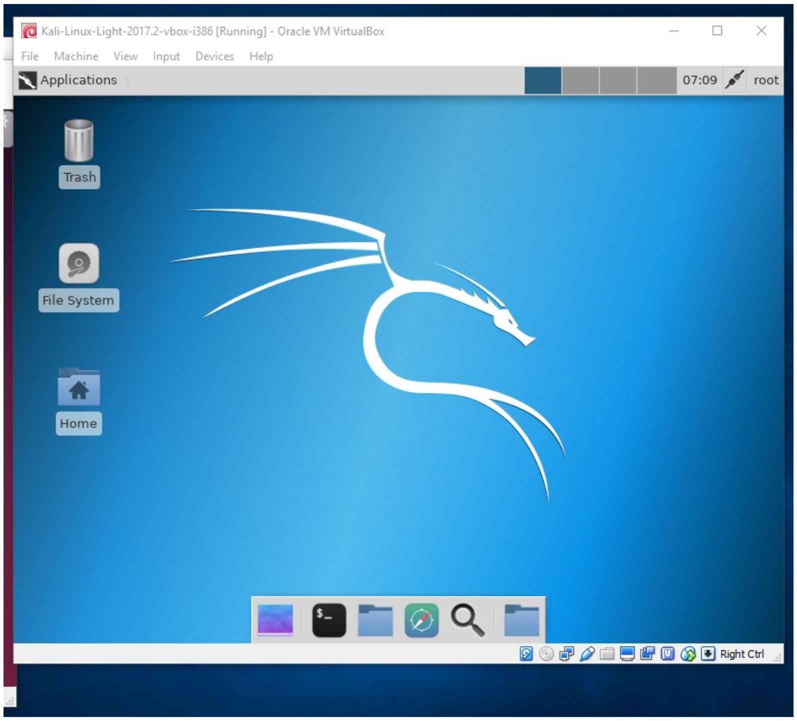
Name: Madara Uciha

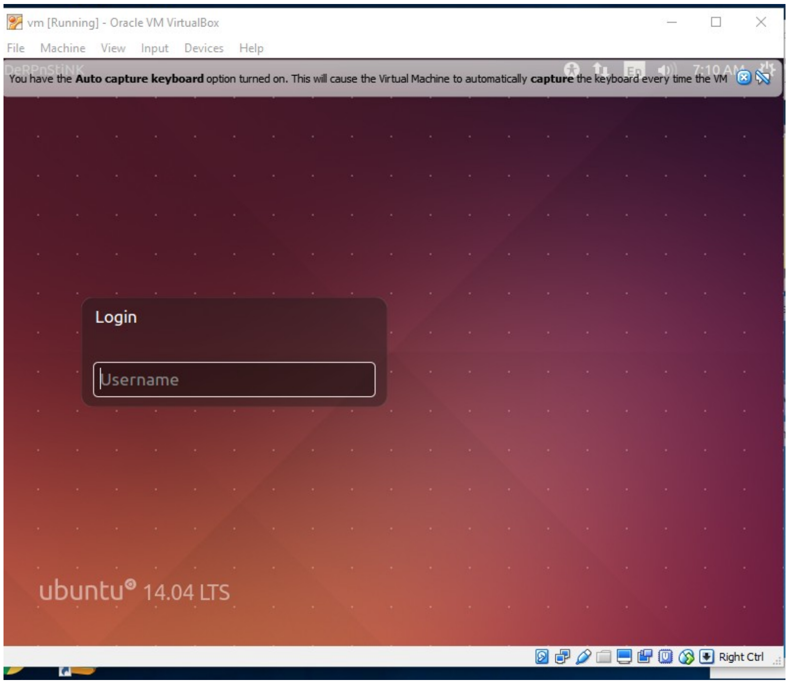
Report Hacking Wordpress Using VirtualBox

If you want to hacking wordpres using virtualbox you can prefare tool virtualbox,kali linux and target ubuntu.

1. You can import kali linux using virtualbox


Kali-Linux-Light-2017.2-vbox-i386 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Applications
07:09
root
Trash
File System
Home
Right Ctrl

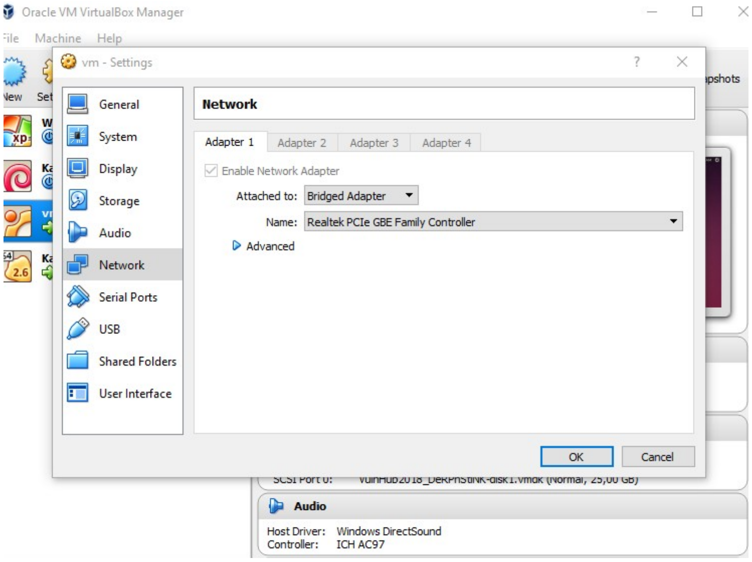
2. And you can import ubuntu target using virtualbox


vm [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
7:10 AM
Login
Username
ubuntu® 14.04 LTS
Right Ctrl

You have the **Auto capture keyboard** option turned on. This will cause the Virtual Machine to automatically **capture** the keyboard every time the VM

Name: Madara Uciha

3. You can setting network for ubuntu target



Network

Adapter 1 | Adapter 2 | Adapter 3 | Adapter 4

☑ Enable Network Adapter

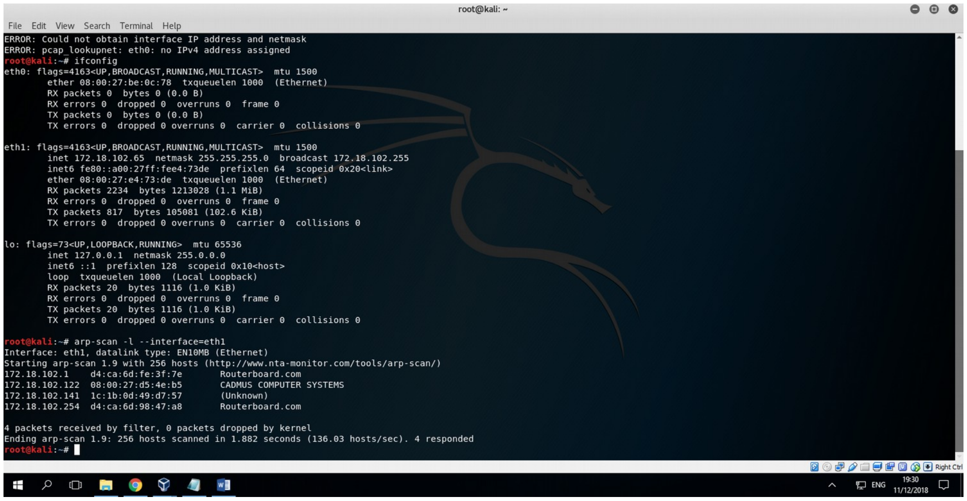
Attached to: Bridged Adapter

Name: Realtek PCIe GBE Family Controller

SCSI Port 0: VulnHub2018_DeRPnStiNK-disk1.vmdk (Normal, 25,00 GB)

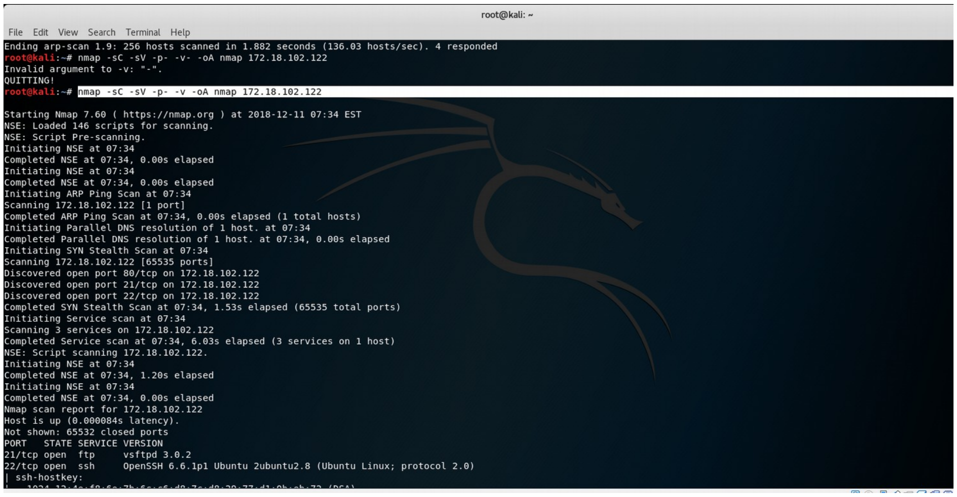
Host Driver: Windows DirectSound
Controller: ICH AC97

4. You can scanning ip target using command “**arp-scan –l --interface=eth1**” because we can get ip your computer

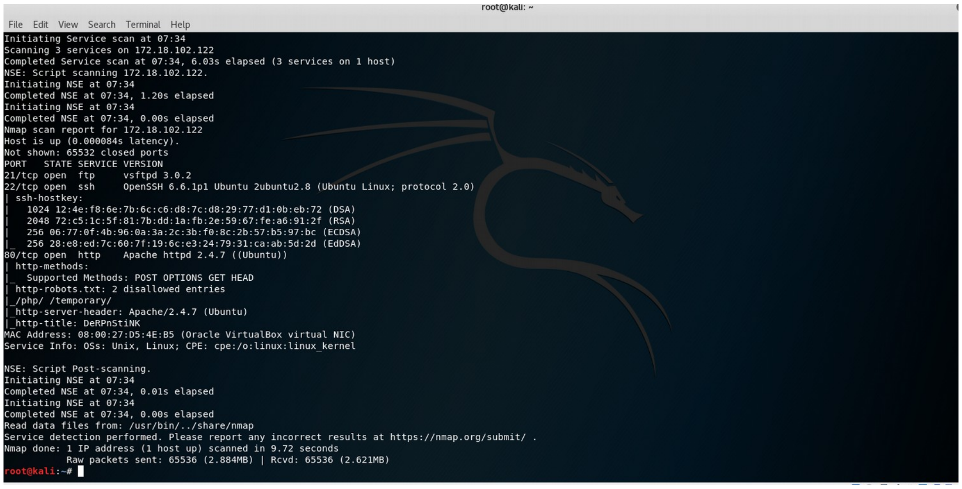


```
ERROR: Could not obtain interface IP address and netmask
ERROR: pcap_lookupnet: eth0: no IPv4 address assigned
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 08:00:27:be:0c:78  txqueuelen 1000  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        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

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.102.65  netmask 255.255.255.0  broadcast 172.18.102.255
        inet6 fe80::a00:27ff:fee4:73de  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:e4:73:de  txqueuelen 1000  (Ethernet)
        RX packets 2234  bytes 1213028 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 817  bytes 105081 (102.6 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 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# arp-scan -l --interface=eth1
Interface: eth1, datalink type: EN10MB (Ethernet)
Starting arp-scan 1.9 with 256 hosts (http://www.nta-monitor.com/tools/arp-scan/)
172.18.102.1    d4:ca:6d:fe:3f:7e       Routerboard.com
172.18.102.122  08:00:27:d5:4e:b5       CADMUS COMPUTER SYSTEMS
172.18.102.141  1c:1b:0d:49:d7:57       (Unknown)
172.18.102.254  d4:ca:6d:98:47:a8       Routerboard.com

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9: 256 hosts scanned in 1.882 seconds (136.03 hosts/sec). 4 responded
root@kali:~# 
```

5. You can running nmap command “nmap -sC -sV -p- -v -oA nmap ip-addr”

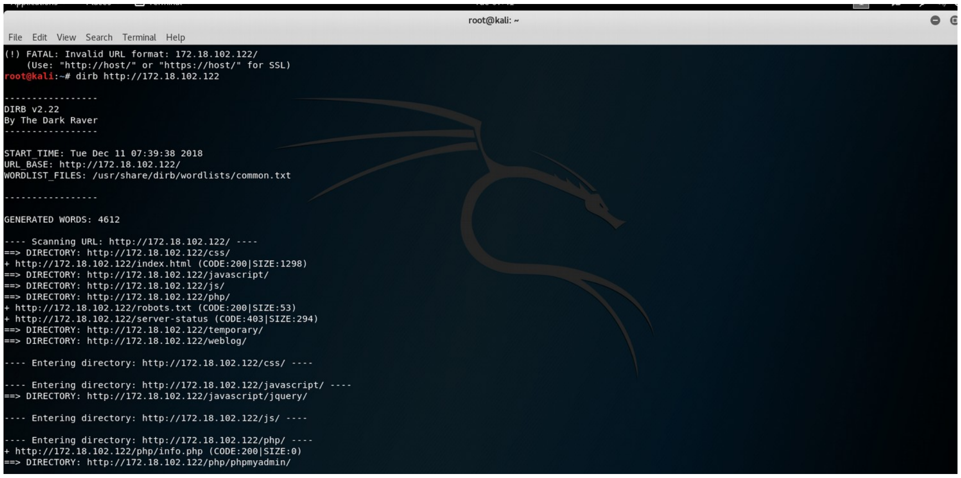


```
Ending arp-scan 1.9: 256 hosts scanned in 1.882 seconds (136.03 hosts/sec). 4 responded
root@kali:~# nmap -sC -sV -p- -v- -oA nmap 172.18.102.122
Invalid argument to -v: "-".
QUITTING!
root@kali:~# nmap -sC -sV -p- -v -oA nmap 172.18.102.122

Starting Nmap 7.60 ( https://nmap.org ) at 2018-12-11 07:34 EST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 07:34
Completed NSE at 07:34, 0.00s elapsed
Initiating NSE at 07:34
Completed NSE at 07:34, 0.00s elapsed
Initiating ARP Ping Scan at 07:34
Scanning 172.18.102.122 [1 port]
Completed ARP Ping Scan at 07:34, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:34
Completed Parallel DNS resolution of 1 host. at 07:34, 0.00s elapsed
Initiating SYN Stealth Scan at 07:34
Scanning 172.18.102.122 [65535 ports]
Discovered open port 80/tcp on 172.18.102.122
Discovered open port 21/tcp on 172.18.102.122
Discovered open port 22/tcp on 172.18.102.122
Completed SYN Stealth Scan at 07:34, 1.53s elapsed (65535 total ports)
Initiating Service scan at 07:34
Scanning 3 services on 172.18.102.122
Completed Service scan at 07:34, 6.03s elapsed (3 services on 1 host)
NSE: Script scanning 172.18.102.122.
Initiating NSE at 07:34
Completed NSE at 07:34, 1.20s elapsed
Initiating NSE at 07:34
Completed NSE at 07:34, 0.00s elapsed
Nmap scan report for 172.18.102.122
Host is up (0.000084s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
```



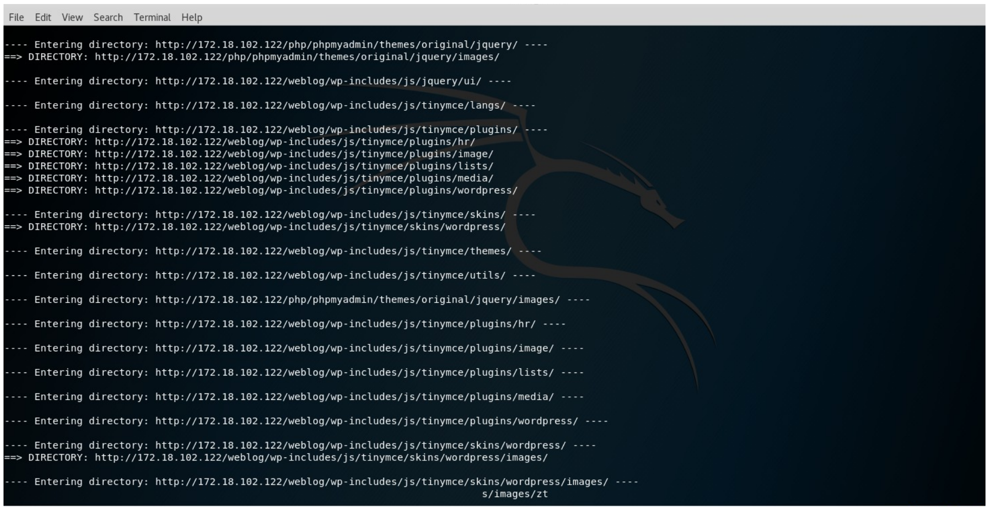
```
Initiating Service scan at 07:34
Scanning 3 services on 172.18.102.122
Completed Service scan at 07:34, 6.03s elapsed (3 services on 1 host)
NSE: Script scanning 172.18.102.122.
Initiating NSE at 07:34
Completed NSE at 07:34, 1.20s elapsed
Initiating NSE at 07:34
Completed NSE at 07:34, 0.00s elapsed
Nmap scan report for 172.18.102.122
Host is up (0.000084s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.2
22/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 12:4e:f8:6e:7b:6c:c6:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
|   2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)
|   256 06:77:0f:4b:96:0a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)
|_  256 28:e8:ed:7c:60:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (EdDSA)
80/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS GET HEAD
| http-robots.txt: 2 disallowed entries
|_/php/ /temporary/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: DeRPnStiNK
MAC Address: 08:00:27:D5:4E:B5 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

NSE: Script Post-scanning.
Initiating NSE at 07:34
Completed NSE at 07:34, 0.01s elapsed
Initiating NSE at 07:34
Completed NSE at 07:34, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.72 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
root@kali:~#
```

6. You can typing command “dirb http://ipaddr”



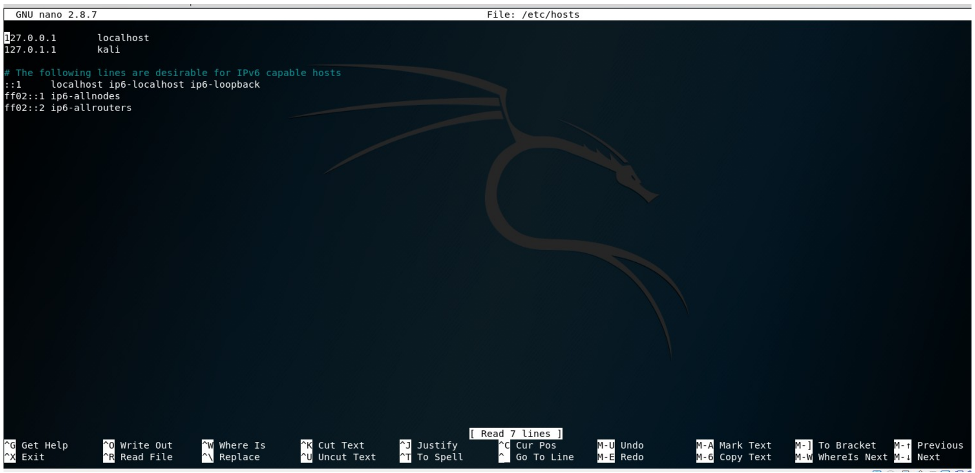
```
(!) FATAL: Invalid URL format: 172.18.102.122/
    (Use: "http://host/" or "https://host/" for SSL)
root@kali:~# dirb http://172.18.102.122

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Dec 11 07:39:38 2018
URL_BASE: http://172.18.102.122/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.18.102.122/ ----
==> DIRECTORY: http://172.18.102.122/css/
+ http://172.18.102.122/index.html (CODE:200|SIZE:1298)
==> DIRECTORY: http://172.18.102.122/javascript/
==> DIRECTORY: http://172.18.102.122/js/
==> DIRECTORY: http://172.18.102.122/php/
+ http://172.18.102.122/robots.txt (CODE:200|SIZE:53)
+ http://172.18.102.122/server-status (CODE:403|SIZE:294)
==> DIRECTORY: http://172.18.102.122/temporary/
==> DIRECTORY: http://172.18.102.122/weblog/

---- Entering directory: http://172.18.102.122/css/ ----

---- Entering directory: http://172.18.102.122/javascript/ ----
==> DIRECTORY: http://172.18.102.122/javascript/jquery/

---- Entering directory: http://172.18.102.122/js/ ----

---- Entering directory: http://172.18.102.122/php/ ----
+ http://172.18.102.122/php/info.php (CODE:200|SIZE:0)
==> DIRECTORY: http://172.18.102.122/php/phpmyadmin/
```

Name: Madara Uciha



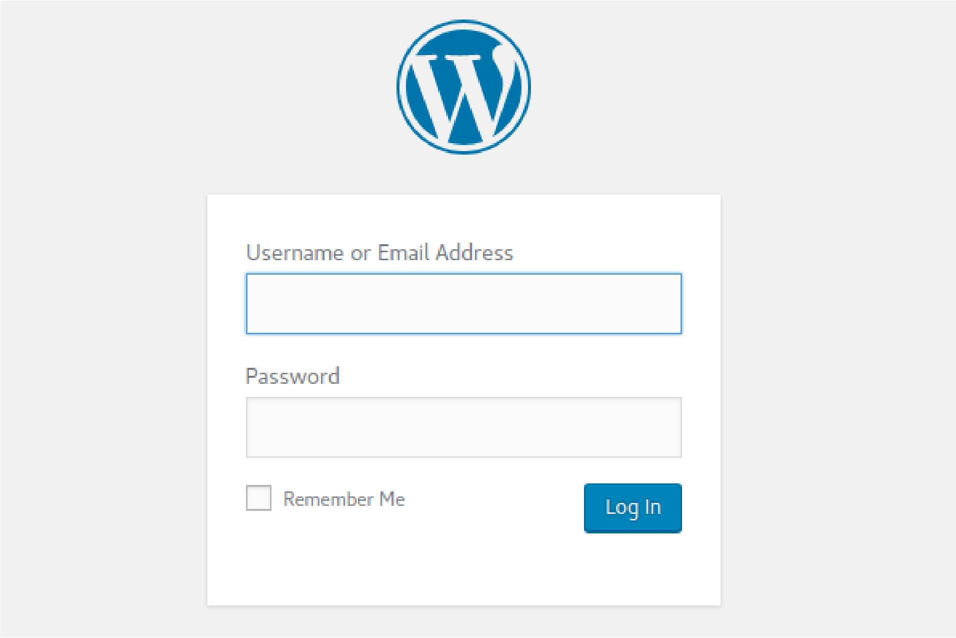
```
---- Entering directory: http://172.18.102.122/php/phpmyadmin/themes/original/jquery/ ----
==> DIRECTORY: http://172.18.102.122/php/phpmyadmin/themes/original/jquery/images/

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/jquery/ui/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/langs/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/ ----
==> DIRECTORY: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/hr/
==> DIRECTORY: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/image/
==> DIRECTORY: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/lists/
==> DIRECTORY: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/media/
==> DIRECTORY: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/wordpress/

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/skins/ ----
==> DIRECTORY: http://172.18.102.122/weblog/wp-includes/js/tinymce/skins/wordpress/

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/themes/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/utils/ ----

---- Entering directory: http://172.18.102.122/php/phpmyadmin/themes/original/jquery/images/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/hr/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/image/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/lists/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/media/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/plugins/wordpress/ ----

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/skins/wordpress/ ----
==> DIRECTORY: http://172.18.102.122/weblog/wp-includes/js/tinymce/skins/wordpress/images/

---- Entering directory: http://172.18.102.122/weblog/wp-includes/js/tinymce/skins/wordpress/images/ ----
                                                                           s/images/zt
```

7. You can typing direktories “pico /etc/hosts” and typing ip your target



```
  GNU nano 2.8.7                                                        File: /etc/hosts

127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

                                                             [ Read 7 lines ]
^G Get Help     ^O Write Out    ^W Where Is     ^K Cut Text     ^J Justify      ^C Cur Pos      M-U Undo        M-A Mark Text   M-] To Bracket  M-↑ Previous
^X Exit         ^R Read File    ^\ Replace      ^U Uncut Text   ^T To Spell     ^_ Go To Line   M-E Redo        M-6 Copy Text   M-W WhereIs Next M-↓ Next
```

8. You can access from web browser



Username or Email Address

Password

☐ Remember Me

Log In

Name: Madara Uciha

9. you can use sql injection to log in and enter the dashboard page

10.