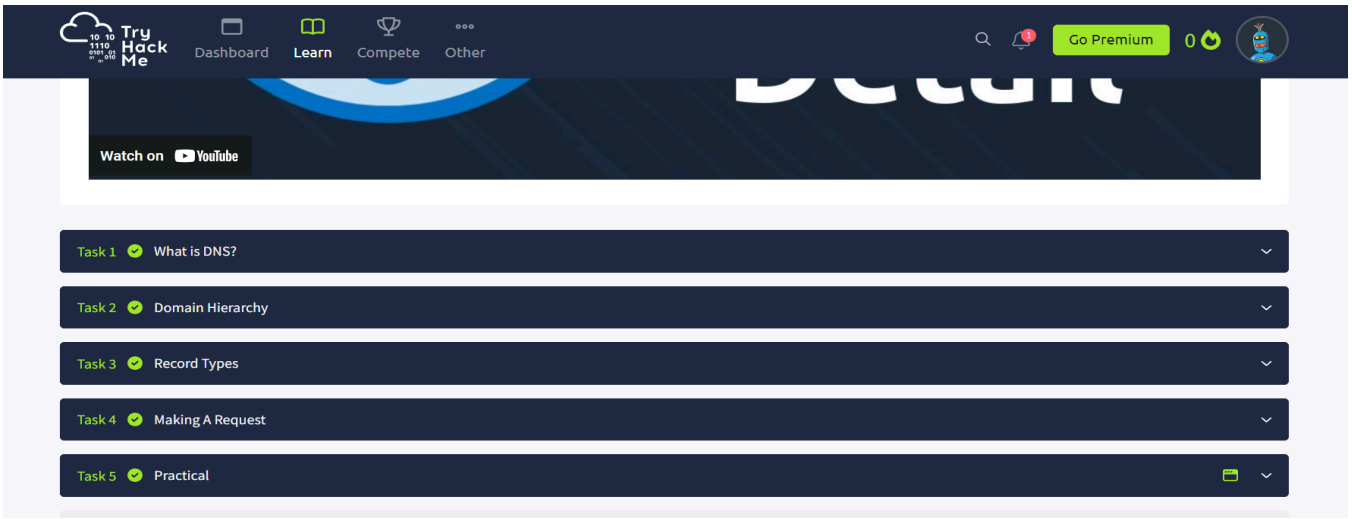
DNS enumeration:

TryHackMe exercises:



1. What is the ip address of adlp-corp.com ?
   Your response Your command:

```
└─$ nmap adlp-corp.com
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-10 05:41 EDT
Nmap scan report for adlp-corp.com (52.51.133.160)
```

```
└─$ host -t a adlp-corp.com
adlp-corp.com has address 52.51.133.160
```

   Dig adlp-corp.com a : will also give the ip address

2. What is the TXT record of adlp-corp.com?
   Your response Your command

```
└─$ host -t txt adlp-corp.com
adlp-corp.com descriptive text "BC{DESCRIPTIVE-DOMAIN-TXT}"
```

3. What are the MX records of becode.org ?
   Your response Your command

```
└─$ host -t mx becode.org
becode.org mail is handled by 1 aspmx.l.google.com.
becode.org mail is handled by 5 alt2.aspmx.l.google.com.
becode.org mail is handled by 10 alt4.aspmx.l.google.com.
becode.org mail is handled by 5 alt1.aspmx.l.google.com.
becode.org mail is handled by 10 alt3.aspmx.l.google.com.
```

4. What are the MX records of adlp-corp.com ?
   Your response Your command

```
└─$ host -t mx adlp-corp.com
adlp-corp.com mail is handled by 10 alt4.aspmx.l.google.com.
adlp-corp.com mail is handled by 1 aspmx.l.google.com.
adlp-corp.com mail is handled by 10 alt3.aspmx.l.google.com.
adlp-corp.com mail is handled by 5 alt2.aspmx.l.google.com.
adlp-corp.com mail is handled by 5 alt1.aspmx.l.google.com.
```

5. What is the first NS name server of adlp-corp.com?
   Your response Your command

```
└─$ host -t ns adlp-corp.com
adlp-corp.com name server ns-1997.awsdns-57.co.uk.
```

6. Uses a brute force tool to find subdomains of adlp-corp.com. How many did you find?
   Your response Your command

```
┌──(kali㉿kali)-[~]
└─$ dnsenum adlp-corp.com
dnsenum VERSION:1.3.1
```

```
Brute forcing with /usr/share/dnsenum/dns.txt:
_______________________________________________

admin.adlp-corp.com.                    300      IN    A        52.51.133.160
ftp.adlp-corp.com.                      300      IN    A        52.51.133.160
mail.adlp-corp.com.                     300      IN    A        52.51.133.160
mail2.adlp-corp.com.                    300      IN    A        52.51.133.160
smtp.adlp-corp.com.                     300      IN    A        52.51.133.160
```

```
┌──(kali㉿kali)-[~]
└─$ dnsmap adlp-corp.com
dnsmap 0.36 - DNS Network Mapper

[+] searching (sub)domains for adlp-corp.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

admin.adlp-corp.com
IP address #1: 52.51.133.160

ftp.adlp-corp.com
IP address #1: 52.51.133.160
```

7. Use theHarvester tool at becode.org. How many Linkedin Users?
   Your response Your command

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d becode.org -l 50 -b all
```

```
[*] LinkedIn Links found: 0
___________________________
```

Alternatively:

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d becode.org -b Linkedin

Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*******************************************************************
*                                                                 *
* | |_| |__   ___        ^  /\__ _ _ ___   _____ ___| |_ ___ _ __ *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.6.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************

[!] Invalid source.
```

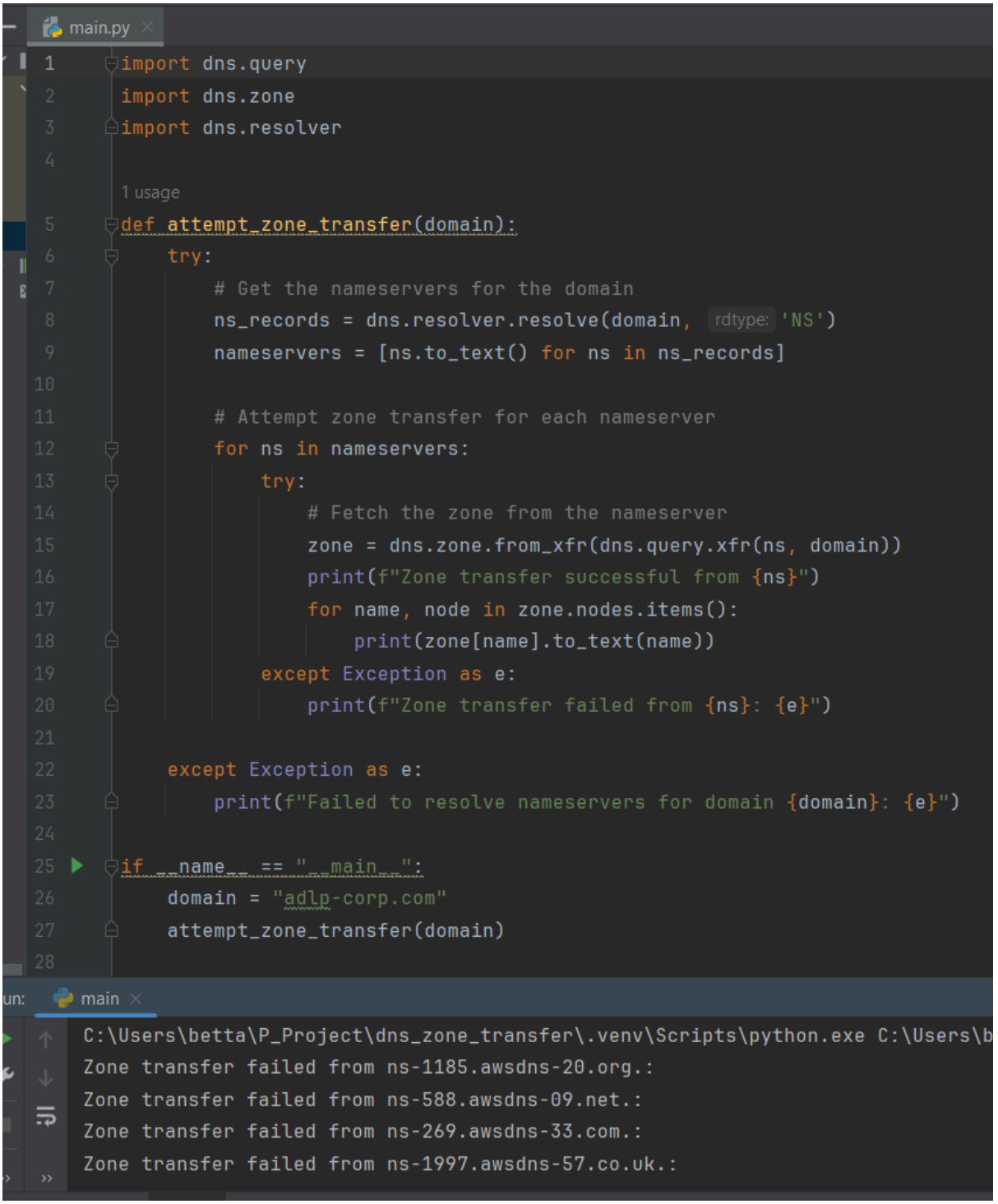
```
-b SOURCE, --source SOURCE
                      anubis, baidu, bevigil, binaryedge, bing, bingapi, bufferoverun, brave, censys,
                      certspotter, criminalip, crtsh, dnsdumpster, duckduckgo, fullhunt, github-code,
                      hackertarget, hunter, hunterhow, intelx, netlas, onyphe, otx, pentesttools,
                      projectdiscovery, rapiddns, rocketreach, securityTrails, sitedossier, subdomaincenter,
                      subdomainfinderc99, threatminer, tomba, urlscan, virustotal, yahoo, zoomeye
```

8. Use theHarvester tool at becode.org. How many ip addresses did you find?
   Your response Your command

```
┌──(kali㉿kali)-[~]
└─$ theHarvester -d becode.org -l 50 -b all
```

```
[*] IPs found: 36
-------------------
104.19.244.91
104.19.245.91
108.129.32.135
109.197.246.221
18.200.133.185
185.199.108.153
185.199.109.153
```

9. Write a small script to attempt a zone transfer from adlp-corp.com using a higher-level scripting language such as Python, Perl, or Ruby
   Your Script

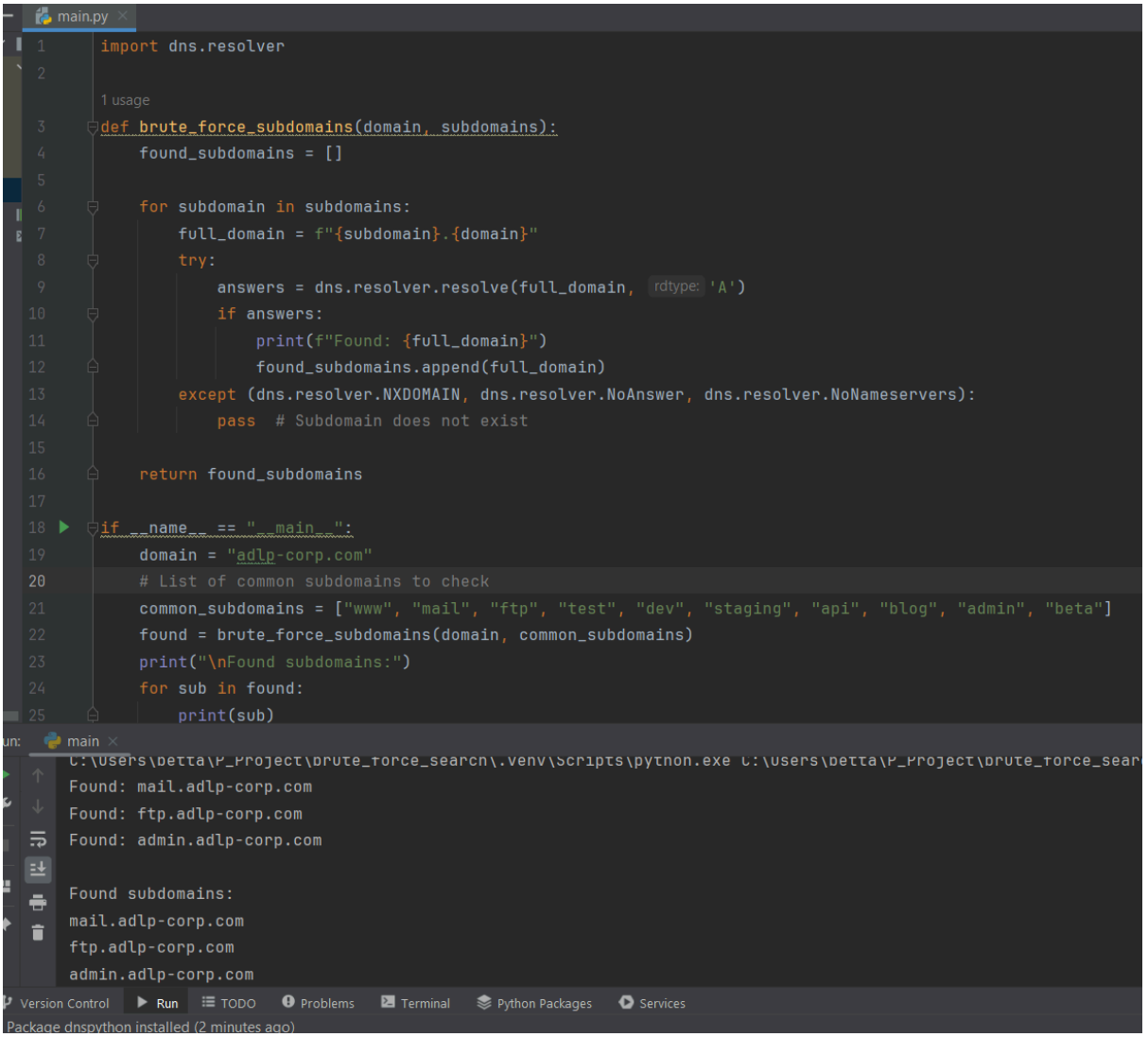


Important Notes

Performing a DNS zone transfer without permission is often considered unauthorized access and may violate policies or laws. Always ensure you have explicit permission to conduct such activities on a domain.

Many DNS servers are configured to disallow zone transfers for security reasons, so it's common for these attempts to fail even with legitimate permission.

10. Write a small script to attempt a brute force search for subdomains using a higher level scripting language such as Python, Perl or Ruby.
Your Script


main.py
import dns.resolver
1 usage
def brute_force_subdomains(domain, subdomains):
found_subdomains = []
for subdomain in subdomains:
full_domain = f"{subdomain}.{domain}"
try:
answers = dns.resolver.resolve(full_domain, rdtype: 'A')
if answers:
print(f"Found: {full_domain}")
found_subdomains.append(full_domain)
except (dns.resolver.NXDOMAIN, dns.resolver.NoAnswer, dns.resolver.NoNameservers):
pass # Subdomain does not exist
return found_subdomains
if __name__ == "__main__":
domain = "adlp-corp.com"
# List of common subdomains to check
common_subdomains = ["www", "mail", "ftp", "test", "dev", "staging", "api", "blog", "admin", "beta"]
found = brute_force_subdomains(domain, common_subdomains)
print("\nFound subdomains:")
for sub in found:
print(sub)
main
C:\Users\betta\P_Project\brute_force_search\.venv\Scripts\python.exe C:\Users\betta\P_Project\brute_force_sear
Found: mail.adlp-corp.com
Found: ftp.adlp-corp.com
Found: admin.adlp-corp.com
Found subdomains:
mail.adlp-corp.com
ftp.adlp-corp.com
admin.adlp-corp.com
Version Control
Run
TODO
Problems
Terminal
Python Packages
Services
Package dnspython installed (2 minutes ago)