2 D MOON USER MANUAL

GROUP 3 - NSSECU2 (ADVANCED AND OFFENSIVE SECURITY)

Gaw, Pierreson Reinwald S.
Herrera, Arquiel M.
King, Julia Ann S.
Muros, Don David D.
Panahon, Jan Corwin D.

DECEMBER 09 2022

PROGRAM MENU

1 - DNS Enumeration
2 - Subdomain Enumeration
3 - Reverse DNS Lookup
4 - DNS Zone Transfer
5 - DNS Cheat Sheet
6 - Exit.

MENU FUNCTIONS

1 - DNS Enumeration

- Enter domain name

```
1 - DNS Enumeration
2 - Subdomain Enumeration
3 - Reverse DNS Lookup
4 - DNS Zone Transfer
5 - DNS Cheat Sheet
6 - EXIT
Instruction: 1
Enter Domain:
```

- After entering a domain name, the program will ask for a record type to enumerate. The record types that the program supports include: AAAA, A, MX, NS, CNAME, SOA, TXT.

```
Enter Domain: youtube.com
Record Type: A

A record
------------------------------
1 - DNS Enumeration
2 - Subdomain Enumeration
3 - Reverse DNS Lookup
4 - DNS Zone Transfer
5 - DNS Cheat Sheet
6 - EXIT
```

- The user can also choose to enumerate all of the record types the program can support by entering “ALL”.

```
Enter Domain: youtube.com
Record Type: ALL
A record
------------------------------
youtube.com. 250 IN A 142.250.66.110


AAAA record
------------------------------
youtube.com. 282 IN AAAA 2404:6800:4005:81c::200e


MX record
------------------------------
youtube.com. 300 IN MX 0 smtp.google.com.
```

```
NS record
------------------------------
youtube.com. 127433 IN NS ns2.google.com.
youtube.com. 127433 IN NS ns1.google.com.
youtube.com. 127433 IN NS ns3.google.com.
youtube.com. 127433 IN NS ns4.google.com.


SOA record
------------------------------
youtube.com. 60 IN SOA ns1.google.com. dns-admin.google.co
m. 493848506 900 900 1800 60
```

- If the user enters a domain that does not exist, the program will flag an error.

```
Enter Domain: domainthatdoesnotexist.com
Record Type: ALL

Domain does not exist
```

2 - Subdomain Enumeration

- Enter domain name

```
1 - DNS Enumeration
2 - Subdomain Enumeration
3 - Reverse DNS Lookup
4 - DNS Zone Transfer
5 - DNS Cheat Sheet
6 - EXIT
Instruction: 2
Enter Domain: youtube.com
```

- Select between using a different wordlist or the code's own subdomain list.

```
Use a different wordlist? MP/wordlist.txt
www.google.com valid
mail.google.com valid
smtp.google.com valid
ns1.google.com valid
ns2.google.com valid
m.google.com valid
ns.google.com valid
blog.google.com valid
```

```
Use a different wordlist? n
www.youtube.com valid
m.youtube.com valid
admin.youtube.com valid
news.youtube.com valid
mx.youtube.com valid
img.youtube.com valid
ads.youtube.com valid
```

- At the end of the output, invalid subdomains will be displayed.

```
INVALID SUBDOMAINS:
ftp.google.com
localhost.google.com
webmail.google.com
pop.google.com
webdisk.google.com
cpanel.google.com
whm.google.com
autodiscover.google.com
autoconfig.google.com
imap.google.com
test.google.com
pop3.google.com
dev.google.com
```

3 - Reverse DNS Lookup

- Enter IP address

```
1 - DNS Enumeration
2 - Subdomain Enumeration
3 - Reverse DNS Lookup
4 - DNS Zone Transfer
5 - DNS Cheat Sheet
6 - EXIT
Instruction: 3
Enter IP:
```

- After entering the IP address, the record for the domain name of the IP address will be looked up.

```
Instruction: 3
Enter IP: 8.8.8.8
Domain name of 8.8.8.8 is dns.google.
------------------------------
```

```
Instruction: 3
Enter IP: 216.239.32.10
Domain name of 216.239.32.10 is ns1.google.com.
------------------------------
```

```
Instruction: 3
Enter IP: 157.240.199.35
Domain name of 157.240.199.35 is edge-star-mini-shv-01-hkg4.facebook.com.
------------------------------
```

- If the IP address entered is invalid, the program will flag an error that the domain does not exist.

```
Instruction: 3
Enter IP: 192.168.232.139
Does not exist
------------------------------
```

4 - DNS Zone Transfer

- Enter Domain Name

```
1 - DNS Enumeration
2 - Subdomain Enumeration
3 - Reverse DNS Lookup
4 - DNS Zone Transfer
5 - DNS Cheat Sheet
6 - EXIT
Instruction: 4
Enter Domain:
```

- The domain entered should be the root domain in order to get accurate results. After entering the domain, the name servers, its IP address, and the status of the zone transfer will be displayed.

```
Instruction: 4
Enter Domain: gooogle.com
[*] Found NS: ns1.google.com.
[*] IP for ns1.google.com. is 216.239.32.10
[*] NS ns1.google.com. refused zone transfer!
[*] Found NS: ns3.google.com.
[*] IP for ns3.google.com. is 216.239.36.10
[*] NS ns3.google.com. refused zone transfer!
[*] Found NS: ns2.google.com.
[*] IP for ns2.google.com. is 216.239.34.10
[*] NS ns2.google.com. refused zone transfer!
[*] Found NS: ns4.google.com.
[*] IP for ns4.google.com. is 216.239.38.10
[*] NS ns4.google.com. refused zone transfer!
```

- If zone transfer is allowed, then the program will output the zone file that contains different hosts and database information from the domain.

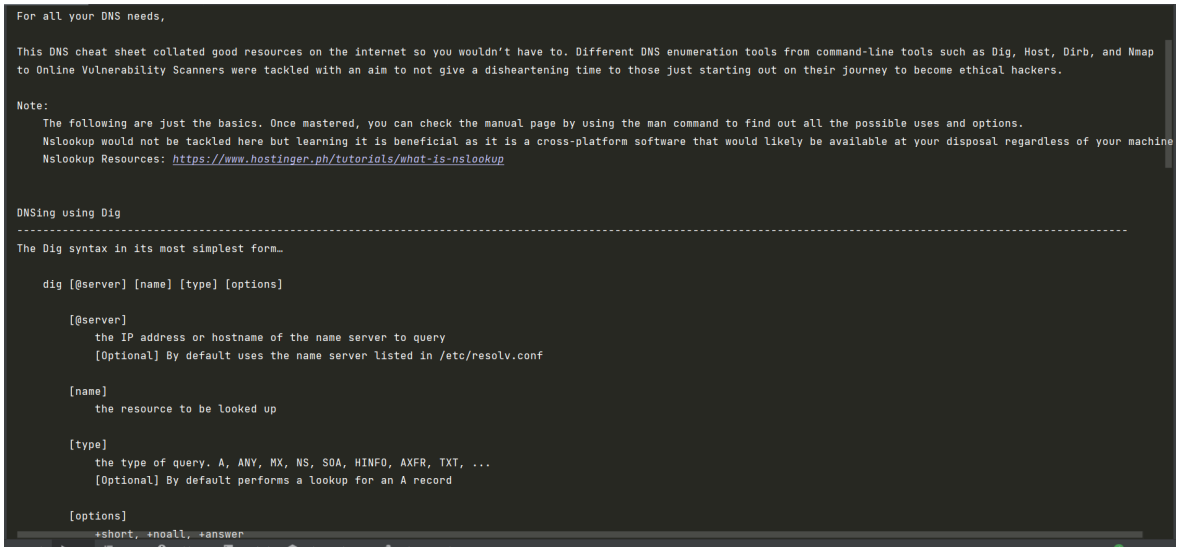
```
Instruction: 4
Enter Domain: zonetransfer.me
[*] Found NS: nsztm2.digi.ninja.
[*] IP for nsztm2.digi.ninja. is 34.225.33.2
[*] Found Host: @
[*] Found Host: _acme-challenge
[*] Found Host: _sip._tcp
[*] Found Host: 14.105.196.5.IN-ADDR.ARPA
[*] Found Host: asfdbauthdns
[*] Found Host: asfdbbox
[*] Found Host: asfdbvolume
[*] Found Host: canberra-office
[*] Found Host: cmdexec
[*] Found Host: contact
[*] Found Host: dc-office
[*] Found Host: deadbeef
[*] Found Host: dr
[*] Found Host: DZC
[*] Found Host: email
[*] Found Host: Hello
[*] Found Host: home
[*] Found Host: Info
[*] Found Host: internal
[*] Found Host: intns1
[*] Found Host: intns2
[*] Found Host: office
[*] Found Host: ipv6actnow.org
[*] Found Host: owa
[*] Found Host: robinwood
[*] Found Host: rp
```

- If the user enters a domain that does not exist, the program will flag an error.

```
Instruction: 4
Enter Domain: notworkingdomain.com

Domain does not exist
```

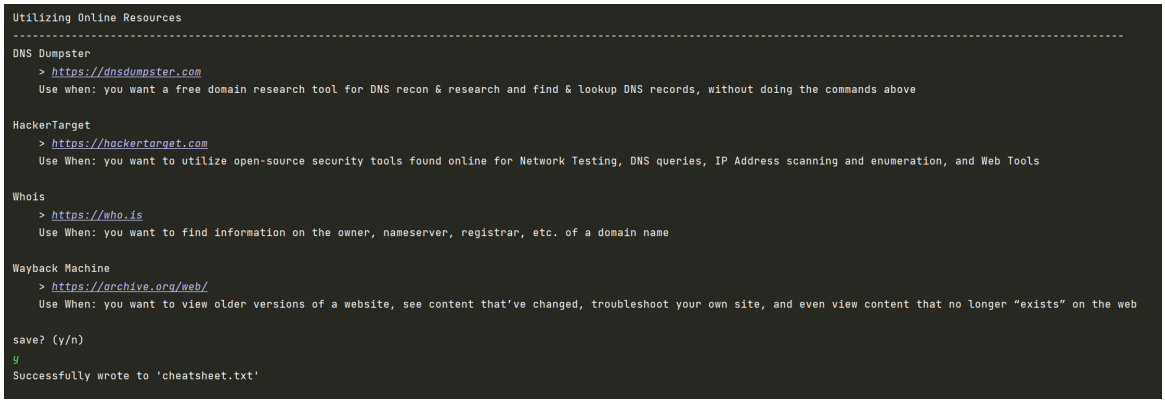
5 - DNS Cheat Sheet

- The contents of the DNS cheat sheet is outputted.



```
For all your DNS needs,

This DNS cheat sheet collated good resources on the internet so you wouldn't have to. Different DNS enumeration tools from command-line tools such as Dig, Host, Dirb, and Nmap
to Online Vulnerability Scanners were tackled with an aim to not give a disheartening time to those just starting out on their journey to become ethical hackers.

Note:
    The following are just the basics. Once mastered, you can check the manual page by using the man command to find out all the possible uses and options.
    Nslookup would not be tackled here but learning it is beneficial as it is a cross-platform software that would likely be available at your disposal regardless of your machine
    Nslookup Resources: https://www.hostinger.ph/tutorials/what-is-nslookup


DNSing using Dig
----------------------------------------------------------------------------------------------------------------------------------------------------------------------
The Dig syntax in its most simplest form…

    dig [@server] [name] [type] [options]

        [@server]
            the IP address or hostname of the name server to query
            [Optional] By default uses the name server listed in /etc/resolv.conf

        [name]
            the resource to be looked up

        [type]
            the type of query. A, ANY, MX, NS, SOA, HINFO, AXFR, TXT, ...
            [Optional] By default performs a lookup for an A record

        [options]
            +short, +noall, +answer
```

- An option to export the cheat sheet is given. If the user enters 'y', a text file named 'cheatsheet.txt' will be saved to the current directory.



```
Utilizing Online Resources
----------------------------------------------------------------------------------------------------------------------------------------------------------------------
DNS Dumpster
    > https://dnsdumpster.com
    Use when: you want a free domain research tool for DNS recon & research and find & lookup DNS records, without doing the commands above

HackerTarget
    > https://hackertarget.com
    Use When: you want to utilize open-source security tools found online for Network Testing, DNS queries, IP Address scanning and enumeration, and Web Tools

Whois
    > https://who.is
    Use When: you want to find information on the owner, nameserver, registrar, etc. of a domain name

Wayback Machine
    > https://archive.org/web/
    Use When: you want to view older versions of a website, see content that've changed, troubleshoot your own site, and even view content that no longer "exists" on the web

save? (y/n)
y
Successfully wrote to 'cheatsheet.txt'
```