Lab Tasks 3: Passive and Active Recon

Name: Noman Masood Khan
Roll Number: 211042-A
Course: CY243L - Penetration Testing - Lab
Date: 23/10/2023
Total Questions: 6
Attempted Questions: 6

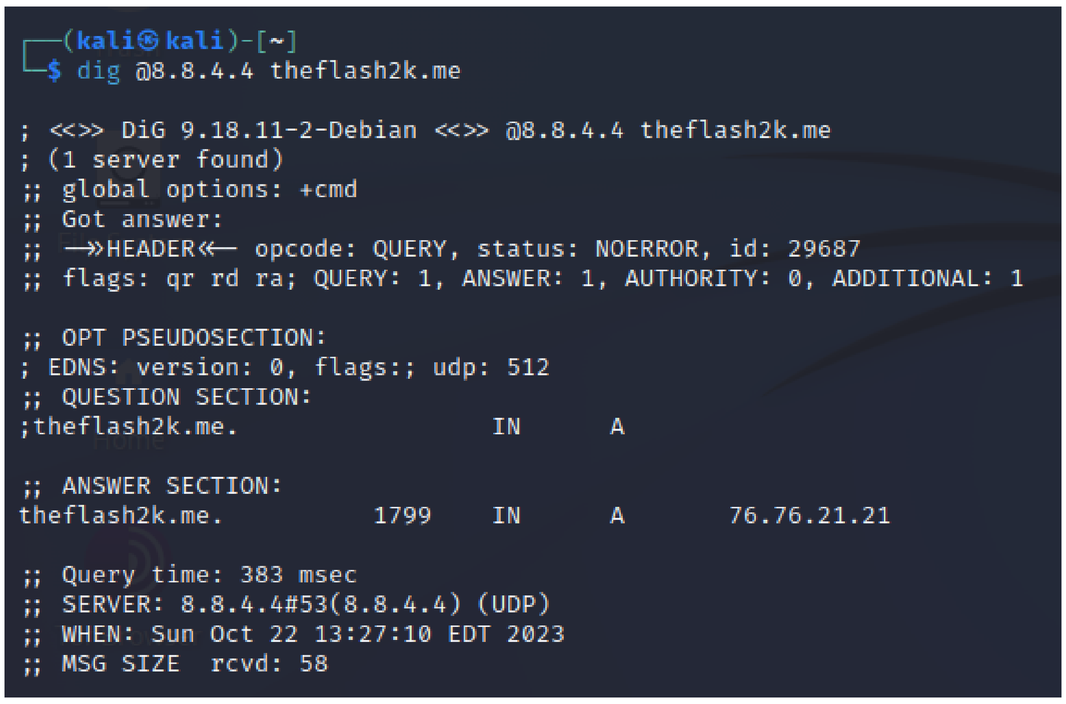
Tasks 1: Finding Ip Address of theflash2k.me

Command:

```
dig @8.8.4.4 theflash2k.me
```

dig is the command which is used to query the DNS server to perform DNS look-up for the targeted domain. Both the 8.8.8.8 and the 8.8.4.4 are google public DNS servers.

Output:

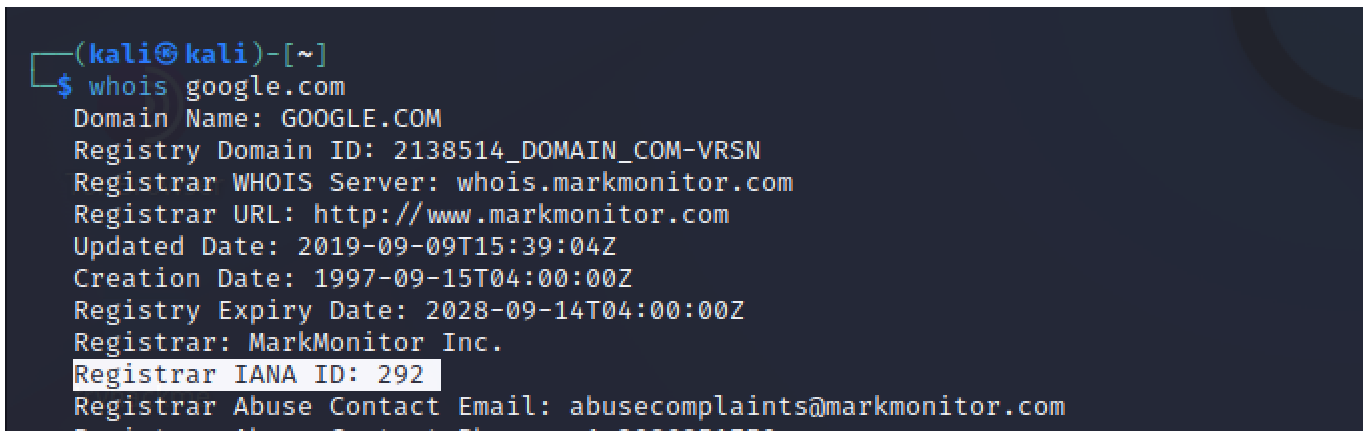


```
┌──(kali㉿kali)-[~]
└─$ dig @8.8.4.4 theflash2k.me

; <<>> DiG 9.18.11-2-Debian <<>> @8.8.4.4 theflash2k.me
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29687
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;theflash2k.me.                 IN      A

;; ANSWER SECTION:
theflash2k.me.          1799    IN      A       76.76.21.21

;; Query time: 383 msec
;; SERVER: 8.8.4.4#53(8.8.4.4) (UDP)
;; WHEN: Sun Oct 22 13:27:10 EDT 2023
;; MSG SIZE  rcvd: 58
```

⛳ **theflash2k.me** IP address is **76.76.21.21**

Tasks 2: WHOIS Look-Up on google.com

WHOIS look-up is used to retrieve information about the domain name, their registrar, their creation expiration date etc.



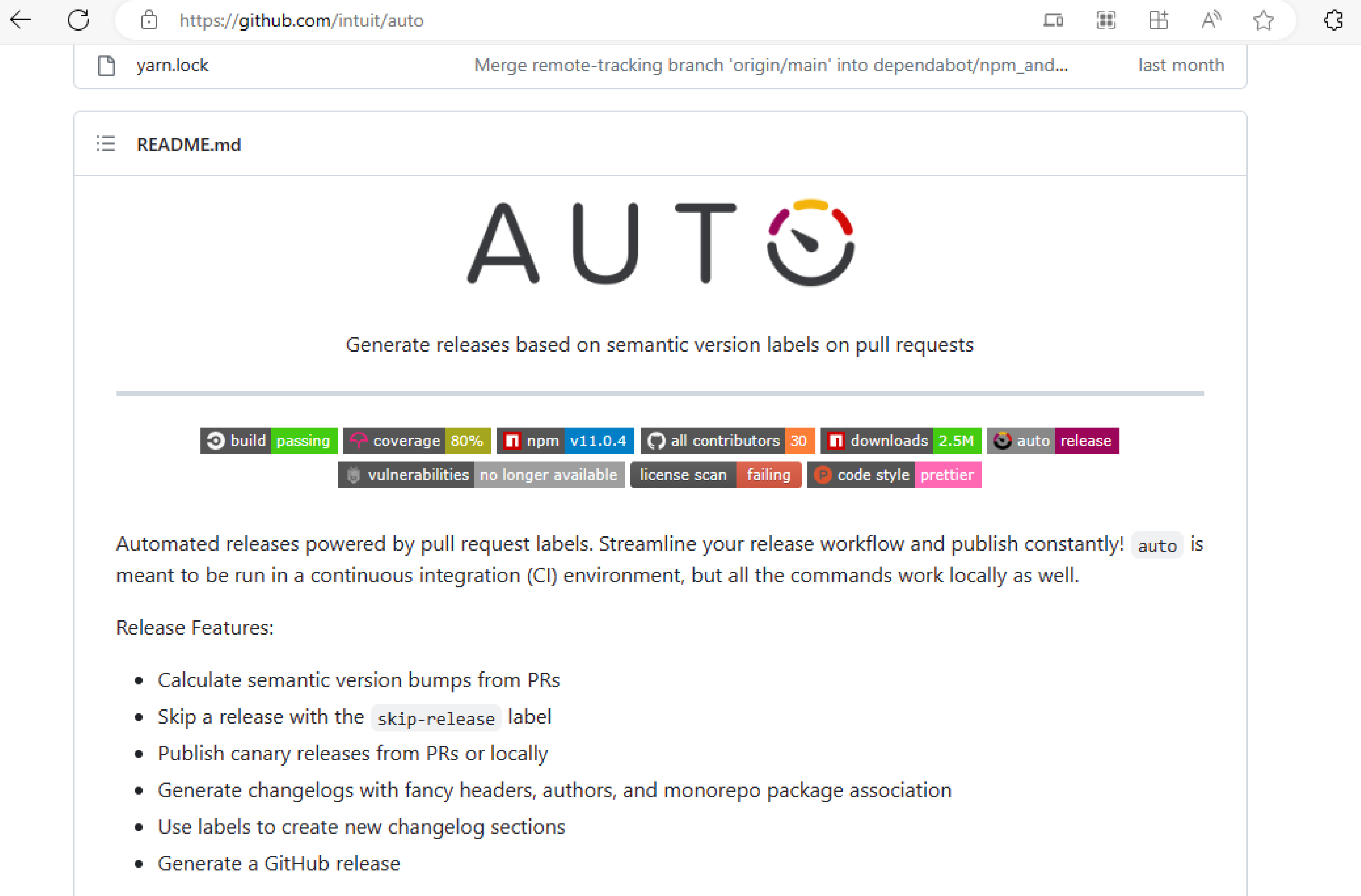
```
┌──(kali㉿kali)-[~]
└─$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
```

```
Google Registrar IANA ID: 292
Google Domain Creation Date: 1997-09-15
```

Tasks 3: Google Dorking for the finding the repos

```
Updated Dork : intext:"auto" "inurl:github"

URL of the Respository Found: https://github.com/intuit/auto
```

Screenshot of the Repository:



Generate releases based on semantic version labels on pull requests

Automated releases powered by pull request labels. Streamline your release workflow and publish constantly! `auto` is meant to be run in a continuous integration (CI) environment, but all the commands work locally as well.

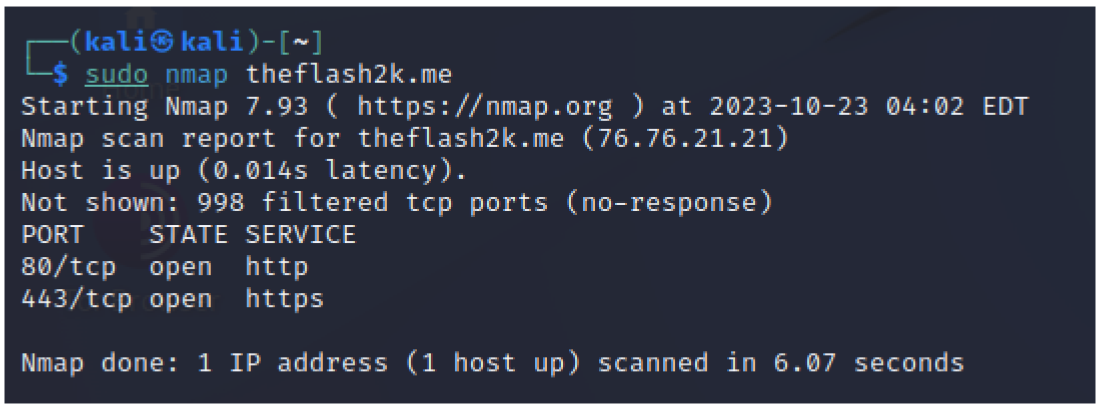
Release Features:

- Calculate semantic version bumps from PRs
- Skip a release with the `skip-release` label
- Publish canary releases from PRs or locally
- Generate changelogs with fancy headers, authors, and monorepo package association
- Use labels to create new changelog sections
- Generate a GitHub release

Active Reconnaissance

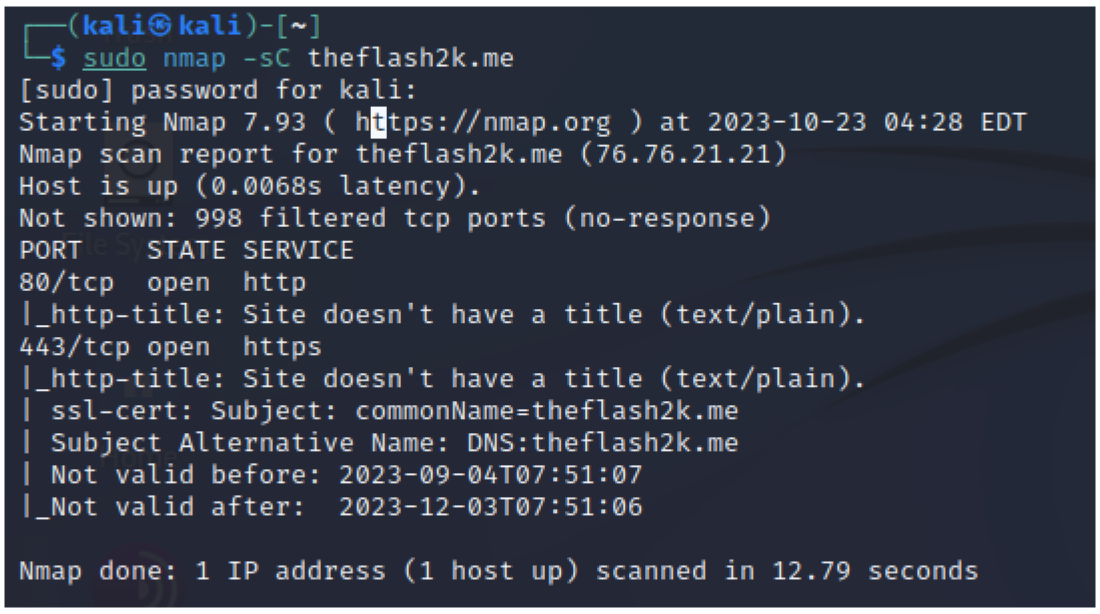
Tasks 1: How many ports are open on theflash2k.me.

The total **ports 80 and 443** are open on the theflash2k.me.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap theflash2k.me
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-23 04:02 EDT
Nmap scan report for theflash2k.me (76.76.21.21)
Host is up (0.014s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 6.07 seconds
```

```
Port 80 : service HTTP
Port 443 : service HTTPS
```

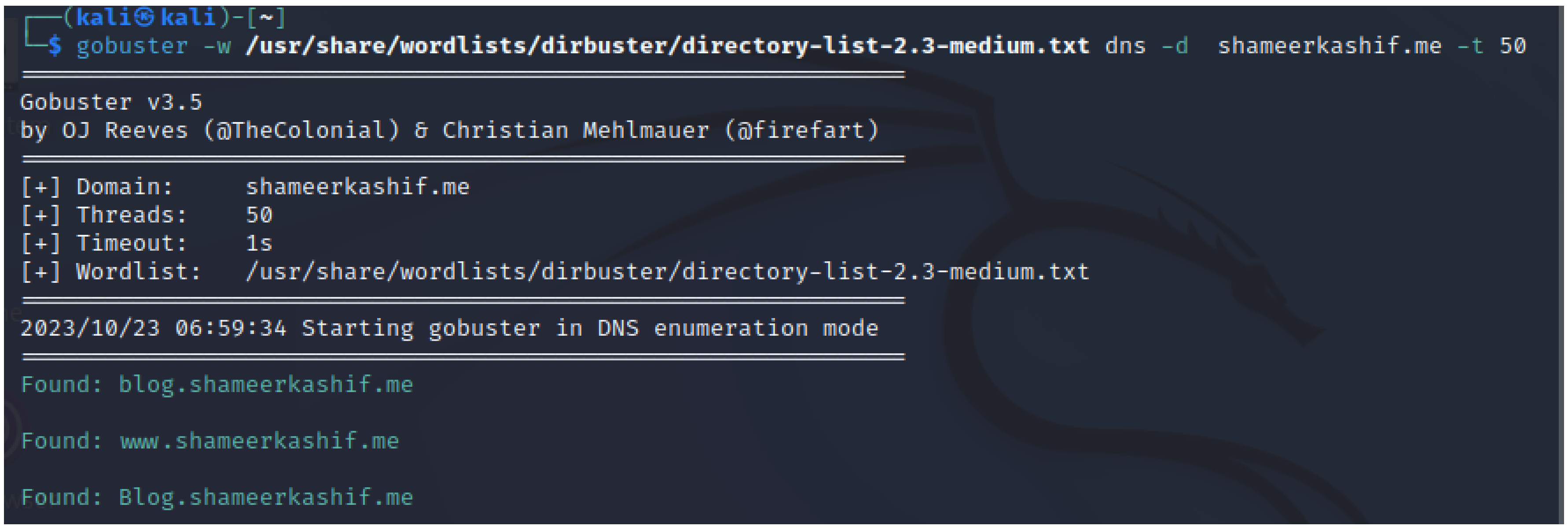


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC theflash2k.me
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-23 04:28 EDT
Nmap scan report for theflash2k.me (76.76.21.21)
Host is up (0.0068s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
|_http-title: Site doesn't have a title (text/plain).
443/tcp open  https
|_http-title: Site doesn't have a title (text/plain).
| ssl-cert: Subject: commonName=theflash2k.me
| Subject Alternative Name: DNS:theflash2k.me
| Not valid before: 2023-09-04T07:51:07
|_Not valid after:  2023-12-03T07:51:06

Nmap done: 1 IP address (1 host up) scanned in 12.79 seconds
```

Tasks 5: Finding the subdomains of the shameerkashif.me

The found subdirectories of the shameerkashif.me with the tool go-buster are:

```
Found: blog.shameerkashif.me

Found: www.shameerkashif.me

Found: Blog.shameerkashif.me
```



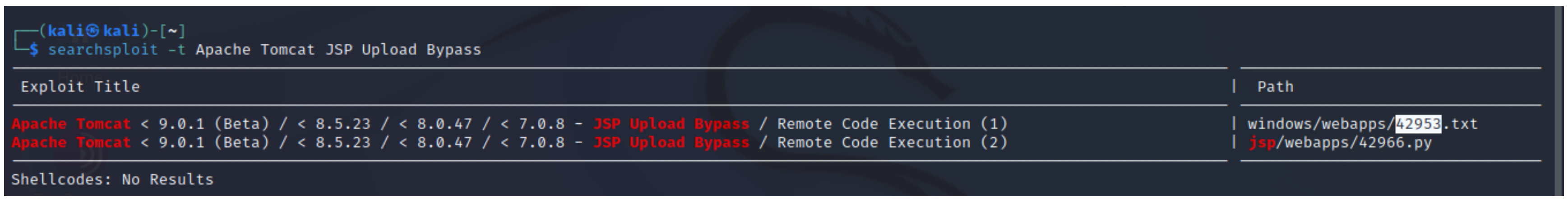
```
┌──(kali㉿kali)-[~]
└─$ gobuster -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt dns -d  shameerkashif.me -t 50
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Domain:     shameerkashif.me
[+] Threads:    50
[+] Timeout:    1s
[+] Wordlist:   /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
2023/10/23 06:59:34 Starting gobuster in DNS enumeration mode
===============================================================
Found: blog.shameerkashif.me

Found: www.shameerkashif.me

Found: Blog.shameerkashif.me
```

Tasks 6: Finding the subdomains of the shameerkashif.me

Command used:

```
searchsploit -t Apache Tomcat JSP Upload Bypass
```

Output:



```
┌──(kali㉿kali)-[~]
└─$ searchsploit -t Apache Tomcat JSP Upload Bypass
------------------------------------------------------------------------------------------------------ ---------------------------------
 Exploit Title                                                                                        |  Path
------------------------------------------------------------------------------------------------------ ---------------------------------
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2) | jsp/webapps/42966.py
------------------------------------------------------------------------------------------------------ ---------------------------------
Shellcodes: No Results
```

Searchsploit result for the Apache Tomcat

CVE	42953 and 42966
Exploit Title:	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1) Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)
Path	windows/webapps/42953.txt jsp/webapps/42966.py