una la línea que copiaremos del archivo de log de SSH /var/log/auth.log y crearemos un patrón simple que reconozca el evento:

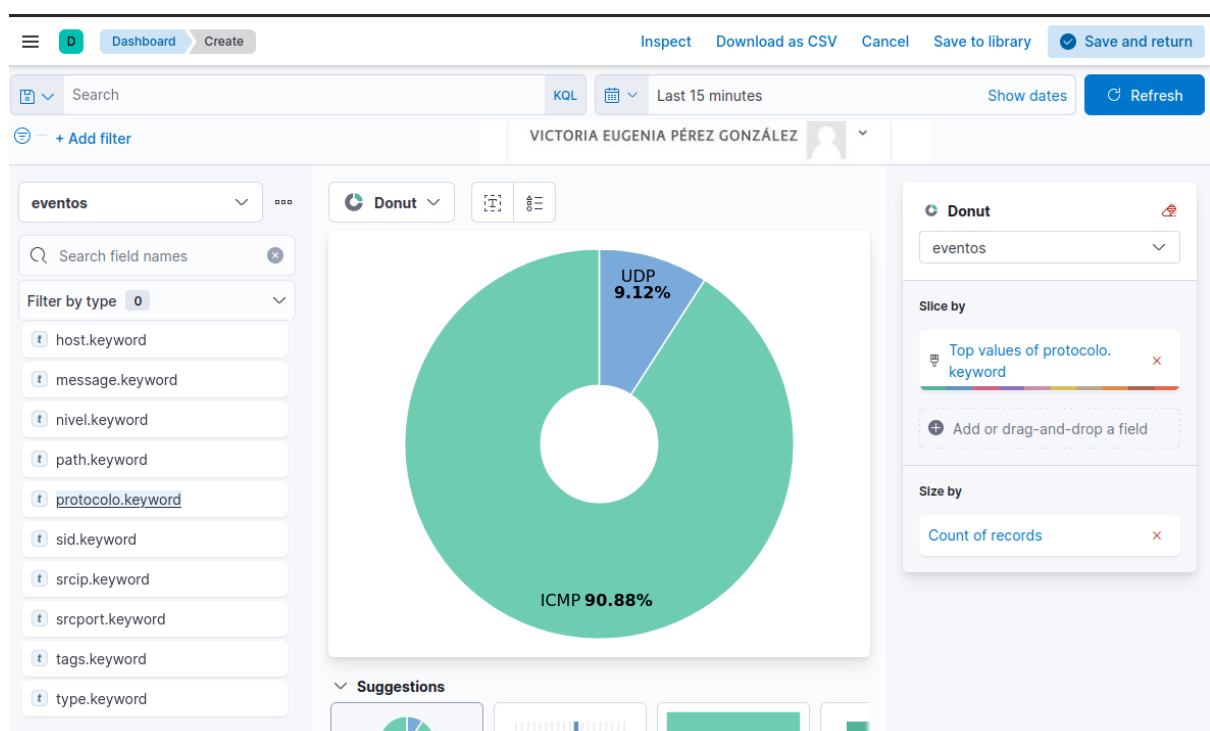
1,766 hits [Reset search](#)

[Chart options](#)

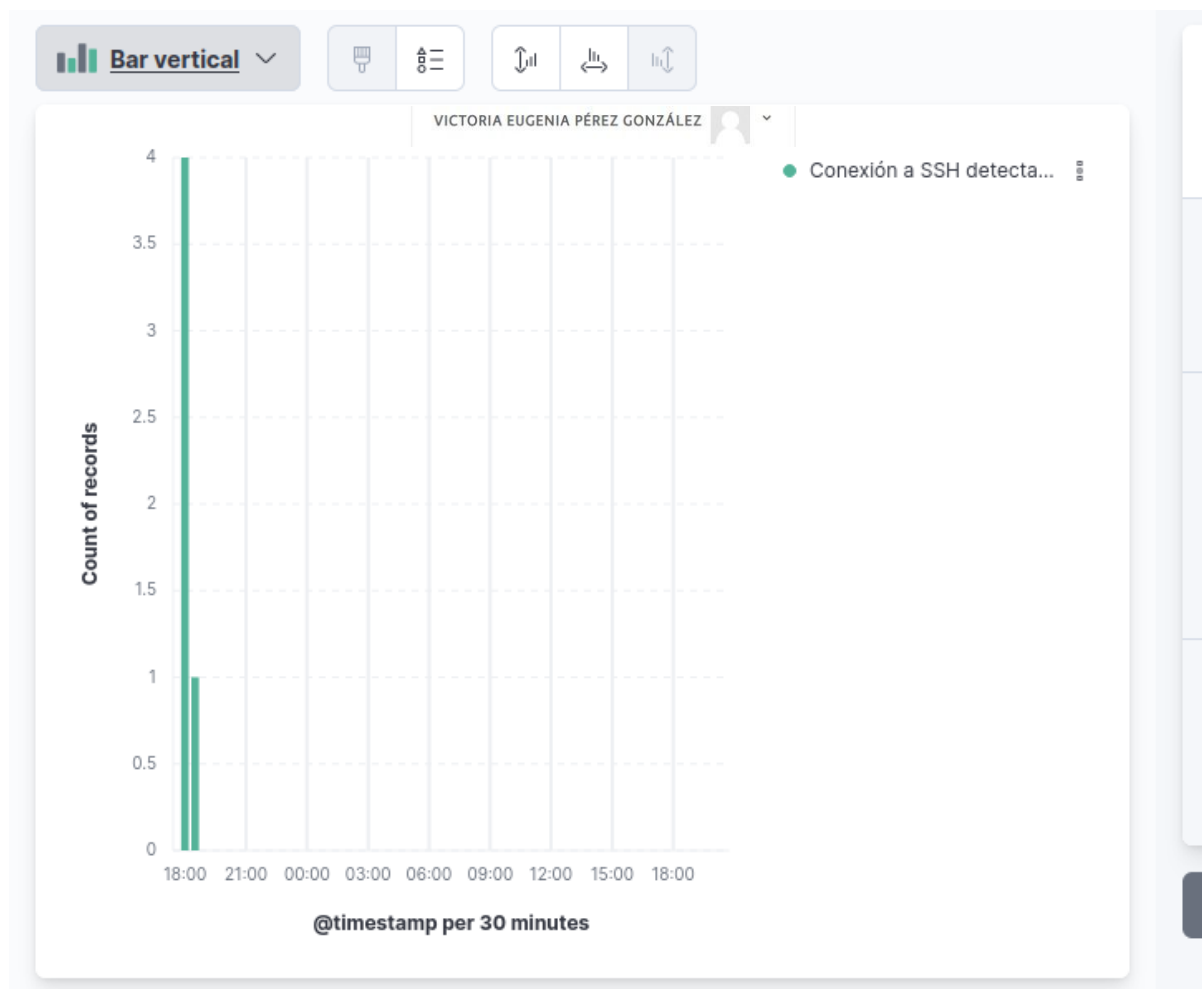


Time ↓	dstip	nivel	type	evento	usuario
> Jan 30, 2023 @ 18:11:20.457	54.222.60.218	3	suricata	Detectado trafico con un pais prohibido [**] [Clas sification: (null)]	victoriap
> Jan 30, 2023 @ 18:11:20.457	192.168.24.135	3	suricata	Detectado trafico con un pais prohibido [**] [Clas sification: (null)]	victoriap
> Jan 30, 2023 @ 18:11:19.456	54.222.60.218	3	suricata	Detectado trafico con un pais prohibido [**] [Clas sification: (null)]	victoriap
> Jan 30, 2023 @ 18:11:19.456	192.168.24.135	3	suricata	Detectado trafico con un pais prohibido [**] [Clas sification: (null)]	victoriap
> Jan 30, 2023 @ 18:11:19.456	172.20.200.1	3	suricata	Petición dns a google detectada [**] [Classificati on: (null)]	victoriap
> Jan 30, 2023 @ 18:11:19.456	172.20.200.1	3	suricata	Petición dns a google detectada [**] [Classificati on: (null)]	victoriap
> Jan 30, 2023 @ 18:11:18.455	192.168.24.135	3	suricata	Detectado trafico con un pais prohibido [**] [Clas sification: (null)]	victoriap
> Jan 30, 2023 @ 18:11:18.454	54.222.60.218	3	suricata	Detectado trafico con un pais prohibido [**] [Clas sification: (null)]	victoriap
> Jan 30, 2023 @ 18:11:17.452	54.222.60.218	3	suricata	Detectado trafico con un pais prohibido [**] [Clas sification: (null)]	victoriap


3.- Crear un nuevo dashboard en el SIEM ELK que muestre las siguientes gráficas a partir de los eventos recibidos: a) Un gráfico circular con el porcentaje de tráfico de cada tipo de protocolo (TCP, UDP, ICMP): Accederemos a la opción de menú Analytics->Dashboard y crearemos un nuevo dashboard:



b) Una gráfica de barras con la evolución temporal de la cantidad de conexiones SSH detectadas:



c) Una tabla con las 10 direcciones IP de destino que más aparecen en los eventos de seguridad:


Table

Top values of dstip.keyword		Count of records
54.222.60.218		1,899
192.168.24.135	VICTORIA EUGENIA PÉREZ GONZÁLEZ	1,792
172.20.200.1		265

d) Añadir un contador de la cantidad de webs prohibidas visitadas:



Finalmente mostraremos el panel dashboard con las cuatro gráficas creadas:

