

# Lab Task 3

## ⇒ Passive Recon

### Task - 1:

Using dig , and 8.8.4.4 as the dns, can you find the IP Address of theflash2k.me ?

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

```
(kali㉿kali)-[~/Desktop]
$ dig theflash2k.me @8.8.4.4

; <<>> DiG 9.19.17-1-Debian <<>> theflash2k.me @8.8.4.4
;; global options: +cmd
;; Got answer:
;; —>HEADER<— opcode: QUERY, status: NOERROR, id: 21545
;; 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: 467 msec
;; SERVER: 8.8.4.4#53(8.8.4.4) (UDP)
;; WHEN: Sat Oct 21 06:49:09 EDT 2023
;; MSG SIZE rcvd: 58
```

IP address: 76.76.21.21

### Task - 2:

Performing WHOIS Lookup on google.com , what is the Registrar's IANA ID and Creation Date?

```
whois google.com
```

```
(kali㉿kali)-[~/Desktop]
$ 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
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
```

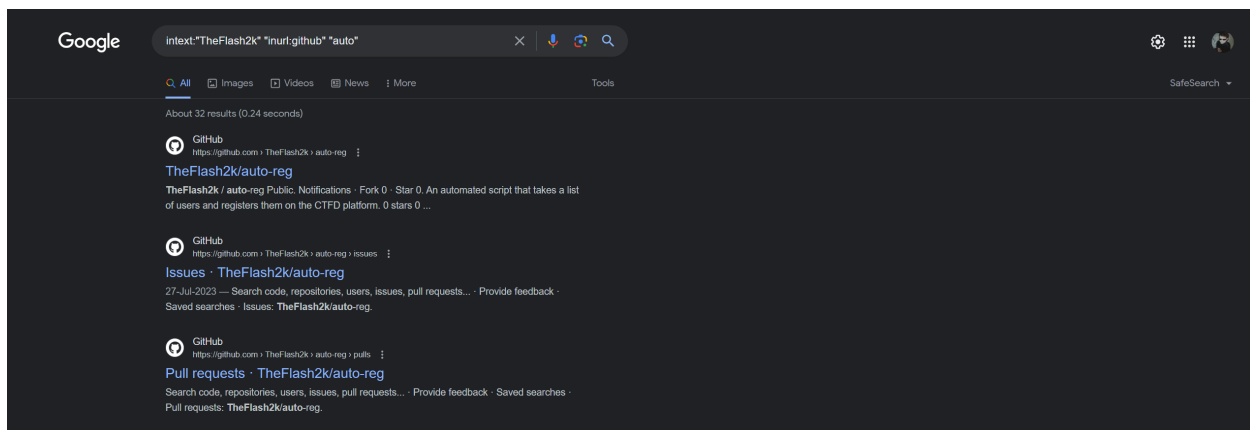
Creation Date: 1997-09-15T04:00:00Z

Registrar IANA ID: 292

### Task - 3:

Using the following google dork: `intext:"TheFlash2k" "inurl:github"` , can you find the REPO that contains the word auto ? Modify the dork and answer with the updated dork, and the screenshot + url of the repository found.

```
intext:"TheFlash2k" "inurl:github" "auto"
```



Repository URL: <https://github.com/TheFlash2k/auto-reg>

## ⇒ Active Recon

### Task - 4:

How many ports are open on theflash2k.me . Also, add a screenshot of the service and script scan that you ran against the open ports.

```
(kali㉿kali)-[~/Desktop]
└─$ nmap -T4 theflash2k.me
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-21 06:59 EDT
Nmap scan report for theflash2k.me (76.76.21.21)
Host is up (0.051s 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 9.22 seconds
```



Using searchsploit, what is the exact CVE , the Exploit Title and Path for Apache Tomcat JSP Upload Bypass . Answer should be like: CVE-2023, Microsoft Shares < 9.0, jsp/webapps/91251.py

```
(kali㉿kali)-[~/Desktop]
└─$ searchsploit --cve Apache Tomcat JSP Upload Bypass
```

Exploit Title

Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - .

Shellcodes: No Results

The screenshot shows the Exploit Database website interface. The main title is "EXPLOIT DATABASE". The search results for "Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)" are displayed. The details are as follows:

EDB-ID:		CVE:		Author:		Type:		Platform:		Date:	
42966		2017-12617		INTX0X80		WEBAPPS		JSP		2017-10-09	
EDB Verified: ✓				Exploit: 📄 / {}				Vulnerable App:			

CVE: CVE-2017-12617