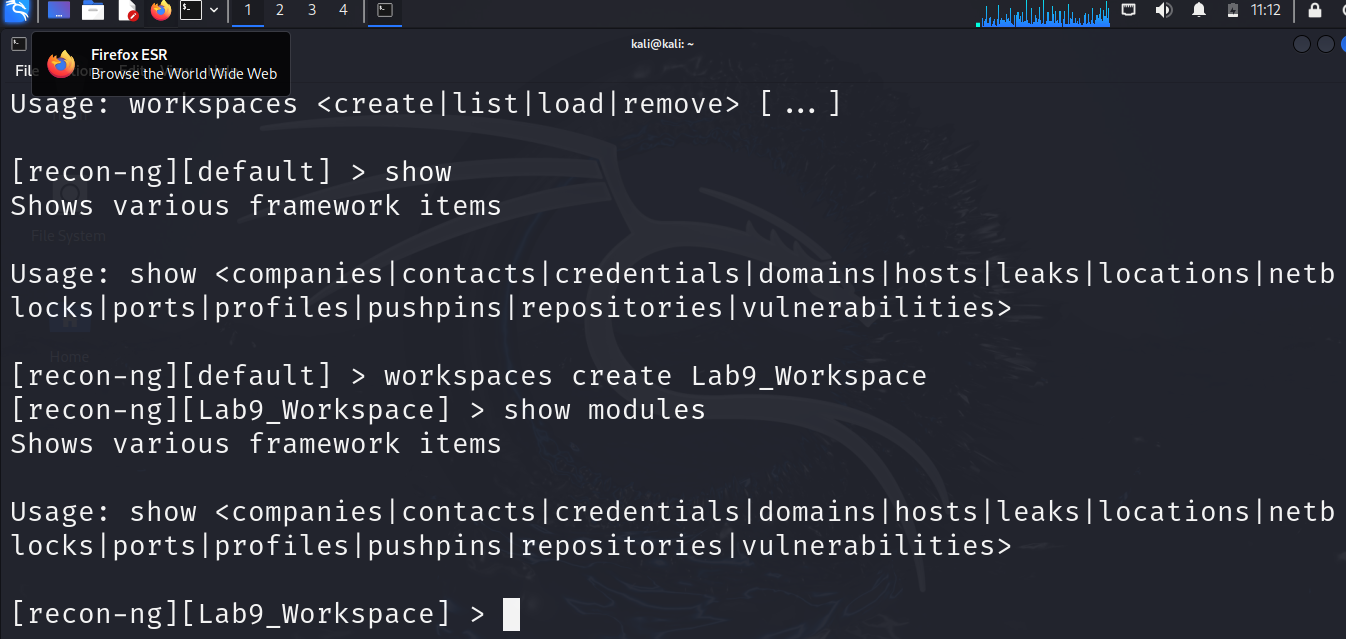
**Lab 9: Information Gathering with Recon-ng and Shodan**

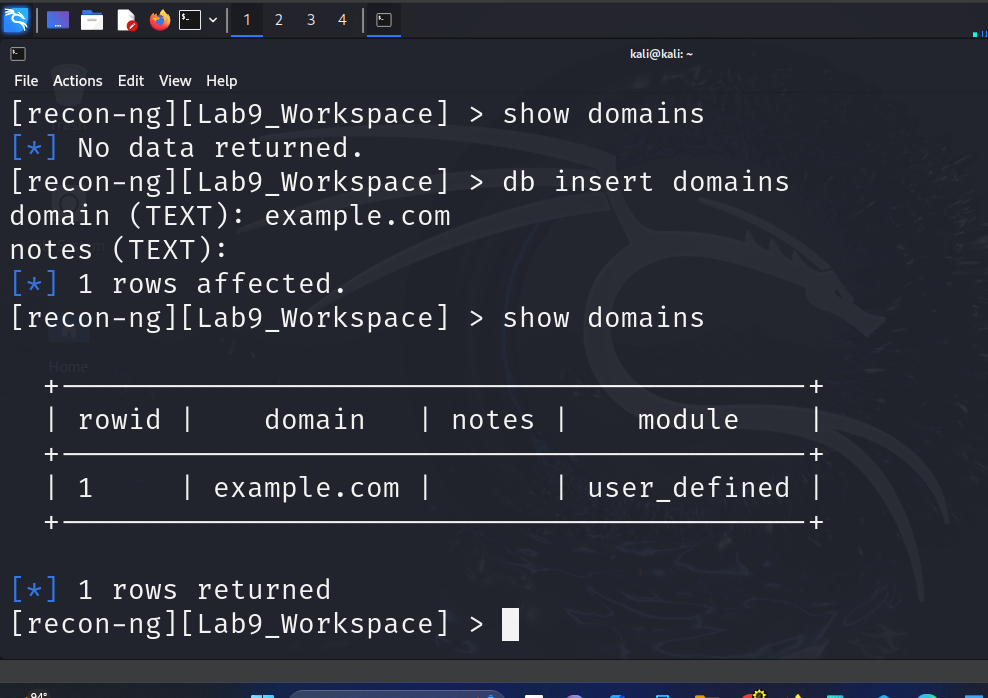
**Exercise 1:**

• List the modules that can be used for domain reconnaissance. What are some key modules you might consider?

Company, contact, credentials, domain, hosts, leaks, location, netblocks, ports, profiles, pushpins, repository and vulnerabilities.

The kay framework worth considering are domain, port, repository and vulnerabilities.

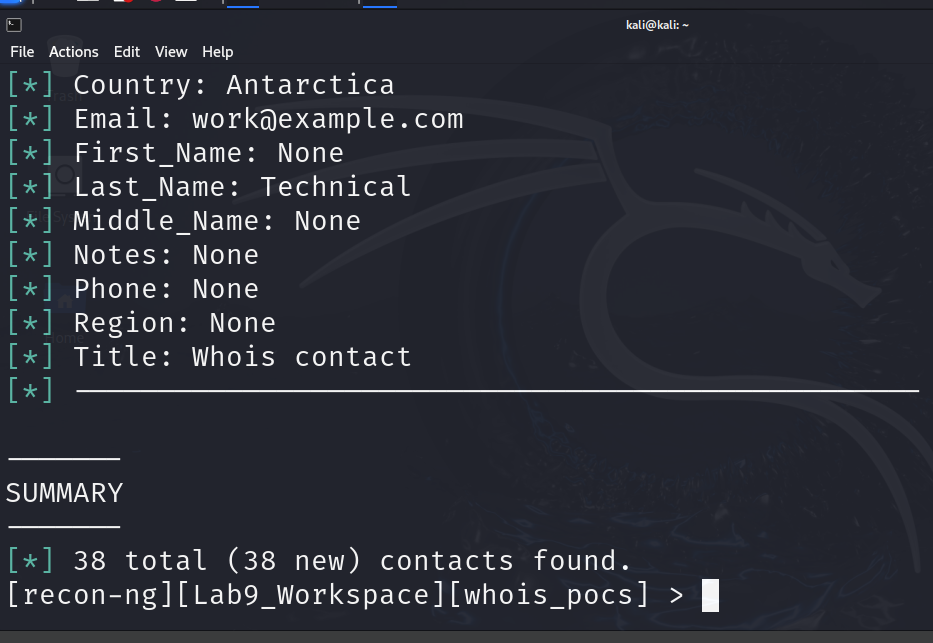




**Exercise 2:**

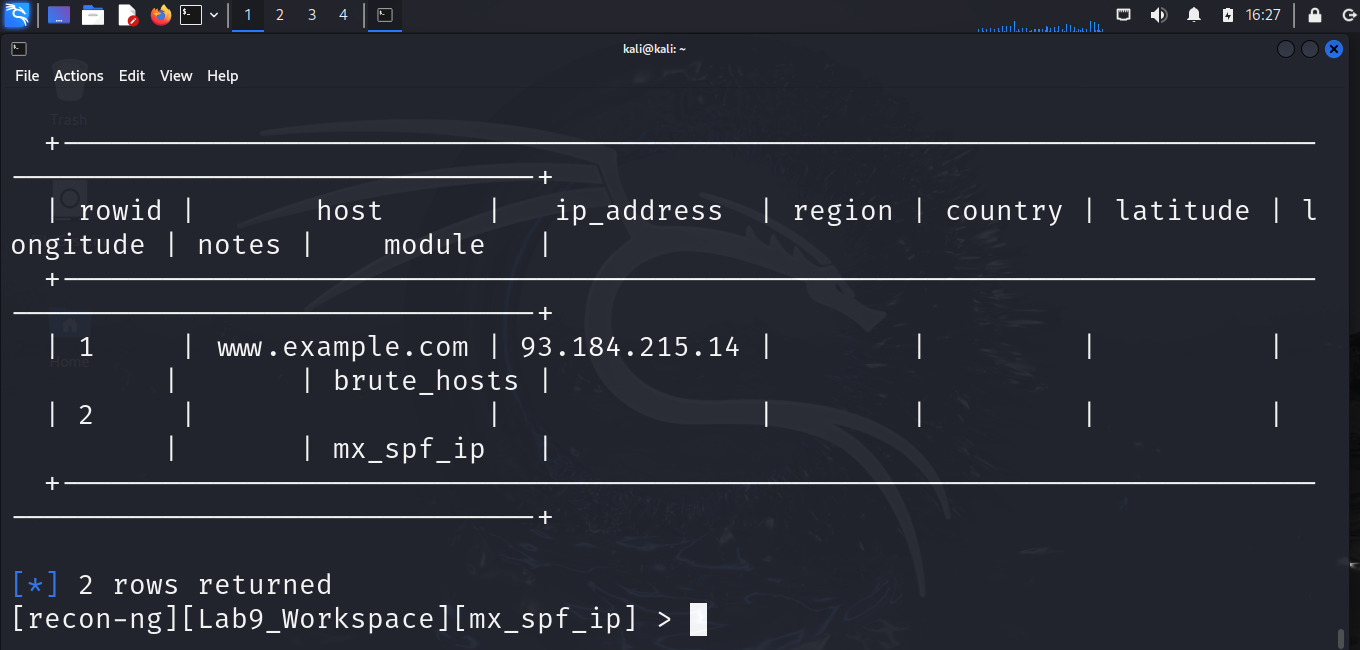
• Document the registration details obtained from the whois module. What information did you find useful?

38 New contacts found and these include country, Email, and Names.



**Exercise 3:**

• What new information was discovered about the target domain? List the subdomains or IP addresses obtained.



Exercise 5:

• What devices were discovered related to the target domain? Provide a brief description of the findings.

I don’t have Queries left.

Exercise 6:

• Perform an advanced search using two different filters. Document the results and discuss what types of devices you found

**Lab 10: DNS Query Tools and SMB Enumeration**

Exercise 1:

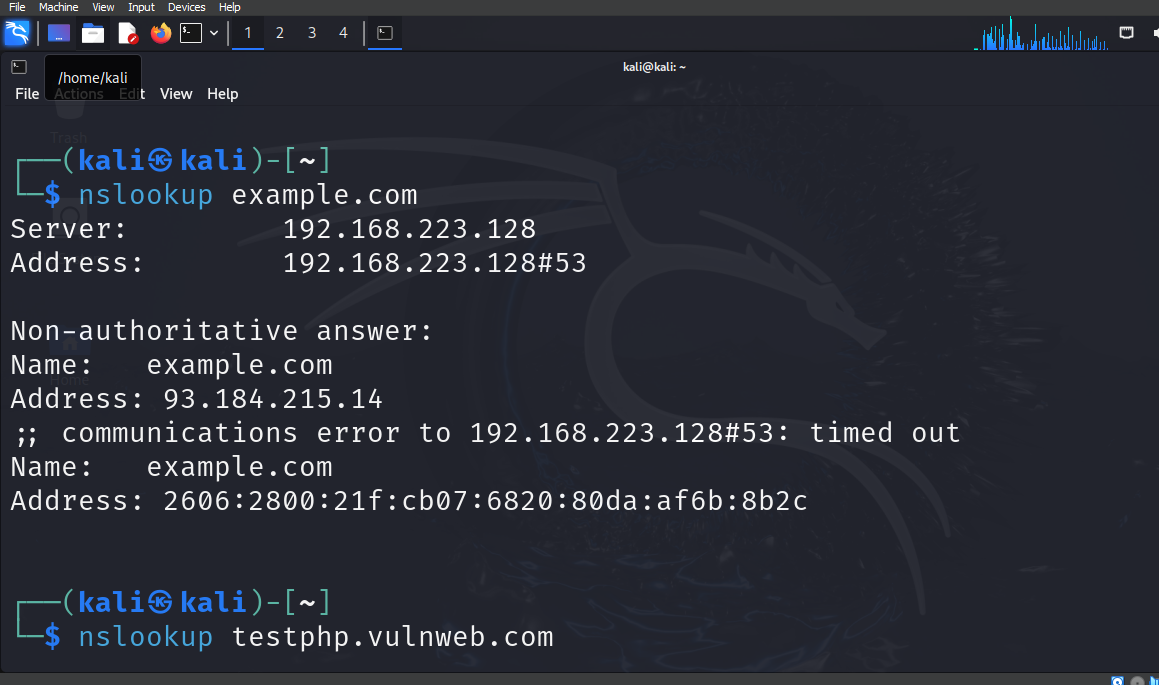
• What information did you obtain from the nslookup command? Document the IP addresses and any additional records retrieved.

Server: 192.168.223.128

Address: 192.168.223.128#53

Name: example.com

Address: 93.184.215.14

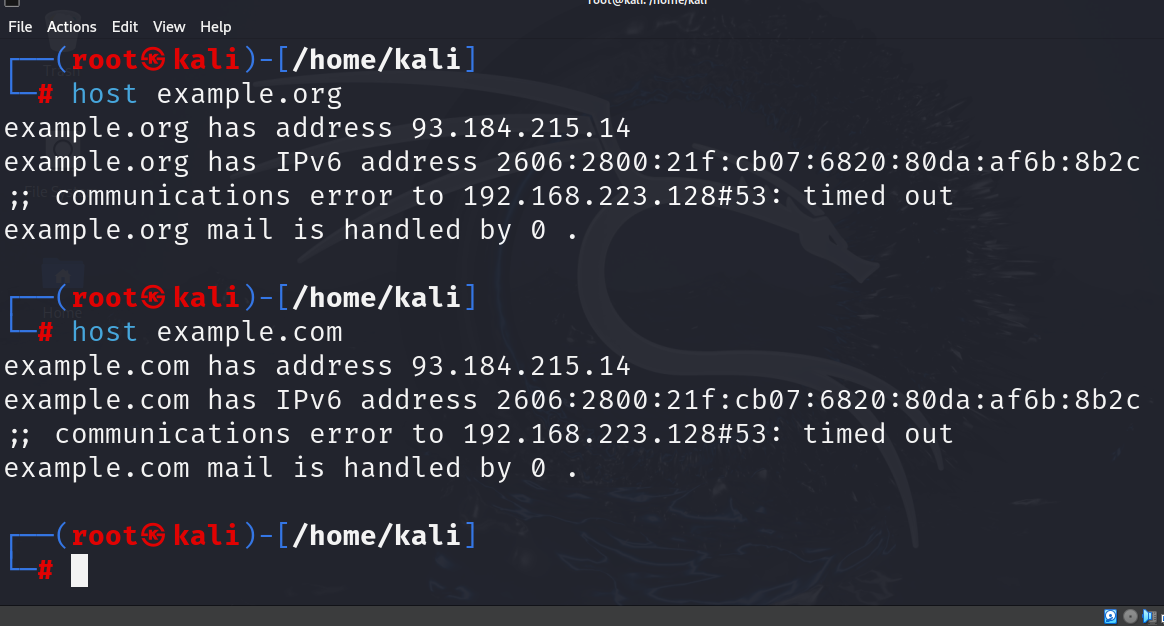


Exercise 2:

• Compare the output of host with nslookup. What differences did you observe?

Both testphp.vulnweb.com and example.com were scanned using host, testphp.vulnweb.com has address 44.228.249.3, example.com has address 93.184.215.14

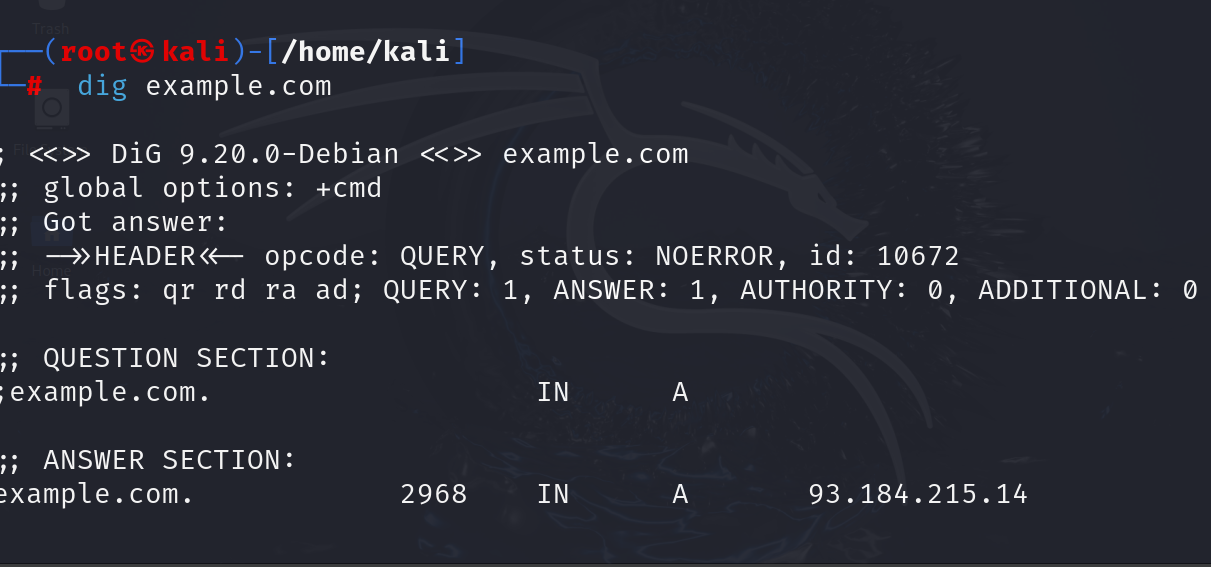
example.com has IPv6 address 2606:2800:21f:cb07:6820:80da:af6b:8b2c while nslookup was used to scan the sane domain, the answers are the same, they both find the same IP address.



Exercise 3:

• Analyze the output of the dig command. What additional information can you extract compared to the previous tools?

The additional information from dig command is that it shows flags, query and IP address which make it a bit different from nslookup and host.

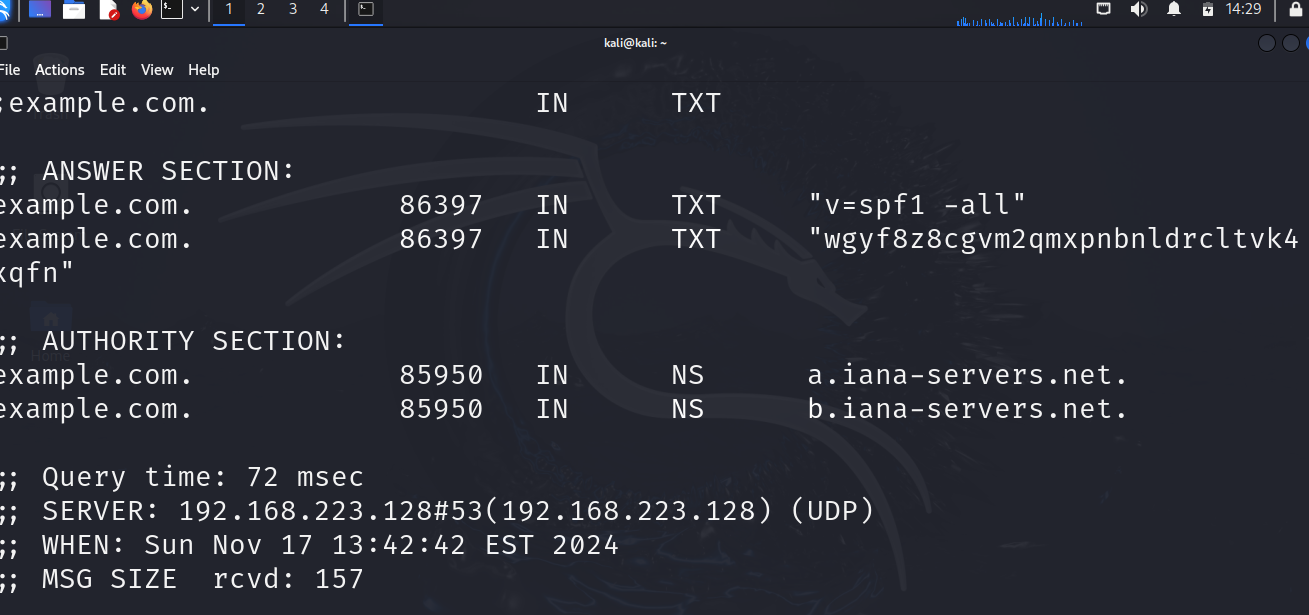
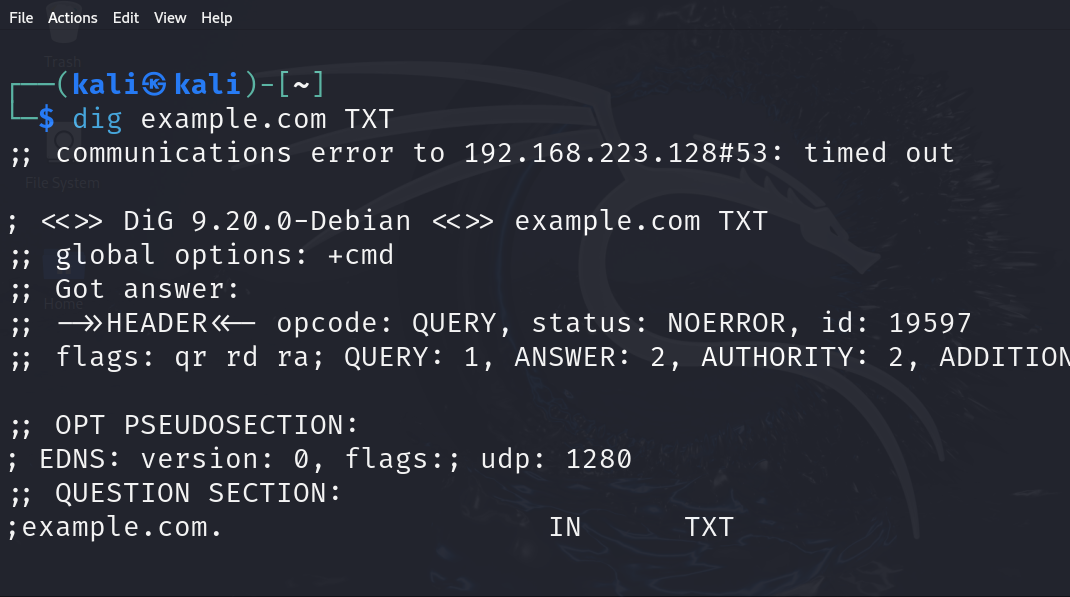


Exercise 4:

• What did you learn from querying different record types? How can this information be useful in a penetration test?

Querying DNS records is a critical step in reconnaissance during penetration testing. It provides a detailed view of the target’s infrastructure, which can be used to identify vulnerabilities, misconfigurations, and opportunities for attacks. Understanding how each record type contributes to the broader security landscape enables a penetration tester to plan more effective and targeted tests.

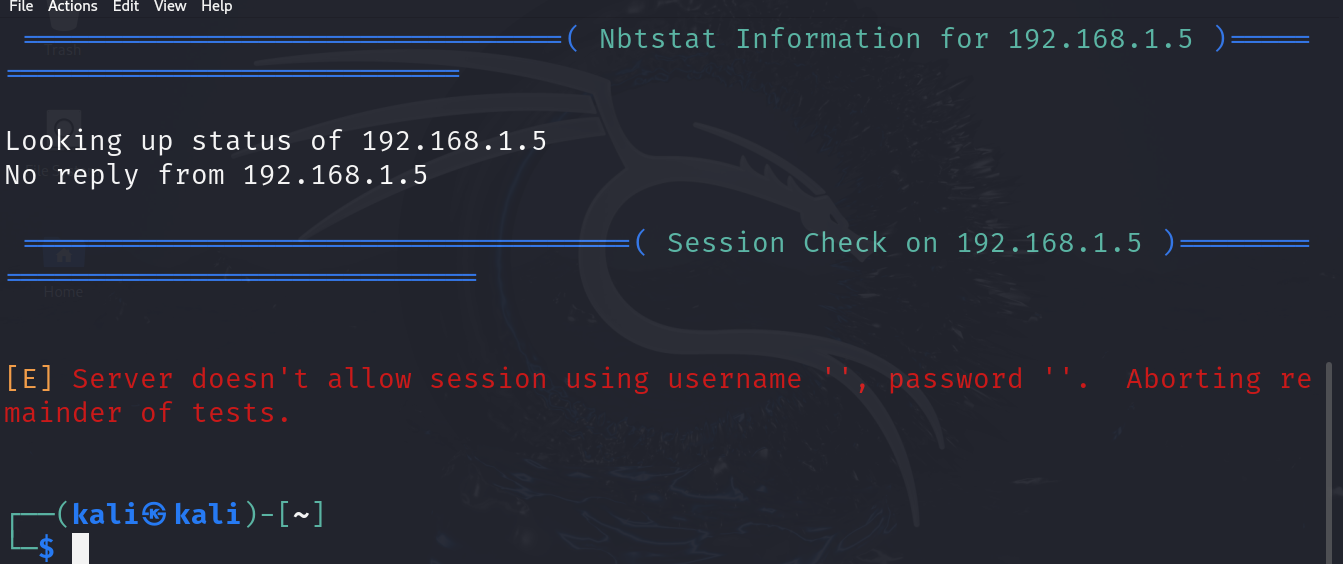




Exercise 5:

• What information did you gather about the target system? Document the shares, users, and any other relevant details found.

No information was found on the target system.



Exercise 6:

• Compare the results obtained from enum4linux with your findings from DNS queries. What insights can you gain about the target network?

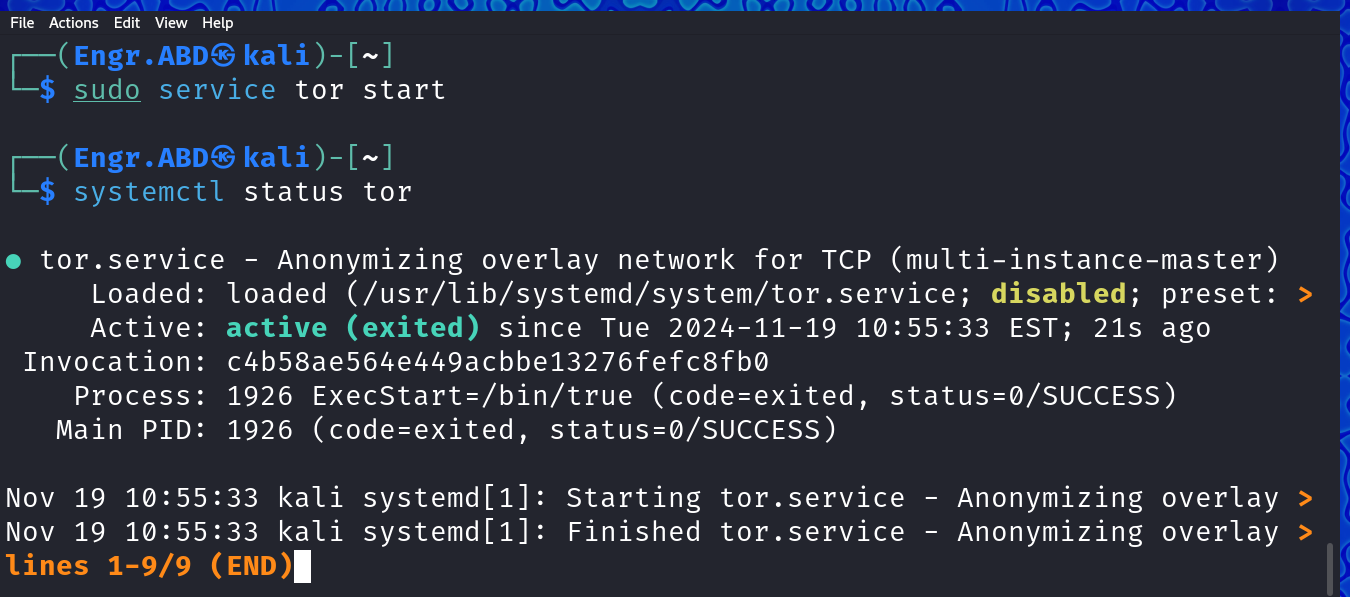
Nothing was found in both users and share

**– Lab 11: Tor and Proxychains Lab Overview**

Exercise 1:

• What output do you see when checking the Tor status? Is it running?

The output shows that the Tor is active and main parent ID (PID) is run.



Exercise 2:

• What are the different proxy modes available in Proxychains? Briefly explain each

**dynamic\_chain**

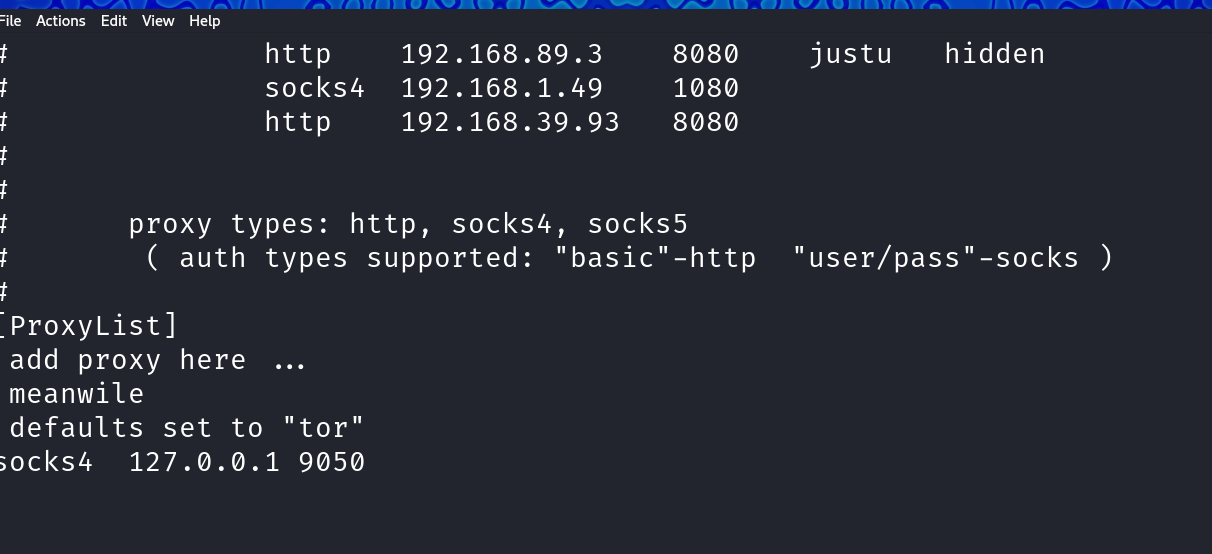
#Dynamic - Each connection will be done via chained proxies, all proxies chained in the order as they appear in the list at least one proxy must be online to play in chain (dead proxies are skipped) otherwise EINTR is returned to the app

**strict\_chain**

# Strict - Each connection will be done via chained proxies, all proxies chained in the order as they appear in the list, all proxies must be online to play in chain otherwise EINTR is returned to the app

**random\_chain**

# Random - Each connection will be done via random proxy (or proxy chain, see chain\_len) from the list. This option is good to test your IDS :) Make sense only if random\_chain, chain\_len = 2 Quiet mode (no output from library) quiet\_mode



**Exercise 3**:

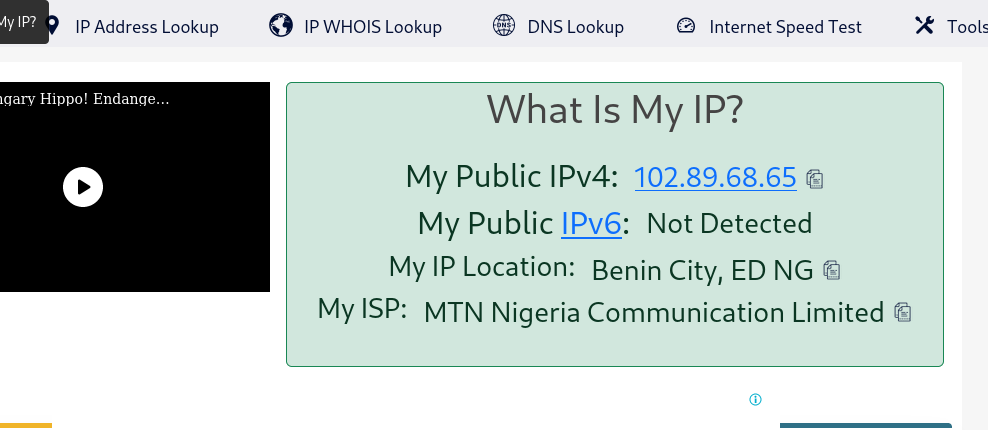
• What IP address do you see in the output? How does it compare to your actual IP address?

The output IP address is "102.89.69.153" the actual IP address 52.20.148.183



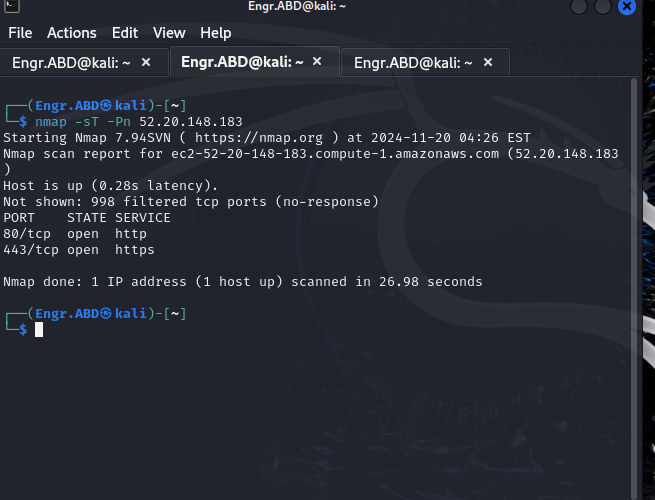
**Exercise 4:**

• Navigate to any website and check your IP address using a service like https://www.whatismyip.com/. Does it show the Tor exit node IP address?



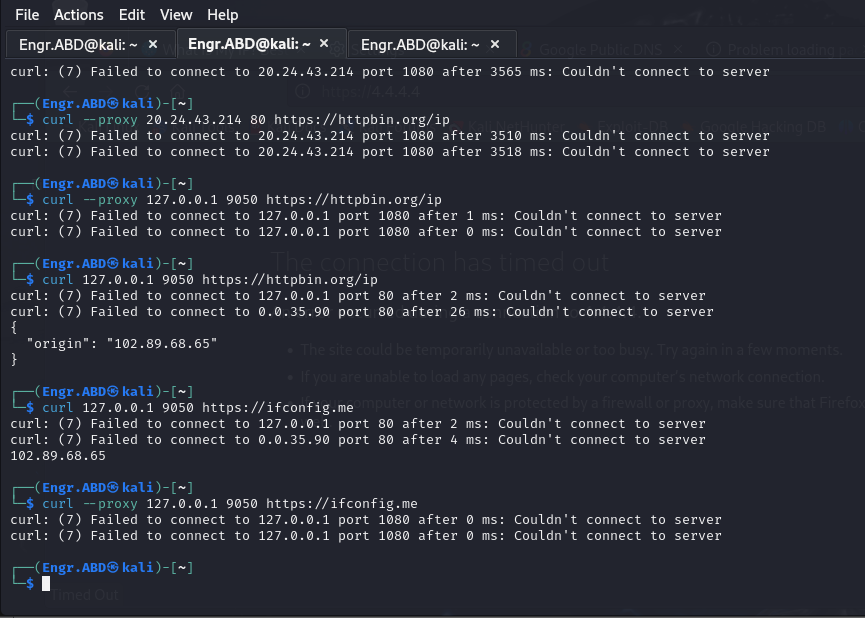
**Exercise 5:**

• How does routing your Nmap scans through Tor affect your scanning capabilities? What limitations did you encounter?



Exercise 6:

• Experiment with adding another HTTP proxy (e.g., a public proxy server) and rerun your curl command. How does the response change?

The response is failed, and couldn’t connect to server.

**Risks Associated with Using Tor**

1. **Malicious Exit Nodes**
   * Some exit nodes (the last relay in the Tor network) may be operated by malicious actors who can monitor unencrypted traffic.
   * Sensitive data, if transmitted without encryption (e.g., HTTP instead of HTTPS), can be intercepted.
2. **False Sense of Security**
   * Tor does not protect against all threats. For example, it doesn’t encrypt traffic beyond the exit node, nor does it anonymize actions tied to your identity (e.g., logging into personal accounts).
3. **Targeting by Authorities**
   * Some governments or organizations monitor Tor usage and may flag users for surveillance or block Tor connections entirely.
4. **Slow Speeds**
   * The relaying of traffic through multiple nodes results in slower internet speeds, which can be frustrating for certain activities.
5. **Exploitation via Scripts and Plugins**
   * JavaScript, browser plugins (e.g., Flash), and media files can leak your real IP address or other identifying information.
6. **Legal or Ethical Concerns**
   * While Tor itself is legal in most jurisdictions, its use is associated with accessing the dark web, which may attract unwanted attention.
7. **Phishing and Malware**
   * Websites accessed via Tor, especially on the dark web, may host malicious content, phishing scams, or files containing malware.

**Precautions to Take While Using Tor**

1. **Use HTTPS Whenever Possible**
   * Install HTTPS Everywhere or verify that sites use HTTPS to encrypt data end-to-end.
2. **Avoid Logging into Personal Accounts**
   * Logging into accounts tied to your identity (e.g., email, social media) can de-anonymize you. Use pseudonyms if necessary.
3. **Disable Scripts and Plugins**
   * Use the Tor Browser's built-in safeguards to disable JavaScript and prevent plugins from running automatically.
4. **Be Cautious with Downloads**
   * Avoid downloading files, especially executable ones, as they might bypass Tor and expose your real IP.
5. **Update Tor Regularly**
   * Ensure your Tor Browser is up to date to protect against known vulnerabilities.
6. **Do Not Use P2P Applications**
   * Peer-to-peer file-sharing applications like BitTorrent can reveal your real IP address, even when used over Tor.
7. **Combine Tor with a VPN (Optional)**
   * A VPN before Tor (VPN → Tor) can hide your Tor usage from your ISP, though it won’t anonymize your activities inside the Tor network. Choose a no-log VPN.
8. **Avoid Opening Suspicious Links**
   * Be careful about visiting unknown sites or clicking on dark web links, as they could host harmful content.
9. **Use a Clean Device**
   * Run Tor on a secure, malware-free device. For higher security, consider using Tails OS, which is designed for privacy and anonymty.
10. **Understand Tor’s Limitations**
    * Know that Tor only anonymizes your browsing traffic. Other activities, like email or messaging, require additional tools (e.g., ProtonMail, Signal).

**Final Thoughts**

Tor is a powerful tool for privacy and anonymity but is not foolproof. Combining Tor with good security practices, encryption, and safe browsing habits can significantly reduce the risks. Always assume that your anonymity could be compromised if you fail to take the necessary precautions.

**Lab 12: John the Rippe**

Exercise 1:

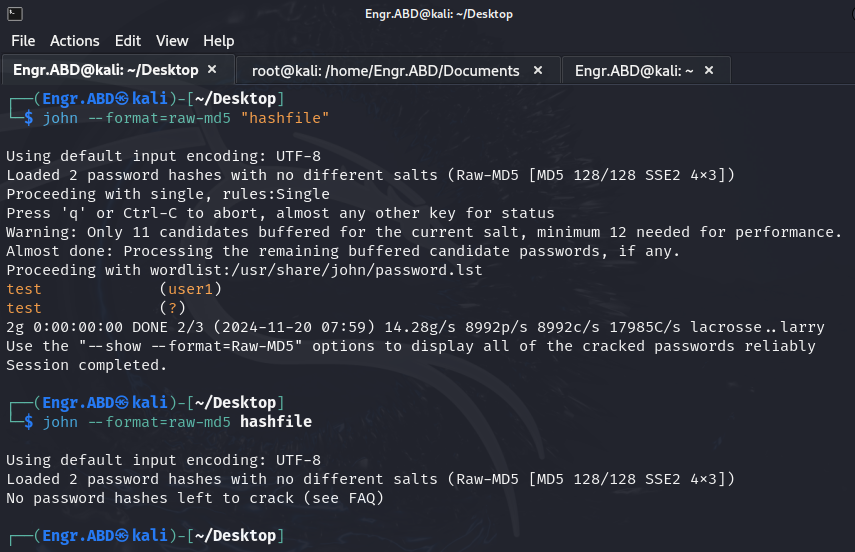
• What version of John the Ripper are you using?

Exercise 2:

• Using John the Ripper, how do you identify the type of a given hash? Run the following command on sample hashes: John --format=raw-md5 hashfile

A screenshot of a computer

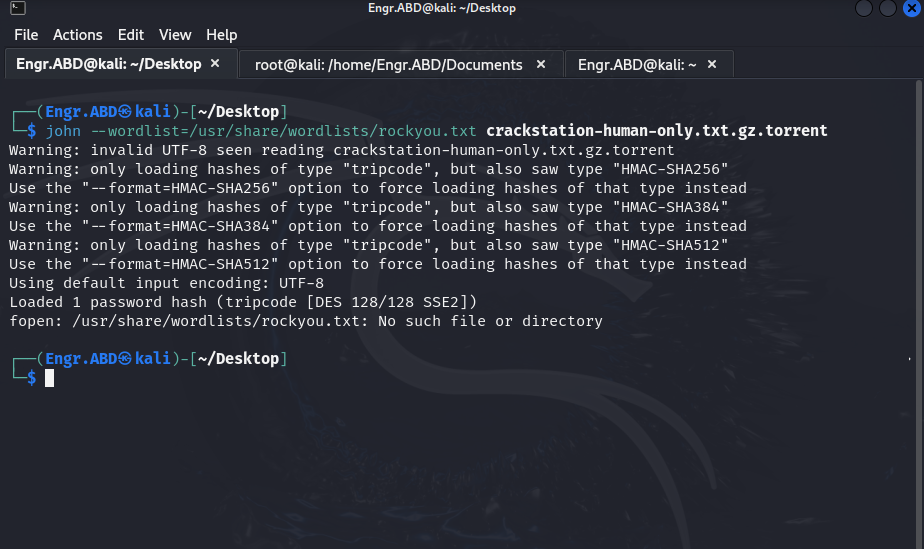
Description automatically generated



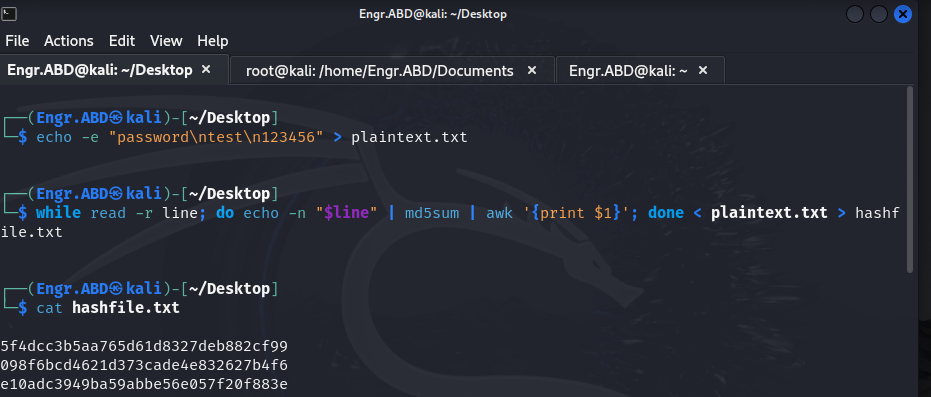
**Exercise 3**:

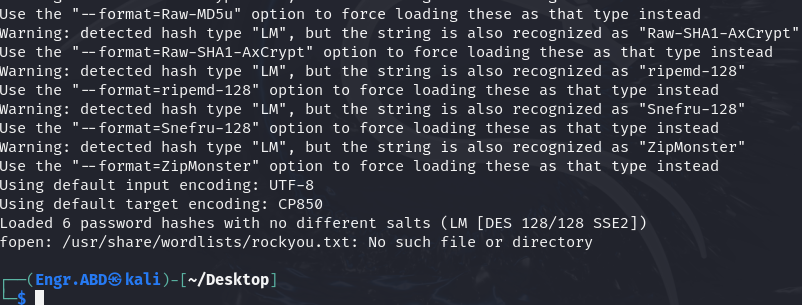
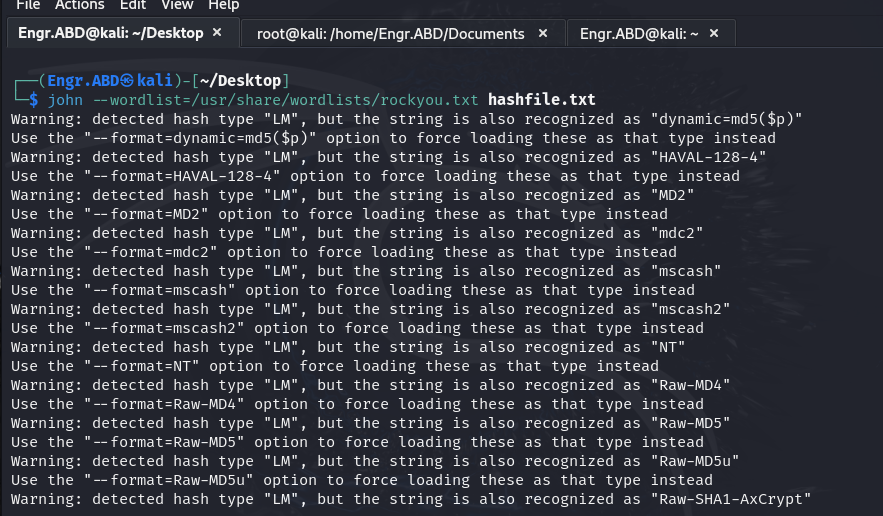
• Download a sample hash and crack it using the wordlist. What was the password? Was it successful?

A sample hash was downloaded from <https://crackstation.net/>, and crack with worldlist, 1 password hash was loaded.



I created a file called plaintext.txt and Generate MD5 hashes for these passwords. 6 passwords were loaded.

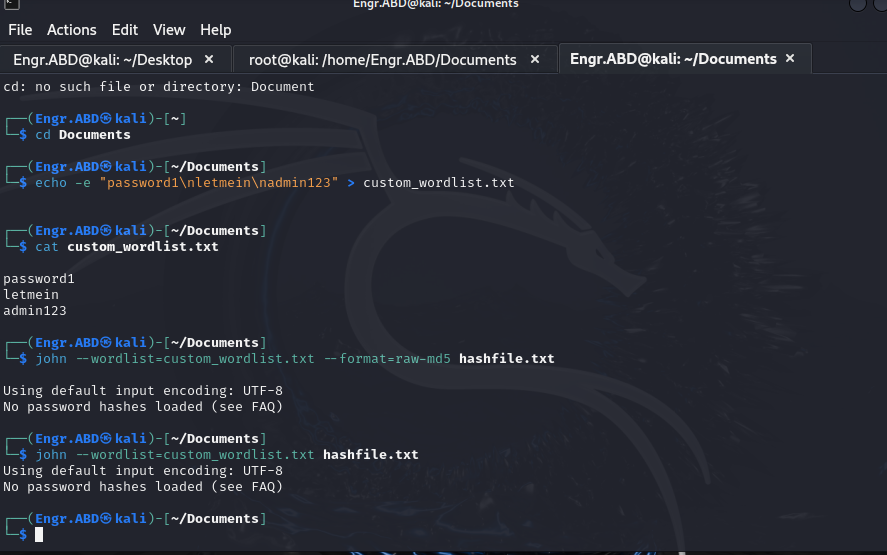




**Exercise 4:**

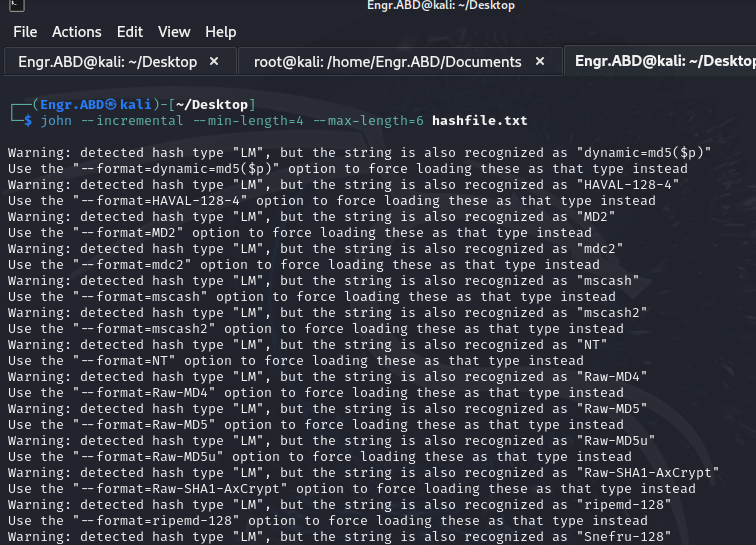
• Run John with your custom wordlist on a given hash. Was your list successful in cracking the hash?

No, the cracking wasn’t successful



Exercise 5:

• Perform a brute force attack on a hash. How long did the attack take, and was it successful?



A screenshot of a computer screen

Description automatically generated

**Exercise 6:**

• Attempt cracking NTLM hashes using the rockyou.txt wordlist. Were you successful? How complex was the password?