مجلة جامعة بني وليد للعلوم الإنسانية والتطبيقية

تصدر عن جامعة بني وليد – ليبيا

Website: https://jhas-bwu.com/index.php/bwjhas/index

العدد التاسع والعشرون، 2023

Phishing Attack on Credential Harvester (Google)

Haytham F. Dhaw[1*], Alhadi A. Alajeili[2], Khalid M. Ajbrah[3], Abdesalam A. Almarimi[4]
Mohammed A. Abdulsalam[5]

[1]Dept. of General Section/ Higher Institute of Medical Technology Baniwalid, Libya
[2]Libyan Center for Engineering Research and information Technology, Baniwalid, Libya
[3]Dept. of Computer Engineering & IT/ College of Electronic Technology Baniwalid, Libya
[4]Dept. of Computer Engineering & IT/ Higher Institute of Engineering Technologies Baniwalid, Libya
[5]Libyan Center for Engineering Research and information Technology, Tripoly, Libya
*Crosspnding author:: h.mondo89@gmail.com

تاريخ الاستلام: 09-06-2023 تاريخ القبول: 27-06-2023 تاريخ النشر : 07-09-2023

Abstract—Vulnerabilities and weaknesses of web applications are targeting by attackers. Therefore, penetration testing techniques are very important for building strategies which make the system is secure. This paper proposes a penetration testing model for phishing attack which is a common these days. The proposed model was implemented using the latest versions of VMware-machine, kali-Linux, and Windows 10. The Hiddeneye, Ngrok, and bitly tools were used. This was achieved by information gathering method. The obtained results of the phishing attack were identified and their appropriate countermeasures were defined.

Keywords: Computer security, Web security, Ethical hacking.

Introduction

This Phishing is a cybercrime in which scammers send a malicious email to individual(s) or mass users of any organization by impersonating a recognized individual or a business partner or a service provider, these emails are carefully created such that it is opened it without any suspicion. Criminals have countless methods and types of phishing emails to fake email users. Phishing is the electronic version of social engineering and has found a huge market in our email-obsessed world. Hackers send fraudulent emails out to literally millions of people, hoping a few will click on the attached links, documents, or pictures, with the goal of getting recipients to willingly provide valuable private information such as; social security numbers, passwords, banking numbers, PINs, credit card numbers and so on [1].

This can be achieved through a few different methods. Sometimes, cybercriminals trick email recipients into opening an email attachment that loads harmful malware onto their system. Other times, they fool recipients into providing sensitive personal information directly via web forms. Either way, these seemingly small mistakes could send serious ripples across an organization, compromising a corporate or personal security. These types of phishing attacks open the door for attackers to enter into the victim system and access confidential data like bank account details, credit card numbers, social security number, passwords, etc. [2].

Once the information is obtained, the phishers immediately send or sell it to people who misuse them. Sometimes, phishing not only results in loss of information but also injects viruses into the victim's computer or phone. As soon as infected, phishers gain control over devices, through

which they can send emails and messages to other people connected through the server.

According to the APWG report, the number of unique phishing websites had reached 73.80% from October 2017 to March 2018, and, 48.60% of the reported phishing incidents had used ".COM" domain. The domains and websites that interacted with assumed are safe, but hackers do trick us with different types of phishing attacks, by using impersonated domains and cloned websites. Scammers use Social Engineering to know the online behavior and preferences of the potential victim [3]. This helps them to craft a sophisticated attack.

According to the Kaspersky report in the second quarter of 2019, the average share of spam in global mail traffic cut down to 57.64%, while the Anti-Phishing system prohibited more than 130 million redirects to phishing sites, up 18 million during the previous reporting period. Throughout the second quarter of 2019, their security solutions detected a total of 43,907,840 malicious email attachments. The most prevalent malware in mail traffic was Exploit.MSOffice.CVE-2017-11882.gen with a share of 7.53%, while Backdoor.Win32.Androm, with an 8% share, was the most common malicious family [4].

In the third quarter of 2019, first place by prevalence in mail traffic went to the Office malware Exploit.MSOffice.CVE-2017-11882.gen (7.13%); in second place was the Worm.Win32.WBVB.vam worm (4.13%), and in third was another malware aimed at Microsoft Office users, Trojan.MSOffice.SAgent.gen (2.24%). In the third quarter of 2019, the Anti-Phishing system prevented 105,220,094 attempts to direct users to scam websites. The percentage of unique attacked users was 11.28% of the total number of users of Kaspersky products worldwide. The rating of categories of organizations attacked by phishers is based on triggers of the Anti-Phishing component on user computers. It is activated every time the user attempts to open a phishing page, either by clicking a link in an email or a social media message, or as a result of malware activity. When the component is triggered, a banner is displayed in the browser warning the user about a potential threat. This is the first time, in 2019, the share of attacks on organizations in the Global Internet Portals category (23.81%) exceeded the share of attacks on credit organizations (22.46%). Social networks (20.48%) took third place [5].

PHISHING ATTACK

Phishing can take many forms and can be achieved with many tools and techniques. Here, we highlight the most common tools and techniques that are used to carry out phishing scams. There are many sophisticated types of phishing involving email fishing [6].

1. **Email Phishing**

Most phishing attacks are sent by email. The crook will register a fake domain that impersonators a genuine organization and sends thousands out thousands of common requests. The fake domain often involves character substitution, like using 'r' and 'n' next to each other to create 'rn' instead of 'm'.

There are some reasons why phishing attacks are frequently conducted through email:

• Wide Reach: Email is a widely used communication channel, with billions of emails sent and received every day. Attackers leverage this extensive reach to target a large number of potential victims simultaneously.

• Easy Spoofing: Attackers can easily spoof the sender's information in an email, making it appear as if the email is coming from a reputable source or a trusted organization. They may manipulate the display name, email address, or even use techniques like email header forgery to make the email seem legitimate.

• Social Engineering: Phishing emails often employ social engineering techniques to manipulate recipients into taking desired actions. They may use urgency, fear, curiosity, or the promise of rewards to entice users into clicking on malicious links, opening infected attachments, or disclosing sensitive information.

• Link Manipulation: Phishing emails commonly contain manipulated or fraudulent links. As mentioned earlier, attackers alter the URLs to lead recipients to fake websites that mimic legitimate ones. These fake sites are designed to collect login credentials or personal information.

• Malicious Attachments: Phishing emails may also include attachments that contain malware or viruses. These attachments often masquerade as harmless files, such as PDFs, documents, or invoices, but they can infect the recipient's device once opened.

• Automation and Scalability: Phishing attacks can be automated, allowing attackers to send a large volume of emails quickly and easily. They can use tools to generate phishing emails en masse, targeting a broad range of recipients and increasing the chances of success.

It's important to stay vigilant and exercise caution when interacting with emails, especially those that appear suspicious or unexpected. Be wary of unsolicited emails asking for personal information, urging immediate action, or containing suspicious links or attachments. Verify the legitimacy of emails independently, by contacting the supposed sender through a trusted source or using official contact information.

Alternatively, they might use the organization's name in the local part of the email address such as 'google@domainregistrar.com' in the hopes that the sender's name will simply appear as 'google' in the recipient's inbox.

There are several ways to spot a phishing email. Here are some common signs to look out for:

Phishing: Phishing attacks involve sending deceptive emails that appear to be from legitimate sources, such as banks, online services, or trusted organizations. The goal is to trick recipients into divulging sensitive information, such as login credentials, credit card numbers, or personal data.

• Spear Phishing: Spear phishing attacks are targeted phishing attempts aimed at specific individuals or organizations. Attackers gather information about their targets to create personalized and convincing emails, making it more likely for recipients to fall for the scam.

• Whaling: Whaling attacks are a form of spear phishing that specifically targets high-profile individuals like CEOs or senior executives. Attackers craft sophisticated emails pretending to be from trusted sources, aiming to trick these individuals into divulging sensitive information or performing actions that benefit the attacker.

• Email Spoofing: Email spoofing involves forging the sender's email address to make it appear as if the email is coming from someone else. Attackers can manipulate the "From" field to make it seem like the email is from a trusted source, tricking recipients into trusting the message and taking action.

• Malware Attachments: Attackers may send emails with malicious attachments, such as infected documents or executable files. Opening these attachments can result in the installation of malware on the recipient's device, leading to unauthorized access, data theft, or other malicious activities.

• Man-in-the-Middle (MitM) Attacks: In a MitM attack, an attacker intercepts communication between the sender and recipient of an email. The attacker can eavesdrop on the conversation, modify the content of the emails, or even impersonate one of the parties involved.

- Email Account Compromise: Attackers may gain unauthorized access to someone's email account by guessing or stealing login credentials. Once they gain control, they can use the compromised account to launch further attacks, send spam, or access sensitive information.
- Phishing Sub-Domains Attackers can create sub-domains that mimic legitimate websites to launch phishing attacks. For example, they may create a sub-domain like "login.example.com" that looks similar to a legitimate login page. Unsuspecting users who enter their credentials on such sub-domains unknowingly provide their information to the attacker.

2. Hidden URL phishing attack is a technique used by attackers to deceive users by hiding the actual destination of a URL within a seemingly legitimate one. This manipulation aims to trick users into clicking on the link, thinking it leads to a trusted website when, in reality, it redirects them to a malicious or fraudulent webpage. Here's how a hidden URL phishing attack can occur:
   - Text masking: Attackers can hide the actual URL by using text masking techniques. They may display a text hyperlink that appears legitimate but, when clicked, directs the user to a different website. For example, the displayed link may show "www.example.com," but the actual URL leads to a malicious site.
   - HTML anchor tags: Attackers can leverage HTML anchor tags to manipulate the URL. By using code, they can specify a different URL in the anchor tag's "href" attribute than what is displayed to the user. This allows them to show a legitimate-looking link while redirecting users to a different site.
   - URL shorteners: Attackers often use URL shortening services to mask the actual destination of a link. They generate a shortened URL that appears harmless or intriguing, but it leads to a malicious website. Users may not be able to discern the true destination before clicking on the shortened link.
3. pop-up phishing attack, also known as a pop-up scam or pop-up phishing, is a tactic employed by attackers to deceive users through fraudulent pop-up windows. These pop-ups are designed to mimic legitimate websites or system messages in order to trick users into revealing sensitive information or downloading malware. Here's how a pop-up phishing attack typically works:
   - Unauthorized Pop-up Windows: Attackers create pop-up windows that appear during browsing sessions or when visiting specific websites. These pop-ups may overlay the current page or open in new browser windows.
   - Mimicking Legitimate Sources: Pop-up windows are designed to imitate trustworthy sources, such as legitimate websites, software updates, or system alerts. They may use logos, branding, or language similar to those used by reputable organizations to appear convincing.
   - Urgency and Fear Tactics: Attackers often employ urgency or fear tactics to prompt users into taking immediate action. The pop-up may claim that the user's computer is infected, personal data has been compromised, or their account is at risk. This creates a sense of urgency and can lead users to make hasty decisions without proper scrutiny.
   - Soliciting Personal Information: Pop-up phishing attacks may request users to enter sensitive information, such as login credentials, credit card details, or personal identification information. The intention is to trick users into providing their confidential data, which can later be misused for identity theft or fraud.
   - Malware Downloads: Pop-up windows can also trick users into downloading and installing malware-infected files or applications. These malicious downloads can compromise the user's device, leading to unauthorized access, data theft, or other harmful consequences.

THE PROPOSED MODEL

In this paper, a penetration testing model was proposed as a model to test the integrity and confidentiality of data on the network security throughout a particular four phases of procedures as shown in "Fig. 1". Several tools and techniques are used for social engineering and information gathering to generate the domain and attacks on the intended network security. Therefore, the test network laboratory was setup in attempt to simulate attacks on the given network with a few information about the target system or network, hence, the used type of penetration testing known as a grey-box approach. It reduces the number of irrelevant tests and minimize the possibility of damage to the system or network.

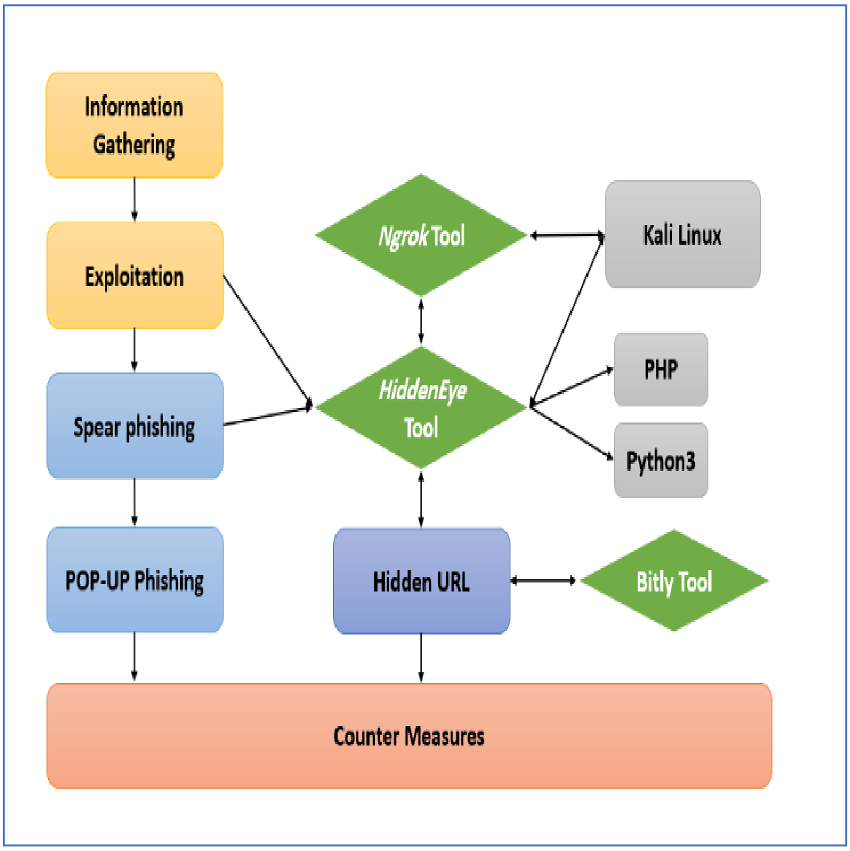


Fig. 1: The Proposed Penetration Testing Model

The overall process of penetration testing is divided into several phases collectively they form a comprehensive penetration testing methodology. Different methodologies may have different nomenclature for various phases, but these methodologies share the same objective. There are four phases as shown in "Fig. 2", to be used by the network penetration tester.

LABAROTORY SETUP

The proposed penetration testing model is implemented using specific tools and techniques. First, we have installed the VM Ware version 15.5, which is virtualization software that allows us to use different operating systems on the virtual machine, to emulate a cross-platform environment. Second, two machines OSs (Kali Linux and Windows 10) software were installed and the firewall is activated with each machine as depicted in "Fig. 2". Moreover, this OS software served as a target or victim machine throughout the test.

The HiddenEye, Ngrok, and Bitly are the main tools that were used to conduct the penetration test. The HiddenEye modern tool requires PHP and Python3 to be installed. The We have installed Ngrok tool on Kali machine, as one of the penetration testing tools during the victim exploitation process.

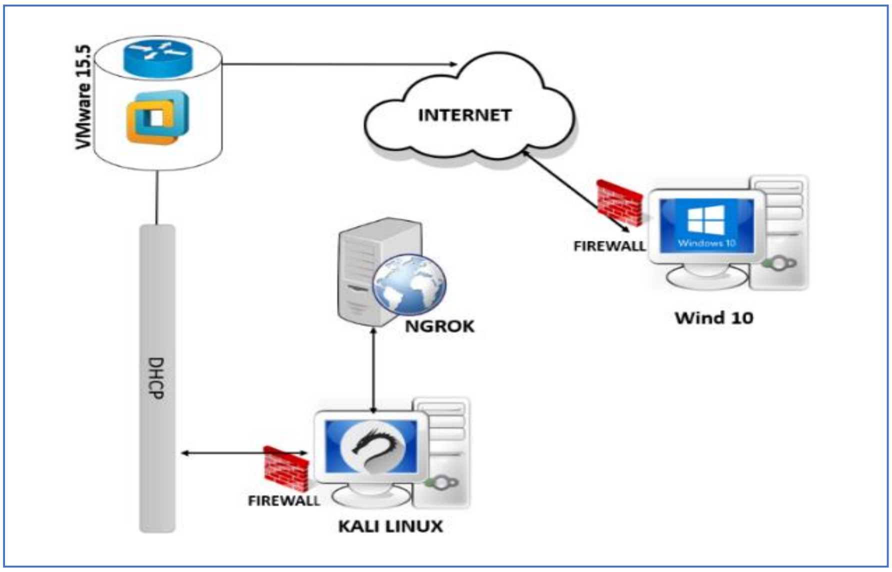
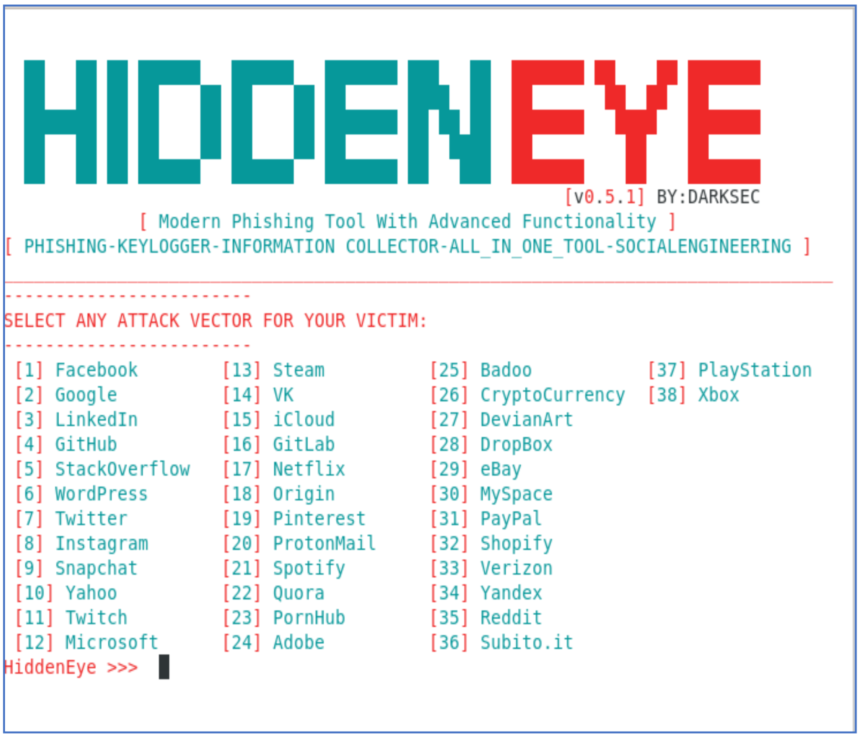


Fig. 2: Laboratory Infrastructure

EXPERIMENTAL RESULTS

In this section, the implementation of phishing attack of the proposed model is presented with the obtained results. Such an attack is carried out as following:

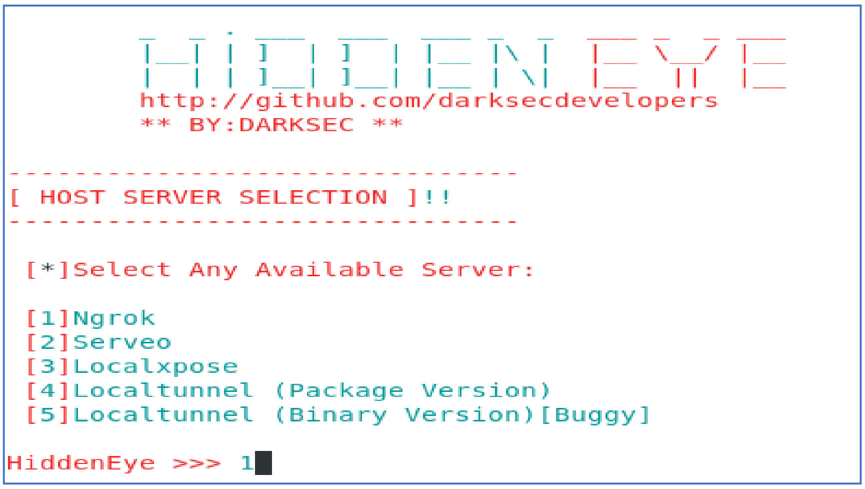
- Step 1: the phishing attack is started by downloading the hiddeneye tool. We have selected the Google site to test the username and password against broken based on the hiddeneye sequence number which is 2 for the Google service as shown in "Fig. 3".



```
HIDDENEYE
                                                    [v0.5.1] BY:DARKSEC
              [ Modern Phishing Tool With Advanced Functionality ]
[ PHISHING-KEYLOGGER-INFORMATION COLLECTOR-ALL_IN_ONE_TOOL-SOCIALENGINEERING ]
________________________________________________________________________________
------------------------
SELECT ANY ATTACK VECTOR FOR YOUR VICTIM:
------------------------
 [1] Facebook        [13] Steam          [25] Badoo            [37] PlayStation
 [2] Google          [14] VK             [26] CryptoCurrency   [38] Xbox
 [3] LinkedIn        [15] iCloud         [27] DevianArt
 [4] GitHub          [16] GitLab         [28] DropBox
 [5] StackOverflow   [17] Netflix        [29] eBay
 [6] WordPress       [18] Origin         [30] MySpace
 [7] Twitter         [19] Pinterest      [31] PayPal
 [8] Instagram       [20] ProtonMail     [32] Shopify
 [9] Snapchat        [21] Spotify        [33] Verizon
 [10] Yahoo          [22] Quora          [34] Yandex
 [11] Twitch         [23] PornHub        [35] Reddit
 [12] Microsoft      [24] Adobe          [36] Subito.it
HiddenEye >>> █
```

Fig. 3: Selecting Google Page

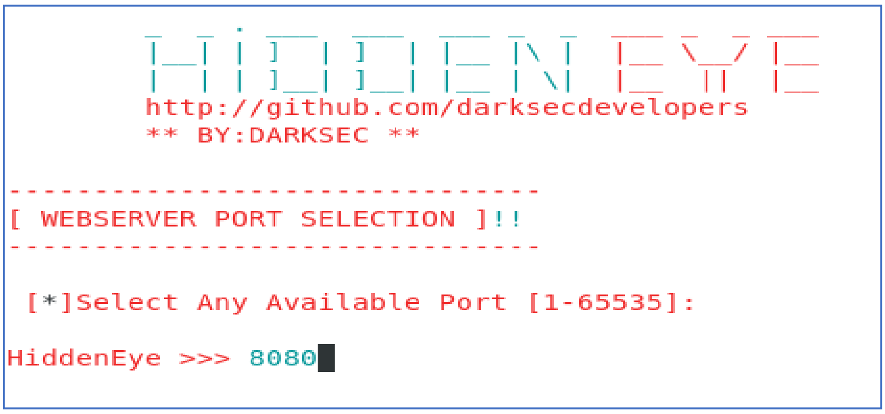
- Step 2, Ngrok tool (multiplatform tunneling) is selected as reverse proxy software to establishe secure tunnels from a public endpoint such as Internet to a locally running network service while capturing all traffic for detailed inspection and replay [8]. "Fig. 4" shows establishing secure tunnels.



```
http://github.com/darksecdevelopers
** BY:DARKSEC **

--------------------------------
[ HOST SERVER SELECTION ]!!
--------------------------------

 [*]Select Any Available Server:

 [1]Ngrok
 [2]Serveo
 [3]Localxpose
 [4]Localtunnel (Package Version)
 [5]Localtunnel (Binary Version)[Buggy]

HiddenEye >>> 1
```

Fig. 4: Establishing Secure Tunnels.

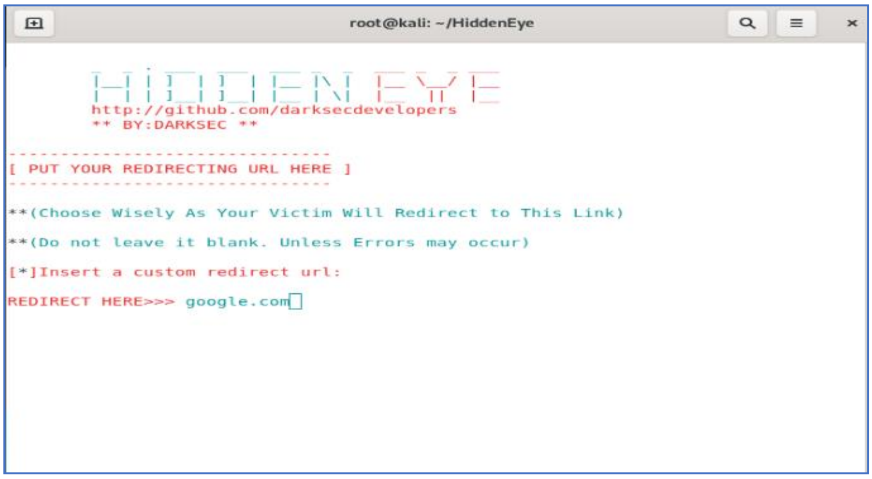
- Step 3: Identifying reverse connecting port of the victim machine for making redirects connection via port 8080 using Ngrok tool for Kali Linux machine with domain generator. "Fig. 5" shows the implantation of this task.



```
http://github.com/darksecdevelopers
** BY:DARKSEC **

--------------------------------
[ WEBSERVER PORT SELECTION ]!!
--------------------------------

 [*]Select Any Available Port [1-65535]:

HiddenEye >>> 8080
```

Fig.5: Redirecting Connection Port

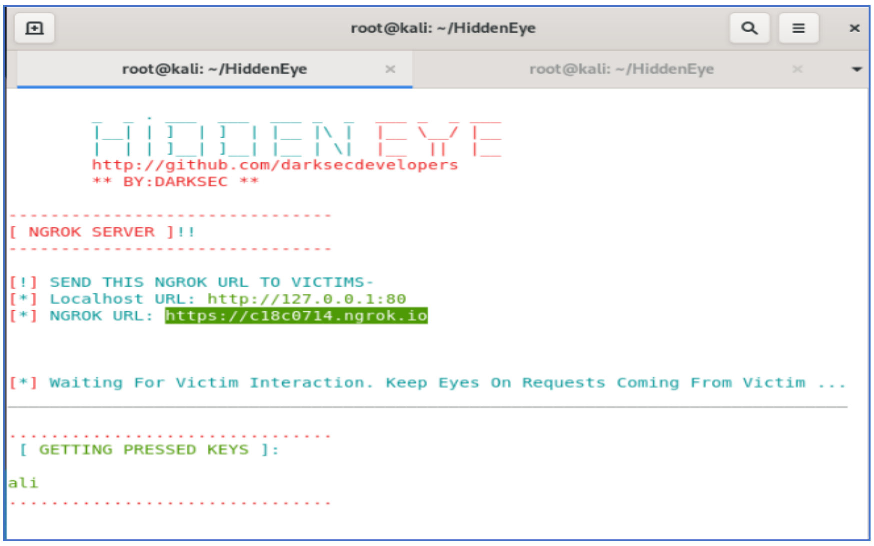
- Step 4: Inserting a custom redirect URL 'google.com' as shown in "Fig. 6".



```
http://github.com/darksecdevelopers
** BY:DARKSEC **

--------------------------------
[ PUT YOUR REDIRECTING URL HERE ]
--------------------------------

**(Choose Wisely As Your Victim Will Redirect to This Link)

**(Do not leave it blank. Unless Errors may occur)

[*]Insert a custom redirect url:

REDIRECT HERE>>> google.com
```

Fig. 6: Redirecting URL

- Step 5: A new URL is generated as shown in "Fig. 7". Then, it will be hided using bitly tool, that make the victim does not expect that such a link is sent from a server as shown in "Fig. 8". The hidden URL is sent either by creating a fake-email or through social media to make the user of a victim website clicking the link to confirm some information.



```
        http://github.com/darksecdevelopers
        ** BY:DARKSEC **

------------------------------
[ NGROK SERVER ]!!
------------------------------

[!] SEND THIS NGROK URL TO VICTIMS-
[*] Localhost URL: http://127.0.0.1:80
[*] NGROK URL: https://c18c0714.ngrok.io


[*] Waiting For Victim Interaction. Keep Eyes On Requests Coming From Victim ...

..............................
 [ GETTING PRESSED KEYS ]:

ali
..............................
```

Fig. 7: Generating URL by Ngrok.

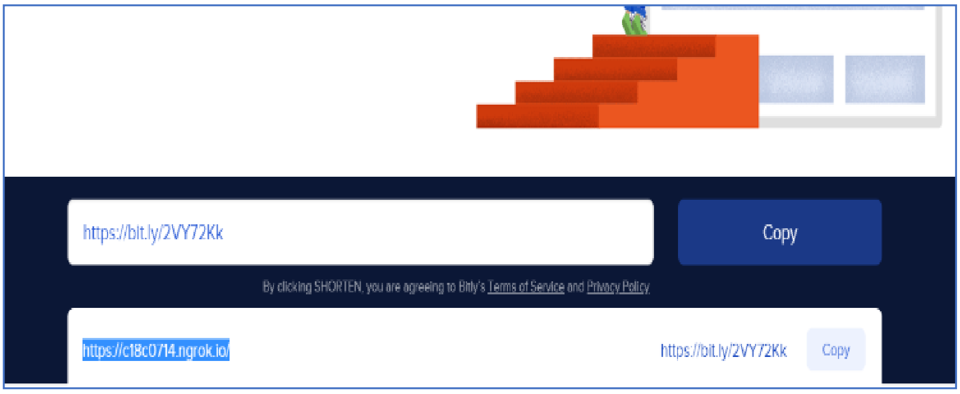
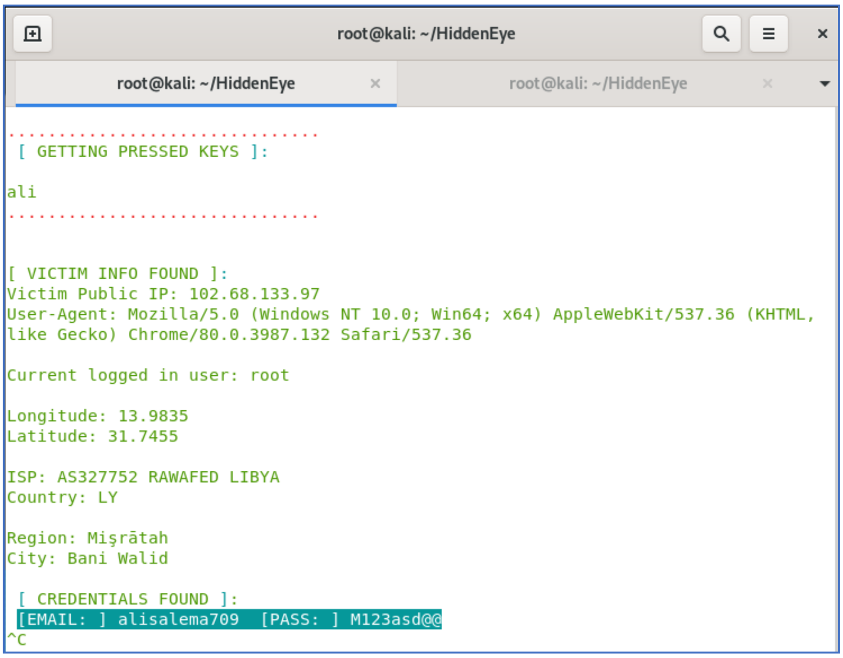

https://bit.ly/2VY72Kk
Copy
By clicking SHORTEN, you are agreeing to Bitly's Terms of Service and Privacy Policy
https://c18c0714.ngrok.io/
https://bit.ly/2VY72Kk
Copy

Fig. 8: Hiding the URL.

• Step 6: Finally, once the link is clicked by the victim, then user name and the password are obtained using hiddeneye tool. Moreover, specifications of the victim's device, the public IP, and the state/country are displayed as shown in the "Fig. 10".



```
..............................
 [ GETTING PRESSED KEYS ]:

ali
..............................


[ VICTIM INFO FOUND ]:
Victim Public IP: 102.68.133.97
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/80.0.3987.132 Safari/537.36

Current logged in user: root

Longitude: 13.9835
Latitude: 31.7455

ISP: AS327752 RAWAFED LIBYA
Country: LY

Region: Mişrātah
City: Bani Walid

 [ CREDENTIALS FOUND ]:
 [EMAIL: ] alisalema709  [PASS: ] M123asd@@
^C
```

Fig. 9: The Result of the Success Attack

COUNTERMEASURES

The victim machine became compromised. So, the below proposed techniques should be considered and highly recommended as countermeasures to make a victim machine protected from phishing attack. Such techniques are listed as following:

- To make a victim machine protected from the pop-up phishing, users should avoid the responding for the popup windows that appear spontaneously and clicking a hyperlink. Moreover, block pop-ups in the browser settings and always log out of the banking sessions and other sensitive accounts as soon as the work is completed [9].
- Filter emails for phishing threats using multi software tools to detect a lot of malwares in an email and to detect known malicious URLs and security analytics to alert on unknown ones such as 'Rapid7 UserInsight' tool.
- Updating client-side, software, and plug-ins in
- Updating the operating systems, browsers, and its plug-ins such as Flash and Java. This is required due to some phishing emails include URLs to exploit vulnerabilities.
- Implementing 2-factor authentication and adding 2-factor authentication (2FA) to any external device to stop attackers from using stolen passwords.
- Training employees on security awareness due to any phishing attack can succeed only if a target victim clicks on the link. So, creating awareness and educating the employees and other users about the types of phishing attacks in the network is the best way to prevent phishing attacks.
- Reading sender’s email address carefully is also a way to prevent phishing attacks.
- Copying and pasting characters in an email address in the notepad to check the use of numeric or special characters.
- Checking the website address to avoid a fake address which is a very similar to the real one. For example, there is a typo in the link that people can easily miss: 'www.citiibank.com' instead of 'www.citibank.com', and ‘amazon.com,’ that will be redirected to ‘arnazon.com’, which belongs to the attacker.

CONCLUSIONS

We have presented a penetration testing model for phishing attack. Such a model was implemented and suitable counter measures were defined. We have found that security methodologies and tools, if properly utilized, can prove their usefulness for understanding the weaknesses of the network or system and how they might be exploited. Penetration testing is not an alternative to other security measures however, it can be used to complement the defence in depth principle. Moreover, the use of old systems should be avoided as it may have serious vulnerabilities.

Absolute security cannot be achieved, this is one of the fundamental principles of security, but a high rate of safety could be achieved through the implementation of network penetration testing periodically. Therefore, penetration testing techniques is very useful for building strategies for measuring the extent of securing data in order to improve the management performance, through the filtration of data.

Finally, in order to perform a successful penetration tests, the underlying methodology should use different security tools.

REFERENCES

[1] L. Irwin, "The 5 most common types of phishing attack," July.09.2019. Available: https://www.itgovernance.eu/blog/en/the-5-most-common-types-of-phishing-attack. [Accessed Dec.26.2019].

[2] H. Farag. and A. Almarimi, "Investigation of Threats for Common Network Attacks," In the Proceeding of LICTEE2019'02, Tripoli, Libya, Mar, 2019.

[3] Apwg, "Phishing Activity Trends Reports," Oct.26.2019. Available: https://apwg.org/trendsreports/. [Accessed: Dec.25.2019].

[4] Maria V. and other, "Spam and phishing in Q2 2019," Nov.26.2019. Available: https://securelist.com/spam-and-phishing-in-q2-2019/92379/ [Accessed: Dec.30.2019].

[5] Maria V. and other, "Spam and phishing in Q3 2019," Nov.26.2019. Available: https://securelist.com/spam-report-q3-2019/95177/ [Accessed: Dec.30.2019].

[6] S. Phirashisha, G. Mary, K. Ushamary, S. Bobby. "Phishing-An Analysis on the Types, Causes, Preventive Measuresand Case Studies in the Current Situation," Journal of Computer Engineering (IOSR), p-ISSN: 2278-8727, 2015, PP. 01-08.

[7] B. Jan-Willem, M. Lorena, J. Marianne, H. Pieter, "Spear phishing in organisations explained," Information and Computer Security. 25. 00-00. 10.1108/ICS-03-2017-0009, 2017, pp. 593-613.

[8] "Ngrok," Dec.3.2019. [online]. Available: https://ngrok.com/product. [Accessed: Dec.30.2019].

[9] B. Gupta, A. Nalin, P. Kostas. "Defending against Phishing Attacks: Taxonomy of Methods, Current Issues and Future Directions," Telecommunication Systems. 2017, 10.1007/s11235-017-0334-z.