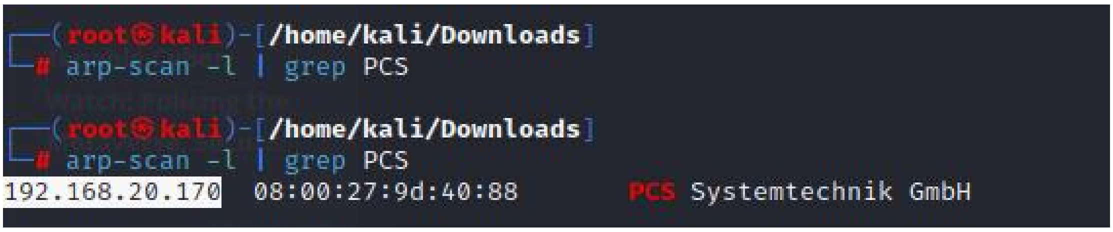
Cyber Security Exam Module 2,4 (ID : 30005)

Answer to the Question Number 4:

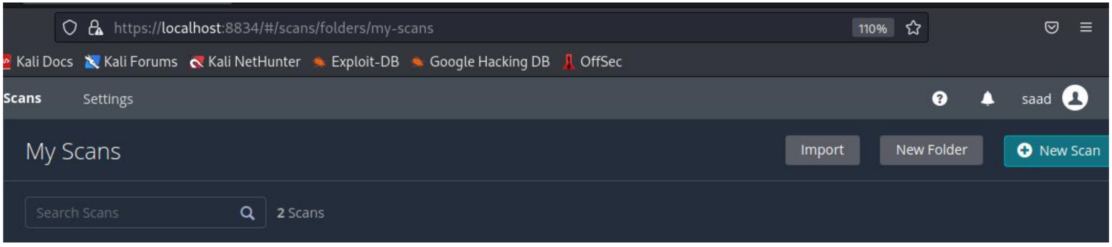
(A)
The steps to install nessus given below
1. First download deb package from web
2. Install nessus with this command : dpkg -I Nessus-10.1.1-debian6_amd64.deb -t
3. Then the command : systemctl enable nessusd ; to enable the nessus service
4. Then command: systemctl start nessusd
5. Then sign up to nessus https://localhost:8834/ from this link.
6. Then login with valid credential

(B)
To scan the PCS Systemtecnik GmbH we need to scan and find the ip address

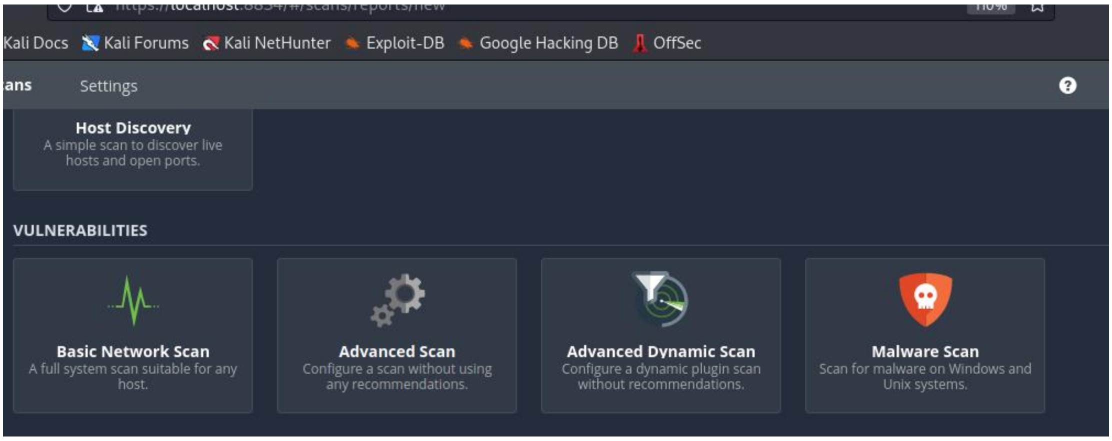


```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# arp-scan -l | grep PCS

┌──(root㉿kali)-[/home/kali/Downloads]
└─# arp-scan -l | grep PCS
192.168.20.170  08:00:27:9d:40:88       PCS Systemtechnik GmbH
```

Then we need to collect the ip scan and login to nessus.
Then we have to click the “NEW SCAN” button in the top right corner

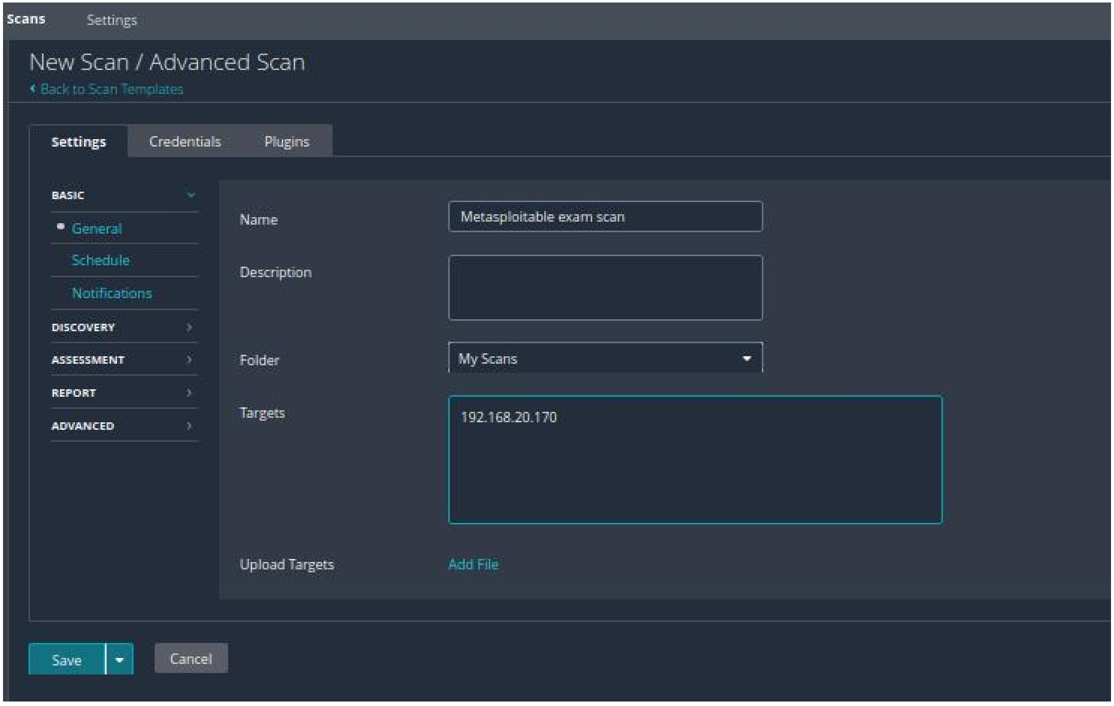


Then we will click the “Advance Scan”



https://localhost:8834/#/scans/reports/new
110%
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
ans
Settings
Host Discovery
A simple scan to discover live hosts and open ports.
VULNERABILITIES
Basic Network Scan
A full system scan suitable for any host.
Advanced Scan
Configure a scan without using any recommendations.
Advanced Dynamic Scan
Configure a dynamic plugin scan without recommendations.
Malware Scan
Scan for malware on Windows and Unix systems.

Then we will give the scan a name and put the ip addfress. Then we shall click save.



New Scan / Advanced Scan

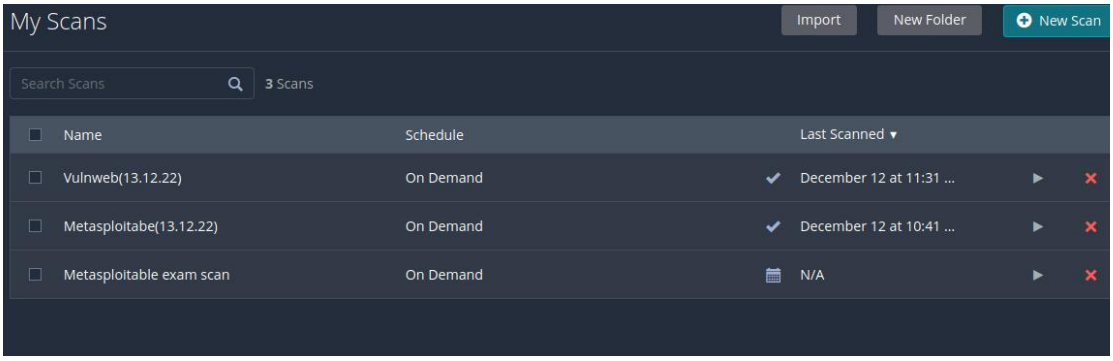
Name: Metasploitable exam scan

Description:

Folder: My Scans

Targets: 192.168.20.170

Then from my scan page we shall click the launch button and launch the particular scan.

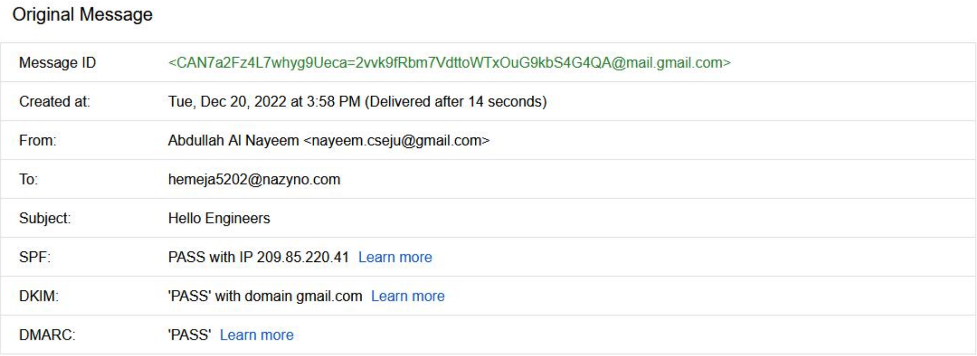


Name	Schedule		Last Scanned ▾		
Vulnweb(13.12.22)	On Demand	✓	December 12 at 11:31 ...	▶	✕
Metasploitabe(13.12.22)	On Demand	✓	December 12 at 10:41 ...	▶	✕
Metasploitable exam scan	On Demand	📅	N/A	▶	✕

(C) The pdf is attached with the answer script.

Answer to the question number 3:

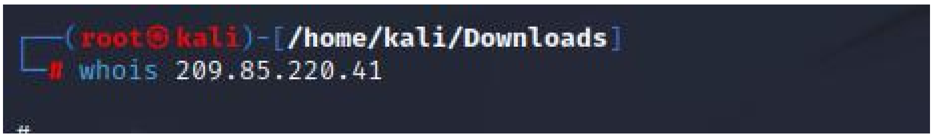
From the email header we get the ip address: 209. 85. 220. 41



Original Message

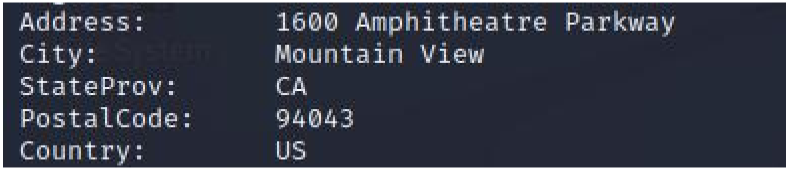
Message ID	<CAN7a2Fz4L7whyg9Ueca=2vvk9fRbm7VdttoWTxOuG9kbS4G4QA@mail.gmail.com>
Created at:	Tue, Dec 20, 2022 at 3:58 PM (Delivered after 14 seconds)
From:	Abdullah Al Nayeem <nayeem.cseju@gmail.com>
To:	hemeja5202@nazyno.com
Subject:	Hello Engineers
SPF:	PASS with IP 209.85.220.41 Learn more
DKIM:	'PASS' with domain gmail.com Learn more
DMARC:	'PASS' Learn more

We will do whois scan to find the location of the email



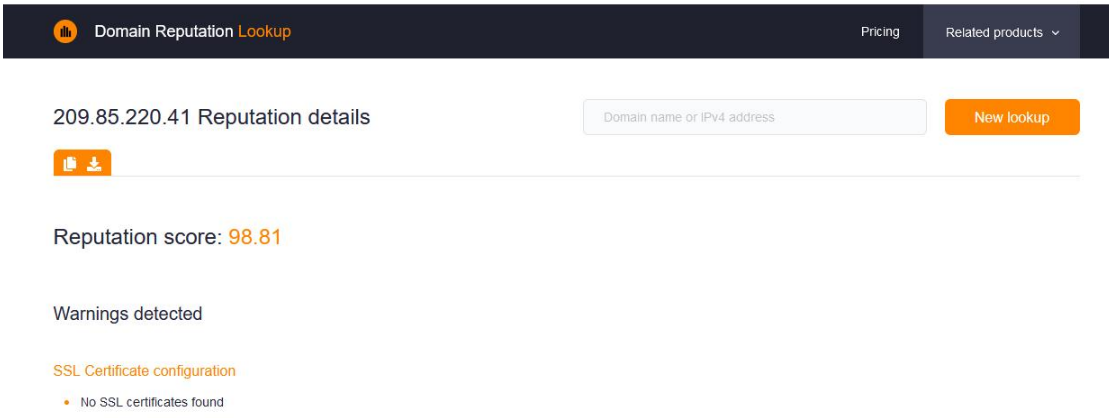
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# whois 209.85.220.41
```

From the command we get the following location information:



```
Address:        1600 Amphitheatre Parkway
City:           Mountain View
StateProv:      CA
PostalCode:     94043
Country:        US
```

The reputation and lookup of the ip



209.85.220.41 Reputation details

Reputation score: 98.81

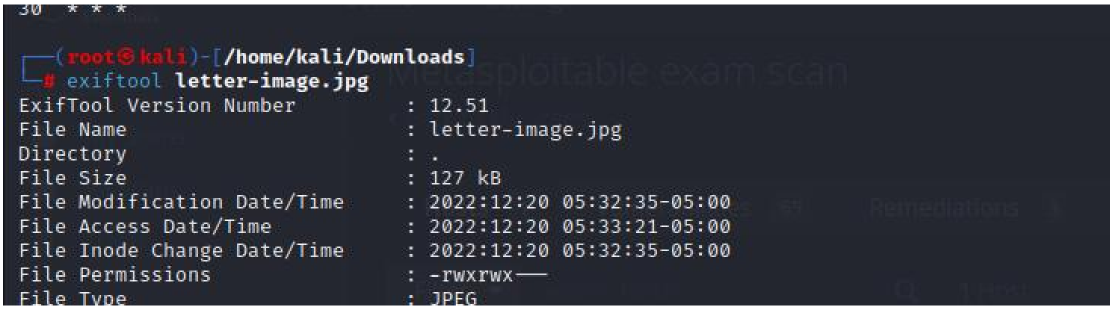
Warnings detected

SSL Certificate configuration

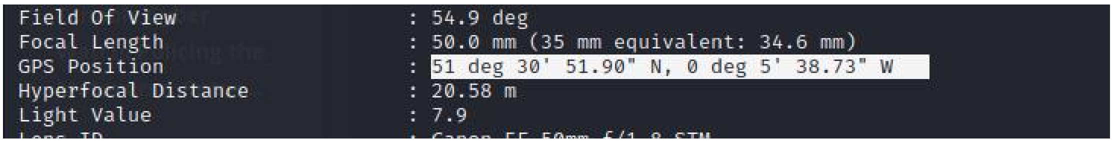
- No SSL certificates found

and

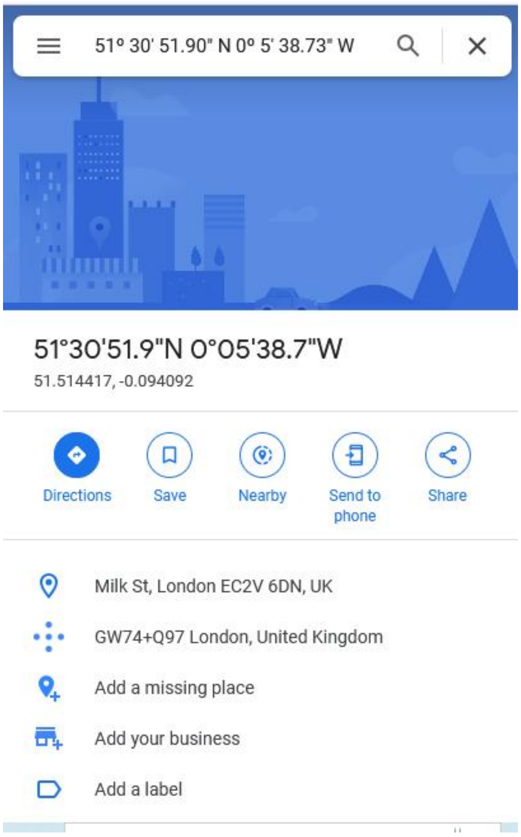
(B) Using command : exiftool letter-image.jpg ; we can get the location of the image taken.



```
30  * * *

┌──(root㉿kali)-[/home/kali/Downloads]
└─# exiftool letter-image.jpg
ExifTool Version Number         : 12.51
File Name                       : letter-image.jpg
Directory                       : .
File Size                       : 127 kB
File Modification Date/Time     : 2022:12:20 05:32:35-05:00
File Access Date/Time           : 2022:12:20 05:33:21-05:00
File Inode Change Date/Time     : 2022:12:20 05:32:35-05:00
File Permissions                : -rwxrwx---
File Type                       : JPEG
```



```
Field Of View                   : 54.9 deg
Focal Length                    : 50.0 mm (35 mm equivalent: 34.6 mm)
GPS Position                    : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
Hyperfocal Distance             : 20.58 m
Light Value                     : 7.9
Lens ID                         : Canon EF 50mm f/1.8 STM
```



51º 30' 51.90" N 0º 5' 38.73" W

51°30'51.9"N 0°05'38.7"W

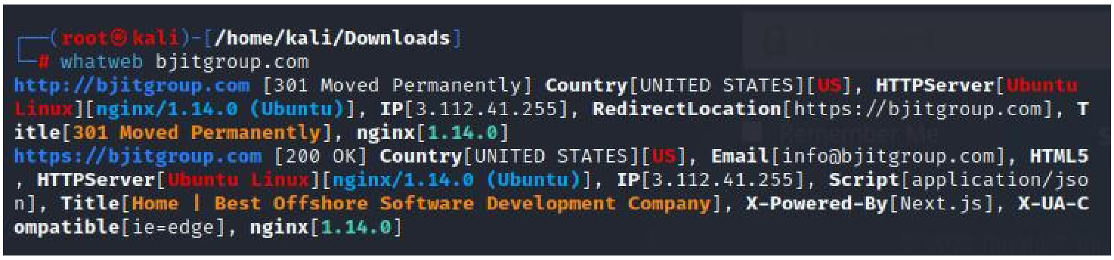
51.514417, -0.094092

Milk St, London EC2V 6DN, UK

GW74+Q97 London, United Kingdom

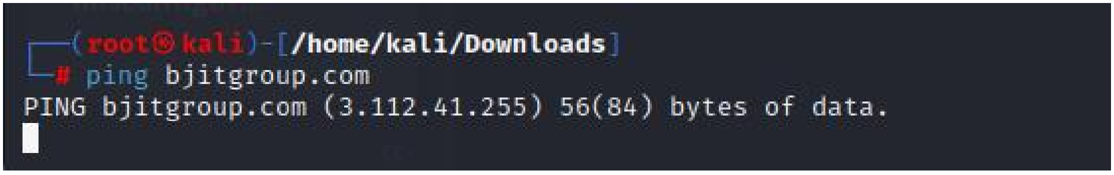
Answer to the question number : 1

i. The initial information:



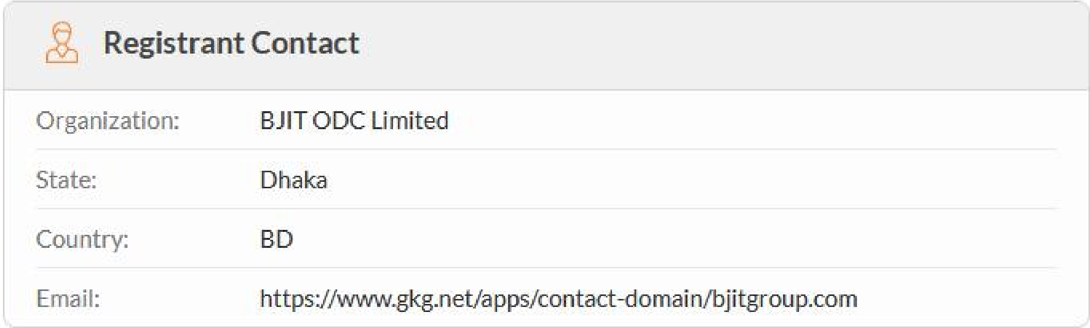
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# whatweb bjitgroup.com
http://bjitgroup.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[Ubuntu
Linux][nginx/1.14.0 (Ubuntu)], IP[3.112.41.255], RedirectLocation[https://bjitgroup.com], T
itle[301 Moved Permanently], nginx[1.14.0]
https://bjitgroup.com [200 OK] Country[UNITED STATES][US], Email[info@bjitgroup.com], HTML5
, HTTPServer[Ubuntu Linux][nginx/1.14.0 (Ubuntu)], IP[3.112.41.255], Script[application/jso
n], Title[Home | Best Offshore Software Development Company], X-Powered-By[Next.js], X-UA-C
ompatible[ie=edge], nginx[1.14.0]
```

ii) IP Address



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ping bjitgroup.com
PING bjitgroup.com (3.112.41.255) 56(84) bytes of data.
```

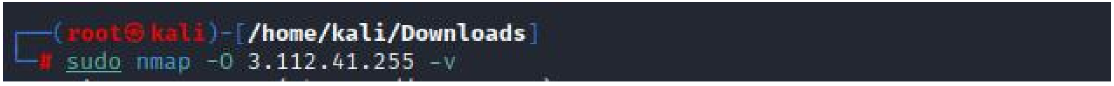
Location



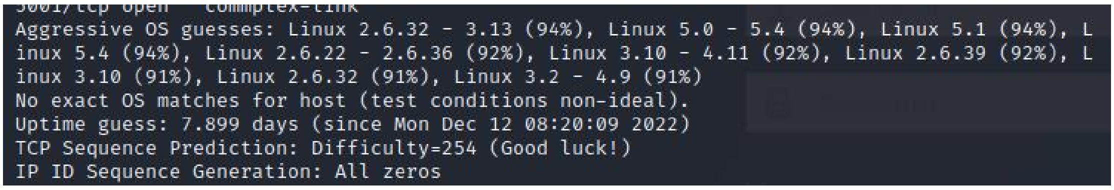
Registrant Contact

Organization:	BJIT ODC Limited
State:	Dhaka
Country:	BD
Email:	https://www.gkg.net/apps/contact-domain/bjitgroup.com

iv) to find the OS information the following command is used:

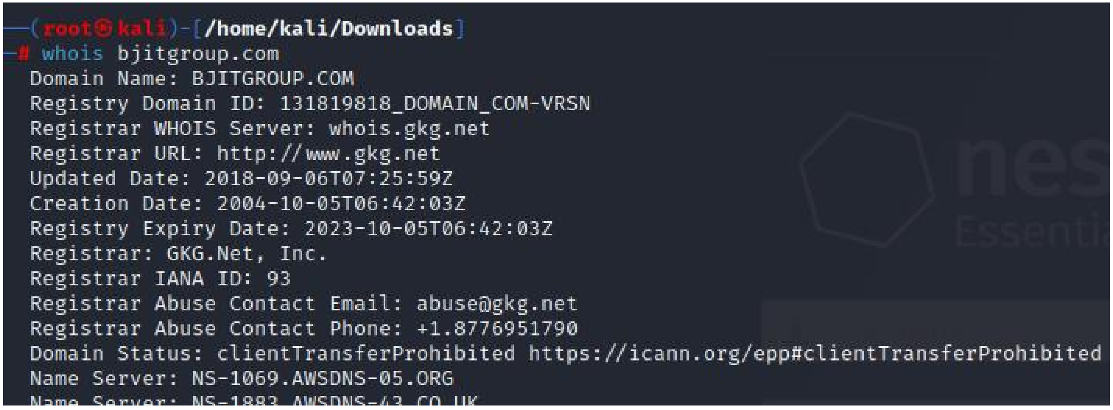


```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# sudo nmap -O 3.112.41.255 -v
```



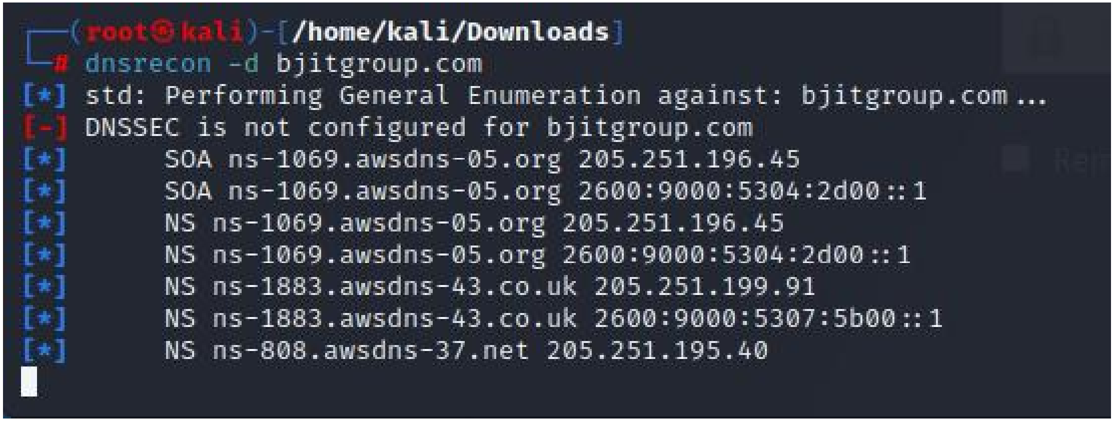
```
3001/tcp open   commplex-link
Aggressive OS guesses: Linux 2.6.32 - 3.13 (94%), Linux 5.0 - 5.4 (94%), Linux 5.1 (94%), L
inux 5.4 (94%), Linux 2.6.22 - 2.6.36 (92%), Linux 3.10 - 4.11 (92%), Linux 2.6.39 (92%), L
inux 3.10 (91%), Linux 2.6.32 (91%), Linux 3.2 - 4.9 (91%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 7.899 days (since Mon Dec 12 08:20:09 2022)
TCP Sequence Prediction: Difficulty=254 (Good luck!)
IP ID Sequence Generation: All zeros
```

V) to find the whois information we run the following command.



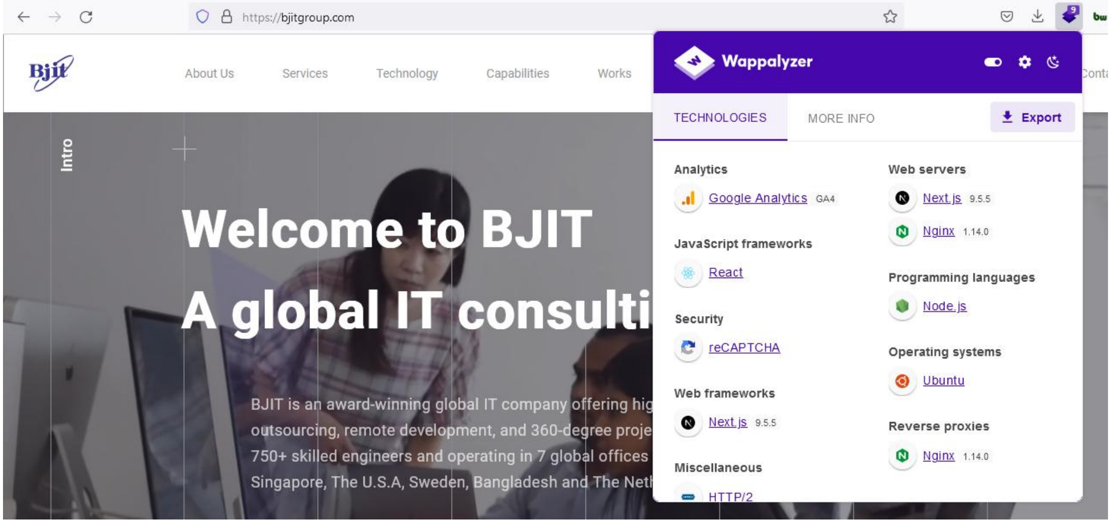
```
──(root㉿kali)-[/home/kali/Downloads]
─# whois bjitgroup.com
  Domain Name: BJITGROUP.COM
  Registry Domain ID: 131819818_DOMAIN_COM-VRSN
  Registrar WHOIS Server: whois.gkg.net
  Registrar URL: http://www.gkg.net
  Updated Date: 2018-09-06T07:25:59Z
  Creation Date: 2004-10-05T06:42:03Z
  Registry Expiry Date: 2023-10-05T06:42:03Z
  Registrar: GKG.Net, Inc.
  Registrar IANA ID: 93
  Registrar Abuse Contact Email: abuse@gkg.net
  Registrar Abuse Contact Phone: +1.8776951790
  Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
  Name Server: NS-1069.AWSDNS-05.ORG
  Name Server: NS-1883.AWSDNS-43.CO.UK
```

Vi) DNS information the following command is used



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# dnsrecon -d bjitgroup.com
[*] std: Performing General Enumeration against: bjitgroup.com...
[-] DNSSEC is not configured for bjitgroup.com
[*]      SOA ns-1069.awsdns-05.org 205.251.196.45
[*]      SOA ns-1069.awsdns-05.org 2600:9000:5304:2d00::1
[*]      NS ns-1069.awsdns-05.org 205.251.196.45
[*]      NS ns-1069.awsdns-05.org 2600:9000:5304:2d00::1
[*]      NS ns-1883.awsdns-43.co.uk 205.251.199.91
[*]      NS ns-1883.awsdns-43.co.uk 2600:9000:5307:5b00::1
[*]      NS ns-808.awsdns-37.net 205.251.195.40
```

Vii) Technologies used in bjitgroup.com



https://bjitgroup.com
Bjit
About Us
Services
Technology
Capabilities
Works
Conta
Intro
Welcome to BJIT
A global IT consulti
BJIT is an award-winning global IT company offering hig
outsourcing, remote development, and 360-degree proje
750+ skilled engineers and operating in 7 global offices
Singapore, The U.S.A, Sweden, Bangladesh and The Neth
Wappalyzer
TECHNOLOGIES
MORE INFO
Export

Analytics
Google Analytics GA4

JavaScript frameworks
React

Security
reCAPTCHA

Web frameworks
Next.js 9.5.5

Miscellaneous
HTTP/2

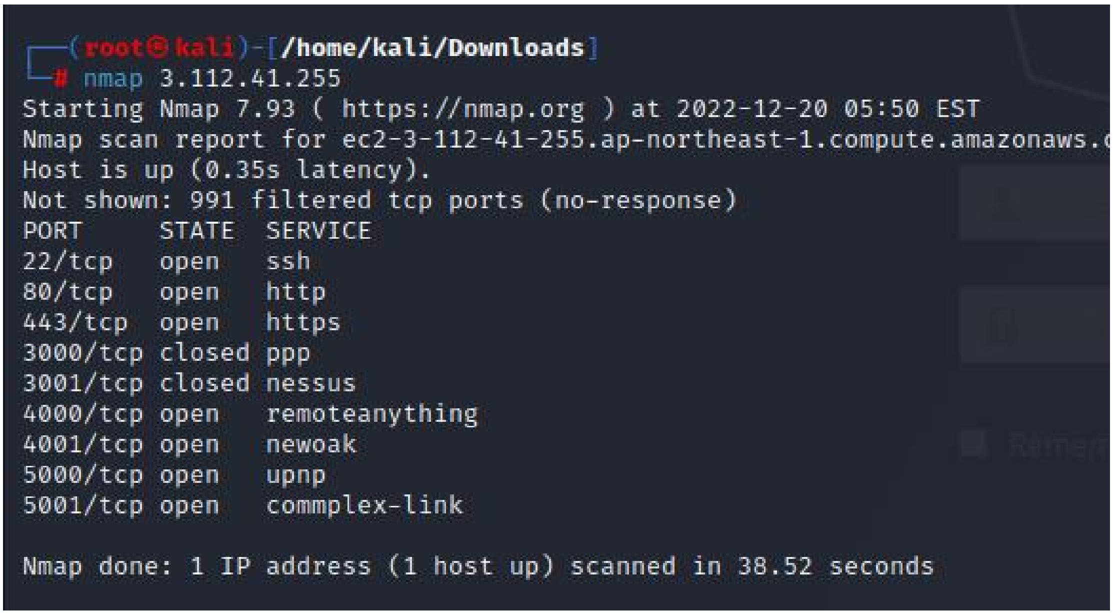
Web servers
Next.js 9.5.5
Nginx 1.14.0

Programming languages
Node.js

Operating systems
Ubuntu

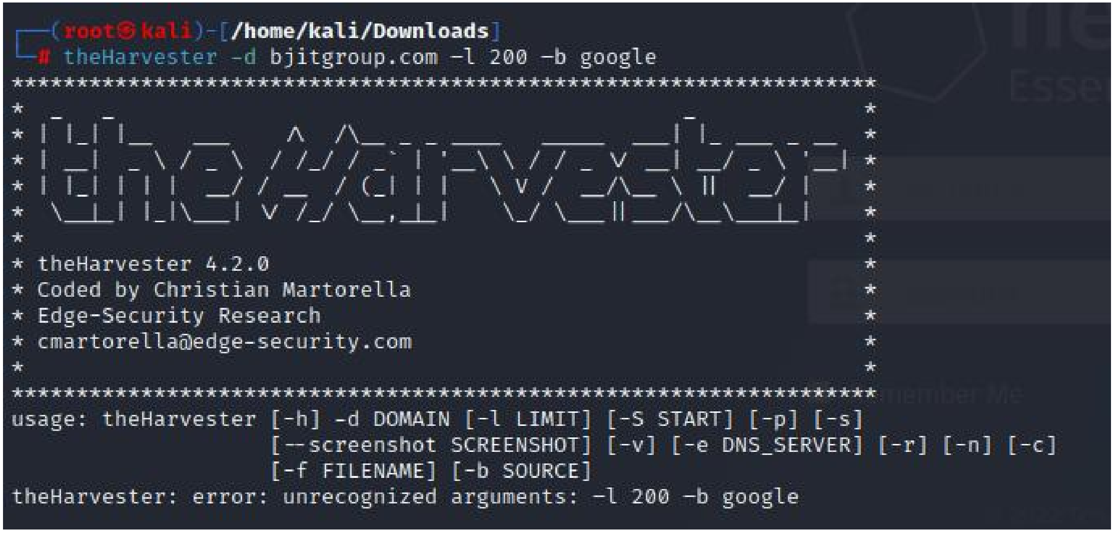
Reverse proxies
Nginx 1.14.0

Viii) to discover open ports we use : **nmap 3.112.41.255**



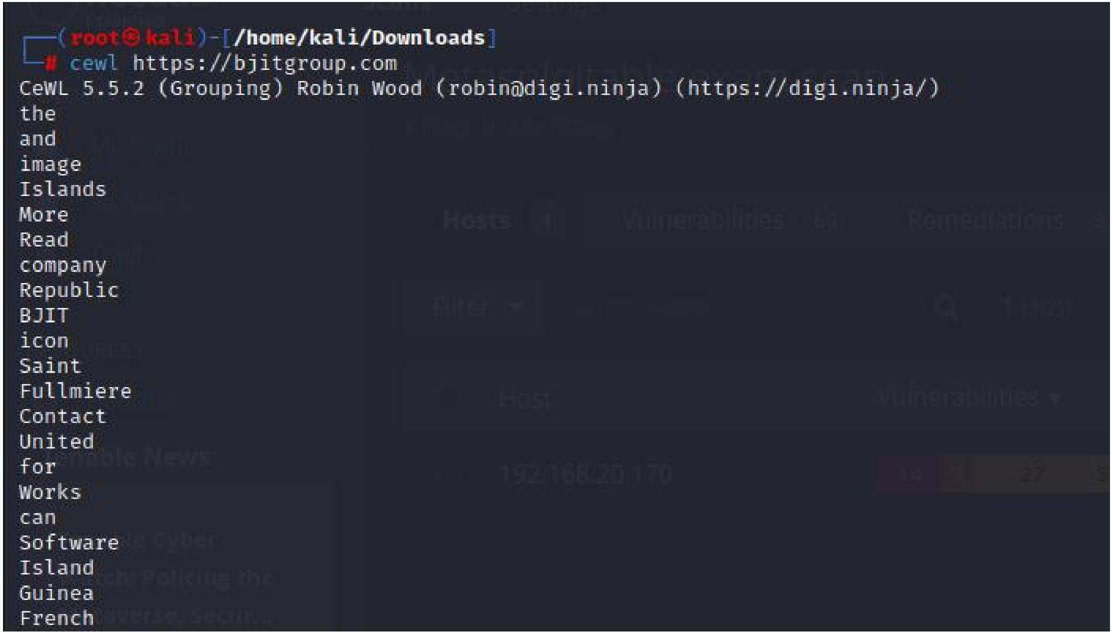
```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# nmap 3.112.41.255
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-20 05:50 EST
Nmap scan report for ec2-3-112-41-255.ap-northeast-1.compute.amazonaws.c
Host is up (0.35s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
443/tcp  open   https
3000/tcp closed ppp
3001/tcp closed nessus
4000/tcp open   remoteanything
4001/tcp open   newoak
5000/tcp open   upnp
5001/tcp open   commplex-link

Nmap done: 1 IP address (1 host up) scanned in 38.52 seconds
```

IX) to do the email address enumeration and people enumeration we use the following command.



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# theHarvester -d bjitgroup.com -l 200 -b google
*******************************************************************
*  _   _                                            _             *
* | |_| |__   ___    /\  /\__ _ _ ____   _____  ___| |_ ___ _ __  *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ \/ __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| \/ /_/ \__,_|_|    \_/ \___||___/\__\___|_|    *
*                                                                 *
* theHarvester 4.2.0                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************
usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-p] [-s]
                    [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-r] [-n] [-c]
                    [-f FILENAME] [-b SOURCE]
theHarvester: error: unrecognized arguments: -l 200 -b google
```

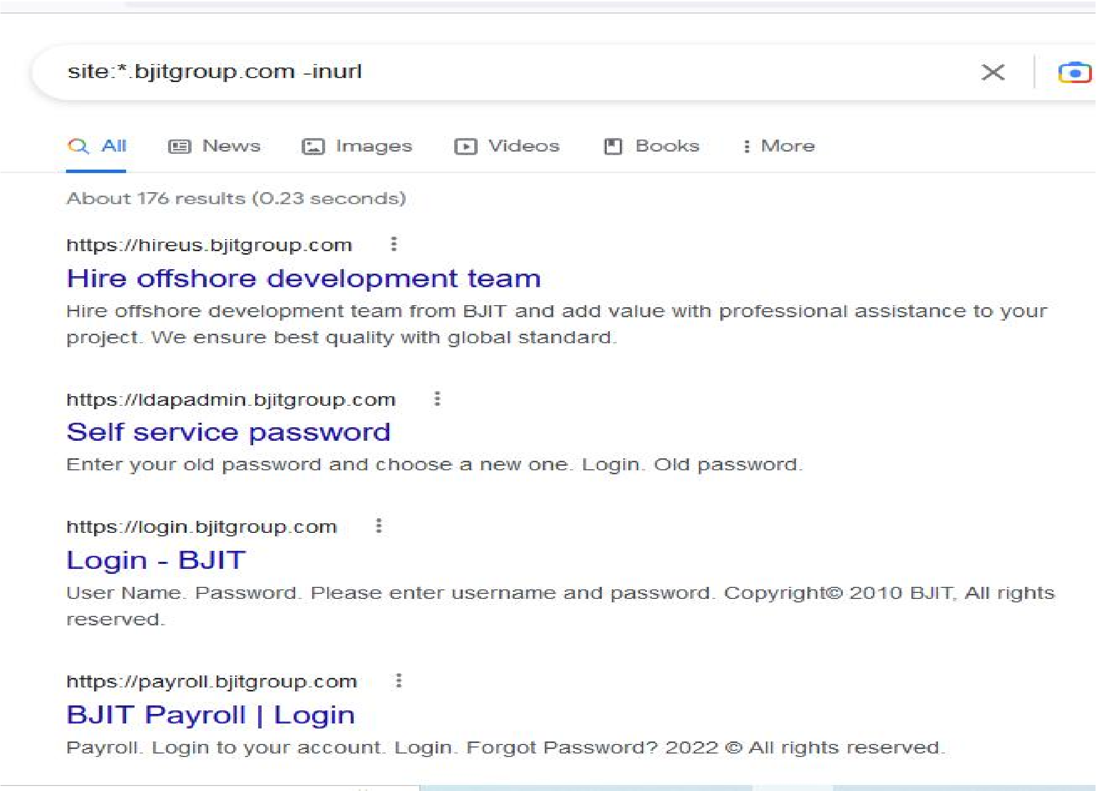
xi) to gather wordlists the following command is to be used



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# cewl https://bjitgroup.com
CeWL 5.5.2 (Grouping) Robin Wood (robin@digi.ninja) (https://digi.ninja/)
the
and
image
Islands
More
Read
company
Republic
BJIT
icon
Saint
Fullmiere
Contact
United
for
Works
can
Software
Island
Guinea
French
```

Answer to the question number 2:

(A) To find the subdomain using google dorkings we use : site:*.bjitgroup.com -inurl



About 176 results (0.23 seconds)

https://hireus.bjitgroup.com

Hire offshore development team

Hire offshore development team from BJIT and add value with professional assistance to your project. We ensure best quality with global standard.

https://ldapadmin.bjitgroup.com

Self service password

Enter your old password and choose a new one. Login. Old password.

https://login.bjitgroup.com

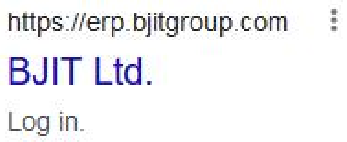
Login - BJIT

User Name. Password. Please enter username and password. Copyright© 2010 BJIT, All rights reserved.

https://payroll.bjitgroup.com

BJIT Payroll | Login

Payroll. Login to your account. Login. Forgot Password? 2022 © All rights reserved.



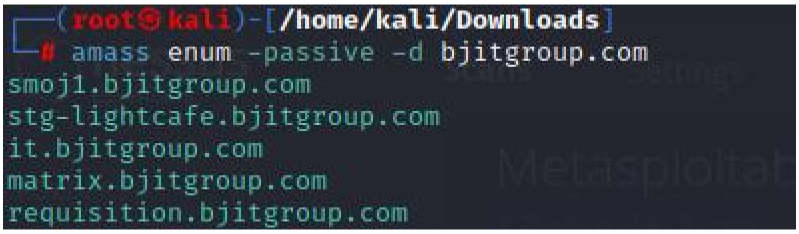
https://erp.bjitgroup.com

BJIT Ltd.

Log in.

To find the subdomain using CLI automated tool we use the following command :

amass enum -passive -d bjitgroup.com



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# amass enum -passive -d bjitgroup.com
smoj1.bjitgroup.com
stg-lightcafe.bjitgroup.com
it.bjitgroup.com
matrix.bjitgroup.com
requisition.bjitgroup.com
```