

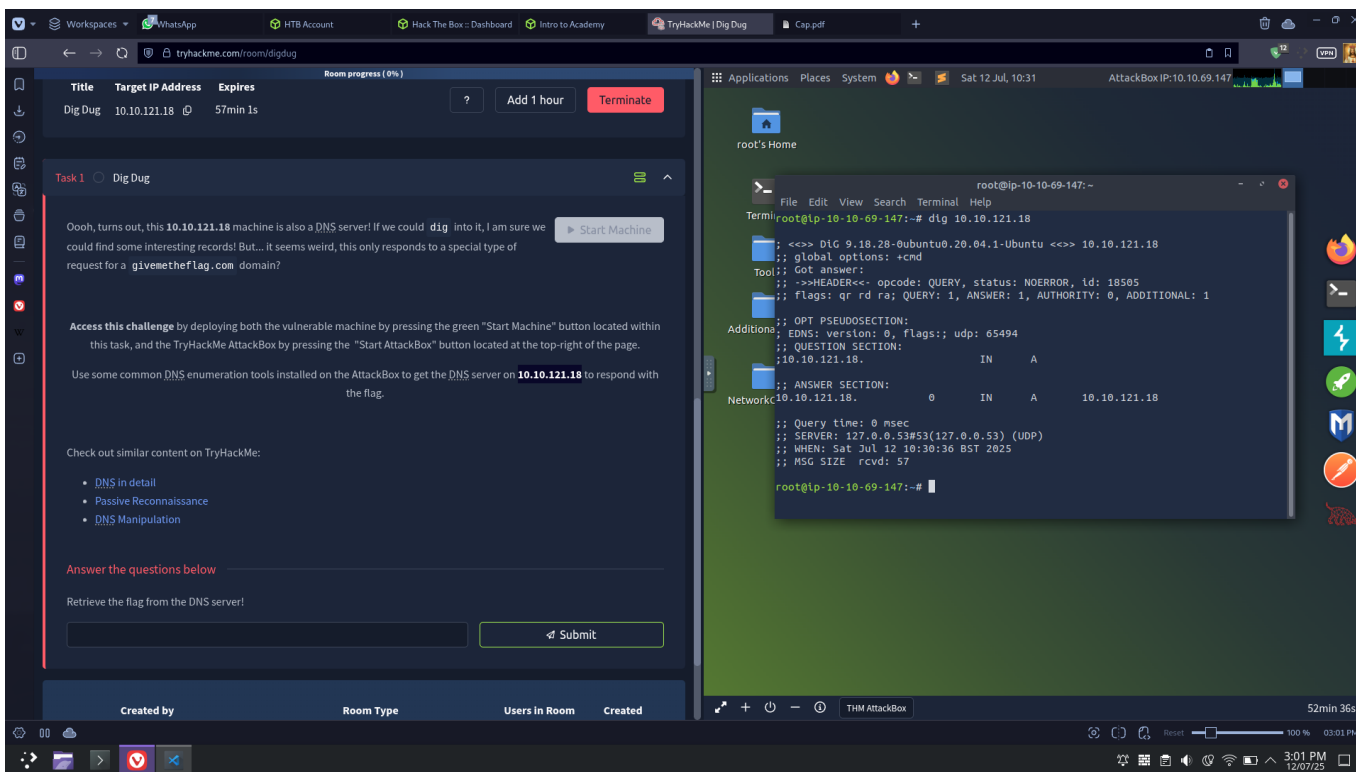
TryHackMe – Dig Dug Writeup

🔍 Challenge Overview

- **Room Name:** Dig Dug
- **Platform:** TryHackMe
- **Difficulty:** Very Easy (Intro to DNS)
- **Objective:** Query a DNS server to retrieve a hidden flag.
- **Room Link:** <https://tryhackme.com/room/digdug>

1. Deploy the Attack Box & Target Machine

Connect using OpenVPN or deploy the TryHackMe AttackBox and the Dig Dug machine. The target's IP is denoted here as **<MACHINE_IP>** (10.10.121.18).



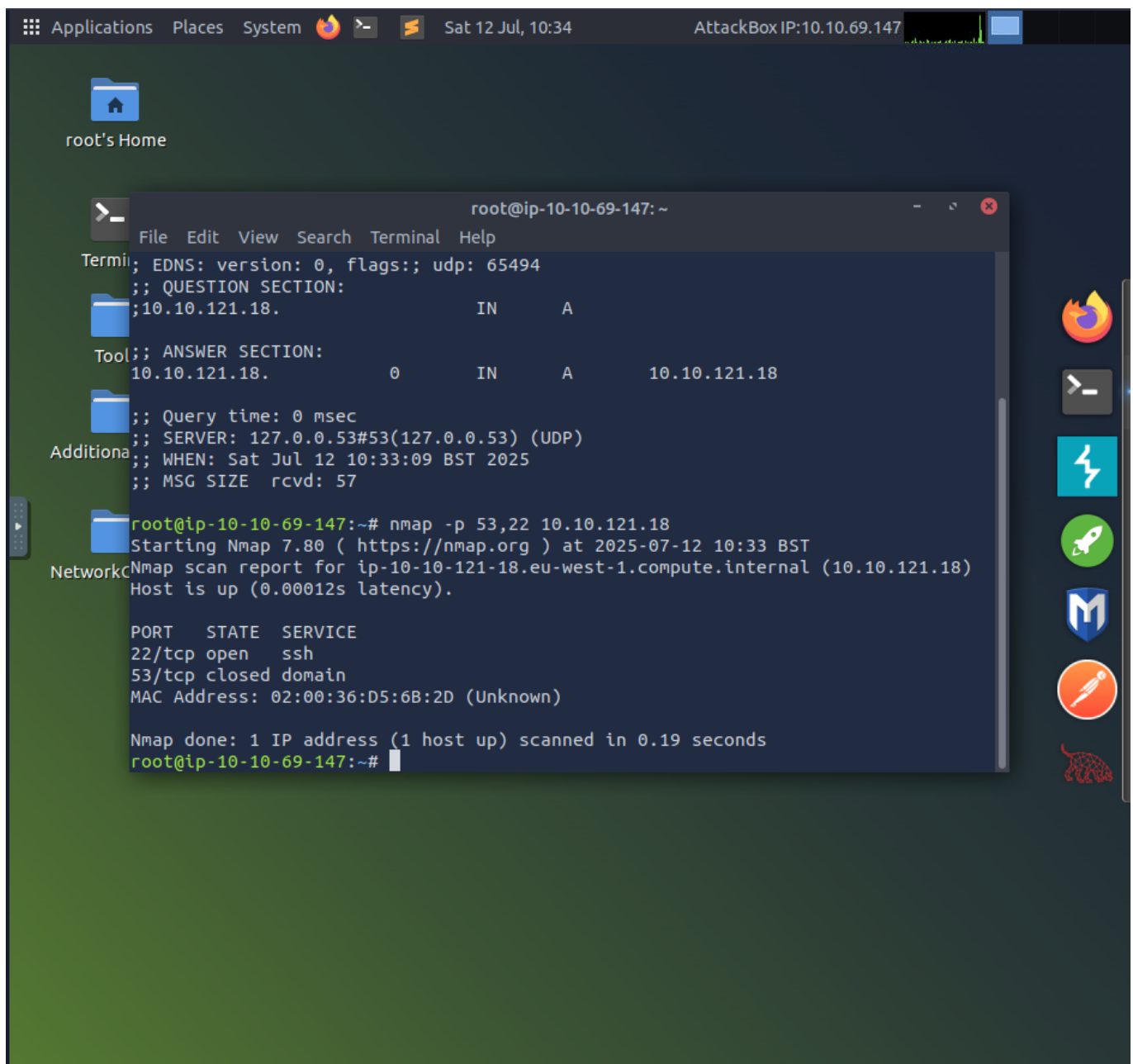
The screenshot shows the TryHackMe interface for the 'Dig Dug' challenge. On the left, the challenge details are visible, including the target IP address 10.10.121.18 and a task description. The task description states: 'Oooh, turns out, this 10.10.121.18 machine is also a DNS server! If we could dig into it, I am sure we could find some interesting records! But... it seems weird, this only responds to a special type of request for a givemetheflag.com domain?'. Below this, there are instructions on how to access the challenge and a list of related topics: DNS in detail, Passive Reconnaissance, and DNS Manipulation. On the right, a terminal window shows the command 'dig 10.10.121.18' being executed, resulting in a successful query for the 'givemetheflag.com' domain. The terminal output includes the following details: 'Dig 9.18.28-0ubuntu0.20.04.1-Ubuntu <>> 10.10.121.18', 'global options: +cmd', 'Tool: Got answer:', 'opcode: QUERY, status: NOERROR, id: 18505', 'Flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1', 'OPT PSEUDOSECTION:', 'EDNS: version: 0, flags:; udp: 65494', 'QUESTION SECTION:', '10.10.121.18. IN A', 'ANSWER SECTION:', '10.10.121.18. 0 IN A 10.10.121.18', 'Query time: 0 msec', 'SERVER: 127.0.0.53#53(127.0.0.53) (UDP)', 'WHEN: Sat Jul 12 10:30:36 BST 2025', 'MSG SIZE rcvd: 57'.

2. Recon – Identify DNS Service

Scan ports with Nmap:

```
nmap -p 53,22 <MACHINE_IP>
```

```
nmap -p 53,22 10.10.121.18
```



3. Understand the Goal

The room description mentions the server only responds to requests for the domain `givemetheflag.com`. This hints that querying this domain directly will reveal the flag.

4. Query the DNS Server

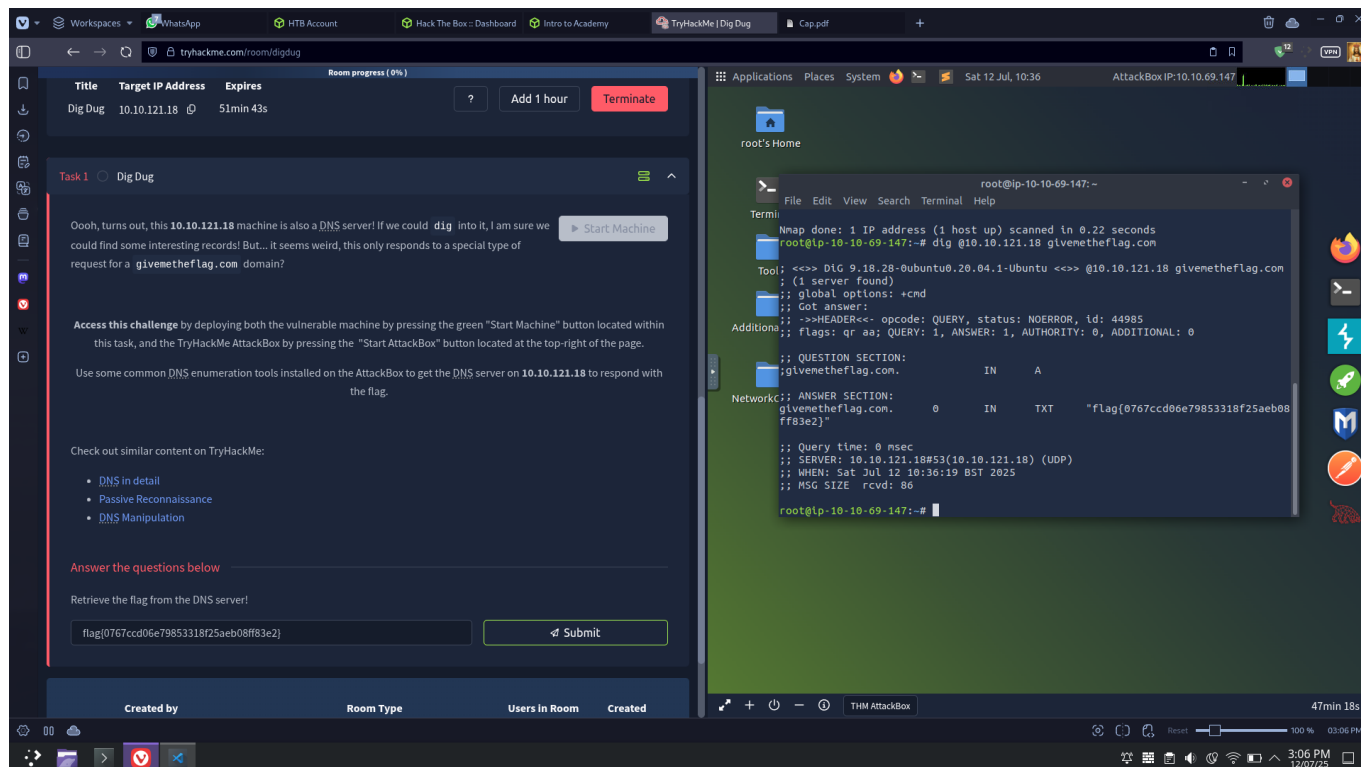
- Using `dig`:

```
dig @<MACHINE_IP> givemetheflag.com
```

```
dig @10.10.121.18 givemetheflag.com
```

Response reveals:

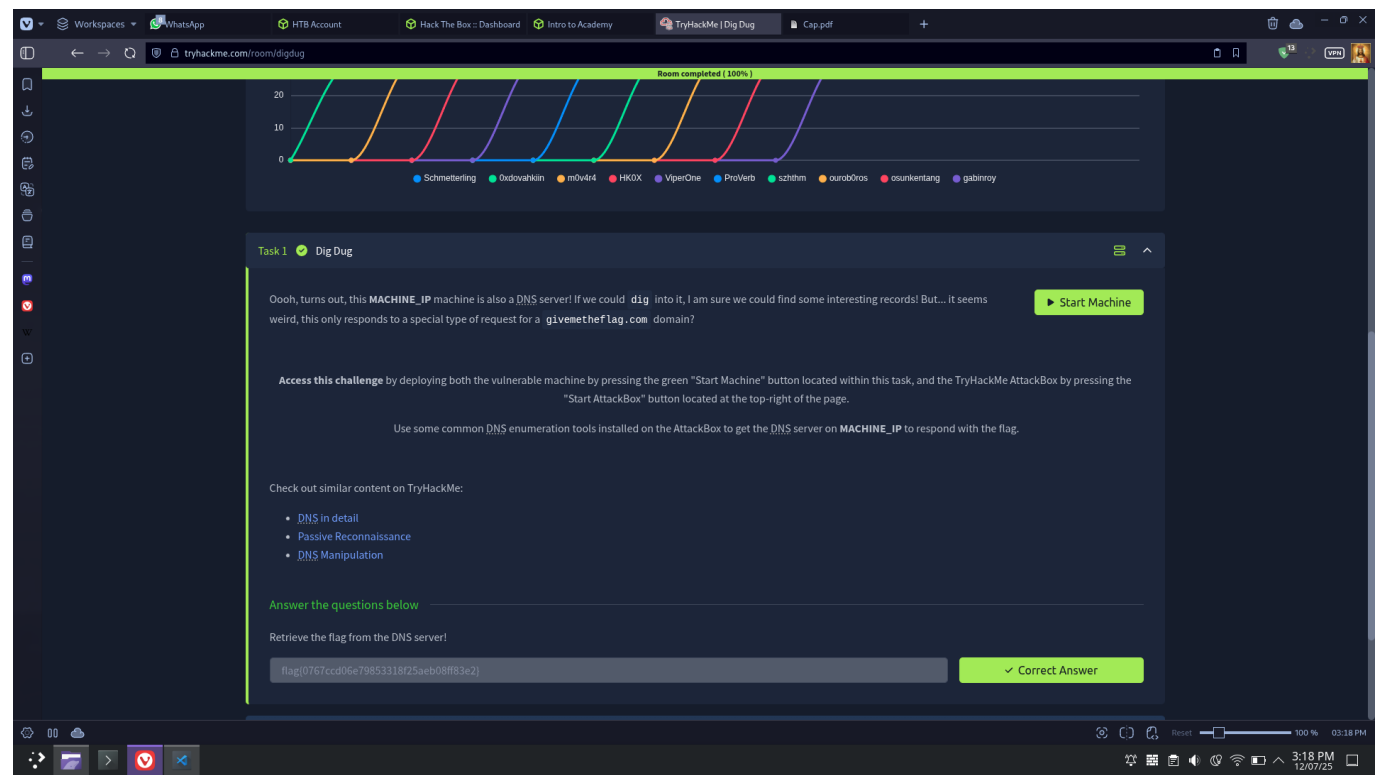
```
;; ANSWER SECTION:
givemetheflag.com. 0 IN TXT
"flag{0767ccd06e79853318f25aeb08ff83e2}"
```



5. Capture & Submit the Flag

Copy the string enclosed in quotes from the TXT record (format: `flag{...}`) and submit it. That's game over!

Flag : `flag{0767ccd06e79853318f25aeb08ff83e2}`



Conclusion

Dig Dug is a great introduction to DNS enumeration. With just one command, you can query a custom domain on a DNS server and extract information hidden in TXT records. It's an essential skill in web and red-team operations.