

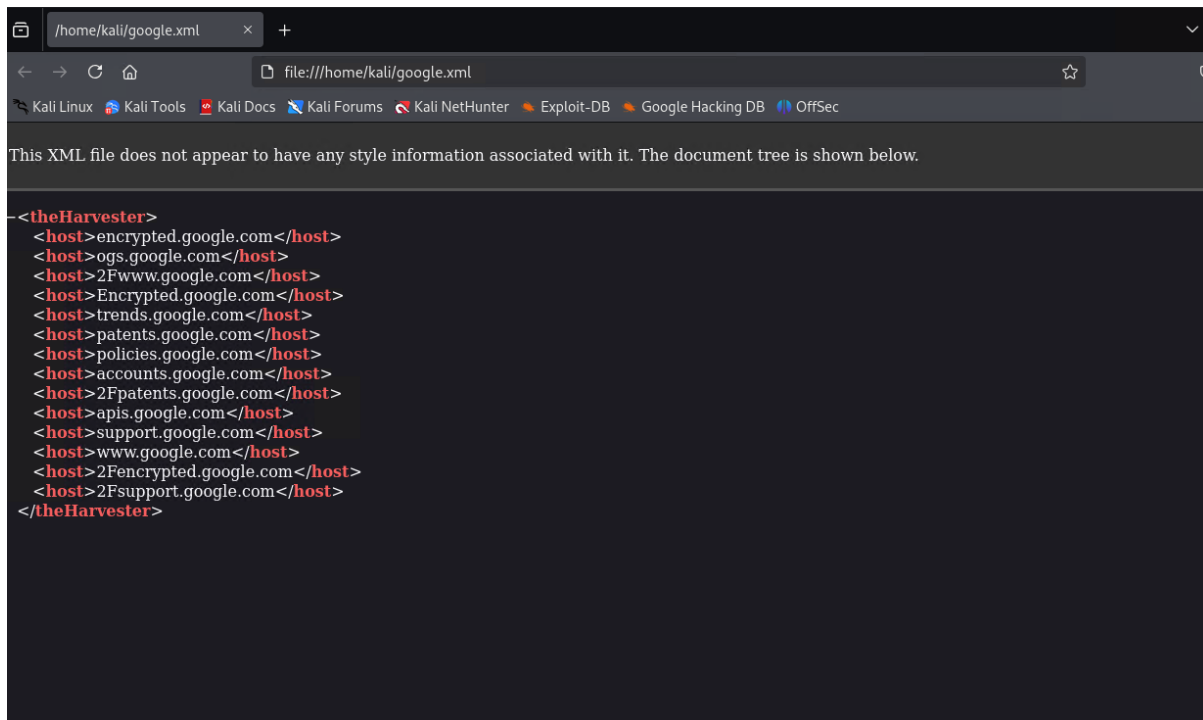
Lab 1

```
kali@kali: ~  
File Actions Edit View Help  
subdomainfinder99, threatminer, tomba, urlscan, virustotal, yahoo, zoomeye  
  
(kali@kali)-[~]  
$ theHarvester -d google.com -l 500 -b duckduckgo -f google  
Read proxies.yaml from /home/kali/.theHarvester/proxies.yaml  
*****  
*  
* [TheHarvester] *  
* [TheHarvester] *  
* [TheHarvester] *  
* [TheHarvester] *  
* [TheHarvester] *  
* [TheHarvester] *  
* theHarvester 4.6.0 *  
* Coded by Christian Martorella *  
* Edge-Security Research *  
* cmartorella@edge-security.com *  
* *  
*****  
[*] Target: google.com  
[*] Searching Duckduckgo.  
[*] No IPs found.  
[*] No emails found.
```

Ran harvester against google.com

```
kali@kali: ~  
File Actions Edit View Help  
[*] Target: google.com  
[*] Searching Duckduckgo.  
[*] No IPs found.  
[*] No emails found.  
[*] Hosts found: 12  
2Fencrypted.google.com  
2Fpatents.google.com  
2Fsupport.google.com  
Encrypted.google.com  
accounts.google.com  
apis.google.com  
encrypted.google.com  
ogs.google.com  
patents.google.com  
policies.google.com  
support.google.com  
trends.google.com  
[*] Reporting started.  
[*] XML File saved.  
[*] JSON File saved.
```

Information listed



Also able to view through xml file but the content is same

```
(kali@kali)-[~]
$ sublist3r -h
usage: sublist3r [-h] -d DOMAIN [-b [BRUTEFORCE]] [-p PORTS] [-v [VERBOSE]] [-t THREADS] [-e ENGINES]
               [-o OUTPUT] [-n]

OPTIONS:
  -h, --help            show this help message and exit
  -d DOMAIN, --domain DOMAIN
                        Domain name to enumerate it's subdomains
  -b [BRUTEFORCE], --bruteforce [BRUTEFORCE]
                        Enable the subbrute bruteforce module
  -p PORTS, --ports PORTS
                        Scan the found subdomains against specified tcp ports
  -v [VERBOSE], --verbose [VERBOSE]
                        Enable Verbosity and display results in realtime
  -t THREADS, --threads THREADS
                        Number of threads to use for subbrute bruteforce
  -e ENGINES, --engines ENGINES
                        Specify a comma-separated list of search engines
  -o OUTPUT, --output OUTPUT
                        Save the results to text file
  -n, --no-color        Output without color

Example: python3 /usr/bin/sublist3r -d google.com
```

help command of sublist3r

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sublist3r -d google.com -o google.txt  
  
SUBLIST3R  
# Coded By Ahmed Aboul-Ela - @aboul3la  
  
[-] Enumerating subdomains now for google.com  
[-] Searching now in Baidu..  
[-] Searching now in Yahoo..  
[-] Searching now in Google..  
[-] Searching now in Bing..  
[-] Searching now in Ask..  
[-] Searching now in Netcraft..  
[-] Searching now in DNSdumpster..  
[-] Searching now in Virustotal..  
[-] Searching now in ThreatCrowd..  
[-] Searching now in SSL Certificates..  
[-] Searching now in PassiveDNS..  
Process DNSdumpster-8:  
Traceback (most recent call last):  
  File "/usr/lib/python3.12/multiprocessing/process.py", line 314, in _bootstrap
```

ran the scan using sublist3r

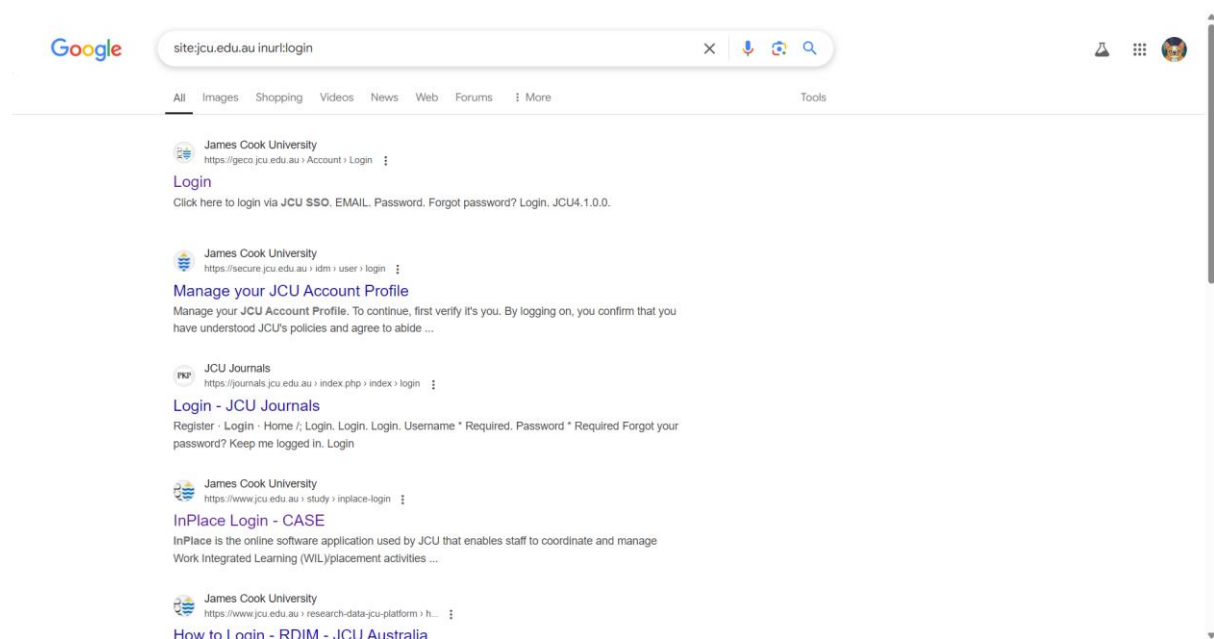
```
~/google.txt - Mousepad  
File Edit Search View Document Help  
  
1 www.google.com  
2 accounts.google.com  
3 freezone.accounts.google.com  
4 adwords.google.com  
5 qa.adz.google.com  
6 answers.google.com  
7 apps-secure-data-connector.google.com  
8 audioads.google.com  
9 checkout.google.com  
10 mtv-da-1.ad.corp.google.com  
11 ads-compare.eem.corp.google.com  
12 da.ext.corp.google.com  
13 m.guts.corp.google.com  
14 m.gutsdev.corp.google.com  
15 login.corp.google.com  
16 mtv-da.corp.google.com  
17 mygeist.corp.google.com  
18 mygeist2010.corp.google.com  
19 proxyconfig.corp.google.com  
20 reseed.corp.google.com  
21 twdsalesgsa.twd.corp.google.com  
22 uberproxy.corp.google.com  
23 uberproxv-nocert.corp.google.com
```

there are loads of urls when scanned through sublist3r

This thing happens because compared to theHarvester, sublit3r uses multiple search engines to gather information, and when theHarvester is doing information gathering, it requires api keys while sublit3r does not

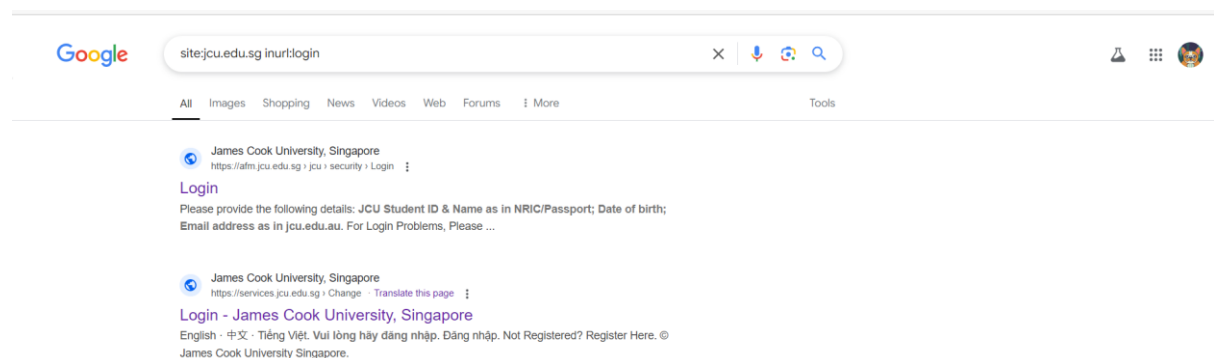
Following the difference, when gathering information for hacking purposes, using sublit3r is beneficial due to its wide range of gathering related information

Lab 2



Firstly searched login pages of jcu.edu.au

There were multiple pages of login



But when searched Singapore there were only 2 results

I think this happens because when logging into jcu server, we pass through au domain either campus

Our learn jcu portal's domain is au

Google dorking could be effective when finding the main domain of a enterprise or schools like jcu, because if such thing similar to sg and au happens, the attacker will instantly notice au is where the jcu main campus is located

Lab 3

NS Records						
ns0200.secondary.cloudflare.co	162.159.33.75	ASN: 13335	CLOUDFLARENET	http: cloudflare		⋮
ns0200.secondary.cloudflare.co	162.159.32.0/23			title: Direct IP access not allowed		
				tech: Cloudflare		
				http8080: cloudflare		
				title: Direct IP access not allowed		
				tech: Cloudflare		
ns0074.secondary.cloudflare.co	162.159.32.75	ASN: 13335	CLOUDFLARENET	http: cloudflare		⋮
ns0074.secondary.cloudflare.co	162.159.32.0/23			title: Direct IP access not allowed		
				tech: Cloudflare		
				http8080: cloudflare		
				title: Direct IP access not allowed		
				tech: Cloudflare		

162.159.33.75 and 162.159.32.75 is the ns ip address

The ip belongs to cloudflare from here we can know that jcu uses cloudflare as dns provider

MX Records					
0 smtp-in.jcu.edu.au	137.219.20.34	ASN: 24434	JCU-AS-AP James Cook University, AU		⋮
	smtp-in.jcu.edu.au	137.219.0.0/18	Australia		
0 smtp-in-cns.jcu.edu.au	137.219.220.34	ASN: 24434	JCU-AS-AP James Cook University, AU		⋮
	smtp-in-cns.jcu.edu.au	137.219.220.0/22	Australia		

137.219.20.34 and 137.219.220.34

A Records (subdomains from dataset)						
Host	IP	ASN	ASN Name	Open Services (from DB)	RevIP	
3dprinter01.jcu.edu.au	10.132.61.21	ASN:	Reserved (Local Network)		1	⋮
aa1.jcu.edu.au	137.219.18.44	ASN: 24434	JCU-AS-AP James Cook University, AU		1	⋮
	aa1.jcu.edu.au	137.219.0.0/18	Australia			
aa2.jcu.edu.au	137.219.218.44	ASN: 24434	JCU-AS-AP James Cook University, AU		1	⋮
	aa2.jcu.edu.au	137.219.218.0/24	Australia			
aa2m.jcu.edu.au	10.17.20.44	ASN:	Reserved (Local Network)		1	⋮
academs.jcu.edu.au	137.219.16.27	ASN: 24434	JCU-AS-AP James Cook University, AU		1	⋮
	academs.jcu.edu.au	137.219.0.0/18	Australia			
access.jcu.edu.au	137.219.6.88	ASN: 24434	JCU-AS-AP James Cook University, AU	https: BigIP cn: access.jcu.edu.au o: James Cook University tech: F5 BigIP	1	⋮
access-all.jcu.edu.au	137.219.6.85	ASN: 24434	JCU-AS-AP James Cook University, AU	https: BigIP cn: access-all.jcu.edu.au o: James Cook University tech: F5 BigIP	1	⋮
access-alt.jcu.edu.au	137.219.6.86	ASN: 24434	JCU-AS-AP James Cook University, AU	https: BigIP cn: access-alt.jcu.edu.au o: James Cook University tech: F5 BigIP	1	⋮
access-dev.jcu.edu.au	137.219.6.87	ASN: 24434	JCU-AS-AP James Cook University, AU	https: BigIP cn: access-dev.jcu.edu.au o: James Cook University tech: F5 BigIP	1	⋮

				cn: secure.levartdistributionsystems.com.au tech: Apache HTTP Server		
saintscatholiccollege.accommodation.jcu.edu.au	103.10.8.50 web.levart.com.au	ASN: 38830 103.10.8.0/24	LEVART-AS-AU-AP Levart Distribution Systems Pty Ltd, AU Australia	http: Apache title: 403 Forbidden tech: Apache HTTP Server https: Apache title: 403 Forbidden cn: secure.levartdistributionsystems.com.au tech: Apache HTTP Server	1009	⋮
www.saintscatholiccollege.accommodation.jcu.edu.au	103.10.8.50 web.levart.com.au	ASN: 38830 103.10.8.0/24	LEVART-AS-AU-AP Levart Distribution Systems Pty Ltd, AU Australia	http: Apache title: 403 Forbidden tech: Apache HTTP Server https: Apache title: 403 Forbidden cn: secure.levartdistributionsystems.com.au tech: Apache HTTP Server	1009	⋮
ad-bdc-dc-1.jcu.edu.au	137.219.218.13 ad-bdc-dc-1.ad.jcu.edu.au	ASN: 24434 137.219.218.0/24	JCU-AS-AP James Cook University, AU Australia		1	⋮
ad-bdc-dc-2.jcu.edu.au	137.219.218.14 ad-bdc-dc-2.ad.jcu.edu.au	ASN: 24434 137.219.218.0/24	JCU-AS-AP James Cook University, AU Australia		1	⋮
ad-tdc-ca-1.jcu.edu.au	137.219.18.21 ad-tdc-ca-1.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
ad-tdc-dc-1.jcu.edu.au	137.219.18.11 ad-tdc-dc-1.ad.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
ad-tdc-dc-2.jcu.edu.au	137.219.18.12 ad-tdc-dc-2.ad.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮
adfs.jcu.edu.au	137.219.20.61 adfs.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	⋮

adfs-test.jcu.edu.au	137.219.20.80 adfs-test.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
aims.jcu.edu.au	45.42.212.136 ips136.securedns-host.com	ASN: 13649 45.42.212.0/24	ASN-FLEXENTIAL United States	ftp: 20- Welcome to Pure-FTPd privsep TLS - 20-You are user number 1 of 50 allowed. 20- Local time is now 1 http: Apache tech: Apache HTTP Server https: Apache title: Index of / cn: .beta.mobi tech: Apache HTTP Server	516	:
aimswebbox.jcu.edu.au	137.219.5.12 aimswebbox.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
airflow.jcu.edu.au	137.219.20.159 airflow.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
airflow-dev01.jcu.edu.au	137.219.20.135 airflow-dev01.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
airflow-dev02.jcu.edu.au	137.219.20.138 airflow-dev02.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
airflow-dl.jcu.edu.au	137.219.20.158 airflow-dl.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
airflow-uat.jcu.edu.au	137.219.20.144 airflow-uat.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
aithm.jcu.edu.au	101.0.92.98 ded116126.smartservers.co m.au	ASN: 55803 101.0.64.0/18	HOSTOPIA-AU Hostopia Australia Web Pty Ltd, AU Australia	http: Apache tech: Apache HTTP Server		:
www.aithm.jcu.edu.au	101.0.92.98 ded116126.smartservers.co	ASN: 55803 101.0.64.0/18	HOSTOPIA-AU Hostopia Australia Web Pty Ltd, AU	http: Apache tech: Apache HTTP Server		:

xargo.aithm.jcu.edu.au	101.0.92.98 ded116126.smartservers.co m.au	ASN: 55803 101.0.64.0/18	HOSTOPIA-AU Hostopia Australia Web Pty Ltd, AU Australia	http: Apache tech: Apache HTTP Server		:
aithmtrf.jcu.edu.au	54.252.90.196 cpt.awsia.com	ASN: 16509 54.252.0.0/17	AMAZON-02 Australia		20	:
alesco.jcu.edu.au	137.219.23.126 alesco.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
alesco-dev02.jcu.edu.au	137.219.23.176 riams-dev1.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		2	:
alesco-dev03.jcu.edu.au	137.219.23.182 alesco-dev03.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
alesco-sup01.jcu.edu.au	137.219.20.162 idcard-admin.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia			:
alesco-test02.jcu.edu.au	137.219.23.170 alesco-test02.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
alesco-train02.jcu.edu.au	137.219.23.173 alesco-train02.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
alesco-tst02.jcu.edu.au	137.219.20.165 alesco-tst02.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
alesco-uat02.jcu.edu.au	137.219.23.179 alesco-uat02.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
amxrms.jcu.edu.au	137.219.23.101 amxrms.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
amxrmsdb01.jcu.edu.au	137.219.23.102 amxrmsdb01.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:
angler.jcu.edu.au	137.219.3.32 angler.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		1	:

anypoint.jcu.edu.au	137.219.20.11 anypoint.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
anypoint-test.jcu.edu.au	137.219.23.30 anypoint-test.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
anypoint-uat.jcu.edu.au	137.219.23.31 anypoint-uat.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
api.jcu.edu.au	137.219.20.137 api.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
api-designer.jcu.edu.au	137.219.20.66 api-designer.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
api-test.jcu.edu.au	137.219.23.32 api-test.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia		⋮
api-uat.jcu.edu.au	137.219.23.33 api-uat.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮
artifactory.jcu.edu.au	137.219.20.96 artifactory.jcu.edu.au	ASN: 24434 137.219.0.0/18	JCU-AS-AP James Cook University, AU Australia	1	⋮

There are a lot records of A record

137.219.218.13

137.219.218.14

137.219.18.21

137.219.18.11

137.219.18.12

These ip addresses have ad which is active directory controlling services, possibly be used as ldap server

Ns records show dns sesrvers

Mx records show email servers where received email of jcu is handled

A records show ip address of domain name and their ip addresses

Dns dumpster helps in mapping the attack surface, identifying subdomains

But the accuracy is not certified and only 50 results were visible limiting the information for hackig