

# AI FOR CYBER SECURITY WITH IBM QRADAR

**Name:** J. Manasa

## **TASK-7:** Gather information about the websites through Footprinting and Reconnaissance

For this task, the website used here is [www.lifeat.io](http://www.lifeat.io)

First of all, the information related to the above website is gathered through [nslookup.io](http://nslookup.io) for cross verification.

IP Address: 76.76.21.21 (Cloudflare)

### DNS records for **lifeat.io**

CloudflareGoogle DNSOpenDNSAuthoritativeLocal DNS

The Cloudflare DNS server responded with these DNS records. Cloudflare will serve these records for as long as the time to live (TTL) has not expired. After this period, Cloudflare will update its cache by querying one of the authoritative name servers.

#### A records

IPv4 address	Revalidate in
> a 76.76.21.21	1h

#### AAAA records


No AAAA records found.


#### CNAME record


No CNAME record found.


#### TXT records

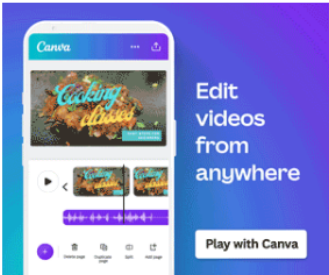
##### Site ownership verification

**Firebase**  
  
Firebase  
lifeatspaces-prod

**Google**  
  
Google  
YKKwwwKkvA72b2i5Lml

**Google**  
  
Google  
zc\_Rl1rdJKbPhOiiVC7i17

**Microsoft**  
  
Microsoft  
ms51258695



Cloudflare Google DNS OpenDNS Authoritative Local DNS			
NS records			
Name server		Revalidate in	
ns-cloud-a1.googledomains.com.		6h	
ns-cloud-a2.googledomains.com.		6h	
ns-cloud-a3.googledomains.com.		6h	
ns-cloud-a4.googledomains.com.		6h	
MX records			
Mail server	Priority	Revalidate in	
aspmx.l.google.com.	1 Primary	1h	
alt1.aspmx.l.google.com.	5	1h	
alt2.aspmx.l.google.com.	5	1h	
alt3.aspmx.l.google.com.	10	1h	
alt4.aspmx.l.google.com.	10	1h	
Other records			
SOA			
SOA data			Revalidate in
Start of authority	ns-cloud-a1.googledomains.com.	6h	
Email	cloud-dns-hostmaster@google.com		
Serial	83		
Refresh	6h		
Retry	1h		
Expire	72h		
Negative cache TTL	5m		

Foot printing:

For footprinting, the harvester tool was used.

```

/bin/bash
/bin/bash 149x35
theHarvester
theHarvester 4.0.3
Coded by Christian Martorella
Edge-Security Research
cmartorella@edge-security.com

[*] Target: llifeat.io

[!] Missing API key for Spyse.
[!] Missing API key for Censys ID and/or Secret.
[!] Missing API key for Github.
[!] Missing API key for fullhunt.
[!] Missing API key for Hunter.
[!] Missing API key for binaryedge.
[!] Missing API key for Intelx.
[!] Missing API key for ProjectDiscovery.
[!] Missing API key for RocketReach.

```

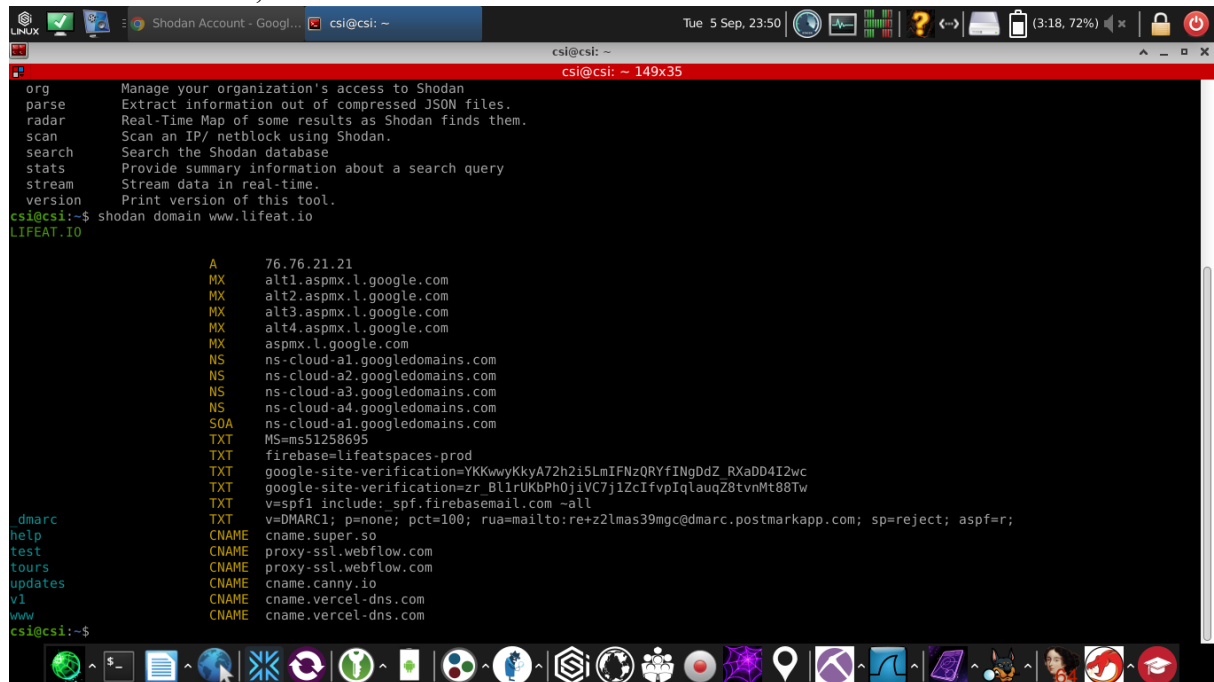
```
Linux tmp-lifeat.io... Facebook ... x-terminal-e... YAD Question Wed 6 Sep, 00:08 /bin/bash /bin/bash 149x35
[*] Searching Google.
[*] ASNS found: 2
-----
AS14618
AS16509
[*] Interesting Urls found: 3
-----
https://lifeat.io/
https://lifeat.io/room/tJPtsrpYi2XAYC0G?space=130&host=jean%27s+room
https://updates.lifeat.io/
[*] No Twitter users found.
[*] No LinkedIn users found.
[*] LinkedIn Links found: 0
-----
[*] No Trello URLs found.
[*] IPs found: 27
-----
3.214.76.85
18.214.52.112
34.208.226.23
34.209.167.56
34.218.6.194
35.166.52.177
44.214.112.154
```

```
Linux tmp-lifeat.io... Facebook ... x-terminal-e... YAD Question Wed 6 Sep, 00:08 /bin/bash /bin/bash 149x35
[*] Hosts found: 20
-----
help.lifeat.io:76.76.21.164, 76.76.21.9
help.lifeat.io:76.76.21.9, 76.76.21.164
o3.info.lifeat.io:159.183.175.163
o4.out.mail.lifeat.io:168.245.31.241
test.lifeat.io:13.234.100.116, 13.200.123.229, 65.0.79.182
test.lifeat.io:13.200.123.229, 13.234.100.116, 65.0.79.182
tours.lifeat.io:65.0.79.182, 13.234.100.116, 13.200.123.229
tours.lifeat.io:proxy-ssl-geo.webflow.com
tours.lifeat.io:65.0.79.182, 13.200.123.229, 13.234.100.116
tours.lifeat.io:proxy-ssl.webflow.com
tours.lifeat.io:proxy-ssl.webflow.com
updates.lifeat.io:44.214.112.154
v1.lifeat.io:76.76.21.164, 76.76.21.9
v1.lifeat.io:76.76.21.9, 76.76.21.164
v1.lifeat.io:cname.vercel-dns.com
www.lifeat.io:cname.vercel-dns.com
www.lifeat.io:76.76.21.164, 76.76.21.9
[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.
INFO: Checking lifeat.io
+ 76.76.21.21 [VERCEL-01]
INFO: Checking www.lifeat.io
+ CNAME: cname.vercel-dns.com
+ 76.76.21.9 [VERCEL-01]
+ 76.76.21.164 [VERCEL-01]
INFO: Checking test.lifeat.io
+ CNAME: proxy-ssl.webflow.com
+ CNAME: proxy-ssl-geo.webflow.com
```

```
Linux tmp-lifeat.io... Facebook ... x-terminal-e... YAD Question Wed 6 Sep, 00:09 /bin/bash /bin/bash 149x35
INFO: Checking lifeat.io
+ 76.76.21.21 [VERCEL-01]
INFO: Checking www.lifeat.io
+ CNAME: cname.vercel-dns.com
+ 76.76.21.9 [VERCEL-01]
+ 76.76.21.164 [VERCEL-01]
INFO: Checking test.lifeat.io
+ CNAME: proxy-ssl.webflow.com
+ CNAME: proxy-ssl-geo.webflow.com
+ 13.200.123.229 [AMAZON-BOM]
+ 13.234.100.116 [AMAZON-BOM]
+ 65.0.79.182 [AMAZON-BOM]
INFO: Subdomain enumeration progress [22/976]
INFO: Subdomain enumeration progress [42/976]
INFO: Subdomain enumeration progress [62/976]
INFO: Subdomain enumeration progress [82/976]
INFO: Subdomain enumeration progress [102/976]
INFO: Subdomain enumeration progress [122/976]
INFO: Checking help.lifeat.io
+ CNAME: cname.super.so
+ CNAME: cname.vercel-dns.com
+ 76.76.21.9 [VERCEL-01]
+ 76.76.21.164 [VERCEL-01]
INFO: Subdomain enumeration progress [143/976]
INFO: Subdomain enumeration progress [163/976]
INFO: Subdomain enumeration progress [183/976]
INFO: Subdomain enumeration progress [203/976]
INFO: Subdomain enumeration progress [223/976]
INFO: Subdomain enumeration progress [243/976]
INFO: Subdomain enumeration progress [263/976]
INFO: Subdomain enumeration progress [283/976]
INFO: Subdomain enumeration progress [303/976]
INFO: Subdomain enumeration progress [323/976]
```

## Reconnaissance:

For reconnaissance, Shodan tool was used.



```
org      Manage your organization's access to Shodan
parse    Extract information out of compressed JSON files.
radar    Real-Time Map of some results as Shodan finds them.
scan     Scan an IP/ netblock using Shodan.
search   Search the Shodan database
stats    Provide summary information about a search query
stream   Stream data in real-time.
version  Print version of this tool.

csi@csi:~$ shodan domain www.lifeat.io
LIFEAT.IO

A        76.76.21.21
MX       alt1.aspmx.l.google.com
MX       alt2.aspmx.l.google.com
MX       alt3.aspmx.l.google.com
MX       alt4.aspmx.l.google.com
MX       aspmx.l.google.com
NS       ns-cloud-a1.googledomains.com
NS       ns-cloud-a2.googledomains.com
NS       ns-cloud-a3.googledomains.com
NS       ns-cloud-a4.googledomains.com
SOA      ns-cloud-a1.googledomains.com
TXT      MS=ms51258695
TXT      firebase=lifeatspaces-prod
TXT      google-site-verification=YKKwvyKkyA72h2i5LmIFNzQRYfINGdDZ_RXaDD4I2wc
TXT      google-site-verification=zr_BllrUKbPh0jiVC7j1ZcIfvpIqlauqZ8tvnMt88Tw
TXT      v=spf1 include:spf.firebasemail.com ~all
TXT      v=DMARC1; p=none; pct=100; rua=mailto:re+z2lmas39mgc@dmarc.postmarkapp.com; sp=reject; aspf=r;
CNAME    cname.super.so
CNAME    proxy-ssl.webflow.com
CNAME    proxy-ssl.webflow.com
CNAME    cname.canny.io
CNAME    cname.vercel-dns.com
CNAME    cname.vercel-dns.com

dmarc
help
test
tours
updates
v1
www
csi@csi:~$
```