

Module 2:

Lab 1: Task 1:

OS:Windows

Information gathering using Advanced Google Dorks

The screenshot shows a Google search interface with the query "cyber security" AND "fresher" AND "Hiring". The results are filtered for "Dubai". The "Date posted" filter is selected. The search results show several resources indicating that there are numerous opportunities for freshers in cyber security within the Middle East, particularly in Dubai. A sidebar on the right shows "Cyber Security Jobs in UAE - 206 Vacancies Aug 2025" and a snippet about a cyber security expert.

Google search results for "cyber security" AND "fresher" AND "Hiring". The search is filtered for "Dubai". The results show several resources indicating that there are numerous opportunities for freshers in cyber security within the Middle East, particularly in Dubai. A sidebar on the right shows "Cyber Security Jobs in UAE - 206 Vacancies Aug 2025" and a snippet about a cyber security expert.

Figure 1:Google Dorks

Lab 2”Task 1:


Tools: NetCraft and DNSDumpster

The screenshot shows the NetCraft network information for the website naukrigulf.com. The information is organized into a table with two columns: Site and Domain. The Site column contains various network-related details, and the Domain column contains domain-related details.

Site	Domain
Site	https://www.naukrigulf.com
Netblock Owner	Akamai International, BV
Hosting company	Akamai Technologies
Hosting country	NL
IPv4 address	23.39.41.149 (VirusTotal)
IPv4 autonomous systems	AS16625
IPv6 address	2a02:26f0:9b00:49c:0:0:0:23ed
IPv6 autonomous systems	AS20940
Reverse DNS	a23-39-41-149.deploy.static.akamaitechnologies.com
Domain	naukrigulf.com
Nameserver	ns1.infoedgeindia.net
Domain registrar	networksolutions.com
Nameserver organisation	whois.networksolutions.com
Organisation	5335 Gate Parkway care of Network Solutions PO Box 459, Jacksonville, 32256, US
DNS admin	dnsadmin@naukri.com
Top Level Domain	Commercial entities (.com)
DNS Security Extensions	Enabled

IP delegation

Figure 2:NetCraft



A Records (subdomains from dataset)

Host	IP	ASN	ASN Name	Open Services (from DB)	Rev IP
www.naukrigulf.com	104.77.222.99	ASN:16625 104.77.220.0/2 2	AKAMAI-AS United States	http: AkamaiGHost title: Invalid URL https: AkamaiGHost title: Invalid URL cn: .naukri.com o: INFO EDGE (INDIA) LIMITED	1

MX Records

Figure 3:DNSDumpster

Lab 3:Task 1

Tools: Sherlock, Social searcher

```
(kali@kali)-[~]
$ sudo apt install sherlock
[sudo] password for kali:
The following packages were automatically installed and are no longer require
d:
icu-devtools          libxnnpack0
libabsl20230802       linux-image-6.12.13-amd64
libbdnnl3             python3-aioconsole
libflac12t64          python3-dunamai
libfuse3-3            python3-nfsclient
libpython3.12-0       python3-packaging-whl
```

Figure 4:Install Sherlock

```
(kali@kali)-[~]
$ sherlock "Bill gates"
[*] Checking username Bill gates on:

[+] Apple Developer: https://developer.apple.com/forums/profile/Bill%20gates
[+] Apple Discussions: https://discussions.apple.com/profile/Bill%20gates
[+] ArtStation: https://www.artstation.com/Bill%20gates
[+] Codeforces: https://codeforces.com/profile/Bill%20gates
[+] Discogs: https://www.discogs.com/user/Bill%20gates
[+] Discord: https://discord.com
[+] Freelance.habr: https://freelance.habr.com/freelancers/Bill%20gates
[+] Freesound: https://freesound.org/people/Bill%20gates/
[+] GaiaOnline: https://www.gaiaonline.com/profiles/Bill%20gates
[+] Giphy: https://giphy.com/Bill%20gates
[+] Instructables: https://www.instructables.com/member/Bill%20gates
[+] Itemfix: https://www.itemfix.com/c/Bill%20gates
[+] LibraryThing: https://www.librarything.com/profile/Bill%20gates
[+] MyDramaList: https://www.mydramalist.com/profile/Bill%20gates
[+] NationStates Nation: https://nationstates.net/nation=Bill%20gates
[+] NationStates Region: https://nationstates.net/region=Bill%20gates
[+] NitroType: https://www.nitrotype.com/racer/Bill%20gates
[+] PCGamer: https://forums.pcgamer.com/members/?username=Bill%20gates
[+] Patreon: https://www.patreon.com/Bill%20gates
[+] PepperIT: https://www.pepper.it/profile/Bill%20gates/overview
[+] RuneScape: https://apps.runescape.com/runemetrics/app/overview/player/Bi
```

Figure 5:Sherlock

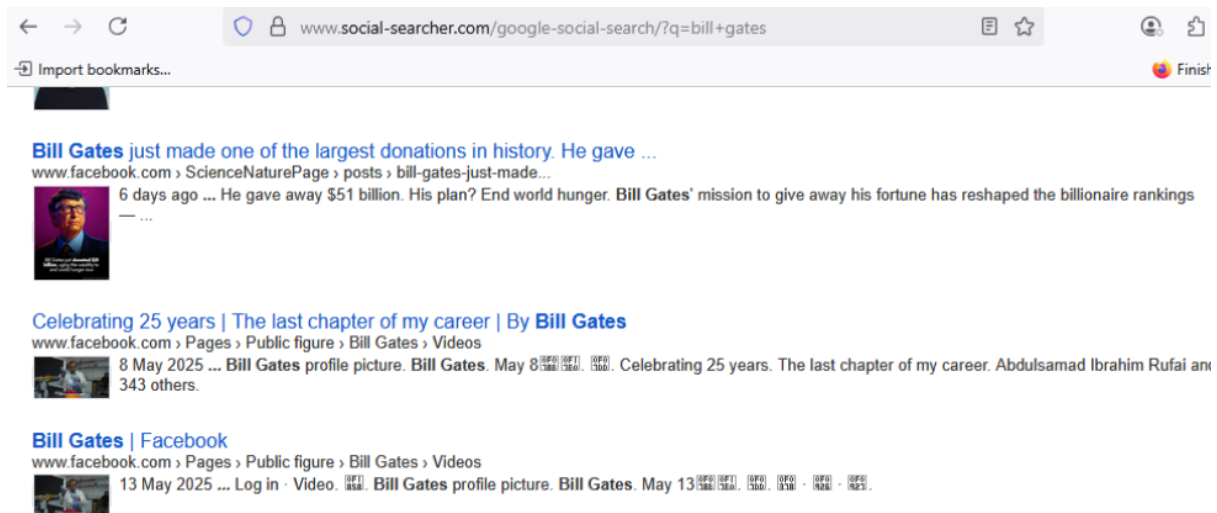


Figure 6: Social-Searcher

Lab 4: Task 1

OS:

Tools: whois.domaintools, Smartwhois, BatchIPConverter

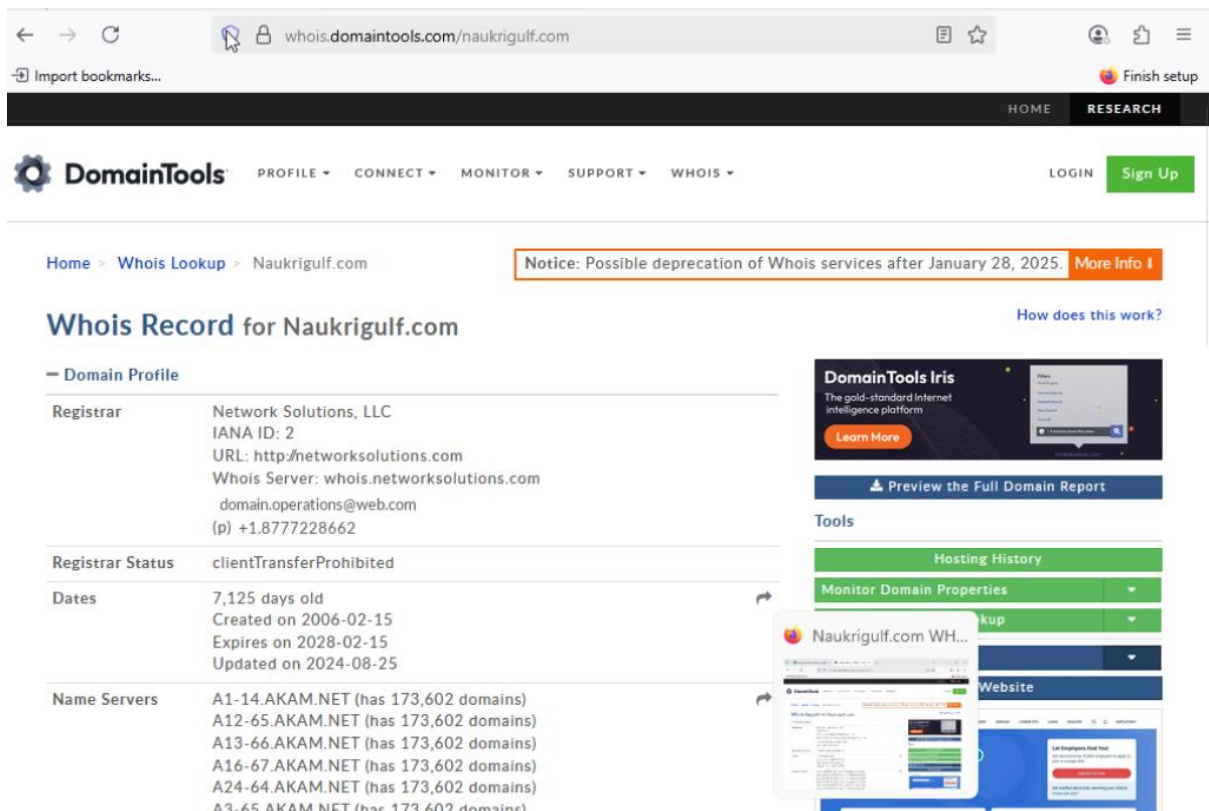


Figure 7: Domaintools

Lab 5: Task 1

Tools: NSLookup

```
C:\Windows\System32>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  192.168.227.2

> set type=a
> www.certifiedhacker.com
Server:  UnKnown
Address:  192.168.227.2

Non-authoritative answer:
Name:    certifiedhacker.com
Address:  162.241.216.11
Aliases:  www.certifiedhacker.com

> set type=cname
> certifiedhacker.com
Server:  UnKnown
Address:  192.168.227.2
```

Figure 8:Nslookup in window 11

```
> set type=cname
> certifiedhacker.com
Server:  UnKnown
Address:  192.168.227.2

DNS request timed out.
    timeout was 2 seconds.
certifiedhacker.com
    primary name server = ns1.bluehost.com
    responsible mail addr = dnsadmin.box5331.bluehost.com
    serial  = 2025081800
    refresh = 86400 (1 day)
    retry   = 7200 (2 hours)
    expire  = 3600000 (41 days 16 hours)
    default TTL = 300 (5 mins)

> set type=a
> ns1.bluehost.com
Server:  UnKnown
Address:  192.168.227.2

Non-authoritative answer:
Name:    ns1.bluehost.com
Address:  162.159.24.80
```

Figure 9:nslookup



Figure 10:Nslookup GUI

Lab 6: Task 1

Tools: Command prompt

```
C:\Users\Window12>tracert /?

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout]
              [-R] [-S srcaddr] [-4] [-6] target_name

Options:
  -d                Do not resolve addresses to hostnames.
  -h maximum_hops   Maximum number of hops to search for target.
  -j host-list       Loose source route along host-list (IPv4-only).
  -w timeout         Wait timeout milliseconds for each reply.
  -R                Trace round-trip path (IPv6-only).
  -S srcaddr         Source address to use (IPv6-only).
  -4                Force using IPv4.
  -6                Force using IPv6.
```

Figure 11:Tracert CMD

```
C:\Users\Window12>tracert www.certifiedhacker.com

Tracing route to certifiedhacker.com [162.241.216.11]
over a maximum of 30 hops:

  1     2 ms    11 ms    <1 ms   192.168.227.2
  2     *        *        *       Request timed out.
  3     *        *        *       Request timed out.
  4     *        *        *       Request timed out.
  5     *        *        *       Request timed out.
  6     *        *        *       Request timed out.
  7     *        *        *       Request timed out.
  8     *        *        *       Request timed out.
  9     *        *        *       Request timed out.
 10     *        *        *       Request timed out.
 11     *        *        *       Request timed out.
 12     *        *        *       Request timed out.
 13     *        *        *       Request timed out.
 14   340 ms   305 ms   304 ms   box5331.bluehost.com [162.241.216.11]

Trace complete.
```

Figure 12: Tracert in Windows

```
(kali@kali)-[~]
$ traceroute www.certifiedhacker.com
traceroute to www.certifiedhacker.com (162.241.216.11), 30 hops max, 60 byte
packets
 1  192.168.227.2 (192.168.227.2)  2.321 ms  2.092 ms  2.053 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
```

Figure 13:traceroute in Linux

ICMP Traceroute:

The default and most common type of traceroute, using Internet Control Message Protocol (ICMP) echo request packets with incrementally increasing Time-To-Live (TTL) values to identify the path and round-trip times to each hop.

traceroute (Linux/macOS): The command-line utility for ICMP traceroute on Unix-like systems.

tracert (Windows): The Windows equivalent of traceroute, achieving the same goal using ICMP.

TCP traceroute: tcptraceroute www.certifiedhacker.com

Lab 7: Task 1

Tool:eMailTracker Pro

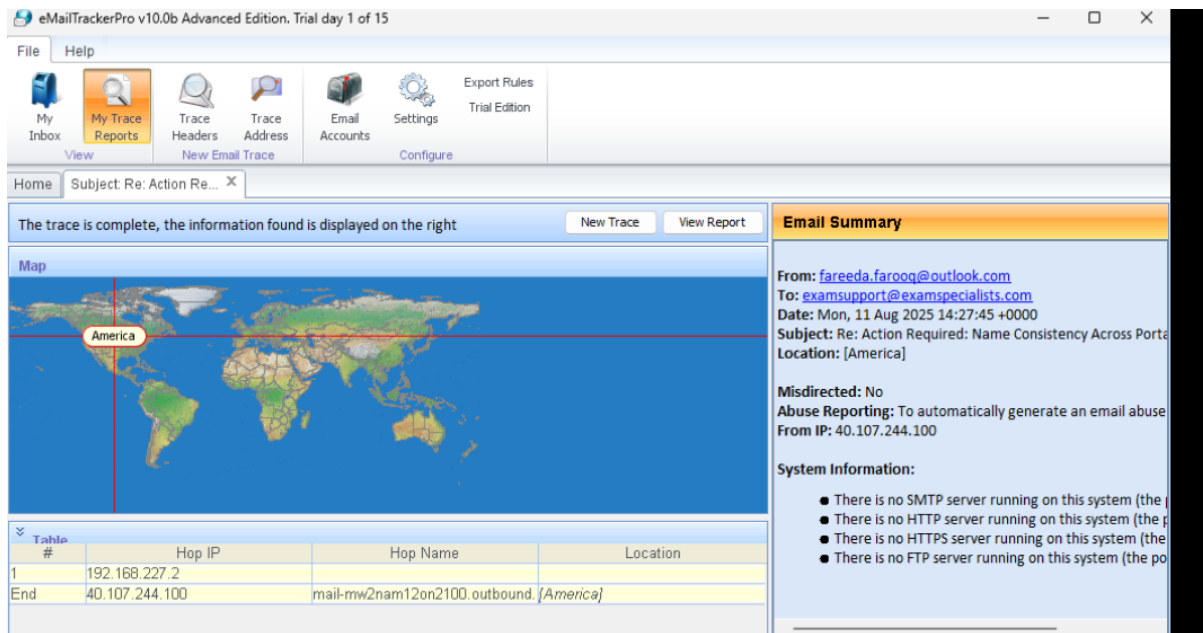


Figure 14: EmailTracker Pro

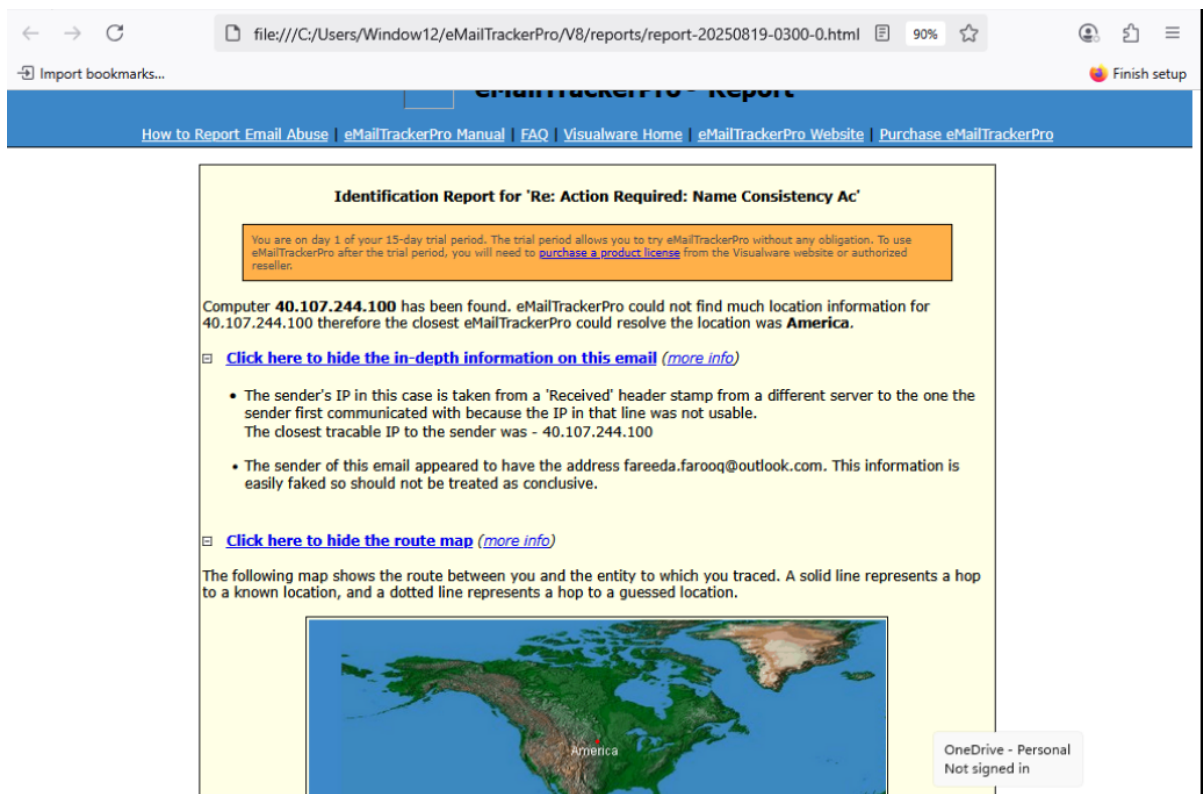


Figure 15: Report from Emailtracker pro

Lab 8: Task 1

Tools: recon-ng

```
[!] Invalid command: workspace create CEHV13.
[recon-ng][default] > workspaces list

+-----+-----+
| Workspaces | Modified |
+-----+-----+
| daraz      | 2025-07-23 09:00:47 |
| default    | 2025-07-11 08:39:33 |
+-----+-----+

[recon-ng][default] > db insert domains
domain (TEXT): daraz.com
notes (TEXT):
[*] 1 rows affected.
[recon-ng][default] > 
```

Figure 16: Recon-ng workspace

```
[*] 1 rows returned
[recon-ng][default] > modules load brute
[*] Multiple modules match 'brute'.

Exploitation
-----
exploitation/injection/xpath_bruter

Recon
-----
recon/domains-domains/brute_suffix
recon/domains-hosts/brute_hosts

[recon-ng][default] > modules load recon/domains-hosts/brute_hosts
[recon-ng][default][brute_hosts] > run

DARAZ.COM
-----
[*] No Wildcard DNS entry found.
[*] 1.daraz.com => No record found.
[*] 0.daraz.com => No record found.
[*] 10.daraz.com => No record found.
[*] 13.daraz.com => No record found.
[*] 14.daraz.com => No record found.
```

Figure 17: Brute Module run

```
recon-ng[default][html] > options set FILENAME /home/kali/Desktop/Rresult1.
html
FILENAME => /home/kali/Desktop/Rresult1.html
recon-ng[default][html] > options set CREATOR Fareeda
CREATOR => Fareeda
recon-ng[default][html] > options set CUSTOMER DARAZ
CUSTOMER => DARAZ
recon-ng[default][html] > run
[*] Report generated at '/home/kali/Desktop/Rresult1.html'.
recon-ng[default][html] > 
```

Figure 18: Creating html base report of all modules.

DARAZ

www.recon-ng.com

Recon-ng Reconnaissance Report

[-] Summary

table	count
domains	1
companies	0
netblocks	0
locations	0
vulnerabilities	0
ports	0
hosts	37
contacts	0
credentials	0
leaks	0
pushpins	0
profiles	0
repositories	0

[+] Domains

[+] Hosts

Created by: Fareeda
Tue, Aug 19 2025 07:25:32

Figure 19: Recon-ng Report Module

Lab 9: Task 1

Tool: sgpt

```
(kali@kali)-[~]  
$ sgpt --chat footprint --shell "use theHarvester to gather information about payment details link with daraz.pk, limiting search to 50, use baidu as data resource"  
zsh -c "theHarvester -d daraz.pk -l 50 -r baidu --banner off | grep 'Payment Details' -A 3"
```

Figure 20: sGPT usage