

DNS enumeration:

TryHackMe exercises:

The screenshot shows the TryHackMe platform interface. At the top, there's a navigation bar with icons for Dashboard, Learn, Compete, Other, a search bar, and user stats (0 challenges, 1 solved). Below the navigation is a banner with a 'Watch on YouTube' button. The main content area displays five tasks related to DNS:

- Task 1: What is DNS?
- Task 2: Domain Hierarchy
- Task 3: Record Types
- Task 4: Making A Request
- Task 5: Practical

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:

Oxford Wordlist

Subdomain	Type	Count	IN	A	IP Address
admin.adlp-corp.com	includes the 500 most frequently used words by children in our wordlist	300	IN	A	52.51.133.160
ftp.adlp-corp.com	includes the 500 most frequently used words by children in our wordlist	300	IN	A	52.51.133.160
mail.adlp-corp.com	includes the 500 most frequently used words by children in our wordlist	300	IN	A	52.51.133.160
mail2.adlp-corp.com	includes the 500 most frequently used words by children in our wordlist	300	IN	A	52.51.133.160
smtp.adlp-corp.com	includes the 500 most frequently used words by children in our wordlist	300	IN	A	52.51.133.160

Hackage

```
└(kali㉿kali)-[~]
```

```
└$ dnsmap adlp-corp.com College of Technology
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 forums Kali NetHunter Exploit-...
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml
*****
*
* [!] Invalid source.
*****
```

```
-b SOURCE, --source SOURCE tool to get random words
22 Mar 2023 — Readme for theHarvester
outputs a random list of words
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

```
main.py
1 import dns.query
2 import dns.zone
3 import dns.resolver
4
5 def attempt_zone_transfer(domain):
6     try:
7         # Get the nameservers for the domain
8         ns_records = dns.resolver.resolve(domain, rdtype='NS')
9         nameservers = [ns.to_text() for ns in ns_records]
10
11         # Attempt zone transfer for each nameserver
12         for ns in nameservers:
13             try:
14                 # Fetch the zone from the nameserver
15                 zone = dns.zone.from_xfr(dns.query.xfr(ns, domain))
16                 print(f"Zone transfer successful from {ns}")
17                 for name, node in zone.nodes.items():
18                     print(zone[name].to_text(name))
19             except Exception as e:
20                 print(f"Zone transfer failed from {ns}: {e}")
21
22         except Exception as e:
23             print(f"Failed to resolve nameservers for domain {domain}: {e}")
24
25 if __name__ == "__main__":
26     domain = "adlp-corp.com"
27     attempt_zone_transfer(domain)
```

run: main

```
C:\Users\betta\P_Project\dns_zone_transfer\.venv\Scripts\python.exe C:\Users\b...
Zone transfer failed from ns-1185.awsdns-20.org.:
Zone transfer failed from ns-588.awsdns-09.net.:
Zone transfer failed from ns-269.awsdns-33.com.:
Zone transfer failed from ns-1997.awsdns-57.co.uk.:
```

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
1 import dns.resolver
2
3     1 usage
4 def brute_force_subdomains(domain, subdomains):
5     found_subdomains = []
6
7         for subdomain in subdomains:
8             full_domain = f"{subdomain}.{domain}"
9             try:
10                 answers = dns.resolver.resolve(full_domain, rdtype='A')
11                 if answers:
12                     print(f"Found: {full_domain}")
13                     found_subdomains.append(full_domain)
14             except (dns.resolver.NXDOMAIN, dns.resolver.NoAnswer, dns.resolver.NoNameservers):
15                 pass # Subdomain does not exist
16
17     return found_subdomains
18
19 if __name__ == "__main__":
20     domain = "adlp-corp.com"
21     # List of common subdomains to check
22     common_subdomains = ["www", "mail", "ftp", "test", "dev", "staging", "api", "blog", "admin", "beta"]
23     found = brute_force_subdomains(domain, common_subdomains)
24     print("\nFound subdomains:")
25     for sub in found:
26         print(sub)
run: main
L:\Users\DETTA\P_Project\brute_force_search\.venv\Scripts\python.exe L:\Users\DETTA\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)
```