NAME: Chavan Mukul Manish

REG.NO: 20BIT0238

SUBJECT: CSE3502

FACULTY : SUMAYA THASEEN

DIGITAL – ASSIGNMENT 4

1. Perform a credential harvesting using setoolkit by cloning any web template like google/facebook using your Kali IP. (4 marks)

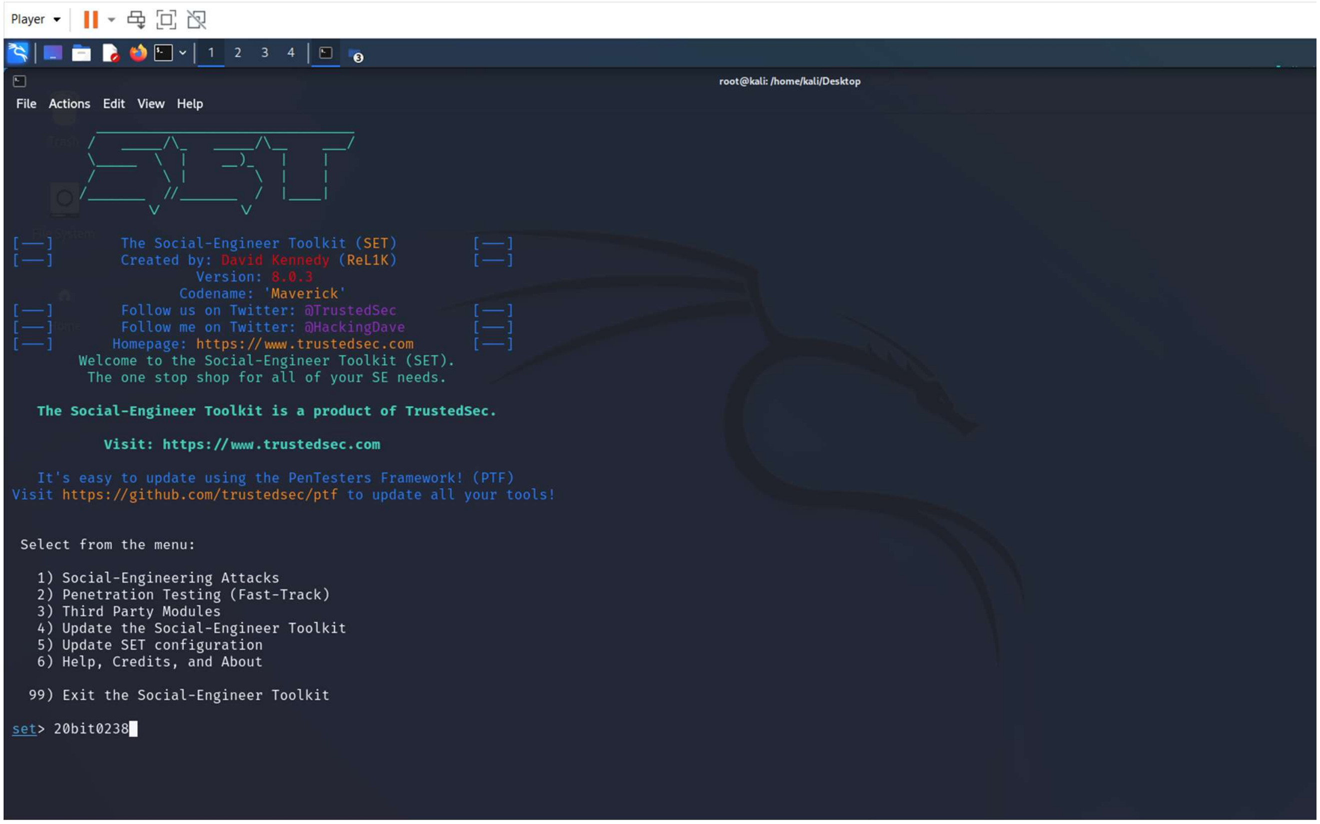
Give the snapshot of the following

▯ Kali IP in the browser

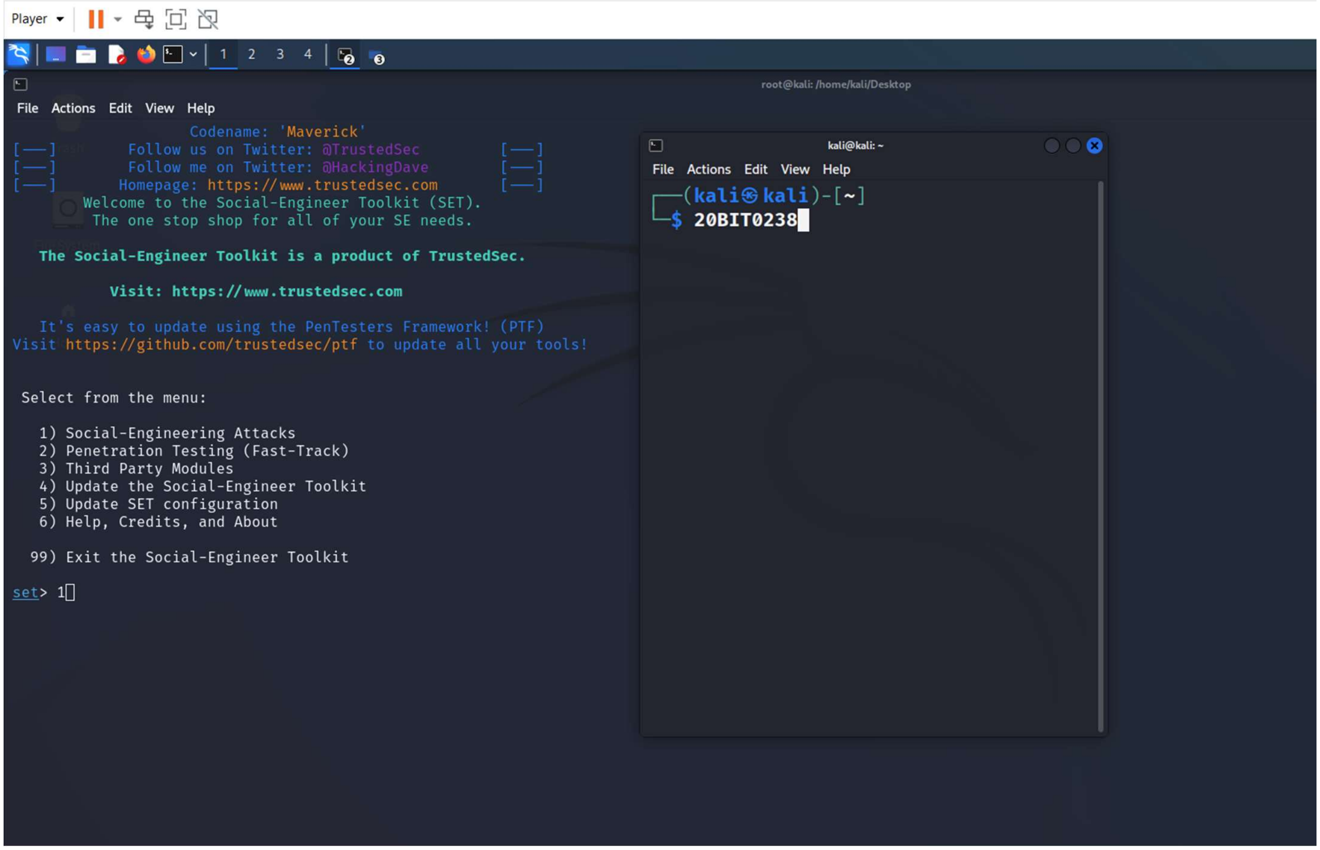
▯ Sniff the username as your registration number and password as your full name in the Kali Console

▯ Save the results in a .txt file and also in a google drive link

Command : setoolkit

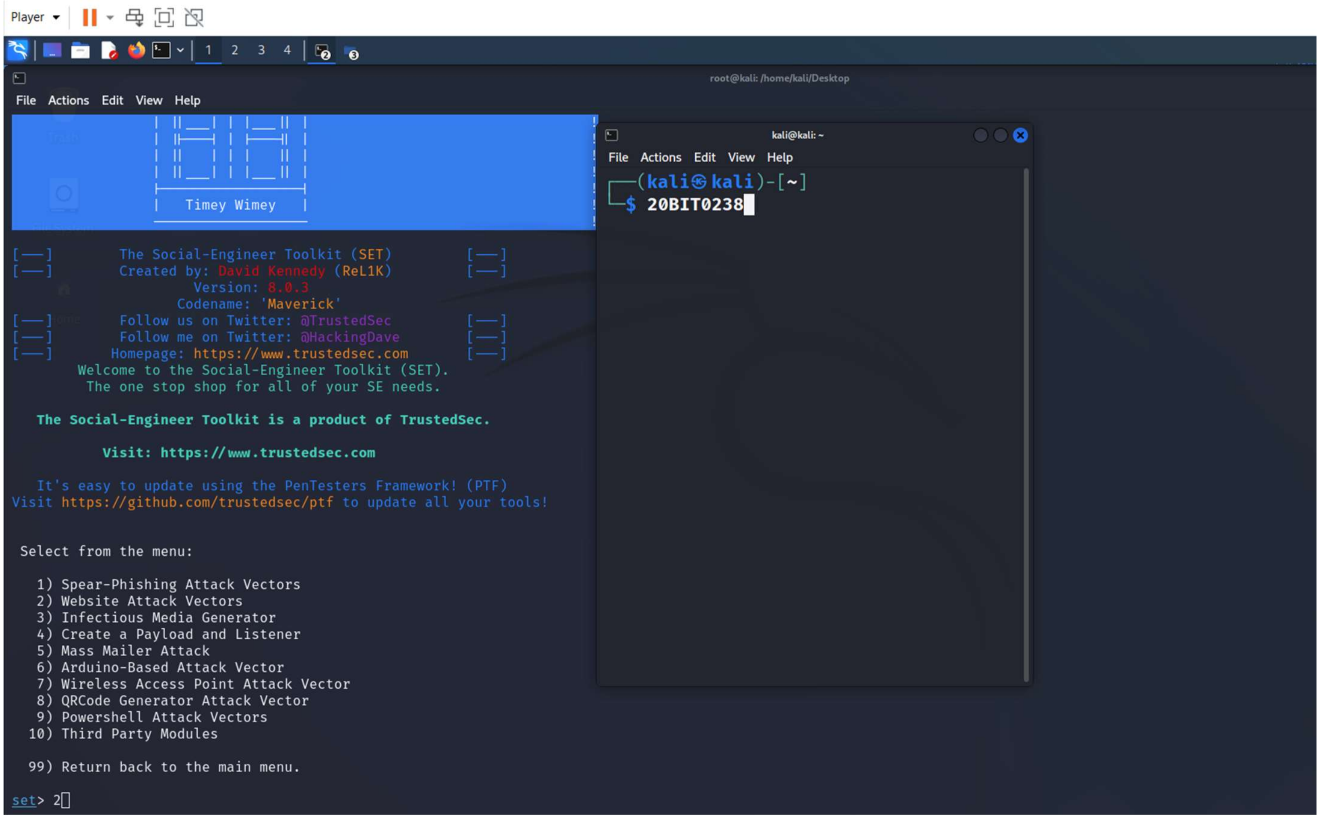


```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 20bit0238
```



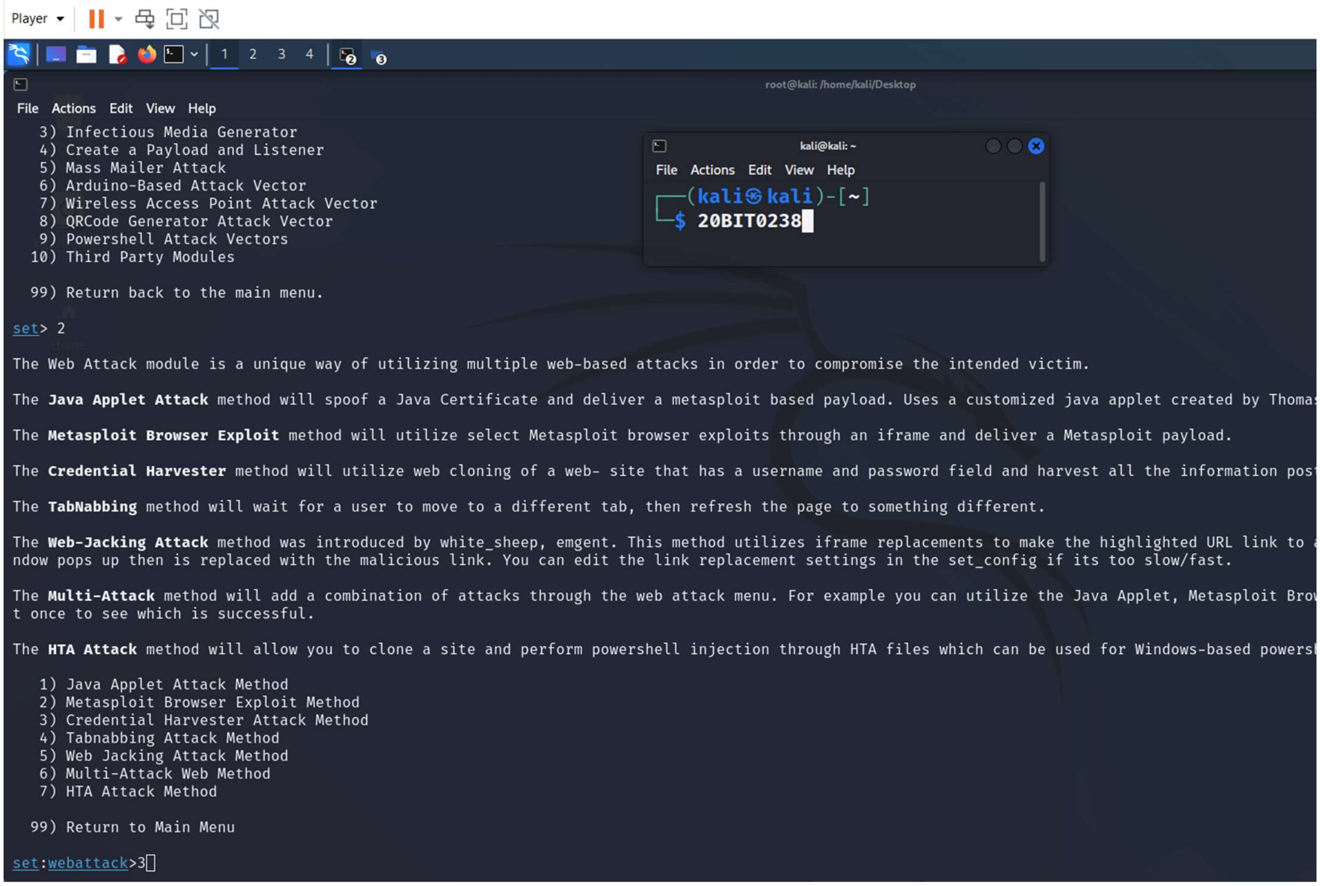
```
                   Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```



```
                |  ||___|  |  |___||  |
                |  ||---|  |  |---||  |
                |  ||   |  |  |   ||  |
                |  ||___|  |  |___||  |
                |-------------------- |
                |     Timey Wimey     |
                 ---------------------

[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                   Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
        Welcome to the Social-Engineer Toolkit (SET).
         The one stop shop for all of your SE needs.

   The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2
```

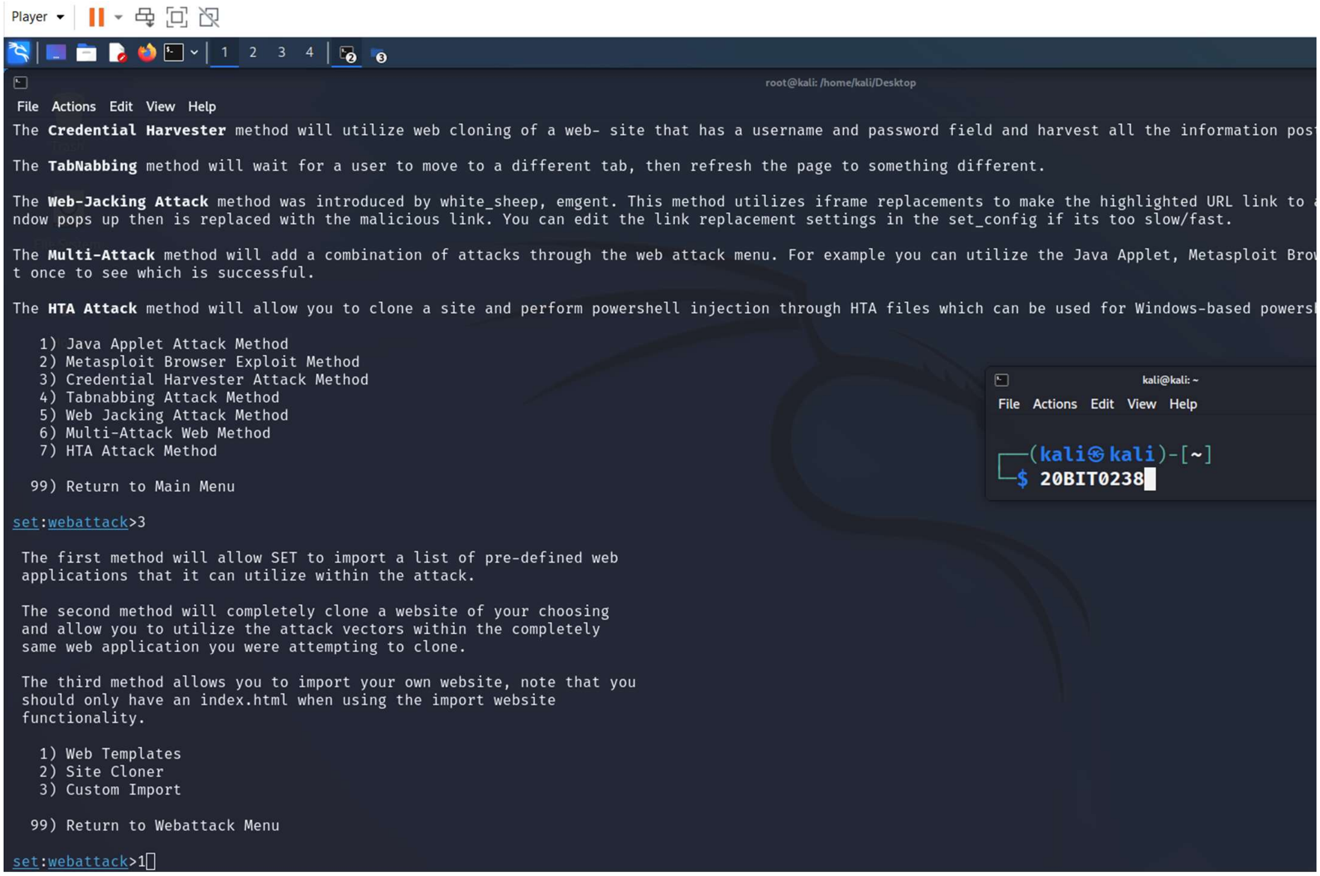
```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```



Player
1
2
3
4
root@kali: /home/kali/Desktop
File Actions Edit View Help
kali@kali: ~
File Actions Edit View Help

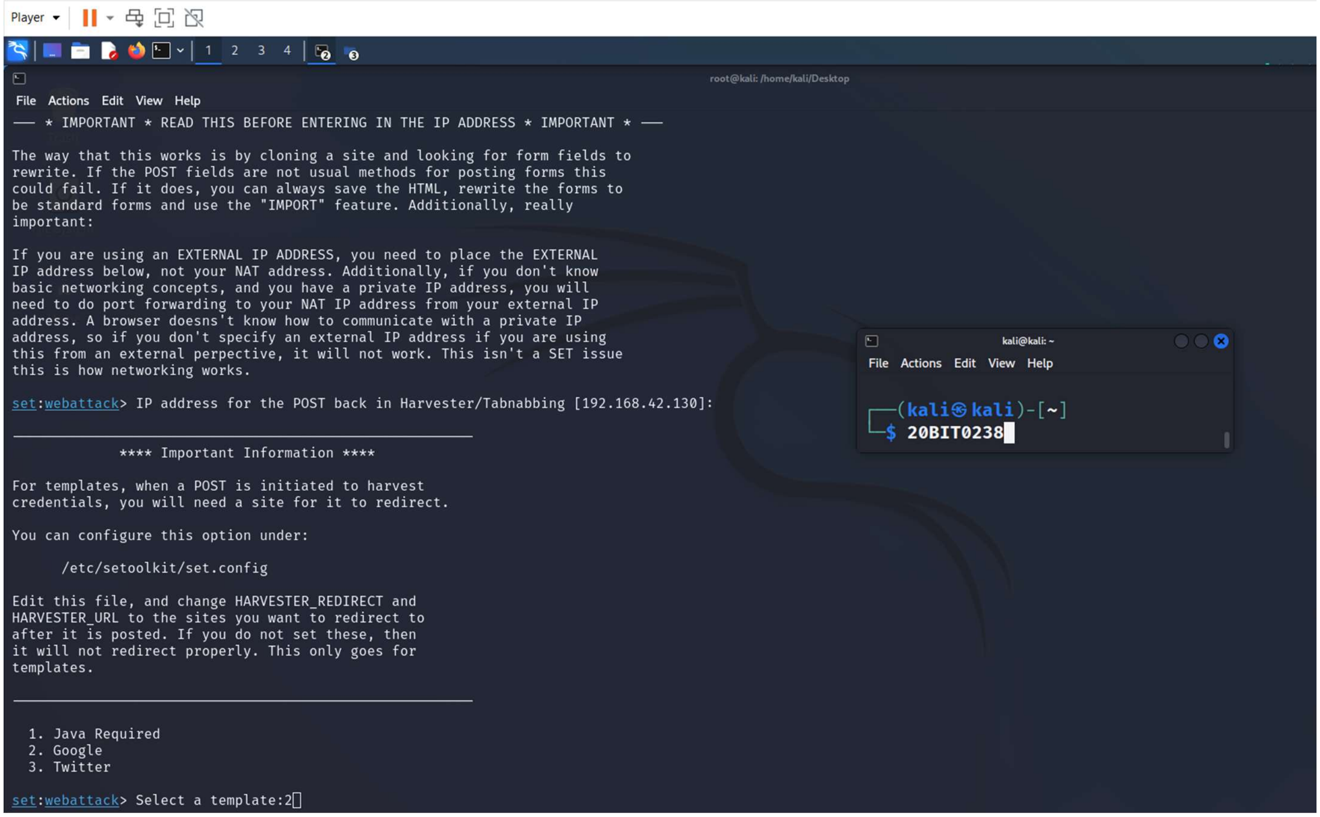
```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```

```
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 2

The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The Java Applet Attack method will spoof a Java Certificate and deliver a metasploit based payload. Uses a customized java applet created by Thomas

The Metasploit Browser Exploit method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information post

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to a
ndow pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Brow
t once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powersh

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```


Player
1 2 3 4
root@kali: /home/kali/Desktop
File Actions Edit View Help
kali@kali: ~
File Actions Edit View Help

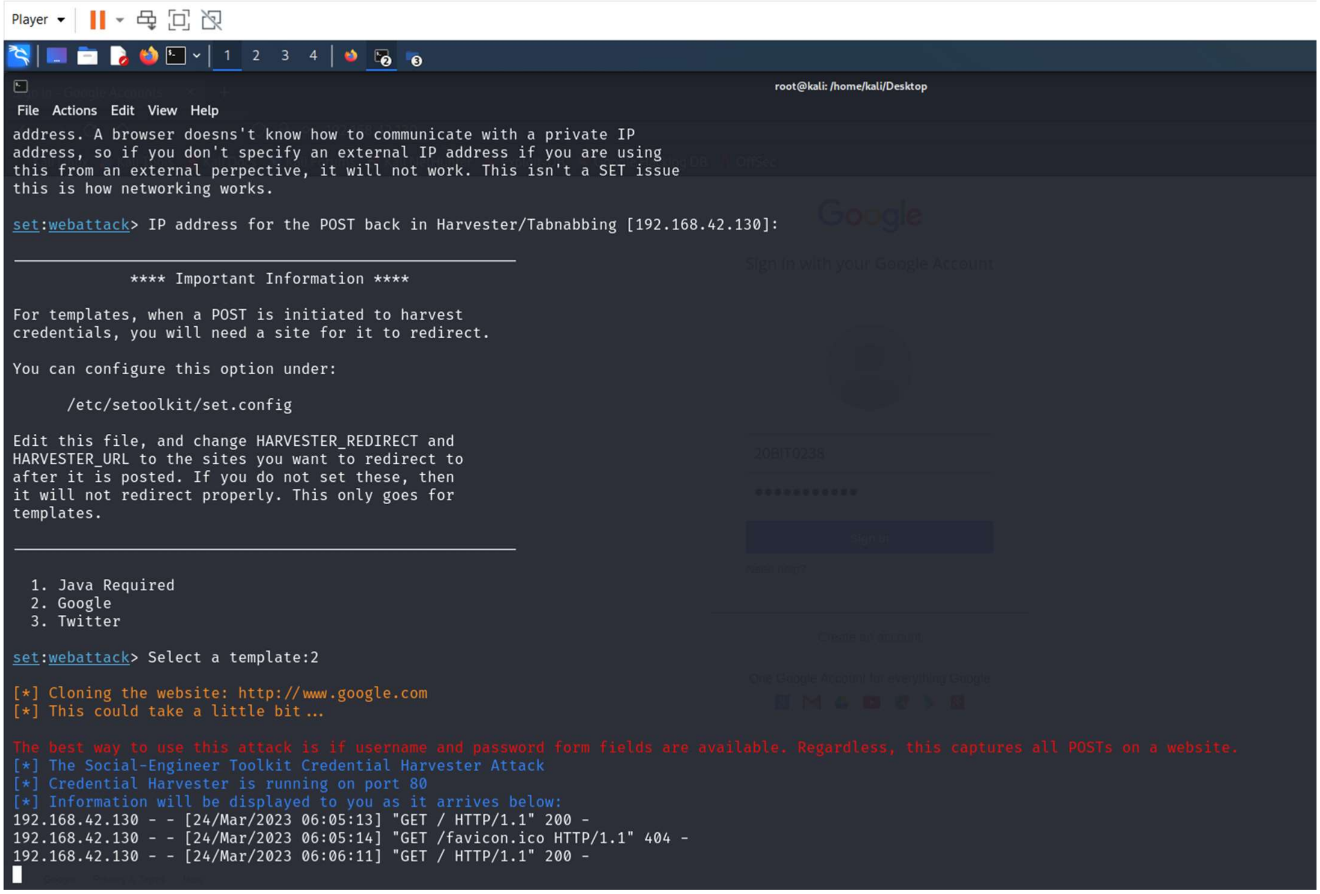
```
The Credential Harvester method will utilize web cloning of a web- site that has a username and password field and harvest all the information pos

The TabNabbing method will wait for a user to move to a different tab, then refresh the page to something different.

The Web-Jacking Attack method was introduced by white_sheep, emgent. This method utilizes iframe replacements to make the highlighted URL link to a
ndow pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow/fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Brow
t once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powers

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) HTA Attack Method

  99) Return to Main Menu

set:webattack>3

 The first method will allow SET to import a list of pre-defined web
 applications that it can utilize within the attack.

 The second method will completely clone a website of your choosing
 and allow you to utilize the attack vectors within the completely
 same web application you were attempting to clone.

 The third method allows you to import your own website, note that you
 should only have an index.html when using the import website
 functionality.

   1) Web Templates
   2) Site Cloner
   3) Custom Import

  99) Return to Webattack Menu

set:webattack>1
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```


Player
1 2 3 4
root@kali: /home/kali/Desktop
File Actions Edit View Help
kali@kali: ~
File Actions Edit View Help

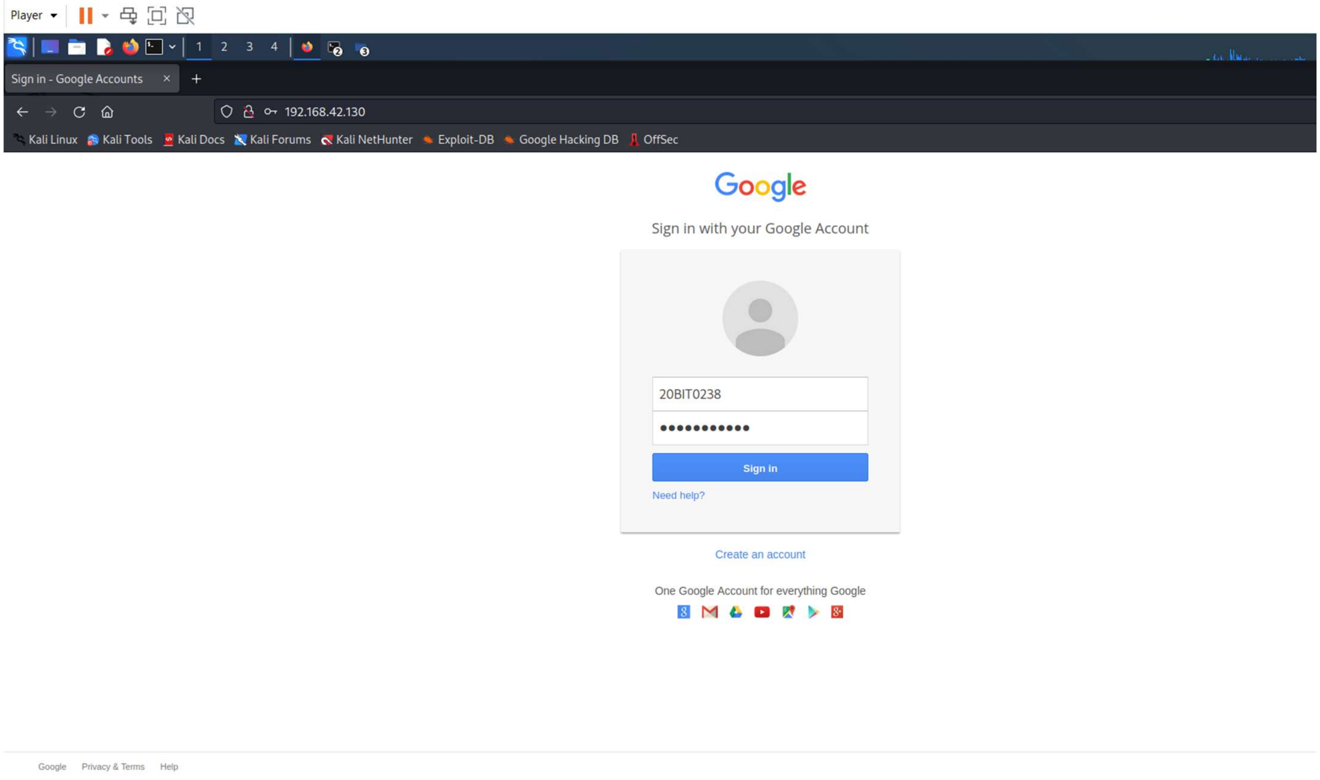
```
── * IMPORTANT * READ THIS BEFORE ENTERING IN THE IP ADDRESS * IMPORTANT * ──

The way that this works is by cloning a site and looking for form fields to
rewrite. If the POST fields are not usual methods for posting forms this
could fail. If it does, you can always save the HTML, rewrite the forms to
be standard forms and use the "IMPORT" feature. Additionally, really
important:

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL
IP address below, not your NAT address. Additionally, if you don't know
basic networking concepts, and you have a private IP address, you will
need to do port forwarding to your NAT IP address from your external IP
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.42.130]:

─────────────────────────────────────────────────────────────
              **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

─────────────────────────────────────────────────────────────

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2
```

```
┌──(kali㉿kali)-[~]
└─$ 20BIT0238
```



```
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.42.130]:

________________________________________________________

              **** Important Information ****

For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

________________________________________________________

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.42.130 - - [24/Mar/2023 06:05:13] "GET / HTTP/1.1" 200 -
192.168.42.130 - - [24/Mar/2023 06:05:14] "GET /favicon.ico HTTP/1.1" 404 -
192.168.42.130 - - [24/Mar/2023 06:06:11] "GET / HTTP/1.1" 200 -
```

VICTIM OPENING THE LINK AND ENTERING CREDENTIALS



Sign in with your Google Account

20BIT0238

●●●●●●●●●●●

Sign in

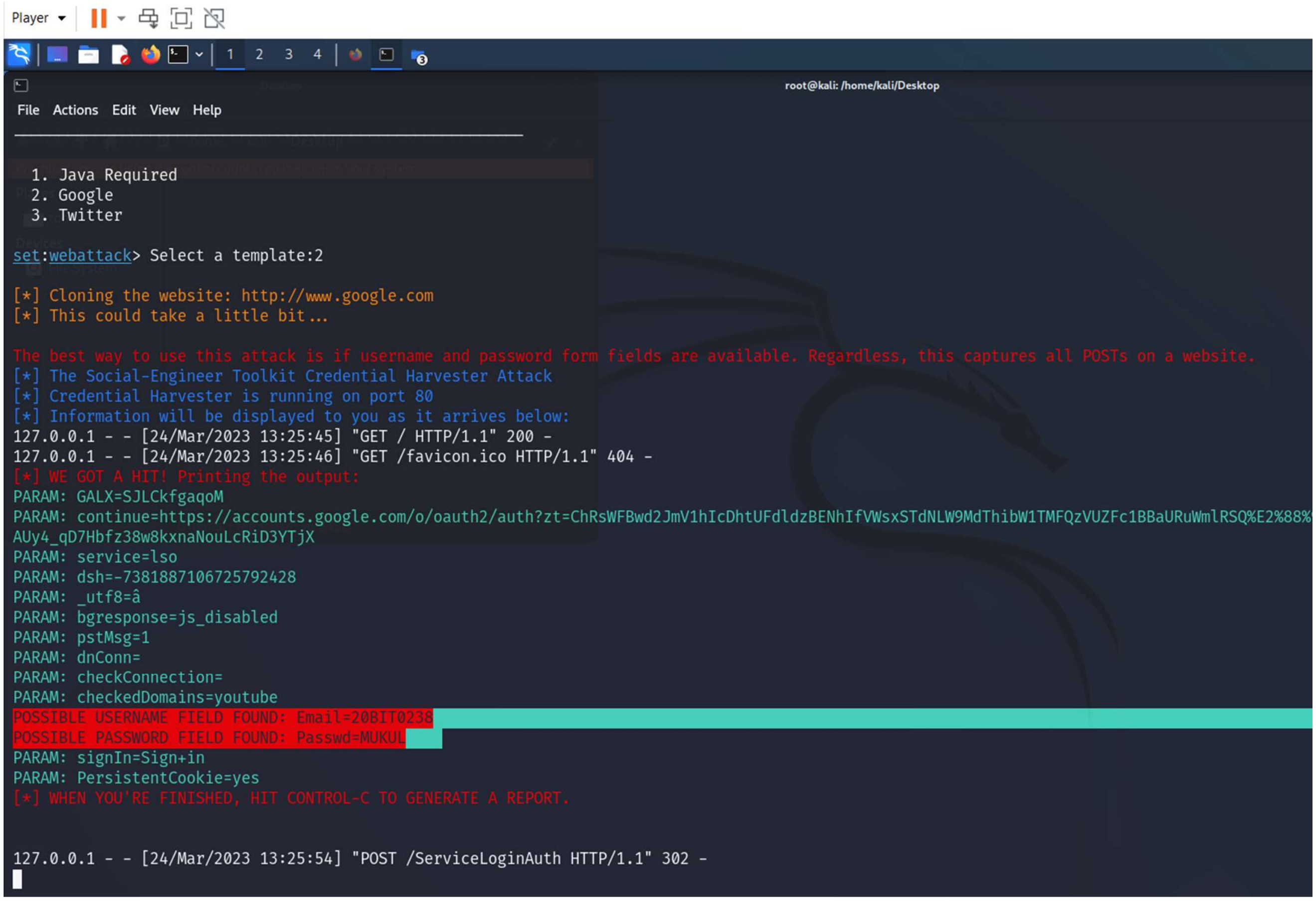
Need help?

Create an account

One Google Account for everything Google

Google Privacy & Terms Help

CREDENTIALS-CAPTURED SUCCESSFULLY

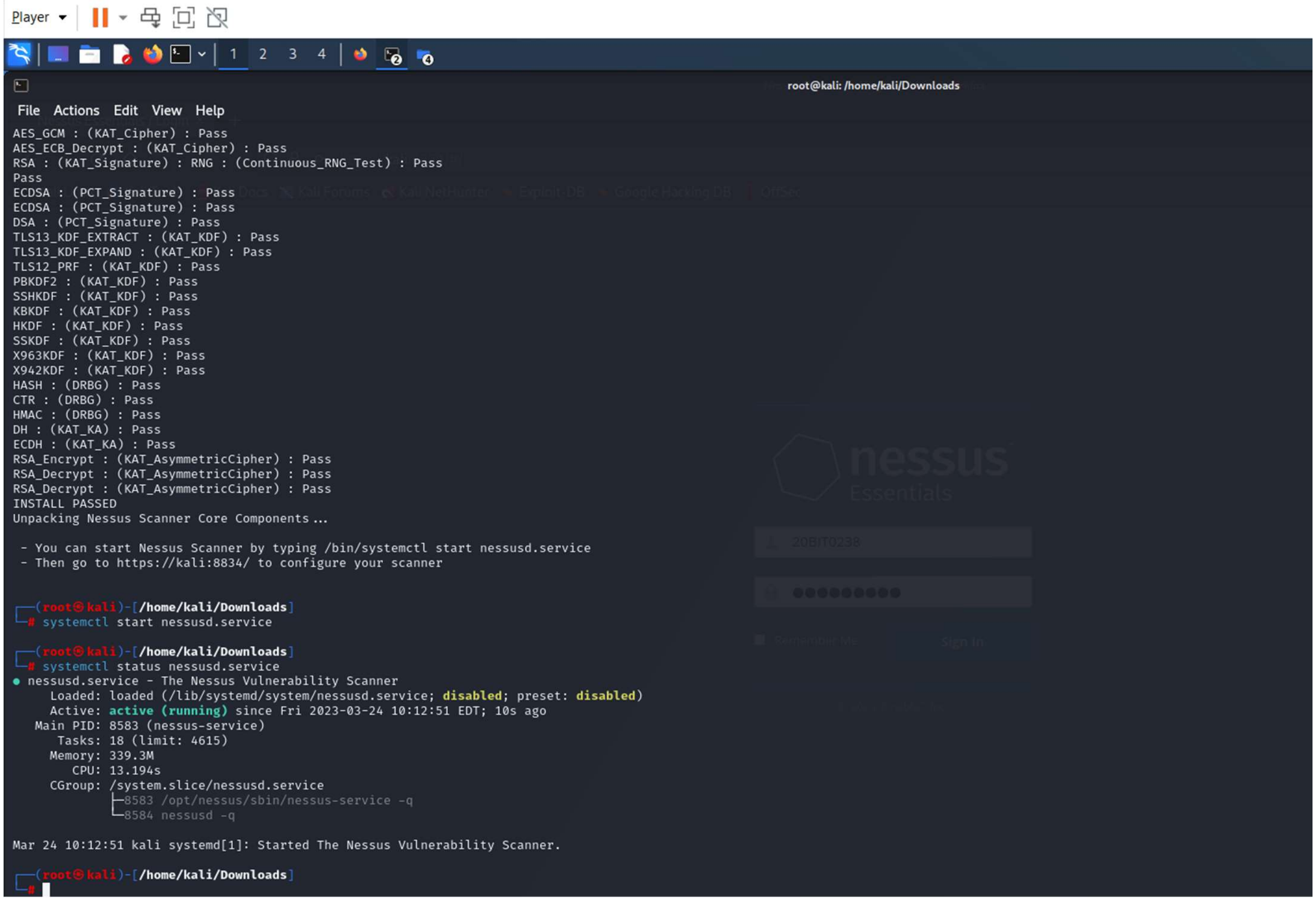


```
  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
127.0.0.1 - - [24/Mar/2023 13:25:45] "GET / HTTP/1.1" 200 -
127.0.0.1 - - [24/Mar/2023 13:25:46] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCkfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmlRSQ%E2%88%
AUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=20BIT0238
POSSIBLE PASSWORD FIELD FOUND: Passwd=MUKUL
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.


127.0.0.1 - - [24/Mar/2023 13:25:54] "POST /ServiceLoginAuth HTTP/1.1" 302 -
█
```

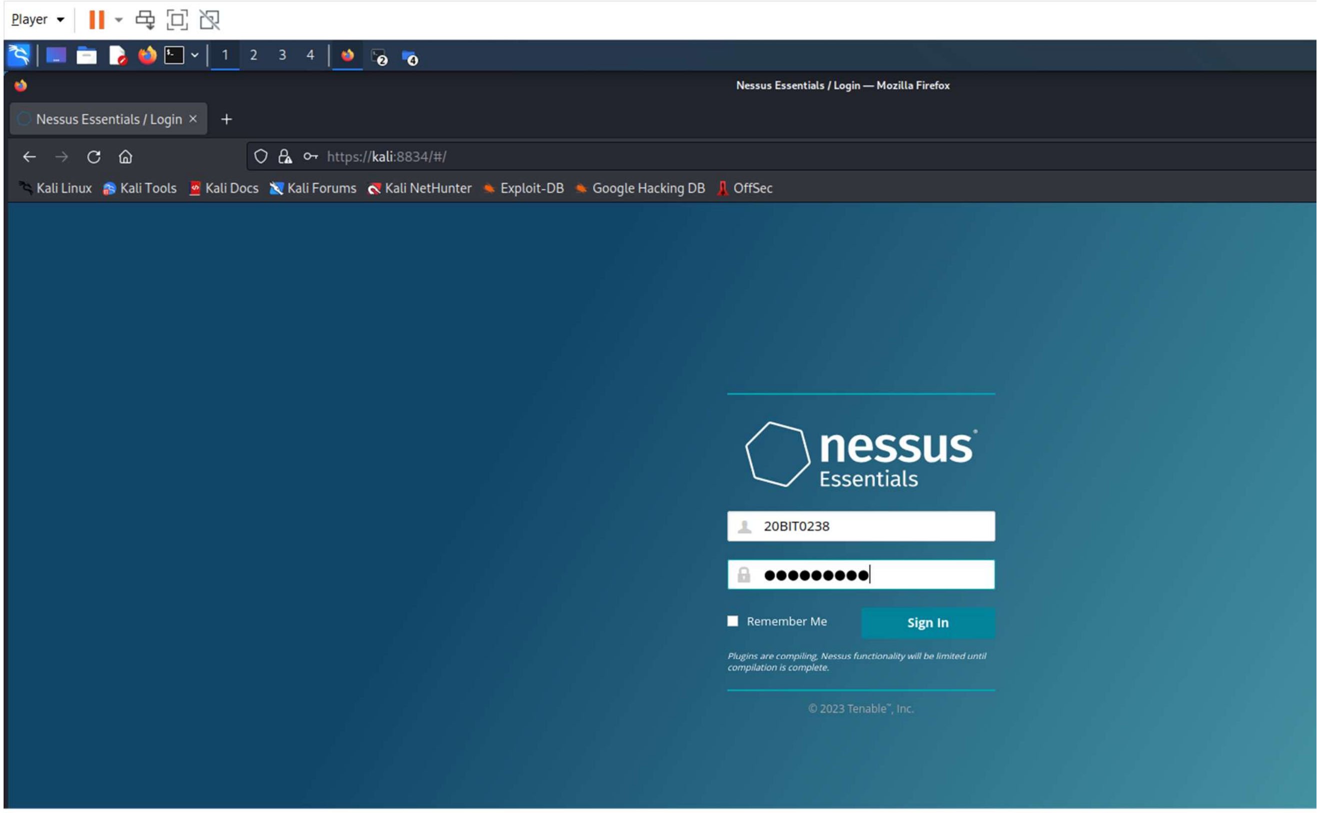
GOOGLE DRIVE LINK(setoolkit victim post details captured)

https://drive.google.com/drive/folders/1v39kBkcz81LjFIHG3iyKWUl_ZD42eG2J?usp=sharing

2. Perform a Web application scan using Nessus on metasploitable ip and identify the vulnerabilities. The login snapshot should be shared. Export the report in a pdf format and share it in the google drive. (Date of the scan should be 7-3-23). (6 marks).



```
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner


┌──(root㉿kali)-[/home/kali/Downloads]
└─# systemctl start nessusd.service

┌──(root㉿kali)-[/home/kali/Downloads]
└─# systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Fri 2023-03-24 10:12:51 EDT; 10s ago
   Main PID: 8583 (nessus-service)
      Tasks: 18 (limit: 4615)
     Memory: 339.3M
        CPU: 13.194s
     CGroup: /system.slice/nessusd.service
             ├─8583 /opt/nessus/sbin/nessus-service -q
             └─8584 nessusd -q

Mar 24 10:12:51 kali systemd[1]: Started The Nessus Vulnerability Scanner.

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



Nessus Essentials / Login — Mozilla Firefox

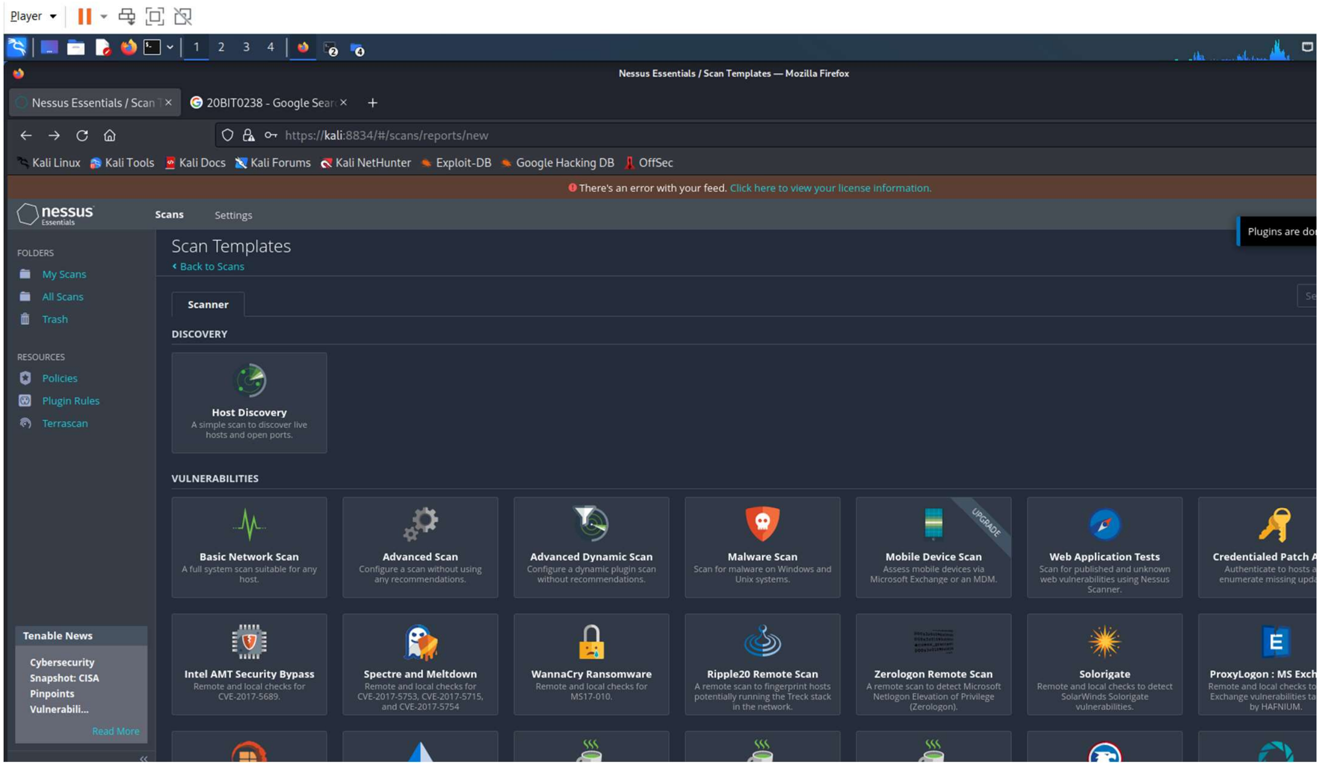
https://kali:8834/#/

20BIT0238

●●●●●●●●●●

Plugins are compiling. Nessus functionality will be limited until compilation is complete.

© 2023 Tenable™, Inc.



Nessus Essentials / Scan Templates — Mozilla Firefox

https://kali:8834/#/scans/reports/new

There's an error with your feed. Click here to view your license information.

Plugins are do

Scan Templates

DISCOVERY

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.

Mobile Device Scan Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch A Authenticate to hosts a enumerate missing upda

Intel AMT Security Bypass Remote and local checks for CVE-2017-5689.

Spectre and Meltdown Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware Remote and local checks for MS17-010.

Ripple20 Remote Scan A remote scan to fingerprint hosts potentially running the Treck stack in the network.

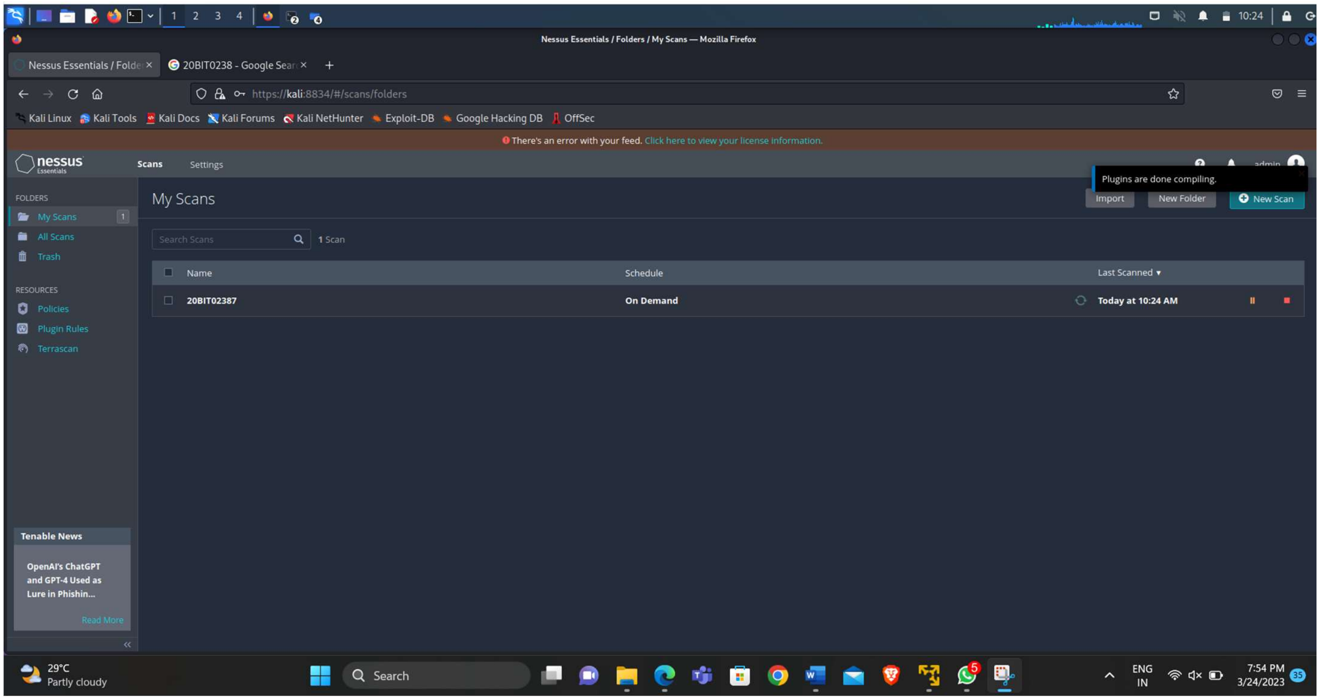
Zerologon Remote Scan A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

Solorigate Remote and local checks to detect SolarWinds Solorigate vulnerabilities.

ProxyLogon : MS Exch Remote and local checks to Exchange vulnerabilities ta by HAFNIUM.

Tenable News

Cybersecurity Snapshot: CISA Pinpoints Vulnerabili...



Nessus Essentials / Folders / My Scans — Mozilla Firefox

https://kali:8834/#/scans/folders

There's an error with your feed. Click here to view your license information.

Plugins are done compiling.

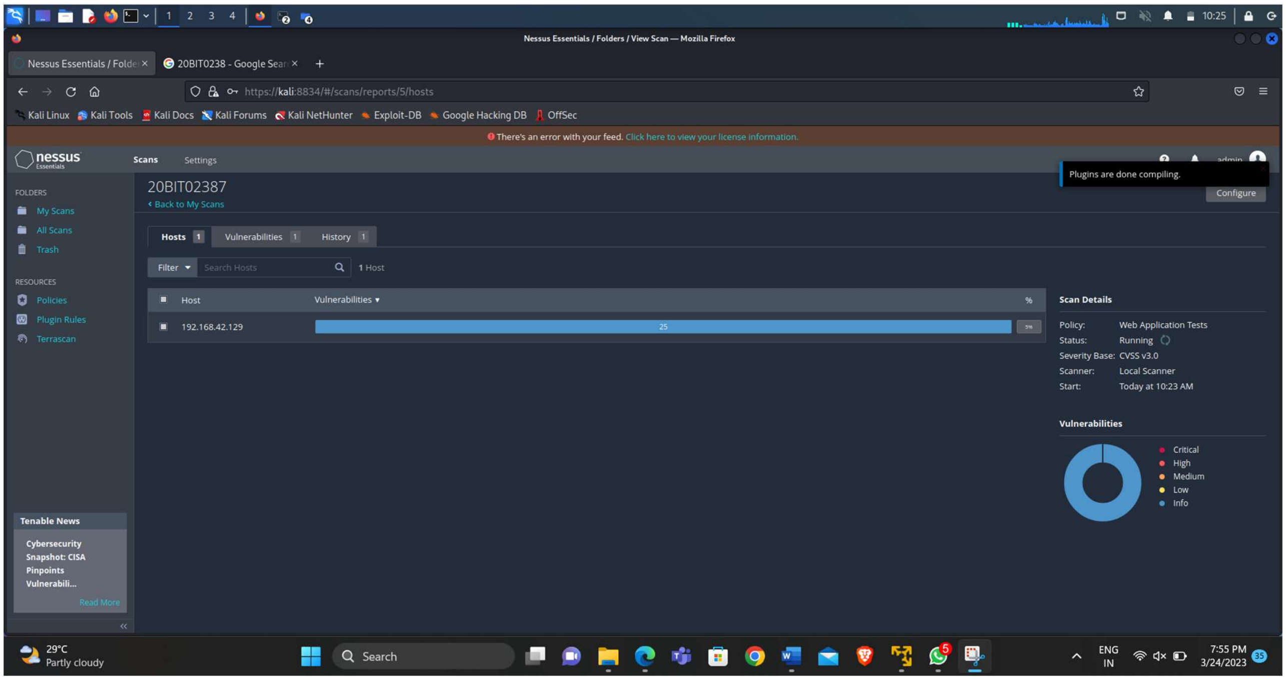
My Scans

1 Scan

Name	Schedule	Last Scanned ▾
20BIT02387	On Demand	Today at 10:24 AM

Tenable News

OpenAI's ChatGPT and GPT-4 Used as Lure in Phishin...



Nessus Essentials / Folders / View Scan — Mozilla Firefox

https://kali:8834/#/scans/reports/5/hosts

There's an error with your feed. Click here to view your license information.

Plugins are done compiling.

20BIT02387

1 Host

Host	Vulnerabilities ▾	%
192.168.42.129	25	5%

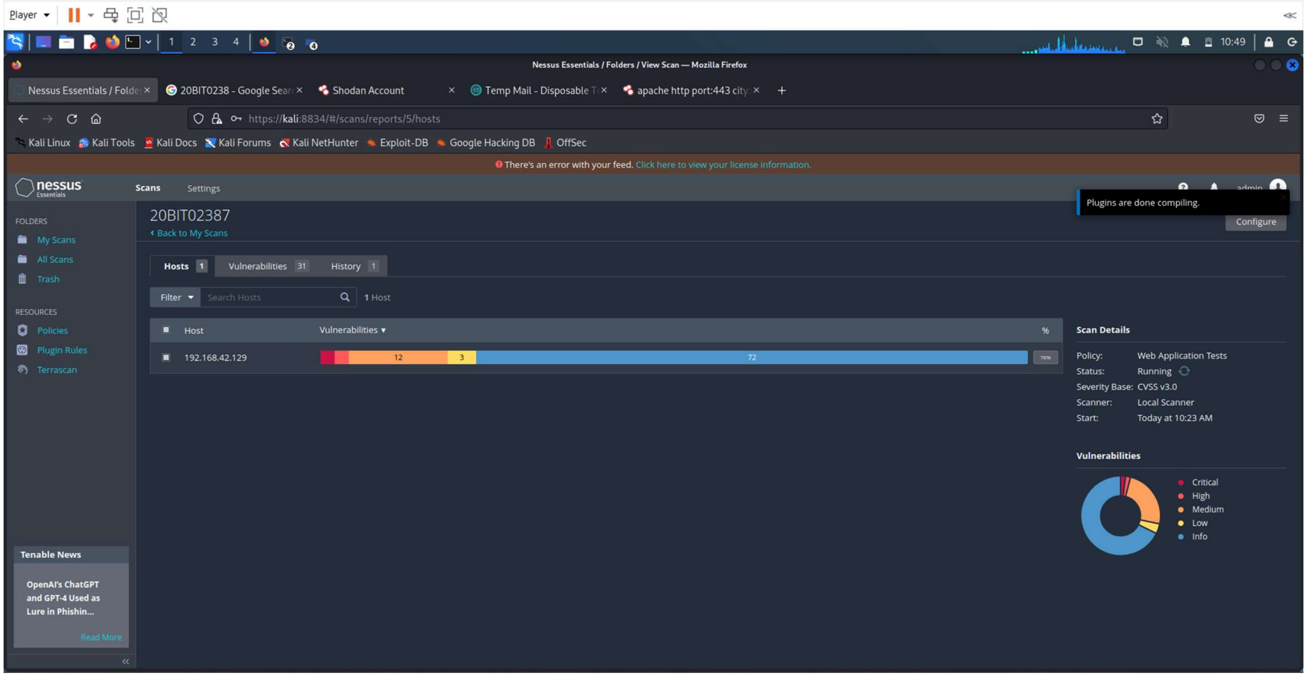
Scan Details

Policy: Web Application Tests
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:23 AM

Vulnerabilities

Tenable News

Cybersecurity Snapshot: CISA Pinpoints Vulnerabili...



There's an error with your feed. Click here to view your license information.

Plugins are done compiling.

20BIT02387

Back to My Scans

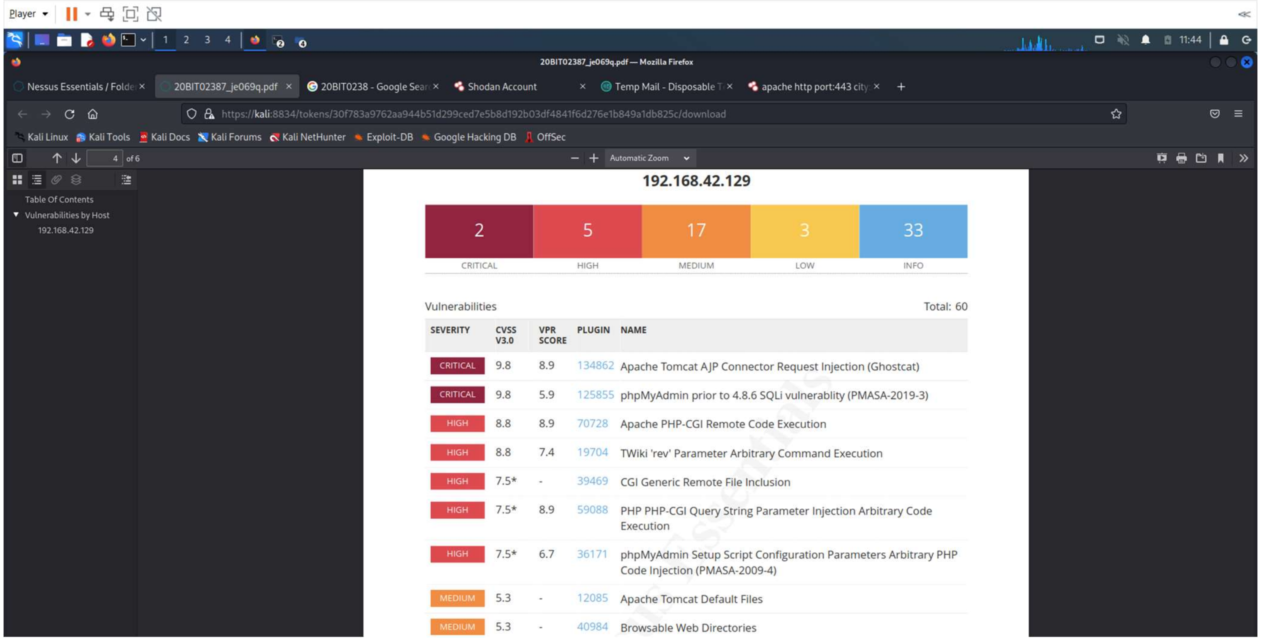
Host	Vulnerabilities	%
192.168.42.129	12 3 72	76%

Scan Details

Policy: Web Application Tests
Status: Running
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 10:23 AM

Vulnerabilities

SCAN-RESULTS



192.168.42.129

CRITICAL	HIGH	MEDIUM	LOW	INFO
2	5	17	3	33

Vulnerabilities Total: 60

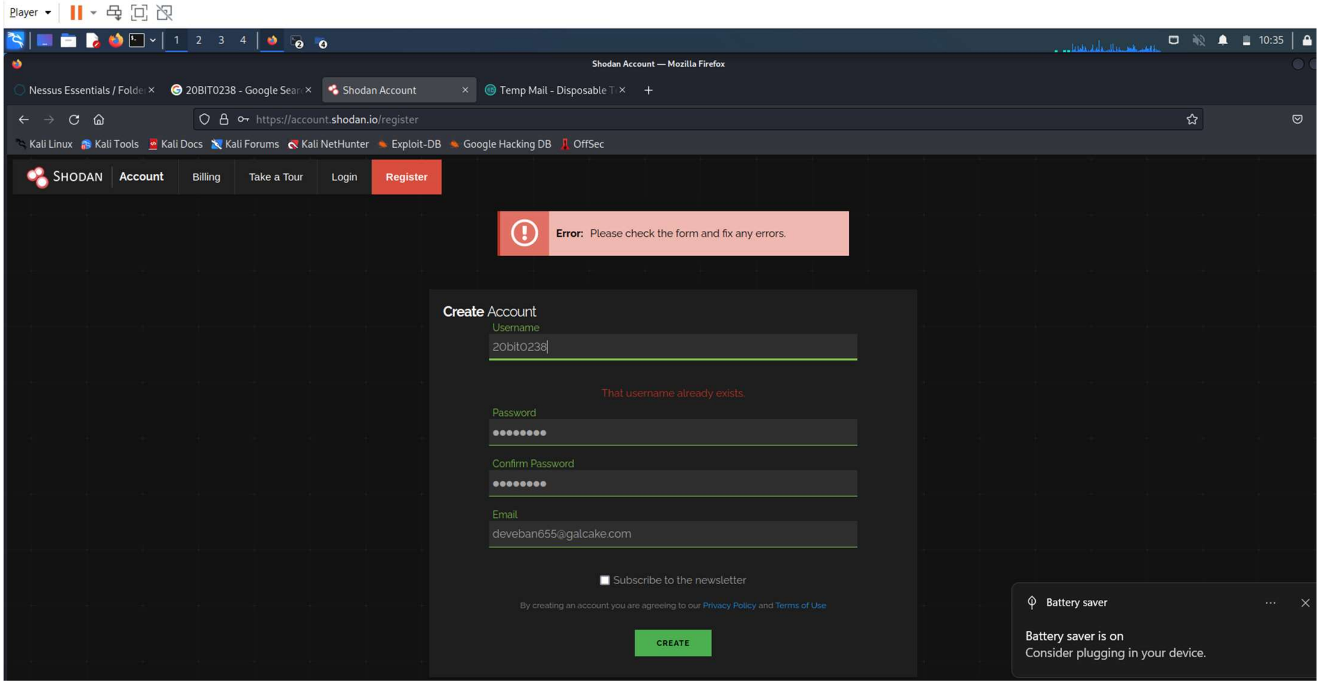
SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	8.9	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	5.9	125855	phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)
HIGH	8.8	8.9	70728	Apache PHP-CGI Remote Code Execution
HIGH	8.8	7.4	19704	TWiki 'rev' Parameter Arbitrary Command Execution
HIGH	7.5*	-	39469	CGI Generic Remote File Inclusion
HIGH	7.5*	8.9	59088	PHP PHP-CGI Query String Parameter Injection Arbitrary Code Execution
HIGH	7.5*	6.7	36171	phpMyAdmin Setup Script Configuration Parameters Arbitrary PHP Code Injection (PMASA-2009-4)
MEDIUM	5.3	-	12085	Apache Tomcat Default Files
MEDIUM	5.3	-	40984	Browsable Web Directories

GOOGLE-DRIVE LINK (nessus scan results - exported pdf uploaded)

https://drive.google.com/drive/folders/1v39kBkcz81LjFIHG3iyKWUl_ZD42eG2J?usp=sharing

3. Perform a search on Shodan to identify the list of devices using Apache and http port:443 in your birth city. If your city is not listed, then select the nearest city. [3 marks]

command: apache http port:443 city:mumbai



https://account.shodan.io/register

Error: Please check the form and fix any errors.

Create Account

Username: 20bit0238

That username already exists

Password: ••••••••

Confirm Password: ••••••••

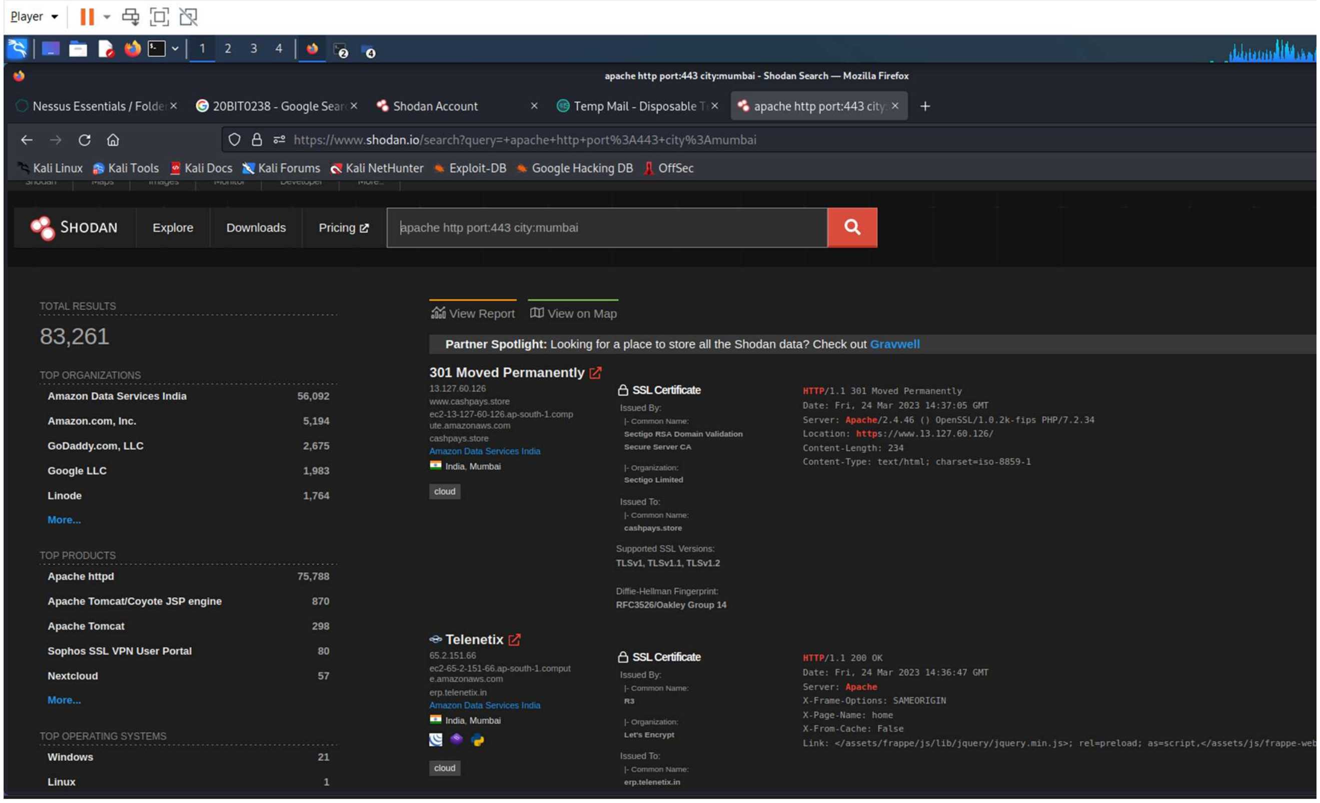
Email: deveban655@galcake.com

□ Subscribe to the newsletter

By creating an account you are agreeing to our Privacy Policy and Terms of Use

Battery saver

Battery saver is on
Consider plugging in your device.



https://www.shodan.io/search?query=+apache+http+port%3A443+city%3Amumbai

apache http port:443 city:mumbai

TOTAL RESULTS

83,261

TOP ORGANIZATIONS	
Amazon Data Services India	56,092
Amazon.com, Inc.	5,194
GoDaddy.com, LLC	2,675
Google LLC	1,983
Linode	1,764
More...	

TOP PRODUCTS	
Apache httpd	75,788
Apache Tomcat/Coyote JSP engine	870
Apache Tomcat	298
Sophos SSL VPN User Portal	80
Nextcloud	57
More...	

TOP OPERATING SYSTEMS	
Windows	21
Linux	1

Partner Spotlight: Looking for a place to store all the Shodan data? Check out Gravwell

301 Moved Permanently
13.127.60.126
www.cashpays.store
ec2-13-127-60-126.ap-south-1.compute.amazonaws.com
cashpays.store
Amazon Data Services India
India, Mumbai

SSL Certificate
Issued By:
|- Common Name:
Sectigo RSA Domain Validation Secure Server CA
|- Organization:
Sectigo Limited
Issued To:
|- Common Name:
cashpays.store
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Fingerprint:
RFC3526/Oakley Group 14

```
HTTP/1.1 301 Moved Permanently
Date: Fri, 24 Mar 2023 14:37:05 GMT
Server: Apache/2.4.46 () OpenSSL/1.0.2k-fips PHP/7.2.34
Location: https://www.13.127.60.126/
Content-Length: 234
Content-Type: text/html; charset=iso-8859-1
```

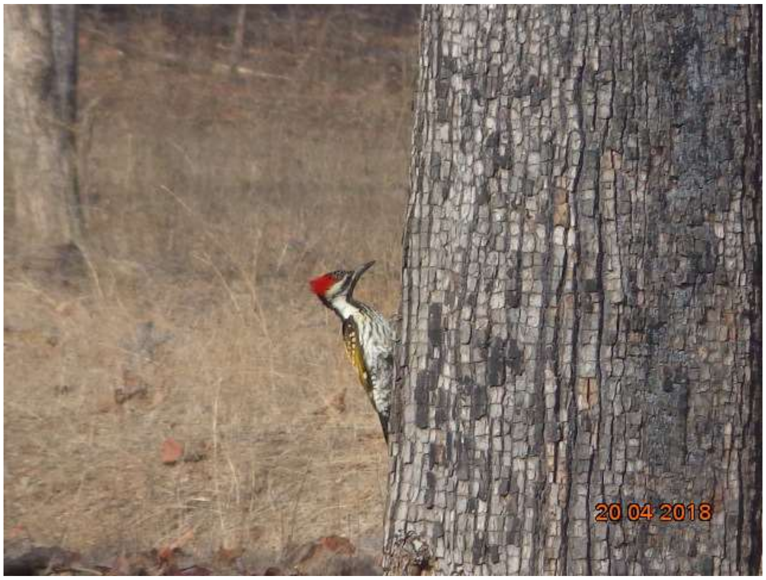
Telenetix
65.2.151.66
ec2-65-2-151-66.ap-south-1.compute.amazonaws.com
erp.telenetix.in
Amazon Data Services India
India, Mumbai

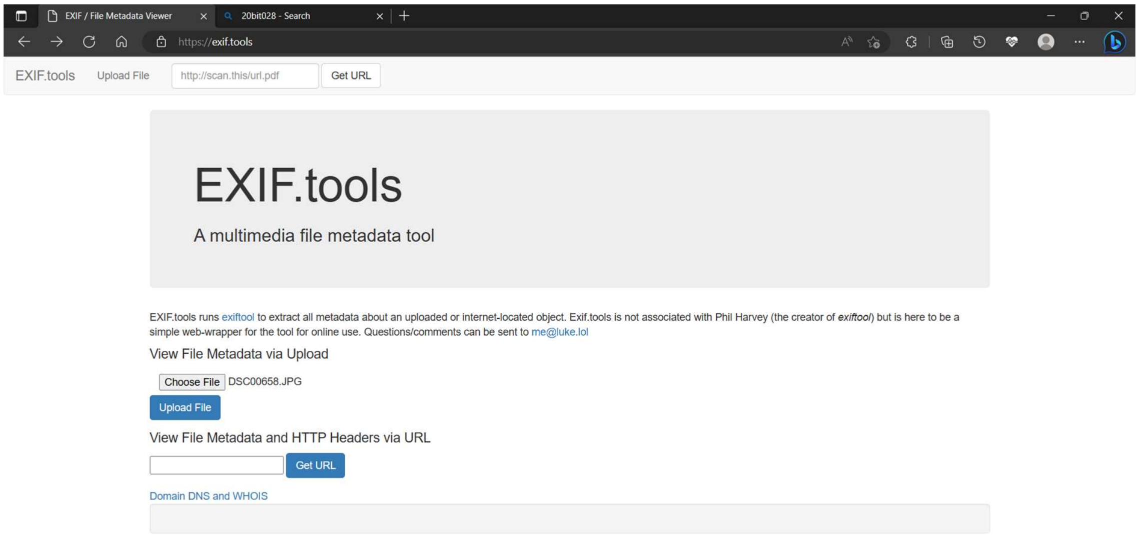
SSL Certificate
Issued By:
|- Common Name:
R3
|- Organization:
Let's Encrypt
Issued To:
|- Common Name:
erp.telenetix.in

```
HTTP/1.1 200 OK
Date: Fri, 24 Mar 2023 14:36:47 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
X-Page-Name: home
X-From-Cache: False
Link: </assets/frappe/js/lib/jquery/jquery.min.js>; rel=preload; as=script,</assets/js/frappe-web
```

4. Perform an image forensics on exif.tools to gather meta data about the photo wherein you are present and provide information about the place, geo coordinates, date of photo captured etc. [2 marks]

Image





EXIF.tools

A multimedia file metadata tool

EXIF.tools runs exiftool to extract all metadata about an uploaded or internet-located object. Exif.tools is not associated with Phil Harvey (the creator of *exiftool*) but is here to be a simple web-wrapper for the tool for online use. Questions/comments can be sent to me@luke.lol

View File Metadata via Upload

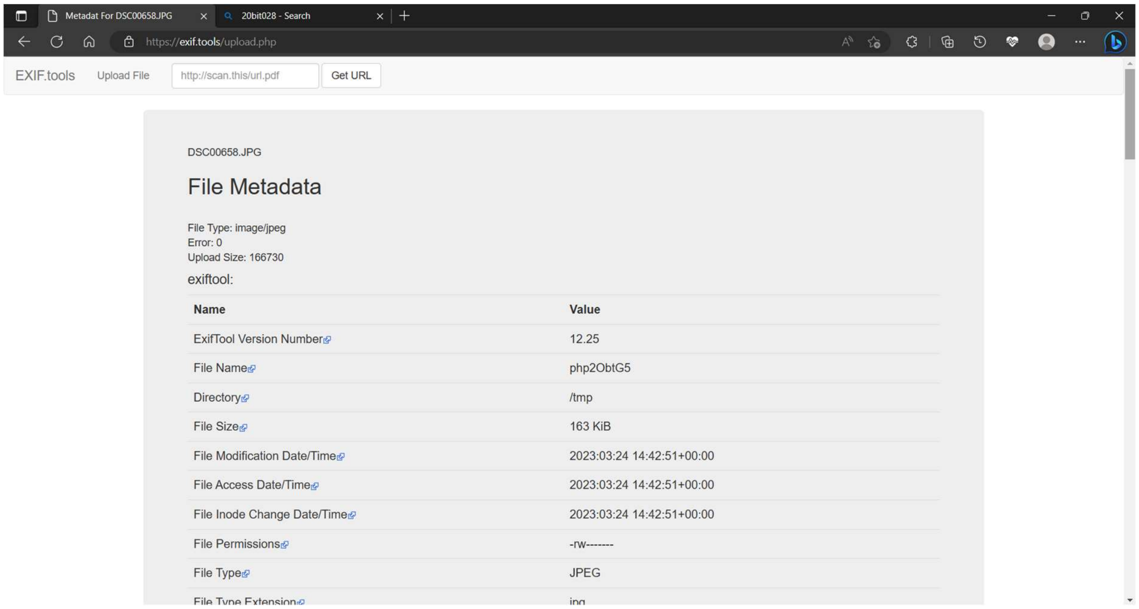
Choose File DSC00658.JPG

Upload File

View File Metadata and HTTP Headers via URL

Get URL

Domain DNS and WHOIS



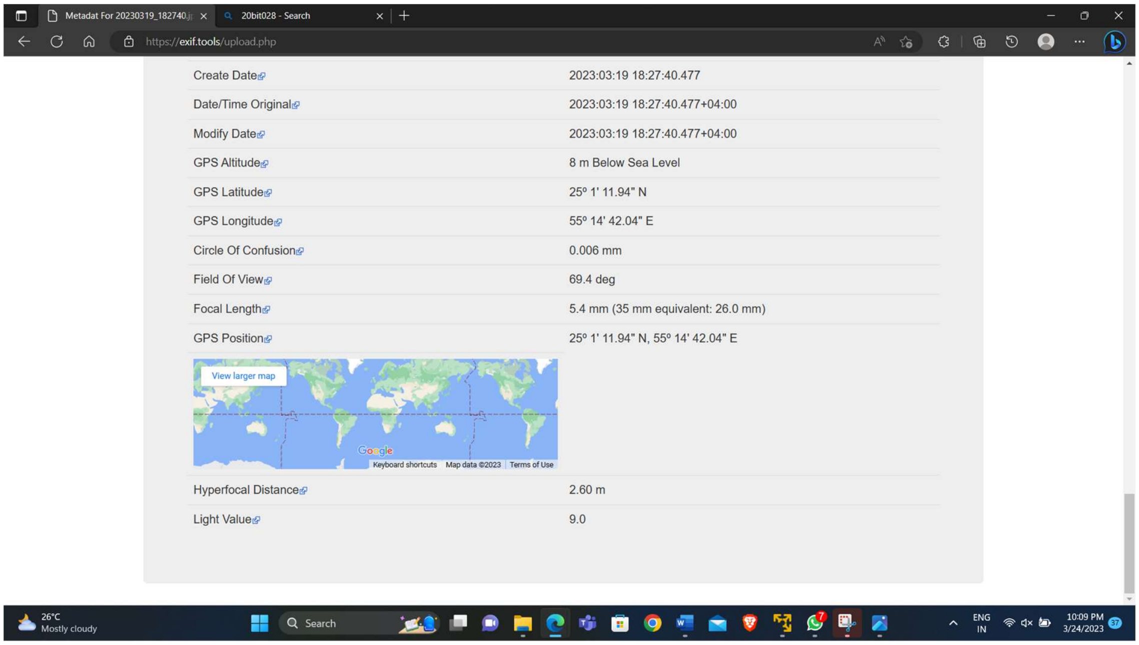
DSC00658.JPG

File Metadata

File Type: image/jpeg
Error: 0
Upload Size: 166730

exiftool:

Name	Value
ExifTool Version Number	12.25
File Name	php2ObtG5
Directory	/tmp
File Size	163 KiB
File Modification Date/Time	2023:03:24 14:42:51+00:00
File Access Date/Time	2023:03:24 14:42:51+00:00
File Inode Change Date/Time	2023:03:24 14:42:51+00:00
File Permissions	-rw-------
File Type	JPEG
File Type Extension	jpg



Create Date	2023:03:19 18:27:40.477
Date/Time Original	2023:03:19 18:27:40.477+04:00
Modify Date	2023:03:19 18:27:40.477+04:00
GPS Altitude	8 m Below Sea Level
GPS Latitude	25º 1' 11.94" N
GPS Longitude	55º 14' 42.04" E
Circle Of Confusion	0.006 mm
Field Of View	69.4 deg
Focal Length	5.4 mm (35 mm equivalent: 26.0 mm)
GPS Position	25º 1' 11.94" N, 55º 14' 42.04" E
Hyperfocal Distance	2.60 m
Light Value	9.0