Phishing Attack on Websites

Almuteb, Amal Nasier ; Premsagar, Gutha ; Sree choudari, Sunkara
analmuteb1s@semo.edu, pgutha1s@semo.edu, ssunkara1s@semo.edu
Southeast Missouri State University
Cape Girardeau, MO, 63701

Abstract: ***This report gives you a brief view of out project Phishing attack on websites, we attack various kinds of websites and clone the website and steal login credential information from the user without their conscience Users' passwords are stored in secure systems by using some special algorithms known as "hashing." But hackers are well trained to crack any kind of algorithms and secure firewalls. in the same way, we came up with one of the fake website phishing attack concept where hackers can steal login credentials by sending a fake cloned website instead of the genuine website, a pity user enters their login credentials and after submitting them the page refreshes immediately and redirect to the genuine website from fake cloned one. in this refresh moment login credentials are sent to hackers and a genuine site appears Hackers try to access these passwords using different techniques, using a few hacking concepts in the Kali Linux operating system. we will manipulate users' views on a website and then after user entering their details, we extract their information without user consciousness.***

Keywords: Phishing, Security, Malware, Social engineering, Spam

I. INTRODUCTION

This Project report will demonstrate how to apply a few hacking concepts and tools available in Kali Linux using any virtual machine or in the direct operating system. one of the major tools we used for making this phishing attack is SET that is social engineering tool kit. It specifically designed to perform advanced attacks against the human element. In this kit a powerful attribute of Social Engineering is also included, it is a kind of attack targeting human behavior by manipulating and playing with their trust, with the aim to gain confidential information, such as banking account, social media, email, even access to the target computer.

II. APPLICATION AND PROTECTION

Cybercriminals are finding it more difficult to maintain the malicious URLs and deceptive domains used for phishing attacks for more than a few hours because the action is being taken to remove them from the internet much more quickly, That doesn't mean that phishing -- one of the most common means of performing cyber-attacks -- is any less dangerous, but a faster approach to dealing with the issue is starting to hinder attacks. In our application we need to use SET to initialize social engineering tool so that we can attack website vectors by using credential harvester method through site cloner, form there we clone a desired website to get user credentials without user conscious to acquire their data.

When a social engineering attack is performed, the weakest link in the chain is not the computer system, the firewall, services, or apps. It's us, the humans behind those technologies.   1.Develop a security policy that includes but isn't limited to password expiration and complexity. 2.Deploy a web filter to block malicious websites. Require encryption for users with more complexity. 3.broken authentication of sensitive data exposure should be restricted   4.Redirect malicious outbound communication to internal sinkholes to identify and block compromised hosts. 5.being alert and recognize what we are doing and on what website we are logging in

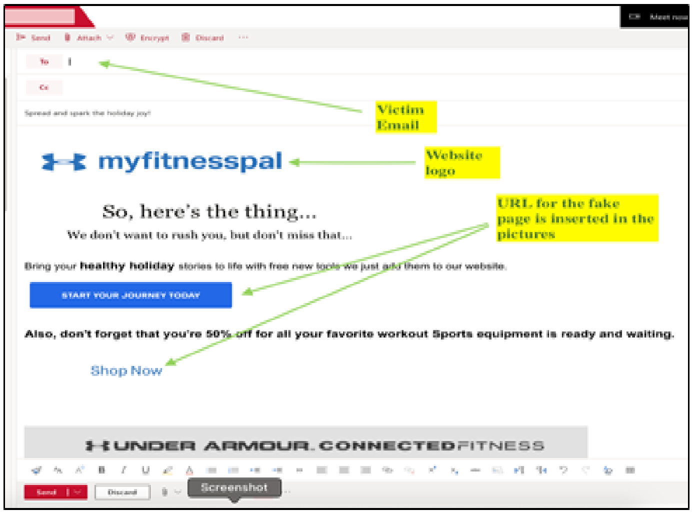
III. EXECUTION

In general, A basic phishing attack attempts to trick a user into entering personal details or other confidential information, and email is the most common method of performing these attacks. We involved Kali Linux using Setoolkit and social engineering tools to clone and attack website vectors to extract user Login credentials. It is a Multi-platform, It can run on Linux, Unix, and Windows that Support integration with third-party modules Allows multiple tweaks from the configuration menu.

IV. DESIGN OF EXPERIMENTS

A. The hacker sends a phishing email and encourages the victim to click on a link and perform a task

We generally made some lengths to make the email seem legitimate. For example, the logos and important titles. there are also some discounts and deadlines in the message, to encourage the victim to act quickly.



Spread and spark the holiday joy!

So, here's the thing...

We don't want to rush you, but don't miss that...

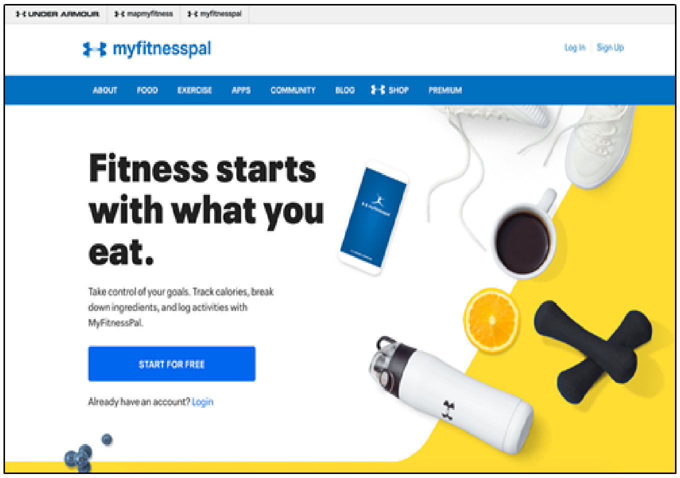
Bring your **healthy holiday** stories to life with free new tools we just add them to our website.

Also, don't forget that you're 50% off for all your favorite workout Sports equipment is ready and waiting.

Fig 1

B. The link takes the victim to a web page.

Much like the phishing email, the web page will look legitimate. We elaborated phishing schemes is to make a replica of a real website that the user has used frequently to track his/her diet and fitness, and we choose this website: https://www.myfitnesspal.com , which is one of the most popular web-based exercises and fitness social media applications by calculating and track daily diet and workout.



Fitness starts with what you eat.

Take control of your goals. Track calories, break down ingredients, and log activities with MyFitnessPal.

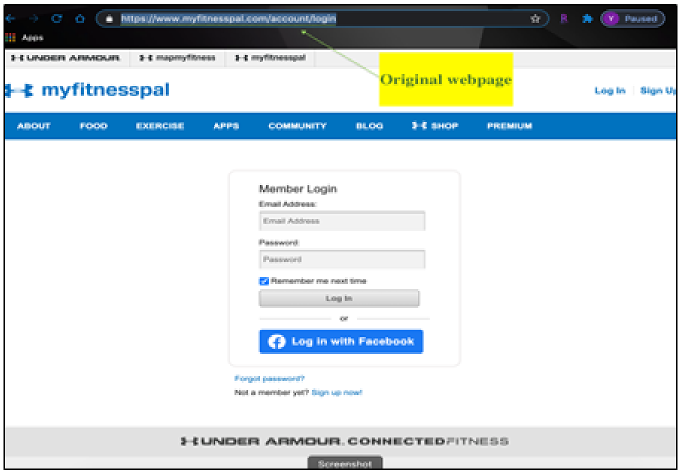
Already have an account? Login

Fig 2

C. The victim tricked into entering the email address and password.

Usually, the original page will be re-directed without the user noticing. so the user will assume it's some internet connection issue and try to login again but this time it will work as a regular normal genuine website. when the refresh happens two things occur first one is the credentials will be sent to hackers in the backend and secondly the fake page will be redirected to the genuine site so that user will not feel any suspicious

Original genuine page



https://www.myfitnesspal.com/account/login

Member Login

Email Address: Email Address

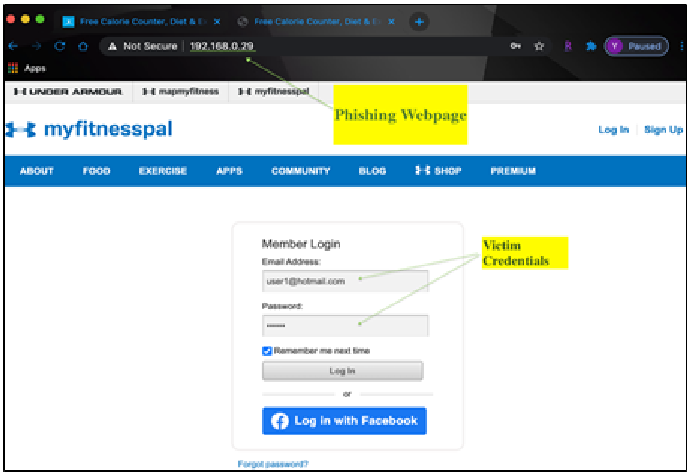
Password: Password

☑ Remember me next time

Not a member yet? Sign up now!

Fig 3

Fake cloned webpage



Not Secure | 192.168.0.29

Member Login

Email Address: user1@hotmail.com

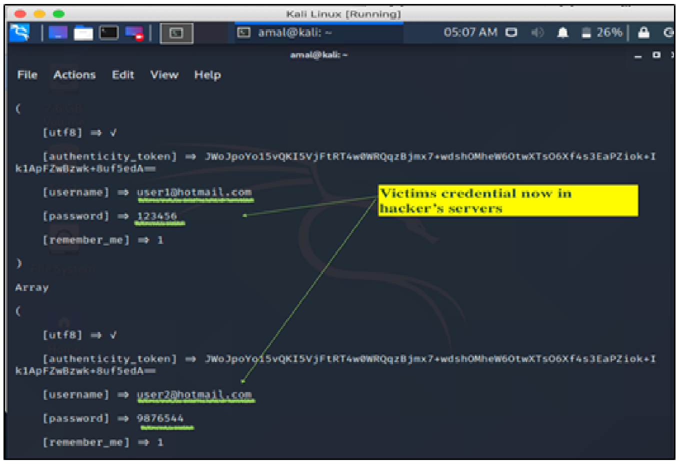
Password: •••••••

☑ Remember me next time

Fig 4

D. The hacker retrieves the password from his server

The webpage might be a clone of something legitimate, but the back end of it is set to send information right to the hacker server

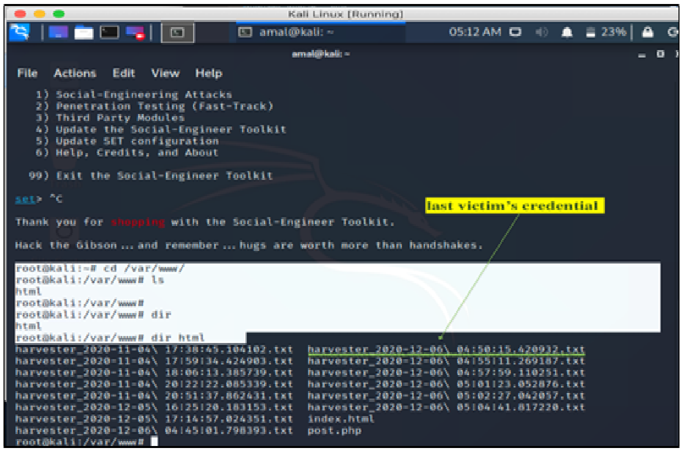


```
(
    [utf8] => √
    [authenticity_token] => JWoJpoYo15vQKI5VjFtRT4w0WRQqzBjmx7+wdshOMheW6OtwXTsO6Xf4s3EaPZiok+I
k1ApFZwBzwk+8uf5edA==
    [username] => user1@hotmail.com
    [password] => 123456
    [remember_me] => 1
)
Array
(
    [utf8] => √
    [authenticity_token] => JWoJpoYo15vQKI5VjFtRT4w0WRQqzBjmx7+wdshOMheW6OtwXTsO6Xf4s3EaPZiok+I
k1ApFZwBzwk+8uf5edA==
    [username] => user2@hotmail.com
    [password] => 9876544
    [remember_me] => 1
```

Fig 5

E. The hacker exploits the victim's harvested credentials.

Once they have them, the hacker can save it in files and use the harvested credentials in a number of ways including gaining access to the victim information to track him or use his bank card which is saved on the website to buy anything through the website or steal his bank information



```
   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> ^C

Thank you for shopping with the Social-Engineer Toolkit.

Hack the Gibson ... and remember ... hugs are worth more than handshakes.

root@kali:~# cd /var/www/
root@kali:/var/www# ls
html
root@kali:/var/www#
root@kali:/var/www# dir
html
root@kali:/var/www# dir html
harvester_2020-11-04\ 17:38:45.104102.txt  harvester_2020-12-06\ 04:50:15.420932.txt
harvester_2020-11-04\ 17:59:34.424903.txt  harvester_2020-12-06\ 04:55:11.269187.txt
harvester_2020-11-04\ 18:06:13.385739.txt  harvester_2020-12-06\ 04:57:59.110251.txt
harvester_2020-11-04\ 20:22:22.085339.txt  harvester_2020-12-06\ 05:01:23.052876.txt
harvester_2020-11-04\ 20:51:37.862431.txt  harvester_2020-12-06\ 05:02:27.042057.txt
harvester_2020-12-05\ 16:25:20.183153.txt  harvester_2020-12-06\ 05:04:41.817220.txt
harvester_2020-12-05\ 17:14:57.024351.txt  index.html
harvester_2020-12-06\ 04:45:01.798393.txt  post.php
root@kali:/var/www# █
```

Fig6

V. METRICS AND MEASUREMENTS

VI. FUTURE WORK

Similar techniques are used in other scams in which attackers claim to be from a bank or other financial institution looking to verify details, online shops attempting to verify non-existent purchases or sometimes -- even more cheekily -- attackers will claim to be from tech security companies and that they need access to information in order to keep their customers safe. similarly, we can use this work to use hack another important website which is very tough to go through and get lots of information and steal all data as well as money form users bank accounts

Other scams, usually more sophisticated, aimed at business users. Here we attackers might also pose as someone from within the same organization or one of its suppliers and will ask you to download an attachment that they claim contains information about a contract or deal. In some cases, the aim may be to harvest personal data, but in many cases, it's also used to deploy ransomware or rope systems into a botnet. There are many ways like these to steal any kind of information and finance as well,world is huge there is billions of ob gigabytes of data to hack all we need is an innocent victim and the right time and platform to hack

VII.CONCLUSION

A phishing attack on a website, cloned fake website Pretends to be trusted entity to steal information and attack your information like bank accounts and Gmail and some other social media pages and accounts where kali Linux plays a significant role to process this and make a phishing attack. Phishers continue to be successful as their attack methods are constantly evolving and users frequently disregard the recommendations provided by expert systems. A typical phishing attack includes an email and an attachment. The email contains information that is specific to the end-user and an attachment looks genuine to the user. The designing of the message is done in such a manner so as to allure the user in carrying out the intended tasks by a phished. There are many issues and security risks that are associated with such types of attacks.

VII. REFERENCES

[1] Hong, J. (2012). The state of phishing attacks. *Communications of the ACM*, *55*(1), 74-81.

[2] Ramzan, Z. (2010). Phishing attacks and countermeasures. In Handbook of information and communication security (pp. 433-448). Springer, Berlin, Heidelberg.

[3] Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

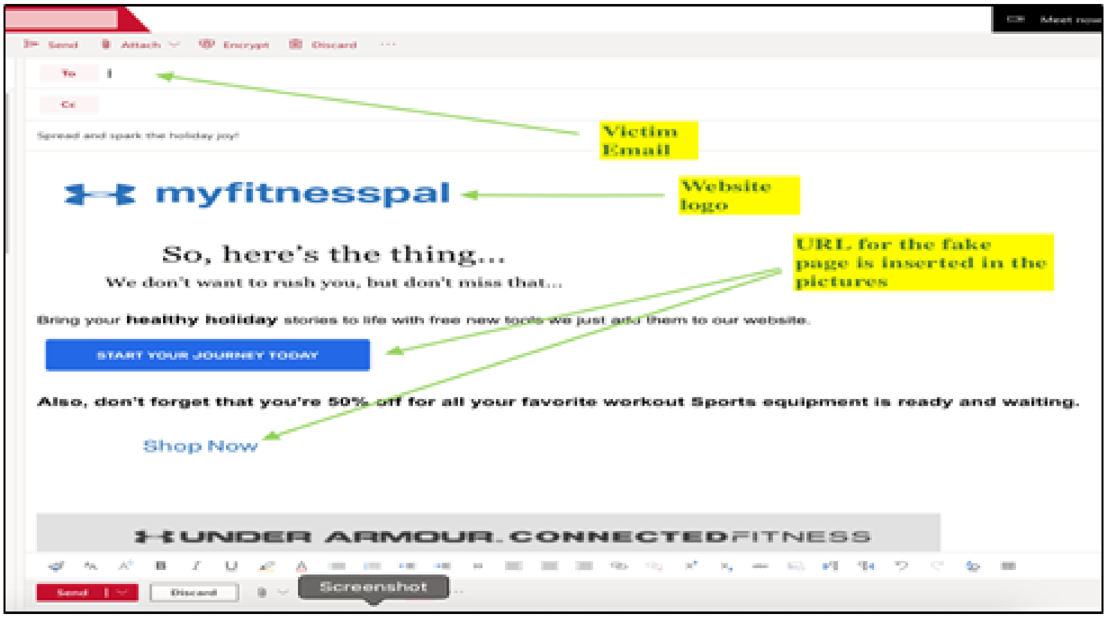
[4] Pavković, N., & Perkov, L. (2011, May). Social Engineering Toolkit—A systematic approach to social engineering. In *2011 Proceedings of the 34th International Convention MIPRO* (pp. 1485-1489). IEEE.

[5] Al-tarawneh, A. M., & Al-Hamami, A. H. SOCIAL ENGINEERING ATTACK USING SETOOLKIT PACKGES IN KALI LINUX-IP ADRESS APPROACH.

[6] Jakobsson, M. (2005, February). Modeling and preventing phishing attacks. In *Financial Cryptography* (Vol. 5).

Image Reference:

Fig1:



Spread and spark the holiday joy!

myfitnesspal

So, here's the thing...

We don't want to rush you, but don't miss that...

Bring your **healthy holiday** stories to life with free new tools we just add them to our website.

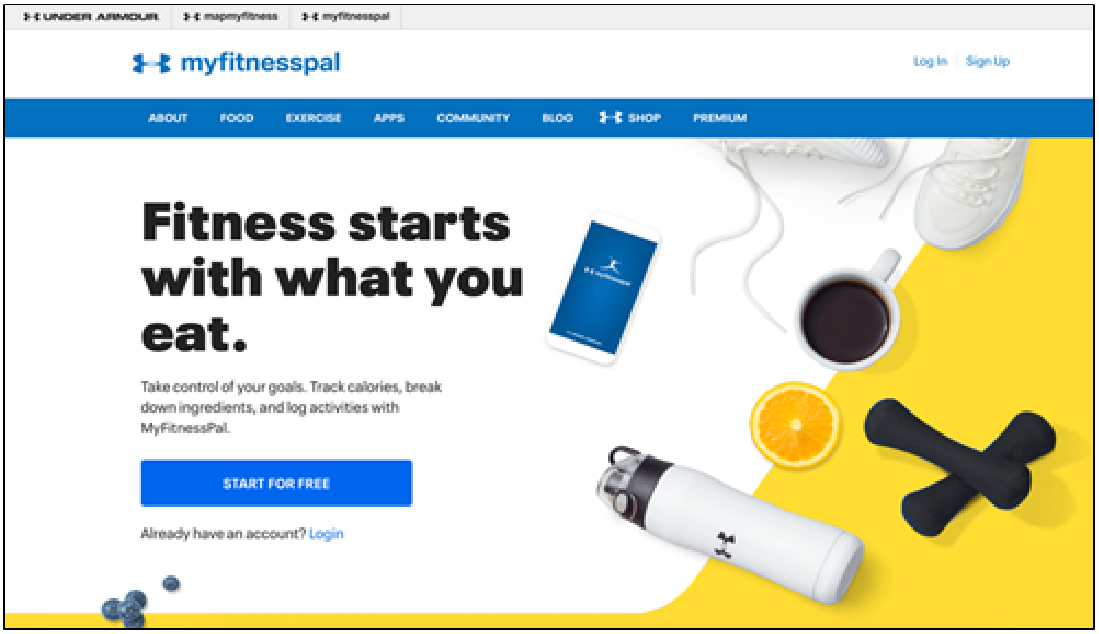
START YOUR JOURNEY TODAY

Also, don't forget that you're 50% off for all your favorite workout Sports equipment is ready and waiting.

Shop Now

UNDER ARMOUR. CONNECTEDFITNESS

Fig 2:



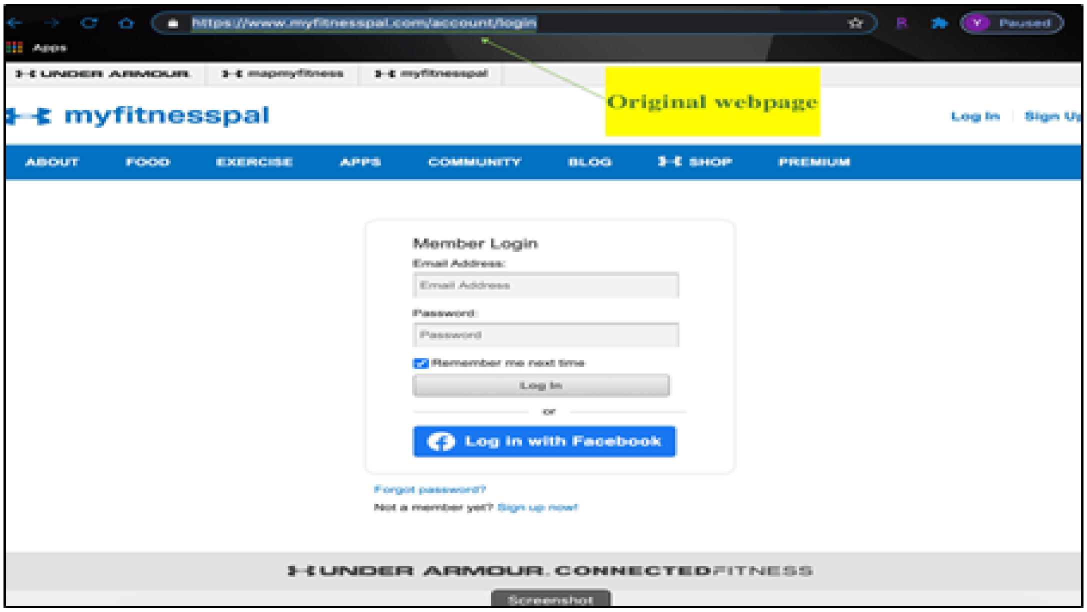
Fitness starts with what you eat.

Take control of your goals. Track calories, break down ingredients, and log activities with MyFitnessPal.

START FOR FREE

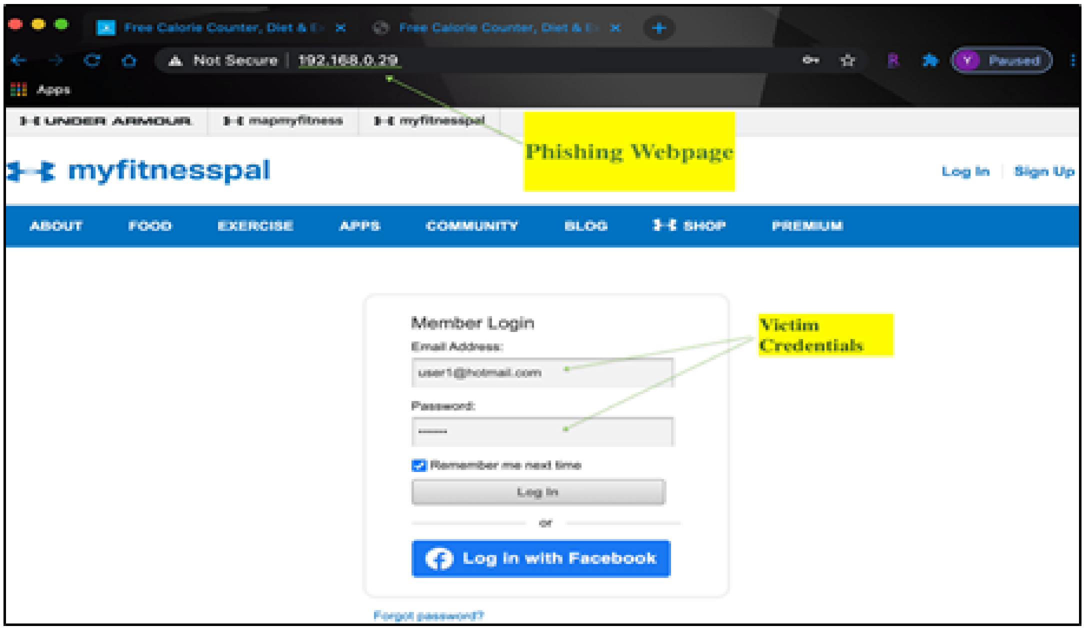
Already have an account? Login

Fig 3:



https://www.myfitnesspal.com/account/login

Fig 4:

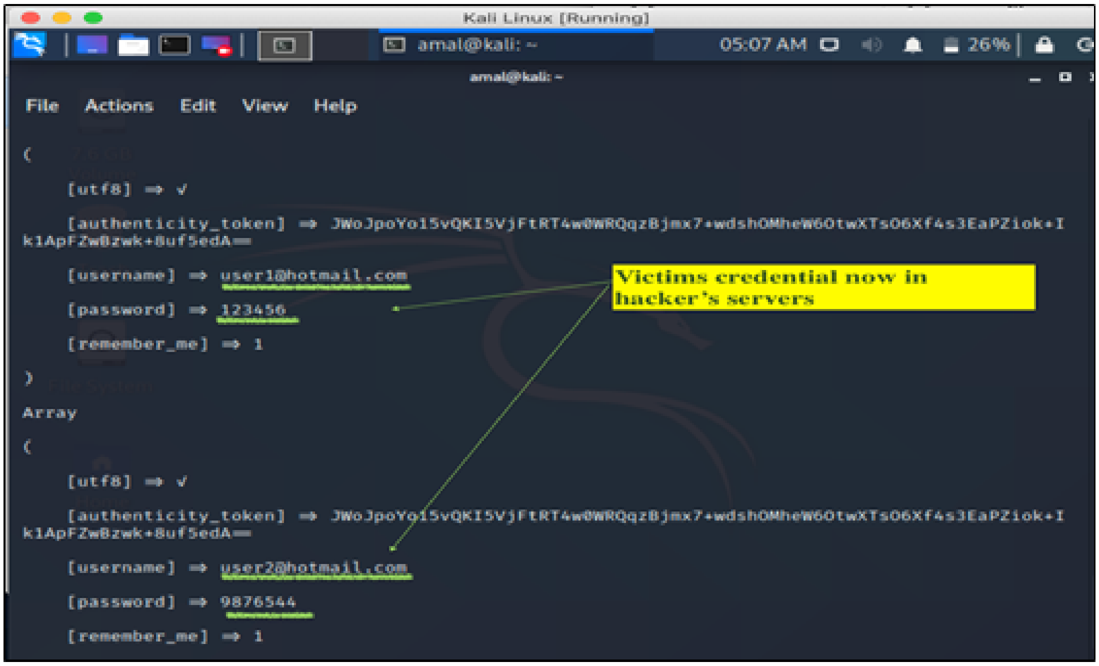


Not Secure | 192.168.0.29

Email Address: user1@hotmail.com

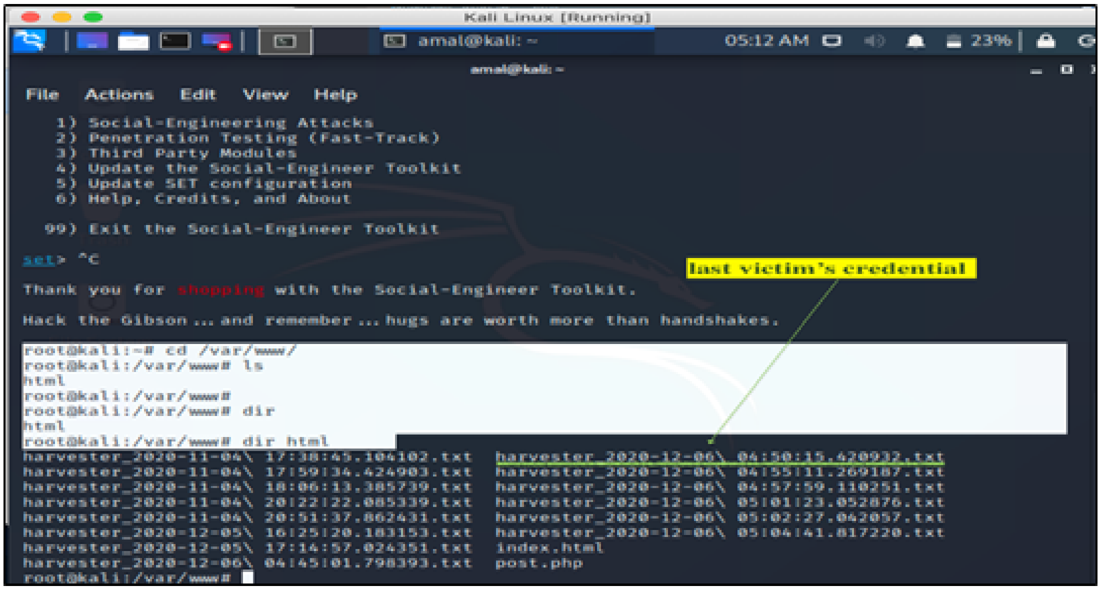
Password: •••••••

Fig 5:



```
(
    [utf8] ⇒ √
    [authenticity_token] ⇒ JWoJpoYo15vQKI5VjFtRT4w0WRQqzBjmx7+wdshOMheW6OtwXTsO6Xf4s3EaPZiok+I
k1ApFZwBzwk+8uf5edA==
    [username] ⇒ user1@hotmail.com
    [password] ⇒ 123456
    [remember_me] ⇒ 1
)
Array
(
    [utf8] ⇒ √
    [authenticity_token] ⇒ JWoJpoYo15vQKI5VjFtRT4w0WRQqzBjmx7+wdshOMheW6OtwXTsO6Xf4s3EaPZiok+I
k1ApFZwBzwk+8uf5edA==
    [username] ⇒ user2@hotmail.com
    [password] ⇒ 9876544
    [remember_me] ⇒ 1
```

Fig 6:



```
    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> ^C

Thank you for shopping with the Social-Engineer Toolkit.

Hack the Gibson ... and remember ... hugs are worth more than handshakes.

root@kali:~# cd /var/www/
root@kali:/var/www# ls
html
root@kali:/var/www#
root@kali:/var/www# dir
html
root@kali:/var/www# dir html
harvester_2020-11-04\ 17:38:45.104102.txt  harvester_2020-12-06\ 04:50:15.420932.txt
harvester_2020-11-04\ 17:59:34.424903.txt  harvester_2020-12-06\ 04:55:11.269187.txt
harvester_2020-11-04\ 18:06:13.385739.txt  harvester_2020-12-06\ 04:57:59.110251.txt
harvester_2020-11-04\ 20:22:22.085339.txt  harvester_2020-12-06\ 05:01:23.052876.txt
harvester_2020-11-04\ 20:51:37.862431.txt  harvester_2020-12-06\ 05:02:27.042057.txt
harvester_2020-12-05\ 16:25:20.183153.txt  harvester_2020-12-06\ 05:04:41.817220.txt
harvester_2020-12-05\ 17:14:57.024351.txt  index.html
harvester_2020-12-06\ 04:45:01.798393.txt  post.php
root@kali:/var/www# 
```